

"İŞ, GÜÇ" ENDÜSTRİ İLİŞKİLERİ VE İNSAN KAYNAKLARI DERGİSİ

"IS, GUC" INDUSTRIAL RELATIONS AND HUMAN RESOURCES JOURNAL

2018 Cilt/Vol: 20/Num:4 Sayfa/Page: 91-112

Editörler Kurulu / Executive Editorial Group

Aşkın Keser (Uludağ University)
K. Ahmet Sevimli (Uludağ University)
Şenol Baştürk (Uludağ University)

Editör / Editor in Chief

Şenol Baştürk (Uludağ University)

Yayın Kurulu / Editorial Board

Doç. Dr. Erdem Cam (Ankara University)
Yrd. Doç. Dr. Zerrin Fırat (Uludağ University)
Prof. Dr. Aşkın Keser (Uludağ University)
Prof. Dr. Ahmet Selamoğlu (Kocaeli University)
Yrd. Doç. Dr. Ahmet Sevimli (Uludağ University)
Prof. Dr. Abdulkadir Şenkal (Kocaeli University)
Doç. Dr. Gözde Yılmaz (Marmara University)
Yrd. Doç. Dr. Memet Zencirkıran (Uludağ University)

Uluslararası Danışma Kurulu / International Advisory Board

Prof. Dr. Ronald Burke (York University-Kanada)
Assoc. Prof. Dr. Glenn Dawes (James Cook University-Avustralya)
Prof. Dr. Jan Dul (Erasmus University-Hollanda)
Prof. Dr. Alev Efendioğlu (University of San Francisco-ABD)
Prof. Dr. Adrian Furnham (University College London-İngiltere)
Prof. Dr. Alan Geare (University of Otago- Yeni Zelanda)
Prof. Dr. Ricky Griffin (TAMU-Texas A&M University-ABD)
Assoc. Prof. Dr. Diana Lipinskiene (Kaunos University-Litvanya)
Prof. Dr. George Manning (Northern Kentucky University-ABD)
Prof. Dr. William (L.) Murray (University of San Francisco-ABD)
Prof. Dr. Mustafa Özbilgin (Brunel University-UK)
Assoc. Prof. Owen Stanley (James Cook University-Avustralya)
Prof. Dr. Işık Urla Zeytinoğlu (McMaster University-Kanada)

Ulusal Danışma Kurulu / National Advisory Board

Prof. Dr. Yusuf Alper (Uludağ University)
Prof. Dr. Veysel Bozkurt (İstanbul University)
Prof. Dr. Toker Dereli (Işık University)
Prof. Dr. Nihat Erdoğan (İstanbul Şehir University)
Prof. Dr. Ahmet Makal (Ankara University)
Prof. Dr. Ahmet Selamoğlu (Kocaeli University)
Prof. Dr. Nadir Suğur (Anadolu University)
Prof. Dr. Nursel Telman (Maltepe University)
Prof. Dr. Cavide Uyargil (İstanbul University)
Prof. Dr. Engin Yıldırım (Anayasa Mahkemesi)
Prof. Dr. Arzu Wasti (Sabancı University)

İş, Güç, Endüstri İlişkileri ve İnsan Kaynakları Dergisi, yılda dört kez yayınlanan hakemli, bilimsel elektronik dergidir. Çalışma hayatına ilişkin makalelere yer verilen derginin temel amacı, belirlenen alanda akademik gelişime ve paylaşım katkıda bulunmaktadır. "İş, Güç," Endüstri İlişkileri ve İnsan Kaynakları Dergisi, 'Türkçe' ve 'İngilizce' olarak iki dilde makale yayınlanmaktadır.

"Is, Güc" The Journal of Industrial Relations and Human Resources is peer-reviewed, quarterly and electronic open sources journal. "Is, Güc" covers all aspects of working life and aims sharing new developments in industrial relations and human resources also adding values on related disciplines. "Is, Güc" The Journal of Industrial Relations and Human Resources is published Turkish or English language.

TARANDIĞIMIZ INDEXLER



Dergide yayınlanan yazılardaki görüşler ve bu konudaki sorumluluk yazarlarına aittir.
Yayınlanan eserlerde yer alan tüm içerik kaynak gösterilmeden kullanılamaz.

All the opinions written in articles are under responsibilities of the authors.
The published contents in the articles cannot be used without being cited

“İş, Güç” Endüstri İlişkileri ve İnsan Kaynakları Dergisi - © 2000-2018

“Is, Guc” The Journal of Industrial Relations and Human Resources - © 2000-2018

İÇİNDEKİLER

Yıl: 2018 / Cilt: 20 Sayı: 4

SIRA	MAKALE BAŞLIĞI	SAYFA NUMARALARI
1	Prof. Dr. Nuran Bayram Arlı, Arş. Gör. Mine Aydemir, Arş. Gör. Elif Çelik, “Çalışan Kıskançlığı Ölçeğinin Türkçe Geçerlik Ve Güvenirlik Çalışması”,	5
2	Doç. Dr. Sedat BOSTAN, Arş. Gör. Eyyüp YILDIZ, “Kamu ve Özel İşletmelerin Acil Durum Planlarının İncelenmesi Üzerine Bir Araştırma”	23
3	Prof. Dr. Özlem ÇAKIR, Yavuz TANĞ “Türkiye’de Sağlık Çalışanlarında Tükenmişlik Sendromu: Bir Meta Analiz Çalışması”	43
4	Prof. Dr. Deniz KAĞNICIOĞLU, Dr. Öğr. Üyesi Emin Cihan DUYAN, Arş. Gör. Dr. Hilmi ETCİ “Y Kuşağının Kariyer Değerleri ve Kişilik Özelliklerinin Araştırılması Ve Karşılaştırılması”	65
5	Doç. Dr. Kurtuluş KAYMAZ, Halil ERBİ, “Bilgi Güvenliğinde Stres Faktörlerinin İş Tatmini Üzerindeki Etkileri: Ar-Ge Merkezi Olan İşletmeler Üzerinde Bir Araştırma”	95
6	Mert Okan YAZICI, Doç. Dr. Barış SEÇER “İşe Alma ve Yerleştirmede Nepotizm”	117
7	Dr. Öğr. Üyesi Memet ZENCİRKIRAN “1980’li Yıllarda Türkiye’de Ekonomide Yaşanan Değişimler	141
8	Arş. Gör. Mehmet ÖÇAL, Prof. Dr. Adem KORKMAZ, “Türkiye’de Çalışma Ekonomisi Ve Endüstri İlişkileri Bölümlerinin Yeniden Yapılanma Sorunsalı Üzerine Bir Araştırma”	163

BİLGİ GÜVENLİĞİNDE STRES FAKTÖRLERİNİN İŞ TATMİNİ ÜZERİNDEKİ ETKİLERİ: AR-GE MERKEZİ OLAN İŞLETMELER ÜZERİNDE BİR ARAŞTIRMA

Kurtuluş KAYMAZ¹

Uludağ Üniversitesi

İktisadi ve İdari Bilimler Fakültesi

İşletme Bölümü, Yönetim ve Organizasyon Ana Bilim Dalı

Görükle Kampüsü, Bursa, Türkiye

kurtuluskaymaz@uludag.edu.tr

Halil Erbi²

Uludağ Üniversitesi

Sosyal Bilimler Enstitüsü

İşletme Ana Bilim Dalı

Görükle Kampüsü, Bursa, Türkiye

halilerbi@prysmiangroup.com

ÖZET

Bilgi ve iletişim teknolojilerinin yoğun kullanımına bağlı olarak elektronik ortamda bilgi güvenliğinin sağlanması bir gereklilik haline gelmiştir. Siber ortamda gerçekleştirilen ataklar ve bilgi kaybı olasılığı işletmeleri bilgi güvenliğine yatırım yapmaya zorlamaktadır. Bilgi güvenliği olgusu çoğu zaman teknoloji temelli önlemleri gerekli kılıyor gibi görünse de insanın bu süreçteki rolü zamanla daha fazla fark edilmektedir. Kurumsal açıdan bakıldığında, bilgi kaybı ile sonuçlanan vak'aların çoğunda insandan kaynaklı hataların olduğu görülmektedir. Dolayısıyla insan unsurunu, bilgi güvenliği politikaları ile uyumlu davranmaya zorlayan yöntemler geliştirilmeye çalışılmaktadır. Bu zorlayıcı mekanizma, daha az hata yapmaya imkân vermekle birlikte bireyin, bilgi güvenliği politikalarına uyum sağlarken fazladan iş yüküne maruz kalmasına, kişisel bilgilerinin ihlal edilmesine, bürokrasiye bağlı zaman kaybına uğramasına ve gerilim yaşamasına neden olmaktadır. Dolayısıyla bu araştırma, işletmelerin bilgi güvenliği gerekliliklerini yerine getirirken uygulamış oldukları politikalara uyum sağlamaya çalışan bireyin maruz kaldığı iş engellerinin ve gizlilik ihlallerinin, bilgi güvenliğinde stres ve iş tatmini üzerindeki etkilerini ölçümlemeyi amaçlamaktadır. Araştırma, Ar-Ge merkezi olan işletmeler üzerinde gerçekleştirilmiştir. Araştırmada iki önemli bulguya ulaşılmıştır. İlk bulgu, bilgi güvenliği uygulamalarının yarattığı iş engellerinin ve gizlilik ihlallerinin, bilgi güvenliğinde stres üzerinde etkili olduğu yönündedir. İkinci bulgu ise bilgi güvenliğinde stres değişkeninin, iş tatminini negatif yönde etkilediği doğrultusundadır.

Anahtar Kelimeler: *Bilgi güvenliği, iş engeli, gizlilik ihlali, bilgi güvenliğinde stres, iş tatmini*

1 Doç.Dr.

2 Yüksek Lisans Öğrencisi

THE EFFECTS OF INFORMATION SECURITY STRESSORS ON JOB SATISFACTION: A RESEARCH ON R&D STRUCTURED ORGANIZATIONS

ABSTRACT

Depending upon the intensive usage of information and communication technologies, providing the security of information became as a requirement. The attacks in cyberspace and possibility of losing the information forced organizations invest on information security. The information security concept seem to be more related to technology at first but the role of human in this process became realized recently. From the perspective of organizations, there are human based errors most while losing the datas. Therefore, organizations try to develop methods force human to comply with the information security policies. This normative mechanism help individuals to make less errors but on the other side complying with the information security policies bring workload, impediments, invasion of privacy, time loss and strain. This research is aimed to determine the effects of impediments and invasion of privacy on the information security stress and job satisfaction while complying with the information security requirements. The study is conducted in R&D structured organizations. We reached two main findings. First, impediments and invasion of privacy are the information security stressors. Second, information security stress has a negative effect on the job satisfaction.

Key Words: *Information security, work impediment, invasion of privacy, information security stress, job satisfaction.*

GİRİŞ

Bilgi güvenliği riskleri, iş ve sosyal yaşamı gittikçe daha fazla oranda tehdit etmektedir. World Ekonomik Forum 2016 Raporu'na göre siber saldırılar, Global Risk listesinde bir teknoloji riski olarak tanımlanmaktadır. Aynı raporda, veri hırsızlığı en önemli 10 Global Risk sıralamasında 8.sırada yer almaktadır. MMC Cyber Handbook (2018) verilerine göre, 2016 yılında 1.1 milyar kullanıcı siber açıklar nedeniyle saldırıya maruz kalmıştır. Son 8 yılda sözkonusu rakam 7.1 milyar kullanıcı seviyesindedir. Aynı raporda, fidye amaçlı kötü yazılım açısından, 2016 yılında 463.841 adet atakta, ortalama 1.077 dolar seviyesinde fidyenin temin edildiği görülmektedir. Özellikle siber saldırıların belirgin şekilde enerji, sağlık, perakende ve toptan satış, finans ve üretim endüstrilerinde yoğunlukta olduğu ifade edilmektedir. Diğer bir raporda (The Global State of Information Security Survey-2018), Singapur'da 2017 yılında maruz kalınan siber saldırıların %38'inin mevcut çalışanların hatalarından kaynaklandığı belirtilmektedir. Data Breach Investigations Raporu'nda (2017), çalışanların dışarıdan saldırılarda çoğu zaman rasyonel olarak kullanılan bir kurum içi işbirlikçi olduğu, çalışanların bu tarz işbirliklerini para kazanmak için yaptıkları, bu nedenle çalışanların işleri ile doğrudan bağlı olmayan bilgilere erişimlerinin sınırlandırılması gerektiği ve gözlem altında tutulmalarının yararlı olacağı belirtilmektedir. Bir başka raporda (Klahr vd., 2017) ise siber saldırıların hep dış kaynaklı olmadığı, çalışanların yaptıkları hatalar, güncel olmayan program kullanma, güvenilir olmayan anti-virüs programları kullanma ya da çalışanların siber güvenlik konularındaki bilgi ve farkındalık eksikliklerinin önemli açıklar yarattığı belirtilmektedir.

Bu araştırma, bilgi güvenliği uygulamalarında ortaya çıkan stres faktörlerinin çalışanların iş tatmini üzerindeki etkilerini analiz etmeyi amaçlamaktadır. Bilgi güvenliği literatüründe, birey odaklı çalışmalar son derece sınırlıdır. Bilgi güvenliği politikalarına bireyin uyumu ve farkındalık geliştirme üzerine çalışan Bulgurcu vd. (2010), bilgi güvenliğine uyumda stres faktörlerini analiz eden Lee vd. (2016), tekno-stres ve iş tatmini arasındaki ilişkileri inceleyen Ayyagari vd. (2011) ilgili literatürde öne çıkan çalışmaları oluşturmaktadır. Bununla paralel olarak, teknoloji bazlı stres ve iş tatmini arasındaki ilişkileri inceleyen farklı araştırmalar da mevcuttur (Jena, 2015; Khan vd. 2013; Kinman ve Jones, 2005; Qiu, 2013).

Bilgi güvenliği uygulamalarında genel anlamda çalışanların nasıl davranmaları gerektiği konusu ihmal edilmektedir. Bilgi güvenliği alanı çoğu zaman teknolojik bir bakış açısıyla değerlendirilmekte, kulancı perspektifi ikinci plana atılmaktadır. Çoğu zaman teknoloji temelli çözümler (firewalls, antivirus software and VPNs) güvenlik sorunlarını gidermek için tatmin edici sonuçlar üretememektedir. Dolayısıyla, çalışanların bilgi güvenliği politikalarına uygun hareket etmelerini sağlayacak yönetsel önlemler önem kazanmaktadır (Kirsch ve Boss, 2007). Özellikle bireyin farkındalık düzeyini geliştirmek, eğitim almasını sağlamak gibi uygulamalar ile bilgi güvenliği politikalarına olan uyumun hızlandırılmaya çalışıldığı görülmektedir (Kim vd., 2014). Bilgi teknolojileri, siber saldırılara karşı koymak açısından "insani" en kritik değişken olarak tanımlanmaktadır. İnsan odaklı hatalar, teknik hatalara nazaran daha ciddi ve derin bilgi güvenliği açıkları yaratmaktadır (Ahmed vd., 2012; Pollock, 2017). Ahmed vd., insan kaynaklı hataları 3 sınıfa ayırmaktadır. Bunlar; çalışanların beceri eksikliğinden kaynaklı hatalar, bilgi güvenliği politikaları kapsamında oluşturulan kurallara uygun hareket etmemekten kaynaklı hatalar ve çalışanların bilgi eksikliklerinden kaynaklı hatalar. Lewis (2003), ekonomik kayıpla sonuçlanan bilgi güvenliği açıklarının %65'inin insan unsurundan kaynaklı olduğunu belirtmektedir.

Araştırma, Şekil 1'de ifade edilen model esas alınarak yapılandırılmıştır. Çalışmada, öncelikle literatür gözden geçirilmiş, model çerçevesinde test edilecek hipotezler oluşturulmuştur. Elde edilen sonuçlar ilgili yazındaki benzer çalışmalar ile karşılaştırmalı olarak tartışılmıştır. Araştırma, kısıtların ve gelecek çalışma kapsamının belirtilmesi ile tamamlanmıştır.

Teorik Çerçeve

Planlı Davranış Teorisi ve Kişi-Çevre Uyumu Modeli

Bilgi güvenliği davranışı literatüründe bu çalışma ile bağlantılı iki teori öne çıkmaktadır. Bunlar; planlı davranış teorisi (*planned behavior theory*) ve kişi-çevre uyumu modeli (*person-environment fit model*) dir. "*Theory of reasoned action*" (Ajzen ve Fishbein, 1980) perspektifinin genişletilmiş versiyonu olarak planlı davranış teorisinin odağında, bir davranışa yönelimi sağlayan "niyet" bulunmaktadır. Bu bağlamda niyet, bir davranışı sergilemek için bireyin ne kadar istekli olduğunu, ne kadarlık bir efor sarf etmeyi planladığını göstermektedir. Bir davranışa yönelik niyetin gücü bir anlamda sergilenen performansın da bir göstergesidir. Planlı davranış teorisi, niyete etki eden üç değişkenin olduğunu ifade etmektedir. Bunlar; davranışa yönelik tutum, subjektif normlar ve öz-yeterlilik (Ajzen, 1991). Planlı davranış teorisi çerçevesinde bu araştırma, bilgi güvenliğinde tutuma etki ettiği varsayılan iş engeli, gizlilik ihlali ve bilgi güvenliğinde stres değişkenleri üzerine odaklanmaktadır.

Kişi-çevre uyumu modeli ise bireysel karakteristikler (beceriler, yetenekler, ihtiyaçlar, arzular, değerler, hedefler, kişilik) ile çevre arasında uyumun derecesi olarak tanımlanmaktadır (Kristof, 1996). Bireysel beceriler, ihtiyaçlar, değerler vb. ile çevre arasındaki uyumun artması çalışanların iş tatmini ve performansını da artırmaktadır (Ostroff ve Schulte, 2007; Dawis ve Lofquist, 1987). Kavram zamanla, kişi-iş, kişi-grup, kişi-yönetici ve kişi-örgüt uyumu biçiminde farklı düzeylerde ele alınmıştır. Bu çalışma, birey-organizasyon uyumu çerçevesinde, çalışanların bilgi güvenliği davranışları ile organizasyonun bilgi güvenliği hedefleri arasındaki uyuma odaklanmaktadır. Birey-çevre ya da daha spesifik düzeyde birey-organizasyon uyumsuzluğunun her iki taraf açısından stres yaratacağı (Edwards vd., 1998) savından hareket edilmektedir. Dolayısıyla, bireyin bilgi güvenliği davranışı ile organizasyonun bilgi güvenliği politikaları arasında uyum dengesi bozuldukça hem birey hem de örgüt açısından stres düzeyi artmaktadır. Bilgi güvenliği uygulamaları bazında gizlilik ihlali ve iş engelleri konusunda çalışanların örgütsel beklentilere cevap verememesinin ve çalışanların yetkinlik düzeylerinin organizasyonel gereklilikler ile uyumsuz olmasının bilgi güvenliği uygulamalarında stres yaratacağı varsayılmaktadır.

Gizlilik İhlali ve İş Engeli

OECD, 1980 yılından bu yana, uluslararası konsensüs ile kamu ve özel sektörde kişisel bilgilerin korunması ve gizliliğin sağlanması yönünde rehber yayınlamaktadır. Bilgi güvenliği açıkları, sağlık hassasiyetleri gibi doğrudan insan hayatını tehdit etmese de, bireyler güvenli bir ortamda bilgi teknolojilerini kullanmayı tercih etmektedirler. İnsanlar, olası bilgi güvenliği tehditlerini fark etmiyor olsalar da, kişisel bilgilerin çalınması, silinmesi, değiştirilmesi ya da kişisel bilgilere ulaşımın engellenmesi gibi risklerle her an karşı karşıyadırlar (Siponen, 2000). Bu bağlamda bakıldığında, güvenlik ve gizlilik, bilişim teknolojilerinin kullanımında bireylerin en hassas oldukları iki noktayı oluşturmaktadır (Turn ve Ware, 1976) ve bilgi teknolojilerinin gelişimine bağlı olarak evrim geçirmektedir (Wieczorkowski ve Polak, 2017). Daha geniş networklerin oluşması, internet kullanıcılarının sayısının artması, bilgi teknolojileri altyapılarının gelişmesi ve özel/kamu sektörlerinin temel faaliyetlerini yerine getirmeleri için bilgi teknolojilerine olan ihtiyaçlarının artması, bilgi güvenliği ve gizlilik unsurlarını zamanla daha fazla önemli hale getirmiştir (OTA, 1994). Buna karşın, bilgi güvenliği tehditleri ve buna bağlı oluşan kişisel düzeydeki gizlilik ihlalleri (*invasion of privacy*) aynı zamanda stres yaratan bir faktör olarak görülmektedir. Lee vd. (2016) tarafından, bilgi güvenliğinde stres faktörleri üzerine gerçekleştirilen bir araştırmanın bulguları, gizlilik ihlalinin, bilgi güvenliğinde stres yaratan bir değişken olduğunu doğrulamaktadır. Genel olarak ihlal, birçok çalışmada da (Wang vd., 2008; Shu vd., 2011; Tarafdar vd., 2007; Ragu-Nathan vd., 2008) bir tekno-stress kaynağı olarak değerlendirilmektedir.

İş engeli (*work impediment*), bilgi güvenliği uygulamalarında stres yaratan diğer bir faktör olarak görülmektedir. Bulgurcu vd. (2010) iş engelini, bir çalışanın bilgi güvenliği politikalarına uyum sağlamaya çalışırken günlük olarak işiyle ilgili görevleri yerine getirmesini engelleyen ya da zarar veren durum olarak tanımlamaktadır. Çalışmada iş engeli, çalışanlar tarafından bilgi güvenliği politikalarına uyum getirdiği bir maliyet olarak değerlendirilmektedir. Aynı çalışmada, bilgi güvenliği gereksinimlerinin zaman kaybı yarattığı ve bu yönüyle bilgi güvenliği politikalarına uygun tutum geliştirme sürecine iş engellerinin negatif yönde etkilerinin olduğu bulgulanmıştır. Diğer bir çalışmada (Li, 2015), bilgi güvenliği politikalarının yarattığı iş engellerinin, kullanıcıların yararlı olabilecek güvenlik aksiyonları (IT departmanının desteğini alma, izleme faaliyetlerinde bulunma) almalarını engelleyen ya da güçleştiren unsurlar olduğu ifade edilmektedir. Bilgi güvenliği politikaları, çalışanlar için belirli oranlarda iş yükü yaratmakta, iş yükü ise zaman kaybı yaratmaktadır. Söz konusu zaman kaybı ise iş engeli oluşturmaktadır (Frangopoulos vd., 2013). Bilgi güvenliği uygulamalarının yarattığı yüksek düzeyde iş yükü, bilgi güvenliği sisteminin fonksiyonel düzeyde zayıflamasına, insan kaynaklı hataların ortaya çıkmasına ve bir bütün olarak bilgi güvenliği sisteminin performansının düşmesine neden olmaktadır (Kraemer, 2009). Aşırı iş yükü aynı zamanda bilgisayar kullanıcılarının da performansını düşürecek etkiler yaratmaktadır.

Bilgi Güvenliğinde Stres ve İş Tatmini

Bilgi güvenliğinde stres kavramı, tekno-stres olgusu ile doğrudan ilişkilidir. Tekno-stres kavramı, bilgi ve iletişim teknolojilerinin gelişimine paralel olarak, çoğunlukla yeni teknolojilere uyum sağlanmakta zorlanılan, çalışanların görevlerini yerine getirmeleri için gereken düzeyde beceriye ya da yetkinliğe sahip olmadığı koşullarda ortaya çıkan (Tarafdar vd., 2007; Park ve Im, 2012) teknoloji kaynaklı stres durumunu ifade etmek için kullanılmaktadır. Yoğun cep telefonu ve bilgisayar kullanımı, e-mail trafiği, elektronik mesajlaşma, gün içinde yoğun telefon görüşmeleri, devamlı surette şifre kullanma/güncelleme, yazılım güncelleme, siber saldırılara maruz kalma vb. faktörler teknolojik bazı strese neden olabilmektedir. Bilişim ortamında bilgiyi kaybetme korkusu, kişisel bilgilerin ihlali ve güvenlik sorunu,

hızlı işlem yapmaya bağlı hata yapma korkusu, teknoloji temelli iş yükü artışı olası tekno-stres kaynakları arasında gösterilmektedir. (Mahboob ve Khan, 2016; Salanova vd., 2013).

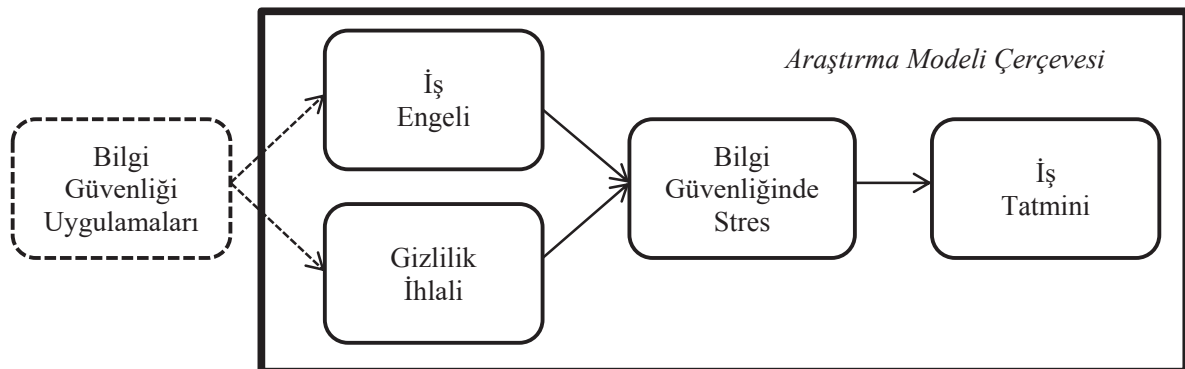
İlgili literatürde, tekno-stres ile iş tatmini arasındaki ilişkiyi irdeleyen araştırmalara rastlamak mümkündür. Nagu-Rathan vd. (2008), yapısal eşitlik modellemesi ile 608 son kullanıcı üzerinde gerçekleştirdikleri bir araştırmanın sonuçlarına göre; tekno-stres yaratan faktörlerin (tekno-işyükü, tekno-ihlal, tekno-karmaşıklık, tekno-güvenlik ve tekno-belirsizlik) iş tatminini azalttığı yönünde bulgulara ulaşılmıştır. Bir başka araştırmada (Taraftar vd., 2011), tekno-stres faktörlerinin psikolojik ve davranışsal gerginlik üzerindeki etkileri incelenmiş, teknoloji temelli stres unsurlarının çalışanların iş tatminini azaltıcı etkilerinin olduğu bulgulanmıştır. Aynı araştırmada ayrıca tekno-stres faktörlerinin örgütsel bağlılık, yenilikçi davranış ve kullanıcı tatminini olumsuz yönde etkilediği de ifade edilmektedir. Benzer biçimde diğer araştırmalar da (Jena, 2015; Kumar vd., 2013), tekno-stresin iş tatmini üzerinde negatif etkiye sahip olduğu bulgusuna ulaşmışlardır. Tekno-stres sadece iş tatminini değil, benzer biçimde çalışanların verimini düşürecek etkiler de ortaya çıkarmaktadır (Tu vd., 2005).

Bilgi güvenliği, yönetsel, fiziksel ve teknolojik kontrol olmak üzere 3 boyutlu bir yapıyı gerekli kılmaktadır. Yönetsel güvenlik boyutu; bilgi koruma politikası oluşturmak, örgütsel yapı ve bağlantılı sorumlulukları tasarlamak, kritik bilgi varlıklarını tanımlamak, süreci yönetecek işgücünü istihdam etmek, gelecek kriz senaryoları oluşturmak ve sistematik denetimler yapmak olarak ifade edilebilecek faaliyetler içermektedir. Teknolojik kontrol boyutu; bilgisayarların ve networklerin yönetimi, sistem giriş kontrolleri, sistem geliştirme, bakım kontrolleri gibi çalışmalarını gerekli kılmaktadır. Fiziksel kontrol boyutunda ise bilgisayar ünitelerinin ve gerekli malzeme ihtiyaçlarının yönetimi gündeme gelmektedir (Jeong ve Jeong, 2011). Bu bağlamda, bir tekno-stres kaynağı olarak bilgi güvenliği uygulamalarının yarattığı sorumluluklar ve iş yükü çalışanlar nezdinde stres yaratabilmektedir ve bu stres faktörü çalışanların iş tatminini negatif yönde etkilemektedir (Park ve Cho, 2016). Bulgurcu vd. (2010), bilgi güvenliği uygulamalarının ortaya çıkardığı iş engellerinin çalışanlar nezdinde stres yarattığını bulgulamışlardır.

Araştırma Modeli ve Hipotezler

Bilgi güvenliği uygulamalarının yarattığı iş engeli, gizlilik ihlali ve stresin iş tatmini üzerindeki etkilerini analiz etmek üzere Şekil 1'deki model esas alınmıştır. İş engeli, gizlilik ihlali ve stres bağımsız değişkenler olarak modele dahil edilirken, iş tatmini bağımlı değişken olarak belirlenmiştir. Bu kapsamda ilgili model ve hipotezler aşağıda ifade edilmektedir.

Şekil 1: Araştırma Modeli



Model baz alınarak oluşturulan ve test edilen temel hipotezler aşağıda sıralanmaktadır.

H1: Bilgi güvenliği uygulamalarının yarattığı iş engelleri, stres değişkeni üzerinde pozitif etkiye sahiptir.

H2: Bilgi güvenliği uygulamalarının yarattığı gizlilik ihlali, stres değişkeni üzerinde pozitif etkiye sahiptir.

H3: Bilgi güvenliği uygulamalarının yarattığı stres, çalışan tatmini üzerinde negatif etkiye sahiptir.

Metod, Örneklem ve Ölçekler

Veriler, anket yöntemi kullanılarak toplanmıştır. Veri güvenliğini sağlamak üzere, anketlerin tüm katılımcılarla yüz yüze olacak biçimde doldurulmasını sağlanmıştır. Ankette yer alan ifadelerin ne derecede anlaşıldığını test etmek, ön geçerlilik ve güvenilirlik analizlerini yapmak üzere toplam 50 anketten oluşan bir pilot çalışma gerçekleştirilmiştir. Pilot çalışma kapsamında, gizlilik ihlali soru grubunda yer alan ve anlamları çok yakın olarak algılanan 2 ifade birleştirilerek, tek ifade haline dönüştürülmüştür.

Araştırmanın ana kütesini, Bursa'da faaliyet gösteren ve 5746 sayılı Araştırma, Geliştirme ve Tasarım Faaliyetlerinin Desteklenmesi Hakkında Kanun uyarınca kurulmuş Ar-Ge Merkezi olan üretim işletmeleri oluşturmaktadır. Sözkonusu statüde Ar-Ge Merkezi olan işletmelerin tercih edilmesinin nedeni, bu işletmelerde marka, patent, endüstriyel tasarım ve faydalı model geliştirme çalışmalarının yoğun olması ve bu yolla üretilen bilginin gelişmiş bir bilgi güvenliği sistemini gerekli kılmasıdır. Bu kapsamda, Bursa'da 87 Ar-Ge Merkezi statüsüne sahip işletme bulunmaktadır. Ancak, bu denli geniş bir ana kütleyle ulaşmak maliyet ve zaman açısından mümkün değildir. Bu nedenle veriler belirli bir örneklem üzerinden elde edilmiştir. Örneklem, "kartopu örnekleme" tekniğine dayanılarak toplanmıştır. Pilot çalışma sonrasında ankette gerekli revizyonlar tamamlanmış ve uygulama gerçekleştirilmiştir. Araştırmada özellikle bilgi güvenliğinin daha fazla önemsendiği, ISO 27001 bilgi güvenliği sertifikasyonu olan ve bilgi güvenliği politikalarıyla uyumlu süreçler geliştirmiş firmalar tercih edilmiştir. Bu kapsamda, otomotiv, tekstil, cam ve kablo endüstrilerinden olmak üzere toplam 215 çalışan üzerinde anket uygulaması gerçekleştirilmiştir.

Araştırmada, bağımlı ve bağımsız değişkenler için birden fazla ölçek kullanılmıştır. Ölçeklerde yer alan ifadeler, ilgili literatür taraması sonucu tespit edilmiş birden çok ifadenin içinden, araştırmanın amacına uygun olarak seçilmiştir. Araştırmada ayrıca 2 farklı Likert tipi skala [Kesinlikle Katılmıyorum (1) - Kesinlikle Katılıyorum (5); Hiçbir Zaman (1) - Her Zaman (5)] kullanılmıştır. Araştırma kapsamında kullanılan ölçekler ve istatistiksel nitelikleri aşağıda verilmektedir.

İş Engeli Ölçeği

İş engeli ölçeği, Bulgurcu vd. (2010) çalışmalarında yer alan 3 ifadeden oluşmaktadır. Orijinal araştırmada cronbach alpha değeri 0.92 olarak tespit edilmiştir. Bu araştırmada ise iş engeli ölçeğinin cronbach alpha katsayısı 0.88 seviyesindedir. İş engeli ölçeğinde, Hiçbir Zaman (1) - Her Zaman (5) skalası kullanılmıştır.

Gizlilik İhlali Ölçeği

Gizlilik ihlali ölçeği, Ayyagari vd. (2011) tarafından geliştirilen 4 ifadeden oluşmaktadır. Orijinal ölçekteki ifadelerden sadece 3 tanesi araştırmaya dahil edilmiştir. Sözkonusu ifadeler için orijinal kaynakta tespit edilen cronbach alpha değeri 0.88 değerinin üzerindedir. Bu araştırmada ise 3 ifadenin cronbach alpha katsayısı 0.87 olarak tespit edilmiştir. Ölçekte, Kesinlikle Katılmıyorum (1) - Kesinlikle Katılıyorum (5) skalası kullanılmıştır.

Bilgi Güvenliğinde Stres Ölçeği

Bilgi güvenliğinde stres ölçeği, Ayyagari vd. (2011) tarafından geliştirilmiştir ve 8 ifadeden oluşmaktadır. Orijinal ölçekte cronbach alpha değeri 0.88 değerinin üzerinde tespit edilmiştir. Bu araştırmada ise stres ölçeği için belirlenen güvenilirlik katsayısı 0.93 düzeyindedir. Ölçekte, Kesinlikle Katılmıyorum (1) - Kesinlikle Katılıyorum (5) skalası kullanılmıştır.

İş Tatmini Ölçeği

İş tatminini ölçümlemek üzere Cammann vd. (1983) tarafından kullanılan 2 ifadeye yer verilmiştir. Camman vd. araştırmalarında iş tatmini ölçeğinin güvenilirlik katsayısını 0.90 olarak tespit etmişlerdir. Sözkonusu iki ifade için bu araştırmada cronbach alpha katsayısı 0.89 olarak bulgulanmıştır. Ölçekte, Kesinlikle Katılmıyorum (1) - Kesinlikle Katılıyorum (5) skalası kullanılmıştır.

Tüm ölçeğin güvenilirlik katsayısı 0.89 seviyesindedir. Ölçeklerde yer alan ifadeler Tablo 1'de gösterilmektedir.

Tablo 1: Modelde yer alan değişkenlere ait ölçekler, ifadeler ve kaynaklar

Değişkenler	İfadeler	Kaynak
İş Engeli	<ol style="list-style-type: none"> 1. Bilgi güvenliği gerekliliklerini yerine getirirken günlük olarak yaptığım işi aksatabiliyorum. 2. Bilgi güvenliği gerekliliklerini yerine getirirken yöneticilerime, çalışma arkadaşlarıma ya da müşterilere zamanında geri dönemiyorum. 3. Bilgi güvenliği gerekliliklerini yerine getirmeye çalışırken işimdeki verimliliğin azaldığını düşünüyorum. 	Bulgurcu vd. (2010)
Gizlilik İhlali	<ol style="list-style-type: none"> 1. İletişim teknolojilerini (e-mail, skype, cep telefonu uygulamaları vb.) kullanırken, bilgi güvenliği kapsamında bile olsa takip ediliyor olmam beni rahatsız ediyor. 2. Bilgi güvenliği faaliyetleri kapsamında izleniyor olmam dolayısıyla özel yaşamımın ihlal edildiğini düşünüyorum. 3. Bilgi güvenliği faaliyetleri neden gösterilerek işverenin çalışanları takip ettiğini düşünüyorum. 	Ayyagari at al. (2011)
Bilgi Güvenliğinde Stres	<ol style="list-style-type: none"> 1. Bilgi güvenliği politikalarının yarattığı gereklilikleri yerine getirirken yorulduğumu hissediyorum. 2. Tüm gün bilgi güvenliği gerekliliklerini yerine getirmek bende stres yaratıyor. 3. Bilgi güvenliği politikalarının yarattığı gereklilikleri yerine getirirken tükenmişimi hissediyorum. 4. Kurumumdaki bilgi güvenliği faaliyetleri kapsamında benden talep edilenler, işimi yaparken ilave yük yaratıyor. 5. Kurumumdaki bilgi güvenliği faaliyetleri kapsamında yürütülen işler problemler yaratabiliyor. 6. Kurumumdaki bilgi güvenliği faaliyetleri kapsamında yürütülen işlerle ilgili şikâyetler duyuyorum. 7. Bilgi güvenliğini ilgilendiren işler beni fazlasıyla meşgul ediyor, zaman kaybına neden oluyor. 8. Bilgi güvenliğini ilgilendiren işleri yaparken baskı altında hissediyorum. 	Ayyagari at al. (2011)
İş Tatmini	<ol style="list-style-type: none"> 1. İşimden genel olarak memnunum. 2. Genel olarak bu kurumda çalışmayı seviyorum. 	Cammann vd. (1983)

Bulgular

Katılımcıların Demografik Profili

Ankette cevaplayıcıların demografik özelliklerinin tespitine yönelik 5 ifadeye (cinsiyet, eğitim, yaş, kıdem, departman) yer verilmiştir. Örneklemin demografik profili Tablo 2'de görülmektedir.

Tablo 2: Katılımcıların Demografik Özellikleri

		N	%
Cinsiyet	<i>Kadın</i>	81	37.7
	<i>Erkek</i>	134	67.3
Yaş	<i>20 yaşına kadar</i>	-	-
	<i>21-30</i>	68	31.6
	<i>31-40</i>	97	45.1
	<i>41-50</i>	39	18.1
	<i>51 ve üstü</i>	11	5.1
Eğitim	<i>İlköğretim</i>	-	-
	<i>Lise</i>	8	3.7
	<i>Ön Lisans</i>	5	2.3
	<i>Lisans</i>	160	74.4
	<i>Yüksek Lisans</i>	39	18.1
	<i>Doktora</i>	3	1.4
Kıdem	<i>1 yıldan az</i>	27	12.6
	<i>1-5 yıl</i>	74	34.4
	<i>6-10 yıl</i>	44	20.5
	<i>11-15 yıl</i>	24	11.2
	<i>16 yıl ve üstü</i>	46	21.4
Departman	<i>Ar-Ge</i>	35	16.3
	<i>Finansman</i>	21	9.8
	<i>Muhasebe</i>	30	14.0
	<i>İnsan Kaynakları</i>	14	6.5
	<i>Satın Alma</i>	6	2.8
	<i>Bilgi İşlem</i>	9	4.2
	<i>Pazarlama Satış</i>	24	11.2
	<i>Lojistik</i>	28	13.0
	<i>Üretim</i>	21	9.8
	<i>Diğer (Kalite, Dış Ticaret, İş Güvenliği)</i>	27	12.6

Korelasyon Analizi

Araştırmada, bağımsız değişkenler arası pozitif ve güçlü ilişkiler tespit edilmiştir (Tablo 3). Bu bağlamda, en güçlü doğrusal ilişki iş engeli ile bilgi güvenliğinde stres değişkeni arasında mevcuttur (0.604). Diğer taraftan gizlilik ihlali ile bilgi güvenliğinde stres arasında da pozitif yönlü ve güçlü bir ilişki bulunmuştur (0.436). İş tatmini ile bilgi güvenliğinde stres değişkeni arasında negatif yönlü doğrusal bir ilişki tespit edilmiştir (-0.194).

Tablo 3: İş engeli, gizlilik ihlali, bilgi güvenliğinde stres ve iş tatmini değişkenleri arasındaki korelasyonlar, ortalama, standart sapma ve cronbach alpha değerleri

	M	Standart Sapma	Cronbach Alpha	İE	Gİ	BGS	İT
İş Engeli (İE)	1.78	0.77	0.88	1			
Gizlilik İhlali (Gİ)	2.84	1.07	0.87	.319**	1		
Bilgi Güvenliğinde Stres (BGS)	1.81	0.73	0.93	.604**	.436**	1	
İş Tatmini (İT)	4.08	0.72	0.89	-.075	-.156*	-.194**	1

** Correlation is significant at the 0.01 level (2-tailed).

* Correlation is significant at the 0.05 level (2-tailed).

Açıklayıcı Faktör Analizi

Araştırmada, yapısal eşitlik modellemesine alt yapı oluşturmak üzere Temel Bileşen Analizi (Principal Components Analysis-PCA) metodu ile faktör analizi uygulanmıştır. KMO ve Bartlett test sonucu (0.876, $\chi^2=2516.882$; $df=120$; $p=.000$), verilerin bir faktör analizi için uygun olduğunu ortaya koymaktadır. Tüm ifadelerin öz değeri 1'den büyük 4 boyut altında toplandığı görülmüştür. 4 boyut için toplam açıklanan varyans %76.2 seviyesindedir. Faktörler ve faktör yükleri dağılımı Tablo 4'de görülmektedir.

Tablo 4: Açıklayıcı Faktör Analizi Sonuçları

İfadeler	Faktör Yükleri				Cronbach Alpha
	1	2	3	4	
İş Engeli					0.88
Bilgi güvenliği gerekliliklerini yerine getirirken günlük olarak yaptığım işi aksatabiliyorum.	.840				
Bilgi güvenliği gerekliliklerini yerine getirirken yöneticilerime, çalışma arkadaşlarıma ya da müşterilere zamanında geri dönemiyorum.	.834				
Bilgi güvenliği gerekliliklerini yerine getirmeye çalışırken işimdeki verimliliğin azaldığını düşünüyorum.	.783				
Gizlilik İhlali					0.87
İletişim teknolojilerini (e-mail, skype, cep telefonu uygulamaları vb.) kullanırken, bilgi güvenliği kapsamında bile olsa takip ediliyor olmam beni rahatsız ediyor.		.900			
Bilgi güvenliği faaliyetleri kapsamında izleniyor olmam dolayısıyla özel yaşamımın ihlal edildiğini düşünüyorum.		.898			
Bilgi güvenliği faaliyetleri neden gösterilerek işverenin çalışanları takip ettiğini düşünüyorum.		.758			
Bilgi Güvenliğinde Stres					0.93

Bilgi güvenliği politikalarının yarattığı gereklilikleri yerine getirirken yorulduğumu hissediyorum.			.817		
Tüm gün bilgi güvenliği gerekliliklerini yerine getirmek bende stres yaratıyor.			.807		
Bilgi güvenliği politikalarının yarattığı gereklilikleri yerine getirirken tükendiğimi hissediyorum.			.776		
Kurumumdaki bilgi güvenliği faaliyetleri kapsamında benden talep edilenler, işimi yaparken ilave yük yaratıyor.			.700		
Kurumumdaki bilgi güvenliği faaliyetleri kapsamında yürütülen işler problemler yaratabiliyor.			.739		
Kurumumdaki bilgi güvenliği faaliyetleri kapsamında yürütülen işlerle ilgili şikâyetler duyuyorum.			.689		
Bilgi güvenliğini ilgilendiren işler beni fazlasıyla meşgul ediyor, zaman kaybına neden oluyor.			.800		
Bilgi güvenliğini ilgilendiren işleri yaparken baskı altında hissediyorum.			.770		
İş Tatmini					0.89
İşimden genel olarak memnunum.				.940	
Genel olarak bu kurumda çalışmayı seviyorum.				.936	

Doğrulayıcı Faktör Analizi

Doğrulayıcı faktör analizi, belirlenen bir ölçme modelinin tutarlılığının istatistiksel olarak anlamlı olup olmadığını test etmek amacıyla yapılmaktadır. Doğrulayıcı faktör analizi, geleneksel yöntemle yapılan faktör analizlerinden farklı olarak, daha önceden araştırmacı tarafından belirlenmiş bir faktöryel yapının doğrulanmasını test etmek amacıyla kullanılmaktadır. Bu tür çalışmalarda, ölçek maddeleri tarafından yapılandırıldığı düşünülen birden fazla örtük (latent) değişkenin, bir başka örtük değişken tarafından açıklandığı varsayılır ve bu varsayımın veriye uygunluğu test edilir.

Model uygunluğunun değerlendirilmesinde kullanılan birbirinden farklı uyum iyiliği indeksleri ve bu indekslerin sahip olduğu istatistiksel fonksiyonlar bulunmaktadır. Analizde, uyum iyiliği indeksi (goodness of fit index-**GFI**), standardize edilmiş kök ortalama kare artık (Standardized **RMR**) ve kök ortalama kare yaklaşım hatası (Root mean square error of approximation-**RMSEA**), Bentler karşılaştırmalı uyum indeksi (Bentler Comparative Fit Index-**CFI**) dikkate alınmaktadır. Söz konusu modelin ölçme gücünün tespitinde yukarıda ifade edilen indekslerin belirli uyum değerlerine sahip olması beklenmektedir. Bu değerler Tablo 5'te yer almaktadır.

Tablo 5: Modelin Uyum Değerleri ve Standart Uyum Ölçütleri

Uyum Ölçüleri	İyi Uyum Değerleri	Kabul Edilebilir Uyum Değerleri
RMSEA	0.00<RMSEA<0.05	0.05<RMSEA<0.10
SRMR	0.00<SRMR<0.05	0.05<SRMR<0.10
GFI	0.95<GFI<1.00	0.90<GFI<0.95
CFI	0.95<CFI<1.00	0.90<CFI<0.95

Elde edilen veriler kapsamında, araştırma modelinin ölçme gücünü veya diğer bir deyimle ölçme aracının geçerliliğini sınamak amacıyla AMOS istatistiksel paket programı aracılığı ile doğrulayıcı faktör analizi yapılmıştır. Analiz çerçevesinde, iş engeli, gizlilik ihlali, bilgi güvenliğinde stres ölçekleri ve tüm model bazında indeks uyum değerleri hesaplanmıştır. Sonuçlar Tablo 6'da görülmektedir. Uyum iyiliği değerlerinin genel olarak kabul edilebilir limitler arasında olduğu ve dolayısıyla ölçme aracının geçerliliğinin bulunduğu tespit edilmiştir.

Tablo 6: Araştırma Modeli Uyum İyiliği Değerleri

	χ^2	df	χ^2/df	GFI	CFI	RMSEA	SRMR
<i>Bilgi Güvenliğinde Stres</i>	40.643	17	2.391	.95	.98	.08	.04
<i>İş Engeli</i>	.00	0	-	1.00	1.00	.71	.00
<i>Gizlilik İhlali</i>	.00	0	-	1.00	1.00	.76	.00
<i>Tüm Model Uyumu</i>	166.391	97	1.715	.91	.97	.06	.06

Normallik testi sonuçlarına bakıldığında, araştırmada kullanılan değişkenlerin çarpıklık ve basıklık değerlerinin genel olarak -1 ile +1 arasında yer aldığı görülmüştür. Skewness ve kurtosis değerlerinin, -1 ile +1 arasında yer alması halinde normallik varsayımının karşılandığı ifade edilmektedir (Kalaycı, 2005).

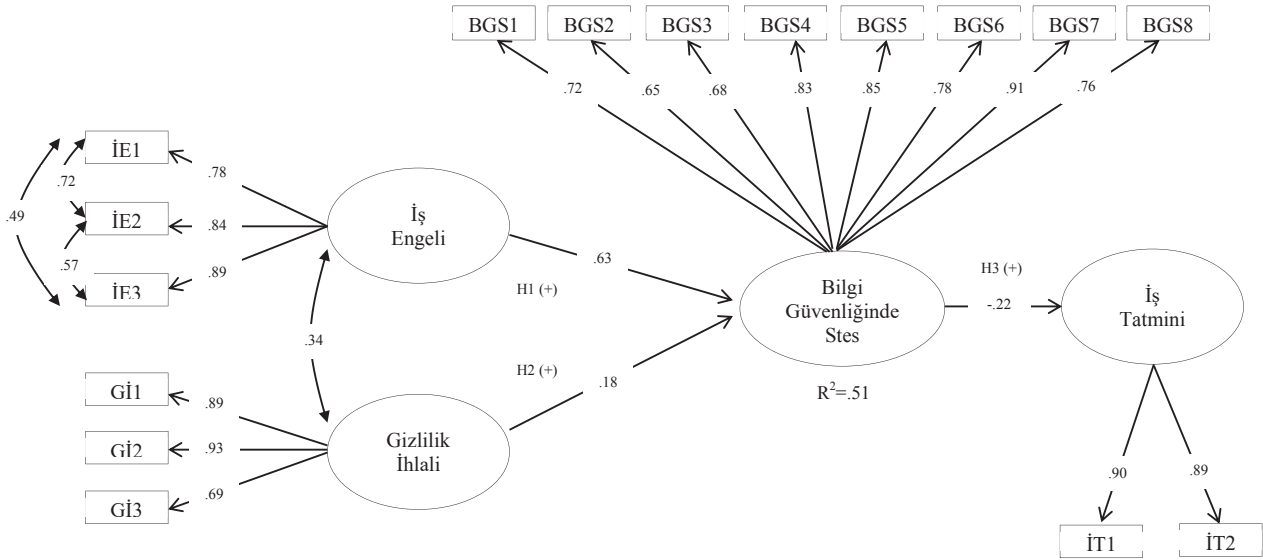
Yapısal Eşitlik Modellemesi Analizi

Modelde yer alan ifadelerin genel anlamda faktör yükleri ve bağımsız değişkenlerin bağımlı değişkeni açıklama düzeyi yüksektir. Bu kapsamda, iş engeli, gizlilik ihlali ve bilgi güvenliğinde stres bağımsız değişkenleri, iş tatmini bağımlı değişkeni ($R^2= 0.51$) düzeyinde açıklamaktadır.

Araştırmanın başlangıcında, iş engeli, gizlilik ihlali ve bilgi güvenliğinde stres değişkenlerinin doğrudan iş tatmini üzerinde etkilerine odaklanılmıştır. Ancak, pilot test aşamasında, doğrulayıcı faktör analizi sonuçları, bilgi güvenliğinde stres değişkeninin bir aracı değişken olduğunu ortaya koymuştur. Bu bağlamda, stres değişkeninin modeldeki yeri değiştirilmiştir.

Yapısal eşitlik modellemesi sonuçları incelendiğinde, iş engelinin, bilgi güvenliğinde stres değişkeni üzerinde pozitif bir etkiye sahip olduğu bulgulanmıştır (parametre tahmini=.618; $p=.000$). Bu bağlamda, "H1: Bilgi güvenliği uygulamalarının yarattığı iş engelleri, stres değişkeni üzerinde pozitif etkiye sahiptir." hipotezi kabul edilmiştir. Diğer taraftan, gizlilik ihlali değişkeninin de bilgi güvenliği değişkeni üzerinde pozitif bir etkiye sahip olduğu tespit edilmiştir (parametre tahmini=.153; $p=.005$). Dolayısıyla, "H2: Bilgi güvenliği uygulamalarının yarattığı gizlilik ihlali, stres değişkeni üzerinde pozitif etkiye sahiptir." hipotezi de kabul edilmiştir. Son olarak, bilgi güvenliğinde stres değişkeninin, iş tatmini üzerindeki etkilerine bakılmıştır. Analiz sonuçları, bilgi güvenliğinde stres değişkeninin, iş tatmini değişkeni üzerinde negatif etkiye sahip olduğunu doğrulamaktadır (parametre tahmini= -.203; $p=.006$). Bu çerçevede, "H3: Bilgi güvenliği uygulamalarının yarattığı stres, çalışan tatmini üzerinde negatif etkiye sahiptir." hipotezi kabul edilmiştir. Genel olarak, araştırmanın tüm hipotezleri kabul edilmiştir. Yapısal eşitlik modellemesi analiz sonuçları toplu olarak Şekil 2'de görülmektedir.

Şekil 2: Yapısal Eşitlik Modellemesi Analiz Sonuçları



$$\chi^2=166.391; df= 97; \chi^2/df= 1.715 (p=.000); GFI=.91; CFI=.97; RMSEA=.06; SRMR=.06$$

Sonuç ve Tartışma

Bilgi güvenliğini sağlamak işletmenin bilgi sermayesini korumak açısından kritik önem taşımaktadır. Bilgi güvenliği politikaları geliştirmek, ISO 27001 Bilgi Güvenliği Sertifikasyonun gerekliliklerini yerine getirmek, bilgi teknolojilerine yatırım yapmak bilgi üreten ve bilgi eksikliğini rekabet eden kurumların stratejik önceliği haline gelmiştir. Maddi nitelik taşıyan girişimler devam ederken, işletmelerin bilgi güvenliği kapsamında beşeri unsurun da bilgi güvenliği politikalarıyla uyumlu davranışlar sergilemesi için çaba harcanmaktadır. İnsan, bilgi güvenliği zincirinin en zayıf halkasını oluşturmaktadır ve güvenliği sağlamada en fazla zorluk çıkaran faktör konumundadır. Çalışanların bilgi güvenliği farkındalıklarının zayıf olması, bilgi kaybının ya da güvenlik zafiyetinin yaratacağı mali kayıplar hakkındaki bilgisizlik, bireysel düzeyde bilgi güvenliği becerilerinden yoksunluk ya da bilgi güvenliği politikaları doğrultusunda yönlendirme eksiklikleri “*insan odaklı*” hataların ortaya çıkmasına neden olmakta, kurum bilgi güvenliği tehdidi altına girmektedir. Dolayısıyla bilgi güvenliğini yaratmada çalışan perspektifi öncelikli alanlardan biri haline gelmiştir.

Bilgi güvenliği politikaları diğer taraftan çalışanları bireysel olarak etkileyecek sonuçlar da yaratmaktadır. Bilgi güvenliği politikalarının yarattığı iş engelleri, gizlilik ihlali oluşturacak takip mekanizmaları, bilgi güvenliği bazında stresin ortaya çıkmasına neden olmaktadır. Genel anlamda, örgütsel stres kaynakları arasında birçok faktör sayılabilmekle birlikte, son zamanlarda teknoloji bazlı stres unsurlarının da örgütsel stresin nedenleri arasında ön plana çıktığı görülmektedir. Kinman ve Jones (2005) çalışmalarında, özellikle yeni teknoloji kullanımının hızlı olmayı gerektirdiğini, düşünmeye zaman kalmadığını ve her şeyin standartlaştığını belirtmekte, bu durumun ise çalışanların stres düzeylerini arttırdığı ifade edilmektedir.

Araştırmada karşımıza çıkan ilk bulgu, bilgi güvenliği uygulamaları kapsamında ortaya çıkan iş engellerinin, bilgi güvenliğinde stres değişkeni üzerinde etkili olduğu yönündedir. Bulguru vd. (2010), araştırmalarında çalışanların bilgi güvenliği politikalarına uyumun belirli oranlarda iş engeli yarattığını, bilgi güvenliği gereklilikleri çerçevesinde çalışanların zaman ayırmaları gerektiğini, bunun da günlük

işleri görel olarak aksattığını bulgulamışlardır. Bu araştırmayla, Bulgurcu vd. bulgusunu tamamlayacak şekilde, bilgi güvenliği politikalarının neden olduğu iş engellerinin bir stres faktörü olduğu ve çalışanları negatif yönde etkilediği ortaya çıkmaktadır. Bu kapsamda, uygulamanın yapıldığı işletmelerde bilgi güvenliği uygulamalarının çalışanların günlük olarak yaptıkları işleri aksatabileceği, zaman yönetimi açısından sorunlar oluşturabileceği, iş verimliliğini azaltacak (Tu vd., 2005) etkiler yaratabileceği ve sözkonusu negatif etkilerin bilgi güvenliğinde stres yaratabileceği yönünde tespitlere ulaşılmıştır. Diğer taraftan Lee vd. (2016) yürüttükleri çalışmalarında, bilgi güvenliği uygulamalarının belirli oranlarda iş yükünü artırdığını ve bunun da çalışanların bilgi güvenli uygulamaları bağlamında strese neden olduğunu doğrulamaktadır. Dolayısıyla araştırmamız Lee vd. bulgularını destekler niteliktedir.

Araştırmada dikkati çeken diğer bir önemli bulgu da bilgi güvenliği uygulamalarının ortaya çıkarıldığı gizlilik ihlali algısının çalışanların stres düzeyini artırmasıdır. Çalışanların, iletişim teknolojilerinin kullanıma bağlı olarak takip edildikleri hissine kapılıyor olmaları, özel yaşantılarının ihlal edildiğini düşünüyor olmaları ve işveren tarafından takip edildiklerine dair algının varlığı bilgi güvenliği kapsamında çalışanlarda stres oluşturmaktadır. Bu sonuç, Ayyagari vd. (2011) çalışmaları ile uyum göstermektedir. Ayyagari vd.'nin tekno-stres üzerine gerçekleştirdikleri araştırmanın bulguları, gizliliğin ihlal edildiğine dair bireysel algı ile stres arasında pozitif yönlü ilişkinin olduğunu ispatlamaktadır. Bilgi güvenliğinde stres faktörlerinin belirlenmesine dönük diğer bir araştırmada ise Lee vd. (2016), gizlilik ihlalinin önemli bir bilgi güvenliği stres unsuru olduğu bulgulanmıştır. Bu yönüyle mevcut araştırma, Lee vd. bulguları ile de paralel sonuçlar yaratmıştır. Gizlilik ihlali, doğrudan internet kullanıcılarının da en fazla hassasiyet gösterdikleri konuların başında gelmektedir. Udo (2001) tarafından, internet ortamında alışveriş yapan kullanıcılar üzerinde gerçekleştirilen bir araştırmada, gizlilik ihlali ve güvenlik açıklarının internette alışveriş yapmayı engelleyen en önemli faktörler olduğu tespit edilmiştir. Dolayısıyla, kişisel gizliliği tehdit eden koşulların bilişim alanında farklı boyutlarda bile olsa bireyleri tedirgin ettiğini söylemek mümkündür.

Araştırmanın en dikkat çekici bulgusu ise bilgi güvenliğinde stres faktörlerinin, çalışanların iş tatmini üzerinde etkisidir. Bu bağlamda, bilgi güvenliği gerekliliklerini yerine getirirken çalışanların yorgunluk, tükenme ve stres hissettikleri ve bunun da iş tatminini negatif yönde etkilediği saptanmıştır. Bilgi güvenliği bağlamında ortaya çıkan stres faktörlerinin (tekno iş yükü ve gizlilik ihlali), teknoloji kaynaklı olduğu varsayımı altında, tekno-stress unsurlarının iş tatminini negatif yönlü etkilediğini ortaya koyan araştırmalara rastlamak mümkündür. Jena (2015), Hindistanlı akademisyenler üzerinde gerçekleştirdiği araştırmasında, tekno-stress faktörlerinin iş tatmini üzerindeki olumsuz etkilerine dikkat çekmiştir. Qiu (2013), tekno-stress ile iş tatmini arasındaki bağ üzerine gerçekleştirdiği çalışmasında, tekno-stress unsurlarının iş tatminini etkileyen önemli bir değişken olduğunu vurgulamaktadır. Benzer biçimde Khan vd. (2013), yine tekno-stress faktörlerinin iş tatminini negatif yönde etkilediğine dair bulgulara ulaşmışlardır. Dolayısıyla, bu araştırmada ortaya çıkan tekno-stress (bilgi güvenliği bağlamında) iş tatmini ilişkisi, literatürdeki benzer çalışmalar ile paralellik göstermektedir.

Genel olarak denilebilir ki, ilk etapta bilişim ana ekseninde düşünülen bilgi güvenliği uygulamalarının esasen beşeri yapı ile çok yakından ilişkisi bulunmaktadır. Bilgi güvenliği politikalarının etkinliği ciddi bir oranda çalışanların uyma davranışı göstermelerine bağlıdır. Çalışanların kişisel ihmali ile ortaya çıkabilecek çok sayıda bilgi güvenliği tehdidi bulunmaktadır. Bilgi güvenliği açıklarının işletmelere mali, yönetsel ve toplumsal düzeyde yük getirdiği düşünüldüğünde, çalışanların ve işletme yönetimlerinin konuya hassasiyetle yaklaşmaları gereği daha net ortaya çıkmaktadır. Bu bağlamda, çalışanların bilgi güvenliği politikalarına uyma davranışı sergilemelerini temin etmek üzere, planlı davranış

teorisinde de vurgulandığı üzere, tutumları etkileyen gizlilik ihlali ve iş engeli faktörlerine karşı daha duyarlı yaklaşmak gerekmektedir.

Araştırmanın Kısıtları ve Gelecek Araştırma

Araştırmanın en önemli kısıtı, bilgi güvenliği konusunun hassasiyet içermesi ve işletmelerin bu konudaki araştırmalara temkinli yaklaşım göstermeleridir. Bir şirketin, çalışanlar bazında bilgi güvenliği açıklarının ortaya çıkması ve bunun paylaşılması çoğu yönetici tarafından olumsuz karşılanmıştır. Bu durum, anket sayısının daha yüksek seviyelere ulaşmasını engellemiştir. Özellikle anketler, bizzat kişisel yakınlıklar üzerinden yürütülerek doldurulmuştur.

Bir sonraki araştırmada, bilgi güvenliği konusunun farklı boyutlarını da kapsayan bir planlamaya yer verilecektir. Buna göre, bilgi güvenliği farkındalığı, bilgi güvenliğinde uyma ya da uymama davranışları, tutum geliştirme, bilgi güvenliğinde normatif baskı kurma, bilgi güvenliğinde öz yeterlilik boyutlarını içeren ve daha geniş bir örneklem ile analiz yapılabilecek bir çalışma gerçekleştirilecektir.

KAYNAKLAR

- Ajzen, I., Fishbein, M. (1980). *Understanding Attitude and Predicting Social Behavior*, Englewood Cliffs, NJ: Prentice-Hall.
- Ajzen, I. (1991). "The Theory of Planned Behavior", *Organizational Behavior and Human Decision Processes*, 50, 179-211.
- Ahmed, M., Sharif, L., Kabir, M. ve Al-Maimani, M. (2012). "Human Errors in Information Security", *International Journal of Advanced Trends in Computer Science and Engineering*, 1(3), 82-87.
- Ayyagari, R., Grover, V. ve Purvis, R. (2011). "Technostress: Technological Antecedents and Implications", *MIS Quarterly*, 35(4), 831-858.
- Bulgurcu, B., Çavuşoğlu, 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.
- Cammann, C., Fichman, M., Jenkins, D., ve Klesh, J. (1983). Assessing the attitudes and perceptions of organizational members. in Seashore, S., Lawler, E., Mirvis, P., and Cammann, C. (eds.), *Assessing organizational change: A guide to methods, measures and practices*. New York, NY: John Wiley, 71-138.
- Data Breach Investigations Report (2017). "Verizon Enterprise" 10th Edition.
- Dawis, R. ve Lofquist, L.H. (1987). "Measurement of Person-Environment Fit and Prediction of Satisfaction in the Theory of Work Adjustment", *Journal of Vocational Behavior*, 31(3), 297-318.
- Edwards, J. R., Caplan, R. D. ve Harrison, R. V. (1998). "Person-Environment Fit Theory: Conceptual Foundations, Empirical Evidence, and Directions For Future Research", In C. L. Cooper (Ed.), *Theories of Organizational Stress* (28-67). Oxford: Oxford University Press.
- Frangopoulos, E.D., Eloff, M.M. ve Venter, L.M. (2013). "Psychosocial Risks: Can Their Effects on the Security of Information Systems Really be Ignored?", *Information Management & Computer Security*, 21(1), 53-65.
- Jena, R.K. (2015). "Impact of Technostress on Job Satisfaction: An Empirical Study among Indian Academician", *The International Technology Management Review*, 5(3), 117-124.
- Jeong, G. ve Jeong, S. (2011). "The Effect of Information Protection Control Activities on Organizational Effectiveness: Mediating Effects of Information Application", *Intellectual Information System*, 17(1), 71-90.
- Kalaycı, Ş. (2005). *SPSS Uygulamalı Çok Değişkenli İstatistik Teknikleri*, Ankara: Asil Yayın Dağıtım.
- Khan, A., Rehman, H. ve Rehman, S. (2013). "An Empirical Analysis of Correlation Between

- Technostress and Job Satisfaction: A Case of KPK, Pakistan", *Pakistan Journal Of Library and Information Science*, 14, 9-15.
- Klahr, R., Shah, J.N., Sheriffs, P., Rossington, T., Pestell, G., Button, M. ve Wang, V. (2017). "Cyber Security Breaches Survey, Main Report".
- Kim, S.H., Yang, K.H. ve Park, S. (2014). "An Integrative Behavioral Model of Information Security Policy Compliance", *Scientific World Journal*, ID 463870, 1-12.
- Kinman, G. ve Jones, F. (2005). "Lay Representations of Workplace Stress: What Do People Really Mean When They Say They Are Stressed?", *Work & Stress*, 19(2), 101-120.
- Kirsch, L. ve Boss, S. (2007). "The Last Line of Defense: Motivating Employees to Follow Corporate Security Guidelines", *International Conference on Information Systems Proceedings*, 103.
- Kraemer, S., Carayon, P. ve Clem, J. (2009). "Human and Organizational Factors in Computer and Information Security: Pathways to Vulnerabilities", *Computers and Security*, doi:10.1016/j.cose.2009.04.006.
- Kristof, A.L. (1996). "Person-Organization Fit: An Integrative Review of Its Conceptualizations, Measurement, and Implications", *Personnel Psychology*, 49, 1-49.
- Kumar, R., Lal, R., Bansal, Y. ve Sharma, S.K. (2013). "Technostress in Relation to Job Satisfaction and Organisational Commitment among IT Professionals", *International Journal of Scientific and Research Publications*, 3(12), 1-3.
- Lee, C., Lee, C.C. ve Kim, S. (2016). "Understanding Information Security Stress: Focusing on the Type of Information Security Compliance Activity", *Computers and Security*, 59, 60-70.
- Lewis, J. (2003). "Cyber Terror: Missing in Action", *Knowledge, Technology & Policy*, 16(2), 34-41.
- Li, Y. (2015). "Users' Information Systems (IS) Security Behavior In Different Contexts", University of Oulu, Finland, ISBN 978-952-62-0938-8.
- Mahboob, A. ve Khan. T. (2016). "Technostress and Its Management Techniques: A Literature Review", *Journal of Human Resource Management*, 4(3), 28-31.
- MMC Cyber Handbook (2018). "Perspectives on the Next Wave of Cyber", Marsch and McLennan Global Risk Center.
- Park, C. ve Im, M., (2012). "The Impact of Technostress on Information Security Perception and Organizational Outcomes", *The Journal of KIIT*, 10(1), 97-109.
- Park, H.J. ve Cho, J.S. (2016). "The Influence of Information Security Technostress on the Job Satisfaction of Employees", *Journal of Business and Retail Management Research*, 11(1), 66-75.
- Pollock, T. (2017). "Reducing human error in cyber security using the Human Factors Analysis Classification System (HFACS)", *Kennesaw State University Proceedings on Cybersecurity Education, Research and Practice 2*.
- Ragu-Nathan, T.S., Tarafdar, M., Ragu-Nathan, B.S. and Tu, Q. (2008). "The Consequences of Technostress for End Users in Organizations: Conceptual Development and Empirical Validation", *Information Systems Research*, 19(4), 417-433.
- Salanova, M., Llorens, S. ve Cifre, E. (2013). "The Dark Side of Technologies: Technostress Among Users of Information and Communication Technologies", *International Journal of Psychology*, 48(3), 422-436.
- Shu, Q., Tu, Q., ve Wang, K. (2011). "The Impact of Computer Self-Efficacy and Technology Dependence on Computer-Related Technostress: A Social Cognitive Theory Perspective", *International Journal of Human-Computer Interaction*, 27(10), 923-939.
- Siponen, M.T. (2000). "A Conceptual Foundation for Organizational Information Security Awareness", *Information Management & Computer Security*, 8(1), 31-41.
- Qiu, W. (2013). "The Impact of Technostress on Job Satisfaction and Organizational Commitment", Master Thesis, Massey University.
- Ostroff, C., ve Schulte, M. (2007). Multiple Perspectives of Fit In Organizations Across Levels of Analysis. In C. Ostroff & T.Judge (Eds.), *Perspectives on Organizational Fit* (3-69). New York: Lawrence Erlbaum Associates.
- Tarafdar, M., Tu, Q. ve Ragu-Nathan, T.S. (2007). "The Impact of Technostress on Role Stress and

- Productivity", *Journal of Management Information Systems*, 24(1). 301-328.
- Tu, Q., Wang, K., ve Shu, Q. (2005). "Computer-Related Technostress in China", *Communications of the ACM*, 48(4), 77-81.
- Turn, R. ve Ware, W.H. (1976). "Privacy and Security Issues in Information Systems", IEEE Transactions on Computers, The Rand Paper Series.
- Udo, G.J. (2001). "Privacy and Security Concerns as Major Barriers For e-Commerce: A Survey Study", *Information Management & Computer Security*, 9(4), 165-174.
- U.S. Congress, Office of Technology Assessment (1994). Information Security and Privacy in Network Environments, OTA-TCT-606 (Washington, DC: U.S. Government Printing Office).
- Wang, K., Shu, Q. ve Tu, Q. (2008). "Technostress Under Different Organizational Environments: An Empirical Investigation", *Computers in Human Behavior*, 24(6), 3002-3013.
- Wiczorkowski, J. ve Polak, P. (2017). "Big Data and Privacy: The Study of Privacy Invasion Acceptance in the World of Big Data", *Online Journal of Applied Knowledge Management*, 5(1), 57-71.
- World Economic Forum (2016). "The Global Risks Report, 11.Baskı".