İŞLETME ARAŞTIRMALARI DERGİSİ
JOURNAL OF BUSINESS RESEARCH-TURK
2022, 14(1), 1-15
https://doi.org/10.20491/isarder.2022.1363

Sağlık Çalışanlarının Bilgi Güvenliği Farkındalığının İş Performansı Üzerindeki Etkisinde Bilgi Güvenliği Stresinin Aracı Rolü: Covid 19 Pandemi Döneminde Bir Araştırma

(Mediator Role of Information Security Stress in the Effect of Information Security Awareness of Health Personnel on Job Performance: A Research in Covid-19 Pandemic Period)

İsmail GÜN [a] **Mazlum ÇELİK** [b]

[a] Hasan Kalyoncu Üniversitesi, Sosyal Bilimler Enstitüsü, Gaziantep, Türkiye, gun.47@hotmail.com
[b] Hasan Kalyoncu Üniversitesi, İktisadi, İdari ve Sosyal Bilimler Fakültesi, Gaziantep, Türkiye, mazlum.celik@gmail.com

MAKALE BİLGİSİ

Anahtar Kelimeler:
Sağlık
Bilgi Güvenliği
Bilgi Güvenliği Farkındalığı
İş Performansı
Bilgi Güvenliği Stresi

Gönderilme Tarihi 19 Aralık 2021
Revizyon Tarihi 8 Ocak 2022
Kabul Tarihi 15 Ocak 2022

Makale Kategorisi:
Araştırma Makalesi

ÖZET

Amaç – COVID 19 döneminde iş yaşamında teknolojinin daha yoğun şekilde kullanılmasından ötürü, bu süreçte çalışanlar nezdinde bilgi güvenliğine ilişkin konuların önemi artış göstermiştir. Bu araştırmanın amacı, COVID 19 pandemisi döneminde sağlık çalışanlarında bilgi güvenliği farkındalığının iş performansı üzerindeki etkisini ölçmek ve bu etkide bilgi güvenliği stresinin aracı rolünün bulunup bulunmadığını araştırmaktır.

Yöntem – Örneklem olarak, Mardin Devlet Hastanesi sağlık personeli seçilmiştir. Nicel araştırma yönteminin uygulandığı bu çalışmada, açıklayıcı araştırma tekniğinden yararlanılmış ve veri toplamak üzere anket tekniği kullanılmıştır. Bilgi güvenliği farkındalığı için Keser ve Güldüren (2015) tarafından geliştirilen 34 maddelik ölçek, iş performansı için Kirkman ve Rosen (1999) tarafından geliştirilip Çöl (2008) tarafından Türkçe uyarlaması yapılan 4 maddelik ölçek, bilgi güvenliği stresi için Ayyagari, Grover ve Purvis (2011) tarafından geliştirilen 8 maddelik ölçek kullanılmıştır. Toplanan veriler SPSS-23 programı aracılığıyla analiz edilmiştir. Analiz için faktör analizi, güvenilirlik analizi, korelasyon analizi ve regresyon analizi kullanılmıştır.

Bulgular – Araştırmada, sağlık çalışanlarında bilgi güvenliği farkındalığının iş performansı üzerinde pozitif ve anlamlı etkiye sahip olduğu ve bu etkide bilgi güvenliği stresinin kısmi aracılık rolünün olduğu bulgularına erişilmiştir.

Tartışma – Bilgi güvenliği farkındalığının iş performansı üzerinde anlamlı etkisi olduğuna ilişkin bulgunun, bilgi güvenliği farkındalığının bilgi güvenliği stresi üzerinde anlamlı etkiye sahip olduğuna ilişkin bulgunun, bilgi güvenliği stresinin iş performansı üzerinde anlamlı etkiye sahip olduğuna ilişkin bulgunun, bilgi güvenliği farkındalığının iş performansı üzerindeki etkisinde bilgi güvenliği stresinin kısmi aracı rolünün olduğuna ilişkin bulgunun, literatürdeki önceki çalışmaların bulgularıyla paralel olduğu tespit edilmiştir.

ARTICLE INFO

Keywords:
Health
Information Security
Information Security Awareness
Job Performance
Information Security Stress

Received 19 December 2021
Revised 8 January 2022
Accepted 15 January 2022

Article Classification:
Research Article

ABSTRACT

Purpose - Since technology has been started to be used more in working life during COVID-19, the importance of issues about information security has risen in terms of employees in this process. The aim of this research is to measure the effect of information security awareness on job performance in terms of health personnel, and whether or not there is mediator role of information security stress in this effect in COVID-19 pandemic period.

Design/methodology/approach - Health personnel of Mardin State Hospital was chosen as the sample group. In this study in which quantitative research method was used, explanatory research technique was used, and survey technique was used to gather data. 34 itemed scale developed by Keser and Güldüren (2015) for information security awareness, 4 itemed scale developed by Kirkman and Rosen (1999) and adapted into Turkish by Çöl (2008) for job performance, 8 itemed scale developed by Ayyagari, Grover & Purvis (2011) for information security stress were used. For data analysis, factor analysis, reliability analysis, correlation analysis, and regression analysis were used.

Findings - In the research, the findings that information security awareness has positive and significant effect on job performance in health personnel, and there is partial mediator role of information security stress in this effect, were reached.

Önerilen Atıf/ Suggested Citation
Gün, İ., Çelik, M. (2022). Sağlık Çalışanlarının Bilgi Güvenliği Farkındalığının İş Performansı Üzerindeki Etkisinde Bilgi Güvenliği Stresinin Aracı Rolü: Covıd 19 Pandemi Döneminde Bir Araştırma, *İşletme Araştırmaları Dergisi*, 14 (1), 1-15.

Discussion – It was determined that the findings about the significant effect of information security awareness on job performance, significant effect of information security awareness on information security stress, significant effect of information security awareness on job performance, and the partial mediator role of information security stress in the effect of information security awareness on job performance, are parallel with the findings of previous studies in literature.

1. Giriş

Teknolojiyle bilgisayarın yaygın şekilde kullanımının olmadığı dönemlerde durağan bir niteliğe sahip olan bilgi, günümüz koşullarındaki teknolojilerle dinamik bir niteliğe bürünmüştür (İlbaş, 2009). Günümüz koşullarında bilgi teknolojilerinin kullanılmasıyla bilginin üretimi, depolanması, paylaşımı ve kullanımı kolaylaşmıştır. Bu doğrultuda bilgi, bilgi teknolojilerinin yaygınlaşmasının neticesinde hızlı ve devamlı biçimde üretilebilmekte, geliştirilebilmekte, taşınabilmekte, bölünebilmekte, paylaşılabilmekte olan bir ürün durumuna gelmiştir (Vardal, 2009). Bilginin elde edilebilmesi hususunda zamanla emek harcanması, elde edilmekte olan bilginin işlevsel olması halinde hayatın bütün alanlarında farklılıklar meydana getirmesinden ötürü bilgi, korunması gerekli olan bir değer niteliğindedir (Brykczynski ve Small, 2003). Zira dijital araçların kullanılmasındaki artış insan yaşamındaki birçok şeyi etkilemektedir. Bilgiye erişilmesi ve bilginin üretilmesi, bankacılık, eğitim, ticaret gibi sektörlerdeki alışkanlıkları değişime uğratırken, bu sektördeki işlemlerle süreçleri kolaylaştırmış durumdadır. Bu doğrultuda, dijital ortamlarda saklanmakta olan bilgiler çeşitlenirken, saklanması gerekli olan bilginin miktarı da giderek artmaktadır. Bu durumda bilginin güvenliğiyle ilintili tehditler ortaya çıkmaktadır (Yılmaz, Şahin ve Akbulut, 2016).

Bilgi güvenliği farkındalığı, güvenlik bakımından pozitif nitelikli davranışlara sebebiyet veren güvenlik bilincini anahtar bir unsur şeklinde ele alır. Bilgi güvenliği farkındalığı, kullanıcılarca bilgi güvenliğinin öneminin algılanması, sorumluluklar, kuruma uygun bilgi güvenliği seviyesi ve davranışları şeklinde ifade edilmektedir (Kruger ve Kearney, 2006). Bilgi ve iletişim teknolojilerinin gittikçe yaygınlaşması, internetin kullanımının yaygınlaşması ve internette kullanılmakta olan online uygulamalarda yaşanan artışlar doğrultusunda güvenlik açıklarının da artması neticesinde, bilgi güvenliğinin sağlanması vazifesi toplumlarda yalnızca bilgi güvenliğinden sorumlu olan kişilerle kurumların işi olmaktan çıkmış durumdadır (Vural ve Sağıroğlu, 2011). Günümüz koşullarında bilgi sistemlerinin globalleşmesinin neticesinde, bilgi sistemleriyle doğrudan ya da dolaylı şekilde bağlantılı durumdaki ve bu sistemlerden faydalanan bütün fertlerle kuruluşların artık bilgi güvenliğine katkı sağlamaları zaruridir (Vural ve Sağıroğlu, 2011). Ancak bilgi güvenliği hakkında yeterli bilgi ve farkındalığa sahip olmayan kişilerde, zaman içerisinde teknostres, bilgi güvenliği stresi gibi problemler ortaya çıkabilmektedir.

Kurumlarda bilgi güvenliğiyle ilintili politikalara uyuma etki etmekte olan bir bileşen niteliğindeki stres, son senelerde bilgi güvenliğine ilişkin çalışmalarda ele alınan önemli bir faktör konumundadır. Lee, Lee ve Kim (2016) tarafından bilgi güvenliği stresini anlama maksadıyla, bilgi güvenliği uyum faaliyet türleri incelenmiştir. Yapılan çalışma neticesinde; aşırı iş yükü ile mahremiyetin ihlal edilmesinin, bilgi güvenliği stresini etkilemekte olduğu tespit edilmiştir. Ament ve Haag (2016) tarafından yapılan çalışmada ise, bilgi güvenliği bilincinin arttırılması maksadıyla gerçekleştirilmekte olan aktivitelerin işgörenlerde strese sebebiyet verdiği ortaya konulmuştur. Yanı sıra, çalışanların bilgi güvenliğine ilişkin farkındalık sahibi olmaları ve bilgi güvenliğine ilişkin sahip oldukları stres düzeyi, diğer pek çok örgütsel değişken gibi çalışanların iş performansları üzerinde etkiye sahip olabilmektedir.

İş performansı, organizasyonların devamlı şekilde değerlendirdikleri, geliştirilmesiyle yönlendirilmesine gereksinim duydukları önemli bir örgütsel davranış değişkeni niteliğindedir (Murphy ve Cleveland, 1995). İşlerin teknik ve uzmanlık yönü ile ilintili olan iş performansı, herhangi bir işin bir diğer işten farklılıklarını ortaya koymakta olan vazifelerle sorumluluklardır (Jawahar ve Carr, 2007). Organizasyonların belirlenmiş olan amaçlarla hedeflere erişebilmeleri, içinde yer aldıkları piyasada rekabet avantajı elde etmeleriyle, dolayısıyla işgörenlerinin yüksek iş performanslarıyla gerçekleşebilmektedir (Youndt ve Snell, 2004). Bu bakımdan, örgütlerde her daim yüksek iş performansı sergilemekte olan işgörenlere gereksinim duyulmakta olduğu söylenebilir. Nitekim iş performansının seviyesi işgörenlerin ve organizasyonların etkili olabilmelerinin önemli bir göstergesidir (Richard, Devinney, Yip ve Johnson, 2008). Ayrıca işgörenlerin örgütteki performanslarının yüksekliği; onların mesleki açıdan yeterlilikleri, çalışma ortamındaki şartlar, görev tanımlamasının net olarak gerçekleştirilmiş olması ve etik nitelikler ile ilişkilidir (Özdevecioğlu ve Kanıgür, 2009).

Teknolojik alandaki gelişmelerin giderek artması ve insan hayatı ile bütünleşmesi neticesinde bilgi güvenliğinin önemi de giderek artmaktadır. Bu noktada her bir bireyin bilgi güvenliğine ilişkin farkındalık sahibi olması gereklidir. Ayrıca bilgi güvenliği ile ilgili konular ve bilgi güvenliği konusundaki bilgilerin/farkındalığın düşüklüğü çalışan bireylerde strese neden olabilmektedir. İşyerinde stres iş performansının düşmesine sebebiyet verirken, bilgi güvenliğine ilişkin farkındalık ise iş performansının artmasını sağlayabilmektedir (Aslandağ, 2010; Akyol, 2013). Araştırma çerçevesinde ele alınan değişkenler arası ilişkilere yönelik olarak literatürde oldukça az sayıda çalışma bulunmaktadır. COVID 19 salgını döneminde sağlık çalışanları üzerinde yapılan bu çalışmanın hem dönem açısından hem de örneklem açısından önemli olduğu ve bulguların literatüre katkı sağlayacağı öngörülmektedir. Bununla birlikte, araştırma neticesinde elde edilecek olan bulgular sayesinde Mardin ilindeki sağlık çalışanlarının bilgi güvenliğine ilişkin tutumlarının, farkındalık düzeylerinin, stres düzeylerinin ölçülecek olması da sektörde çalışanlar hakkında fikir sahibi olunmasını sağlayacaktır.

2. KAVRAMSAL ÇERÇEVE

2.1. Bilgi ve Bilgi Güvenliği

Bilgi güvenliği; bilgiye sürekli ulaşılabilirliğin gerçekleşmekte olduğu bir yapının içinde, bilginin kaynağından alıcısına erişinceye değin kontrollü biçimde herhangi bir değişikliğe uğramaksızın, ilgili alıcılara erişmesinin sağlanması süreciyle ilintilidir (Vural, 2007). Canbek ve Sağıroğlu (2006) bilgi güvenliğini; bilginin bir değer şeklinde dışarıdan gerçekleştirilecek arzu edilmeyen müdahalelere karşı muhafaza edilmesi, değiştirilememesi, sadece istenen kişilerce erişilebilmesi ve kullanılabilmesi şeklinde ifade etmektedir.

Bilgi güvenliğinin; gizlilik, bütünlük, erişilebilirlik şeklinde 3 ana unsuru mevcuttur (Keser ve Güldüren, 2015). Gizlilik, bilginin bulunmakta olduğu ortamdan göndericiden alıcıya iletilmesi sürecinde, izinsiz biçimde herhangi bir kişi ya da grup tarafınca erişiminin engellenmesiyle ilintilidir. Verinin bütünlüğü, bilginin aktarılması sırasında istenmeyen kişilerce bilginin bozulması, silinmesi, bilgiye yeni veriler eklenmesi ya da çıkartılması gibi risklere karşılık verinin içeriğini korunmasıyla ilgilidir. Erişilebilirlik, yetkili kişilerin istenen bilgiye gerektiği zamanda doğru ve güvenilir biçimde ulaşabilmesiyle alakalıdır (Keser ve Güldüren, 2015). Bahsi geçen bu 3 temel unsurun yanı sıra, bilgi güvenliğiyle ilintili olarak literatürde yer alan çeşitli unsurlar da bulunmaktadır. Bunlar temel olarak güvenilirlik, inkâr edememe, kimlik sınaması, yetkilendirme ve izlenebilirlik/kayıt tutma şeklindedir. Güvenilirlik unsuru, sistemin öngörülen ve beklenen davranışıyla elde edilmekte olan neticelerin arasındaki tutarlılık durumunu ifade etmektedir. İnkâr edememe, kaynakla alıcının arasında gerçekleşen bilgi iletiminde gerek kaynağın gerekse de alıcının veriyi doğru şekilde aldığının karşılıklı biçimde doğrulanmasıyla alakalıdır. Kimlik sınaması, sistemin kullanılması esnasında cihaz ya da kullanıcının önceden belirlenmiş olan kriterleri karşılayacak biçimde kimliğinin doğrulanmasına ilişkindir. Yetkilendirme, kullanıcı adıyla parolası doğrulanmış olan fertlere özel, belirli hak ve sorumlulukların verilmesiyle ilintilidir. İzlenebilirlik/kayıt tutma, bir sorun oluşması halinde sorunun kaynağının doğru şekilde tespit edilmesi hususunda kullanılan sistemlerde tüm kullanıcıların gerçekleştirdikleri işlemlerin kayıt altına alınması ve ihtiyaç duyulması halinde sorunların çözümlenmesi noktasında bu kayıtların kullanılabilir olmasıyla ilgilidir (Başaranoğlu, 2016).

Sayarı (2009) dijital ortamda tutulmakta olan bilginin güvenliğinin sağlanamaması halinde genellikle şu risklerin ortaya çıkabileceğinden bahsetmektedir:

- Kuruluşların sahibi bulundukları ve özellikle gizli içeriğe sahip bilgiler, üçüncü kişilerin ellerine geçebilir.
- Sahibi olduğu bilgiyi muhafaza edemeyen ve üçüncü kişilerin ellerine geçmesini engelleyemeyen kuruluşlar ciddi itibar kayıplarıyla karşılaşabilir.
- Kamu kuruluşlarında kaybedilen hassas bilgiler, ülkenin çıkarlarına zarar verebilir.
- Bilginin kaybedilmesi, onun tekrar sağlanabilmesi hususunda belirli bir süre işle zaman kaybına neden olabilir.
- Özellikle kamusal alamda ve çeşitli önem arz eden kurumlar nezdinde kanuni bakımdan ciddi yaptırımlara maruz kalabilir.

2.2. Bilgi Güvenliği Farkındalığı

Teknolojinin gelişmesiyle sürekli değişmesine paralel şekilde bilgi güvenliğiyle ilintili risklerle tehditler çeşitlenmiş durumdadır. Günümüz koşullarında bilgi güvenliğinin elde edilmesi noktasında ağırlıklı şekilde uygulamalarla teknolojik çözümlerin üzerine odaklanılmış olduğu görülebilmektedir. Bilgi güvenliğinin sağlanması hususunda uygulamalarla teknolojik çözümleri geliştirmenin maliyeti oldukça yüksek olmaktadır. Ancak kullanıcılara bilgi güvenliğine ilişkin farkındalığın kazandırılmasının maliyeti çok daha azdır. Bu sebeple, bilgi güvenliği alanında farkındalık kavramının önemi gün geçtikçe daha fazla artmaktadır (Erol ve Sağıroğlu, 2018).

Bilgi güvenliği farkındalığı, bilgi güvenliğini tehdit etmekte olan unsurlara karşılık alınabilecek önlemler ile meydana getirilen güvenlik politikalarından haberdar olunması şeklinde ifade edilmektedir (Şahinaslan, Kandemir ve Şahinaslan, 2009). Bilgi güvenliğinin teknolojiyle ilintili yönlerinin güvenli bir ortamı garanti edemediği, bireylerin bilgi güvenliğine yönelik davranışlarının bu durumda göz önünde bulundurulması gerektiği ifade edilmektedir (Furnell ve Clarke, 2012).

Bilgi güvenliğine ilişkin risklerden korunmanın en etkili yolu, bilgi teknolojileri için çok fazla para harcanmasıyla korunma maksatlı teknolojilerden daha fazla faydalanmadan ziyade, fertlerin bilinçlendirilmesi ve gereksinim hissedilen güvenlik teknolojisinin doğru yer ve zamanda kullanılması şeklindedir (Siponen, 2001). İnsan unsuruna bağlı bilgi güvenliği risklerinin hiçbir zaman tamamıyla ortadan kaldırılması mümkün olmamakla birlikte, iyi planlanmış bir farkındalık etkinlikleriyle bilgi güvenliğine ilişkin riskler kabul edilebilir düzeye çekilebilir (Acılar, 2009).

Fertlerde oluşan bilgi güvenliğine ilişkin farkındalıktan ötürü, fertlerin karşılaşmakta oldukları bilgi güvenliği tehditlerinin karşısında mevcut bilgilerini davranışa dönüştürmek suretiyle en az hasarı almaları beklenmektedir. Bilgi güvenliğiyle ilgili farkındalığın oluşması hususunda tehdit, algı, farkındalık ve davranış şeklinde dört temel öğeden bahsedilebilmektedir. Tehdit, bir yapının zarar görmesine sebebiyet veren istenmeyen bir olayın arkasında bulunan bilinmeyen nedendir (Erdoğmuş, 2017). Algı, bilgi güvenliğiyle ilintili öğelerin kalıcı davranışa dönüştürülmesi suretiyle içselleştirilmesidir (Huang, Rau ve Salvendy, 2010). Farkındalık, bilgi güvenliğine ilişkin ilkelerle kurallara uyulmadığı takdirde ortaya çıkabilecek istenmeyen neticelerin bilinçli biçimde kavranmasıdır. Bu bağlamda bilgi güvenliği farkındalığı, tehditlerin algılanmasını müteakiben ortaya çıkabilecek negatif davranışların yaratacağı risklerin değerlendirilmesi ve bu doğrultuda uygulanabilecek davranışları kapsamaktadır (Erol ve Sağıroğlu, 2018). Davranış, bilgi teknolojilerinin kullanılması sırasında oluşabilecek risklerin farkında olunması ve bu risklerin giderilmesi hususunda gereken politikalarla süreçlerin bilinçli biçimde uygulanmasıyla ilgilidir (Kruger ve Kearney, 2006).

Bilgi güvenliğinin elde edilebilmesi noktasında gerçekleştirilebilecek olan uygulamaların içine dahil edilmesi gerekli olan en önemli unsur, insan unsuruna bağlı olan bilgi güvenliği riskleri şeklindedir (Keser ve Güldüren, 2015). Bu risklerin tamamıyla ortadan kaldırılması mümkün olmamakla beraber, dikkatli ve iyi eğitime sahip fertlerle bu riskler azaltılabilmektedir. Öztemiz ve Yılmaz (2013) fertlerin herhangi bir sağlık problemi oluşmadan hastaneye gitmemeleri gibi, herhangi bir bilgi güvenliği tehdidi ile karşılaşmaksızın bilgi güvenliğine ilişkin farkındalık oluşturma çabasında bulunmadıklarını belirterek, bilgi güvenliği farkındalığını sağlık durumuyla ile örneklendirmiştir. Bu doğrultuda, fertlerin sağlık önlemleri almaları gibi bilgi güvenliğine yönelik olarak da farkındalık çalışmalarında bulunmaları gereklidir. Bu bağlamda, toplumsal açıdan fertlerin sahibi bulundukları konumları çerçevesinde bilgi güvenliği farkındalıklarının arttırılması hususunda gereken eğitimlerin sağlanması gerekmektedir.

Bilgi güvenliğine ilişkin farkındalık çalışmalarına Türkiye'nin gereksinimi bulunduğundan bahsetmiş olan Ünver, Canbay ve Mirzaoğlu (2011), gerçekleştirmiş oldukları çalışmada bilgi güvenliğinin elde edilmesini; Türkiye'de hem kamusal sektörde hem de özel sektörde uygulanmakta olan genel yaklaşımın, var olan riskleri azaltabilecek risk yönetimi uygulamalarının yapılması suretiyle, bilgi ve iletişim kaynaklarının muhafaza edilmesi biçiminde olduğu ve bilgi güvenliğinden bahsedildiğinde teknik önlemler şeklinde algılanması ve teknolojik çözümlemelere ağırlık verilmesinin neticesinde konunun yasal, idari, iktisadi ve sosyal boyut çerçevesinde ele alınması vasıtasıyla, kapsamlı bir çözüm geliştirilmesinin önüne geçtiğini, işin yasal boyutundaysa kanunların bilgi güvenliğini her yönü ile ele alacak kadar detaylı olmadığını ve güvenlik kuvvetleriyle adli personelin yeterince bilgi ve uzmanlık düzeyine sahip olmadıklarını, idari açıdan kamu yönetimiyle çalışanlarının gereken bilgi güvenliği farkındalığıyla yeterince siber güvenlik kapasitesine sahip

olmadıklarını, iktisadi bakımdan bilgi güvenliğinin elde edilmesi hususunda farkındalık çalışmalarına yeterince kaynağın ayrılmadığını ifade etmiştir.

2.3. Bilgi Güvenliği Stresi

Bilgilere erişilmesini hızlandırıp kolaylaştırmakta olan internet ve ilgili diğer teknolojilerdeki gelişimler, mobil cihaz ile akıllı telefon kullanım oranının hızlı biçimde yaygınlaşması, dil, zaman, mekân vb. kavramların ortadan kalkması pek çok riski, tehdidi ve etik problemleri de beraberinde getirmiş durumdadır. İnsanlar açısından vazgeçilmez ve değerli bir varlığa dönüşmüş durumdaki bilginin teknoloji alanındaki gelişimlerin neticesinde risklerle tehditlere karşılık muhafaza edilmesi ve güvenliğinin sağlanması bir zorunluluk durumuna gelmiş haldedir. Yeni bilgilerin üretimi, geliştirilmesi, bu bilgilerin kullanıcılar ile paylaşılması, ortaya çıkabilecek tehditlerle saldırılara karşılık bilgilerin muhafaza edilmesi sürecinde sürekliliğin elde edilebilmesi noktasında etkili bir planlamanın gerçekleştirilmesi gereklidir (Erdoğmuş, 2017).

Temelde stres, fertlerin gereksinmelerinden vazgeçmelerine veya bir tepkide bulunmalarına zorlayıcı, kişinin içinden ve dışından gelmekte olan ve çoğunlukla gerilim, üzüntü, çöküntü gibi durumların yaşanmasına neden olan bir güçtür (Tengilimoğlu, Işık ve Akbolat, 2014). Stres, fertlerin kontrollerinin dışında gelişim gösteren ve bu kontrolsüzlükten ötürü kişinin zihinsel ve psikolojik sağlığını negatif biçimde etkilemekte olan bir durumdur (Tutar, 2016). Bireylerin esenliğiyle huzuru bakımından bir tehlike işareti, bir uyarı biçiminde algılanmakta olan ve bu nedenle yetersiz biçimde ele alınan olaylara gösterilmekte olan, belirgin olmayan fizyolojik ve psikolojik tepkiye stres ismi verilmektedir (Akgemci, 2001).

Bilgi güvenliğinde stres olgusu, tekno-stres kavramıyla bağlantılıdır. Tekno-stres, bilgi ve iletişim teknolojilerinin gelişimiyle paralel şekilde, genellikle yeni teknolojilere uyumluluk sağlanmasında zorlanılmakta olan, işgörenlerin vazifelerini gerçekleştirmeleri hususunda gerekli olan seviyede beceri veya yetkinliğe sahip olmadıkları durumlarda ortaya çıkmakta olan teknolojiden kaynaklanan stres halini belirtmek üzere kullanılmaktadır (Tarafdar, Tu, Ragu-Nathan ve Ragu-Nathan, 2007). Yoğun şekilde cep/mobil telefon ile bilgisayar kullanılması, e-posta trafiği, elektronik mesajlaşma, gün içerisinde yoğun şekilde yapılan telefon görüşmeleri, sürekli olarak şifre kullanma ve güncelleme, yazılımların güncellenmesi, siber saldırılara maruz kalma gibi birtakım unsurlar teknoloji temelli strese sebebiyet verebilmektedir. Bilginin kaybedilmesi korkusu, kişisel bilgilerin ihlal edilmesi ve buna ilişkin güvenlik problemleri, hızlı işlemde bulunmaya ilişkin olarak hata gerçekleştirme korkusu, teknoloji temelli olarak iş yükünün artması tekno-stresin muhtemel kaynakları arasındadır (Mahboob ve Khan, 2016).

2.4. İş Performansı

Performans, planlı ve amaçlanmış faaliyetlerin neticesinde ortaya konulanı nicel ve/veya nitel açıdan belirlemekte olan bir kavram niteliğindedir (Şimşek ve Nursoy, 2002). Rotundo ve Sackett (2002) performans kavramını, bir organizasyonun amacıyla hedeflerine katkı sağlayan, fertlerin denetimi altında bulunan davranış ve faaliyet biçimi şeklinde betimlemiştir. Kutal ve Büyükuluslu (1996) tarafından performans, amaçlara erişilebilmesi hususunda harcanan çaba şeklinde açıklanmıştır. Performans, fertlerin sosyal yaşamlarında ve/veya iş yaşamlarında bir şeyleri başarmak üzere harcadıkları çabadır. Performans, her bir ferdin sorumluluk alma duygusunu geliştirmeye, hedefleriyle amaçlarını tespit etmesine ve vizyonlarını genişletmesine yardımcı olmaktadır. Performans doğrudan şekilde verimliliği açıklamaktadır ve işgörenlerin işlerine yönelik sadakatlerine, bir vazifeyi gerçekleştirmeye ilişkin istekliliklerine karşılık gelmektedir. Organizasyonların belirlenmiş amaçlarına erişebilmeleri ve sürdürülebilir rekabet üstünlüğü elde edebilmeleri hususunda işgörenlerin motivasyonlarıyla bağlılıkları önemli unsurlardır. Performans ise gerçekleştirilmekte olan faaliyetlerin neticelerinin değerlendirilmesiyle tespit edilmektedir (Doğan ve Özdevecioğlu, 2009).

Viswesvaran ve Ones (2000) iş performansını, organizasyonların amaçlarına erişmeleri hususunda katkıda bulunan işgörenlerin iş sonuçları ve davranışları şeklinde ifade etmektedir. Bu doğrultuda iş performansı, fertlerin kendilerine verilmiş olan işleri ne oranda gerçekleştirdikleri, işin gereklerini yerine getirme seviyesi, başarısı, verimliliği ve işe ilişkin etik yaklaşımları içine almakta olan geniş bir kavram durumundadır. Fertlerin kişisel özelliklerinin öznel birtakım yargıları içermesiyle karmaşık olması, iş performansının tanımının yapılmasını güçleştirse de, iş performansı seviyesinin tespiti konusunda birtakım kriterler mevcuttur. Nitekim iş performansı, işgörenlere ceza verilmesinden ziyade iş verimliliğinin arttırılması

amaçlandığında daha faydalıdır. Kariyer fırsatlarının varlığı, terfi, ücret vb. durumlar ile işten çıkarma gibi önemli yönetsel kararların verilmesi, işgörenlerin iş performanslarını etkilemekte olan önemli unsurlar arasındadır (Murphy ve Clevaland, 1995).

Endüstri devriminin başlangıcından yakın tarihlere değin performansın temel unsurları yalnızca maliyet ve karlılık şeklinde nitelendirilmiştir. Lakin ilerleyen dönemlerde bilim insanları tarafınca performansın iki temel unsur bulunduğu belirtilmiş ve bunlar etkinlik ile verimlilik şeklinde ifade edilmiştir. Son dönemlerdeyse bu unsurlara girdilerden faydalanma, kalite, yenilik ve çalışma hayatının kalitesi gibi unsurlar da ilave edilmiştir. Bu doğrultuda performans kavramı daha geniş unsurlar ile ele alınmaya başlanmıştır. Günümüz koşullarında ise performansın unsurları arasına işgören davranışı, pazar ortamı, ürün liderliği, kamu sorumluluğu vb. muhtelif unsurlar da eklenmiştir (Karaman, 2009).

Organizasyonlarda değişimlerin proaktif şekilde gerçekleşebilmesi hususunda, organizasyonların uyarlanabilir yeteneklerini geliştirmeleri suretiyle, çevrenin değişim gösteren gereksinimleriyle başa çıkmaları ve iş dünyasında mükemmelleşebilmek üzere bir dönüşüme girmeleri gerektiği ifade edilebilir. Bu bağlamda, örgütlerin sürdürülebilirlikleri, işgörenlerin yetenekleri, becerileri, bilgileri ve deneyimlerinin yanı sıra onların performanslarına da bağlı durumdadır. Örgütlerin başarıları, işgörenlerinin yaratıcılıklarına, yenilikçiliklerine ve örgütsel bağlılıklarına dayandığından, örgüt açısından bir işgörenin etkili performansı, mutlak gerekli olan bir araç niteliğindedir (Bayram, 2005). Bunun yanında, işgörenlerin performansları yalnızca örgüt bakımından değil, ayrıca toplum bakımından da önem arz etmektedir. İşgörenlerinin yüksek bir performansa sahip olması, örgütün hem sosyal hem de iktisadi amaçlarına erişmesinde öncü bir rol üstlenmekteyken; elde edilecek terfi fırsatları, maddi ödüller gibi unsurlar da kişisel hedeflerin gerçekleştirilmesini sağlamaktadır (Ertan, 2008).

İş performansı, bağlamsal performans ve görev performansı şeklinde iki temel boyuta ayrılmaktadır. Bağlamsal performans, fertlerin daha çok çalışmak üzere gönüllü olmaları, işlerini hevesli şekilde yapmaları, iş birliğine yatkın olma, örgütü sahiplenme ve destekleme ile kurallara uyulmasını içermektedir. Bağlamsal performans çerçevesinde ekibin başarısı hususunda çalışılmaktadır (Özdevecioğlu ve Kanıgür, 2009). Bağlamsal performans, işletmedeki organizasyon, sosyal ve ruhsal atmosfere katkıda bulunan aktiviteleri kapsamaktadır. Örgütteki verimlilikle ekibin başarısı son derece önemlidir. İş ortamını zenginleştirmekte olan bağlamsal performans, sosyal ve motivasyonel örgüt iklimine de katkıda bulunmaktadır (Ünlü ve Yürür, 2011).

Görev performansı, organizasyonun teknik süreçlerini yürütüp, buna ilişkin gereksinimlerle ilgilenmekledir ve yetenekler ile ilişki içindedir. Görev performansı, kişinin uzmanlığı ve teknik tarafı ile açıklanmaktadır (Özdevecioğlu ve Kanıgür, 2009). Görev performansı, kişinin işiyle ilintili aktiviteleri yürütmesine ilişkindir. Örgütteki teknik yapıyı meydana getiren ana aktivitelerin yürütülmesini kapsamaktadır. İşletmede çalışmakta olan fertlerin, işlerini gerçekleştirebilmeleri hususunda teknik bilgileriyle becerilerini kullanmaları, görev performansıyla ilintilidir (Doğan ve Özdevecioğlu, 2009).

2.5. Hipotezlerin Oluşturulması

Kurumların bilgi güvenliklerinden yalnızca bilgi güvenliğinde çalışan personel değil, aksine kurumda çalışan bütün personel ile paydaşlar sorumlu durumdadır. Bu doğrultuda, kurumların bilgi güvenliği politikaları çerçevesinde gerçekleştirilen farkındalık arttırma faaliyetleri ile çalışanlarda güvenlik bilinci oluşturulmaktayken, hangi bilgilerin muhafaza edilmesi gerektiği, bunların ne gibi tehditlere karşı olarak ne şekilde muhafaza edilmesi gerektiğine ilişkin bilinçlendirmelerin yapılması gereklidir (Şahinaslan, Kantürk, Şahinaslan ve Borandağ, 2009). Örgütlerin faaliyet gösterdikleri sektördeki bilgi güvenliği ihtiyaçları çerçevesinde uygulanan bilgi güvenliği yönetim sistemi, o örgütte çalışmakta olan personelin memnuniyetiyle performansını pozitif yönlü olarak arttırarak, örgütün genel performansını da pozitif yönlü şekilde etkileyecektir (Aslandağ, 2010). Akyol (2013) ise COBİT gibi iç denetim sistemi uygulamakta olan örgütlerdeki bilgi güvenliği politikalarının işletme, personel ve süreçlere yönelik etkilerini incelediği çalışmasında, çalışanların performanslarının bilgi, eğilim ve farkındalık kavramlarıyla pozitif bir ilişkiye sahip olduğunu tespit etmiştir. Bilgi güvenliği farkındalığına ilişkin olarak, bilgi güvenliği tehditlerinin farkında olan ve bu bağlamda bu tehditlere yönelik gerekli önlemleri alabilen kişilerin daha etkin şekilde çalışabilmeleri ve bu doğrultuda daha yüksek iş performansı göstermeleri beklenmektedir. Bu doğrultuda, araştırmanın H1 ana hipotezi ile H1a ve H1b alt hipotezleri şu şekilde kurulmuştur:

H1: Bilgi güvenliği farkındalığı, iş performansını pozitif ve anlamlı olarak etkilemektedir.

H1a: Saldırı ve tehditler, iş performansını pozitif ve anlamlı olarak etkilemektedir.

H1b: Kişisel verilerin korunması, iş performansını pozitif ve anlamlı olarak etkilemektedir.

COVID-19 enfeksiyon riski bakımından sağlık çalışanları çok yüksek risk grubunun içerisinde yer almaktadır. Aynı zamanda sağlık çalışanlarının genel olarak sağlık, güvenlik ve bilgi güvenliği açısından da en riskli iş kollarından birinde vazife gördüklerinden bahsedilebilir. Bu durumda, COVID-19 koşulları altında; fiziksel, kimyasal, biyolojik ve psikososyal risk faktörlerinden ötürü sağlık çalışanlarının ciddi bir stres durumu yaşadıkları ifade edilebilir. Sağlık çalışanlarından beklenmekte olan hizmetle çalışanların bu beklenen hizmeti karşılayabilme becerileri de sağlık çalışanların stres seviyelerini belirlemektedir. Ayrıca sağlık çalışanları, insan sağlığına ilişkin önemli bir sorumluluğu taşıdıkları için, pandemi sürecinde çalışma ortamından kaynaklanmakta olan her tür stresi daha yoğun şekilde yaşamaktadır (Sakaoğlu, Orbatu, Emiroğlu ve Çakır, 2020). Sağlık çalışanları özellikle de COVID-19 sürecinde ciddi mesleki zorluklara sahiptirler. Zira sağlık çalışanlarının üzerinde bu dönemde önemli bir iş baskısı ve zaman baskısı bulunmakta olup, halen tam bir tedavisinin olmadığı pandemi tehdidine karşı hem kendilerini hem de hastaları koruma gayreti içerisindedirler.

Bilgi güveliğiyle ilintili olarak yaşanan stres, diğer pek çok sektörde olduğu gibi, sağlık sektöründe çalışanlar bağlamında da oldukça önemli bir konudur. 24 Mart 2016 tarihli ve 6698 sayılı "Kişisel Verilerin Korunması Kanunu" çerçevesinde, 21 Haziran 2019 tarihinde "Kişisel Sağlık Verileri Hakkında Yönetmelik" yayımlanmıştır. Yönetmelik kapsamında, sağlık hizmetlerinde bilgi güvenliğine ilişkin konu ve kavramlara değinilmiş, hangi sağlık verisine kim tarafından erişilebileceği ve bu verilerin nasıl korunacağı açıklanmıştır. Bu doğrultuda, bilgi güvenliğiyle ilintili tehditlerin farkında olma durumu ve buna ilişkin önlemleri alabilme durumunun, sağlık çalışanlarında bilgi güvenliği ile ilgili stres yaşama durumu ile yakın bir ilişkide olacağı düşünülmektedir. Nitekim bu tehditlerin farkında olmayan ve gerekli önlemleri alamayan kişilerde stres yoğunluğu artış gösterecektir. Literatür bulguları değerlendirildiğinde, Lee vd. (2016)'ne göre, aşırı iş yüküyle mahremiyetin ihlal edilmesi bilgi güvenliği stresini arttırmaktadır. Ament ve Haag (2016) ise, bilgi güvenliği farkındalığının arttırılmasına yönelik örgütlerde yapılan faaliyetlerin personelde strese yol açtığından bahsetmiştir. Bu doğrultuda, araştırmanın H2 ana hipotezi ile H2a ve H2b alt hipotezleri şu şekilde kurulmuştur:

H2: Bilgi güvenliği farkındalığı, bilgi güvenliği stresini pozitif ve anlamlı olarak etkilemektedir.

H2a: Saldırı ve tehditler, bilgi güvenliği stresini pozitif ve anlamlı olarak etkilemektedir.

H2b: Kişisel verilerin korunması, bilgi güvenliği stresini pozitif ve anlamlı olarak etkilemektedir.

Bassi (1997) bilgi yönetiminin, örgütsel performansın geliştirilmesi hususunda bilginin yaratılması, ele geçirilmesi ve kullanılmasını içeren bir süreç olduğundan bahsetmiştir. Smith (2002) bilgi yönetiminin; çağdaş dünyanın hızlıca artmakta olan belirsizliğiyle karmaşıklığının karşısında, örgütlerin yaşamlarını ve performanslarını arttırmaya çalışmalarıyla alakalı olduğuna değinmiştir.

Bilgi güvenliği uygulamalarının getirdiği yüksek seviyede iş yükü, bilgi güvenliği sistemlerinin işlevsel açıdan zayıflamasına, insan kaynaklı hataların yaşanmasına ve bilgi güvenliği sistemi performansının düşüş göstermesine sebebiyet vermektedir (Kraemer, Carayon ve Clem, 2009). Aşırı iş yükünün getirdiği stres ise çalışanların performanslarını düşürücü etkiler yaratmaktadır (Erbi, 2018). Tarafdar, Pullins ve Ragu-Nathan (2011) bilgi güvenliği stresinin profesyonel satış personellerinin performansları üzerindeki etkisini incelemiş ve bilgi güvenliği stresiyle performans arasında negatif bir ilişki olduğunu bulmuştur. Saganuwan, Ismail ve Ahmad (2013) muhasebe bilgi sistemi etkinliğiyle işgörenlerin bilgi güvenliği stresi sorunlarına odaklandıkları çalışmada, bilgi güvenliği stresinin işgörenlerin iş doyumları ve iş performansları ile muhasebe bilgi sistemi etkinliği arasındaki ilişkide aracı bir role sahip olduğu neticesine erişmiştir. Azam, Abidin, Yusof, Emang ve Entigar (2014) tarafından yapılan çalışmada bilgi güvenliği stresi yaratan unsurlar ile işgörenlerin çalışma performansları arasındaki ilişki incelenmiş ve bilgi güvenliği stres faktörlerinin iş performansı üzerinde önemli bir etkiye sahip olduğu bulunmuştur. Bu doğrultuda, araştırmanın H3 ve H4 ana hipotezleri ile H4a ve H4b alt hipotezleri şu şekilde kurulmuştur:

H3: Bilgi güvenliği stresi, iş performansını pozitif ve anlamlı olarak etkilemektedir.

H4: Bilgi güvenliği farkındalığının iş performansı üzerindeki etkisinde bilgi güvenliği stresinin aracı rolü vardır.

H4a: Saldırı ve tehditlerin iş performansı üzerindeki etkisinde bilgi güvenliği stresinin aracı rolü vardır.

H4b: Kişisel verilerin korunmasının iş performansı üzerindeki etkisinde bilgi güvenliği stresinin aracı rolü vardır.

3. YÖNTEM

Bilgi güvenliği farkındalığının iş performansı üzerindeki etkisinde bilgi güvenliği stresinin aracı rolünü incelemeye yönelik bu çalışmada, önce örneklem ve ölçeklere ilişkin bilgilere yer verilmiştir. Sonrasında SPSS 22.0 paket programı vasıtasıyla, örneklem grubundan elde edilmiş olan veriler çerçevesinde Şekil 1'de yer alan araştırma modeline ilişkin analizler gerçekleştirilmiştir. Yapılan analizlerin neticesinde elde edilen bulgular, literatürdeki önceki araştırmaların bulguları ile karşılaştırılarak önerilerde bulunulmuştur. Kuramdan ve görgül araştırmalardan yola çıkılarak meydana getirilen araştırma modeli Şekil 1'de yer almaktadır. Model çerçevesinde bağımlı değişken iş performansıdır. Bağımsız değişken ise bilgi güvenliği farkındalığıdır. Bağımlı değişken ile bağımsız değişkenin arasında bulunan ilişkinin yönü ve tesirinin üzerinde rolü bulunduğu düşünülen aracı değişken ise bilgi güvenliği stresidir.

Şekil 1. Araştırma Modeli

3.1. Örneklem

Araştırmanın evrenini, Türkiye'nin Mardin ilinde çalışan sağlık personeli oluşturmaktadır. Evrende 2.000 kişi bulunmaktadır. %95 güvenilirlik düzeyinde evreni temsil edebilecek örneklem sayısı 322 olarak hesaplanmıştır. Bu doğrultuda, 500 kişiye anket formu gönderilmiş, 345 kişinden geri dönüş olmuş, 15 kişiye ait veriler özensiz doldurma nedeniyle analiz dışı tutulmuş, kalan 330 kişi ile analize devam edilmiştir. Örneklem olarak sağlık kurumunun seçilmesinin sebebi, COVID-19 sürecinde bilgi güvenliğinin sağlık kuruluşlarında her zamankinden daha önemli hale gelmesi ve bu durumun çalışanların tutum ve davranışlarına etkisinin olabileceği düşüncesinden kaynaklanmaktadır. Basit tesadüfi örnekleme tekniği ile Mardin Devlet Hastanesi çalışanları üzerinde, aşağıda detayları yer alan anket formu uygulanmıştır. Anket uygulaması 10 Nisan 2020 ile 10 Haziran 2020 tarihleri arasında gerçekleştirilmiştir. Anket uygulamasına ilişkin olarak, T.C. Sağlık Bakanlığı Mardin İl Sağlık Müdürlüğü'nden 01.04.2020 tarihinde 37201737-806.02.02 sayılı etik kurul izni alınmıştır.

Araştırmaya katılanların cinsiyet açısından 130'u (%39,4) kadın, 200'ü (%60,6) erkektir. Yaş grubuna göre, 43 kişi (%13,0) 18-25 yaş grubunda, 145 kişi (%43,9) 26-34 yaş grubunda, 108 kişi (%32,7) 35-44 yaş grubunda, 34 kişi (%10,4) 45 ve üzeri yaş grubundadır. Medeni durum bakımından, 113 kişi (%34,2) bekar, 209 kişi (%63,3) evli olup, 8 kişi (%2,4) diğer seçeneğini işaretlemiştir. Eğitim durumu açısından, 117 kişi (%35,5) lise mezunu, 55 kişi (%16,7) önlisans mezunu, 123 kişi (%37,3) lisans mezunu, 18 kişi (%5,5) yüksek lisans mezunu, 17 kişi (%5,2) doktora mezunudur. Mesleki tecrübeye göre, 21 kişi (%6,4) 1 yıldan az, 30 kişi (%9,1) 1-3 yıllık, 63 kişi (%19,1) 3-5 yıllık, 94 kişi (%28,5) 5-10 yıllık, 122 kişi (%37,0) 10 yıldan fazla mesleki tecrübeye sahiptir. Kurumda çalışma süresi bakımından, 35 kişi (%10,6) 1 yıldan az süredir, 66 kişi (%20,0) 1-3 yıldır, 80 kişi (%24,2) 3-5 yıldır, 72 kişi (%21,8) 5-10 yıldır, 77 kişi (%23,3) 10 yıldan fazla süredir aynı kurumda çalışmaktadır. Kurumdaki görev açısından, 31 kişi (%9,4) hekim olarak, 130 kişi (%39,4) hemşire olarak, 169 kişi (%51,2) diğer sağlık personeli olarak vazife yapmaktadır.

3.2. Araştırmanın Ölçekleri

Sağlık personeli üzerinde uygulanan anket formu dört bölümden meydana gelmektedir. Anket formunun ilk bölümünde, katılımcıların demografik özelliklerini tespit etmeye yönelik olarak cinsiyet, yaş, medeni durum, eğitim düzeyi, mesleki tecrübe, kurumda çalışma süresi ve çalışılan bölüm olmak üzere 7 soru bulunan Kişisel Bilgi Formu yer almaktadır.

Anket formunun ikinci bölümde, çalışanların bilgi güvenliği farkındalıklarını belirlemek üzere Keser ve Güldüren (2015) tarafından geliştirilen 34 maddelik Bilgi Güvenliği Farkındalık Ölçeği kullanılmıştır. Ölçek; saldırı ve tehditler ile kişisel verilerin korunması şeklinde iki alt boyuttan meydana gelmektedir. Ölçek 5'li likert tipi ölçektir.

Ölçek üzerinde faktör analizinde ortaya çıkan KMO değeri (0,963) üzerinde çalışılan örneklem grubunun sayısal anlamda faktör analizinin gerçekleştirilmesi konusunda yeterli olduğunu göstermiştir. Bartlett Küresellik Testi sonucunun anlamlı çıkmış olması (Ki-Kare: 9319,479; sd: 325; Sig.: 0,000) ise bu ölçek üzerinde faktör analizi yapılabileceğini göstermektedir. Faktör analizinde en uygun faktör yapılarına ulaşabilmek maksadıyla 8 ifade ölçekten çıkartılmıştır.[1] Gerçekleştirilen faktör analizi neticesinde, ölçeğin iki faktörden meydana geldiği tespit edilmiş ve elde edilen faktörler orijinal ölçekle uyumlu şekilde "saldırı ve tehditler" (ST) ile "kişisel verilerin korunması" (KVK) biçiminde isimlendirilmiştir. Ölçeğin toplam açıklanan varyansı %70,231'dir. ST faktörü varyansın %39,36'sını, KVK faktörü varyansın %30,87'sini açıklamaktadır. Yapılan güvenilirlik analizi neticesinde; ölçeğin güvenilirliğinin 0,975; ST faktörünün güvenilirliğinin 0,970; KVK faktörünün güvenilirliğinin 0,950 ile oldukça yüksek düzeyde olduğu tespit edilmiştir.

Anket formunun üçüncü bölümde, çalışanların bilgi güvenliği stres düzeylerini ölçmek üzere Ayyagari vd. (2011) tarafından geliştirilen 8 maddelik Bilgi Güvenliği Stresi Ölçeği kullanılmıştır. Ölçek tek boyutlu olup, 5'li likert tipidir.

Ölçek üzerinde gerçekleştirilen faktör analizinde ortaya çıkan KMO değeri (0,933) üzerinde çalışılan örneklem grubunun sayısal anlamda faktör analizinin gerçekleştirilmesi konusunda yeterli olduğunu göstermiştir. Bartlett Küresellik Testi sonucunun anlamlı çıkmış olması (Ki-Kare: 2771,189; sd: 28; Sig.: 0,000) ise bu ölçek üzerinde faktör analizi yapılabileceğini göstermektedir. Gerçekleştirilen faktör analizi neticesinde, ölçeğin orijinal ölçekle uyumlu şekilde tek faktörden meydana geldiği tespit edilmiştir. Ölçeğin toplam açıklanan varyansı %77,316'dır. Yapılan güvenilirlik analizi neticesinde, ölçeğin güvenilirliği 0,958 ile oldukça yüksek düzeyde çıkmıştır.

Anket formunun dördüncü bölümde, çalışan performansını ölçmek üzere Kirkman ve Rosen (1999) tarafından geliştirilen, Çöl (2008) tarafından Türkçe uyarlaması yapılan 4 maddelik İşgören Performans Ölçeği kullanılmıştır. Ölçek tek boyutlu olup, 5'li likerttir.

Ölçek üzerinde gerçekleştirilen faktör analizinde ortaya çıkan KMO değeri (0,845) üzerinde çalışılan örneklem grubunun sayısal anlamda faktör analizinin gerçekleştirilmesi konusunda yeterli olduğunu göstermiştir. Bartlett Küresellik Testi sonucunun anlamlı çıkmış olması (Ki-Kare: 1205,929; sd: 6; Sig.: 0,000) ise bu ölçek üzerinde faktör analizi yapılabileceğini göstermektedir. Gerçekleştirilen faktör analizi neticesinde, ölçeğin orijinal ölçekle uyumlu şekilde tek faktörden meydana geldiği tespit edilmiştir. Ölçeğin toplam açıklanan varyansı %84,642'dir. Yapılan güvenilirlik analizi neticesinde, ölçeğin güvenilirliği 0,939 ile oldukça yüksek düzeyde çıkmıştır.

Ölçekler üzerinde gerçekleştirilen faktör ve güvenilirlikleri neticesinde ortaya çıkan faktörler incelendiğinde; ST faktörünün ortalaması $\bar{x}$=2,9574 ile ortalamanın biraz altında, KVK faktörünün ortalaması $\bar{x}$=3,3873 ile ortalamanın üzerinde, BGF ölçeğinin ortalaması $\bar{x}$=3,1393 ile ortalamanın biraz üzerinde, BGS ölçeğinin ortalaması $\bar{x}$=2,9920 ile ortalamanın biraz altında, İP ölçeğinin ortalaması ise $\bar{x}$=4,0402 ile yüksek düzeyde

[1] Bu ifadeler sırasıyla "BGF17-Bilgi güvenliğinin ne anlama geldiğini biliyorum.", "BGF21-Bilgisayarımdaki virüs koruma yazılımının gerçek zamanlı koruma (real tim eprotection) özelliğini kullanmaktayım.", "BGF22-Bilgisayarımdaki virüs koruma yazılımının otomatik güncelleştirme yapmasını sağlayabilirim.", "BGF6-Bilgisayarıma casus yazılım yüklenmesini engelleme yöntemlerini biliyorum.", "BGF4-Zincir e-postalara (chain e-mail) karşı nasıl hareket etmem gerektiğini biliyorum.", "BGF27-İstenmeyen elektronik posta miktarını azaltmak için gerekli bilgiye sahibim.", "BGF3-Aldatmaca (hoax) nedir biliyorum." ve "BGF18-Bilgi güvenliği ile ilgili sorumluluklarımın ne olduğunu biliyorum." şeklindedir.

çıkmıştır. Her bir faktörün basıklık ve çarpıklık değerlerine bakıldığında, basıklık ve çarpıklık değerlerinin (-2) ile (+2) arasında olmasından ötürü, faktörlerin normal dağılıma sahip oldukları söylenebilir ($ST_{çarpıklık}$=-0,107; $ST_{basıklık}$=-0,934; $KVK_{çarpıklık}$=-0,479; $KVK_{basıklık}$=-0,623; $BGF_{çarpıklık}$=-0,257; $ST_{basıklık}$=-0,746; $BGS_{çarpıklık}$=-0,063; $BGS_{basıklık}$=-0,815; $İP_{çarpıklık}$=-1,177; $ST_{basıklık}$=1,275).

4. BULGULAR

Araştırma kapsamında öncelikle katılımcıların bilgi güvenliği farkındalığının saldırı ve tehditler ile kişisel verilerin korunması faktörleri, bilgi güvenliği stresi ve iş performansı düzeylerine yönelik olarak elde edilmiş olan verilerin ortalamaları, standart sapmaları ve aralarındaki ilişkilere bakılmıştır. Analizin ikinci safhasında, kurulmuş olan modelle ilintili olarak regresyon analizleri vasıtasıyla aracılık testi yapılmıştır.

Analiz sonucunda elde edilen ortalamalar, standart sapmalar ve korelasyon değerleri Tablo 1'de gösterilmiştir. Tablo 1'de görüldüğü üzere, tüm değişkenlerin arasında pozitif yönlü ve anlamlı ilişkilere rastlanmıştır.

Tablo 1. Korelasyon Analizi Bulguları

Değişkenler	Ort.	SS	1	2	3	4
Saldırı ve Tehditler	2,9574	1,10549	(0,970)			
Kişisel Verilerin Korunması	3,3873	1,08386	,771**	(0,950)		
Bilgi Güvenliği Stresi	2,992	1,04877	,145**	,177**	(0,958)	
İş Performansı	4,0402	0,89859	,224**	,328**	,195**	(0,939)
**. 0,01 anlamlılık düzeyinde anlamlı; ( ): Güvenilirlik düzeyi						

Bilgi güvenliği farkındalığının iş performansı üzerindeki etkisinde bilgi güvenliği stresinin aracı rolünün olup olmadığını saptamak için, SPSS uygulamasında PROCESS v4.0'tan faydalanılarak, Andrew F. Hayes tarafından geliştirilen Hayes macrosu model 4 kullanılmıştır. Bu modellemeye göre bağımsız değişkenin hem bağımlı değişken hem de aracı değişken üzerinde anlamlı etkisinin bulunması gerekmektedir. Bununla beraber, aracı değişkenin de bağımsız değişkenle birlikte analize dâhil edilmesiyle, bağımsız değişkenin bağımlı değişken üzerindeki regresyon katsayısının düşmesi, aracı değişkenin de bağımlı değişkenin üzerindeki anlamlı etkisinin sürmesi gereklidir (Preacher ve Hayes 2008).

BGF, ST ve KVK şeklinde iki faktörden meydana geldiğinden, her bir faktörün (ST ve KVK) İP üzerindeki etkisinde BGS'nin aracı rolünü saptamak için ayrı ayrı regresyon analizleri yapılmıştır.

Öncelikle ST'nin, İP üzerindeki etkisinde BGS'nin aracı rolü incelenmiştir. Analiz bulguları Tablo 2'de verilmiştir. Bu noktada ilk olarak ST'nin BGS üzerindeki etkisi incelenmiştir. Yapılan analizde; R^2 değeri 0,021; F değeri 6,9999; p değeri 0,0085 şeklinde bulunmuştur. Buna göre, regresyon modelinin istatistiksel bakımdan anlamlı olduğu söylenebilir. Bağımsız değişken olan ST'nin (ß=0,1371; p=0,0085) BGS üzerinde anlamlı, pozitif yönlü ve düşük düzeyli etkisi bulunduğu saptanmıştır. LLCI ve ULCI güven aralıklarına bakıldığında, analiz sonucunun anlamlı olduğu teyit edilmiştir. "*H2a: Saldırı ve tehditler, bilgi güvenliği stresini pozitif ve anlamlı olarak etkilemektedir*." hipotezi kabul edilmiştir. İkinci olarak ST'nin İP üzerindeki etkisi incelenmiştir. Yapılan analizde; R^2 değeri 0,050; F değeri 17,397; p değeri 0,000 şeklinde bulunmuştur. Buna göre, regresyon modelinin istatistiksel bakımdan anlamlı olduğu söylenebilir. Bağımsız değişken olan ST'nin (ß=0,1824; p=0,00) İP üzerinde anlamlı, pozitif yönlü ve düşük düzeyli etkisi bulunduğu saptanmıştır. LLCI ve ULCI güven aralıklarına bakıldığında, analiz sonucunun anlamlı olduğu teyit edilmiştir. Bu doğrultuda, "*H1a: Saldırı ve tehditler, iş performansını pozitif ve anlamlı olarak etkilemektedir*." hipotezi kabul edilmiştir. Üçüncü olarak aracı değişken olan BGS'nin ve bağımsız değişken olan ST'nin bağımlı değişken olan İP üzerinde birlikte etkisi incelenmiştir. Yapılan analizde; R^2 değeri 0,077; F değeri 13,7125; p değeri 0,000 şeklinde bulunmuştur. Buna göre, regresyon modelinin istatistiksel bakımdan anlamlı olduğu söylenebilir. Bağımsız değişken olan ST'nin (ß=0,1629; p=0,0002) İP üzerinde anlamlı, pozitif yönlü ve düşük düzeyli etkisi bulunduğu, ayrıca aracı değişken olan BGS'nin (ß=0,1423; p=0,0021) İP üzerinde anlamlı, pozitif yönlü ve düşük düzeyli etkisi bulunduğu saptanmıştır. LLCI ve ULCI güven aralıklarına bakıldığında, analiz

sonucunun anlamlı olduğu teyit edilmiştir. Bu doğrultuda, "*H3: Bilgi güvenliği stresi, iş performansını pozitif ve anlamlı olarak etkilemektedir*." hipotezi kabul edilmiştir. Yanı sıra, ST'nin İP üzerindeki etkisinde 0,0195 düzeyinde bir azalma görülmüştür. ST'nin İP üzerindeki etkisine ilişkin elde edilen sigma değeri yine (p<0,05) olduğundan, BGS'nin, ST'nin İP üzerindeki etkisinde kısmi, pozitif yönlü ve düşük düzeyli bir aracılık rolünün olduğu bulgusu elde edilmiştir. Bu doğrultuda, "*H4a: Saldırı ve tehditlerin iş performansı üzerindeki etkisinde bilgi güvenliği stresinin aracı rolü vardır*." hipotezi kısmen kabul edilmiştir.

Tablo 2. ST'nin İP Üzerindeki Etkisinde BGS'nin Aracı Rolüne İlişkin Test Sonuçları

Bağımlı Değişken: BGS	**ß-değeri**	**t-değeri**	**p-değeri**	**R^2**	**Model F-değeri**	**Model p-değeri**	**LLCI**	**ULCI**
ST	0,1371	2,6457	0,0085	0,021	6,9999	0,0085	0,035	0,239
Bağımlı Değişken: İP	**ß-değeri**	**t-değeri**	**p-değeri**	**R^2**	**Model F-değeri**	**Model p-değeri**	**LLCI**	**ULCI**
ST	0,1824	4,1710	0,0000	0,050	17,397	0,0000	0,096	0,269
Bağımlı Değişken: İP	**ß-değeri**	**t-değeri**	**p-değeri**	**R^2**	**Model F-değeri**	**Model p-değeri**	**LLCI**	**ULCI**
ST	0,1629	3,7335	0,0002	0,077	13,7125	0,0000	0,077	0,249
BGS	0,1423	3,0941	0,0021				0,052	0,233
Aracılık Rolü	**ß-değeri**						**LLCI**	**ULCI**
BGS	0,0195						0,002	0,056

İkinci olarak KVK'nın, İP üzerindeki etkisinde BGS'nin aracı rolü incelenmiştir. Analiz bulguları Tabo 3'te verilmiştir. Bu noktada ilk olarak KVK'nın BGS üzerindeki etkisi incelenmiştir. Yapılan analizde; R^2 değeri 0,031; F değeri 10,6135; p değeri 0,0012 şeklinde bulunmuştur. Buna göre, regresyon modelinin istatistiksel bakımdan anlamlı olduğu söylenebilir. Bağımsız değişken olan KVK'nın (ß=0,1713; p=0,0012) BGS üzerinde anlamlı, pozitif yönlü ve düşük düzeyli etkisi bulunduğu saptanmıştır. LLCI ve ULCI güven aralıklarına bakıldığında, analiz sonucunun anlamlı olduğu teyit edilmiştir. "*H2b: Kişisel verilerin korunması, bilgi güvenliği stresini pozitif ve anlamlı olarak etkilemektedir*." hipotezi kabul edilmiştir. İkinci olarak KVK'nın İP üzerindeki etkisi incelenmiştir. Yapılan analizde; R^2 değeri 0,108; F değeri 39,5565; p değeri 0,000 şeklinde bulunmuştur. Buna göre, regresyon modelinin istatistiksel bakımdan anlamlı olduğu söylenebilir. Bağımsız değişken olan KVK'nın (ß=0,2720; p=0,000) İP üzerinde anlamlı, pozitif yönlü ve düşük düzeyli etkisi bulunduğu saptanmıştır. LLCI ve ULCI güven aralıklarına bakıldığında, analiz sonucunun anlamlı olduğu teyit edilmiştir. Bu doğrultuda, "*H2a: Kişisel verilerin korunması, iş performansını pozitif ve anlamlı olarak etkilemektedir*." hipotezi kabul edilmiştir. Üçüncü olarak aracı değişken olan BGS'nin ve bağımsız değişken olan KVK'nın bağımlı değişken olan İP üzerinde birlikte etkisi incelenmiştir. Yapılan analizde; R^2 değeri 0,127; F değeri 23,7836; p değeri 0,000 şeklinde bulunmuştur. Buna göre, regresyon modelinin istatistiksel bakımdan anlamlı olduğu söylenebilir. Bağımsız değişken olan KVK'nın (ß=0,2512; p=0,000) İP üzerinde anlamlı, pozitif yönlü ve düşük düzeyli etkisi bulunduğu, ayrıca aracı değişken olan BGS'nin (ß=0,1212; p=0,0074) İP üzerinde anlamlı, pozitif yönlü ve düşük düzeyli etkisi bulunduğu saptanmıştır. LLCI ve ULCI güven aralıklarına bakıldığında, analiz sonucunun anlamlı olduğu teyit edilmiştir. Bu doğrultuda, "*H3: Bilgi güvenliği stresi, iş performansını pozitif ve anlamlı olarak etkilemektedir*." hipotezi kabul edilmiştir. Yanı sıra, KVK'nın İP üzerindeki etkisinde 0,0208 düzeyinde bir azalma görülmüştür. KVK'nın İP üzerindeki etkisine ilişkin elde edilen sigma değeri yine (p<0,05) olduğundan, BGS'nin, KVK'nın İP üzerindeki etkisinde kısmi, pozitif yönlü ve düşük düzeyli bir aracılık rolünün olduğu bulgusu elde edilmiştir. Bu doğrultuda, "*H4b: Saldırı ve tehditlerin iş performansı üzerindeki etkisinde bilgi güvenliği stresinin aracı rolü vardır*." hipotezi kısmen kabul edilmiştir.

Tablo 3. KVK'nın İP Üzerindeki Etkisinde BGS'nin Aracı Rolüne İlişkin Test Sonuçları

Bağımlı Değişken: BGS	**ß-değeri**	**t-değeri**	**p-değeri**	**R2**	**Model F-değeri**	**Model p-değeri**	**LLCI**	**ULCI**
KVK	0,1713	3,2578	0,0012	0,031	10,6135	0,0012	0,068	0,275
Bağımlı Değişken: İP	**ß-değeri**	**t-değeri**	**p-değeri**	**R2**	**Model F-değeri**	**Model p-değeri**	**LLCI**	**ULCI**
KVK	0,2720	6,2894	0,0000	0,108	39,5565	0,0000	0,187	0,357
Bağımlı Değişken: İP	**ß-değeri**	**t-değeri**	**p-değeri**	**R2**	**Model F-değeri**	**Model p-değeri**	**LLCI**	**ULCI**
KVK	0,2512	5,7719	0,0000	0,127	23,7836	0,0000	0,166	0,337
BGS	0,1212	2,6937	0,0074				0,033	0,21
Aracılık Rolü	**ß-değeri**						**LLCI**	**ULCI**
BGS	0,0208						0,002	0,047

Hipotez testleri sonucunda elde edilen bulgulara göre:

- H_{1a} ve H_{1b} kabul edildiğinden, "***H1***: Bilgi güvenliği farkındalığı, iş performansını etkilemektedir." hipotezi kabul edilmiştir.
- H_{2a} ve H_{2b} kabul edildiğinden, "***H2:*** Bilgi güvenliği farkındalığı, bilgi güvenliği stresini etkilemektedir." hipotezi kabul edilmiştir.
- "***H3:*** Bilgi güvenliği stresi, iş performansını etkilemektedir." hipotezi kabul edilmiştir.
- H_{4a} ve H_{4b} kısmen kabul edildiğinden, "***H4:*** Bilgi güvenliği farkındalığının iş performansı üzerindeki etkisinde bilgi güvenliği stresinin aracı rolü vardır." hipotezi kısmen kabul edilmiştir.

5. TARTIŞMA VE SONUÇ

Bu çalışmada Mardin ilindeki sağlık çalışanlarının bilgi güvenliği farkındalıklarının iş performansları üzerindeki etkisinde bilgi güvenliği stresinin aracı rolünün incelenmesi amaçlanmıştır. Bu doğrultuda, COVID-19 pandemi koşulları altında, 10 Nisan 2020 ile 10 Haziran 2020 tarihleri arasında Mardin Devlet Hastanesi çalışanları üzerinde anket uygulaması gerçekleştirilmiştir.

Çalışmanın hipotezlerini test etmek üzere gerçekleştirilen regresyon analizlerinin sonucunda, bilgi güvenliği farkındalığının iş performansı üzerinde anlamlı, pozitif yönlü ve düşük düzeyli etkiye sahip olduğu tespit edilmiştir. Elde edilen bu bulgu, literatürde önceden yapılmış olan çalışmaların bulgularıyla paralellik göstermektedir (Aslandağ, 2010; Akyol, 2013). Bir başka bulgu olarak bilgi güvenliği farkındalığının, bilgi güvenliği stresi üzerinde anlamlı, pozitif yönlü ve düşük düzeyli etkiye sahip olduğu saptanmıştır. Elde edilen bu bulgu, literatürde önceden yapılmış olan çalışmaların bulgularıyla paralellik göstermektedir (Lee vd., 2016; Ament ve Haag, 2016). Diğer bir bulgu olarak bilgi güvenliği stresinin, iş performansı üzerinde anlamlı, pozitif yönlü ve düşük düzeyli etkiye sahip olduğu bulgusu elde edilmiştir. Elde edilen bu bulgu, literatürde önceden yapılmış olan çalışmaların bulgularını desteklemektedir (Bassi, 1997; Smith, 2002; Tarafdar vd., 2011; Azam vd., 2014; Erbi, 2018). Son olarak, bilgi güvenliği farkındalığının iş performansı üzerindeki etkisinde bilgi güvenliği stresinin kısmi, pozitif yönlü ve düşük düzeyli bir aracı rolünün bulunduğu tespit edilmiştir. Elde edilen bu bulgu, literatürde önceden yapılmış olan çalışmaların bulgularını desteklemektedir (Saganuwan vd., 2013).

Sonuç olarak bu çalışma çerçevesinde, COVID-19 pandemi koşulları altında sağlık çalışanları özelinde bilgi güvenliği farkındalığının iş performansı üzerinde etkiye sahip olduğu ve bu etkide bilgi güvenliği stresinin kısmi aracılık rolünün olduğu bulgularına erişilmiştir.

Bu çalışmanın çeşitli sınırlılıkları bulunmaktadır. Konu sınırlılığı açısından araştırma, bilgi güvenliği farkındalığı, bilgi güvenliği stresi ve iş performansı konularıyla sınırlıdır. Bununla birlikte araştırma, anket formunda yer alan sorular ve ölçek maddeleriyle sınırlandırılmıştır. Örneklem bakımından araştırma, Mardin Devlet Hastanesi çalışanları ile sınırlı durumdadır. Araştırmada zaman sınırlılığı vardır. Anket uygulaması 10 Nisan 2020 ile 10 Haziran 2020 tarihleri arasında gerçekleştirilmiştir. Bahsi geçen tarih aralığı, Türkiye'de COVID-19 pandemi sürecinin başlayıp gelişim gösterdiği sürece denk gelmektedir.

Elde edilen bulgular doğrultusunda, sağlık çalışanlarının bilgi güvenliği farkındalığını artırmaya yönelik olarak hastanelerde çeşitli düzenlemeler ve faaliyetler gerçekleştirilmesi gerektiği, bilgi güvenliğini stresini azaltmak üzere bilgi güvenliği farkındalığının artırılması gerektiği, iş performansının yükseltilmesi hususunda bilgi güvenliği farkındalığı konusuna hastanelerde ehemmiyet verilmesi gerektiği söylenebilir.

İleride yapılabilecek olan çalışmalarda, benzer araştırmalar farklı sektörlerde uygulanabilir. Ayrıca sağlık çalışanlarının bilgi güvenliği farkındalıkları ile ilgili olarak başka şehirlerde araştırmalar gerçekleştirilmesi önerilebilir. Bunun yanı sıra, sağlık çalışanlarının iş performansını etkileyen başka faktörlerle ilgili araştırmalar yapılabilir.

KAYNAKÇA

Acılar, A. (2009). İşletmelerde bilgi güvenliği ve örgüt kültürü. *Organizasyon ve Yönetim Bilimleri Dergisi, 1*(1), 25-33.

Akgemci, T. (2001). Örgütlerde stres ve yönetimi. *Atatürk Üniversitesi İktisadi ve İdari Bilimler Dergisi, 5*(1-2), 301-309.

Akyol, F. (2013). *COBİT uygulayan şirketlerdeki bilgi güvenliği politikalarının şirket personel ve süreçlere etkileri*. Yayımlanmamış Yüksek Lisans Tezi. Beykent Üniversitesi, İstanbul.

Ament, C., & Haag, S. (2016). *How information security requirements stress employees*, Thirty Seventh International Conference on Information Systems, Dublin, 13-15.

Aslandağ, K. (2010). *Bilgi güvenliği kavramı ve bilgi güvenliği yönetim sistemleri ile şirket performansı ilişkisine dair bir uygulama*. Yayımlanmamış Yüksek Lisans Tezi. Gebze Yüksek Teknoloji Enstitüsü, Gebze.

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

Azam, N. H. N., Abidin, N. E., Yusof, M. A. M., Emang, S., & Entigar, G. S. (2014). A case study: Technostress creators and employees' job performance in Universiti Teknologi Mara Melaka". *Australian Journal of Basic and Applied Science, 8*(23), 33-37.

Bassi, J. B. (1997). Intellectual capital. *Training & Development*, (December), 25-30.

Başaranoğlu, E. (2016). Bilgi güvenliği unsurları (CIA ve diğerleri). Siberportal, 25 Ocak, https://www.siberportal.org/white-team/securing-information/bilgi-guvenligi-unsurlari-cia-ve-digerleri/ adresinden 20 Mayıs 2020 tarihinde edinilmiştir.

Bayram, L. (2005). Yönetimde yeni bir paradigma: Örgütsel bağlılık. *Sayıştay Dergisi*, (59), 125-139.

Brykczynski, B., & Small, B. (2003). Securing your organization's information assets". *CROSSTALK The Journal of Defense Software Engineering, 16*(5), 12-16.

Canbek, G., & Sağıroğlu, Ş. (2006). Bilgi, bilgi güvenliği ve süreçleri üzerine bir inceleme. *Politeknik Dergisi, 9*(3), 165-174.

Çöl, G. (2008). Algılanan güçlendirmenin işgören performansı üzerine etkileri. *Doğuş Üniversitesi Dergisi, 9*(1), 35 46.

Doğan, Y., & Özdevecioğlu, M. (2009). Pozitif ve negatif duygusallığın çalışanların performansları üzerindeki etkisi. *SÜ İİBF Sosyal ve Ekonomik Araştırmalar Dergisi, 12*(18), 165-190.

Erbi, H. (2018). *Bilgi güvenliği stres faktörlerinin iş tatmini üzerindeki etkileri: Ar-ge merkezi olan işletmeler üzerine bir araştırma*. Yayımlanmamış Yüksek Lisans Tezi. Uludağ Üniversitesi, Bursa.

Erdoğmuş, A. (2017). *Üniversite öğrencilerinin bilgi güvenliği kazanımlarının farkındalıkları üzerindeki etkilerinin analizi: Afyon Kocatepe Üniversitesi örneği.* Yayımlanmamış Yüksek Lisans Tezi. Afyon Kocatepe Üniversitesi, Afyonkarahisar.

Erol, S., & Sağıroğlu, Ş. (2018). Siber güvenlik farkındalığı, farkındalık ölçümü, yöntem ve modelleri, *Siber güvenlik ve savunma* içinde, Ş. Sağıroğlu, & M. Alkan (Eds.), 104-141. Ankara: Grafiker Yayınları.

Ertan, H. (2008). *Örgütsel bağlılık, iş motivasyonu ve iş performansı arasındaki ilişki: Antalya'da beş yıldızlı otel işletmelerinde bir inceleme*. Yayınlanmış Doktora Tezi. Afyon Kocatepe Üniversitesi, Afyonkarahisar.

Furnell, S., & Clarke, N. (2012). Power to the people? The evolving recognition of human aspects of security. *Computers and Security, 31*(8).

Huang, D. L., Rau, P., & Salvendy, G. (2010). Perception of information security. *Behaviour & Information Technology, 29*(3), 221-232.

İlbaş, Ç. (2009). *Bilişim suçlarının sosyo-kültürel seviyelere göre algı analizi*. Yayımlanmamış Yüksek Lisans Tezi, Başkent Üniversitesi, Ankara.

Jawahar, I. M., & Carr, D. (2007). Conscientiousness and contextual performance the compensatory effects of perceived organizational support and leader-member exchange. *Journal of Managerial Psychology*, (22), 330-349.

Karaman, R. (2009). İşletmelerde performans ölçümünün önemi ve modern bir performans ölçme aracı olarak balanced scorecard. *Sosyal Ekonomik Araştırmalar Dergisi, 8*(16), 410-427.

Keser, H., & Güldüren, C. (2015). Bilgi güvenliği farkındalık ölçeği (BGFÖ) geliştirme çalışması. *Kastamonu Üniversitesi Kastamonu Eğitim Dergisi, 23*(3), 1167-1184.

Kirkman, B. L., & Rosen, B. (1999). Beyond self-management: Antecedents and consequences of team empowerment. *Academy of Management Journal, 42*(1), 58-74.

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

Kruger, H. A., & Kearney, W. D. (2006). Prototype for assessing information security awareness. *Computers & Security, 25*(4), 289-296.

Kutal, G., & Büyükuluslu, A. R. (1996). *Endüstri ilişkileri boyutunda çok uluslu şirketler ve insan kaynağı yönetimi teori ve uygulama*. İstanbul: Der Yayınları.

Lee, C., Lee, C. C., & Kim, S. (2016). Understanding information security stress: Focusing on the type of information security compliance activity. *Computers & Science*, (59), 60-70.

Mahboob, A., & Khan, T. (2016). Technostress and its management techniques: A literature review. *Journal of Human Resource Management, 4*(3), 28-31.

Murphy, K. R., & Cleveland, J. (1995). *Understanding performance appraisal: Social, organizational, and goal-based perspectives*. London: Sage Publication.

Özdevecioğlu, M., & Kanıgur, S. (2009). Çalışanların ilişki ve görev yönelimli liderlik algılamalarının performansları üzerindeki etkileri. *KMU İİBF Dergisi*, (11), 53-82.

Öztemiz, S., & Yılmaz, B. (2013). Bilgi merkezlerinde bilgi güvenliği farkındalığı: Ankara'daki üniversite kütüphaneleri örneği. *Bilgi Dünyası, 14*(1), 87-100.

Preacher, K. J., & Hayes, A. F. (2008). Asymptotic and resampling strategies for assessing and comparing indirect effects in multiple mediator models. *Behavior Research Methods*, (40), 879-891.

Richard, P. J., Devinney, T. M., Yip, G. S., & Johnson, G. (2008). Measuring organizational performance as a dependent variable: Towards methodological best practice. *Journal of Management, 35*(3), 718-804.

Rotundo, M., & Sackett, P. R. (2002). The relative importance of task, citizenship, and counterproductive performance to global ratings of job performance: A policy-capturing approach. *Journal of Applied Psychology, 87*(1), 66-80.

Saganuwan, M. U., Ismail, W. K. W., & Ahmad, U. N. U. (2013). Technostress: Mediating accounting information system performance. *Information Management and Business Review, 5*(6), 270-277.

Sakaoğlu, H. H., Orbatu, D., Emiroğlu, M., & Çakır, Ö. (2020). Covid-19 salgını sırasında sağlık çalışanlarında Spielberger durumluk ve sürekli kaygı düzeyi: Tepecik Hastanesi örneği. *Tepecik Eğitim ve Araştırma Hastanesi Dergisi*, *30*(Ek sayı), 1-9.

Sayarı, N. (2009). *Bilgi güvenliği ve yönetimi*. Ankara: Türkiye Bilişim Derneği.

Siponen, M. T. (2001). Five dimensions of İnformation security awareness". *Computer and Society*, (June), 24-29.

Smith, P. (2002). A performance based approach to knowledge management. *Journal of Knowledge Management Practice*, (March).

Şahinaslan, E., Kandemir, R., & Şahinaslan, Ö. (2009). *Bilgi güvenliği farkındalık eğitim örneği*. Akademik Bilişim 2009 - XI. Akademik Bilişim Konferansı Bildirileri, 11-13 Şubat, Harran Üniversitesi, Şanlıurfa.

Şahinaslan, E., Kantürk, A., Şahinaslan, Ö., & Borandağ, E. (2009). *Kurumlarda bilgi güvenliği farkındalığı, önemi ve oluşturma yöntemleri*. Akademik Bilişim'09 - XI. Akademik Bilişim Konferansı Bildirileri. 11-13 Şubat 2009 Harran Üniversitesi, Şanlıurfa.

Şimşek, M., & Nursoy, M. (2002). *Toplam kalite yönetiminde performans ölçümü*. İstanbul: Hayat Yayıncılık.

Tarafdar, M., Tu, Q., Ragu-Nathan, B. S., & Ragu-Nathan, T. S. (2007). The impact of technostress on role stress and productivity. *Journal of Management Information Systems, 24*(1), 307-334.

Tarafdar, M., Pullins, E., & Ragu-Nathan, T. S. (2011). *Examining impacts of technostress on the professional salesperson's performance*. AMCIS 2011 Proceedings-All Submissions.

Tengilimoğlu, D., Işık, O., & Akbolat, M. (2014). *Sağlık işletmeleri yönetimi*, 6. Basım. Ankara: Nobel Akademik Yayıncılık.

Tutar, H. (2016). *Kriz ve stres yönetimi*, 4. Basım. Ankara: Seçkin Yayıncılık.

Ünlü, O., & Yürür, S. (2011). Duygusal emek, duygusal tükenme ve görev/bağlamsal performans ilişkisi: Yalova'da hizmet sektörü çalışanları ile bir araştırma. *Erciyes Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, (37), 183-207.

Ünver, M., Canbay, C., & Mirzaoğlu, A. G. (2011) *Siber güvenliğin sağlanması: türkiye'deki mevcut durum ve alınması gereken tedbirler*. Ankara: Bilgi Teknolojileri ve İletişim Kurumu.

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

Viswesvaran, C. ve D. S. Ones (2000). Job performance: assessment issues in personnel selection, in *Handbook of personnel selection,* A. Evers, N. Anderson, & O. Voskuijl (Eds.). London: Oxford.

Vural, Y. (2007). *Kurumsal bilgi güvenliği ve sızma (penetrasyon) testleri.* Yayımlanmamış Yüksek Lisans Tezi. Gazi Üniversitesi, Ankara.

Vural, Y., & Sağıroğlu, Ş. (2011). Kurumsal bilgi güvenliğinde güvenlik testleri ve öneriler. *Mühendislik Mimarlık Fakültesi Dergisi, 26*(1), 89-103.

Yılmaz, E., Şahin, Y., & Akbulut, Y. (2016). Öğretmenlerin dijital veri güvenliği farkındalığı. *Sakarya University Journal of Education, 6*(2), 26-45.

Youndt, M. A., & Snell, S. A. (2004). Human resource configurations, intellectual capital and organizational performance. *Journal of Managerial Issues, 16*(3), 337-360.