LOJİSTİK BİLGİ SİSTEMİ GÜVENLİĞİ KÜLTÜRÜ ÜZERİNE BİLGİ SİSTEM GÜVENLİĞİ FARKINDALIĞI VE BAĞLILIĞININ ETKİSİ: KARGO LOJİSTİK FİRMALARINDAN BULGULAR

Yrd. Doç. Dr. Salih Börteçine AVCİ
Atatürk Üniversitesi İktisadi ve İdari Bilimler Fakültesi Kamu Yönetimi Bölümü
savci@atauni.edu.tr

Arş. Gör. Adnan KARATAŞ
Atatürk Üniversitesi İktisadi ve İdari Bilimler Fakültesi Kamu Yönetimi Bölümü
adnan.karatas@atauni.edu.tr

Özet

Tedarik zinciri yönetimindeki lojistik faaliyetlerin büyük bir kısmını günümüzde lojistik bilgi sistemleri üstlenmektedir. Bu kritik önemi nedeniyle lojistik bilgi sistemlerinin güvenliğine yönelik alınan teknik tedbirlerin yanında, örgütsel tedbirlere de ihtiyaç duyulmaktadır. Bu anlamda bilgi sistem güvenliği yalnızca teknik personel değil diğer tüm çalışanlarında katılımını gerektirir. Örgüt içerisinde oluşturulacak kültürel tedbirler ve yöneticilerin bilgi sistem güvenliği farkındalığı ile lojistik firmaların bu konudaki açıklarını ortadan kaldırması söz konusu olabilir. Bu bakış açısıyla mevcut çalışma kargo lojistik firmalarında yerleşik bilgi sistem güveliğine ilişkin kültürel bir yapının varlığı ve yöneticilerin bu konudaki farkındalığının sorgulanması üzerine oluşturulmuştur. Bu amaçla Erzurum ilinde faaliyet gösteren kargo lojistik firmalarında ankete dayalı bir araştırma yapılmıştır. İstatistiksel değerlendirmeler ışığında elde edilen bulgular yöneticiler ve politika yapıcılar açısından değerli sonuçlar barındırmaktadır.

Anahtar Kelimeler: Lojistik Bilgi Sistemi, Bilgi Sistem Kültürü, Bilgi Sistem Bağlılığı, Bilgi Sistem Farkındalığı

THE EFFECT OF LOGISTICS INFORMATION SYSTEM SECURITY AWARENESS AND COMMITMENT ON LOGISTICS INFORMATION SYSTEM SECURITY CULTURE: EVIDENCE FROM CARGO LOGISTICS COMPANIES

Abstract

Logistics information systems undertakes a large part of logistics services in supply chain management, nowadays. For its critical importance, there is a need to take organizational measures besides technical measures related to logistics information systems security. In this sense, information system security requires the participation of not only the technical staff but all other employees. Logistics companies can eliminate the insufficiency in this area with the help of cultural measures which will be established within the organization and the managers' awareness of information system. From this perspective, this study is formed in order to ascertain existence of a cultural structure related the embedded information systems security and to determine managers' awareness about the information system security in the cargo logistics company. For this purpose, questionnaire has been applied to cargo logistics companies which are operating in city of Erzurum in this study. Findings of the study which have been obtained in the light of statistical assessments have significant out comes for managers and policy makers.

Keywords: Logistics İnformation System, İnformation System Culture, İnformation System Commitment, Information System Awareness

1. GİRİŞ

Bilgi sistem güvenliği, dünya çapında tüm organizasyonların üzerinde dikkatle durduğu kritik konulardan biridir. Modern ulusal ekonomiler ve devlet kurumları ve diğer işletmeler hayatta kalabilmek için bilgiye ve bu bilgiyi istenildiği anda ulaşılabilir kılmak için bilgi sistem teknolojilerine ihtiyaç duyarlar. Lojistik sektörü açısından bakıldığında ise bilgi sistemleri; firmaların performansını artıran, maliyet ve rekabet avantajı sağlayan önemli bir araçtır.(Fawcett ve diğ., 2011). Lojistik bilgi sistemine bağlı faaliyetlerde ve bilgi sistemlerine yönelik ihlaller, hırsızlıklar, silinmeler ve diğer türdeki bilgi kaynaklarının kaybında bilgi sistemlerinin güvenliği sorunu ön plana çıkmaktadır(Stanton ve diğ., 2003). Bilgi güvenliği ile ilgili yapılan çalışmalar bilgi varlıklarına yönelik tehditleri azaltmak ve koruma sağlamak için teknik, davranışsal, yönetimsel, filozofik ve örgütsel yaklaşımlara ihtiyaç duyulduğunu ortaya koymuştur.(Zafar ve Clark, 2009). Bu anlamda yapılan bazı çalışmalar güvenliğe yönelik sosyo-filozofik ya da sosyo-organizasyonel konuların teknik konular kadar önemli olduğunu göstermektedir.(Zafar ve Clark, 2009).

Kurumlar kendi sistemlerinin dış saldırılara karşı kırılganlığından şikâyetçi olmalarına rağmen güvenlik ihlallerinin büyük bir çoğunluğu organizasyonların iç faaliyetlerinden kaynaklanmaktadır.(Stanton ve diğ., 2003). Bu hususta organizasyonda yer alan tüm bireyler bilgi kaynaklarına ulaşma, kullanma, yönetme ve sürdürme konusunda eşit düzeyde sorumluluğa sahiptir.(Stanton ve diğ., 2003). Dolayısıyla bilgi güvenliği tüm organizasyonun etkin katılımını gerektiren ve örgütün kültürel yapısı üzerine temellendirilmesi gereken bir konudur.

Lojistik bilgi sistem güvenliğinin başarısı bireylerin etkin davranışlarından geçmektedir. Sistem yöneticilerinin ve diğer çalışanların uygun ve yapıcı davranışları bilgi güvenliğinin etkinliğini artırır.(Stanton ve diğ., 2003). Kurum personelinin davranışlarını şekillendirilmesinde önemli rolü olan örgüt kültürü ile lojistik bilgi sistem güvenliği arasında yakın bir ilişki bulunmaktadır.(Acılar, 2009). Çalışanların algıladıkları bilgi güvenlik düzeyleri ve yaptıkları uygulamalarla ilişkili olan bilgi güvenliği faaliyetleri aynı zamanda örgüt içindeki davranışlara yön veren örgüt kültürünün bir parçasıdır. Bu hiyerarşik ilişki sebebiyle örgüt kültürünün, bilgi sistem güvenliğini kapsayan çok geniş bir alan olduğunu söyleyebiliriz.(Woodhouse, 2007). Etkili lojistik bilgi sistem güvenliği oluşturulmasının yolu lojistik bilgi sistem güvenliği kültürünün oluşturulmasından geçmektedir ve oluşturulacak kültür ile çalışanlar örgütün varlığı için risk değil teminat bekçisi haline gelmiş olur.(Von Solms, 2000).

Lojistik bilgi sistem güvenliği kültürünün geliştirilebilmesi için bu konu üzerinde çalışan araştırmacılar verimli ve etkin bir lojistik bilgi sistem güvenliğine yönelik üst yönetimin bağlılığının gerekliliğine inanmaktadırlar.(Knapp ve diğ., 2006; Patnayakuni ve Patnayakuni, 2014; Barton ve diğ., 2016). Üst yönetimin bağlılığı, organizasyonların lojistik bilgi sistem güvenliklerinin etkinliği açısından önemlidir. Lojistik bilgi sistem güvenliğine yönelik üst yönetimin bağlılığı esasında organizasyon ve bilgi sistemine yönelik güvenlik riskini azaltacak örgütsel dinamizmin kaynağı olarak kabul edilebilir.(Barton ve diğ., 2016). İnsan davranışları, karmaşık ve çok yüzlü bir özelliğe sahip olması ile lojistik bilgi sistem güvenliğine ilişkin kontrol ve öngörülere karşı meydan okuma potansiyeline sahiptir. Bu nedenle yöneticilerin bilgi sistem güvenliğine yönelik bağlılığı, istenen iş davranışlarının geliştirilmesi açısından önemli bir niteliğe sahiptir.(Stanton ve diğ., 2003).

Bağlılık kadar üst yönetimin lojistik bilgi sistem güvenliğine yönelik farkındalığı da önemlidir. Örgütsel perspektiften baktığımızda lojistik bilgi sistem güvenliğine yönelik farkındalığın olmaması, kurumun başarısızlığına ve bilgi kayıplarına yol açan temel problem olarak karşımıza çıkmaktadır.(Chen, Shaw ve Yang, 2006). Lojistik bilgi sistem güvenliği farkındalığı, lojistik bilgi sistem güvenliğinin ne kadar önemli olduğu konusundaki vurguyu artırarak oluşabilecek muhtemel hatalardan doğan olumsuz etkileri gün yüzüne çıkaran bir etkiye sahiptir.(Hansche, 2001).

Yukarıdaki açıklamalar ışığında bu çalışmanın amacı kargo lojistik firmalarının lojistik bilgi sistem güvenliğinin sağlanmasında, davranışsal bir nitelik taşıyan lojistik bilgi sistem güvenliği kültürünün oluşturulmasının önemi ile ilgili bir konsept geliştirmektir. Bu konsept yardımıyla lojistik bilgi sistem güvenliği kültürünün geliştirilmesinde üst yönetimin lojistik bilgi sistem güvenliğine bağlılığı ve farkındalığının, kültür üzerindeki etkisini araştırmak maksadı ile Erzurum genelinde kargo lojistik firmalarından veriler toplanarak değerlendirmelerde bulunulmuştur. Bu amaçla ilerleyen bölümler öncelikle teorik alt yapının değerlendirilmesi ardından istatistiksel analizler yoluyla bulguların değerlendirmesine ayrılmıştır.

1.1. Lojistik Bilgi Sistem Güvenliği Kültürü

Lojistik hizmetlerde bilgi sistem güvenliğinin rolü; faaliyetlere ve kuruma ilişkin bilginin gizliliği sağlamak, bütünlüğü korumak ve yok olmasına neden olan zararlı şeylerden korumaktır.(Acılar, 2009). Modern teknolojik gelişmelerin getirdiği kolaylıklar ve imkânlar sayesinde çoğu sektörde olduğu gibi lojistik sektöründe de bilgi kaynaklarının bilgisayar ortamına aktarılması söz konusu olmuştur. Bu sebepten ötürü bilgi sistem güvenliği ile bilgi iletişim teknolojileri güvenliği çoğu zaman birbirinin aynısı gibi düşünülmüştür. Bilgi iletişim teknolojileri güvenliği; yazılım, donanım güvenliği ve gizliliğini kapsamaktadır.(Acılar, 2009). Bilgi sistem güvenliğindeki en büyük paradigmalardan olan ve bilgi sistem güvenliğini sadece bilgi teknolojileri güveliği olarak kabul etme düşüncesi, kurumların bilgi sistem güvenliklerine yönelik alacakları önlemlerin teknik düzeyde kalmasına ve bu işi sadece teknik personele bırakmasına neden olmaktadır. Ancak bu işlemler sadece teknik personelle çözülemeyecek kadar önemlidir ve üst yönetimin da katılımını gerektirmektedir.(Woodhouse, 2007).

Lojistik bilgi sistem güvenliğinde örgüt kültürünün öneminden bahsetmeden ve örgüt kültürünü tanımlamadan önce kültürü tanımlamak gerekmektedir. Kültür; bir topluluğu aynı duyuş ve düşünüş birlikteliğine iten topluluk içinde geleneksel hale gelmiş her türlü davranış, düşünce, tutum ve inançlardır.(Acılar, 2009). Örgüt kültürü ise, örgüt içindeki dinamikleri ve örgütün en temel elemanı olan insanın davranışlarını tanımlamak için yapılan birçok araştırmayı içinde barındıran geniş kapsamlı bir alandır.(Ilvonen, 2011). Nihayetinde lojistik bilgi sitem güvenliği kültürü ise; lojistik işletmelerin, gündelik faaliyetlerini yerine getirirken kullandıkları bilginin nasıl kullanılması ve kullanılırken nasıl korunması yönünde güçlü bir anlayışı içerisinde barındırır ve bu anlayışı çalışanlara zamanla kazanılır. Aynı zamanda bu kültür, çalışanlara faaliyetleri yürütürken nasıl davranmaları gerektiğini ve ne tarz davranışların bilgi sistem güvenliği açısından kabul edilebilir olduğunu gösterir.(Adele Da Veiga, Martins ve Eloff, 2007).

Etkili lojistik bilgi sistem güvenliği oluşturulmasının yolu ise lojistik bilgi sistem güvenliği kültürü oluşturmaktan geçmekte ve oluşturulacak kültür ile çalışanlar örgütün varlığı için risk değil teminat bekçisi halini almaktadır.(Von Solms, 2000). Örgüt içinde bilgi sistem güveliği kültürü oluşturulması için önerilen ve literatürde en çok ilgi görmüş model (Nonaka, 1994)'nın "Bilinç Oluşturma Modeli" dir. Bu modelde bilginin tüm kurumlarda geniş bir taban bulması ve yaygınlaşması için dört aşamalı bilgi oluşum sürecini açıklamaktadır. İlk aşama olan sosyalleşme aşamasında; gözükmeyen kültürel değerlerin kişiler arasında geçişi, ikinci adım olan dışsallaşma da ise ilk aşamada paylaşılan gözükmeyen değerlerin, duygu ve düşüncelerin ifade edilmesiyle görünür hale gelmesidir.(Nonaka, 1994). Üçüncü aşama kombinasyon evresidir ve bu evrede görünür hale gelen kültürel değerin çeşitli iletişim araçlarla veya kişisel iletişimle örgüt genelinde yağın bir hal almasıdır.(Nonaka, 1994).Yani kural benzeri bir duruma gelmesidir. Son aşamada ise örgüt geneline yayılan görünür haldeki kültürel değerin bireyler tarafından yeniden içselleşip görünmez bir hal alması yani içselleşmesidir.(Nonaka, 1994).

İşletmedeki personelinin davranışlarını şekillendirilmesinde önemli rolü olan örgüt kültürü ile lojistik bilgi sistem güvenliği arasında yakın ilişki mevcuttur.(Acılar, 2009). Çalışanların algıladıkları bilgi güvenlik düzeyleri ve yaptıkları uygulamalarla ilişkili olan lojistik bilgi güvenlik kültürü; kurum içerisindeki tüm faaliyetleri ve tüm bireyleri kapsayan

aynı zamanda örgüt içindeki davranışlara yön veren örgüt kültürünün bir parçasıdır. Bu hiyerarşik ilişki sebebiyle örgüt kültürünün, bilgi sistem güvenliğini kapsayan çok geniş bir alan olduğunu söyleyebiliriz.(Woodhouse, 2007). Örgüt kültürü hiyerarşik olarak en üst kısımda kabul ettiğimizde kurumsal bilgi sistem güveliği kültürünü onun bir alt dalı kabul edebiliriz. Bilgi güvenliği kültürü de insan faktörünü, eğitimi, teknolojik alt yapıyı içine alan ayrı bir çatı yapı olarak düşünebiliriz.(Vural ve Sağıroğlu, 2008).Örgüt kültürünün çatı yapı olarak kabul ettiğimizde, bilgi sistem güveliği kültürü onun alt kültürel bir paçası olmaktadır. Fakat bu alt kültürel yapı çalışanların gördüğü veya örgüt dışından birinin anlayabileceği şekilde değildir. Örnek vermek gerekirse buz dağının alt kısmını oluşturan bilgi sistem güvenliğinin gözüken kısmı; bilgi sistem güvenliği iklimi olarak adlandırılmaktadır. Daha büyük olan kısım ise bilgi sistem güvenliği kültürünü oluşturmaktadır. Güvenlik iklimi kendi içinde homojen bir yapı sergilemesine karşın, bizim üzerinde durduğumuz konu olan bilgi sistem güveliği kültürü daha çeşitlidir. Bu çeşitliliğin oluşma sebebi kurum içindeki farklı birimler ve farklı çalışma şekillerinden dolayıdır.(Cooper Ph. D, 2000).

Örgüt içerisinde güvenlik kültürü oluşumunu sağlamak amaçlı uygun bir ortamın oluşturulabilmesi için çalışanların örgüt güvenlik kültürüne itaat etmesi gerekmesinin yanı sıra üst yönetimin de bu kültürün yerleşik bir hal alamsını sağlamak için çeşitli uygulamalar yapması, güvenlik politikaları üretmesi ve güvenlik kültürüne karşı ihlalleri önlemek için cezai yaptırımlar uygulaması gerekmektedir. (Ilvonen, 2011). Lojistik bilgi sistem güvenliği konusunda bir lojistik işletmede kültürel değerler oluşup, işletme bünyesinde bu kültürün içselleşmesi için işletmede yer alması gereken kontrol alanlar şu şekilde sıralanabilir.(Marşap, Akalp ve Yeniman, 2010: 38);

- Lojistik işletmelerde bilgi güvenliği politikaları
- Lojistik işletmelerde bilgi güvenliği organizasyonu
- Lojistik işletmelerde bilgi yönetim sistemi
- Lojistikte insan kaynakları güvenliği
- Lojistik bilgi güvenliği sistemlerinde çevresel güvenlik
- Lojistik işletmelerde iletişim ve güvenli iletişim yönetimi
- Lojistik bilgi sistemlerinde çoklu erişim denetimi ve güvenliği
- Lojistik bilgi sistemleri gelişimi ve bakımı
- Lojistikte bilgi güvenliği ihlalleri yönetimi
- Lojistikte bilgi güvenliği ihlalleri yönetimi

1.2. Lojistik Bilgi Sistem Güvenliği Farkındalığı

Örgütsel perspektiften bakıldığında, lojistik kurumlarda bilgi sistemlerine yönelik bilgi eksikliği ve farkındalığın olmaması; kurumun başarısızlığına ve bilgi kayıplarına yol açan temel problem olarak karşımıza çıkmaktadır.(Chen ve diğ., 2006). Kurumların varlıklarını devam ettirebilmeleri ve faaliyetlerini yaparken sorunlarla karşılaşmamak ya da sorun oluştuğunda anında çözüm üretebilmek için sahip olduğu bilginin gizliliği ve bütünlüğünün kontrol altında tutulması gerekmektedir.(Mitnick ve Simon, 2011).

Lojistik bilgi sistem güvenliği farkındalığı, kurum içerisinde çalışan insanların, kurumun sahip olduğu bilginin öneminin ve bu bilgilerin korunabilmesi için kendi güvenlik misyonunun farkında olması ile ilgilidir.(Siponen, 2000). Farkındalık; oluşması muhtemel hataların önüne geçtiği gibi aynı zamanda çalışanların bakış açılarında da değişime sebep olur.(Siponen, 2000). Lojistik bilgi sistem güvenliği yönetimi açısından oldukça önemli olan lojistik bilgi sistem güvenliği farkındalığı, hem genel bilgi sistem güvenliğini hem de lojistik bilgi sistem güvenliği politikaları hakkında bilgi sahibi olunmasını ve uygulanmasını içermektedir.(Bulgurcu, Cavusoglu ve Benbasat, 2010).

Etkili bir lojistik bilgi sistem güveliği politikası oluşturabilmek, kurum içerisindeki yöneticilerin farkındalığını artırmak ve etkili lojistik bilgi güvenliği yönetim sistemi oluşturabilmek için kurum içerisinde teknik ve bilişsel kontrol mekanizmaları oluşturulması oldukça önemlidir.(Kruger ve Kearney, 2006). Lojistik bilgi sistem güvenliği farkındalığı programlarının amacı lojistik bilgi sistem güvenliğinin ne kadar önemli olduğunu konusundaki vurguyu artırmak ve oluşabilecek muhtemel hatalardan doğan olumsuz etkileri gün yüzüne çıkarmaktır.(Hansche, 2001).

Lojistik bilgi sistem güvenliği farkındalığı sağlanması ve eğitim verilmesi gibi konularında kurumun eğitimin gerekliliğini kabul etmesi, üst yönetimin konu hakkında farkındalığının bir göstergesidir.(Katsikas, 2000). Çalışanların lojistik bilgi sistem güvenliği konusunda farkındalığının artırılması minvalinde üst yönetimin -başta kendisi dikkat etmek şartıyla- belli başlı önlemler alması gerekmektedir. Alacakları önlemlerin çoğunluğu personelin bilmediği veya bildiği ancak uygulamadığı işlemlerden oluşacaktır. Ancak çalışanlara yalın olarak bu işlemleri nasıl yapmaları gerektiğinin bildirilmesi, normatif anlam yüklü olması sebebiyle çalışanlar tarafından içselleştirilememe olasılığı taşımaktadır.(Siponen, 2000).

Farkındalık sağlayabilmek için(Kruger ve Kearney, 2006)'in "Altın Kurallar" olarak adlandırdığı altı faktör literatürde genel olarak kabul görmüş ve kurumlar tarafından kullanılmaktadır. Bu kurallar genel itibariyle çalışanları ilgilendirse bile üst yönetiminde uygulaması gerekmektedir. Bunları lojistik işletmeler açısından şu şekilde revize edebiliriz;

- Her durumda ve şartta işletmenin kurallarına sadık kalınmalıdır.

- Kullanıcı adı ve şifrelerini başkalarıyla paylaşılmamalıdır.

- E-posta ve internet kullanırken zararlı siteleri girilmemeli ve eklentiler açılmalıdır.

- Kargo faaliyetlerinde kullanılan, taşınabilir imza aletlerin sorumlusu dışında kullanımını önlenmelidir.

- Bilgi sisteminde oluşan hataları, virüsleri, veri kayıplarını etkili birime bildirilmelidir.

Bu açıklamalar ışığında aşağıdaki hipotez oluşturulmuştur;

H1: Lojistik bilgi sistem güvenliğine yönelik yönetici farkındalığı lojistik bilgi sistem güvenliği kültürünü pozitif ve anlamlı bir şekilde etkiler.

1.3. Lojistik Bilgi Sistem Güvenliğine Yönelik Yönetici Bağlılığı

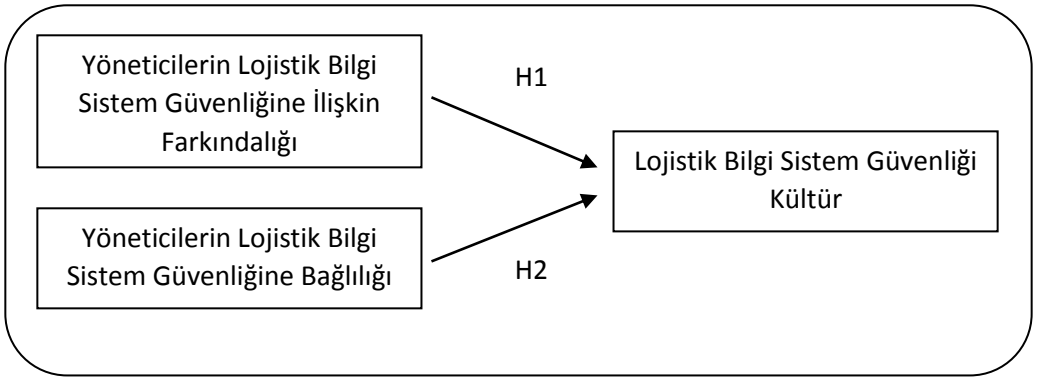
Lojistik sektöründe üst yönetimin bağlılığı konusu, organizasyonların bilgi sistem güvenliğinin etkinliği açısından önemli bir yere sahiptir.(Barton ve diğ., 2016: 9-10). Bağlılık iki yolla tanımlanmaktadır. Bazı çalışmalar da organizasyon ve bireyleri bir davranış hattında tutan psikolojik bir durum olarak kabul etmektedir. Diğer perspektifte ise davranış sürekliliği olarak da kabul edilen bağlılık davranışsal bir perspektiften yorumlanmaktadır. Örneğin bilgi sistem gelişim projesi için bağlılık; sistem gelişiminin adımları, yüklenmesi ve problemlerinin önceden anlaşılması ve bu şekilde davranış geliştirilmesi olarak tanımlanabilir. (Sabherwal, Sein ve Marakas, 2003: 782).

Bu çalışma konseptinden bakıldığında bağlılık, bilgi güvenliği ile ilgili bireylerin zihniyeti ile ilgili geliştirdikleri bir davranış şeklidir. Örgütsel bağlılık bireylerin organizasyonları ile ve örgütsel amaçların başlatılmasına katkıda bulunma isteği ile ilgili psikolojik bir bağ olarak kabul edilmektedir. Bağlılığın üç temel maddesi bulunmaktadır bunlar duygusal, devam ve normatif bağlılıktır. Duygusal bağlılık örgüte yönelik duygusal bir referans noktası olarak kabul edilir. Duygusal bağlılık bireyin örgüte katılım ve örgüt ile tanımlanmaya yönelik olarak psikolojik ve duygusal bağı ifade eder. Devam bağlılığı ise örgütten ayrılmayacağına dair bir teminatı içerir. Burada birey örgütten ayrılmanın kendisi için bir maliyeti olduğunun farkındadır. Normatif bağlılık ise örgütte kalmaya yönelik etik sorumluluğu ifade etmektedir. Yani bireyin bir örgüt ile çalışmasının devamına yönelik sorumluluk hissi ile açıklanabilir (Allen ve Meyer, 1990).

Yapılan çalışmalar da lojistik bilgi sistemlerine yönelik yönetimin desteği vurgulanarak, bu desteğin yöneticinin katılımı ve bağlılığı ile sağlanabileceği vurgulanmıştır. Katılım, bilgi sistemine yönelik planlama, geliştirme ve uygulama gibi bireysel faaliyetler olarak tanımlanırken, bağlılık üst yönetimin bilgi sistemine yönelik ilgisinin derecesini ifade eden yönetimin psikolojik durumunu ifade etmektedir. Üst yönetimin hem katılımı hem de bağlılığı organizasyonun lojistik bilgi sistemine yönelik başarısı için önemlidir ancak yöneticinin bilgi sistem güvenliğine bağlılığı daha etkin bir yere sahiptir. Üst yönetimin lojistik bilgi sistem güvenliğine bağlılığı; örgütlerin kritik düzeyde kurum ortakları ile bilgi paylaşımına imkân sağlayan ve altyapılarını destekleyen bir ön koşuldur (Barton ve diğ., 2016: 10).

Sosyo-örgütsel faktörler ile bilgi sistem güvenliği başarısı arasında kritik bir bağ bulunmaktadır. Lojistik bilgi sistem güvenliğine yönelik üst yönetimin desteği, lojistik bilgi sistem güvenliği kültürünü ve lojistik bilgi sistem güvenliği politikalarına yönelik çalışan kabullerini pozitif olarak etkilemektedir.(Knapp ve diğ., 2006; Adéle Da Veiga ve Martins, 2015; Barton ve diğ., 2016). Bunun yanında üst yönetimin bağlılığı, lojistik bilgi sistem güvenliği kültürünün geliştirilmesi ve etkin bir lojistik bilgi sistem güvenlik kontrol yönetimi için bir gereklilik olarak karşımıza çıkmaktadır. (Barton ve diğ., 2016: 12). Bu açıklamalar ışığında aşağıdaki hipotez oluşturulmuştur.

H2: Lojistik bilgi sistem güvenliğine yönelik yönetici bağlılığı lojistik bilgi sistem güvenliği kültürünü pozitif ve anlamlı bir şekilde etkiler.



Şekil 1: Araştırma Modeli

2. METEDOLOJİ

2.1. Araştırma Soruları

Lojistik sektöründe bilgi sistem güvenliğine ilişkin yapılan çalışmaların büyük bir kısmı teknik konularla ilgilidir. Oysaki bilgi güvenliği teknik bir konu olduğu kadar davranışsal bir özelliğe de sahiptir (Stanton ve diğ., 2003). Lojistik bilgi sistem güvenliğinin davranışsal boyutunda karşılaşılan ilk husus bilgi güvenlik kültürüdür. Davranışsal perspektiften, lojistik firmalarda oluşturulacak bilgi güvenlik kültürü, kurum içi bilgi güvenlik problemlerinin büyük bir kısmını önleyecek şekilde çalışanların katılımını içermektedir. Ancak geliştirilecek bilgi güvenlik kültürünün korunmasında birinci dereceden sorumluluk yöneticilere aittir. Özellikle yöneticilerin bilgi güvenlik kültürünün gelişimi adına, bağlılıkları ve farkındalıklarının önemli bir yere sahiptir. Bilgi güvenliğine ilişkin yöneticilerin bağlılıkları ve farkındalıkları konuları ile bilgi güvenliği kültürü arasındaki ilişki lojistik sektöründe yeterince araştırılmadığı yapılan literatür taraması ile ortaya konmuştur. Bu bakımdan aşağıdaki sorulara dair aranan cevaplar bu çalışmanın temel motivasyon kaynağını oluşturmaktadır:

1- Kargo lojistik kurumlarında; yöneticilerin bilgi sistem güvenliğine bağlılıklarının bilgi sistem güvenliği kültürüne etkisi var mıdır?

2- Kargo lojistik kurumlarında; yöneticilerin bilgi sistem güvenliğine ilişkin farkındalıklarının bilgi sistem güvenliği kültürüne etkisi var mıdır?

2.2. Araştırmanın Kapsamı ve Önemi

Bu çalışma kargo lojistik firmalarında lojistik bilgi sistem güvenliği konusunun davranışsal perspektiften değerlendirilmesi amacı ile hazırlanmıştır. Bu bölümde çalışmaya ilişkin örneğin seçilmesi, örneklemden verilerin toplanması için araçların geliştirilmesi, verilerin toplanma süreci, verilerin toplandığı anket soruların niteliği ve anketin geçerlilik ve güvenilirlik çalışmaları açıklanmıştır.

2.2.1. Ölçek geliştirme ve Örneklem

Araştırmada esas olarak nicel verilere dayalı ölçme yöntemi belirlenmiştir. Bu amaçla bilgi sistem güvenliği kültürü, bilgi sistem güvenliği farkındalığı ve bağlılığı konusunda yöneticilerin tutumlarının değerlendirilmesine yönelik anket soruları hazırlanmıştır. Çalışmaya konu olan faktörleri ölçmek amacıyla yerli, yabancı, kuramsal ve araştırmaya dayalı akademik yayınlar incelenmiştir. Özellikle Mcintosh, (2011) ve Bess, (2012) kitaplarından kültür faktörüyle ilgili, Bulgurcu, (2010) çalışmasından farkındalık ile ilgili soruları hazırlanırken, bağlılık ile ilgili sorular hazırlanırken Allen ve Meyer,(1990)'in çalışmasından yararlanılmıştır. Nihayetinde yazarlarımız tarafından anket soruları hazırlanmıştır.

Anket formu hazırlanırken ilk beş soru lojistik bilgi sistem güveliği kültürünü kurum içerinde varlığının tespitine ilişkin hazırlanmıştır. Ardından çalışanların lojistik bilgi sistem güvenliği konuşunda farkındalık düzeylerinin belirlenmesine ilişkin yedi adet soru hazırlanmıştır. Ardından son değişken olan lojistik bilgi sistem güvenliği bağlılığının ölçülmesi için altı soru hazırlanmıştır. Son olarak demografik özellikler alınmıştır.

Anket soruları 5'li Likert Ölçeği(1-Kesinlikle Katılmıyorum…5- Kesinlikle katılıyorum) şeklinde hazırlanmıştır. Anket çalışması yapılmadan önce anket sorularında tam ifade edilemeyen veya ihtilaflı olan ifadelerin düzeltilmesi için konunun uzmanlarına danışılarak bir ön test yapılmıştır. Ön test sonuçlarına göre nihai anket formu hazırlanmıştır.

Nihai şekli verilen anket, araştırmayı yapan yazarlar tarafından ilgili kurumlara gidilerek yüz yüze görüşme yöntemi ile doldurtulmuştur. Ankete verilecek cevapların samimi, objektif ve amacına uygun olabilmesi için hem anketi yapanlar tarafında çalışanlar bilgilendirilmiş hem de anketin üst kısmına uyarılar yazılarak bilgilendirme yapılmıştır.

Çalışmanın anakütlesi olarak Erzurum ilinde faaliyet gösteren kargo lojistik firmaları seçilmiş ve çalışma Erzurum ili örneği olarak yürütülmüştür. Bu sebepten Erzurum ili sınırları içerisinde faaliyet gösteren özel kargo işletmelerinde ve bir kamu işletmesi olan PTT'nin kargo departmanında çalışan yöneticiler ağırlıklı olarak rastgele yöntemlerle seçilerek anket çalışması yürütülmüştür. Uygulanan anketlerde katılımcıların rastgele cevapladıkları ve boş bırakılan anketler elenerek sonuçta çalışmaya konu olan 51 anket analize dâhil edilmiştir.

2.3. Bulgular

Bu bölümde; araştırma örneğinin demografik özelliklerine ilişkin frekans ve yüzde dağılımlarına, anket sorularına verilen cevapların ortalama ve standart sapmalarına, araştırma kapsamında hazırlanan ölçeklerin güvenilirlik ve geçerliliğine ilişkin olarak yapılan analizlere yer verilmiştir. Son olarak korelasyon ve regresyon analizleri ile istatistiksel değerlendirmeler bitirilmiştir

2.3.1. Araştırma ölçeğinin demografik özellikleri

Tablo 1'de görüldüğü katılımcıların %52,9'u alt düzey yönetici, %47,1'i de orta düzey yöneticilerden oluşmaktadır. Yöneticilerin %82,4'ü kargo %17,6'sının lojistik biriminde çalıştığı ve %19,6'sının beş yılın üzerinde deneyimi olan kişilerden oluştuğu görülmektedir. Diğer taraftan katılımcıların %68,6'sının 25 yaş üzeri, eğitim durumlarının %98,1'inin lise ve üzeri olduğu tespit edilmiştir.

Tablo 1: Araştırma kapsamındaki katılımcıların demografik özellikleri

Cinsiyet	N	%
Erkek	42	82,4
Kadın	9	17,6
Yaş		
18-25	16	31,4
26-35	27	52,9
36-45	8	15,7
Çalıştığı Birim		
Kargo	42	82,4
Lojistik	9	17,6
Çalıştığı Pozisyon		
Alt düzey yönetici	27	52,9
Orta düzey yönetici	24	47,1

Kurumdaki Çalışma Süresi	N	%
0-1 Yıl	15	29,4
1-5 Yıl	26	51,0
6-10 Yıl	8	15,7
11 Yıl ve üstü	2	3,9
Öğrenim Durumu		
İlköğretim	1	2,0
Lise	19	37,3
Üniversite	31	60,8
Sektördeki Çalışma Süresi		
0-1 Yıl	13	25,5
1-5 Yıl	25	49,0
6-10 Yıl	10	19,6
11 Yıl ve üstü	3	5,9

2.3.2. Araştırmada Kullanılan Ölçekler Ve Temel İstatistiksel Sonuçlar

Araştırmanın üç temel değişkeni olan kültür, farkındalık ve bağlılık faktörlerine ait ortalama ve standart sapma değerleri tablo 2'de görülmektedir. Kültür sorularının genel ortalaması 3,814, farkındalık sorularının genel ortalaması 4,213 ve bağlılık sorularının genel ortalaması 3,64 olarak bulunmuştur. Her üç boyutun ortalaması 3,5'un üzerinde gerçekleşmiştir.

Tablo 2: Faktörlere ilişkin anket soruları ve temel istatistik sonuçları

Faktörler	Ort.	Std.sap.
Kültür		
K1-Yönetim, tüm birimlere yönelik bilgi sistem güvenliğine ilişkin bilgilendirme yapmaktadır	4,10	0,922
K2-Yönetim, bilgi sistem güvenliğine ilişkin personelin sorumluluğunu arttırıcı politikalar uygulamaktadır	3,84	0,946
K3-Yönetim lojistik bilgi sistem güvenliği programlarına güçlü bir destek verir	3,64	1,139
K4-Lojistik bilgi sistem güvenliği kurumun güvenlik politikalarına uygun bir şekilde hazırlanır	3,39	1,021
K5-Lojistik bilgi sistem güvenliğine ilişkin düzenli bir denetim sistemi uygulanır	4,10	0,671
Farkındalık		
F1-Bilgi sistemi güvenliğinin bizim işletmemiz için önemli faydalar sağladığının farkındayım	3,98	1,104
F2-Kullandığım tüm bilgi sistem cihazlarının güvenliğini sağlamadan işimi bırakmam	4,27	0,874
F3-Bana ait kullanıcı ad ve şifremi başkaları ile paylaşmam	4,18	1,034
F4-Faaliyet alanıma giren bilgileri orta yerde bırakmamam gerektiğinin farkındayım	4,24	0,815
F5-Bilgi güvenliğine ilişkin her tür ihlali vakit kaybetmeden ilgililere bildirmem gerektiğinin farkındayım	4,29	0,855
F6-Virüslerin bilgi sistemleri için oluşturduğu tehlikenin ve zararların farkındayım	4,27	0,940
F7-Çalıştığım kurum ile ilgili şüpheli bir mail geldiğinde bunu yetkili mercilere bildirmem gerektiğinin farkındayım	4,26	0,777
Bağlılık		
B1-Firmamın bilgi sistem güvenliğine yönelik güvenim tamdır	4,08	0,913
B2-Kullanılan bilgi güvenlik sisteminin değiştirilmesi gerektiğini düşünmüyorum	3,37	1,428
B3-Kullanılan bu bilgi güvenlik sisteminin değiştirilmesi durumunda problem çıkacağını düşünüyorum	3,53	1,239
B4-Sektörde kullanılan tüm bilgi güvenlik sistemlerinin aynı düzeyde olduğunu düşünmekteyim	3,27	1,333
B5-Kullanılan bilgi sistem güvenliği programını değiştirmek maliyetli ve risklidir	3,61	1,112
B6-Lojistik bilgi güvenlik sisteminin korunması yönünde bir sorumluluğum olmadığını düşünüyorum ® (sonuç düzeltilmiş haliyle verilmiştir)	3,98	1,040

2.3.3. Faktör ve Güvenilirlik Analizi Sonuçları

Tablo 3'de kültür değişkenine ait beş, farkındalık değişkenine ait yedi, bağlılık değişkenine ait altı sorunun güvenilirlik ve faktör analizi sonuçları bulunmaktadır. Lojistik bilgi güvenliği kültürü sorularını ölçen soruların Cronbach alfa güvenilirlik katsayısı 0,661 ve faktör yükleri 0,428-0,701 arasında bulunmuştur. Lojistik bilgi güvenliğine ilişkin yöneticilerin farkındalığı sorularını ölçen soruların Cronbach alfa güvenilirlik katsayısı 0,738 ve faktör yükleri 0,433-0,764 arasında değerler almıştır. Son olarak lojistik bilgi güvenliğine ilişkin yöneticilerin bağlılığı sorularını ölçen soruların Cronbach alfa güvenilirlik katsayısı 0,697 ve faktör yükleri 0,527-0,748 arasında değerler almıştır. Her üç değişkene ilişkin güvenilirlik ve geçerlilik düzeylerinin kabul edilebilir sınırlar arasında yer aldığı ortaya çıkmıştır

Tablo 3: Faktörlere ilişkin faktör ve güvenilirlik analizi sonuçları

Değişkenler	SoruSayısı	FaktörünAçıklığı (%)	Cronbach-Alfa	FaktörYükleri
Kültür	5	51,529	0,661	0,428-0,701
Farkındalık	7	19,629	0,738	0,433-0,764
Bağlılık	6	37,615	0,697	0,527-0,748

2.3.4. Lojistik bilgi sistem güvenliği kültürü, bağlılık ve farkındalık arasındaki ilişki

Araştırmada lojistik bilgi güvenliği kültürü, bağlılığı ve farkındalık arasındaki ilişkiyi belirlemek maksadıyla korelasyon analizinden yararlanılmıştır. Bu analize göre kültür ile farkındalık arasında 0,99 önem düzeyinde olumlu yönlü ve anlamlı bir ilişki olduğu (r=0,555) bulunmuştur (Tablo 4). Kültür ve bağlılık arasındaki ilişkiye bakıldığında ise 0,95 önem düzeyinde olumlu yönlü, anlamlı fakat düşük düzeyli bir ilişki (r=0.290) tespit edilmiştir. Son olarak bağlılık ve farkındalık arasındaki ilişkiye bakıldığında 0,95 önem düzeyinde yine olumlu yönlü ve anlamlı bir ilişki (r=0,281) olduğu görülmüştür.

Tablo 4: Korelasyon analizi

Değişkenler	1	2	3
Kültür (1)	1		
Farkındalık (2)	0,555**	1	
Bağlılık (3)	0,290*	0,281*	1

** 0,01 anlamlılık seviyesinde korelasyon (çift yönlü)

* 0,05 anlamlılık seviyesinde korelasyon (çift yönlü)

Korelasyon analizi yardımıyla lojistik bilgi sistem güvenliği kültürü ile lojistik bilgi sistem güvenliğine ilişkin yöneticilerin farkındalığı ve bağlılığı arasındaki ilişkinin varlığı tespit edildikten sonra lojistik bilgi güvenliği kültürü üzerine farkındalık ve bağlılığın etkisini belirlemek maksadıyla basit doğrusal regresyon analizi yapılmıştır.

Bu analizlerden birincisi lojistik bilgi sistem güvenliğine ilişkin yöneticilerin farkındalığının lojistik bilgi sistem güvenliği kültürü üzerindeki etkisini ele almaktadır. Tablo 5'te görüldüğü gibi farkındalık boyutunun kültür boyutu üzerine etkisinde toplam varyansın %30,8'ini açıkladığı ve $p<0.001$ önem düzeyinde anlamlı olduğu görülmektedir (R^2=0,308 ve F=21,849). Farkındalığın kültürü etkileme gücünün (β=0,555 ve $p<0.001$) yüksek düzeyde olduğu görülmektedir. Bu sonuca göre H1 hipotezi kabul edilmiştir.

Tablo 5: Lojistik bilgi sistem güvenliğine ilişkin yöneticilerin farkındalığının lojistik bilgi sistem güvenliği kültürü üzerine etkisi

Faktörler	Bağımlı Değişken: Lojistik Bilgi Sistem Kültürü	
	β	t
Farkındalık	0,555***	4,674
R^2	0,308	
Düzeltilmiş R^2	0,294	
F	21,849***	

*p<0,05 **p<0,01 ***p<0,001

Regresyon analizinin ikinci kısmında ise lojistik bilgi sistem güvenliğine ilişkin yöneticilerin bağlılığının lojistik bilgi sistem güvenliği kültürü üzerine etkisini tespit etmeye yöneliktir. Tablo 6'ya bakıldığında bağımlılık boyutunun kültür boyutu üzerine etkisinde toplam varyansın %8,5'ini açıkladığı ve p<0.05 önem düzeyinde anlamlı olduğu görülmektedir (R^2=0,085 ve F=4,491).Bağımlılığın bağımsız değişken kültürün bağımlı değişken olduğu bu ilişkide bağlılığın kültürü etkileme gücünün (β = 0,290 ve p<0.001) olduğu bulunmuştur. Bu sonuç ise H2 hipotezini desteklemiştir.

Tablo 6: Lojistik bilgi sistem güvenliğine ilişkin yöneticilerin bağlılığının lojistik bilgi sistem güvenliği kültürü üzerine etkisi

Faktörler	Bağımlı Değişken: Lojistik Bilgi Sistem Kültürü	
	β	t
Bağlılık	0,290***	2,119
R^2	0,085	
Düzeltilmiş R^2	0,065	
F	4,491*	

*p<0,05 **p<0,01 ***p<0,001

3. SONUÇ

Bu çalışmanın temel hedefi lojistik bilgi sistem güvenliğini davranışsal bir perspektiften değerlendirerek lojistik bilgi sistem güvenliği kültürü üzerine, yöneticilerin farkındalığı ve bağlılığının etki gücünü tespit etmektir. Bilgi sistemleri dendiğinde akla ilk gelen hep teknik konular olmaktadır. Teknik konuların sosyal ve psikolojik yönleri ele alınmadan yapılacak değerlendirmelerin eksik kalacağı bir gerçektir. Özellikle hızla gelişen ve büyüyen kargo lojistik sektöründe lojistik bilgi sistem güvenliği konusunun davranışsal perspektiften değerlendirilmesi ihtiyacı önem arz etmektedir.

Ülkemizde kargo lojistik sektörü insan kaynağına yönelik uzmanlık açığını kapatmak için gerek sektörel gerekse de eğitim faaliyetleri anlamında gelişmelere sahne olmaktadır. Kargo lojistik sektöründe kurumların problemlerinin çoğu örgütsel nitelik taşımakta ve insan kaynaklı sorunlar ön plana çıkmaktadır. Kargo lojistik sektöründe bilgi sistemlerine gün geçtikçe daha fazla ihtiyaç duyulacağı açıktır. Bu ihtiyaç beraberinde güvenlik sorunlarını gündeme getirmekte ve güvenliğe ilişkin problemlerin çözümü ise insan kaynağından geçmektedir. Özellikle lojistik bilgi sistem güvenliğine ilişkin yegâne sorumluluk yöneticilere aittir. Kargo lojistik örgütlerinde, lojistik bilgi sistem güvenliğine ilişkin faaliyetlerin etkinliği bu konuda geliştirilecek kültürel altyapıya bağlıdır. Firmalarda geliştirilecek lojistik bilgi sistem güvenliği kültürünü destekleyecek nitelikte hazırlıkların yönetici bazında karşılanma ihtiyacı bu anlamda

güncelliğini korumaktadır. Bu amaçla hazırlanan çalışmada bir kültürün gelişmesinde rolü olan farkındalık ve bağlılık konusu lojistik bilgi sistem güvenliği çerçevesinde ele alınmıştır.

Bu çalışma bulgularına göre lojistik bilgi sistem güvenliğine yönelik yönetici farkındalığının ($\overline{X}$ = 4,213) , lojistik bilgi sistem güvenliği kültürü ($\overline{X}$ = 3,814) üzerine etkisi ile ilgili sonuç değerlendirmesi yapıldığında öncelikle kargo lojistik firmalarında belirli düzeyde bilgi sistem güvenliği kültürüne sahip olduğu görülmüştür. Farkındalık konusunda yöneticilerin lojistik bilgi sistem güvenliğine yönelik farkındalıkları ortalamanın üzerindedir. Bu sonuç ankete katılan yöneticilerin lojistik bilgi güvenliğini bütüncül bir bakış açısı ile ele alabildikleri ve bu konunun firmanın rekabet edebilirliği üzerindeki etkisini parça-bütün ilişkisi içerisinde değerlendirebildiklerini göstermektedir. Araştırmanın hipotezlerinden birincisinin üzerine kurulduğu farkındalığın kültür üzerine etkisinde, lojistik bilgi sistem güvenliğine yönelik yönetici bağlılığı firma içerisinde lojistik bilgi sistem güvenliği kültürünü pozitif ve anlamlı bir şekilde etkilediği bulunmuştur. Bilgi sistem güvenliği farkındalığı, kurum içerisinde çalışan insanların, kurumun sahip olduğu bilginin öneminin ve bu bilgilerin korunabilmesi için kendi güvenlik misyonunun farkında olması ile ilgilidir.(Siponen, 2000). Dolayısıyla bulgularımız kültür inşasında ve kültürün devamında yöneticilerin farkındalık düzeyinin pozitif etkileri dikkat alınmalıdır.

Lojistik bilgi sistem güvenliğine yönelik yönetici bağlılığının lojistik bilgi sistem güvenliği kültürü üzerine etkisi ile ilgili sonuç değerlendirmesi yapıldığında ise yöneticilerin lojistik bilgi sistem güvenliği bağlılığı ($\overline{X}$ = 3,64) ile ilgili ankete katılan yöneticilere ait genel ortalamanın yüksek bir düzeyde olduğu tespit edilmiştir. Bu sonuca göre kargo lojistik firma yöneticilerinin firmalarında bulunan lojistik bilgi sistem güvenliği konusuna yönelik olarak güvenlerinin yüksek olduğu ve sistemin korunmasına yönünde sorumluluk sahibi oldukları görülmektedir. Araştırmanın ikinci hipotezi olan lojistik bilgi sistem güvenliği bağlılığının lojistik bilgi sistem güvenliği kültürü üzerine etkisine bakıldığında pozitif ve anlamlı bir ilişki bulunmuştur. Bağlılık bireylerin organizasyonları ile ve örgütsel amaçların başlatılmasına katkıda bulunma isteği ile ilgili psikolojik bir bağ olarak kabul edilmektedir (Allen ve Meyer, 1990). Çalışmanın bu sonucu literatürü destekleyecek tarzda çıkmıştır. Yapılan çalışmalarda bilgi sistem güvenliğine yönelik üst yönetimin desteğinin bilgi sistem güvenliği kültürünü ve bilgi sistem güvenliği politikalarına yönelik çalışan kabullerini pozitif olarak etkilediği bulunmuştur (Knapp ve diğ., 2006; Adéle Da Veiga ve Martins, 2015; Barton ve diğ., 2016).

Bu çalışma sonuçları gelecekte yapılacak araştırmalar için yol gösterici olması açısından yararlı olabilir. Özellikle politika yapıcılar ve yöneticilerin lojistik bilgi sistem güvenliğine yönelik teknik hazırlıklar kadar örgüt içerisinde insan kaynağına yönelik davranışsal hazırlıklarda yapmalarının gerekliliği bu çalışma ile ortaya konmuştur.

KAYNAKLAR

Acılar, A. (2009). "İşletmelerde Bilgi Güvenliği ve Örgüt Kültürü". *Organizasyon Ve Yönetim Bilimleri Dergisi, 1*(1), 25-33.

Allen, N J, Meyer, J P. (1990). "The measurement and antecedents of affective, continuance and normative commitment to the organization". *Journal of occupational psychology, 63*(1), 1-18.

Barton, K A, Tejay, G, Lane, M, Terrell, S. (2016). "Information system security commitment: A study of external influences on senior management". *Computers & Security, 59*, 9-25.

Bess, D A. (2012). *Understanding Information Security Culture in an Organization: An Interpretive Case Study*: ERIC.

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

Chen, C C, Shaw, R, Yang, S C. (2006). "Mitigating information security risks by increasing user security awareness: A case study of an information security awareness system". *Information Technology, Learning, and Performance Journal, 24*(1), 1.

Cooper Ph. D, M. (2000). "Towards a model of safety culture". *Safety science, 36*(2), 111-136.

Da Veiga, A, Martins, N. (2015). "Improving the information security culture through monitoring and implementation actions illustrated through a case study". *Computers & Security, 49*, 162-176.

Da Veiga, A, Martins, N, Eloff, J H. (2007). "Information security culture–validation of an assessment instrument". *Southern African Business Review, 11*(1), 147-166.

Fawcett, S E, Wallin, C, Allred, C, Fawcett, A M, Magnan, G M. (2011). "Information technology as an enabler of supply chain collaboration: a dynamic-capabilities perspective". *Journal of Supply Chain Management, 47*(1), 38-59.

Hansche, S. (2001). "Designing a security awareness program: Part 1". *Information systems security, 9*(6), 1-9.

Ilvonen, I. (2011). *Information Security Culture or Information Safety Culture-What do Words Convey?* Paper presented at the European Conference on Information Warfare and Security.

Katsikas, S K. (2000). "Health care management and information systems security: awareness, training or education?". *International journal of medical informatics, 60*(2), 129-135.

Knapp, K J, Marshall, T E, Kelly Rainer, R, Nelson Ford, F. (2006). "Information security: management's effect on culture and policy". *Information Management & Computer Security, 14*(1), 24-36.

Kruger, H A, Kearney, W D. (2006). "A prototype for assessing information security awareness". *computers & security, 25*(4), 289-296.

Marşap, A, Akalp, G, Yeniman, E. (2010). "Sağlık işletmelerinde insan kaynağının kurumsal bilgi güvenliği kültürü gelişimi". *International Journal Of Informatics Technologies, 3*(1).

Mcintosh, B. (2011). *An ethnographic investigation of the assimilation of new organizational members into an information security culture*: Nova Southeastern University.

Mitnick, K D, Simon, W L. (2011). *The art of deception: Controlling the human element of security*: John Wiley & Sons.

Nonaka, I. (1994). "A dynamic theory of organizational knowledge creation". *Organization science, 5*(1), 14-37.

Patnayakuni, R, Patnayakuni, N. (2014). "Information security in value chains: a governance perspective".

Sabherwal, R, Sein, M K, Marakas, G M. (2003). "Escalating commitment to information system projects: findings from two simulated experiments". *Information & Management, 40*(8), 781-798.

Siponen, M T. (2000). "A conceptual foundation for organizational information security awareness". *Information Management & Computer Security, 8*(1), 31-41.

Stanton, J M, Stam, K R, Guzman, I, Caldera, C. (2003). *Examining the linkage between organizational commitment and information security.* Paper presented at the Ieee International Conference on Systems Man and Cybernetics.

Von Solms, B. (2000). "Information security—the third wave?". *Computers & Security, 19*(7), 615-620.

Vural, Y, Sağıroğlu, Ş. (2008). "Kurumsal Bilgi Güvenliği Ve Standartları Üzerine Bir İnceleme". *Gazi Üniversitesi Mühendislik-Mimarlık Fakültesi Dergisi, 23*(2).

Woodhouse, S. (2007). *Information security: end user behavior and corporate culture.* Paper presented at the Computer and Information Technology, 2007. CIT 2007. 7th IEEE International Conference on.

Zafar, H, Clark, J G. (2009). "Current state of information security research in IS". *Communications of the Association for Information Systems, 24*(1), 34.