Üniversitelerde Bilişim Teknolojileri Risk Yönetimi Başarısını Etkileyen Faktörler Üzerine Nitel Bir Araştırma: Ankara İli Örneği

A Qualitative Study about the Factors Effecting Information Technology Risk Management Success in Universities (Ankara Sample)

Vildan ATEŞ ve Bilal GÜNEŞ***

Öz

Bu çalışmanın amacı, Ankara'daki devlet üniversitelerinin Bilişim Teknolojileri (BT) risk yönetim başarısını etkileyen faktörleri ve bu faktörlerin göstergelerini belirlemektir. Bu çalışmada nitel araştırma yöntemi ve örneklem seçimi için amaçlı örnekleme tekniklerinden kritik durum örneklemesi kullanılmıştır. Yarı yapılandırılmış görüşme tekniği ile Ankara'daki devlet üniversiteleri Bilgi İşlem Dairesi Başkanlıklarında yönetici pozisyonlarında çalışan yedi kişi ile görüşmeler yapılarak veriler toplanmış ve toplanan verilerde elde edilen bilgiler tekrarlandığından, diğer bir deyişle bilgiler doymaya başladığından görüşmeler sonlandırılmıştır. Görüşmeler sonucu elde edilen veriler için betimsel analiz teknikleri kullanılmıştır. Analizlerin sonucunda BT risk yönetim başarısına etki eden göstergeler belirlenmiş ve bu göstergelerin kurumsal, insan, çevresel ve teknolojik faktörler adı altında BT risk yönetimi başarısı üzerinde etkisi olduğu görülmüştür. Bulgular alanyazını doğrultusunda tartışılmış ve önerilerde bulunulmuştur.

Anahtar sözcükler: *BT yönetimi, risk yönetimi, devlet üniversiteleri*

Abstract

In this study, the indicators and factors affecting IT risk management success of state universities in Ankara were investigated. In this research, qualitative research method was used. A semi-structured interview technique was used to collect qualitative data of the study. The participants were seven computer center administrators working in state universities in Ankara. Data obtained from this study were analyzed by using descriptive analyses techniques. After analyzing the data, the indicators effecting IT risk management success were determined and classified under institutional, human, environmental and technological factors. Results were compared with findings of previous studies and recommendations were presented to researchers and practitioners.

Keywords: *IT management, risk management, state universities*

* Uzman Dr., Gazi Üniversitesi Rektörlüğü, Ankara (vates@gazi.edu.tr)

** Prof.Dr., Gazi Üniversitesi, Gazi Eğitim Fakültesi, Fizik Eğitimi Anabilim Dalı, Ankara (bgunes@gazi.edu.tr)

Giriş

Bilişim teknolojileri (BT) günümüzde kurumlarının işleyişinde önemli bir rol oynamakta ve BT'ye olan bağımlılık giderek artmaktadır. Bu gelişmeler kurumların sahip oldukları BT varlıklarını hedef alan açıklıkları ve tehditleri çoğaltmaktadır. Kurumların sahip olduğu ve bilişim sistemlerinde kullandıkları uygulama, veri tabanı, elektronik posta, web sunucusu gibi kaynaklar, bu kaynaklara erişim için kullanılan bilgi ağı kaynakları kurumlar için başlıca BT varlıklarıdır (Emiral, 2003). Kurumlar buna paralel olarak BT varlıklarını olası açıklık ve tehditlerden korumak zorunda kalmaktadır. BT varlıklarını korumak için kurumların uyguladığı sistematik süreç BT risk yönetimi olarak adlandırılmaktadır. Gerber ve Solms (2005) ile Pfleeger (2000) risk yönetiminin iki temel bölümden oluştuğunu vurgulamaktadır. Bu bölümler risk analizi ve risk yönetimi olup, riskin yönetiminin risk analizi aktivitesi sonucu elde edilen bilgiler doğrultusunda planlama, izleme ve kontrol aktivitelerinden oluştuğu ifade edilmektedir.

Üniversiteler bilişim sistemlerini kurum işleyişlerinin her aşamasında yaygın olarak kullanan kurumlardan birisidir. Bu doğrultuda üniversiteler de korumaları gereken BT varlıklarını oluşabilecek risklere karşı korumak zorunda kalmaktadır. Dolayısıyla üniversitelerin de BT risk yönetimini başarılı bir şekilde yürütmesi önem teşkil etmektedir. Günümüzde üniversitelerde uygulanması zorunlu bir ihtiyaç haline gelen BT risk yönetiminin başlıca amaçları; üniversitelerin misyonunu gerçekleştirmesine yardımcı olmak, üniversitelerin iç ve dış paydaşlarına kesintisiz hizmet ve servis sunmak, üniversitelerde risk farkındalığı gelişmiş bir kültür oluşturmak, üniversitenin toplumsal değerini (saygı, itibar) artırmak, diğer üniversitelere karşı rekabet sürecinde avantaj sağlamak, kanun, yönetmelik ve standartlara uyum sağlamak ve toplumu risk yönetimi konusunda bilgilendirmek şeklinde sıralanabilir.

Değişik ülkelerdeki üniversiteler ve yükseköğretim kurumları BT risk yönetimi süreçleri ve farkındalığı açısından incelendiğinde, Amerika Birleşik Devletlerinde (ABD) bulunan Virjinya Üniversitesi bu süreci iyi yöneten kurumlardan birisi olarak öne çıkmaktadır. Virjinya Üniversitesi tarafından yayımlanan genelgede, BT risk yönetiminin amacı, yöneticiler için karşılaşılabilecek risklerin maliyetleri ile bu riskleri azaltmak için uygulanacak kontrollerin maliyetleri arasındaki dengeye yardımcı olmak şeklinde ifade edilmiştir. Genelgede, bu süreci verimli bir şekilde yönetmenin yasal bir zorunluluk olduğuna, üniversitelerinin bilgisayar ortamı olarak çok zengin olduğuna ve BT varlıkları üzerindeki herhangi bir aksaklığın katlanılamaz olduğuna vurgu yapılmaktadır (Virginia University, 2013).

Üniversitelerin BT risk yönetimi sürecinde karşılaştıkları en yaygın risklerden birinin bilgi ve kimlik hırsızlığı olduğu görülmektedir. Yapılan çalışmalarda, bu veri ihlallerinin büyük çoğunluğunun (%80) teknolojik sistemlerin yetersizliği sonucu değil, kullanıcı (insan) hatası sonucu meydana geldiği görülmektedir (Princeton University, 2013). Ayrıca Ahlan ve Arshad (2012) yaptıkları çalışmada, BT yönetimi ile ilişkili risklerin

çok sık değiştiği; bu bağlamda üniversitelerin her yıl kapsamlı bir BT risk yönetimi sürecini uygulamaları gerektiğini vurgulamaktadırlar. Bilgilerin gizlilik, erişilebilirlik ve bütünlüğünü sağlamak için sürekli güncelleştirmelerin yapılması gerektiği de ayrıca ifade edilmektedir.

Rezgui ve Marks (2008), yaptıkları araştırma sonucunda üniversite personelinin ve öğrencilerin BT güvenliği farkındalık düzeyinin çok düşük olduğunu ifade etmektedirler. Bununla birlikte, üniversitelerdeki BT risk yönetimi başarısı konusundaki alanyazınında fazla çalışma bulunmadığı ve bu konuda yeni çalışmalara ihtiyaç olduğu dikkat çekmektedir. Örneğin, Yeo, Rahim ve Miri (2007) ve Goel ve Chen (2010), risk değerlendirmesini etkileyen faktörler hakkında çok az çalışma bulunduğunu vurgularken; Kotulic (2001), Saleh ve Alfantookh (2011) de güvenlik risk yönetimi alanındaki araştırma sayısında ciddi bir eksiklik olduğunu belirtmektedirler. Aktaş ve Soğukpınar (2010) bilgi güvenliği faaliyetlerinde anahtar kavramın risk analizi olduğunu, sistemlerdeki güvenlik seviyesini tespit etmek ve daha iyi hale getirebilmek için mevcut riskleri belirleyebilmenin, bunları analiz etmenin, karşı tedbirler geliştirebilmenin, kısacası bu süreci yönetmenin gerekliliğine dikkat çekmişlerdir.

Sonuç olarak, üniversiteler sahip oldukları BT varlıklarını korumak için BT risk yönetimini yönetim süreçleri içerisinde düşünmek ve uygulamak zorundadır (Franklin, 2010). Bu nedenle üniversitelerde BT risk yönetimi başarısını etkileyen faktörleri belirlemek ve bu faktörlerin birbirleri arasındaki örüntüyü ortaya çıkarmak, bu kurumların BT risk yönetimi başarısı için kilit konumdadır.

Bu çalışmada, Ankara'daki devlet üniversitelerinin BT risk yönetimi başarısını etkileyen dışsal faktörler nelerdir? sorusuna cevap aranmıştır. Bununla birlikte, belirlenen dışsal faktörlerin göstergelerinin neler olduğu sorusuna da yanıt aranmaya çalışılmıştır.

Yöntem

Bu araştırmada, nitel araştırma yöntemi kullanılmıştır. Nitel araştırma çalışılan konuyu derinlemesine ve tüm olası ayrıntıları ile incelemeyi amaç edinmektedir (Yıldırım ve Şimşek, 2008, s.56). Çalışmada yarı yapılandırılmış görüşme formu ile veriler toplanmış ve veriler betimsel analiz teknikleri kullanılarak analiz edilmiştir. Araştırmanın tamamı araştırmacı tarafından yürütülmüştür.

Örneklem Yöntemi

Araştırmada, nitel verilerin örneklem seçimi için amaçlı örnekleme yöntemlerinden kritik durum örneklemesi kullanılmıştır. Kritik durum örneklemesi Yıldırım ve Şimşek tarafından şu şekilde açıklanmaktadır (2008, s.111), seçilen kritik bir durum veya durumların varlığına işaret eden en önemli gösterge burada oluyorsa ya da olmuyorsa şeklinde düşünüp cevap olaraksa başka benzer durumlarda da olur ya da olmaz

şeklinde tanımlanmaktadır. Bir veya birkaç durumun kabul edilebilir hale gelmesi, benzer durumlara ilişkin genellemelerin yapılmasına olanak vermemektedir (Patton, 1987). Bununla birlikte kritik durum örneklemesi araştırma sonucunda elde edilen veriye dayalı sonuçların zenginliği ve inandırıcılığı sınırlı ölçüde genellemeler yapma imkânı verdiği için bu çalışmada tercih edilmiştir (Yıldırım ve Şimşek, 2008, s.110-111).

Çalışma Grubu

Araştırmanın kapsamı, çalışmanın yapıldığı tarihte Ankara'da bulunan devlet üniversiteleridir. Vakıf üniversitelerinin yapısı, yönetim şekli ve işleyişinin devlet üniversitelerinden farklı olduğu düşünüldüğünden bu çalışmaya dâhil edilmemiştir. Araştırmanın çalışma grubu, Ankara'daki devlet üniversiteleri Bilgi İşlem Dairesi Başkanlıkları'nda yönetici pozisyonlarında çalışan 7 kişiden (Ankara ve Gazi Üniversite'lerinden ikişer kişi, Hacettepe, ODTÜ ve Yıldırım Beyazıt Üniversite'lerinden birer kişi) oluşmaktadır. Yapılan görüşmeler sonunda elde edilen bilgiler tekrarlandığı, diğer bir deyişle bilgiler doymaya başladığı için görüşmeler sonlandırılmıştır.

Veri Toplama Aracı

Nitel verileri toplamak için katılımcılar ile yüz yüze görüşmeler yapılmıştır. Yüz yüze görüşme tekniği nitel araştırmalarda en sık kullanılan veri toplama yöntemidir (Yıldırım ve Şimşek, 2008: 119). Patton (1987:108) görüşmenin amacını, bireyin iç dünyasına girmek ve onun bakış açısını anlamak şeklinde belirtmektedir. Bailey'e (2007) göre görüşme yönteminin güçlü yönleri esneklik, yanıt oranı, sözel olmayan davranışlar, ortam kontrolü, soru sırası, anlık tepki, tamlık ve derinlemesine bilgi olarak sıralanabilir.

Araştırmada yarı yapılandırılmış görüşme tekniği kullanılmıştır. Yarı yapılandırılmış görüşmenin seçilmesinin nedeni, görüşmenin önceden hazırlanmış görüşme sorularına bağlı olarak sürdürülmesi ile daha sistematik bilgi sunmasıdır. Görüşme yapılmadan önce görüşme formu için tüm sorular hazırlanmış ve görüşme yapılacak katılımcılara aynı sorular sorulmuştur. Buna ilaveten yarı yapılandırılmış görüşme, yapılandırılmış görüşmeden biraz daha esnektir. Katılımcıların yanıtlarını açması ve detaylandırılması için görüşmenin akışına bağlı olarak görüşme formunda bulunan sorulardan farklı ya da alt sorular sorularak görüşmenin akışı şekillendirilebilmektedir.

Bu çalışmada kullanılan yarı yapılandırılmış görüşme soruları hazırlanırken aşağıdaki adımlar izlenmiştir. İlk olarak, BT risk yönetimi başarısını etkileyen faktörlerin ve bu faktörlere ait göstergelerin belirlenmesi için alanyazındaki bildiriler, makaleler ve tezler incelenmiştir (Teo ve Ang, 1999; Young, 2008; Knapp, 2005; Culler, 2009; Yıldırım Akalpa, Aytaç ve Bayram, 2011; Zafar, 2010; Cheng, 2012; Ifinedo, 2008; Kotulic, 2001; Chow, 2008; Jourdan, 2008; Pierce, 2012).

BT risk yönetimi başarısını etkilemesi muhtemel faktörlerin ve bu faktörlere ait göstergelerin belirlenmesinden sonra, taslak olarak bir yarı yapılandırılmış görüşme formu oluşturulmuştur. Görüşme formunun geçerliliğini sağlamak için 9 uzman görüşü (7 endüstri mühendisliği bölümü öğretim üyesi ve 2 işletme bölümü öğretim üyesi) alınmıştır. Taslak halindeki görüşme formu, alan uzmanlarına verilerek bölümlerin ve maddelerin geçerliliği, maddelerin anlaşılırlığı ve uygunluğu konularında görüşleri sorulmuştur. Bu doğrultuda uzman görüşleri dikkate alınarak görüşme formunun üzerinde gerekli değişiklikler yapılmıştır.

Görüşmede sorulacak soruların katılımcı tarafından kolayca anlaşılabilmesi için bu soruların mümkün olduğunca açık ve belirgin bir biçimde ifade edilmesine özen gösterilmiştir. Odaklı sorular hazırlanılmasına dikkat edilmiştir. Bununla birlikte, görüşme formunda bulunan soruların anlaşılır olup olmadığını test etmek amacıyla bilişim alanında çalışan 3 kişi ile görüşmeler yapılmıştır. Görüşmeler sonucu katılımcılardan gelen geri bildirimler doğrultusunda görüşme formuna son hali verilmiştir.

BT risk yönetimini etkileyen dışsal faktörler kurumsal, insan, çevresel ve teknolojik faktörler şeklinde sınıflandırılmıştır. Bu faktörlere ait olan göstergeler de belirlenmiştir. Tablo I'de belirlenen faktörler ve bu faktörlere ait göstergeler sunulmuştur. Sonuç olarak belirlenen faktör ve göstergeler dikkate alınarak toplam 6 sorudan oluşan bir görüşme formu geliştirilmiş ve katılımcılar ile görüşme yapılmıştır. Katılımcılardan düşüncelerini belirtirken (soruları cevaplarken) çalıştıkları kurumun şartlarını ve bilişim alanındaki geçmiş deneyimlerini de dikkate almaları istenmiştir.

Görüşme formunun ilk dört sorusunda katılımcılara BT risk yönetim sürecini etkileyen faktörlerden bir tanesi belirtilmiş ve bu faktörün üniversitelerin bilişim teknolojileri risk yönetimi başarısını etkileyip etkilemediği hakkındaki düşünceleri sorulmuştur. Daha sonra bu faktörlerin göstergeleri belirtilerek ve bu göstergeleri dikkate alarak görüşlerini açıklamaları istenmiştir. Buna ilaveten gerekli görülürse yeni göstergeler de ekleyebilecekleri belirtilmiştir. Görüşmenin beşinci sorusunda katılımcılara bir kurumda BT risk yönetiminin başarılı bir şekilde yapıldığının göstergelerinin neler olduğu sorulmuştur Altıncı ve son soruda üniversitelerde BT risk yönetimi başarısını etkileyebileceğini düşündükleri başka faktör ya da bileşenlerin olup olmadığı sorulmuştur.

Tablo I. BT Risk Yönetimi Başarısını Etkileyen Faktörler ve Göstergeleri

Faktör adı	Göstergeleri
Kurumsal Faktörler	Bilgi Güvenliği Politikaları BT Bütçesi İletişim Kurum Kültürü Kurum Olgunluğu Net Amaç ve Hedefler Net ve Anlaşılır Misyon Üst Yönetim Desteği
İnsan Faktörü	BT Personeli Deneyimi BT Personeli Yetkinliği Eğitim Farkındalık İnsan Hataları Personel Motivasyonu Personel Sayısı
Çevresel Faktörler	Doğal Tehditler Standartlara Uyum Politik Çevre Yasalara Uyum
Teknolojik faktörler	Donanım Güvenliği Kritik Altyapı Analizi Yazılım Güvenliği

Veri Toplama ve Geçerlilik Çalışmaları

Görüşme süreci aşağıda açıklanan dört adımdan oluşmaktadır:

Görüşmelerin ayarlanması: Görüşmelerin yapılması için devlet üniversiteleri bilgi işlem daire başkanlığı yönetim kadrosunda (daire başkanı, daire başkan yardımcısı, birim sorumlusu) bulunan personel ile elektronik posta veya telefon ile iletişime geçilmiş ve görüşme için gerekli planlamalar yapılmıştır.

Hazırlıkların yapılması: Görüşmeler yapılmadan önce görüşme formu çıktısı alınmış ve ses kayıt cihazı hazırlanmıştır.

Görüşmenin gerçekleştirilmesi: Görüşmeler katılımcının isteği doğrultusunda çalışma ofislerinde gerçekleştirilmiş olup, ortalama 30 dakika sürmüştür. Görüşmeler kaydedilmeden önce katılımcıdan kayıt için izin alınmıştır. Görüşmede sorulara verilen cevapların ses kaydı yapılmış aynı zamanda da not alınmıştır. Görüşmelerde kayıt ve not alma yöntemlerinin bir arada kullanılması en istendik durumdur (Yıldırım ve Şimşek, 2008: 147). Araştırmacı sorularını yansız bir dille sormaya özen göstermiştir. Sorulara cevap verirken katılımcılara düşüncelerini sözlü ifade etmeleri ve yüksek sesle

düşünme tekniğini kullanarak izlenimlerini belirtmeleri istenmiştir. Görüşme sorularına başlamadan önce katılımcının kişisel bilgileri sorulmuş, daha sonra görüşme sorularına geçilmiştir. Tüm görüşmeler araştırmacının kendisi tarafından yürütülmüş olup, araştırmacı yansız konumda bulunmuştur. Katılımcılara anlamadıkları soru olduğunda açıklama yapılabileceği belirtilmiştir. Görüşmede sorular konuşma tarzında ve anlaşılır biçimde sorulmuş ve araştırmacı katılımcıya yanıtlarla ilgili geribildirimlerde bulunarak katılımcının cevaplarını onaylamasını sağlamıştır. Sorudan soruya geçerken yanıtlar için elverişli zaman aralıkları bırakılmıştır. İstenen yanıt alınınca hemen yeni bir soruya geçilmemiş, katılımcının açıklamasını bitirmesi beklenmiştir. Böylece cevapların her iki taraf açısından da anlaşılır ve netliği kontrol edilmiştir. Katılımcılar sorular hakkındaki olumlu düşüncelerini anlaşılabilir ve açık gibi ifadeler kullanarak ifade etmişlerdir.

Görüşmenin rapor edilmesi: Katılımcılar 1,2,3...7 şeklinde numaralandırılmış olup katılımcıların ad ve soyadları kullanılmamıştır. Görüşme sonucu yanıtlar olduğu gibi yazılmıştır. Alınan bilgiler aynı gün içerisinde görüşme tamamlandıktan hemen sonra henüz canlı ve tazeyken yazıya dökülmüş ve transkriptler oluşturulmuş her sorunun yanıtı ayrıca yazılmıştır.

Güvenirlik Çalışmaları

Bu çalışmada iç güvenirliği yani tutarlılığı sağlamak için; veriler benzer deneyime ve görevlere sahip katılımcılardan ve benzer süreçlerle toplanmış, verilerin analizinde tutarlılık sağlanmış, verilerin sonuçlarla ilişkisinin kurulması için katılımcıların görüşlerinden birebir alıntılar yapılmış ve amaçlı örnekleme tekniği kullanılmıştır. İç güvenirliği sağlamak için, veriler ses kayıt tekniğiyle toplanmış ve sonuçlarla bütünleştirilmiştir. Dış güvenirliğini sağlamak üzere ise araştırmacılar tarafından veriler ve ulaşılan yargı ve yorumlar denetlemiştir (Yıldırım ve Şimşek; 2008:255).

Verilerin Analizi

Nitel verilerin analizi konusunda alanyazınında farklı kavramlar ve yaklaşımlar bulunmakta ve verinin nasıl analiz edileceği araştırmacıya, veriye ve çalışmanın amacına, bağlı olarak değişebilmektedir (Sözbilir, 2009). Nitel veri analiz sürecini analizin derinliğine göre iki grupta incelemenin mümkün olduğu belirtilmektedir (Yıldırım ve Şimşek, 2008: 223). Bu araştırmada toplanan verilerin analizini daha basit hale getirmek amacıyla Strauss ve Corbin'in (1990) önerdiği betimsel analiz tekniği uygulanmıştır (Strauss ve Corbin, 1990: 89). Altunışık, Çoşkun, Yıldırım ve Bayraktaroğlu (2010:322) betimsel analizin analiz için bir çerçeve oluşturma, tematik çerçeveye göre verilerin işlenmesi, bulguların tanımlanması ve bulguların yorumlanması olmak üzere dört aşamadan oluştuğunu belirtmişlerdir.

Bu çalışmada görüşmeler sonucu elde edilen veriler için betimsel analiz teknikleri uygulanmıştır. Verilerin betimsel analizi görüşme formunda yer alan sorular dikkate

alınarak sunulmuştur. Çalışmadaki her bir faktör bir tema olarak değerlendirilmiş ve betimsel analizde toplanan veriler önceden belirlenen bu faktörlere göre analiz edilmiştir. Elde edilen bulgular düzenlenmiş bir biçimde tablolarda sunulmuş ve gerekli yerlerde doğrudan alıntılarla desteklenmiştir.

Bulgular

Bu bölümde bu araştırmanın verileri ile ilgili bulgular sunulmaktadır. İlk olarak katılımcılarla ilgili demografik bilgiler ve görüşmelerde katılımcılara sorulan altı soruya ait cevaplar ile ilgili bulgular yer almaktadır. Altıncı soruda katılımcılara, sorulan faktöre eklemek istedikleri göstergeler sorulmuş olup cevapları her bir faktörün bulguları için hazırlanan tablolarda sunulmuştur.

Tablo II'de görüşme yapılan katılımcılara ait demografik bilgiler sunulmuştur. Görüşme yapılan 7 katılımcıya ait yaş, unvan, öğrenim durumu, meslek, kurumda çalışma süresi, çalışma alanı, bilişim alanında çalışma süresi ile son beş yılda eğitim alıp almadıkları hakkındaki bilgiler Tablo II'de görülmektedir.

Tablo II. Görüşme Yapılan Katılımcılara Ait Demografik Bilgiler

Görüşme No	Yaşı	Unvanı	Öğrenim Düzeyi	Mesleği	Kurumda Çalışma Süresi (yıl)	Çalışma Alanı	Bilişim Alanında Çalışma Süresi (yıl)	Son 5 Yılda Eğitim Alma Durumu
1	36	Ağ ve Sistem Sorumlusu	Lisans	İdari personel	15	Ağ/Sistem	15	Evet
2	36	Bilgi Güvenliği Birim Yöneticisi	Yüksek Lisans	Akademik Personel	14	Ağ/Sistem Güvenlik	14	Evet
3	33	Daire Başkan Yardımcısı	Yüksek Lisans	Akademik Personel	6	Güvenlik/Yazılım	8	Evet
4	44	Daire Başkan Yardımcısı	Lisans	Akademik Personel	14	Ağ/İdari Hizmetler	14	Hayır
5	36	Ağ ve Sistem Uzmanı	Yüksek Lisans	Akademik Personel	6	Ağ/Sistem/Web Programlama	12	Hayır
6	34	Ağ ve Sistem Uzmanı	Doktora	Akademik Personel	6	Ağ/Sistem/ Yazılım	10	Evet
7	46	Daire Başkanı	Doktora	Akademik Personel	8	Ağ/Sistem	15	Evet

Tablo II incelendiğinde, görüşme yapılan tüm katılımcıların uzun sayılabilecek bir süre (8 ila 15 yıl arasında) bilişim alanında çalıştığı, mevcut kurumda çalışma süreleri de 6 yıl ile 15 yıl arasında olduğu görülmektedir. Katılımcıların bilişim alanında çalışma süreleri bu alanda gerekli tecrübe ve bilgi birikimine sahip olabileceklerini göstermektedir. Kurumda çalışma süreleri, unvanları ve yaşlarına bakıldığında

birimlerinde ve bilişim alanında yeterli yöneticilik deneyimine sahip ve konuya hâkim olabilecekleri düşünülebilir.

Görüşme formunun ilk sorusunda katılımcılara, BT risk yönetim sürecini etkileyen faktörlerden bir tanesinin kurumsal faktörler olduğu ve kurumsal faktörlerin üniversitelerin bilişim teknolojileri risk yönetimi başarısına etkisi konusundaki düşünceleri sorulmuştur. Ayrıca, kurumsal faktörlerin göstergelerini (bilgi güvenliği politikaları, BT için ayrılan bütçe, çalışanlar arası iletişim, kurum kültürü, yönetim desteği) dikkate alarak görüşlerini açıklamaları ve gerekli görülürse yeni göstergeler eklemeleri istenmiştir. Görüşme yapılan tüm katılımcılar kurumsal faktörlerin BT risk yönetimi başarısını etkilediği yönünde görüş bildirmiştir. Bir numaralı katılımcı "*kurumsal faktörlerin üniversitelerin bilişim teknolojileri risk yönetimi başarısını etkilediğini düşünüyorum*" şeklinde belirtirken; 6 numaralı katılımcı da "*BT risk yönetimi başarısı sürecini etkiler. Tüm göstergeler de etkili bence"* olarak belirtmişlerdir.

Katılımcıların kurumsal faktörler ile ilgili soruya verdikleri cevaplar Tablo III'de özetlenmiştir. Tablo III incelendiğinde, katılımcıların altı tanesi üst yönetim desteğinin ve BT bütçesinin, BT risk yönetiminin başarıya ulaşmasında etkili olduğunu belirtmişlerdir.

Tablo III. Katılımcıların Kurumsal Faktörler İle İlgili Soruya Verdikleri Cevaplar

Kurumsal Faktörler	Katılımcılar						
	1	2	3	4	5	6	7
Bilgi güvenliği politikaları	✓	✓	-	✓	-	✓	✓
BT bütçesi	✓	-	✓	✓	✓	✓	✓
İletişim	-	-	-	-	✓	-	✓
Kurum kültürü	-	✓	✓	-	✓	-	✓
Kurum olgunluğu	-	✓	-	-	-	-	✓
Net amaç ve hedefler	-	-	-	-	-	-	✓
Kurum Misyonu	-	-	-	-	-	-	✓
Üst yönetim desteği	✓	✓	✓	✓	✓	✓	-
Eklenen diğer göstergeler	-	-	-	-	-	-	-

Bir numaralı katılımcı düşüncelerini "*tabii ki üst yönetim desteği de çok önemli. Üst yönetim desteklemezse BT risk yönetiminde başarılı olamayız. Bizim isteklerimiz doğrultusunda yazılım ve donanım alımı yapmalı ve süreçlerde bizi desteklemelidir.*" şeklinde ifade etmiştir. Üç numaralı katılımcı da BT bütçesi hakkındaki düşüncesini şöyle ifade etmiştir: *"BT bütçesi en önemli göstergelerden biri. Mesela bize verilen bütçe istediğimiz bütçenin onda biri. Kurumsal faktörler içerisinde en etkili olanının BT bütçesi olduğunu düşünüyorum."* Beş katılımcının bilgi güvenliği politikalarının, dört katılımcının da kurum kültürünün BT risk yönetimi başarısında etkili olduğunu düşündükleri Tablo

III'de görülmektedir. İki katılımcı iletişimin ve kurum olgunluğunun etkisini ifade etmiş olup sadece 1 katılımcı net amaç ve hedefler ile kurum olgunluğunun etkisi olacağını ifade etmiştir. Tablo III'de görüldüğü gibi katılımcılar kurumsal faktörlere eklenebilecek bir gösterge önerisinde bulunmamışlardır.

Görüşme formunun ikinci sorusunda katılımcılara, insan faktörünün BT risk yönetimi başarısını etkileyip etkilemediği sorulmuştur. Düşüncelerini açıklarken insan faktörünün göstergeleri olduğunu düşündüğümüz BT personelinin deneyimi, yetkinliği, farkındalık, eğitim, insan hataları, personel motivasyonu ve sayısına bağlı olarak örneklerle açıklamaları istenmiştir. Görüşmeler sonucu tüm katılımcıların BT risk yönetimi başarısında insan faktörünün etkili olduğunu belirttikleri görülmüştür. 3 numaralı katılımcı *"Kurumda çalışan insan faktörü BT risk yönetimi başarısını çok etkiliyor"* şeklinde ifade ederken; 4 numaralı katılımcı da *"insan faktörü tabii ki çok etkiler"* şeklinde vurgulamıştır. Bununla birlikte 6 numaralı katılımcı da insan faktörü ile kurumsal faktörlerin birbirlerini etkileyeceğini düşündüğünü vurgulamıştır.

Tablo IV. Katılımcıların İnsan Faktörü İle İlgili Soruya Verdikleri Cevaplar

İnsan Faktörü	**Katılımcılar**						
	1	**2**	**3**	**4**	**5**	**6**	**7**
BT Personeli Deneyimi	✓	✓	✓	✓	-	✓	✓
BT Personeli Yetkinliği	✓	✓	-	✓	✓	✓	✓
Farkındalık	-	✓		✓	-	✓	✓
Eğitim	✓	✓	✓	✓	✓	-	-
İnsan hataları	✓	-	-	-	-		✓
Personel motivasyonu	-	-	-	-	✓	✓	-
Personel sayısı	✓	-	-	-	-	-	-
Eklenen diğer göstergeler	-	-	-	-	-	Tanımlanmış roller ve sorumluluklar	-

Tablo IV'de katılımcıların insan faktörü ile ilgili soruya verdikleri cevaplar yer almaktadır. Tablo IV'e göre altı katılımcı, personel deneyimi ve yetkinliğinin BT risk yönetiminin başarısını olumlu yönde etkileyeceğini düşünürken beş katılımcı da eğitimin etkilediğini düşünmektedir. 4 numaralı katılımcı eğitim ve farkındalık hakkındaki düşüncelerini şöyle ifade etmiştir: *"Farkındalık çok önemli. Şahsen üniversitemizde bu farkındalığın oturmuş olduğunu düşünmüyorum. Bu konuda üst yönetim desteği ile eğitimler düzenlenmesi lazım. Farkındalık yaratamadıysanız risklere karşı ne önlem alırsanız alın sonu gelmez yani sonuç alamazsınız. Eğitim ve farkındalık birbirini tamamlıyor."* Dört katılımcı farkındalığın etkisine vurgu yaparken iki katılımcı personel motivasyonu ve insan hatalarının etkisini vurgulamıştır. Sadece bir katılımcı personel sayısının etkili olacağını düşünmektedir. Tablo IV'de görüldüğü gibi altıncı katılımcı insan faktörüne tanımlanmış roller ve sorumluluklar göstergesinin eklenebileceğini belirtmiştir.

Görüşmenin üçüncü sorusunda katılımcılara, ulusal/uluslararası bilgi güvenliği standartlarına uyum, politik çevrelerin tutumu, kurumların yasal düzenlemelere uyumu ve doğal tehditler göstergelerine sahip çevresel faktörlerin, üniversitelerin bilişim teknolojileri risk yönetimi başarısına etkileri hakkındaki düşünceleri sorulmuştur. Görüşme transkriptleri incelendiğinde tüm katılımcıların, kurumsal ve insan faktörü ile ilgili bulgularda olduğu gibi çevresel faktörlerin de BT risk yönetimi başarısında etkili olduğunu düşündükleri belirlenmiştir. 2 numaralı katılımcı bu düşüncesini *"çevresel faktörler BT Risk yönetimi başarısını etkiler"* şeklinde ifade ederken; 7 numaralı katılımcı da "*çevresel faktörler çok önemli"* şeklinde vurgulamışlardır.

Katılımcıların çevresel faktörler ile ilgili soruya verdikleri cevapların detayları Tablo V'de görülmektedir.

Tablo V. Katılımcıların Çevresel Faktörler İle İlgili Soruya Verdikleri Cevaplar

Çevresel Faktörler	**Katılımcılar**						
	1	**2**	**3**	**4**	**5**	**6**	**7**
Standartlara Uyum	✓	✓	✓	✓	✓	✓	✓
Politik Çevre	-	✓	✓	-	✓	✓	-
Yasalara Uyum	✓	-	✓	✓	✓	-	✓
Doğal Tehditler	✓	✓	-	✓	-	✓	✓
Eklenen diğer göstergeler	Elektrik sorunları	-	-	-	-	-	-

Tablo V'e göre katılımcıların hepsi çevresel faktörlerin göstergelerinden biri olan standartlara uyumun BT risk yönetimi başarısı için önemli olduğunu söylemişlerdir. Beşinci katılımcı düşüncelerini "*standartlara uyum kesinlikle önemli ve etkiler diye düşünüyorum. Yasalara uymak çevresel faktör olarak BT risk yönetimi başarısını etkiler*" şeklinde belirtmiştir. Görüşme yapılan beş katılımcı, yasalara uyum göstergesini ve doğal tehditleri önemli bulurken, dört katılımcı politik çevrenin etkili olduğunu belirtmiştir. Tablo V'de görüldüğü gibi birinci katılımcı çevresel faktörlere elektrik sorunları göstergesinin eklenebileceğini belirtmiştir.

Dördüncü soruda katılımcılara, üniversitelerde bilişim teknolojileri risk yönetiminin başarıya ulaşması için dikkate alınması gereken faktörlerden bir diğerinin teknolojik faktörler olduğu ve bu faktör altında kritik altyapı analizi, donanım güvenliği ve yazılım güvenliği gibi göstergelerin BT risk yönetimi sürecindeki rolü hakkındaki düşüncelerinin neler olduğu sorulmuştur. Katılımcıların dördüncü soruya verdikleri cevaplar incelendiğinde, katılımcıların tümü teknolojik faktörlerin BT risk yönetimi başarısında etkili olduğunu ifade etmişlerdir. Üç numaralı katılımcı bu düşüncesini "*teknolojik faktörlerin BT risk yönetimi başarısında etkili olduğunu düşünüyorum*" ve altı numaralı katılımcı da "*teknolojik faktörler etkili olduğunu düşünüyorum ve göstergelerinin üçü de çok önemlidir*" şeklinde ifade etmişlerdir.

Tablo VI'da katılımcıların teknolojik faktörler ile ilgili soruya verdikleri cevaplar özetlenmiştir. Tablo VI incelendiğinde, tüm katılımcılar tarafından yazılım güvenliğinin BT risk yönetiminin başarıya ulaşması için gerekliliği vurgulanmış diğer taraftan katılımcılar teknolojik faktörlere eklenebilecek bir gösterge önerisinde bulunmamışlardır.

Tablo VI. Katılımcıların Teknolojik Faktörler İle İlgili Soruya Verdikleri Cevaplar

Teknolojik Faktörler	**Katılımcılar**						
	1	**2**	**3**	**4**	**5**	**6**	**7**
Kritik altyapı analizi	✓	✓	✓	✓	-	✓	✓
Donanım güvenliği	✓	-	✓	✓	✓	✓	✓
Yazılım güvenliği	✓	✓	✓	✓	✓	✓	✓
Eklenen diğer göstergeler	-	-	-	-	-	-	-

Yazılım güvenliği hakkında 3 ve 5 numaralı katılımcıların düşünceleri şöyledir: *"Yazılım güvenliğinin bu göstergeler içerisinde en önemli kısım olduğunu düşünüyorum. Kurumun bilişim sistemlerinde kullanılan yazılımlarda meydana gelen arızalar sonucu yaşanan zaman ve maddi kayıplar sorun teşkil etmektedir. Örneğin iki hafta ya da iki saat sistemler çalışmazsa kurum itibar kaybı yaşar. Hizmet verememekten maddi kayıplar yaşayabilir." "Yazılım güvenliğinin bu göstergeler içerisinde en önemli kısım olduğunu düşünüyorum."* Katılımcıların altı tanesi donanım güvenliği ve kritik alt yapı analizinin BT risk yönetimi başarısı için gerekli olduğunu ifade etmişlerdir.

Görüşmenin beşinci sorusunda katılımcılara, bir kurumda BT risk yönetimin başarılı bir şekilde gerçekleştirildiğinin göstergeleri sorulmuştur. Katılımcıların BT risk yönetimi başarısı göstergeleri ile ilgili soruya verdikleri cevaplar Tablo VII'de görülmektedir.

Tablo VII. Katılımcıların BT Risk Yönetimi Başarısı Göstergeleri İle İlgili Soruya Verdikleri Cevaplar

BT Risk Yönetimi Başarısı	**Katılımcılar**						
	1	**2**	**3**	**4**	**5**	**6**	**7**
Bütünlük	-	✓	✓	-	✓	✓	✓
Gizlilik	-	✓	✓	-	✓	✓	✓
Güvenlik ihlali	-	✓	✓	✓	✓	✓	-
Hizmet sürekliliği	✓	✓	-	✓	✓	✓	✓
Kullanılabilirlik	✓	✓	✓	-	-	✓	-
Kullanıcı memnuniyeti	✓	-	✓	✓	✓	✓	✓
Eklenen diğer göstergeler	-	-	-	-	-	Verimlilik artışı	Fiziksel güvenlik

Tablo VII'e göre katılımcıların altı tanesi hizmet sürekliliği ve kullanıcı memnuniyetinin BT risk yönetimi başarısı göstergesi olduğunu, beş tanesi de bütünlük, gizlilik, güvenlik ihlali sayısında azalışı gösterge olarak ifade etmişlerdir. Kullanılabilirliğin gösterge olduğunu düşünen katılımcı sayısı dörttür. 6 numaralı katılımcı verimlilik artışını ve 7 numaralı katılımcı da fiziksel güvenlik göstergelerini eklemenin uygun olacağını düşünmektedirler. 1 numaralı katılımcı hizmet sürekliliği göstergesi hakkındaki düşüncesini, "*BT risk yönetimin başarılı bir şekilde gerçekleştirildiğinin en önemli göstergesi hizmet ve servis sürekliliğidir. Sürekli ise risk analizlerini doğru bir şekilde yapmışlardır.*" şeklinde kullanıcı memnuniyetini de "*yüksek kullanıcı memnuniyeti başarının bir göstergesidir. Bunun olması gerekiyor. En önemlilerinden birisi bu bence. "*şeklinde belirtmiştir. Bununla birlikte, 3 numaralı katılımcı da düşüncesini şöyle ifade etmiştir: "*İlk göstergesi hizmet sürekliliği, yüksek kullanıcı memnuniyeti, daha sonra bilgi güvenliği sağlanır. Son olarak güvenlik ihlali sayısında azalma gözlenir*". Diğer taraftan Tablo VII incelendiğinde, altıncı katılımcının verimlilik artışı ve yedinci katılımcının fiziksel güvenlik göstergelerinin eklenebileceği şeklinde öneriler bulunmaktadır.

Ankara'daki devlet üniversitelerinin Bilgi İşlem Dairesi Başkanlıklarında yönetici pozisyonlarında çalışan katılımcılarla yapılan görüşmelerde tüm katılımcılar kurumsal, insan, çevresel ve teknolojik faktörlerin BT risk yönetimi başarısı üzerinde etkisi olduğu yönünde görüş bildirmişlerdir. Kurumsal faktörlerin üst yönetim desteği, bilgi güvenliği politikaları, BT bütçesi ile net amaç ve hedefler göstergeleri; insan faktörünün ise BT personeli deneyim ve yetkinliği ile eğitim göstergelerinin ön plana çıktığı görülmektedir. Çevresel faktörlerin en çok öne çıkan veya vurgulanan göstergelerinin standartlara ve yasalara uyum ile politik çevrenin tutumu olduğu görülmektedir. Teknolojik faktörlerin öne çıkan göstergeleri donanım, yazılım güvenliği ve kritik alt yapı analizi şeklindedir.

Sonuç ve Öneriler

Bu bölümde, bu araştırma kapsamında elde edilen bulguların sonuçlarına ve bu doğrultuda önerilere yer verilmiştir.

Çalışmada, Ankara'daki devlet üniversitelerinin BT risk yönetimi başarısını etkileyen faktörler nelerdir? sorusuna yanıt aranmıştır. Nitel araştırma yöntemi kullanılmış, veriler yarı yapılandırılmış görüşme tekniği ile toplanmış ve değerlendirilmiştir. Bu çalışmada elde edilen bulgulara göre kurumsal, insan, çevresel ve teknolojik faktörlerin BT risk yönetimi başarısı üzerinde etkisi olduğu görülmüştür.

Katılımcıların tamamına yakını kurumsal faktörlerin BT risk yönetimi başarısına etkisi konusunda görüş birliğine sahiptir. Katılımcıların ifadelerinden üst yönetim desteği, BT bütçesi ve bilgi güvenliği politikaları gibi kurumsal faktörlere ait göstergeler ön plana çıkmıştır. Bu bulgu, alanda daha önce yapılan çalışmalarda elde edilen kurumsal faktörlerin BT risk yönetimi başarısına etkisini araştıran çalışmaların bulgularını desteklemektedir (Tohidi, 2011; Knapp ve Marshall, 2007; Chang ve Ho, 2006; Hall,

2011; Al-Awadi ve Renaud, 2009). Benzer bir çalışmada da bilgi güvenliği politikaları, üst yönetim desteği ile BT risk yönetimi başarısına etki eden faktörler arasında yer almaktadır (Kraemer, Carayon ve Clem, 2009).

Kurumsal faktörlerin üst yönetim desteği, bilgi güvenliği politikaları, BT bütçesi ile net amaç ve hedefler göstergeleri dikkat çekmektedir. Üniversite üst yönetiminin desteği en önemli göstergedir. Üst düzey yöneticilerin temel sorumluluklarından birisi de kurumun sahip olduğu BT varlıklarını korumaktır. Bu doğrultuda üst düzey yöneticiler risk yönetimi süreçlerine aktif olarak destek vermelidir. BT risk yönetimi süreci üst yönetim tarafından onaylanmalı ve desteklenmelidir. Üniversitelerin bilgi güvenliği politikalarında çalışanların sorumlulukları, BT varlıklarının yönetimi, korunması ve işlevleri açık olarak ortaya konmalıdır. Bilgi güvenliği politikaları kullanıcıların işini zorlaştırmamalı, tepkiye yol açmamalı ve tatbik edilebilir olmalıdır. BT bütçesi, üçüncü gösterge olup yeterli bütçe üniversitelerde BT alanında ihtiyaç olan yazılım, donanım, personel ve danışmanların sağlanmasını kolaylaştıracaktır.

Katılımcıların insan faktörünün BT risk yönetimi başarısı üzerinde etkisi olduğunu düşündüğü ikinci faktördür. Alanyazında bulunan çalışmalar da insan faktörünün BT risk yönetimi başarısında etkisi olduğunu, ayrıca bilgi güvenliği ve risk yönetiminde insan unsurunun ön plana çıkması gerektiği vurgulanmaktadır (Kraemer ve diğerleri, 2009; Landoll, 2006). Lacey'e (2009) göre güvenlik gerçekten bir insan sorunudur. İnsanlar, teknolojiyi kontrol eder ve tersi geçerli değildir. Diğer bir çalışmada araştırmacılar kurumlarda uygulanan güvenlik programlarının başarısı için iki temel bileşenden birinin insan faktörü olduğunu belirtmişlerdir (Ang, Lee, Madnick, Mistress, ve Siegel, 2006).

İnsan faktörü açısından BT risk yönetimi başarısını artırmak için ilk olarak, üniversitelerde çalışan idari ve akademik personelin bu süreçte yapılması gerekenler, atılması gereken adımlar ve güvenlik farkındalığı konusunda bilgilendirilmesi ve personele BT riskleri ve yönetim süreçleri ile eğitim etkinlikleri düzenlenmesi önemlidir Özellikle BT personeli güncel BT tehditleri ve riskleri konusunda gerekli eğitimleri almalı ve bu konularda yetkin hale gelmelidir.

BT risk yönetimi başarısını etkileyen üçüncü faktörün çevresel faktörler olduğu görülmüştür. Yaraghi ve Langhe (2011), risk yönetimi sistemlerini etkileyen başarı faktörlerini araştırdıkları çalışmalarında 19 tane başarı faktörünün içerisinde çevresel faktörlerin de yer aldığı görülmektedir. Aynı doğrultudaki diğer bir çalışmada, bilgi güvenliği yönetim sistemi başarı faktörleri araştırılmış olup çevresel faktörlerin göstergelerinin kullanıcı başarısı, endüstri karakteri, teknoloji ile altyapı desteği ve yasalar olduğunu belirtmişlerdir (Norman ve Yasin, 2013).

Çevresel faktörlerin öne çıkan göstergelerinin standartlara ve yasalara uyum ile politik çevrenin tutumu olduğu görülmektedir. İlk gösterge standartlara uyum olup, üniversitelerin BT alanındaki standartlara uyumunu önermektedir. Standartlar üniversite

üst yönetiminden BT personeline kadar herkes için görev ve sorumlulukları belirlemeye yardımcı olup üst yönetime ve BT personeline yol göstericidir. Bu alandaki başlıca standartlar; ISO/IEC 13335 77 (International Organization for Standardization), ISO/IEC 17799 (ISO/IEC 27002:2005) 78, ISO/IEC 27000 serisi, ISO/IEC 31000, NIST 94 standartları ve AS/NZS 4360 105'dir (Kouns ve Minoli, 2010). Üniversiteler bilgi güvenliğini sağlama ve BT risk yönetimi süreçlerinde standartlara uygun şekilde süreç yönetim politikalarını belirleyebilir. Standartlar, BT risklerini en aza indirmede yardımcı olabilir ve bu süreçlerin başarıyla yönetilmesinde önemli bir faktör olarak değerlendirilebilir. İkinci gösterge yasalara uyum olup üniversitelerde diğer kurumlar gibi BT alanındaki yasalara uyum sağlamalıdır.

Bu bağlamda, üniversiteler Türkiye Bilimsel ve Teknolojik Araştırma Kurumu'nun (TÜBİTAK) bir enstitüsü olan Ulusal Akademik Ağ ve Bilgi Merkezi (ULAKBİM) tarafından işletilen Ulusal Akademik Ağ'ın (ULAKNET) kullanımına ilişkin usul ve esasları düzenleyen, ULAKNET Kullanım Politikalarını temel alarak bilişim kaynakları kullanım politikaları ve kuralları oluşturulabilir. Bilişim kaynakları kullanım politikaları, üniversitelerin yerel alan ağı, kablosuz ağları, bilgisayarları ve enformatik hizmetlerini kapsamalıdır. Bununla birlikte, üniversiteler bilişimle ilgili yasal düzenlemelerin (kanunlar, yönetmelikler, genelgeler) gereklerini de yerine getirmelidir. Bu konu ile ilgili yasal düzenlemeler "5651 sayılı kanun", "Türk Ceza Kanunu", "Kamu Kurumları İnternet Sitesi Kılavuzu ile ilgili Başbakanlık Genelgesi", "Elektronik İmza Kanunu Hakkındaki Yönetmelik" ile ortaya konmaktadır. Örneğin "5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'a" uyum çözümleri geliştirilebilir. Bu doğrultuda üniversite internet ağına içeriden ve dışarıdan gelebilecek herhangi bir saldırıyı, önleyecek sistem oluşturulabilir. İnternet güvenliğini sağlamak için içerik tabanlı filtreleme sistemi kurulabilir. Kanunda belirtilen ve tutulması istenilen kayıtlar (loglar) tutulmalıdır. Bu yasal düzenlemeler tüm kuruluşların risk yönetimi programları olması gerektiğini ve riskleri yönetmek ve azaltmak için BT risk değerlendirmesi yapmalarını gerektirmektedir. Bu nedenle, BT risk yönetimi hedeflerinin, politikalarının ve uygulamalarının yasal düzenlemelerle tutarlı olması önem taşımaktadır. Üçüncü gösterge politik çevre olup, Yaraghi ve Langhe (2011) politik çevrenin BT alanında olumlu tutuma sahip olmasının kurumların BT risk yönetimi başarısını olumlu yönde etkileyebilecek güçte olduğuna işaret etmektedirler.

Teknolojik faktörler, BT risk yönetimi başarısı üzerinde etkisi olduğu düşünülen son faktördür. Katılımcıların tümü kritik altyapı analizi ve yazılım ile donanım güvenliğinin önemine vurgu yapmışlardır. Benzer şekilde alanyazındaki çalışmaların sonuçları da teknolojik faktörlerin BT risk yönetimi başarısı üzerinde etkisi olduğunu vurgulamaktadır. Werlinger, Hawkey ve Beznosov (2009) tarafından yapılan çalışmada araştırmacılar teknolojik faktörlerin BT risk yönetim sürecine etkisini belirtirken teknolojik faktörleri hareketlilik, açıklıklar ve güvenlik araçlarının desteği olmak üzere üç alt grupta incelemişlerdir.

Teknolojik faktörlerin göstergeleri donanım, yazılım güvenliği ve kritik alt yapı analizi olup başarılı bir BT risk yönetimi için bu göstergeler dikkate alınıp değerlendirilmelidir. Üniversiteler BT varlıklarını tespit etmeli ve güvenliklerini sağlamalıdır. BT varlıklarının alt yapıları analiz edilmeli ve felaket kurtarma merkezleri kurulmalıdır.

Bu çalışma Ankara'daki vakıf üniversiteleri veya diğer kurumları da kapsayacak şekilde genişletilebilir.

Kaynaklar

Ahlan, A.R., Arshad, Y. (2012). Information Technology Risk Management: The Case Of The International Islamic University Malaysia. *Journal of Research and Innovation in Information Systems, 1,* 58-67.

Ang, W. H., Lee, Y., Madnick, S., Mistress, D. ve Siegel, M. (2006, August). House of security: Locale, roles and resources for ensuring information security. *Conference on Information Systems*, Acapulco, Mexico.

Aktaş, F. Ö. ve Soğukpınar, İ. (2010). Bilgi güvenliğinde uygun risk analizi ve yönetimi yönteminin seçimi için bir yaklaşım. *TBV Bilgisayar Bilimleri ve Mühendisliği Dergisi, 3,* 53-62.

Al-Awadi, M. ve Renaud, K. (25-28 Şubat 2009). Successfactors in information security implementation in organizations. *IADIS International Conference e-Society*.

Altunışık, R., Çoşkun, R., Yıldırım, E. ve Bayraktaroğlu, S. (2010). *Sosyal bilimlerde araştırma yöntemleri*, (6. bs.), Sakarya: Sakarya Kitabevi.

Bailey, K. (2007). *Methods of social research* (4th. ed.), New York: NewYork Free Press.

Chang, S. E. ve Ho, C. B. (2006). Organizational factors to the effectiveness of implementing information security management. *Industrial Management & Data Systems, 106,* 345-61.

Cheng, V. V. (2012*). Ensuring the effectiveness of information security policy: The development and validation of an information security policy model*. Yayımlanmamış doktora tezi, The University of Albany, USA.

Chow, K. L. (2008). *The success of information security projects: an investigation of the project management process, project cost, project risks and user acceptance*. Yayımlanmamış doktora tezi, Capella University, USA.

Culler, E. W. (2009). *The degree of relationship between critical success factors and information technology project performance*. Yayımlanmamış doktora tezi, The University of Phoenix, USA.

Emiral, F. (2003). *Bilgi ağı güvenlik denetimi genel yaklaşımı*. 06.01.2016 tarihinde http://www.denetimnet.net/UserFiles/Documents/44_26_1.pdf adresinden erişildi.

Franklin, S. D. (2010). *Managing Information Assets.* 06.01.2016 tarihinde http://www.ucop.edu/ucophome/businit/boi/presentations/2010/09-mging_info_assets_franklin.pdf adresinden erişildi.

Gerber, M. ve Solms, R.V. (2005). Management of risk in the information Age. *Computers & Security*, 24, 16-30.

Goel, S. ve Chen, V. (2010). Information security risk analysis–a matrix-based approach. *Information Resources Management Journal*, 23(2), 33-52.

Hall, J. H. (2011). *Examining impacts of organizational capabilities in information security: A structural equation modeling analysis*. Yayımlanmamış doktora tezi, George Washington University, USA.

Ifinedo, P. (2008). Impacts of business vision, top management support, and external expertise on ERP success. *Business Process Management Journal*, 14(4), 551-568.

Jourdan, S. Z. (2008). *An investigation of organizational information security risk analysis*. Yayımlanmamış doktora tezi, AuburnUniversity, USA.

Knapp, K. J. (2005). *A model of managerial effectiveness in informationsSecurity: From grounded theory to empirical test*. Yayımlanmamış doktora tezi, The University Of Auburn At Alabama, USA.

Knapp, K. J. ve Marshall, T. E. (2007). *Top management support essential for effective information security*. in Tipton, H. F. & Krause, M. (Eds.), Information security management handbook (6th ed.) içinde (pp. 51-58). Boca Raton, FL: Auerbach Publications.

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

Kotulic, A. G. (2001). *The security of the IT resource and management support: Securıty risk management program effectiveness*. Yayımlanmamış Doktora Tezi, The University Of Texas At Arlington, USA.

Kouns, J., Minoli, D. (2010). *Information technology risk management in enterprise environments* (1th. ed.). New Jersey***:*** A John Wiley & Sons Publication.

Lacey, D. (2009). *Managing the human factor in information security: How to win over staff and influence business managers* (1th. ed.). England: Wiley & Sons.

Landoll, D. J. (2006). *The security risk assessment handbook – A complete guide for performing security risk assessments* (2nd. ed.). Florida: CRC PRess.

Norman, A. A. ve Yasin, N. M. (2013). Information systems security management (ISSM) success factor: Retrospection from the scholars. *African Journal of Business Management*, *7*(27), 2646-2656.

Patton, M. Q. (1987). *How to use qualitative methods in evaluation* (2nd. ed.). California: Newbury Park Sage Publication.

Pfleeger, S.L. (2000). Risky business: what we have yet to learn about risk management. *The Journal of Systems and Software*, *53*(3), 265-273.

Pierce, R. E. (2012). *Key factors in the success of an organization's information security culture: A quantitative study and analysis*. Yayımlanmamış doktora tezi, Capella University, USA.

Princeton Üniversite. (2013). *Managing risk to the University's information*. 15.02. 2014 tarihinde http://www.princeton.edu/itsecurity/basics/understanding-policy/ adresinden erişildi.

Rezgui, Y. ve Marks, A. (2008). Information security awareness in higher education: An exploratory study, *Computers&Security, 27,* 241-253.

Saleh, M. S., Alfantookh, A. (2011). A new comprehensive framework for enterprise information security risk management. *Applied Computing and Informatics, 9,* 107–118.

Sözbilir, M. (2009). *Nitel veri analizi*. 02.06.2014 tarihinde https://fenitay.files.wordpress.com/2009/02/1112-nitel-arac59ftc4b1rmada-veri-analizi.pdf adresinden erişildi.

Strauss, A. L. ve Corbin, J. (2007). *Basics of qualitative research: Techniques and procedures for developing grounded theory* (3th. ed.). California: SAGE Publications.

Teo, T. S. H. ve Ang, J. S. K. (1999). Critical success factors in the alignment of IS plans with business plans. *International Journal of Information Management*, *19,* 173-185.

Tohidi, H. (2011). The role of risk management in IT systems of organizations. *Computer Science*, *3,* 881–887.

Virginia University. (2013)**.** Information Technology Security Risk Management (ITS-RM). *Virginia* University.

Werlinger, R., Hawkey, K. ve Beznosov, K. (2009). An integrated view of human, organizational, and technological challenges of IT security management. *Information Management & Computer Security*, *17*(1), 4-19.

Yaraghi, N. ve Langhe, R. G. (2011). Critical success factors for risk management systems. *Journal of Risk Research*, *14*(5), 551-581.

Yeo, A. C., Rahim, M. M. ve Miri, L. (2007). *Understanding factors affecting success of information security risk assessment: The case of an Australian higher education institution*. Paper presented at Pacific Asia Conference on Information Systems *(*PACIS*),* New Zealand.

Yıldırım, E.Y., Akalpa, G., Aytaç, S. ve Bayram, N. (2011). Factors influencing information security management in small and medium-sized enterprises: A case study from Turkey. *International Journal of Information Management*, *31,* 360-365.

Yıldırım, A. ve Şimşek, H. (2008). *Sosyal bilimlerde nitel araştırma yöntemleri* (6. bs.). Ankara: Seçkin Yayınevi.

Young, R. F. (2008). *Defining The information security posture: An empirical examination of structure, integration and managerial effectiveness*. Yayımlanmamış doktora tezi, The University of North Texas, USA.

Zafar, H. (2010). *Critical success factors for an effective security risk management program in an organization: An exploratory case study*. Yayımlanmamış doktora tezi, The University of Auburn At Alabama, USA.