# *BİLİŞİM SİSTEMLERİNDE RİSK YÖNETİMİ BENİMSEME MODELİ*

**Müge Kuyumcuoğlu**
**Doç.Dr. A.Nuri Başoğlu**
Boğaziçi Üniversitesi, Yönetim Bilişim Sistemleri Bölümü

**ÖZET**
Bilişim teknolojileri (BT) kurumlar tarafından daha yaygın kullanır hale geldikçe, BT risklerinin yönetimi de kurumların devamı için giderek artan düzeyde önemli olmuştur. BT risklerinin yönetilmesinde önemli bir nokta da, çalışanların kullandıkları BT güvenliği ile ilgili kontrol ve standartlara bağlılığıdır. Bu çalışmanın amacı, kullanıcıların BT riskleri yönetimi uygulamalarına karşı tutumlarını ve davranışlarını etkileyen faktörleri belirlemektir. Araştırma sonucunda Teknoloji Kabullenme Modelinin temel değişkenleri yanısıra, risk algılaması, kurumsal faktörler ve güvenlik konusundaki kişisel bilgi ve bilincin etkili olduğu bulunmuştur.

**Anahtar Sözcükler:** Bilişim sistemleri, Risk yönetimi, Teknoloji benimseme, Teknoloji Kabullenme Modeli

# INFORMATION SYSTEMS RISK MANAGEMENT ADOPTION MODEL

**ABSTRACT**
As organizations become using information technology (IT) more extensive, IT risk management is turning out to be more crucial for the continuity of the organizations. One important aspect of IT risk management is the commitment of users to IT security standards and controls. This paper aims to find the leading factors that affect the users' attitude and behaviour towards IT risk management procedures. As the result of the research, besides the basic factors of Technology Acceptance Model, risk perception, organizational factors and security knowledge and consciousness have been found to be effective.

**Keywords:** Information systems, Risk management, Technology adoption, Technology Acception Model

## GİRİŞ

Son yıllarda bilgisayarların girdiği alanların çeşitliliği çok artmış, iş dünyasından pek çok farklı işleve destek olarak bilişim sistemlerinin kullanımı yaygınlaşmıştır. Aynı zamanda bu tür sistemlerde kaydettiğimiz verinin hacmi ve çeşitliliği de artmaktadır. IDC'nin (2007) araştırmasına göre 2006-2011 yılları arasında dünya bilişim harcamaları yıllık ortalama %6 artacaktır. Pek çok farklı düzeyde ve değişik bölüm çalışanları yoğun bir şekilde bilişim sistemlerini kullanmaktadır. Zaman içinde bu sistemlere yeni işlevler eklenmesi talep edilmekte ve mevcut sistemler de daha etkin ve verimli kullanılmaya çalışılmaktadır. Bir kurumun bilgi varlığının büyük bir kısmı bu sistemler tarafından kapsanır hale gelmektedir. Bazı bilgilere yirmidört saat evden ve sokaktan erişilebilir hale gelmiştir. Bütün bunların sonucu bilgisayar teknolojilerine olan bağımlılık gittikçe artmaktadır. Türkiye'de iş hayatında bilgisayar kullanan kurumların oranı %87'leri bulmuştur. Bu sayı 250'den fazla çalışanı olanlarda %99,22 dir (DİE, 2007). Bu karmaşık bağımlılığın dikkatle yönetilmesi gerekmektedir

Teknoloji kullanımı sayesinde kazanılan pek çok yarar olmakla birlikte, bu sistemlerin değişik olumsuz etkileri gözlenmektedir. Bilişim sistemlerinn sürekliliğini tehdit eden farklı güvenlik problemleri bulunmaktadır. Değişik güvenlik açıklarının olası etkileri arasında kurum ve kişisel bilgilerin çalınması, değiştirilmesi ve yokedilmesinin yanısıra, bütün sistemin çalışamaz hale gelmesi de vardır.

Bilişim alanının önemli dergilerinden MIS Quarterly'nin bilişim teknolojileri (BT) yöneticileri arasında yaptığı "Kritik BT konuları" başlıklı araştırmanın sonuçlarına göre 2003 yılında bilişim güvenliği önem açısından üçüncü sıraya yükselmiştir (Luftman, ve McLean, 2004). Her yıl CSI'in yaptığı güvenlik araştırmasının 2007 raporuna göre, kuruluşlar BT bütçelerinin %5'ini güvenlik harcamalarına ayırmış, kuruluşların %46'sı son 12 ayda bir güvenlik problemi yaşamış, ve bu problemler sonucu her kuruluşta ortalama 350 bin $'lık bir zarar oluşmuştur (Richardson, 2007). Bir başka önemli bulgu da güvenlik problemlerinin nedenleri arasında ilk sırada kuruluş çalışanlarının yol açtığı açıklar bulunmaktadır.

Sarbanes Oxley, Amerika'da yatırımcıları korumak amacıyla 2002'de yürürlüğe geçirilen, halka açık şirketlerin uymakla yükümlü olduğu, başta muhasebe, denetim, finans konuları olmak üzere şirketlerin bütün faaliyetleriyle ilgili, yönetim ve çalışanlarına ayrıntılı kural ve denetimler getiren geniş kapsamlı kanun reformudur. Bu düzenlemeler bir referans noktası olarak diğer ülkelerde de kullanılmaya başlanmış ve bu çerçevede, Sarbanes Oxley düzenlemeleri kamu kuruluşlarının özellikle Türkiye'de bankaların güvenlik standartlarına uymalarını zorunlu hale getirmektedir. BT risk yönetimi, bu konuda BS7799, COBIT (Control Objectives for Information and Related Technology) vb olgunlaşmış standartların uygulanmasını ve kurum içinde BT kullanımında sistematik bir yaklaşımı barındırmaktadır. Güvenlik

analizlerinde ortaya çıkan bir gerçek en önemli güvenlik açığının çalışanlar üzerinden oluştuğudur (Atkinson, 2005). Diğer yandan sistemlerin güvenlik açıklarının farkedilmesi ve kapatılması konusunda insanların önemli katkısı da gözden kaçmamaktadır. Standartların uygulanması karşısındaki en büyük tehdit, kullanıcıların iyi ya da kötü niyetle kuralları ihlal etmesidir. Bu konuda başarılı olmanın yolu, çalışanların bu uygulamaların gerekliliğine inanmalarıdır.

Kişiler görevlerinin yanısıra bilgisayarları kullanır iken bazı ek işlemler yapmaları, bazı konulara dikkat etmeleri, bazı yeni kavram ve araçlar ile karşılaşmaları gerekmektedir. Bir kısmı teknik tanımlar içeren bu yeniliklerin anlaşılması, anlamlandırılması ve verimli ve sürekli bir şekilde uygulanması gerekmektedir. Hem yeni olması hem de bazı zorluklar içermesi çalışanlar için çok çekici değildir. Genellikle de güvenlik önlemleri dahil benzeri her yeni oluşumun benimsenip kabullenilmesinden önce bir zaman geçmesi beklenmekte, bazı durumlarda da çalışanların bu değişimlere karşı çıkmaları, pasif veya aktif direnişe geçmeleri sözkonusu olabilmektedir. Ama her şekilde bu önlemlerin tutarlı bir şekilde uygulanması gerekmektedir. Bu noktada çalışanların güvenlik önlemlerini benimsemeleri ve kabul etmeleri daha sonraki davranışları açısından çok önemlidir.

Bu araştırmanın odak noktası bilişim sistemleri risk yönetiminin sosyal, davranışsal ve yönetimsel yönleri olacaktır. Bu çalışmada bilişim güvenlik önlemlerini benimseyerek gerçekleştirilmesinde etkili olan faktörler araştırılmaktadır. Bununla ilgili bir model kurulmuş, hipotezler geliştirilmiş ve sahadan toplanan veri ile bazı analizler yapılmıştır. Analiz sonucu elde edilen bulgular tartışılmıştır.

## 1. LİTERATÜR TARAMASI

Bilgi güvenliği yönetimi, firmanın elektronik varlıklarının gizlilik, bütünlük ve kullanılırlık açılarından baştan sona korunmasını sağlamak için; yönetim ekibinin yüklendiği sorumluluk ve gösterdiği liderlik, kurumsal yapı, kullanıcıların farkındalığı ve konuya bağlılığı, kurumsal politikalar, usuller, süreçler, teknolojiler ve yürürlükteki standart ve yasal şartlara uyum mekanizmaları gibi faktörlerin birbirini destekler şekilde çalışmasıdır (von Solms, 2005). Bir risk yönetimi sürecinin temel aşamaları "başlangıç", "risk analizi/çözümlemesi", "riskle ilgili işlem yapılması" ve "kontrol"'dür.

Bilişim risk yönetiminin ana amaçlarını aşağıdaki gibi listelemek mümkündür (Ward ve Clifton, 2002)

Sistemin erişilebilirliğini, ve sürekliliğini sağlamak
Sistemin bütünlüğünü, doğruluğunu sağlamak
Bilginin gizliliğini garanti altına almak.

Risk kavramı, satın alma (Cunningham, 1967; Heijden vd., 2003; Featherman ve Pavlou, 2003), proje yönetimi (Kwak ve LaPlace 2005; Kutsch ve Hall, 2005), teknoloji kullanımı (Broderick, 2001; Caelli, 2002; Siegrist, 2000) gibi farklı

durumlarda incelenmiştir. Firmalarda risk yönetimi prosedürleri ile ilgili neredeyse bütün kararların verilmesi ve yürütülmesi bilgi-teknoloji departmanları tarafından uygulanmasına rağmen, bu uygulamaların başarısında, son kullanıcıların BT risk yönetimi tedbirlerini benimseme ve kabul etmeleri çok önemlidir. Bu kontrollerin pek çoğuna uyum kullanıcılar açısından zorunlu hale getirilmiştir, hatta bir kısmı kullanıcıların kasten ihlal etmesini engelleyecek şekilde tasarlanmıştır. Yine de, kullanıcıların bu kontrollere karşı olumlu tutum geliştirmeleri ve kurumun genel kültürünün bir parçası olarak bu kontrollere uymayı üstlenmeleri ideal olan durumdur. Örnek olarak, risklerin azaltılması (güvenlik) ile esneklik arasında denge kurulması önemlidir, çünkü birini elde etmek için diğerinden vazgeçilmesi gerekir. Bu durumu çözmenin etkili yollarından biri firma içinde güvenlik kültürünü geliştirmektir. Böylece risklere ilişkin iletişim daha verimli yapılabilir ve bilgi güvenliğinden vazgeçmeden, sıkı kontroller koyma gereksinimi azalır (Koskosas ve Paul, 2004). Son kullanıcıların tutum ve davranışları şirketin güvenlik kültürünü oluşturduğu için, bunların kaynaklandığı etmenleri anlamak gereklidir (Schlienger ve Teufel, 2003).

BT risk yönetiminin kapsamı: "Risk analizi yoluyla yalnızca maddi varlıklara yönelik riskleri incelemek değil, aynı zamanda maddi olmayan varlıklara ya da bilgi varlıklarına yönelik riskleri de; kültürel, yasal ya da diğer sosyolojik faktörleri göz önünde bulundurarak incelemektir" (Gerber ve von Solms, 2005). Bu varlıkların korunması teknolojik ve yönetimsel kontrollere bağlıdır ve bu risklerin olumsuz sonuçlarının hem sosyolojik hem de maddi etkileri olabilir (Gerber ve von Solms, 2005).

Risk telafi teorisine göre, riski azaltmaya yönelik yapılan iyileştirmeler, sistemdeki toplam riskin azalması yönünde yeterli olmamakta, sadece şekil değiştirmesine yaramaktadır (Stewart, 2004). Kurumsal özelliklerin, özellikle üst yönetim desteğinin rekabet dezavantajı oluşturabilecek riskin yönetilmesi konusunda etkili olduğu belirtilmektedir (Jarvenpaa ve Ives 1991; Kankanhalli vd., 2003). Kankanhalli vd., (2003) kurum büyüklüğü, üst yönetim desteği ve sektör türünün bilişim güvenlik faaliyetlerinin etkinliğini belirlediğini ölçmüştür.

Bilişim sistemlerinin güvenliğinin sağlanmasındaki başarı kurum çalışanlarının bu konuya inanmalarına bağlı olduğu için, çalışanların güvenlik ile ilgili sorumlulukların bilincinde olmaları gerekmektedir (Ward ve Clifton, 2002).

### 1.1 Risk

Teneyuca'ya göre (2001), risk yönetiminin üç temel bileşeni vardır;

Bir olay,
Olayın gerçekleşme olasılığı,
Olay gerçekleşirse oluşacak etkiler ya da risk altında olan toplam miktar.

Bu çerçevede sistematik düşünen bir kullanıcı için algıladığı BT riskinin büyüklüğü, riskin gerçekleşme olasılığı ve riskin olası

etkisi ile ilişkilidir. Kullanıcılar açısından BT Risklerini iki kategoriye ayırmak mümkündür: Proje riski ve mesleki risk (Wilemon ve Cicero, 1970). Proje riski firma için zarar olasılığıdır, mali kayıpları, performans ya da zaman kayıplarını içerir. Buna karşın mesleki risk, çalışanın kişisel riskidir, bir faaliyetin sonuçlarının çalışanın kişisel hayatını ve kariyerini nasıl etkileyeceği ile ilgilidir. Kwak ve LaPlace'a göre, proje riski klasik risk yönetiminin konusudur, ayrıca çalışanın algıladığı mesleki riske etki eden bağımsız bir unsurdur (2005).

### 1.2 Risk Algılaması

Algılanan risk, bir ürün ya da servisi kullanmanın olumsuz sonuçları olabileceğine dair hissedilen belirsizlik duygusu olarak düşünülür (Featherman ve Pavlou, 2003). Risk kavramına benzer olarak, iki boyutu vardır: meydana gelme olasılığı ve etkisinin büyüklüğü. Bu model geliştirilirken temel alınan varsayıma göre, bir riskin algılanan olasılığının ve etkisinin büyüklüğü arttıkça, kullanıcıların risk yönetimi prosedürlerini faydalı ve gerekli olarak görme oranının arttığı, risk yönetimine karşı tavırlarının olumlu olduğunu düşünülmektedir.

Algılanan riski etkileyen bir değişken de iletişim, yani kişiler, gruplar ve kurumlar arasında riske ilişkin etkileşimli bilgi ve fikir değişimi sürecidir (Jaeger, Renn, Rosa ve Wehler, 2001).

### 1.3 Risk Toleransı ve Beklenen Fayda Teorisi

Risk toleransı, kullanıcılar tarafından riskin algılanışını ve risk karşısındaki tutumlarını açıklamakta önemli bir etmendir. Kişileri üç risk toleransı grubuna göre ayırmak mümkündür: risk karşıtı (risk averse), risk alıcı (risk taking) ve risk tarafsız (risk neutral). Örnek bir grup içindeki kişileri bu bağlamda değerlendirmek için bir fayda eğrisi oluşturmak ve bu sınıflandırmalara göre ayırmak mümkündür (Akçaöz ve Özkan, 2005).

Bu yaklaşımın temelleri risk altında yapılan seçimleri konu edinen beklenen fayda teorisinde (expected utility theory) yatar. Buna göre "sınırlı seçenekler arasında herhangi bir normal tercih ilişkisi beklenen fayda olarak kaydedilebilir" (von Neumann ve Morgenstern, 1953). Risk-değer çerçevesi içinde risk alma çeşitli faktörlerin bir fonksiyonu olarak modellenmiştir (Weber, 2001). Bununla birlikte, beklenen fayda teorisi psikolojik faktörleri tamamen kapsamaz (Pablo, 1997). Risk alma özelliği ile ilgili olduğu bilinen değişkenlerdeki karakter farklılıkları kişilerin risk algılarındaki farklılıklarda etkilerini göstermektedirler (Weber, 2001). Risk alma davranışı hem kararın alındığı özel durumun koşulları hem de karar verici kişinin özellikleri tarafından belirlenmektedir (Weber, 2001).

Ticari faaliyetlerine ve kurumsal kültürlerine göre kurumların risk ile ilgili yerleşmiş inançları ve risk tolerans düzeyleri değişkenlik gösterir (Teneyuca, 2001). Hatta bir firmanın risk toleransı aynı proje içinde bile zamanla değişebilir (Kwak and LaPlace, 2005).

### 1.4 Risk Tutumu

Risk toleransı kavramıyla yakından ilgili bir başka kavram da

kullanıcıların riske yaklaşımı ya da risk tutumudur. Algılanan riske karşı kullanıcının tutumu, diğer bütün faktörlerin eşit olduğu durumlarda, kişilerin algıladıkları riskleri ne derece cazip (ya da tatsız) bulacaklarını, ve buna bağlı olarak daha riskli (ya da daha az riskli) alternatifleri seçeceklerini gösteren ölçüdür (Weber 2001).

Risk toleransı ve risk yaklaşımı bazen eşanlamlı olarak kullanılır. Bu araştırma bağlamında, risk toleransı, riskin olası etkisinin, kişinin, kendisi için tolere edilebilir olarak algıladığı büyüklüğüdür. Weber'in bulgularına göre (2001), kişilerin heyecan arayışı düzeyindeki farklılıklar ile risk almaya yatkın olmaları arasında görülen ilişki; algılanan aynı risk düzeyine karşı farklı tutumları olduğu için değil, algıladıkları risk düzeyinin farklı olmasından kaynaklanır. Bir başka deyişle, yüksek heyecan arayışı özellikleriyle tanınan grupların daha büyük riskler aldıkları görülür. Bunun sebebi bu gruptakilerin riskli alternatifi daha cazip bulmaları değil, aynı risk düzeylerini diğer gruplara göre daha düşük olarak algılamalarıdır. Weber'in (2001) önermesine göre durumsal özellikler ve kişisel özellikler risk alma eğiliminde birlikte etkili olur.

## 1.5 Yeni Süreçleri Kabul ve Uyum Süreci

Kurumsal benimseme ve uygulama modeline göre, bir teknoloji uygulamasının hayata geçirilmesindeki aşamalar aşağıdaki gibidir (Cooper ve Zmud, 1990):

Benimseme - Uygulamaya geçirmek için kaynak ayırma kararı verilmiştir

Uyum sağlama - Yeni teknoloji geliştirilmiş, kurulmuş ve düzenli bakımına başlanmıştır. Bununla ilgili prosedürler geliştirilmiş ve düzenlenmiştir. Kullanıcılar hem yeni prosedürler hem de yeni teknoloji konusunda eğitilmişlerdir.

Kabul etme - Kurumun üyeleri yeni teknolojinin kullanımını sağlamayı üstlenmeye ikna edilmişlerdir

Rutine dönüştürme - Teknoloji uygulamasının kullanımı normal faaliyet olarak desteklenmektedir

Kurum kültürünün parçası olma (infüzyon) - BT uygulamalarının daha kapsamlı ve derinlemesine kullanılması sayesinde işin her türlü boyutu dikkate alınır ve kurumsal verimlilik ve etkinlik artar

Bilgi güvenliği tedbirlerini uygulamaya geçirmek kararı bilgi teknoloji departmanı tarafından verilir. Son kullanıcıların bu kontrolleri kullanmayı kabul etmeleri ise ikincil (kişisel) benimseme olarak adlandırılır (Gallivan, 2001). Yönetimin bir yeni teknolojiyi uygulama kararı olan birincil benimsemeden ayrı olarak, ikincil benimseme son kullanıcıların yeni bir teknolojiyi, yani BT risk ve güvenlik prosedürlerini benimsemesidir.

## 1.6 Teknoloji Kabullenme Modeli

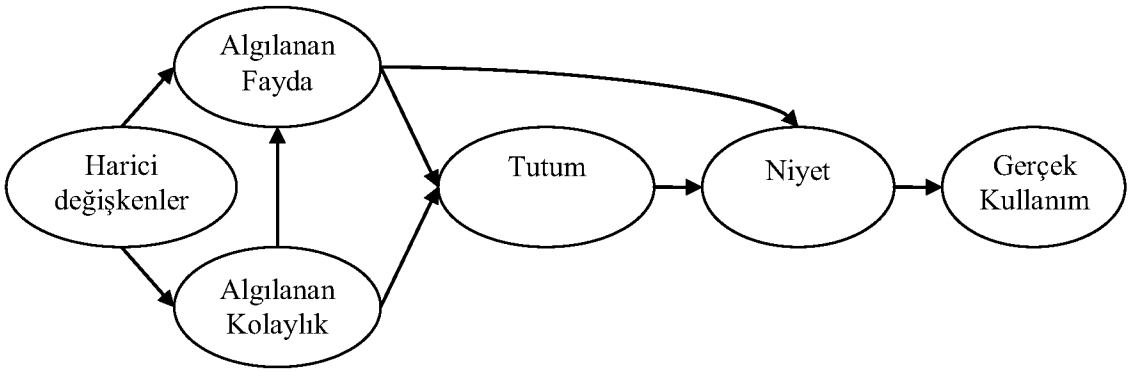
Teknoloji Kabullenme Modeli'ne (TKM) göre, bir kişinin bir sistemi kullanma niyeti kişinin o sisteme olan tutumu ve algılanan yarardan etkilenir, tutumu ise iki inancından kaynaklanır (Davis, 1989):

Algılanan fayda

Algılanan kullanım kolaylığı

*Algılanan fayda,* sistemi kullanmanın işteki performansını arttıracağına ilişkin ne derecede güçlü bir fikir sahibi olduğu; ve *algılanan kullanım kolaylığı*, sistemi kullanmanın zahmetsiz olacağına ilişkin inancının ne derece güçlü olduğudur (Şekil 1). TKM teorisine göre dış etmenlerin (sistemin özellikleri, geliştirme süreci, eğitim) sistemi kullanma niyeti üzerindeki etkileri algılanan fayda ve algılanan kullanım kolaylığı değişkenleri aracılığıyla vuku bulur. TKM'ye göre, algılanan fayda da algılanan kullanım kolaylığından etkilenir, çünkü, diğer özelliklerin denk olduğu durumlarda, kullanımı daha kolay olan bir sistem, kullanıcıya daha çok fayda sağlayabilir (Venkatesh ve Davis, 2000). Bu konuda yapılan pek çok deneysel araştırma TKM'nin kullanım niyeti ve davranışlardaki farklılıkların önemli bir kısmını (%40 civarı) açıkladığını bulmuştur; ayrıca TKM, kendisine alternatif olabilecek Sebepli Eylem Teorisi-SET (Theory of Reason Action-TRA) (Fishbein ve Ajzen, 1975) ya da Planlanan Davranış Teorisi-PDT (Theory of Planned Behaviour-TPB) (Ajzen, I., 1991) gibi diğer modellerle kıyaslandığında daha iyi sonuçlar elde etmektedir (Venkatesh ve Davis, 2000). TKM'nin genişletilmiş versiyonu olan TKM2'de öne sürülen hipoteze göre kullanma niyeti ile ilişkili olan faktörler: gönüllülük, deneyim, kişisel normlar, imaj, iş ile ilgili olma, çıktının kalitesi, ve sonucun ispat edilebilirliğidir (Venkatesh ve Davis, 2000). Venkatesh ve diğerleri (2003) daha sonra modele kolaylaştırıcı faktörler, cinsiyet ve yaş değişkenlerini ekleyerek Teknoloji Kabullenme ve Kullanım Birleşik Teorisi'ni –TKKBT (Unified Theory of Acceptance and Use of Technology-UTAUT) ortaya çıkarmışlardır.

**Şekil 1 : Teknoloji Kabullenme Modeli**




**(Davis, 1989)**

Jones ve Hubona (2005), çalışanın kıdemi, yaş ve eğitim düzeyi değişkenlerinin kullanma davranışını algılanan fayda ve algılanan kullanım kolaylığından bağımsız olarak ve daha fazla etkilediğini öngören hipotezlerini ispatlamışlardır. 11 yıl içinde 400'den fazla referans alan TKM'nin risk yönetimi alanına uyarlanıp bilişim güvenlik tedbirlerini benimseme davranışını inceleyen çalışma bulunamamıştır (Venkatesh ve Davis, 2000).

## 2. KAVRAMSAL MODEL - ARAŞTIRMANIN AMACI, İÇERİĞİ VE SINIRLARI

Bilişim sistemlerinin güvenlik açıkları gittikçe büyümektedir. Sözkonusu güvenlik açıklarının kapatılmasında değişik teknik çalışmaların yanısıra, çalışanların da katkısı beklenebilir. Bu çalışmada, bir kurum ortamında bilişim güvenlik önlemlerinin uygulanmasını etkileyen faktörleri içeren bir model kurulmakta ve analizi yapılmaktadır.

Bilişim sistemlerinin kapasite ve güçlerinin büyümesine paralel olarak maruz kaldıkları tehlikeler de büyümektedir. Sözkonusu güvenlik açıkları için farklı önlemler alınabilir. İnsanlardan oldukça bağımsız, kendi başına işleyen pek çok teknik önlem geliştirmek ve uygulamak mümkündür. Teknik önlemlerin yapı ve boyutlarından konu ile ilgili olmayan diğer çalışanların bir fikri olmayabilir, hatta varlıklarından haberdar bile olmayabilirler. Bu önlemlerin belli bir kısmını çalışanların gerçekleştirmesi gerekmektedir. Çalışanların alabileceği pek çok önlemin güvenliğe önemli katkıları vardır. Hatta bazı hassas güvenlik önlemlerini çalışanların desteğini almadan gerçekleştirmek oldukça zordur.

Bu araştırmada oluşturulan modelin kapsamında 5 ana hipotez tanımlanmıştır.

Risk algılaması iki önemli faktörden etkilenmektedir. Herhangi bir tehdidin verebileceği zararın boyutu ve bu tehdidin gerçekleşebilmesinin olasılığı kişilerin risk algılamasın belirlemektedir. Zararın boyutunun ve olasılığın büyük olması risk algılamasını yükseltmektedir. Beklenen ortalama kayıp, zarar ile olasılığın çarpımı ile elde edilebilir. Çalışmada zarar ve olasılık faktörlerinin yanısıra, zarar ve olasılık değişkenlerin çarpımından oluşan yeni değişken oluşturularak risk algılaması ile ilişkisi analiz edilecektir.

Hipotez 1 : Risk algılaması *Tahmin edilen olasılık ve zararın boyutları ile risk algılaması arasında anlamlı bir ilişki vardır.*

Bu önlemlerin sağladığı yarar, gerçek durumdan farklı algılanabilir. Dolayısıyla algılanan yarar, kavramsal olarak hesaplanan veya gerçekleşen yarardan farklı olabilmektedir. Önlemlerin verileri korumada, saldırıları engellemede ve bilgilerin gizliliğini korumadaki tahmini katkısı, yani yararlılık algılaması değişik faktörleri etkileyebilir. Sözkonusu yarar algılaması kişinin güvenlik önlemlerine karşı tutumunu da şekillendirebilir.

Risk - Belirli bir eşiği aşan risk algılaması dikkati olası tehdide çekmektedir. Bir tehdit hisseden kişi

de bunu yoketmek veya azaltmak için gerekli önlemleri, kendi üzerine düşen sorumluluğu düşünmeye başlamaktadır. Yorucu da olsa, bazı önlemlerin bir yarar sağlayacağı beklenilmektedir.

Bilinçlilik – Şahsi, sosyal veya teknik sebeblerle kişiler güvenlik açıkları ve gerekli önlemler konusunda kafa yormaya başlamakta, bu konu ile ilgili malzemeleri (evrak, belge, kitap vb.) incelemekte, ve bu konudaki harici söylemlere daha duyarlı hale gelmekte, dolayısıyla formel veya enformel (yapısal veya yapısal olmayan) bir şekilde kendilerini yetiştirmektedirler. Güvenlik konusunda daha duyarlı ve bilinçli kişiler, bilişim önlemlerini daha iyi değerlendirebilmekte ve yararlarını takdir etmektedir. Dolayısıyla oluşan bilgi birikimi ve bilincin yararlılık algılamasını etkilediği düşünülmektedir.

Kurum – Bir kurum içinde çalışan kişilerin içinde bulunduğu sosyal iklimi bazı kurumsal oluşumlar belirlemektedir. Sosyal iklim bazı durumlarda kişinin duygu ve davranışlarını sınırlamakta, zorlamakta, yönlendirmekte, teşvik etmekte, bazı işleri esnekleştirir iken, bazılarını da daha standartlaşma yönünde baskı uygulamaktadır. Ayrıca teknik ve sosyal destek de kişilerin davranış ve algılamalarını, bilinç seviyelerini belirlemektedir. Özellikle büyük projelerde ve işlerin çıkmaza girdiği durumlarda üst yönetim desteği anlamlı olmaktadır. Kurumsal yenilikçilik eğilimi hızla gelişen yeni uygulamalara daha sıcak bakılmasını sağlayacak bir sosyal iklim yaratmaktadır. Kurumsal özelliklerin bilişim güvenlik önlemlerinin yararlı bulunmasını etkilediği düşünülmektedir.

Kolaylık – Herhangi bir aletin veya hizmetin kullanılmasının kolay olmasının, yararını yükselttiği düşünülmektedir. Güvenlik önlemlerinin kolay olarak algılanması, sözkonusu önlemlerin daha yüksek bir yarar algılamasına yardımcı olmaktadır. Güvenlik önlemlerinin yararı kadar önlemlerin zorluğu da bu önlemlere karşı tutumları etkilemektedir. Zor olduğu düşünülen önlemleri kişilerin sürekli olarak tekrarlaması pek çekici değildir. Öğrenilmesi kadar, bazı işlemlerin tekrar tekrar hatasız bir şekilde yapılması çalışanlarda bıkkınlık yaratabilir, daha sonra da gerekli titizliğin gösterilmesine engel olur.

Hipotez 2 : Algılanan yararlılık *Risk algılaması, kurumsal faktörler, bilişim güvenliği konusundaki bilinç ve algılanan kolaylığın algılanan yarara anlamlı bir etkisi vardır.*

Bilişim güvenlik tehlikeleri ve gerekli önlemler konusunda bilinçli olan kişilerin güvenlik önlemlerini daha hızlı öğrendikleri, daha sürekli uyguladıklarını gözlemlemek mümkündür. Bu konulardaki bilinçlilik önlemlerin kolay bulunmasını olumlu yönde etkilemektedir. Kurumsal faktörlerin algılanan yararı arttırdığı gibi, kolaylık algılamasını da yükselttiği düşünülebilir. Değişik araçlar ile kişilerin güvenlik önlemlerinin daha kolay olmasını sağlamak mümkündür.

Hipotez 3 : Algılanan kullanım kolaylığı

*Bilişim güvenliği konusundaki bilincin algılanan kolaylığa anlamlı bir etkisi vardır.*

Bir çalışanın özellikle yeni veya karmaşık bir uygulama konusundaki tutumu son derece önemlidir. Bu durum çalışanın uygulama ile uzun dönemli ilişkisini oluşturmakta, üzerinde bir baskı hissetmeksizin, nispeten özgür iradesi ile bir davranışı gerçekleştirmesini sağlamaktadır. Özellikle bir yeniliği uyarlamanın iki önemli belirleyicisi olduğu var sayılmaktadır. Bu varsayım pek çok akademik çalışmada araştırılmıştır. Teknoloji Kabul Modelinin de merkezini bu varsayım oluşturmaktadır. Algılana yarar ve algılanan kolaylık bir kişinin bir nesne, uygulama, hizmet ve bunun benzeri şeylere karşı bakışını, onun hakkındaki duygu ve düşüncelerini oluşturmaktadır. Daha yararlı veya daha kolay olduğu algılanan bir sisteme olan yaklaşım daha olumlu olmaktadır. Yarar ve kolaylık algılaması kişinin tutumunu şekillendirmektedir.

Hipotez 4 : Tutum

*Algılanan yarar ve kullanım kolaylığının bilişim risk önlemlerini uygulama konusundaki tutuma anlamlı bir etkisi vardır.*

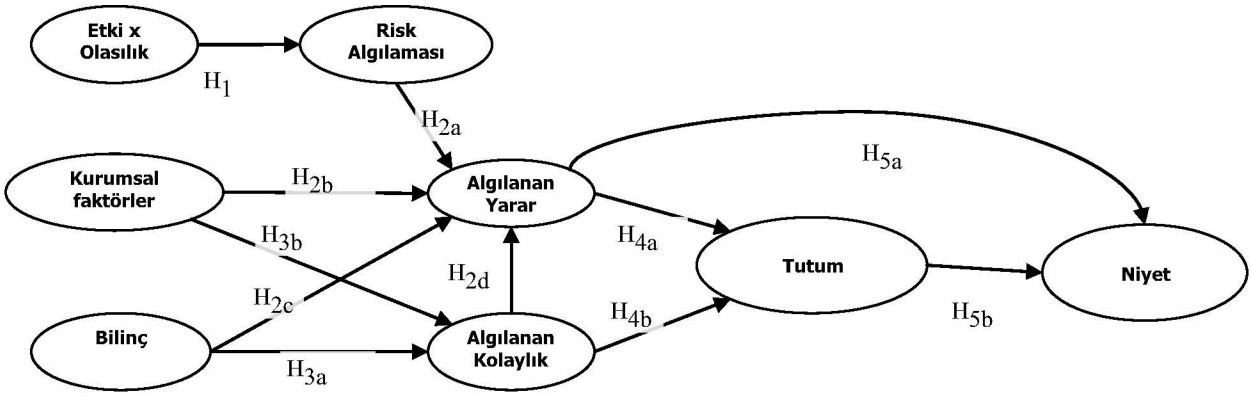
Bir kişinin tutumu o kişinin duygu, düşünce ve davranışlarının merkezindedir. Bir konuya olumu bakan kişi, (belirli şartlar gerçekleşince) söz konusu uygulama ile ilgili davranışlar bütününe daha istekli bir tarzda yaklaşmaktadır. Bir konuya olumlu bakan kişi, uygulama ile ilgili niyet ve planlarını hızla oluşturabilmektedir. Bir uygulamanın yararlı olduğunu düşünen ve uygulamaya sıcak bakan kişinin, sözkonusu uygulamayı gerçekleştirme konusunda ciddi bir niyete sahip olduğu ve planlar yaptığı düşünülmektedir. Bu ilişki literatürde çokça işlenmiş, tartışılmış ve pek çok ampirik araştırmada istatistiki olarak da modellenmiştir.

Hipotez 5 : Niyet

*Algılanan yarar ve tutumun bilişim risk önlemlerini uygulama konusundaki niyete anlamlı bir etkisi vardır.*

Geliştirilen hipotezler özet olarak şekil 2 de sunulmaktadır.

**Şekil 2 : Hipotezlerin görüntülendiği kavramsal çerçeve**




## 3. ARAŞTIRMANIN METODOLOJİSİ

Bu çalışmada bilişim sistemlerinin maruz kaldığı riskleri azaltmaya yönelik önlemlerin çalışanlar tarafından benimsenmesi ve uygulanması ile kurumsal ve kişisel bazı özelliklerin ilişkisi incelenmektedir.

Bu amaçla literatür ve uzmanların görüşleri derlenerek bu alandaki temel kavramlar ele alınıp, bir kavramsal model geliştirilmiş, ve hipotezler oluşturulmuştur. Çalışanların yeni teknolojiler ve uygulamalar noktasında davranışını ele alan modeller incelenmiş, özellikle Teknoloji Kabullenme Modelinin ana değişkenleri sözkonusu modelde temel olarak alınmıştır. Maddeler oluşturulurken literatürde bulunan bazı ölçekler uyarlanarak kullanılmış, ayrıca yeni bazı maddeler eklenmiştir (Ek). Maddelerin oluşturulmasında Davis (1989), Bajaj ve. Nidumolu (1998), Covin vd. (2001), Huang ve Chuang (2004), Knapp vd. (2005), Venkatesh ve Davis (2000) ve Vijayasarathy (2004) ın ölçeklerinden yararlanılmıştır. Demografik soruların haricindeki bütün sorular Likert tipi 5'li ölçek ile ölçülmüştür. 1: kesinlikle katılmıyorum ve 5: kesinlikle katılıyorum şeklinde düzenlenmiştir. Bir pilot çalışma ile sorularda düzenleme yapılarak daha doğru ve kolay olması yönünde düzenlemeler yapılmış, güvenilirlik testleri sonucu bazı sorular iptal edilmiştir. Çok maddeli değişkenlerin cronbach alfa değerleri 0,617 ile 0,831 arasında değişmektedir.

Veri hergün yoğun bir şekilde bilgisayar kullanılan, Türkiye'de önde gelen büyük kuruluşlardan toplanmıştır. Katılımcı kuruluşların ayrı bir bilgiişlem bölümü olması şartı dikkate alınmıştır. Sorular e-posta ile yaklaşık 1.200 kişiye yollanmış ve %11 geri dönüş oranı ile 137 çalışandan cevap gelmiştir.

Elde edilen veriler kontrol edilmiş, düzenlenmiş, bir veritabanına yüklenmiş ve SPSS 15.0 ile değişik incelemelere tabi tutulmuştur.

Veriler ile ilk önce katılımcıların genel özellikleri belirlenmiştir. Daha sonra bazı değişkenlerin maddelerine güvenilirlik

testi uygulanmış, ve bazı maddeler iptal edilerek düzenleme yapılmıştır. Söz konusu temel işlemleri takiben betimleyici istatistik ve korelasyon analizleri yapılmıştır. Regresyon analizi ile kavramsal çerçeve üzerindeki hipotezler sorgulanmıştır. Çıkan sonuçlar incelenip, yorumlandıktan sonra uzmanlar ile yeniden gözden geçirilmiştir.

## 4. ARAŞTIRMANIN BULGULARI

Araştırmada incelenen örnek kütlenin özellikleri Tablo 1'de gösterilmektedir. Buna göre cevap verenlerin %58'i erkek, büyük çoğunluğu da (%87) 20-40 yaşlarındadır. Katılımcıların %74'ü üniversite mezunu olup, çoğunluğun (%56) 5 yıldan fazla iş deneyimi vardır. Yaklaşık %35 bir ağırlığa sahip yönetici ve yardımcılarının yanısıra farklı pozisyonlardaki kişilerden de cevap toplanmıştır. Örnek kütlenin %27'si Bilişim Sistemleri bölümünde çalışmaktadır, hemen arkasından Satış bölümü gelmektedir. Cevap verenlerin sektörel dağılımı ağırlıklı olarak Sigorta/Çağrı merkezi (%39), Finans (%18) ve Teknoloji (%11) dir.

**Tablo 1 : Cevap verenlerin profili**

| Gruplar | | Adet | % |
|---|---|---|---|
| **Cinsiyet** | | | |
| | Kadın | 57 | 41,61 |
| | Erkek | 80 | 58,39 |
| **Yaş** | | | |
| | 20'nin altında | 1 | 0,73 |
| | 21–25 | 46 | 33,58 |
| | 26-30 | 39 | 28,47 |
| | 31–40 | 34 | 24,82 |
| | 41–50 | 13 | 9,49 |
| | 51 ve üstü | 3 | 2,19 |
| | Eksik | 1 | 0,73 |
| **Eğitim** | | | |
| | Lise mezunu | 14 | 10,22 |
| | Üniversite öğrencisi | 21 | 15,33 |
| | Üniversite mezunu | 80 | 58,39 |
| | Yüksek Lisans ve üzeri | 22 | 16,06 |
| **İş deneyimi** | | | |
| | 1 yıldan az | 14 | 10,22 |
| | 1–3 yıldır | 31 | 22,63 |
| | 3–5 yıldır | 15 | 10,95 |
| | 5–10 yıldır | 35 | 25,55 |
| | 10 yıldan fazla | 42 | 30,66 |
| **Bilgisayar kullanma deneyimi** | | | |
| | 1–3 yıldır | 5 | 3,65 |
| | 3–5 yıldır | 13 | 9,49 |
| | 5–10 yıldır | 53 | 38,69 |
| | 10 yıldan fazla | 66 | 48,18 |

Temel betimleyici istatistiki değerler incelendiğinde, risk algılamasının diğerlerine göre oldukça düşük olmasına rağmen, bilişim güvenlik bilincinin yüksek olduğu, güvenlik önlemlerine olumlu bakıldığı ve önlemlerin uygulanması konusunda kuvvetli bir niyet belirtisi görülmektedir (Tablo 2). Kurumsal desteğin ve güvenlik önlemlerinin kolaylığının nispeten diğerleri kadar yüksek olmadığı düşünülebilir. Risk algılamasının oluşumunda tehdit olasığından ziyade etkinin büyüklüğünün daha ağırlıklı olduğu düşünülmektedir.

**Tablo 2 : Temel istatistiki değerler**

| Değişken | N | Ort | Medyan | Minimum | Maksimum | Std. Sapma |
|---|---|---|---|---|---|---|
| Güvenlik bilinci | 136 | 4,07 | 4 | 1,5 | 5 | 0,70 |
| Kurumsal Destek | 137 | 3,63 | 3,64 | 2,43 | 4,79 | 0,49 |
| Riskin Etkisi | 136 | 4,01 | 4 | 1 | 5 | 0,88 |
| Riskin Olasılığı | 135 | 2,81 | 3 | 1 | 5 | 0,95 |
| Etki*Olasılık/5 | 135 | 2,30 | 2,4 | 0,2 | 5 | 1,00 |
| Risk algılaması | 136 | 2,68 | 2,5 | 1 | 5 | 0,95 |
| Algılanan Kolaylık | 136 | 3,63 | 4 | 1,5 | 5 | 0,87 |
| Algılanan Yarar | 136 | 3,99 | 4 | 2,67 | 5 | 0,59 |
| Tutum | 136 | 4,23 | 4 | 2,5 | 5 | 0,58 |
| Niyet | 136 | 4,20 | 4 | 2 | 5 | 0,55 |

Yapılan regresyon analizi sonucunda pek çok hipotezin **desteklendiği** görülmüştür.

H1: Bilişim sistemlerinin görebileceği zararın büyüklüğü ve zarar olasılığının yüksekliği risk algılamasını olumlu yönde etkilemektedir (B: 0,19; $p < 0,05$). Analiz sırasında olasılık ve etki değişkenleri, tek bağımsız değişkenler olarak ele alındığı gibi, etki ve olasılık değişkenlerinin çarpımı yeni bir değişken olarak da yer almıştır. Etki ve olasılığın çarpımından elde edilen değişken ile bir ilişki bulunması, daha anlamlı bir durumdur.

H2: Bilişim sistemi risk algılaması, kurumsal faktörler, ve bilişim güvenlik bilinci ile algılanan yararın ilişkili olduğu görülmüştür.

Kişisel güvenlik bilgi düzeyi ve bilinçlilik faktörlerinin çok kuvvetli bir şekilde yarar algılamasını olumlu yönde belirlediği anlaşılmaktadır (B: 0,29; $p <0,000$). Güvenlik önlemlerinin daha kolay olması önlemlerin daha yararlı bulunmasına etki yapmamaktadır. Teknoloji benimseme modellerinde kolaylık – yararlılık ilişkisi çokça incelenmiş, zaman zaman bu doğrultuda sonuçlar alınmış, zaman zaman da tersi bulunmuştur.

Risk algılamasının yükselmesi yarar algılamasını az da olsa olumlu yönde (B: 0,15; $p < 0,1$), kurumsal faktörler ise nispeten daha yüksek ve olumlu yönde etkilemektedir (B: 0,20; $p<0,05$).

H3: Güvenlik bilgi düzeyi ve bilinçliliğin beklendiği gibi kolaylık algılamasını da olumlu yönde etkilediği görülmektedir (B: 0,25; $p< 0,005$). Kurumsal faktörlerin ise kolaylık algılaması üzerine çok belirgin bir etkisi bulunmamıştır. Pek çok maddeden oluşan kurumsal faktörler eğer daha alt gruplar seviyesinde incelense etkili olan maddelerin bulunabileceği düşünülmektedir.

H4 – H5: Tutum ve niyet ile ilgili hipotezler de desteklenmiştir. Bilişim güvenlik uygulamalarına olan tutumu, yarar algılaması (B: 0,62; $p<0,000$) ve kolaylık algılamasının (B: 0,20; $p<0,05$) çok kuvvetli ve olumlu yönde belirlediği görülmüştür. Benzer

şekilde, güvenlik önlemlerinin gerçekleştirilmesine yönelik niyet ve planlara, tutum (B:0,64 ; p<0,000 ) ve yarar algılamasının (B: 0,25; p<0,000 ) kuvvetli ve olumlu yönde bir etkisi olduğu bulunmuştur. Bu ilişkiler daha önce pek çok çalışmada araştırılmıştır, ve bu çalışmada bulunan sonuçlar literatür ile uyumludur.

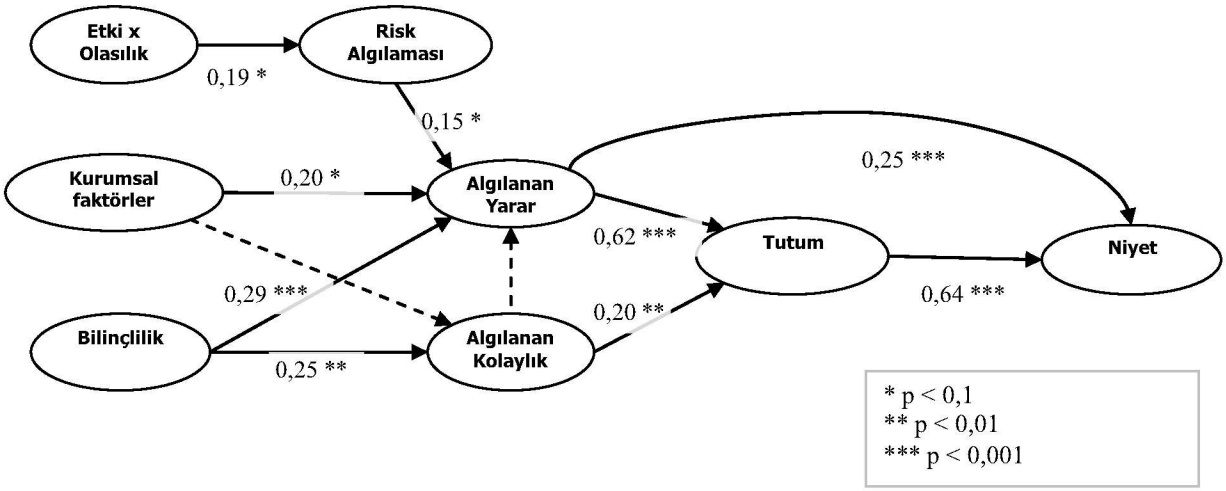
Regresyon analizlerinin ayrıntıları Tablo 3 de gösterilmektedir. Ayrıca modeldeki değişkenler ve ilişkilerin özeti Şekil 3'de verilmektedir.

Analiz sonucu Teknoloji Kabullenme Modelinin ana ilişkileri risk yönetimi alanında tekrar bulunmuştur. Ayrıca kolaylık ve yarar algılamalarını etkileyen önemli değişkenler tespit edilmiştir.

**Tablo 3 : Regresyon analizi sonuçları**

| Bağımlı Değişken | Bağımsız Değişken | Standartlaştırılmamış Katsayı | | Standartlaştırılmış Katsayı | t | Anlam düzeyi |
|---|---|---|---|---|---|---|
| | | B | Std. Hata | Beta | | |
| Risk Algılaması | (Sabit) | 2,26 | 0,20 | | 11,08 | 0,000 |
| | Etki * Olasılık | 0,18 | 0,08 | 0,19 | 2,22 | 0,028 |
| Algılanan yarar | (Sabit) | 1,81 | 0,42 | | 4,28 | 0,000 |
| | Bilinçlilik | 0,25 | 0,07 | 0,29 | 3,57 | 0,000 |
| | Kurumsal faktörler | 0,25 | 0,10 | 0,20 | 2,50 | 0,014 |
| | Risk Algılaması | 0,10 | 0,05 | 0,15 | 1,93 | 0,056 |
| Algılanan kolaylık | (Sabit) | 2,33 | 0,44 | | 5,34 | 0,000 |
| | Bilinçlilik | 0,32 | 0,11 | 0,25 | 3,02 | 0,003 |
| Tutum | (Sabit) | 1,29 | 0,28 | | 4,68 | 0,000 |
| | Algılanan yarar | 0,61 | 0,07 | 0,62 | 9,34 | 0,000 |
| | Algılanan kolaylık | 0,14 | 0,05 | 0,20 | 3,00 | 0,003 |
| Niyet | (Sabit) | 0,74 | 0,22 | | 3,41 | 0,001 |
| | Tutum | 0,60 | 0,06 | 0,64 | 9,46 | 0,000 |
| | Algılanan yarar | 0,23 | 0,06 | 0,25 | 3,64 | 0,000 |

**Sekil 3 : Değişkenler arası ilişkileri özetleyen sonuç görüntüsü**




## SONUÇ

Bu çalışmada bilişim güvenlik önlemlerinin benimsenip, uygulanmasını etkileyen faktörler incelenmiştir. Kurum içindeki çalışanların benimsemesini etkileyen faktörler, Teknoloji Kabullenme Modeli (TKM) üzerine yerleştirilmiş, ve konuya uygun harici etkenler eklenmiştir. Geliştirilen hipotezlerin ikisi hariç hepsinin desteklendiği görülmüştür. Araştırmanın bulgularına göre bilişim güvenlik önlemlerini uygulama konusundaki tutum ve niyeti belirleyenler TKM ile uyumludur. Sonuçlara göre bireylerin yararlılık algılaması ve güvenlik önlemlerine olan tutumu kişinin niyet ve planlarını belirlemekte, tutumunu ise yararlılık ve kolaylık algılaması şekillendirmektedir. Risk yönetimi alanında TKM modelinin test edilmesinin yanısıra, bu alana özgü ek değişkenler de eklenmiş ve test edilmiştir. Yarar algılamasını, risk algılaması, güvenlik konusundaki bilinç ve kurumsal faktörler oluşturmakta, kolaylık algılamasını ise bu konudaki bilinç etkilemektedir. Çok ayrıntılı olmamakla birlikte berlirli bir üst seviyeden, risk algılamasını ve risk yönetimine kişisel tepkiyi ölçen bir başlangıç modeli geliştirilmiştir. Bu alandaki araştırmalar oldukça azdır ve bilişim güvenlik davranış modelleri çok sınırlıdır.

Çalışmalar sırasında bu alandaki uygulamalarda gerçekleştirilen gözlemler, ilgili kişiler ile yapılan görüşmeler konunun derinliğine incelenmesine yardımcı olmuştur. Bu çalışmada literatürdeki farklı risk analiz çalışmalarından ve teknoloji benimseme modelerinden önemli kavramlar alınmış ve yeni bir modelin geliştirilmesinde kullanılmıştır.

### Uygulama Önerileri

Bilişim sistemlerinin gittikçe gelişen gücüne ve yaygınlığına bağlı olarak, bağımlılık artmaktadır. Bilişim sistemlerinin erişilebilirliğinin azaldığı, sağladığı yararlardan mahrum olunduğu veya gizli bilgilerin

ele geçirildiği durumlarda kurum büyük zararlar görebilir. Sağladığı yarara karşılık, bilişim sistemleri güvenliği için fazladan bir külfete katlanmak gerekmektedir. Bu çabayı tek bir yatırım, fazladan donanım ve çalışan alarak çözmek mümkün değildir. Bütün kurumu kapsayan bir güvenlik kültürü geliştirilmesi yönünde herkesi ilgilendiren bir faaliyet sözkonusudur. Dolayısıyla, insan kaynaklarından, kurum yapılarına, mali analizlerden, iş süreç tasarım prensiplerine kadar pek çok stratejik alanda güvenlik kavramı da dikkate alınarak düzenleme yapılması yararlı olacaktır.

Teknik olarak alınacak pek çok önlemin yanısıra, güvenlik açıklarının en büyük faktörü olan çalışanların da dikkatlice yönlendirilmesi gerekmektedir. Kişilerin güvenlik önlemlerini benimseme sürecinde, yönetilebilecek en önemli etken yararlılık algılamasıdır. Bu algılamayı da kişinin güvenlik bilgi ve bilinci oluşturmaktadır. Kişilerin bu görüşünü oluşturmak, şekillendirmek için pek çok şey planlanabilir ve uygulanabilir. Belirli dönemlerde kısa eğitimler, seminerler vererek kişilerin bu konuda duyarlı ve yeniliklere hazır hale getirilmesi, uyguladıkları önlemlerin hassas noktalarını daha derinden anlamalarının sağlanması, uygulamaların daha verimli yapılmasına yol açarak sıkılma, vazgeçme gibi durumlara dönüşmesinin engellenmesi önemlidir. Elektronik veya basılı olarak bu konuda bilgi veren malzemelerin, kısa gerçek hikayelerin derlenmesinin yanısıra bu konuda gerektiğinde destek olabilecek bir kişi/ofis oluşturulması kritik öneme sahiptir. Dikkati sürekli bu konunun üzerinde tutmak için afişler, logolar, sloganlar, maskotlar üretmek faydalı olabilir. İletişim kanalları sürekli açık tutulmalıdır. Yeni tedbirler uygulamaya geçirilmeden önce ve geçirilirken, değişikliklerin kapsamı ve kullanıcıları nasıl etkileyeceği ile ilgili sıklıkla bilgilendirme yapılmalıdır. Kullanıcıların beklentileri yönetilmelidir. Sistem üzerinden takip edilebilecek bazı işlemlerde kişilerin performansını ölçerek yetersizliklerin profilinin çıkartılması, düşük destek gösteren kişilerin eğitilmesi, yönlendirilmesinin sağlanması planlanabilir. Çok kritik işler için bazı cezai kurallar geliştirilebilir veya değişik teşvik mekanizmaları kurulabilir.

Bilişim güvenliği konusunda, dış danışmanlık desteği ve dış denetim almak kurum bilgi seviyesini, yeteneklerini ve hazırlanmışlığını yükseltecektir. Son dönemlerde gittikçe daha fazla yayılmaya başlayan COBIT ve benzeri güvenlik standartlarının uygulamasını veya karşılıklarını incelemek kurumlara bu konuda önemli bir vizyon sağlayacaktır.

Ward ve Clifton (2002) önerdiği önlemler arasında savunma derinliğinin oluşturulması, görevlerin ayrılması, gerektiği kadar bilgi prensibinin uygulanması, çifte gözetim yapılması, hesap verebilme kavramının yerleştirilmesi, her sürecin içine yerleştirilmiş gözetim işevleri bulunmaktadır.

## Araştırmanın Kısıtlamaları Ve Yeni Konu Önerileri

Bu çalışmada kurumsal faktörler tek değişken ile ölçülmüştür ve önemli bir etken olduğu görülmüştür. Daha gerçekçi ve uygulanabilir sonuçlara varabilmek için, kurum içi olgu ve kavramların daha derinlemesine ve ayrıntılı incelenmesinde yarar vardır. TKM'nin bünyesinde bulunan gerçek uygulama değişkeni, bu modeldeki anlamıyla güvenlik önlemlerinin uygulanması, ölçülmemiştir. Bu değişkenin anket yolu ile ölçülmesinde bazı ölçüm problemlerinin olabileceği varsayılmış ve uygulanmamıştır. Farklı bir araştırmada, kişilerin gerçek uygulamalarını teknik araçlar ile ölçüp, somut değerleri kullanmak daha uygun olacaktır.

Kurumsal faktörlerin daha derinleşmesinin yanısıra, risk algılamasında da ele alınabilecek başka değişkenler söz konusudur. Risk tolerans algılaması, kurum ve kişisel riskin ayrılması, takip edilebilirlik ve benzeri kavramlar da bu modele eklenebilir. Farklı sektör ve kurum büyüklüklerinin etkili olabileceği düşünülerek, uygun bir örnek kütlesi ile ölçüm yapmak temsili gücü daha yüksek bir modelin oluşmasını sağlayabilecektir.

## TEŞEKKÜR

Bu projede konu ile ilgili pek çok ayrıntıyı ve kapsamlı deneyimlerini bize sunarak daha gerçekçi bir çalışma yapılmasını sağlayan Erol Lengerli'ye çok teşekkür ederiz.

Ek : Değişkenler ve sorular

| | |
|---|---|
| Etki | Şirketim, bilişim sistemlerinde oluşabilecek hata ya da arızalardan oldukça etkilenir. |
| Olasılık | Şirketimi zarara uğratacak bilgisayar güvenlik problemlerinin olma ihtimali yüksektir. |
| Risk | Bilgisayar kullanarak yaptığım işler ile ilgili verilerin kaybolmayacağından eminim. |
| Bilinçlilik | Bilişim sistemlerini hatalı kullanmamın, ne tür risklere yol açabileceğini biliyorum. |
| | Bilgisayar güvenliği ile ilgili standartların ve kuralların neden gerekli olduğu konusunda bilgim var. |
| Algılanan Kolaylık | Bilgisayar güvenliğiyle ilgili kurallara uymak (şifreler, yedekleme, erişim kısıtlamaları) bana ekstra yük çıkartıyor. |
| | Güvenlik prosedürlerini uygulamak bazen beni çok yoruyor. |
| Algılanan Yarar | Bilgisayar sistemlerinde risk yönetiminin uygulanması işimi güvenli bir şekilde sürdürmeme yarar sağlar. |
| | Bilgisayar sistemlerinde risk yönetiminin uygulanması verilerimin bozulmasına engel olmaktadır. |
| | Kurumumuzdaki bilgisayar güvenlik standardı ve talimatlarına uymakta göstereceğim özen kendi yararımadır. |
| Tutum | Bilgisayar güvenliği ile ilgili belirli kurallar yerleştirilerek önlem alınmasına sıcak bakıyorum. |
| | Bilgisayar güvenliği risklerini azaltmak için önlem almanın iyi bir fikir olduğunu düşünüyorum. |
| Niyet | Bilgisayar güvenliği konusunda, önlem olarak bir takım kurallar ve standartlar getirildiğinde, böyle bir girişimin gereklerine uymaya niyetliyim. |
| | Şirketimde, bilişim sistemlerine ilişkin, güvenliği arttırma amaçlı denetim yapılmasını destekliyorum. |
| Kurum | Şirketimizde BT departmanı kullanıcıları bilgisayar güvenliği ile ilgili gelişmelerden bilgilendiriyor. |
| | Kurumumuzun iletişim kanalları açık olup bilgi akışı yoğundur. |
| | Bilgisayar güvenliği ihlali olabilecek durumların büyük bölümü sistemin içinde otomatik olarak engellendiği için bu kuralları çiğnemek pratikte mümkün değildir. |
| | Bilgisayar güvenliği kuralları, şirketin her yerinde tutarlı bir şekilde yürürlüktedir. |
| | Kurumumuzda belirli standartlar dahilinde formal bir yönetim yapısı vardır. |
| | Kurumumuzda bir işin sonuçlandırılması, prosedürlere uygun hareket edilmesinden önce gelir. |
| | Kurumumuz her türlü yeniliği teşvik eder. |
| | Kurumumuz yenilikleri uygulamayı çok sonra gündemine alır |
| | Kurumumuzda bilgisayar güvenliği önlemlerini uygulamaya karşı direnç göstermek cezalandırılır. |
| | Kurumumuzda bilgisayar güvenlik standardı ve talimatlarına düzenli bir şekilde uyanlar teşvik ve takdir edilir. |
| | Üstlerim sözleri ve yaptıklarıyla da güvenliğin şirketimiz için bir öncelik olduğunu gösterirler. |
| | Üst yönetim güvenlikle ilgili konularla ilgilidir. |
| | İş yerimde, bilişim sistemleri güvenliğiyle ilgili eğitim ve bilgilendirme olanakları mevcuttur |
| | Güvenlik önlemlerini uygulamada karşılaştığımız sorunlarla ilgili olarak bize destek veren bir birim mevcuttur. |

1: Kesinlikle Katılmıyorum - 2: Katılmıyorum - 3: Ne Katılıyorum Ne Katılmıyorum
4: Katılıyorum - 5: Kesinlikle Katılıyorum

## KAYNAKÇA


AJZEN, Icek, 1991, *"The Theory of Planned Behavior"*, ***Organizational Behavior and Human Decision Processes***, 50 (2), s:179-211.

AKÇAÖZ, H. , ÖZKAN, B., 2005, *"Determining Risk Sources and Strategies Among Farmers of Contrasting Risk Awareness: A Case Study For Çukurova Region of Turkey"*, ***Journal of Arid Environments***, 62 (4), s:661-675.

ATKINSON, William, 2005, *"Integrating Risk Management & Security"*, ***Risk Management***, 52 (10) s:32.

BAJAJ, A , NIDUMOLU, S.R., 1998, *"A Feedback Model To Understand Information System Usage"*, ***Information & Management***, 33 (4), s:213-224.

BRODERICK, Stuart., 2001, *"Information Security Risk Management - When Should It Be Managed?"*, ***Information Security Technical Report***, 6 (3), s:12-18.

JONES, A.B. , HUBONA, G.S., 2005, *"Individual Differences and Usage Behavior: Revisiting A Technology Acceptance Model Assumption"*, ***ACM SIGMIS Database***, 36 (2), s:58-77.

CAELLI, William J., 2002, *"Trusted ...or... Trustworthy: The Search For A New Paradigm For Computer and Network Security"*, ***Computers & Security***, 21 (5), s:413-420.

**Computer Security Institute**, CSI-Computer Crime and Security Survey, 2007.

COOPER, R. , ZMUD, R.W., 1990, *"Information Technology Implementation Research: A Technological Diffusion Approach"*, ***Management Science***, 36 (2), s:123-139.

COVIN, J.G. , SLEVIN, D.P. , HEELEY, M.B., 2001, *"Strategic Decision Making In An Intuitive Vs. Technocratic Mode: Structural and Environmental Considerations"*, ***Journal of Business Research***, 52 (1), s:51-67.

CUNNINGHAM, Scott M., 1967, **The Major Dimensions of Perceived Risk., Risk Taking and Information Handling In Consumer Behavior**, Boston, Harvard University Press.

DAVIS, Fred D., 1989, *"Perceived Usefulness, Perceived Ease Of Use, and User Acceptance of Information Technologies"*, ***MIS Quarterly***, 13 (3), s:319–340.

**Devlet İstatistik Kurumu**, Bilişim Teknolojileri Kullanımı Araştırması, Kasım 2007.

FEATHERMAN, M.S. , PAVLOU, P.A., 2003, *"Predicting E-Services Adoption: A Perceived Risk Facets Perspective"*, ***International Journal of Human-Computer Studies***, 59 (4), s:451-474.

FISHBEIN, M. , AJZEN, I. , 1975, **Belief, Attitude, Intention and Behavior: An Introduction To Theory and Research**, MA, Addison-Wesley Pub. Co.

GALLIVAN, Michael J. , 2001, *"Organizational Adoption and Assimilation of Complex*

*Technological Innovations: Development and Application of A New Framework"*, ***ACM SIGMIS Database***, 32 (3), s:51-85.

GERBER, M. , VON SOLMS, R. , 2005, "*Management of Risk In The Information Age"*, ***Computers & Security***, 24 (1), s:16-30.

HUANG, E. , CHUANG, M.H. , 2004, "*Extending The Theory of Planned Behaviour As A Model To Explain Post-Merger Employee Behaviour of Is Use"*, ***Computers In Human Behavior***, 23 (1), s:240-257.

**International Data Corporation**, Worldwide It Spending 2007–2011 Forecast Update: November 2007.

JAEGER, C.C., RENN, O., ROSA, E.A. , WEHLER,T., 2001, **Risk, Certainty, and Rational Action,** Londra, Earthscan.

JARVENPAA, S.L. , IVES, B. , 1991, "*Executive Involvement and Participation In The Management of It"*, ***MIS Quarterly***, 15 (2), s:205-227.

KANKANHALLI, A. , TEO, H. , TAN, B.C.Y. , WEI, K., 2003, "*An Integrative Study of Information Systems Security Effectiveness"*, ***International Journal of Information Management***, 23 (2), s:139-154.

KNAPP, K.J. , MARSHALL, T.E. , RAINER, R.K. Jr. , FORD, F.N. , 2005, "*Managerial Dimensions In Information Security- A Theoretical Model of Organizational Effectiveness"*, **A Research Report Prepared For The (Isc)2 Constituency**.

KOSKOSAS, I.V. , PAUL, R.J. , 2004, "*The Interrelationship and Effect of Culture and Risk Communication In Setting Internet Banking Security Goals"*, Icec'04, **Sixth International Conference On Electronic Commerce.**

KUTSCH, E. , HALL, M., 2005, "*Intervening Conditions On The Management of Project Risk: Dealing With Uncertainty In Information Technology Projects"*, ***International Journal of Project Management***, 23 (8), s:591-599

KWAK, Y.H. , LAPLACE, K.S. , 2005, "*Examining Risk Tolerance In Project-Driven Organization"*, ***Technovation***, 25 (6), s:691-695.

LUFTMAN, J. , MCLEAN, E.R., 2004, "*Key Issues For It Executives"*, ***MIS Quarterly Executive***, 3 (2), s:89-104.

PABLO, Amy L., 1997, "*Reconciling Predictions of Decision Making Under Risk"*, ***Journal of Managerial Psychology,*** 12 (1), s:4–20.

SCHLIENGER, T. , TEUFEL, S., 2003, "*Analyzing Information Security Culture: Increased Trust By An Appropriate Information Security Culture"*, ***Proceedings of The 14th International Workshop On Database and Expert Systems Applications***.

SIEGRIST, Michael, 2000, "*The Influence of Trust and Perceptions of Risks and Benefits On The Acceptance of Gene Technology"*, ***Risk Analysis***, 20 (2), s:195-204.

STEWART, Andrew, 2004, "*On Risk: Perception and Direction"*, ***Computers & Security***, 23 (5), s:362-370.

TENEYUCA, David, 2001, "*Organizational Leader's Use of Risk*

*Management For Information Technology"*, ***Information Security Technical Report***, 6 (3), s:54-59.

VAN DER HEIJDEN, H., VERHAGEN, T. , CREEMERS, M. , 2003, *"Understanding Online Purchase Intentions- Contributions From Technology and Trust Perspectives"*, ***European Journal of Information Systems***, 12 (1), s:41-48.

VENKATESH, V. , DAVIS, F. D., 2000, *"A Theoretical Extension of The Technology Acceptance Model: Four Longitudinal Field Studies"*, ***Management Science***, 46 (2), s:186-204.

VENKATESH, V. , MORRIS, M.G. , DAVIS, G.B. , DAVIS, F.D., 2003, *"User Acceptance of Information Technology: Toward A Unified View"*, ***MIS Quarterly***, 27 (3), s:425-478.

VIJAYASARATHY, Leo R., 2004, *"Predicting Consumer İntentions To Use On-Line Shopping: The Case For An Augmented Technology Acceptance Model"*, ***Information & Management***, 41 (6), s:747-762.

VON NEUMANN, J. , MORGENSTERN, O., 1953, **Theory of Games and Economic Behavior**, Abd, Princeton University Press, 3rd Ed.

VON SOLMS, Basie, 2005, *"Information Security Governance: Cobit Or Iso 17799 Or Both?"*, ***Computers & Security***, 24 (2), s:99-104.

WARD, P. , SMITH, C.L, 2002, *"The Development of Access Control Policies For Information Technology Systems"*, ***Computers & Security***, 21 (4), s:356-371.

WEBER, Elke U., 2001, *"Personality and Risk Taking"*, ***International Encyclopedia of The Social & Behavioral Sciences***, İngiltere, Elsevier Science Limited, s:11274-11276.

WILEMON, D.L., CICERO, J.P., 1970, *"The Project Manager—Anomalies and Ambiguities"*, ***The Academy of Management Journal***, 13 (3), s:269–282.