T. C.

ULUDAĞ ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

İŞLETME ANABİLİM DALI

YÖNETİM VE ORGANİZASYON BİLİM DALI

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

YÜKSEK LİSANS

Halil ERBİ

BURSA - 2018

T. C.

ULUDAĞ ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

İŞLETME ANABİLİM DALI

YÖNETİM VE ORGANİZASYON BİLİM DALI

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

YÜKSEK LİSANS

Halil ERBİ

Danışman:
Doç. Dr. Kurtuluş KAYMAZ

BURSA - 2018

T. C.
ULUDAĞ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ MÜDÜRLÜĞÜNE

İşletme Anabilim, Yönetim ve Organizasyon Bilim Dalı'nda 701520037 numaralı Halil Erbi 'nin hazırladığı "Bilgi Güvenliği Stres Faktörlerinin İş Tatmini Üzerindeki Etkileri: Ar-Ge Merkezi Olan İşletmeler Üzerinde Bir Araştırma" konulu Yüksek Lisans Çalışması ile ilgili tez savunma sınavı, 28 /08 / 2018 günü 09:00 – 10:30 saatleri arasında yapılmış, sorulan sorulara alınan cevaplar sonunda adayın tezinin/çalışmasının (başarılı) olduğuna (oybirliği) ile karar verilmiştir.

.....

Üye
(Tez Danışmanı ve Sınav Komisyonu Başkanı)
Doç. Dr. Kurtuluş KAYMAZ
Uludağ Üniversitesi

Üye
Akademik Unvanı, Adı Soyadı
Doç.Dr. Çağatan TAŞKIN
Uludağ Üniversitesi

Üye
Akademik Unvanı, Adı Soyadı
Dr. Öğretim Üyesi Umut EROĞLU
Çanakkale 18 Mart Üniversitesi

Yedek Üye
Akademik Unvanı, Adı Soyadı

Yedek Üye
Akademik Unvanı, Adı Soyadı

28 / 08 / 2018

SOSYAL BİLİMLER ENSTİTÜSÜ
YÜKSEK LİSANS/DOKTORA İNTİHAL YAZILIM RAPORU

ULUDAĞ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
.....İŞLETME..... ANABİLİM DALI BAŞKANLIĞI'NA

Tarih: 7./8./2018

Tez Başlığı / Konusu: Örgütlerde Bilgi Güvenliği Davranışının İş Tatmini Üzerindeki Etkileri: Ar-Ge Merkezi olan İşletmeler Üzerine Bir Araştırma

Yukarıda başlığı gösterilen tez çalışmamın a) Kapak sayfası, b) Giriş, c) Ana bölümler ve d) Sonuç kısımlarından oluşan toplam ..... sayfalık kısmına ilişkin, 7../8.../2018 tarihinde şahsım tarafından Turnitin..... adlı intihal tespit programından (Turnitin)* aşağıda belirtilen filtrelemeler uygulanarak alınmış olan özgünlük raporuna göre tezimin benzerlik oranı %10 'tür.

Uygulanan filtrelemeler:

1- Kaynakça hariç
2- Alıntılar hariç/dahil
3- 5 kelimeden daha az örtüşme içeren metin kısımları hariç

Uludağ Üniversitesi Sosyal Bilimler Enstitüsü Tez Çalışması Özgünlük Raporu Alınması ve Kullanılması Uygulama Esasları'nı inceledim ve bu Uygulama Esasları'nda belirtilen azami benzerlik oranlarına göre tez çalışmamın herhangi bir intihal içermediğini; aksinin tespit edileceği muhtemel durumda doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi ve yukarıda vermiş olduğum bilgilerin doğru olduğunu beyan ederim.

Gereğini saygılarımla arz ederim.

Tarih ve İmza
7-8-2018

Adı Soyadı: Halil Erbil
Öğrenci No: 701520037
Anabilim Dalı: İşletme
Programı: Yüksek Lisans – Tezden Organizasyon
Statüsü: ☑ Y.Lisans ☐ Doktora

Danışman (Adı, Soyad, Tarih) Doç. Dr. Kurtuluş KAYMAZ

*** Turnitin programına Uludağ Üniversitesi Kütüphane web sayfasından ulaşılabilir.**

T. C.
ULUDAĞ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ MÜDÜRLÜĞÜNE

Yemin Metni

Yüksek Lisans tezi olarak sunduğum "Bilgi Güvenliği Stres Faktörlerinin İş Tatmini Üzerindeki Etkileri: Ar-Ge Merkezi Olan İşletmeler Üzerinde Bir Araştırma" başlıklı çalışmanın bilimsel araştırma, yazma ve etik kurallarına uygun olarak tarafımdan yazıldığına ve tezde yapılan bütün alıntıların kaynaklarının usulüne uygun olarak gösterildiğine, tezimde intihal ürünü cümle veya paragraflar bulunmadığına şerefim üzerine yemin ederim.

Tarih ve İmza
28-08-2018

Adı Soyadı	**: Halil Erbi**
Öğrenci No	**: 701520037**
Ana Bilim Dalı	**: İşletme**
Programı	**: Yönetim ve Organizasyon**
Statüsü	**: Yüksek Lisans**

ÖZET

Yazar Adı ve Soyadı	: Halil Erbi
Üniversite	: Uludağ Üniversitesi
Enstitü	: Sosyal Bilimler Enstitüsü
Anabilim Dalı	: İşletme
Bilim Dalı	: Yönetim ve Organizasyon
Tezin Niteliği	: Yüksek Lisans Tezi
Sayfa Sayısı	: xi + 101
Mezuniyat Tarihi	: …../ … / 2018
Danışmanları	: Doç Dr. Kurtuluş KAYMAZ

Bilgi Güvenliği Stres Faktörlerinin İş Tamini Üzerindeki Etkileri :

Ar-Ge Merkezi Olan İşletmeler Üzerine Bir Araştırma

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

Anahtar kelimeler:

Bilgi güvenliği, iş engeli, gizlilik ihlali, bilgi güvenliğinde stres, iş tatmini

ABSTRACT

Name and Surname	: Halil Erbi
University	: Uludag University
Institution	: Social Science Institution
Field	: Business
Branch	: Management and Organization
Degree Awarded	: Master
Page Number	: xi + 101
Degree Date	: …/ …./ 2018
Supervisor (s)	: Doç Dr. Kurtuluş KAYMAZ

The Effects of Information Security Stressors on the Job Satisfaction : A Research on R&D Structured Organizations

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

Keywords:
Information security, work impediment, invasion of privacy, information security stress, job satisfaction.

İÇİNDEKİLER

II. BÖLÜM
BİLGİ GÜVENLİĞİ UYGULAMALARININ BİREY DÜZEYİNDEKİ YANSIMALARI

III. BÖLÜM

BİLGİ GÜVENLİĞİ UYGULAMALARININ BİREY DÜZEYİNDEKİ YANSIMALARI ÜZERİNE BİR ARAŞTIRMA

TABLOLAR LİSTESİ

ŞEKİLLER LİSTESİ

KISALTMALAR LİSTESİ

Ar-Ge:	Araştırma Geliştirme
BGS:	Bilgi Güvenliği Stresi
BGYS:	Bilgi Güvenliği Yönetimi Sistemi
BSI:	British Standards Institute (İngiliz Standartlar Enstitüsü)
HRIS:	Human Resources Information Systems (İnsan Kaynakları Bilgi Sistemleri)
ISO:	International Organization for Standardization (Uluslararası Standartlar Teşkilatı)
İE:	İş Engeli
İT:	İş Tatmini
Gİ:	Gizlilik İhlali
TC:	Türkiye Cumhuriyeti
TBP:	Planlı Davranış Teorisi (Theory of Planned Behavior)
PDT:	Planlı Davranış Teorisi
TRA:	Sebepli Davranışlar Teorisi' (Theory of Reasoned Action)
KVKK:	Kişisel Verilerin Korunması Kanun

GİRİŞ

Şirketlerin en önemli varlıklarının bilgi olduğu 21. yüzyıl dünyasında, bilginin korunması ve güvenliği de şirketlerin üzerinde önemle durması gereken konuların başında gelmektedir. Bilgi güvenliği, en önemli varlık olan bilginin yalnızca yetkili kimseler tarafından erişebilmesinin garanti edilmesi, bilginin değişmeden ve bütünlüğünü kaybetmeden varlığını sürdürmesi ve bilgiye istenilen her an ulaşılabilmesi anlamındadır. Bilgi güvenliği, şirketlerin iş hayatındaki sürekliliğini sağlamak ve başarısını sürdürmek için kilit rol üstlenmektedir.

Günümüzün çetin rekabet koşullarında şirketlerin ister mal ister hizmet, ne üretirse üretsin, müşterileri, tedarikçileri ve hissedarları ile ilişkileri bilgi birikimleri ile doğrudan ilintilidir. Bilgi varlıklarını artıran ve bu bilgi varlığını koruyabilen kuruluşlar, marka değerlerine değer katabilmektedir. Rekabet edebilme yeteneğini sürdürülebilir kılabilmek için gereken şey bilgi güvenliğine azami ölçüde değer vererek, bunları koruyabilmektir. Özellikle her şeyin dijitalleştiği günümüzde, bilginin dijital ortamlarda üretilmesi ve saklanması, bilgi güvenliğini tehlikeye atabilmektedir. Gelişen internet teknolojileri, iş dünyasını rahatlattığı gibi, bilgi güvenliğini de tehlikeye atmaktadır. Bu nedenle bilginin üretilmesi kadar saklanması, muhafaza edilmesi, yetkisiz ellere geçmesinin önlenmesi, değiştirilmeden varlığını sürdürmesi ve bütünlüğünün korunması şirketlerin birincil önceliği haline gelmiştir.

Bilgi güvenliği uygulamaları, kurumların bilgi varlıklarını koruyabilmek ve kurumun varlığını sürdürebilmek açısından bir zorunluluktur. Kurumların bilgi varlığını koruyabilmesi ise çalışanlarının bilgi güvenliği konusunda bilinçlenmesi ile mümkündür. Bilgi güvenliği uygulamaları, çoğu zaman kısıtlamaları da beraberinde getirdiğinden çalışanların iş tatminlerini etkileyebilmektedir. Bir çalışanın bilmesi gerektiğini düşündüğü bilgiye, bilgi güvenliği kısıtlamaları nedeniyle ulaşamaması, kendisini değersiz hissetmesine neden olabilmekte ve bu da iş tatminlerini etkileyebilmektedir. Çünkü bilgi güvenliği uygulamalarının kısıtları ve iş tatmini, çoğu zaman çatışma halindedir.

Bu çalışma, genel itibariyle Ar&Ge merkezli örgütlerdeki bilgi güvenliği uygulamalarından kaynaklanan bilgi güvenliği davranışlarının, çalışanların iş tatmini üzerindeki etkisini ortaya koyabilmek amacıyla gerçekleştirilecektir. Çalışma üç bölümden oluşacaktır. Çalışmanın birinci bölümünde bilgi yönetimi, bilgi güvenliği yönetim sistemi ve siber güvenlik konularına yer verilecektir. Bu kapsamda öncelikle bilgi ve bilgi yönetimi kavramlarına ve önemine değinilecektir. Bilgi yönetimi sisteminin tarihsel gelişimine ye verilmesinin ardından bilgi yönetimi süreçlerinden bahsedilecektir. Ardından bilgi güvenliği yönetim sistemi, bilgi güvenliği uygulamalarına olan ihtiyacın temel nedenleri, bilgi güvenliği sisteminin yapılandırılması ve bilgi güvenliğine ilişkin standartlara yönelik bilgiler verilecektir. Birinci bölümün son kısmı ise siber güvenlik, siber savaş ve siber suç gibi kavramlara ayrılacaktır.

Çalışmanın ikinci bölümünde bilgi güvenliği uygulamalarının birey düzeyindeki yansımalarına yer verilecektir. Bu kapsamda öncelikle teknoloji ve insanın birlikte yönetimine değinilecek, ardından bilgi güvenliği uygulamalarında bireyin rolü anlatılacaktır. Sonrasında ise bilgi teknolojileri ve insan kaynakları uygulamaları arasındaki ilişkiye yer verilecektir. Devamında bilgi güvenliği uygulamalarında çalışanlara yönelik risk alanlarına yer verilecek ve bilgi güvenliğini riske atan çalışan temelli faktörlere ait bilgiler verilecektir. Akabinde bilgi güvenliğinde kuramsal yaklaşımlara yer verilecektir. Son olarak bilgi güvenliğinde stres faktörleri ve stres – iş tatmini ilişkisine yönelik bilgi verilecektir.

Çalışmanın üçüncü ve son bölümünde ise bilgi güvenliği uygulamalarının çalışanların iş tatmine etkisine yönelik gerçekleştirilen araştırmanın bulgularına yer verilecektir.

I. BÖLÜM
BİLGİ YÖNETİMİ, BİLGİ GÜVENLİĞİ VE BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ

1. BİLGİ, BİLGİ YÖNETİMİ KAVRAMLARI ve ÖNEMİ

Bu kısımda genel hatları ile bilgi, bilgi yönetimi kavramları ve önemi değerlendirilecektir.

1.1. Bilgi ve Bilgi Yönetimi Kavramı

Bilgi kelime ve anlam açısından çok eskilere giden bir tartışma konusu olagelmiştir. Günümüzde ise hemen her disiplinin bilgi kavramı ile bağlantısı bulunmaktadır. Bu açıdan bilgi kavramsal olarak günlük yaşamda sıklıkla başvurulan ve kullanılan bir kaynak olmasının yanı sıra bilimin de temelini oluşturmaktadır. İnsanlık evriminin temellerinden biri kabul edilen bilgi, ilk olarak felsefecilerin tartışmalarına konu edilmiş, sonrasında çeşitli alet, süreç ve ürünlere uygulanmıştır. (Güçlü, 2006: 352) Bilgi, veri ve enformasyon kavramları ile de yakından ilişkili olduğu için ilk olarak içerik ve işlevsel olarak farklılıkları bulunan bu kavramların tanımlanması gerekmektedir.

En yakın hali ile veri bilginin kaynağı ve işlenmemiş hali, nesnel gerçekler, bilginin en küçük parçası, enformasyon yapı taşı, bilgi elde edilmesinde ana unsur ve yorumlanmamış bilgi gibi açıklamalar ile tanımlanmaktadır. (Atlı, 2014: 632) Olaylar konusunda birbirinden bağımsız nesnel gerçekler olan veriler işlenmemiş durumdadır. (Özdemir, 2008: 61)

Enformasyon ise Latince biçim verme eylemi anlamına gelmektedir. Genel olarak verilerin anlamlı hale getirilmesi ve işlem görmüş hali olarak açıklanan enformasyon verilere anlam kazandırılmasıdır. (Atlı, 2014: 632) Enformasyon genel olarak belge, görsel veya işitsel mesaj olarak algılanmaktadır. Burada temel amaç, alıcının düşüncelerini etkilemektir ve alıcı olan kişi, ilgili gönderiyi şekillendirmek mecburiyetindedir. Perspektifinde, düşüncesine yada kavrayışında farklılık ortaya koymalıdır. (Durna, 2008: 133)

Mevcut bilgi düşüncesindeki önemli sorunlardan biri "veri" ve "bilgi" kavramlarının genellikle birbirinin yerine kullanılmaları ya da birbirlerine göre tanımlanmalarıdır. Buna göre geçmişte ilk olarak veri olarak adlandırılan olgu günümüzde bilgi olarak adlandırılmaktadır. (Sundregen ve Stenesko, 2003: 11)

Örgütsel anlamda her toplum bir bilgi topluluğudur ve her organizasyon bir bilgi organizasyonudur. Bu nedenle, bilgi, materyal, para ve personel gibi temel bir kaynak durumundadır. (Adeyeke, 1997: 318) Organizasyonlar açısından bilgi müşteriler, ürünler, süreç, hata ve başarılar konusundaki enformasyon olarak tanımlanmaktadır. (Atılgan, 2009: 202)

Geleneksel olarak üç temel bilgi dünyasının olduğu kabul edilmektedir. Buna göre birincisi, bilgilerin kayda geçirildiği kütüphanelerin ve arşivlerin dünyası iken ikincisi, bilginin toplandığı ve organize edildiği, bilgi merkezleri ve kayıt merkezleridir. Üçüncü bilgi dünyası ise bilgilerin sayısal veya yapılandırılmış olduğu bilgisayarlar, telekomünikasyon ve otomatik bilgi sistemleri veri dünyasıdır. (Adeyeke, 1997: 319)

Buckland' a göre bilgi soyut ve somut olmasına ya da varlık ve süreç olmasına göre farklı sınıflandırma içerisinde değerlendirmektedir. Buna göre bilgi mevcudiyet gibi düşünüldüğünde "bilgi olarak bilgi" soyut olur, "nesne olarak bilgi" ise somutlaşır. Süreç olarak kabul edildiğinde, süreç olarak bilgi soyut, nesneyi (objeyi) işleyerek farklı formasyonda olarak bilgi oluşturma (bilgiyi işleme) ise somut hale geitirmedir. Bu noktada somut olan nesne olan bilgi, bilgi yönetiminin konusu içerisinde girmektedir. (Tonta, 2004: 3)

Tablo 1: Bilgiye 4 Farklı Bakış Açısı

	Soyut	Somut
Varlık	Bilgi olarak bilgi	Nesne olarak bilgi
	Bilgi (knowledge)	Veri, belge, kayıtlı bilgi
Süreç	Süreç olarak bilgi	Bilgi işleme, veri işleme, belge işleme, bilgi mühendisliği
	Bilgilenme	

Kaynak:(Buckland, 1991a: 6'dan aktaran Tonta, 2004: 2)

Bilgi açık bilgi ve örtük bilgi olarak ikili bir sınırlandırmaya da tabi tutulmaktadır. Buna göre kodlanan, kaydedilebilen ve dijital olarak aktarılabilen bilgi açık bilgi olarak adlandırılırken kişinin şahsi kabiliyet , mahareti ve ustalığı ile olan bilgiler , yazılı olarak tutulamayacağı ve aktarılamayacağı için bu oluşan bilgi örtük bilgi olarak nitelendirilmektedir. (Özgür, 2012: 194)

İletişim teknolojilerindeki gelişmeler sonrasında bilgi, iktisadi bir değer olarak da kabul edilmeye başlamış ve bilgi ekonomisi ortaya çıkmıştır. Dolayısıyla yeni oluşan kavramlarla beraber yeni iş biçimleri, yeni iş, yeni uğraş alanları ve iş tanımlamaları meydana gelmiştir. (Atılgan, 2009: 203)

Bilgi yönetiminin içeriği ve kapsamı, çeşitli alanlardan (işletme ve yönetim, organizasyon araştırması, bilgi sistemleri, bilgi ve iletişim teknolojisi, kamu yönetimi, iletişim vb.) araştırmacılar ve uygulayıcılar tarafından yakından incelenmektedir. Genel olarak kavram bir organizasyonun planladığı, organize ettiği, topladığı, kontrol ettiği, yaydığı, elden geçirdiği bilgileri, verimlilik için en üst düzeye çıkarmak istediği araç biçiminde tanımlanmaktadır.

İlk bakışta yönetim ve bilgi , ikisi birlikte kullanılması zorlu ve güçlü iki olgu olarak gibi belirlense de bilginin rekabet üstünlüğü sağlamada daha önemli hale gelmesi sayesinde kurumsal kaynak olarak görülmesini zorunlu hale getirmiş ve konuya daha sistemli yaklaşılması gerekliliği ortaya çıkmıştır. (Özdemirci ve Aydın,2008: 59)

Tonta' ya göre bilgi yönetimi "Her türlü örgütün etkin olarak işletilmesiyle ilgili bilginin sağlanması, düzenlenmesi, denetimi, yayımı ve kullanımına yönetim ilkelerinin uygulanması" (Tonta,2004: 3) olarak tanımlanmıştır.

Bilgi yönetimi organizasyon amaçlarını gerçekleştirmek için kurumsal kaynakların yönetimidir ve bu kaynakların yönetimi ilgili teknolojiler, sistemler, kaynaklar, hizmetler, finansman ve personel yönetimini de içermektedir. (Davies ve Titterington, 1991: 209) Uzun ve Durna ise kavramı, "işletmelerin en iyi kararları alarak rekabet üstünlüğü yaratmaları için bilginin sistematik ve planlı bir şekilde oluşturulması, sürekli olarak yenilenmesi, depolanması, paylaşılması ve kullanılması" (Uzun ve Durna, 2008: 35) şeklinde tanımlamıştır.

Daha geniş kapsamlı bir açıklama ile bilgi yönetimi kişi ve kurumların sahip oldukları her türlü bilgiye yeni anlamlar ekleme ve yeniden yorumlayarak yeni bilgi

üretme, bunları çoğaltma, kullanma, paylaşma ve koruma aşamalarından oluşan bütünsel bir çerçevedir. (Odabaş, 2008: 2)

Bilgi yönetimine bir organizasyondaki entelektüel varlıkların yönetilmesi açısından yaklaşan tanımlar da bulunmaktadır ve buna göre bilgi yönetimi, insanı merkeze alarak mevcut varlıkların yönetilebilmesi için geliştirilen stratejiler ve politikalarla ilgili her çeşit faaliyetlerdir." (Zaim, 2010: 54) 1990'lı yıllardan bu yana bazı bilgi yönetimi tanımları ise aşağıdaki tabloda gösterilmiştir:

Tablo 2: Bilgi Yönetimi Tanımları

Kaynak	**Tanımlar**
Patrash (1996)	Bilgi yönetimi en iyi kararın verilebilmesi için doğru zamanda, doğru kaynaktan doğru bilginin toplanmasıdır.
Wiig (1997)	Bilgi yönetimi, örgütlerin sahip oldukları beceri ve yetenekler ile tecrübeleri yoluyla elde ettikleri ortak akıl ve bilgileri tanımlamak ve işlemektir.
O'Dell (1997)	Bilgi yönetimi, değer yaratmak için bilginin kullanılması, anlaşılması ve bulunması için sistematik yaklaşımların uygulamadır.
Bassi (1997)	Bilgi yönetimi, örgütsel performansı geliştirmek için bilginin yaratılması, ele geçirilmesi ve kullanılmasını içeren süreçtir.
Brooking (1997)	Bilgi yönetimi; insan merkezli değerlerin yönetilmesi için gerekli taktikler ve stratejiler ile ilişkili eylemlerdir.
Beijerse (1999)	Bilgi yönetimi; stratejik bir motivasyonla çalışanların gelişimini kolaylaştırmak, bilgi ve verilerin yorumlanmasında çalışanların yeteneklerini kullanarak örgütsel hedeflerin başarılmasıdır.
Bailey ve Clarke (2000)	Bilgi yönetimi; yöneticilerin örgütsel ve bireysel faydaları ortaya çıkarmak için bilgiyi elde etmesi, iletmesi ve kullanılmasını sağlamasıdır.
Smith (2002)	Bilgi yönetimi; modern dünyanın hızla artan belirsizlik ve karmaşıklığı karşısında, firmaların yaşamını ve performansını artırmaya çalışmasıdır.

Barutçugil (2002)	Bilgi yönetimi bilgiyi örgütsel performansı arttırmak amacıyla yaratma, ele geçirme, paylaşma ve kullanma sürecidir.
Darroch ve Naughton (2003	Bilgi yönetimi örgüt içinde bilginin yaygınlaştırılması ve kullanılmasını yöneten ve bilgiyi oluşturan ya da yerleştiren süreçlerdir.
Özdemirci ve Aydın(2008)	Bilgi yönetimi, bilginin üretilmesini, yayılımını, derlenmesini, düzenlenmesini, depolanmasını, erişilmesini, yorumlanmasını ve kullanılmasını kapsar.

Kaynak: N. Demircan Çakar ve Sibel Yıldız, "Bilgi Yönetimi ve Örgütsel Etkinlik İlişkisi: Örgüt Kültürü ve Örgüt Yapısının Temel Etkileri", *Ege Akademik Bakış Dergisi*, 10(1): 71-93.

Bilgi yönetimi nesnel bilgilerin yönetimi ile ilgili bir kavram olarak kapsamlı bir uygulama alanına sahiptir. Hangi ortamdan elde edilirse edilsin nesnel bilginin seçilmesi, elde edilmesi, düzenlenebilmesi, kullanılabilmesi, korunabilmesi, ayıklanabilmesi, imha edilmesi; özetle bilginin yönetimini oluşturarak kapsamaktadır. (Zaim, 2010: 54)

Bazı çalışmalarda bilgi-yönetimi, bilgi sistemleri, bilgi teknolojisi, veri yönetimi, sistem mühendisliği ve benzeri kavramlarla eşanlamlı kullanılsa da bilgi yönetimi bunların ötesinde bir kavramdır. (Dias, 2001: 271) Tanımların genelinde görülebileceği gibi bilgi yönetimi ile ilgili yaklaşımlarda bilginin niteliğine vurgu yapılarak; kısacası kitle olarak biriken enformasyona dayana bilgilerin mantık çerçevesinde organize edilmesi, doğru vakitte ve doğru insanların bundan yararlanması ön plana çıkarılmaktadır. (Zaim, 2010: 54)

1.2. Bilgi Yönetimi Sisteminin Tarihsel Gelişimi ve Önemi

19. yüzyılın sonundan bu yana, bilgi yönetimi bazı kavramsal ve pratik değişiklikler geçirmiştir. Buna göre bilgi çok hızlı bir şekilde gelişmiş ve teknoloji yardımı ile bilginin işlenmesi, farklı dönemlerde farklı bilgi yönetimi uygulamalarını ortaya çıkarmıştır.

1920'lerde ve 1930'larda, bilgi yönetimine daha organize ve geniş bir perspektifle odaklanan kayıt yönetimi önem kazanmıştır. (Dias, 2001: 270)

Bilgisayar güvenliği veya donanımın fiziksel konumunu dış tehditlerden korumaya duyulan ihtiyaç ilk ana bilgisayarlar geliştirildikten hemen sonra başlamıştır. (Singh, vd, 2014: 1072)

Gerçekte globalleşmenin bilgiye dayalı toplumları meydana getirmesi bilişim teknolojilerinin yıllar boyunca oluşturduğu gelişim ile de doğru orantılıdır. Bilişim teknolojilerinin gelişmeye başladığı 1960'lı yıllarda, sanayi devrimi sonrası meydana gelen alışmışlıkları ve iş yapma proseslerini esaslı bir şekilde değişikliğe uğratmıştır. Bu prosesin devamında kullanılan bilgi toplumu kavramı, oluşan bilgi teknolojilerinin yolunu açtığı iktisadi ve sosyal değişimler olarak da nitelendirilebilir. (Kök, 2006: 124)

1970'lerde, bilgi yönetimi, bir işletmedeki gerekli tüm bilgileri yönetmek için yeni bir strateji olan bilgi kaynakları yönetimi olarak isimlendirilmeye başlanmıştır. (Dias, 2001: 269)

Günümüzde internet milyonlarca güvenli olmayan bilgisayar ağını birbirleriyle iletişim haline getirmiştir. Bu bağlamda her bir bilgisayarın depolanan bilgilerini güvence altına alma, bağlandığı her bilgisayardaki güvenliği de etkilemektedir. İnternet üzerinden yürütülen elektronik veri işleme ve elektronik ticaretin hızla büyümesi ve yaygın kullanımı, sayısız uluslararası terörizm olaylarıyla birlikte, bilgisayarların korunması ve depolandığı, işlenmesi ve iletilmesi ile ilgili daha iyi yöntemlere olan gereksinimi artırmıştır. (Singh, vd, 2014: 1073)

Bilgi yönetiminin önemi öncelikli olarak, bilginin bir kaynak olmasından ileri gelmektedir. Eaton ve Bawden bilginin diğer kaynaklar gibi (yani işgücü, sermaye, toprak ve ekipman gibi) yönetilmesi gereken bir kaynak olduğunu ileri sürmektedir. Bu planlama, maliyetlendirme, bütçeleme ve değerlendirme gibi şirketin bilgi kaynaklarına kaynak yönetim teknikleri uygulamak ve bilgi kaynakları yönetimi sorumlulukları için pozisyonu kuruluş içindeki daha üst düzeylere atamak anlamına gelmektedir. Eaton & Bawden aşağıdaki üç koşulun yerine getirildiğinde bilginin yalnızca bir kaynak olarak yönetilebileceğini göstermektedir: (Maritz, 2003: 76)

- Organizasyonun bir amacına katkıda bulunmak için bilginin üretilmesi,
- Bilgilerin belirtilen amaçla yerine getirilmesi arasındaki ilişki açıkça gösterilebilir. ·
- İlişki deneysel olarak test edilebilir

Yönetim bilimi açısından bilgi ve teknoloji yüzyılımızın en önemli iki kavramı kabul edilmektedir. Bu açıdan bilgi yeni bir üretim faktörü olarak değerlendirilirken, teknoloji de bilginin vazgeçilmez bir parçası haline gelmiştir. Dolayısıyla bilgi çağını yaşadığımız bilgi toplumunda, bilgi yönetimi kurumsal yönetiminin önemli bir unsuru haline gelmiştir. (Özgür, 2012: 203) Ulusların bilgi yönetimindeki başarıları da bilgi teknolojilerine yaklaşımları ve yatırım payı ile doğrudan ilişkilidir. Bu nedenle ar-ge ye yapılan yatırımlar ile birlikte toplam bütçe harcamalarından bilişim ve iletişim teknolojilerine için bütçeden verilen kısımla ile bilgi yönetiminden elde edilecek başarı doğru orantılıdır. (Atılgan, 2009: 208)

Bilgi yönetiminin temel işlevi, farklı düzeylerde üretilen, yayılan ve gittikçe daha fazla kişiye yayılan bilginin örgütler için bir varlık haline dönüştürülmesinde ortaya çıkmaktadır. Daha net ifade edecek olursak bilgi yönetiminin görevi, hem örgüt içerisinde hem de örgüt çevresinde oluşan her çeşit bilgi faaliyeti için zorunlu stratejilerin meydana getirilmesi ve var olan alt- üst yapıyı bunlara göre temin etmektir. Kısacası kurumun oluşturduğu örtük bilgi, açık bilgi, dış bilgi ve iç bilgilerle ve bu bilgilerle ilişkili işlemler bilgi yönetiminin kurum için önemini meydana getirmektedir. (Sağsan, 2002: 217)

Tüm bunların ötesinde bilgi yönetimi, örgütlerin konumlarını iyileştirmek veya geliştirmek için uyguladığı stratejiler dizisinden biridir. Bu stratejiler, organizasyon el veya kurumsal strateji, pazarlama stratejisi ve operasyon yönetimi stratejisini içerir. Bilgi stratejisinin doğasını ve amacını en iyi şekilde anlamak için, bunu, desteklemesi gereken organizasyon stratejisi bağlamında değerlendirmek gerekmektedir. (Chaffey ve Wood, 2005: 180)

Bilgi yönetimi stratejisi örgütsel stratejilerin ve süreçlerin desteklenmesi için organizasyonel bilgi kaynaklarının kontrol edilmesi ve koordinasyonuyla insan kaynakları ve teknoloji kaynakları ile uygulanmasını içermektedir. Bu tanım, bilgi yönetimi stratejisinin bir organizasyonun bilgi varlıklarını, insan kaynakları ve teknoloji kaynakları yönetmek suretiyle yapılandırılması ve kontrol edilmesi gereken bir kaynak olarak ele aldığını göstermektedir. (Chaffey ve Wood, 2005: 180)

Bilgi günümüzde ülkelerin, kurumların ve insanların esas rekabet edecekleri bir platform durumuna gelmiştir. Bilgiye dayalı ekonomilerde, çalışan talebini de global düzeye çıkararak değiştirmektedir. Fiziksel güç ve fiziksel yeteneğin yerine bilgi içeren

faaliyetlerin ve bilgiyi kullanarak, ham maddelerden farklı biçimde yaralanma ve değiştirilmesi ayrıca ucuz emek gücü yerini ise bilişim teknolojilerini içeren uygulamalar, özellikle de buna uygun olarak nitelikli insan gücü kaynağı almaktadır. Bilgiye dayalı ekonomilerde, rekabet avantajı yenilikçiliğe dayanan bilgi yaratma ve örgüt yapılarına uyumlu, yenilikçi, geliştirici yetenekleriyle donatılmış insan gücü yaratılmasına bağlıdır. İşgücü sahasında en yüksek büyümenin ekonomi temelli iş kollarında yaşanması da bunu kanıtlamaktadır. Bu kapsamda işletmelerin her departmanında bilgi sistemi stratejisi önemi ortaya çıkmış ve daha sıklıkla başvurulan bir süreç olmuştur.

Bilgi sistemi bilgi ve veriyi depolamak, yaymak, biriktirmek ve idare etmek için birbiri ile ilişkili elemanlar dizisi olarak tanımlanmaktadır. (Stair ve Raynolds, 2008: 4) Bir başka tanımlamaya göre bilgi sistemi, "işletme içindeki her türlü veri, bilgi ve üst bilgi faktörlerini bir araya getiren, stratejik düzeyden operasyon el düzeye kadar, farklı işletme fonksiyonlarını içerecek şekilde oluşmuş, bilgiye dayalı bir sistemler bütünü" (İlter, 2007: 4) olarak tanımlanmaktadır. Demirhan da kavramı ham bilginin, kullanıcıların gereksinimine uygun ve yararlı duruma getirilmesi amacıyla hazırlanması, işlenmesi ve iletişimi şeklinde ifade etmektedir. (Demirhan, 2002: 118) Kısacası bilgi işleme, veri işleme ve karar destek sistemleri için tasarlanan bilgisayar destekli sistemlere bilgi sistemi adı verilmektedir.

Son yıllarda gelişmiş yönetim bilişim teknolojilerinin geliştirilmesinde özellikle üç alanda oluşan gelişmelerin çok önemli destekleri olmuştur. En önemlisi bilgisayarların ve iletişime dayalı yeni cihazların geliştirilerek kullanıma sunulmasıdır. Muhasebe sistemlerinin ve yönetim teorilerinin farklı bakış açılarıyla geliştirilerek bu gelişmeye çok tesiri etmiştir. 70'li yıllardan sonra hızla hacimleri küçülmüş, işleme hızları ve verileri saklama kapasitelerinin alanları çok büyümüş bilgisayarların üretilerek kullanıma sunulması ise; bilgi sistemlerinin gelişimini hızlandıran bir gelişme olmuştur. (Anameriç, 2005: 29) Özellikle bilgi teknolojilerinin işletmelerin rekabet edebilirliğini güçlendirmek için kullanılmaya başlaması ile bilgi sistemleri ve bilgi teknolojileri işletmeler için stratejik bir önem kazanmıştır. Bilgi teknolojileri literatürü göz gezdirildiğinde çoğunlukla iki farklı stratejik bilgi sistemi olduğu kabul edilmektedir: (Demirhan, 2002: 118)

- ✓ Belirli bir iş sahasında, bazı geliştirilen, yenileştirilen bilgi teknolojilerinden faydalanılarak oluşan yaratıcı düşünceler neticesinde meydana getirilmiş olan sistemlerdir. Bu sistemler kuruma özeldir ve hemen hemen benzerleri bulunmamaktadır.
- ✓ Mevcutta var olan ve kullanım alanı çok olan sistemlerdir. Bunların stratejik değeri nasıl ve ne olarak kullanıldıklarına göre değişmektedir.

Genellikle kurumlar tarafından, yönetim muhasebesi, finansal ve muhasebe sahalarında kullanılan bilgisayar sistemleri, 1990'lı yıllar ile hardware ve Softwarelerin zenginleşmesi ve niteliklerinin artması ile, finansal sahaların ötesinde de yönetimlere yön gösterici, karar vermede çok faydalı duruma gelmişlerdir. Ayrıca internetin dünya çapında yaygın ve kullanılır duruma gelmesi ve haberleşme teknolojilerindeki alt-üst yapılarında iyileştirmelerle , kurumlar açısından bilgi yönetimi çok önemli bir rekabet üstünlüğü yakalayabilen fonksiyon durumuna getirmiştir.

Bilgi sistemi uygulamaları özellikle büyük miktardaki verilerin toplanması, saklanması ve işlenmesi konularında işletmelere rekabet avantajı sunmaktadır. Bu sayede yöneticiler daha etkin kararlar verebilmektedir. Örnek olarak American Airlines'ın, yüzlerce gigabaytlık veriyi gelir yönetimi sistemlerini desteklemek için günlük olarak analiz ederek; yılda 500 milyon dolar ek gelir sağladığı tahmin edilmektedir. (Kurgun, vd, 2007: 262)

İşletme fonksiyonları içerisinde bilgi sistemleri; operasyonel bilgi sistemleri, karar verme amaçlı destek sistemleri, yönetim bilgi sistemleri ve yönetici destek sistemleri olarak ayrışmaktadır.

Operasyonel bilgi işleme sistemleri işletmenin operasyon el düzeyindeki faaliyetlerle ilgili bilgileri işlemekte ve yapısal kararların alınmasında operasyon el düzey yöneticilerine destek sağlamaktadır. Karar destek sistemi orta düzey yöneticilere yarı-yapısal kararların alınmasında destek sağlamaktadır. Yönetim Bilgi Sistemi ise yöneticilere özet rapor üreten bilgi sistemidir. Son olarak yönetici destek sistemi, alt düzey bilgi sisteminden sağlanan bilgiler ışığında karar alınmasını kolaylaştırmak amacıyla; stratejik konumda çalışan yöneticilerin yapısal olmayan kararlarına destek sağlamaktadır. (İlter, 2007: 8) Alt kadroda çalışanlara sağlanan bilgi, orta ve üst kadrolarda çalışanlara sağlanan bilgiden farklıdır. Bu kademede eyleme yönelik

denetleme kararı alan yöneticilerin gereksinim duyduğu bilgi, daha çok organizasyonun iç çevresine yönelik, organizasyonun geçmiş başarılarına ilişkin, iyi tanımlanmış, ayrıntılı ve dar kapsamlı olma özelliğini taşır. Alt kademedeki yönetim bilgi sisteminde işlemlerin çıktıları raporlar; eylem belgeleri ve sorgulama sonuçlarıdır. Bundan dolayı alt kademede üretilen bilginin doğruluk ve güvenilirliği yüksektir. (Anameriç, 2005: 30)

Genel olarak bilgi sistemleri işletme yöneticilerine stratejik aktivitelerde yardımcı olmaktadır. Bilgi sistem stratejisi de özellikle dönem planlaması politikalarının belirlenmesinde ön plana çıkmakta ve işletmenin mevcut durumu ile ilgili haberleşme sağlamakta ve dış çevreden var olan bilginin örgüt üzerindeki gelecek stratejilerini araştırmaktadır. (Tahirov, 2009: 124)

Bilgi sistemleri uygulaması klasik bir bakış açısıyla manüel olabileceği gibi, son yıllarda görülebileceği gibi bilişim sistemlerine dayalı olarak da gerçekleşebilmektedir. Öncelikli olarak veri hacminin küçük olduğu durumlarda klasik yaklaşımlar yeterli olurken; veri kapasitesinin ilerleyen zaman ile çoğalması klasik yaklaşımlar yeterli olamamakta ve problemlerin çözümünde var olan işlemler çok daha komplike bir durum oluşturmaktadır.

1.3. Bilgi Yönetimi Süreçleri

Bilgi yönetimi genel olarak bilgiyi toplayarak, bu bilgiyi kullanabilir bir bilgi haline getirme, bilgileri kurumsal uygulamalarda kullanma süreci, bilgiyi koruma-depolama süreci olmak üzere belirli süreçlerden meydana gelmektedir. Bu kısımda bu süreçler hakkında temel bilgiler sunulacaktır.

1.3.1. Bilgi Toplama

Bilgi toplama süreci, bilgi yönetiminin ilk aşaması kabul edilmektedir ve bu süreç bir bakıma elde etmesi üretme ve yaratma aşamasıdır ve tüm ifadelerin ortak noktası bilginin toplanmasıdır. (Çakar, vd, 2010: 75) Bu süreçte temel nokta mevcut bilginin daha verimli kullanımı ve elde edilmesidir. Buradan hareketle kıyaslama (benchmarking) ve işbirliği temel iki örnek durumundadır. (İpçioğlu ve Kahya, 2016: 181)

Bilgi yönetimi süreci öncelikli olarak bilgi gereksiniminin farkında olunması ile başlamakta ve elde edilen bilgilerin tüm faaliyetlere uyarlanmasına kadar tüm bilgisel faaliyetleri kapsamaktadır. Bu sürecin başarılı bir şekilde yürütülmesi için ilk olarak bilgi yönetiminin sağlayacağı yararların farkında olunması ve sistemin düzenli şekilde uygulanması gerekmektedir. (Odabaş, 2009: 182)

Bilginin oluşturulması, açık olarak ve/veya gizli olarak onu meydana getiren kaynaklardan yepyeni kaynak üretilmesi veya geliştirilmesi faaliyetlerini içermektedir. Bilginin üretimi, hem kurum içi hem de kurum dışı referanslardan faydalanarak bilginin temin edilmesi, düzenlenmesi ve toplanabilmesi, kurumsal öğrenme gibi unsurları içermektedir. (Odabaş, 2009: 185)

Bilginin elde edilmesi sürecinde çevresel (içsel ve dışsal) koşulların incelenmesi ve değişimler ile ilgili enformasyonun transferi gereklidir. Bu yolla daha fazla bilgi elde edilmektedir. Bilginin elde edilmesi içsel ve dışsal olarak iki kısımda incelenmektedir. Bu süreçte dışsal bilgi edimi konferanslar, müşteri ve rakiplerin takibi, organizasyona yeni üyelerin ve yeni organizasyonların katılımı ve diğer örgütler ile işbirliğini kapsamaktadır. İçsel öğrenme ise tecrübe, deney, süreç iyileştirme ve eleştirel yaklaşım yolu ile sağlanmaktadır. (Akgün ve Keskin, 2003: 181)

Örgüte değer katmak için örgütün değişen koşullarına uyum sağlanabilmesine imkan sağlayacak şekilde kurumun sahibi olduğu bilgi referanslarından ve/veya imkan kapasitelerinden en fazla seviyede faydalanmasını sağlamak bilgi yönetimi sürecinin temel amaçlarından birisidir. Odabaş'ın ifadesi ile kurumsal hizmetlerin niteliklerine uyumlu vakit ve süre içerisinde gerçek ve doğru bilgiye erişilmesiyle ölçümlenebilmektedir. Bilgi yönetimi yaklaşımında, bu fonksiyonun en optimal, en iyi biçimde gerçekleştirilebilmesini sağlamakta ve bilgiye emek ve maliyet açısından uygun bir şekilde erişilmesini sağlamaktadır. (Odabaş, 2009: 186)

1.3.2. Bilgiyi Kullanılabilir Bilgiye Dönüştürme

Bilginin kullanılabilir bilgiye dönüştürülmesi sürecinde, bilginin başarılı bir şekilde yönetilmesi bilgi değerinin birleştirilmesi ve bütünleştirilmesi ile bağlantılıdır. Dolayısıyla örgütlerin başarısı açısından bilginin doğru biçimde dönüştürülmesi gereklidir. Değişim odaklı bilgi yönetimi sayesinde kurum oluşan bilgileri organize

edebilir, bütünleştirebilir, birleştirebilir, yapılandırabilir, koordine edebilir veya dağıtma olanağı ile bilgiyi yararlı hale dönüştürülebilmektedir. (Çakar, vd, 2010: 76)

Bir değer olarak bilgi kolaylıkla toplanan veya paylaşılan bir varlık olmadığı için, bilgiden faydalanabilmek için örgüt içerisinde, örgüt koşullarına uyumlu olacak şekilde değiştirebilir ve/veya dönüştürülmesi gerekebilir. "Çalışma hayatında var olan her iş, dört bilgi dönüştürme sürecinden birini kendisine asıl olarak seçerek, iş modellerini ve iş süreçlerini kurmaktadır. Bilgiyi dönüştürme süreci, kısaca bilginin bir biçimden bir başka biçime geçişinde gerçekleşen işlemleri ifade etmektedir." (Zaim ve Seçgin, 2012: 4)

1.3.3. Bilgiyi Kurumsal Uygulamalarda Kullanma

Bilgi yönetimi prosesinin en önemli aşamalarından biri olan bilginin kullanılabilir hale getirilmesi ile depolama, düzeltme, uygulama, katılım ve paylaşım gündeme gelmektedir. (Demircan ve Yıldız, 2010: 76) Bilginin yapılandırılması anlamına da gelen bu süreçte bilgilerin hem geleneksel hem de elektronik olarak kodlanması, analizi, raporlanması ve sınıflandırılması gündeme gelmektedir. Bilginin yapılandırılması ile örgütsel veri tabanlarının oluşturulması analiz aşamasındaki bilginin düzenlenmesi, kümeleme gibi süreçler devreye girmektedir. (Sağsan, 2007: 112) Bilgi yönetimi sürecinde bilginin uygulanmasının büyük önemi vardır. Bilginin uygulanması yeni ürün geliştirilmesi, teknoloji transferi, pazarlama ve yönetim faaliyetleri sırasında ortaya çıkabilecek problemlerin çözümünü ifade etmektedir. Bunun mümkün olmaması performans iyileştirmenin doğru yapılamamasına yol açabilecektir. (Akgün ve Keskin, 2003: 182)

1.3.4. Bilgiyi Koruma

Bilginin korunma sürecinde belge ve bilgi birikimine erişmek için kaynakların analizi, bilgiye erişimin yetkili kişilerin eline bırakılması, kullanışlı bilginin tanımlanması ve bilginin verimli bir şekilde elenmesi gerekmektedir. Bu sayede sistemli bir şekilde düzenlenen bilgi yetkili kişilerin erişebilirlik dâhilinde ulaşılabilir hale gelecektir. (İpçioğlu ve Kahya, 2016: 183)

Bilginin depolanması olmadan hafıza veya uygulama olanağı bulunmamaktadır ve bu nedenle örgütsel hafıza önem kazanmaktadır. Akgün ve Keskin'in tanımlaması ile

örgütsel hafıza bir organizasyonun gelişimi boyunca depolanan enformasyonun verilecek kararlar için bugüne ve geleceğe taşınmasıdır. (Akgün ve Keskin, 2003: 182)

2. BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ

Bilginin gizliliğini, bütünlüğünü ve kesintisiz kullanılabilirliğini sağlamak üzere sistemleri, kuralları belirlenmiş, planlı, yönetilebilir, sürdürülebilir, tasnif edilmiş, yönetimce kabul görmüş ve uluslararası güvenlik standartlarının temel alındığı faaliyetler bütününe "bilgi güvenliği yönetim sistemi" denilmektedir. (Ersoy, 2012: 8)

2.1. Bilgi Güvenliği Kavramı, Bilgi Güvenliği Uygulamalarına Olan İhtiyacın Temel Nedenleri

Her geçen gün bilgi miktarının ve teknolojik olanakların artışı yanı sıra organizasyonların bilişim teknolojilerine bağımlı hale gelmesi bilgi güvenliği olgusunun ortaya çıkmasına yol açmıştır. Bilgi güvenliği, kurumlarda bilgiyi depolamak ve iletmek için kullanılan donanımın ve alt yapının korunması da dâhil olmak üzere hassas bilgilerin üretilmesini, toplanmasını, depolanmasını, kullanılmasını, iletilmesini ve korunmasını kapsamaktadır. (FFIEC, 2010: 1)

Feruza ve Kim bilgi güvenliği kavramını genel bir bakış açısı ile bilgi ve bilgi sistemlerini yetkisiz erişime, kullanıma, açıklama, aksama, değiştirme veya imha etme yollarından koruma olarak tanımlamıştır. (Feruza, 2007: 17) Bu tanım uyarınca bilgi güvenliği, verilerin biçiminden bağımsız olarak gizliliği, bütünlüğü ve kullanılabilirliği ile ilgilidir.

Singh, Vaish ve Keserwani de benzer bir yaklaşım ile kavramı bilginin ve bilgi sisteminin, depolama, işleme veya transit olarak yetkisiz erişime veya bilginin değiştirilmesine karşı korunması ve yetkisiz kullanıcılara hizmet reddine karşı korunması, bu tür tehditleri saptamak, belgelemek ve karşı koymak için gerekli önlem olarak açıklanmıştır. (Singh, vd, 2014: 1072)

Baykara, Daş ve Karadoğan ise kavramı "Bilgiye sürekli olarak erişimin sağlanması gereken bir ortamda, bilginin kaynağından hedefine kadar gizlilik içerisinde,

bozulmadan, değişikliğe uğramadan ve başkaları tarafından ele geçirilmeden iletilmesi süreci ve işlemleri" (Baykara, vd, 2013: 231) şeklinde tanımlamıştır.

Von Solms ve Van Niekerk, siber güvenliğin farklı yönlerini araştırmış ve bilgi güvenliği ile benzer noktalarının olmasına rağmen, farklı anlamlara geldiklerini açıklamışlardır. Buna göre bilgi güvenliğinin genel tanımı kullanılabilirlik, bütünlük ve gizlilikten oluşurken, siber güvenlik, kişisel kapasiteler de dâhil olmak üzere bilgi güvenliğinin resmi sınırlarının ötesine uzanan boyutlarını içermektedir.(Safa, vd, 2016: 71)

Bilgi güvenliği tanımlarında gizlilik, bütünlük ve erişebilirlik ön plana çıkan kavramlardır. Buna göre bilginin gizliliği, bilgiye sadece yetkili kişi ve kişilerin erişimini ifade etmektedir. Bilginin bütünlüğü ile kastedilen, bilginin bozulmadan, orijinal haliyle olduğu gibi korunması anlamına gelmektedir. Son olarak bilginin erişilebilirliği kavramı ile demek istenen, ihtiyaç duyulduğu zaman ve en uygun sürede bilgiye erişilmesi ve kullanılmasıdır. (Baykara, vd, 2013: 238)

Bilişim teknolojilerinin sunduğu olanaklar ile organizasyonlar faaliyetlerinde bilişim teknolojilerine daha faza bağlı durumdadır ve bu bağlılık arttığı ölçüde, organizasyonların bu bilişim teknolojilerinde gerçekleşebilecek problemlere ve siber ataklara karşı hassasiyeti de artmaktadır. (Acılar, 2009: 30) Bilgi güvenliği, saldırılara karşı bilginin gizliliğini, bütünlüğünü ve erişilebilirliğini korumak için araçlar ve mekanizmalar sağlamayı da amaçlamaktadır. Gizlilik, yetkisiz okuma, yetkisiz yazılmış yazılara karşı bütünlük ve bilgilerin silinmesine karşı önlemler içeren bilgi güvenliği, bilgi sistemlerinin içerdiği risklerle ilişkilendirilir. (Pieters, 2011: 329) Özellikle bilgiye uygulanan teknoloji riski yarattığı için bilgi güvenliği bir zorunluluk olarak karşımıza çıkmaktadır. En yaygın şekilde bilgiler yanlışlıkla ifşa edilebilir (gizlilik tehlikeye girebilir), uygun olmayan bir şekilde değiştirilebilir (yani bütünlüğü tehlikeye atılabilir), yok edilmiş veya kaybolmuş olabilir (yani kullanılabilirliği tehlikeye atılabilir). (Blakley, 2001: 97)

Her geçen gün bilgi miktarının ve teknolojik olanakların artışı yanı sıra organizasyonların bilişim teknolojilerine bağımlı hale gelmesi bilgi güvenliği olgusunun ortaya çıkmasına yol açmıştır. Bilgi güvenliği, kurumlarda bilgiyi depolamak ve iletmek için kullanılan donanımın ve alt yapının korunması da dâhil olmak üzere hassas bilgilerin

üretilmesini, toplanmasını, depolanmasını, kullanılmasını, iletilmesini ve korunmasını kapsamaktadır. (FFIEC, 2010: 1)

Feruza ve Kim bilgi güvenliği kavramını genel bir bakış açısı ile bilgi ve bilgi sistemlerini yetkisiz erişime, kullanıma, açıklama, aksama, değiştirme veya imha etme yollarından koruma olarak tanımlamıştır. (Feruza ve Kim, 2007: 17) Bu tanım uyarınca bilgi güvenliği, verilerin biçiminden bağımsız olarak gizliliği, bütünlüğü ve kullanılabilirliği ile ilgilidir.

Singh, Vaish ve Keserwani de benzer bir yaklaşım ile kavramı bilginin ve bilgi sisteminin, depolama, işleme veya transit olarak yetkisiz erişime veya bilginin değiştirilmesine karşı korunması ve yetkisiz kullanıcılara hizmet reddine karşı korunması, bu tür tehditleri saptamak, belgelemek ve karşı koymak için gerekli önlem olarak açıklanmıştır. (Singh, vd, 2014: 1072)

Baykara, Daş ve Karadoğan ise kavramı "Bilgiye sürekli olarak erişimin sağlanması gereken bir ortamda, bilginin kaynağından hedefine kadar gizlilik içerisinde, bozulmadan, değişikliğe uğramadan ve başkaları tarafından ele geçirilmeden iletilmesi süreci ve işlemleri" (Baykara, vd, 2013: 231) şeklinde tanımlamıştır.

Von Solms ve Van Niekerk, siber güvenliğin farklı yönlerini araştırmış ve bilgi güvenliği ile benzer noktalarının olmasına rağmen, farklı anlamlara geldiklerini açıklamışlardır. Buna göre bilgi güvenliğinin genel tanımı kullanılabilirlik, bütünlük ve gizlilikten oluşurken, siber güvenlik, kişisel kapasiteler de dâhil olmak üzere bilgi güvenliğinin resmi sınırlarının ötesine uzanan boyutlarını içermektedir. (Safa vd, 2016: 71)

Bilgi güvenliği tanımlarında gizlilik, bütünlük ve erişebilirlik ön plana çıkan kavramlardır. Buna göre bilginin gizliliği, bilgiye sadece yetkili kişi ve kişilerin erişimini ifade etmektedir. Bilginin bütünlüğü ile kastedilen, bilginin bozulmadan, orijinal haliyle olduğu gibi korunması anlamına gelmektedir. Son olarak bilginin erişilebilirliği kavramı ile kastedilen ise, bilgiye istenilen ve makul zamanda erişilmesi ve kullanılmasıdır. (Baykara, vd, 2013: 238)

Bilişim teknolojilerinin sunduğu olanaklar ile organizasyonlar faaliyetlerinde bilişim teknolojilerine daha faza bağlı durumdadır ve bu bağlılık arttığı ölçüde, organizasyonların bu teknolojilerde meydana gelebilecek arızalara ve saldırılara karşı

duyarlılığı da artmaktadır. (Acılar, 2009: 30) Bilgi güvenliği, saldırılara karşı bilginin gizliliğini, bütünlüğünü ve erişilebilirliğini korumak için araçlar ve mekanizmalar sağlamayı da amaçlamaktadır. Gizlilik, yetkisiz okuma, yetkisiz yazılmış yazılara karşı bütünlük ve bilgilerin silinmesine karşı önlemler içeren bilgi güvenliği, bilgi sistemlerinin içerdiği risklerle ilişkilendirilir. (Pieters, 2011: 329) Özellikle bilgiye uygulanan teknoloji riski yarattığı için bilgi güvenliği bir zorunluluk olarak karşımıza çıkmaktadır. En yaygın şekilde bilgiler yanlışlıkla ifşa edilebilir (gizlilik tehlikeye girebilir), uygun olmayan bir şekilde değiştirilebilir (yani bütünlüğü tehlikeye atılabilir), yok edilmiş veya kaybolmuş olabilir (yani kullanılabilirliği tehlikeye atılabilir). (Blakley, vd, 2001: 97)

Bilgi güvenliği uygulamalarına olan ihtiyacı ana hatları ile şu şekilde sıralamak mümkündür: (Vural ve Sağıroğlu, 2007: 192)

- Güvenlik tehdit ve risklerinin belirlenerek etkin bir risk yönetimini sağlamak,
- Kurumsal itibarı korumak,
- Bilgi kaynağına olan yetkisiz erişimlerin önüne geçmek,
- Personelin bilgi güvenliği konusundaki bilinç düzeyini yükseltmek,
- Bilginin gizliliğini, doğruluğunu ve güvenliğini sağlamak,
- Kurumsal bilginin kötü amaçlı kullanımının engellenmesi,
- Bilgiyi kullanan kişilerin kasıtlı ya da kasıtsız olarak bilgisayar ağlarında meydana getirebileceği arızalardan korunmak.

2.2. Bilgi Güvenliği Sisteminin Yapılandırılması

Bilginin gizliliğini, bütünlüğünü ve kesintisiz kullanılabilirliğini sağlamak üzere sistemleri, kuralları belirlenmiş, planlı, yönetilebilir, sürdürülebilir, tasnif edilmiş, yönetimce kabul görmüş ve uluslararası güvenlik standartlarının temel alındığı faaliyetler bütününe "bilgi güvenliği yönetim sistemi" denilmektedir. (Ersoy, 2012: 8)

Bilgi güvenliği sisteminin yapılandırılması tanımlama, risk değerlendirmesinin yapılması, risk analizi, kontrol hedeflerinin seçimi, yönetim onayı, uygunluk bildirisinin hazırlanması aşamalarından oluşmaktadır ve tüm aşamalar birbirini takip eder niteliktedir.

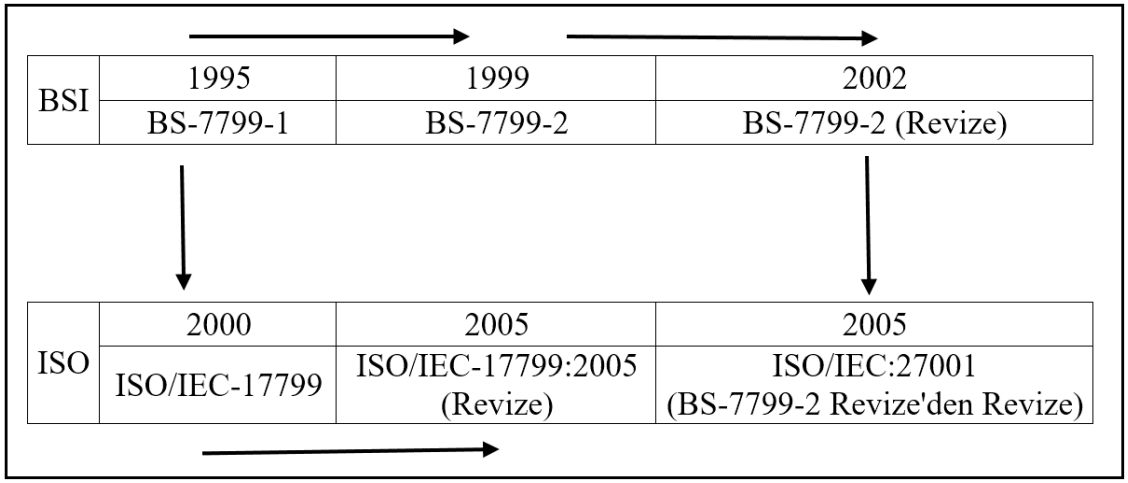
Bilgi güvenliği sisteminin yapılandırılmasında ilk aşama bilgi güvenliği politikalarının tanımlanmasıdır. Bu politikalar, hassas bilgiler ile kimin ne yapmasına izin

verilmesi gerektiğini tanımlamaktadır. (Blakley, 2001: 98) Bilgi güvenliği politikasından yönetime yol verici ve harekete geçirici şekilde, hangi risklerin göz önüne alınacağına ilişkin risk analizi belirleyen bir çerçeve sunması beklenmektedir. Sistemin amacına erişebilmesi için çalışanların yönetim politikası içindeki yazılı olan maddelerin uygulamada fiili olarak iş hayatına geçirileceğine ilişkin kararlılığı yönetim, işgörenlere hissettirmelidir. (Önel, 2008: 12)

2.3. Bilgi Güvenliği Standardı ve Kılavuzlar

Siber güvenliğe yönelik tehditlerin sürekli olarak yenilenmesi ve kullanılan yazılım ve donanımlardaki güvenlik açıklarının takibi gibi nedenlerle bilgi güvenliği sürecinin yönetimi için birtakım standartlar oluşturulmuştur. Standartların öncüsü İngiliz Standartlar Enstitüsü'dür (BSI - British Standards Institute). BSI'nin oluşturduğu standartlar daha sonra ufak revizyonlardan geçirilerek ISO standartları olarak tüm dünyada kabul edilmeye başlanmıştır. (Vural ve Sağıroğlu, 2008: 511) Şekil 1'de Bilgi Güvenliği Standartları'nın gelişimi görülmektedir.

Şekil 1: Bilgi Güvenliği Standartları



Kaynak: Yılmaz Vural, Şeref Sağıroğlu, "Kurumsal Bilgi Güvenliği ve Standartları Üzerine Bir İnceleme", Gazi Üniv. Müh. Mim. Fak. Der. Cilt: 23, No:2, 2008, s. 511'den tarafımca oluşturulmuştur.

3. SİBER GÜVENLİK, SİBER SAVAŞ VE SİBER SUÇ KAVRAMLARI

Günümüz dünyasında internet artık hayatın her alanında karşımıza çıkmaktadır. Geleneksel olarak internetle hiçbir ilgisi olmayan buzdolabı, çamaşır makinesi gibi cihazlar dahi internete bağlanarak "akıllı" hale gelmiştir. Dolayısıyla geleneksel olarak güvenlik alanına giren konulara ek olarak artık dijital ya da siber güvenlik de söz konusudur. Çünkü günümüz dünyasında artık konvansiyonel savaşlardan ziyade siber savaşlar ön plana çıkmaktadır.

Bilişim çağını yaşadığımız 2000'li yıllarla birlikte dünya artık internet üzerinden yönetilmeye ve şekillenmeye başlamıştır. Özellikle kişilerin bilerek, isteyerek ve kasten kişisel bilgilerini, fotoğraflarını sosyal paylaşım sitelerinde paylaşması, siber dünyada bilgilerini kendi elleriyle tehlikeye atmaları anlamına gelmektedir. Ancak yine de bireyler bu davranışları çekinmeden sergilemeye devam etmektedir. Dolayısıyla siber güvenlik için atılması gereken ilk adım bireysel bilinçlenmeden geçmektedir. Sonrasında ise teknik araçlar devreye girmektedir.

Geleneksel güvenlik anlayışının yetersiz kaldığı siber dünyada bireyler, kurum ve kuruluşlar ve hatta devletler, kullandıkları bilişim, ve iletişim teknolojilerinin içinde var olan bilgilere, oluşabilecek tehditlere karşı savunabilmek için siber güvenlik ve siber savunma konusuna önem vermek ve bu yöndeki çabalarını hızlandırmak zorunda kalmıştır. Siber dünyaya yönelik saldırıların etkilerini en aza indirebilmek ve kritik altyapı sistemlerini siber saldırılardan koruyabilmek için siber güvenliğe maksimum derecede önem verilmesi gereği ortaya çıkmıştır.

Siber güvenlik, bilişim ve iletişim teknolojilerinin baş döndürücü bir hızda gelişme gösterdiği çağımızda insanların, örgütlerin ve devletler için en önemli güvenlik mekanizmalarından biri durumuna gelmek zorunda kalmıştır. Şu anda önemli olduğu gibi gelecekte de önemli olmaya devam edecektir. Bilgi ve iletişim teknolojilerine olan bağımlılık arttıkça siber tehditlere daha açık hale gelinecek, buna karşılık siber güvenlik öncelikli güvenlik alanlarından olacaktır.

Yaygın olarak kullanılan siber güvenlik, siber suç ve siber savaş gibi ifadelerin üzerinde mutabakata varılmış, ortak ve tam Türkçe karşılıkları henüz bulunmamaktadır. Bu kavramların tam olarak bir karşılığının olmaması, siber kelimesine bir tanım

bulunamamasından ileri gelmektedir. Bu nedenle siber güvenlik, siber suç, siber savaş gibi kavramlara değinmeden önce siber kelimesini açıklamak yerinde olacaktır.

Siber, bilgisayar ağlarıyla ilgili olan ya bu ağları içeren kavramları kapsamaktadır. Sıklıkla kullanılan siber alan tabiri ile birbiriyle bağlantılı donanım, yazılım, sistem ve insanların etkileşim içerisinde olduğu soyut ve somut alanı tarif etmek için kullanılmaktadır. (Hekim ve Başıbüyük, 2013: 136) Bu alanın güvenliği söz konusu olduğunda siber güvenlikten, bu alanda suç işlendiğinde siber suçtan, bu alanda karşılıklı olarak saldırılar olduğunda ise siber savaştan söz etmek mümkündür.

Siber, bilgisayarlar ve/veya bilgisayar ağlarını ilgilendiren ya da bunları da içeren kavramlar için kullanılmaktadır. Çoğunlukla tek başına "siber" olarak değil, "siber alan" olarak kullanılmaktadır. Siber alan, birbiriyle bağlantılı donanım, yazılım, sistem ve insanların etkileşiminde olduğu soyut ya da somut bir alandır. Bu alanda işlenen suçlar ise siber suç olarak adlandırılmaktadır. (Hekim ve Başıbüyük, 2013: 136)

3.1. Siber Güvenlik

Güvenlik, insanlığın var olduğu günlerden bu yana karşımıza çıkan ve bireysel ve toplumsal olarak kullanılabilen, dolayısıyla birçok farklı anlama gelebilen bir kavramdır. Güvenlik kavramının içinde bireysel güvenlik olduğu gibi ailenin güvenliği, toplumun güvenliği, bölgenin ve makro anlamda devletin güvenliği gibi birçok alan bulunmaktadır. Dolayısıyla güvenlik, yaşamsal bir zorunluluktur. (Daban, 2017: 80) İnternetin yaygınlaşması ile birlikte güvenlik alanlarına siber güvenlik de eklenmiştir.

Siber güvenlik kavramının üzerinde bir fikir birliğine varılmış net ve kesin bir tanımı yoktur. Bu nedenle de birçok farklı tanımı bulunmaktadır. BM'nin bir organı olan Dünya Telekomünikasyon Birliği'nin tanımlamasıyla siber güvenlik, "siber uzayda organizasyon ve kullanıcıların varlıklarını koruyabilmek amacıyla kullanılan her türlü araç, politika, güvenli önlemleri, kurallar, eylemler ve eğitimler ile risk yönetimi yaklaşımlarını içeren teknolojilerin bütünüdür" (Akleylek ve Yüce, 2011: 16).

Siber güvenlik açıklamalarında gizlilik, bütünlük ve erişebilirlik ön plana çıkan özelliklerdir. Gizlilik, bilgiye yalnızca yetkisi olanların erişmesi anlamındayken, bütünlük, bilginin bozulmaksızın orijinal haliyle korunabilmesidir. Erişebilirlik ise

bilgiye istenilen zamanda, makul süre içerisinde ulaşabilmek ve kullanabilmektedir. (Baykara, vd, 2013: 239)

Çağımızın neredeyse tek gerçeği haline gelen bilgiye sahip olma, bilgi miktarının sürekli artması, teknolojik imkanların günden güne gelişimi ve kurum ve kuruluşların sürekli olarak bilişim teknolojilerine çok fazla ihtiyaçları zorunlu bir duruma gelmesiyle, siber güvenliği ve siber güvenlik olgusunun ortaya çıkmasına yol açmıştır. Siber güvenlik, kurumlarda bilgiyi depolayıp iletmek için kullanılan donanım ve altyapı da dahil olmak üzere hassas bilgilerin toplanması, depolanması, korunması, kullanılması ve iletilmesini kapsamaktadır.

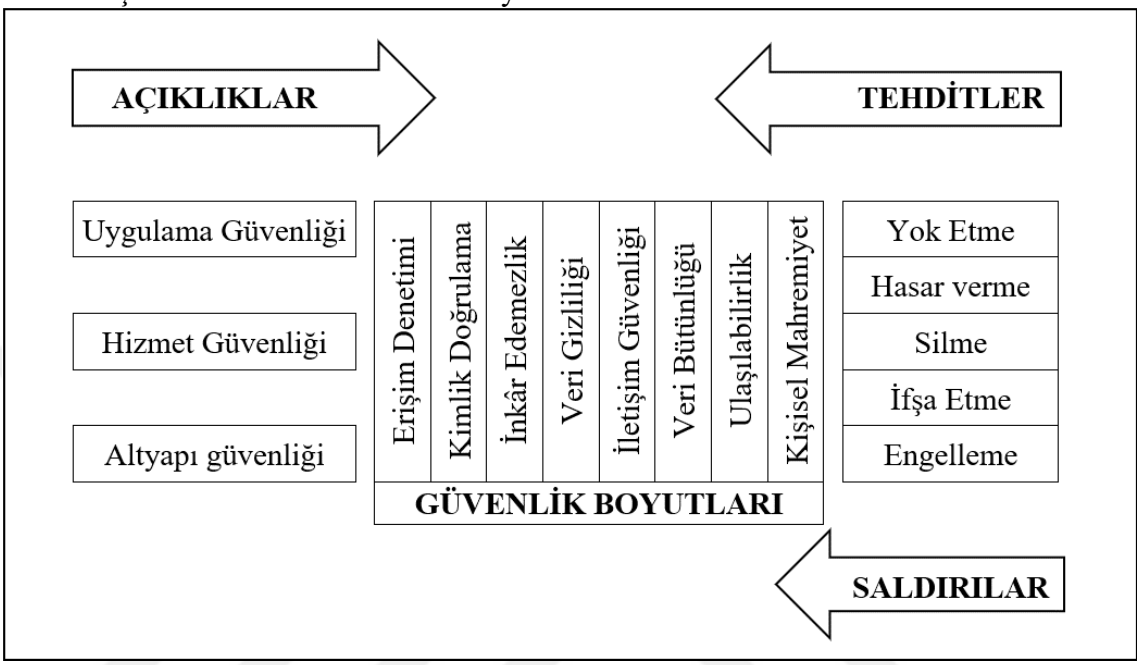
Siber güvenlik, düşük maliyetlerle hemen her sektöre yöneltilebilmesi, ülkelerin askeri ve siyasi yapılanmaları da dahil olmak üzere gizli bilgilerinin deşifre edilebilmesi, toplumsal yapıya yönelik olarak algı oluşturulabilmesi, ülke ekonomisine ve gündelik hayata zarar verilebilmesi ve çevresel problemlere yol açabilmesi bağlamında önemli bir güvenlik sektörü haline gelmiştir. Güvenlik sektörlerinin iç içe geçişi ile birlikte güvenlikli hale getirme uygulamaları kapsamında siber güvenlik kavramı da karşımıza çıkmaktadır. (Eren, 2017: 31)

İnsanların bilgisayarlar aracılığı dünya çapında sınır tanımaksızın birbirleriyle bağlantılı olabilmesi veya ABD Savunma Bakanlığı tarafından İnternetin bulunduğu, haberleşme- iletişim ağlarını ve bilgisayar sistemlerini kapsayan, birbirine bağlı teknolojik altyapılara sahip küresel bir alan olarak tanımlanan siber ataklardan gelebilecek saldırılar ve siber tehditlere karşı, örgüt, kuruluş ve bireylerin bilgi varlıklarını korumak altına almak amacıyla kullandığı politika ve risk yönetimi yaklaşımları siber güvenliği meydana getirmektedir. Siber saldırıların ana hedefi, ülkelerin güvenlik, sağlık, enerji, ulaşım, haberleşme, su, bankacılık ve kamu hizmeti gibi kritik öneme sahip olan hizmetlerini verebilmesini sağlayan bilgi sistemi altyapılarıdır. (http://haber.tobb.org.tr/ekonomikforum/2015/251/012_021_kapak_konusu.pdf:12-21)

Siber güvenlik, kurum, kuruluş ve bireylerin siber ortamdaki varlıklarına ait güvenlik özelliklerinin siber ortamdaki tehlikelere karşı koyabilecek şekilde oluşturulmasını ve idame ettirilmesini sağlamayı amaçlamaktadır. Siber güvenliğin temel hedefi, bilginin erişebilirliğini, bilginin aslına uygun bir şekilde muhafazasını ve inkâr

edilemezliği de dahil olmak üzere bütünlüğünü ve gizliliğini sağlamaktır. (Ünver, vd, 2009: 3) Şekil 2'de siber güvenliğe genel bakış görülmektedir.

Şekil 2: Siber Güvenlik ve Boyutları



Kaynak: Mustafa Ünver, Cafer Canbay, Ayşe Gül Mirzaoğlu. *Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler*, Ankara: Bilgi Teknolojileri ve İletişim Kurumu (BTK), 2009.

Siber güvenliğin sağlanmasında temel olarak teknolojik gelişmeler, iyi üretilen politikalar, yol gösterici yöntemler, güvenlik eğitimleri, küçük yaşlardaki eğitimler, güvenliğin sarsılmasına yönelik tehditlerin bertaraf edilmesine ilişkin projeler ve risk yönetimine karşı alınabilecek tedbirler gibi birçok temel unsur söz konusudur. Siber güvenlik, daha ziyade tehdit ve risklere karşı önlem alınmasını içermektedir. Siber tehdit, bir kurum ya da sistemin zarar görmesini sağlayabilecek faaliyet ya da uygulamalardır. Siber güvenlik, tehditler ortaya çıkmadan önce gerekli tedbirleri almakla görevlidir. Risklerin oluşuma karşı da siber güvenlik ön planda olmaktadır. Siber güvenlik hem riskleri hem de tehditleri oluşmadan önce engellemeye çalışma çabalarıdır. (Daban, 2017: 80)

İnternet kullanımının artmasıyla birlikte artan siber tehditler günden güne daha karmaşık bir yapıya bürünmektedir. Bu nedenle de siber güvenlik ihtiyacı hem bireysel

hem kurumsal hem de ulusal bazda karşımıza çıkmaktadır. Siber güvenliğin sağlanmasına yönelik çalışmalarda bulunması gereken unsurları şu şekilde sıralamak mümkündür: (Arslan, 2017: 127)

- Siber güvenlikle ilgili yapılacak çalışmaların belli hedef doğrultusunda ilerlemesi için ulusal politika ve stratejinin geliştirilmesi,
- Caydırıcılığın sağlanması için ulusal mevzuattaki eksiklerin giderilmesi için yasal çerçevenin oluşturulması,
- Geliştirilecek hukuki düzenlemelerin yanında teknik tedbirlerin geliştirilmesi,
- Belli sorumlulukları olan kurumlar arasında işbirliğinin ve koordinasyonun sağlanması ile siber tehdit ve saldırılar ile etkin bir mücadele için kurumsal yapılanmanın belirlenmesi

Bir ülkenin kurumlarına veya devletin güvenlik fonksiyonlarına yapılabilecek siber saldırıların dünyadaki bağlantı kolaylığı göz önünde bulundurulduğunda, bu tehditlerin herhangi bir kişi, bir grup ya da herhangi bir başkaca ülke tarafından gelebileceği açıktır. Bu nedenle de uluslararası iş birliği ve evrensel kuralların uygulanması şarttır. Siber güvenliği sağlayabilmek için alınacak tedbirlerde göz önünde bulundurulması gereken temel hak ve özgürlüklerin korunması, demokrasiye tam uyum, ölçülülük ilkesine uyum, karar almaya katılım, hukuki, teknik, yönetim, iktisadi, sosyal ve politik konularda bütünü kapsayan bir anlayışla, özgürlük ve güvenlik dengesinin sağlanması, diğer ülke mevzuatlarıyla mümkün olduğunca uyum ve uluslararası iş birliğinin sağlanması gibi hususlar bulunmaktadır. (Yılmaz ve Sağıroğlu, 2013: 158)

İnternet destekli iletişim teknolojilerinin yaygınlaşması ile birlikte siber tehdit ve risklerin önlenmesi yalnızca güvenlik yazılımlarına bırakılmayacak kadar ciddi bir iştir. Bilgi güvenliği davranışı da mutlaka yaygınlaştırılmalıdır. Ciddi siber saldırılardan korunabilmenin ve önlemenin en etkili ve basit yolu, özellikle son kullanıcıların güvenlik tedbirlerinin alınmasıdır. Özellikle bilinçsiz kullanıcıların internete bağlanabilen tüm cihazları, siber güvenlik açısından risk taşımaktadır. (Şahinaslan, vd, 2013: 1081)

Siber güvenlik uygulamalarına olan ihtiyacı ana hatları ile şu şekilde özetlemek mümkündür.

- Güvenlik tehdit ve risklerinin belirlenerek etkin bir risk yönetimini sağlamak,
- Kurumsal itibarı korumak,

- Bilgi kaynağına olan yetkisiz erişimlerin önüne geçmek,
- Personelin bilgi güvenliği konusundaki bilinç düzeyini yükseltmek,
- Bilginin gizliliğini, doğruluğunu ve güvenliğini sağlamak,
- Kurumsal bilginin kötü amaçlı kullanımının engellenmesi,
- Bilgiyi kullanan kişilerin kasıtlı ya da kasıtsız olarak bilgisayar ağlarında meydana getirebileceği arızalardan korunmak.

Siber güvenlik, üç temel aşamada sağlanabilmektedir. Bu aşamalar erişim kontrolü, kimlik denetimi ve yetkilendirmedir. Dolayısıyla siber güvenlik bilgiye yetkisiz erişimin denetlenmesi, kurum ve kuruluşun sunduğu hizmetlerin korunmasını, yetkisiz erişimlerin ve işlemlerin tespitini, çalışma yaşamındaki bilgilerin korunmasını ve erişenlerin kimliğini tespit etmeyi mümkün kılmaktadır. Diğer bir ifadeyle siber güvenlik, hacker, içten ya da dıştan gelebilecek saldırganlar, virüsler, casus yazılımlar, özetle tüm kötücül kişi, davranış ya da yazılımlardan gelebilecek olumsuz ve zararlı eylemleri engellemektir. Siber güvenlik, yetkisiz erişimleri mümkün olduğunca aza indirgemek ya da eğer mümkünse tamamen yok etmekle yükümlüdür. Bu nedenle siber güvenlik hem ulusal hem de uluslararası ilişkilerde önemli bir yer kaplamaktadır. (Daban, 2017: 80)

Güvenlik teknolojilerinin gelişimi ile birlikte teknik açıkları kullanmak daha da zorlaşmaya başladığından, saldırganlar güvenlik uygulamalarının en zayıf halkasını, yani insanı hedef almaya başlamıştır. Herhangi bilişim - iletişim sisteminde verinin - bilginin sahibi olup verileri - bilgileri kullanabilmek veya bilişim -iletişim sistemini yöneten bir kişi olmak, bu durumdaki kişiyi bilgi güvenliği konusunda sorumlu duruma getirmektedir. Bu nedenle de veri - bilgi güvenliğinin farkında olmak, suiistimallerin ve kasıtlı tehditlerin önüne geçmek noktasında atılabilecek ilk adım olmaktadır. (Keser, Güldüren, 2015: 1172)

Kurumlar, siber güvenliği maksimize edebilmek için başta kurum çalışanları olmak üzere tüm paydaşların en değerli varlık olan bilginin korunmasında üzerine düşen görev ve sorumlulukları anlamalarını sağlamalıdır. Kurumlar için kritik öneme sahip olan bilgi varlığının hangi tür saldırı ve tehditlere karşı korunması gerektiğine yönelik bilinçlendirme çalışmaları yapılmalıdır. Dolayısıyla kurumlarda tüm çalışanlar iş tanımlarında yer alan görevlerden sorumlu olduğu gibi, bilgi güvenliğinden ve siber güvenlikten de sorumlu olmalıdır. (Şahinaslan, vd, 2013)

Siber güvenlik ve bilgi güvenliği, eğitim ve teknolojiden etkilendiği kadar insan faktöründen de etkilenmektedir. Bu nedenle kurum içi çalışanların bilgi güvenliğine yeteri kadar önem vermemesi ya da ihmali, bilgi güvenliğini olumsuz etkilemektedir. Siber güvenlik, bilgiye erişimin olduğu bir ortamda bilginin göndericiden alıcıya giderken mesaj ulaşana kadar gizliliğinin sağlanması, içeriğinin bozulmadan ulaşması ve üçüncü kişiler tarafından ele geçirilmeksizin güvenli bir şekilde iletiminden sorumludur. Ancak bilgiyi kullananın insan olduğu göz önünde bulundurulduğunda en ufak bir ihmalkarlığın bilgi güvenliğini tehlikeye düşüreceği unutulmamalıdır. (Kurnaz, Dindaroğlu, 2015: 53)

Siber güvenlik ve bilgi güvenliği konusundaki en büyük ihmal, bireyin ya da kurumun / kuruluşun önceden önlem almaktansa, başına bir siber olay geldikten sonra harekete geçme eğiliminde olmasıdır. Bu nedenle özellikle bilgi güvenliğinden sorumlu yöneticilerin, sonrasında ise tüm çalışanların bilgi güvenliğinde farkındalığa sahip olması, bilgi kültürünün oluşumunda olumlu etki etmektedir. (Yılmaz, vd, 2016: 27)

Bilginin yönetiminin yanında güvenliğinin sağlanması da karmaşık bir süreçtir. Kurumsal ve kişisel bilgilerin güvenliğinin yalnızca güvenlik duvarı, VPN, anti virüs gibi teknik araçlarla sağlanması mümkün değildir. Bu nedenle teknik tedbirlerin yanında insan unsurunu göz önünde bulundurarak bilgi güvenliği konusundaki farkındalığı artırmak hem bilgi güvenliğinin hem de siber güvenliğin en temel çıkış noktasıdır. (Güldüren, vd, 2016: 685)

Siber güvenlik konusundaki en büyük yanlışlardan biri de güvenlikten yalnızca bilişim uzmanlarının sorumlu olduğuna yönelik inançtır. İnternetin kanuni olmayan, illegal uygulamalar ve yöntemlerle üçüncü kişi ya da örgütlerden yasa dışı olarak faydalanmak isteyen kötü amaçlı insanlara imkanlar tanıdığı açıktır. Bilginin açık hedef haline geldiği günümüzde siber suçlara meyilli bilişim korsanlarının son kullanıcılara ait bilgisayara saldırı düzenlemesi sıkça görülen bir durumdur. Bu nedenle konuyu, yalnızca bilişim uzmanlarının sorumluluk sahasına bırakmak, konuya yeterince önem vermemektir. (Akgün ve Topal, 2015: 103)

Siber güvenlik tahminlerini belirleyen forcepoint, 2018 yılı sıralamasında insan odaklı güvenlik tedbirleri dikkati çekmektedir.(forcepoint, www.infonet.com.tr , 2018)

Bazı Üniversitelerimiz, siber güvenlik merkezleri kurmuşlardır. Örneğin Boğaziçi üniversitesi, yönetim bilişim sistemleri siber güvenlik merkezi ile bakış açısını geliştirmeyi hedeflemektedir. (https://siber.boun.edu.tr ,2018)

Türkiye'de siber güvenliğin teminine yönelik yeni çalışmalar için bir belirsizlik ortamı olduğu görülmüş, Yetkili karar verme düzeyinin siber güvenlik alanında kapsamlı teknik bilgiye sahip olmadığı, başka ülke çalışmalarından, uygulamalarından yararlandığı tespit edilmiştir.(Göçoğlu, 2018 : 285)

Siber Güvenliğin Denetim modeli oluşturulması ve uygulanması ve başarılı olması için yönetimlerin desteği gerekmektedir. Yönetimin, denetimler için mali bütçe ayrılması ve liderlik etmesi gerekmektedir. Örgüt Kültürü yaratılması sibe güvenlik denetiminde etkili olmaktadır. (Öztürk, 2018:227)

3.2. Siber Savaş

Hedef olarak belirlenen kişi, örgüt, kurum gibi yapıların bilişim sistemlerine veya telekominikasyon altyapılarına yapılan planlı ve koordineli saldırılar siber saldırı olarak adlandırılırken, benzer türde saldırıların bir devlete veya ülkenin güvenliğine yönelik yapılması durumunda ise siber savaş söz konusudur. Siber savaşta hedefler çoğunlukla ülkelerin kritik altyapı alanları olmaktadır, bunlarda, sağlık, güvenlik, haberleşme, enerji, su ve kanalizasyon, borsa, bankacılık, finansal kuruluşlar ve kamu hizmetleri gibidir. (Yılmaz ve Sağıroğlu, 2013: 158)

Devletlerin, bilgi toplumuna geçme sürecini önceden çok iyi planlayarak yönetemeyen, bütün ülkeler için çok kritik önem derecesine sahip altyapılarının bilişim - iletişim sistemlerinin yönetim sürecinde ulusal standartları belirleyip kullanmayan ülkeler risk altına girmektedir. Bu konudaki en önemli örneklerden biri şüphesiz 2007 yılında Rusya ile Estonya arasında yaşanan siber savaştır. Estonya bilgi toplumuna geçiş sürecini başarılı olarak yönetiyorsa da bilgi varlıklarını korumak konusunda aynı ölçüde başarılı olamayınca saldırılara açık hale gelmiş, bunun sonucunda Rusya'dan gelen siber saldırılar ile bankacılık sistemlerinden trafik ışıklarına kadar tüm ülkedeki sistemler çökmüş ve Estonya çareyi NATO'dan yardım istemekte bulmuştur. (Yılmaz, vd, 2015: 138)

Rusya kaynaklı bir diğer siber saldırı ve siber savaş 2008 yılında Gürcistan'a yönelik olarak gerçekleştirilmiştir. SSCB'nin dağılmasının ardından fiili olarak bağımsız olan Güney Osetya'ya yönelik Gürcistan'ın ülkenin toprak bütünlüğünü sağlamak amacıyla başlattığı operasyona cevaben Rusya, Güney Osetya'ya askeri bir operasyon düzenlemiştir. Bu operasyon ile eş zamanlı olarak Rusya'dan Gürcistan'ın kritik hizmetlerinin altyapısına DDoS saldırıları yapılmıştır. Bu saldırılar, Gürcistan'ın hükümet, medya ve finans sektörlerini felç etmeye yönelik olarak tasarlanmış ve yapılmıştır. Bu saldırıların en önemli özelliği, askeri operasyonlar ile birlikte yapılması ve dolayısıyla tarihte hem askeri hem de siber savaşların aynı anda yapılması nedeniyle ilk hibrit savaş olma özelliği taşımasıdır. (Darıcılı, 2014: 8)

Rusya'nın dağılan SSCB'nin en kuvvetli mirasçısı olması, özellikle eski SSCB ülkelerini politik olarak baskı altına alma çabaları, buna karşılık Estonya, Litvanya, Kırgızistan ve Ukrayna gibi eski SSCB ülkelerinin Batı yanlısı politika izlemek istemesi gibi nedenler, Rusya'dan bu ülkelere yönelik siber saldırılar gerçekleşmesine neden olmaktadır. Ancak Rusya, Gürcistan ve Ukrayna'da olduğu gibi askeri operasyonlarını siber operasyonlarla desteklemekte ve böylece yeni bir savaş doktrini üretmektedir. (Darıcılı, 2014: 10)

Rusya kaynaklı siber savaşların yanı sıra 2008'de Kuzey Kore'nin inşa etmek istediği Suriye deki nükleer tesisin altyapısını İsrail bilişim sistemlerini kullanarak yok etmesinde, Pakistan-Hindistan arasındaki sorunlu bölge Kaşmir anlaşmazlığında, İsrail-Filistin çatışmalarında kullanılan yoğun siber saldırılar, rakip devletler arasındaki siber çatışma örnekleridir. (Kurnaz, 2016: 65)

3.3. Siber Suç

İnternetin yaygınlaşması ve hatta çağın gerçeği haline gelmesiyle birlikte internetin kötü amaçlarla kullanımı da yaygınlaşmaya başlamış ve bunun sonucunda da siber suçlar denilen yeni bir suç türü ortaya çıkmıştır. Bu suçların doğası gereği fiziksel ortamda işlenen suçlardan farklı nitelikte olması nedeniyle literatürde siber suç denilen yeni bir suç türü ortaya çıkmıştır. Emniyet Teşkilatı kaynaklarında internete kapsamında, internete has suçlar olarak anılan bu yeni suç türü, kimi çalışmalarda bilişim suçu, elektronik suç, bilgisayar suçu, dijital suç ya da ileri teknoloji suçları benzeri terimlerle

ifade edilebilmektedir. İşlenen suçun kapsamının oldukça geniş olması sebebiyle bu suçların farklı durumlarda ve içerikte olması mümkündür. (Taşçı ve Can, 2015: 233)

Siber güvenlik tehditlerinin, gerçek dünyada tanımlanabilen, belirgin, açık ve somut bir tanımı bulunmamaktadır. Siber saldırganlar ergen ve hatta çocuk olabileceği gibi terörizme destek veren haydut devletler, terörist kişiler veya kendi menfaatlerine göre davranan ülkeler de olabilmektedir. Siber tehditler, bir merkez bağlı olmaksızın karmaşık bir yapıda olduğundan, kötü niyetli siber saldırganların tehditleri doğrulanamamakta ve gerçekçiliği kanıtlanamamaktadır. Bir ağa bağlanabilen ve bilgisayar sistemlerine sahip olan herhangi bir kişi, dünyanın herhangi bir yerindeki kişinin ya da kurumun bilgisayarına kısa sürede erişebilmekte ve bu bilgisayarları kendi çıkarları uğruna kontrol edebilmektedir. Dolayısıyla teknoloji kötü niyetli ellerde bir silaha dönüşebilmektedir. Siber suç tehditleri genel olarak virüsler ve kötücül yazılımlar, keyloggerler, hacking, spam ve hizmet engelleme saldırıları olarak sınıflandırılabilmektedir. (Kurnaz, 2016: 65-66)

Yerli literatürde siber suç ile bilişim suçları yaygın olarak aynı anlamda kullanılmaktadır. Ancak hem yerli hem de uluslararası literatürde siber suç kavramının içeri konusunda yaygın bir mutabakattan söz etmek mümkün değildir. Buna rağmen siber suçları basitçe bilişim sistemleri aleyhine ya da bilişim sistemleri vasıtasıyla işlenen suçlar olarak tanımlamak mümkündür. (Önok, 2013: 1233)

Bilişim teknolojilerinde yaşanan günlük gelişmeler nedeniyle her an yeni bir suç türüyle karşılaşılabilen siber dünyada, bilgi toplumu ve suç alışkanlıklarının bir sonucu olarak siber suç ile ilgili olarak yapılmış net bir tanım bulunmamaktadır. Ülkeler siber suçları ayrı bir bölüm içinde düzenleyebildiği gibi mevcut suçların tanımlarına dijital ortam ibaresi ekleyerek de açıklayabilmektedir. Siber suçlar en genel ifadeyle bilgisayar üzerinde işlenen suçlardır. Ancak ceza hukukunda suçu tanımlamak için suç aracının suç adı oluşturması düşünülemez. Çünkü iyi niyetli amaçlar uğruna icat edilen ATM, POS cihazı, cep telefonu gibi araçlar, suçun aracı olabilmektedir. Evlerin bile gittikçe akıllandığı günümüz dünyasında günlük kullanılan ev eşyaları dahi siber suçlar için kullanılabilmektedir. Örneğin akıllı ev sistemlerinde bulunan internete bağlanabilen buzdolapları, müzik çalarlar ve uydu alıcısı gibi cihazlar suça aracı olabilmektedir.

Siber suç konusunda yapılan çalışmaların bir kısmında suçluya odaklanırken, bir kısım çalışmalarda ise özel suç davranışlarına odaklanmaktadır. Her iki yaklaşıma göre de ana problem, bu tanımların internetin yaygınlaşmaya başladığı dönemin başlangıcında yapılmış olmasıdır. Ancak sonuç olarak siber suçları geleneksel suçlardan ayıran birtakım faktörler vardır. (Tanılır, 2002: 45)

Tablo 3: Geleneksel / Siber Suç Farklılıkları

Geleneksel Suç	**Siber Suç**
Gerçek zaman içinde meydana gelme eğilimi göstermektedir.	Siber suçlar, zaman, mekân ya da yerden bağımsız olarak meydana gelmekte ve kolayca tanımlanabilecek sınırlara sahip değildir.
Tanımlanmış coğrafik ve sosyal sınırlar dahilinde meydana gelme eğilimi göstermektedir.	Siber suçlar anlıktır.
Dolandırıcılık ve beyaz yaka suçlarının çoğu hariç, geleneksel suçlarla ilgili tartışmaların esas olarak toplumun alt sınıflarına dahil olan bireyler üzerinde odaklanmaktadır.	Üzerinde uzlaşılan değer ve ahlak yargılarının olmaması nedeniyle tartışmalıdır.
Neyin suç oluşturduğu ya da neyin suç oluşturmadığına dair bir uzlaşının hâkimdir.	Kanunlaştırma için önemli ölçüde teknik bilgi gereklidir.
Geleneksel suç biliminin, suç veya mağdurdan ziyade genellikle suçlu odaklıdır.	Neyin suç oluşturduğu ya da neyin suç oluşturmadığına dair bir uzlaşı yoktur
	Siber suç üzerindeki tartışmalar büyük ölçüde suç odaklıdır.

Kaynak: M. Niyazi Tanılır, *İnternet Suçları ve Bireysel Mahremiyet*. Ankara: Liberte Yayınları, 2002, s. 45. den derlenmiştir.

Gerçek dünyada suçluların hedefi çoğunlukla parasal değeri ifade edilebilen nakit, taşınabilir elektronik cihazlar, otomobil, mücevher gibi somut varlıklar ya da doğrudan gerçek kişi ya da hayvandır. Buna karşılık siber uzaydaki hedef, dijital ortamda depolanan ya da aktarımı yapılan, soyut nitelikteki bilgi varlığıdır. Gerçek dünyada her nesne aynı anda tek bir yerde bulunabilmektedir. Ancak siber dünyada bilgiler bire bir aynı olacak şekilde kopyalanabilir, silinerek ortadan kaldırılabilir. Bu nedenle ağa bağlı olan bir bilgisayarda depolanan bilgiler, yetkisiz erişimi sağlayanlar tarafından değiştirilme, kopyalanma, silinme ya da çalınma gibi risklerle karşı karşıyadır.

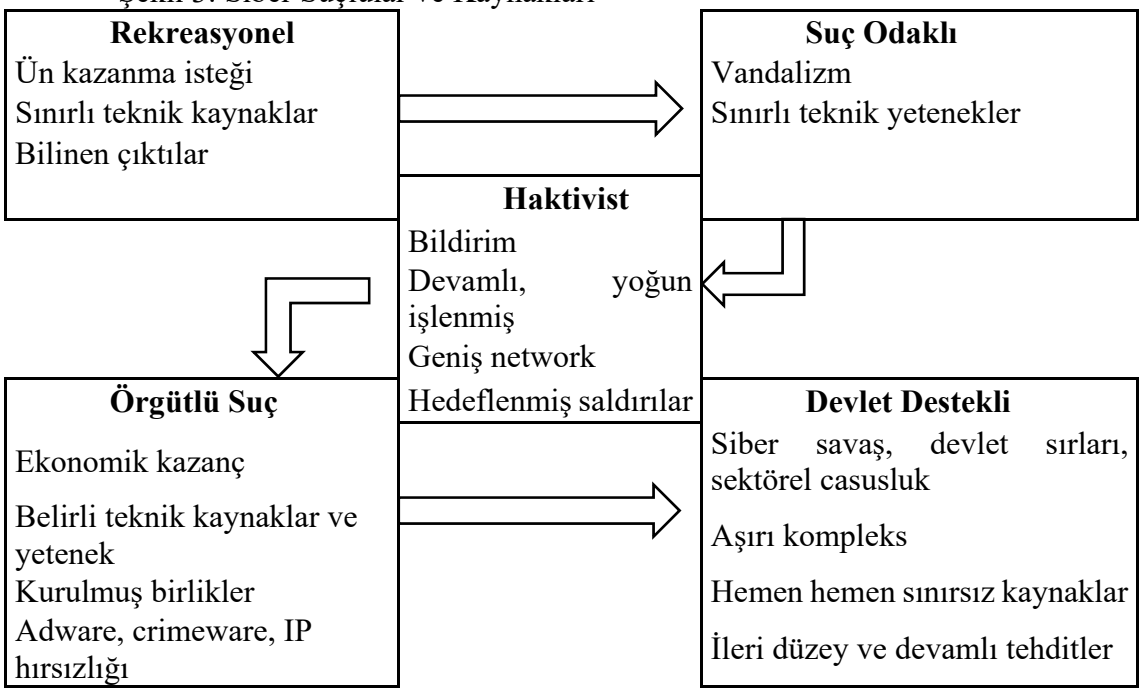
Bilginin siber uzaydaki varlığı soyuttur. Bilginin somut hale gelmesi dijital ortamdaki kaydı ya da yazılı olarak basılmış halidir. Siber uzaydaki değer, maddesel değerden ziyade fikirlerin ifadesiyle ilgilidir. Siber suçluların hedefi, paha biçilemeyen

nitelikteki fikri mülkiyete erişebilmektir. Siber uzayda bilgi, bireyin kimlik numarası, banka hesap ve kredi kartı bilgileri, özel hayatı ve iletişimi gibi kişiye özel verileri olabilmektedir. Bir şirketin fikri mülkiyet bilgileri, projeleri, güvenlik sistemleri, askeri savunma sistemleri, ulusal veri bankaları gibi bilgi varlıkları da siber suçun alanına girebilmektedir.

Siber suçların failleri, sanal dünyanın hukuk kurallarını ihlal eden siber sakinleridir. İnternetin yaygınlaşmaya başladığı günlerden bu yana hacker terimi, siber suçluları ve siber dünyada sapkınca davranışlarda bulunanları temsil etmek üzere geniş ölçüde kullanılan bir tabir olmuştur. Hackerler, tüm bilgilere giriş özgürlüğü olduğuna inanan ve yüksek seviyede uzmanlık gerektiren bilgiye sahip olan "beyaz şapkalı" ya da "siyah şapkalı" kimselerdir. (Tanılır, 2002: 47) "Beyaz şapkalı" hackerler, yüksek seviyedeki uzmanlıklarını sistemlerin açıklarını tespit edip bunu ilgili kurumlara ve birimlere raporlayan, dolayısıyla yeteneklerini iyi bir amaç uğruna kullanan kimselerdir. Buna karşılık "siyah şapkalı" hackerler ise yüksek seviyedeki uzmanlık gerektiren bilgilerini, sistemlere girmek, sistemdeki bilgileri değiştirmek, şifrelemek, silmek veya silmemek için para talep etmek gibi etik olmayan davranışlar sergileyen kimselerdir. (Akkaya, 2014:50)

Şekil 3'te siber suçlular ve kaynakları görülmektedir.

Şekil 3: Siber Suçlular ve Kaynakları



Kaynak: Vahit Güntay, "Ulusal Güvenlik Çerçevesinde Siber Güvenlik Yaklaşımı Oluşturma Sorunu" *Siber Politikalar Dergisi*, Cilt: 1, Sayı: 1, 2016'dan esinlenerek oluşturulmuştur.

Genel hatlarıyla siber suçları şu şekilde sınıflandırmak mümkündür: (Tanılır, 2002: 53)

Siber Hırsızlık: Klasik hırsızlığın bilişim sistemleri aracılığı ile yapılmasıdır. Genellikle suç işleyenler, mağdurun banka hesabını boşaltma, kredi kartını izinsiz olarak kullanma gibi faaliyetler yoluyla mağdurun doğrudan malvarlığına göz dikmektedir.

Nitelikli Dolandırıcılık: Klasik dolandırıcılık suçunun internet ortamında işlenmesidir. İnternet kullanılarak hileli davranışlar yolu ile mağdurun aleyhine olacak şekilde sonuçlar doğuran işlemlerdir. Örneğin internetten bir ürün satın alındığında gelen ürünün hiçbir ekonomik değerinin olmaması ya da daha düşük kıymette bir ürün gönderilmesi; internet üzerinden ev ya da araba satışında peşinat ya da kaparo gibi ön ödeme alınmasına rağmen satışın gerçekleştirilmemesi gibi eylemler nitelikli dolandırıcılığa girmektedir.

Bilişim Sistemine Yönelik Suçlar: TCK'nın 243 ve 244. Maddelerinde düzenlenen sisteme izinsiz ve yetkisiz girme ve sistemde bulunma suçları ile sistemi engelleme, verileri bozma, yok etme ya da değiştirme suçlarını kapsamaktadır.

Çocuk İstismarı / Çocuk Pornosu: Çoğu zaman 15 yaşını dahi doldurmamış çocukların cinsel yönden istismar edildiği yazı, fotoğraf ya da videoları içeren ürünlerin bilişim sistemleri yoluyla depolanması, bulundurulması, yayılması, satışı, kiraya verilmesi gibi suçları içermektedir. Çocuk istismarına yönelik pornografik içeriklerin üretilmesi ve dağıtılması Birleşmiş Milletler ve Avrupa Konseyi Siber Suçlar Sözleşmesi tarafından yasaklanmıştır.

Banka veya Kredi Kartlarının Kötüye Kullanımı: TCK'nın 245. Maddesinde düzenlenmiştir. Kendisine ait olmayan banka ve kredi kartlarını ne şekilde olursa olsun elde eden ve bulunduran bunları asıl sahiplerine haber vermek ve teslim etmek zorundadır. Ayrıca bu kartları kopyalamak, başkasına devretmek ya da satmak da siber suç kapsamına girmektedir.

Sanal Kumar: Ülkemizde kumar oynama ve oynatma suçtur. Bu suçun internet üzerinden işlenmesi de aynı kapsamdadır. Bu nedenle internet üzerinden kredi kartı veya para yerine geçen elektronik ödeme sistemlerini kullanarak kumar oynanmasına imkân tanınması da suçtur.

Elektronik İmza İhlali: Sahibinin rızası dışında elektronik imza verisi oluşturmak, kopyalamak, belgeleri imzalamak, elektronik imza cihazlarının elektronik sertifikalarını tahrif ya da taklit etmek siber suç kapsamına girmektedir

Bilgi Güvenliği Yükümlülüğüne Muhalefet: Ticari faaliyetler sonucunda elde edilen ticari sırların, yetkililerin ya da sahiplerinin bilgisi olmaksızın elde etmek, diğer kişiler için değer ihtiva eden bilgileri elde ederek şahsına ya da başkasına çıkar sağlamak ya da zarar oluşturmak, elde ettiği bu bilgileri satmak ya da gizliliğini deşifre etmek siber suç kapsamındadır.

Haberleşmenin Engellenmesi: Bilişim sistemleri kullanarak haberleşmeyi ve her türlü basın yayın organının yayınlarını engellemek suçtur. Ayrıca kamu kurum ve kuruluşları arasındaki haberleşmeyi takip ederek dinlemek ya da yazışmaları ele geçirmek de bu kapsama girmektedir.

Ekonomi, Sanayi ve Ticaret Karşı Suçlar: Mesleği ya da konumu gereği öğrendiği ticari sırları, müşterilere ait bilgileri ya da bankacılık işlemlerini yapmasına imkân tanıyan bilgileri yetkisiz ve ilgisiz taraflara verme ya da satma ve bu bilgileri ifşa etme siber suç kapsamına girmektedir.

Özel Hayatın Gizliliğine Karşı İşlenen Suçlar: kişiler arasındaki haberleşme içeriğinin dinlenmesi, kaydedilmesi, ifşa edilmesi, tarafların rızası dışında ifşa edilmesi, görüntü alınması, bir ortamdaki söyleşinin habersiz olarak kayıt altına alınması, kişinin özel hayatına ilişkin fotoğraf, video ve seslerin kayda alınarak bilişim sistemleri aracılığı ile yayılması özel hayatın gizliliğine karşı işlenen suçlar kapsamına girmektedir.

Devlet Sırlarına İlişkin Suçlar (Casusluk): Devlet sırrı niteliğindeki her türlü bilgi, belge, teknik buluş, sınai üretim gibi verilerin olduğu sistemlere bilişim sistemleri aracılığı ile sızma, verileri elde etme, başka ülkelere transfer edilmesi gibi eylemlerdir.

Fikir ve Sanat Eserleri Kanununa Karşı Suçlar: Bir eserin hak sahibinin izni olmaksızın kopyalanması ve dağıtılması ile telif hakları ile korunan yazılımların üretici firmanın bilgisi dışında kopyalanması, lisansının kırılması gibi faaliyetlerdir.

Yasadışı Yayınlar ve Terörist Faaliyetler: Ulusal ya da uluslararası yetkili merciler tarafından terör örgütü kabul edilen grupların propagandasını, örgüt içi haberleşmesini, sempatizan kazanmasını, toplumda korku oluşturmaya yönelik çabalarını destekleyici nitelikte faaliyetlerde bulunmak bu kapsama girmektedir.

Dicle ve 19 Mayıs Üniversitesinde yapılan araştırmaya göre, normal yaşamda suç olarak görülen durumların yetkili mercilere yansıtılmasının, sanal ortamdaki ihbarı düşük seviyede olduğu belirlenmiştir. (%12,2) (Ateş ve Tokay,2018 :29)

II. BÖLÜM
BİLGİ GÜVENLİĞİ UYGULAMALARININ BİREY DÜZEYİNDEKİ YANSIMALARI

1. TEKNOLOJİ VE İNSANIN BİRLİKTE YÖNETİMİ

İşletmelerin rekabette öne çıkabilmesi ve ilerleyebilmesi, kapasitesini artırabilmesi amacıyla ne çeşit teknolojilere nasıl bir durumda yatırım yapabileceğini, sürekli gelişen teknolojilerden nasıl bir şekilde üretilebileceği ve bunu ne çeşitte pazarlanacağı, kurumun organizasyonel yapısında teknolojinin gelişmesine bağlı olarak nasıl bir değişiklik yapılacağının belirlenmesi gibi konularla ilgilenen teknoloji yönetimi, yalnızca teknik faaliyetlerden değil aynı zamanda teknoloji üreten ve o teknolojiyi kullanan kişilerin yönetimini de kapsamaktadır. (Karadal ve Türk, 2008: 66)

Teknoloji yönetimi ile organizasyonun stratejik amaçlarının belirlenmesi ve bunlara ulaşmak için ihtiyaç duyulan teknolojinin planlanması, geliştirilmesi ve uygulanması mümkün olmaktadır. Teknolojinin işletmeye olan adaptasyonu ve yönetimi, o teknolojinin üretimi kadar önemlidir. Bu durum işletmeler için hem arzu ettikleri hem de en çok zorlandıkları konuların başında gelmektedir. Bu nedenle teknoloji yönetiminde insan unsuruna dikkat çekilmektedir. Teknoloji yönetiminde nihai olarak kararı verecek olan yüksek teknik bilgiye sahip insan olduğuna göre, etkili bir teknoloji yönetimi teknoloji ile insanın birlikte yönetimi ile mümkün olmaktadır. (Öğüt, 1999: 18)

İşletmelerde kullanılan teknolojinin firmanın örgüt yapısını dahi etkilediği göz önüne alındığında, kullanılan teknolojinin örgüt yapısıyla uyumlu hale getirilmesi ve verimlilik artışı teknoloji yönetimi sayesinde mümkün olabilmektedir. Değişen teknolojik gelişimlere ayak uydurulması, teknolojiyi işletmeye adapte etmek kadar, o teknolojiyi kullanacak personelin de gelişimini zorunlu kılmaktadır. Bu nedenle teknolojik gelişmeler işletmeye adapte edilirken, çalışanların eğitimi atlanmamalıdır. Dolayısıyla işletmeler için sadece teknoloji yönetimi değil, teknolojinin insan ile birlikte yönetimi söz konusudur. (Demir ve Okan, 2009: 58) Değişen teknolojiye ayak uydurmuş işletmelerin, bilgi yönetimi kapsamında siber güvenlik konusunda tedbirlerini baştan alarak siber suçlardan en az etkilenmesi mümkün olmaktadır.

2. BİLGİ GÜVENLİĞİ UYGULAMALARINDA BİREYİN ROLÜ

Bilgi güvenliğine yönelik tehditler ve vakalar son yıllarda önemli ölçüde artmıştır. Artan tehditlerle başa çıkabilmek için yalnızca teknik çözümler değil, aynı zamanda güvenlik politikaları da olmak zorundadır. Bununla birlikte, çalışanlar bu politikalara nadiren uymakta ve örgütlerinin varlıklarını ve işletmelerini riske atmaktadır. (Siponen, vd, 2014: 217) Bu endişeyi gidermek için önceki bölümde bahsedildiği üzere birkaç bilgi güvenliği politikası standardı oluşturulmuştur.

Güvenlik teknolojilerinin gelişmesiyle birlikte teknik açıkları kullanabilmek daha da zorlaşmaya başladığından, saldırganlar bilgi güvenliği uygulamaları sürecinde zafiyet düzeyi en yüksek bağlantı noktası olan insan faktörünü baskı altına almaya çalışmaya başlamıştır. Herhangi bilişim - iletişim sistemi içinde bilgilere - verilere sahip olabilmek, bilgileri - verileri kullanabilmek ya da bilişim - iletişim sistemini yöneten olmak kişiyi bilgi güvenliği konusunda sorumlu kıldığından, bilgi güvenliği konusunda farkındalığa sahip olmak, suiistimallerin ve kasıtlı tehditlerin önüne geçilmesinde ilk adım olabilmektedir. (Keser ve Güldüren, 2015: 1169)

Bilgiye erişimin değerli olduğu kadar, onu korumak da bir o kadar değerlidir. Bu nedenle şahsi bilgi ve verilerin gizliliğinden başlayarak örgütlerin işletme sırlar – know how , fikri mülkiyet haklarına kadar ulaşabilen skalada bireylerin internet, sosyal medya ve iletişimlerinde bilginin değeri önlenemez biçimde artmıştır. Bilgi toplumuna geçiş ile birlikte bireyler, kurumlar, topumlar ve devletler, sahip olduğu maddi manevi değerlerin yanında bilgi çağının bir ürünü olan bilgiyi ve değerini korumayı da başarmak zorundadır. (Evrin ve Demirer, 2011: 25)

İşletmelerde bilgi güvenliği uygulamalarındaki asıl amaç, en öncelikle kurum iş görenleri olması kaydıyla tüm paydaşların, kurumun en değerli varlığı olan bilginin korunmasında üzerine düşen görev ve sorumlulukları anlamalarını sağlamaktır. Kurum için kritik öneme sahip olan bu durumdan, kurumun bilgi güvenliği politikasında açıkça tanımlanan çalışanları, paydaşları ve hatta tedarikçileri olmak üzere tüm bireyler sorumludur. Kurumların bilgi güvenliğinde bilginin ne tür saldırı ve tehditlere karşı korunması gerektiği konusundaki bilinçlendirme çalışmaları yapılmalıdır. Bu nedenle

kurumlarda nasıl ki her çalışan iş tanımında yer alan görevlerden sorumlu tutulmaktaysa, aynı şekilde bilgi güvenliğini de iş görevi olarak sorumlu tutulmalıdır. (Şahinaslan, 2009: 598)

Bilgi güvenliği eğitim ve teknoloji gibi faktörlerin yanı sıra insan faktöründen de etkilenmektedir. Bu nedenle bireysel aktörlerin ve kurum içinde çalışanların yönetimi ile ilgili konuların ihmali, bilgi güvenliğini olumsuz etkilemektedir. Bilgi güvenliği, bilgiye erişimin kolay olduğu bir ortamda bilginin göndericisinden çıkıp alıcısına ulaşana kadar gizliliğinin sağlanması, içeriğinin bozulmadan alıcısına ulaşması ve üçüncü kişiler tarafından ele geçirilmeden güvenli bir şekilde iletilmesi sürecidir. Bilgiyi kullanan da insan olduğuna göre, en ufak bir ihmalkârlık, bilgi güvenliğini tehlikeye düşürmektedir. (Kurnaz ve Dindaroğlu, 2015: 54)

Bilgi güvenliği konusundaki en büyük ihmallerden biri, bireyin, kurumun ya da kuruluşun genellikle başlangıç safhasında disiplinli bir şekilde önleyici tedbirler almaktansa, tehlikeli saldırı veya tehdit meydana geldiğinde, güvenlik konusunada karşı tedbirler alma eğiliminde olmasıdır. Bundan dolayı özellikle bilgi güvenliğinden sorumlu yöneticilerin, sonrasında ise tüm çalışanların bilgi güvenliği farkındalığı, bilgi güvenliği kültürünün oluşumuna da olumlu etki etmektedir. (Yılmaz, vd, 2016: 27)

Bilginin yönetimi kadar bilgi - verilerin güvenlik altına alınması da olabildiğince komplike bir prosestir. Kurumsal - kişisel bilgilerin güvenliğinin yalnızca güvenlik duvarı, VPN, anti virüs gibi teknik önlemlerle sağlanması mümkün değildir. Bu nedenle bilgi – veri güvenliklerinin oluşturulmasında sadece teknik baza dayanan tedbirlere ilave olarak da çalışan – insan unsurunu da dikkate alarak bilgi güvenliği konusundaki farkındalığı artırmak, bilgi güvenliği konusundaki en temel çıkış noktasıdır. (Güldüren, vd, 2016: 684)

Bilgi güvenliği konusundaki en büyük yanlış inançlardan biri de bilgi güvenliğinin yalnızca bilişim uzmanlarının sorumluluğunda olan bir konu olmasıdır. İnternetin kanuni olmayan metotlarla üçüncü kişilerden ya da işletmelerden yaralanmayı amaçlayan iyi niyetli olmayan birçok kişiye geniş olanaklar sağladığı malumdur. (Akgün ve Topal, 2015: 99) Bilginin adeta açık hedef haline geldiği günümüzde siber suçlara meyilli bilişim korsanlarının son kullanıcılara ait bilgisayarlara da saldırı düzenlemeleri

adeta vaka-i adiyedir. Bu nedenle, konuyu yalnızca bilişim uzmanlarının sorumluluğuna bırakmak, konunun önemini yeterince kavrayamamaktır.

Bilgi teknolojileri konusunda yapılan bir başka yanlış, kurumlardaki projelerde güvenliği en başta projeye katmaktansa, projenin sonunda ve alelacele projeye katılması, bu durumun da analiz, tasarım, test ve kontrol süreçlerinde projeye olumsuz yansımasıdır. Hâlbuki bilgi güvenliği, projelerin en sonuna eklenebilecek bir yama değildir. Bu yaklaşım bilgi güvenliğini tehlikeye attığı gibi projeyi de başarısızlığa uğratacaktır. Bu nedenle bilgi güvenliği en baştan itibaren sürecin doğal bir parçası olmalıdır. (Eminağaoğlu ve Gökşen, 2009: 9)

Bilgi güvenliğinde iş görenlerin bilgi ve veri yaklaşım şekilleri, davranışları, görüşleri, tutumlar normal sınırların üzerinde olmalıdır. Ayrıca bilgi güvenliği, yalnızca bilişim uzmanlarının eline bırakılmamalı, aksine tüm örgütün gün içindeki aktivitelerinin her bir noktasında olmalıdır. İş görenlerin veri -bilgi güvenliği konusundaki davranış ve tutumları, kurumun bilgi güvenliği kültürünün oluşumuna da katkı sağlayacaktır. (Karadağ ve Abuhanoğlu, 2015: 385)

3. BİLGİ GÜVENLİĞİ BAĞLAMINDA KRİTİK UNSURLARIN ANALİZİ

Bilgi güvenliğinde farkındalık, bilginin şahsi veya işletme düzlemde güvenliğinin temin edilebilmesi adına veri - bilgilerin kaynağına ve güvenlik sistemine hedef alan tehditlerin ve bu tehditlerin meydana getirebileceği sonuçların kavranmasıdır. Bu farkındalık, kullanıcıların karşılarına çıkan her linke tıklamamalarını, kötü amaçlı yazılımları fark ederek yüklememelerini ve orijinal yazılım kullanarak kırılmış (crack yapılmış) yazılımları kullanmamalarını sağlamaktadır. Bu sayede saldırganların kötü niyetlerinden uzak durarak bilgi sızıntısına alet olmamaları, kişisel ya da kurumsal bilgilerin kaybedilmemesi ve kişisel ve kurumsal itibar kaybına uğramaması mümkün olmaktadır. (Erol, vd, 2016: 8)

Bilgi teknolojilerinde insan unsuru, bilgi güvenliğinin temel ögesidir. Bilgiyi hem üreten, hem kullanan, hem koruyan olarak insan, bilgi güvenliğindeki kayıp ve zararı, açık ve sorunları azaltmak için özel çaba sarf etmek zorundadır. (Eminağaoğlu ve Gökşen, 2009: 7) Ancak maalesef temel sorun, bireylerin ve toplumun bilgiye ve bilgiye sahip olanlara karşı takındığı tavırdır. Bilginin en büyük güç olduğuna inanan bir

toplumda onu korumak da daha kolay olabilecektir. Ancak bilgiden ziyade güce tapanların olduğu bir toplumda, bilgi güvenliğine önem verilmemesi de normaldir.

Bilgiyi üretirken kullanılan en önemli araç hiç şüphesiz teknolojidir. Örgütlerdeki insan kaynakları ihtiyacında da teknolojiden faydalanılmaktadır. Kurumda var olan çalışanlar ile var olan iş tanımları, iş süreçleri çıkarılırken teknolojiden faydalanılmaktadır. İşin tanımı, işin gereklilikleri gibi bilgiler ile adayların nitelikleri işe alım süreçlerinde toplanan verilerdir ve bu veriler karşılaştırılarak en uygun adayın seçimine çalışılmaktadır. Dolayısıyla adayların kişisel bilgilerinin ve niteliklerinin toplanması durumu söz konusudur. Bilgi güvenliğine verilen önem, adayın kişisel verilerinin güvenliğinin sağlanması ile başlamaktadır. (Saldamlı, 2008: 248)

Kurum içindeki bilginin paylaşımında kurum içi ağlar (intranet) etkilidir. Doğru bir yapılandırma ile intranet, bilgi paylaşımını son derece etkin bir hale getirebilmektedir. İntranetin etkinliğinde bilgi üretebilme yeteneği de önemlidir. Çünkü bilgiyi üretebilmek, teknolojinin değil bir kültürün sonucudur. Kurumsal bir bilgi kültürünün yaratılmasıyla kurumun insan kaynaklarının sanal ortamda buluştuğu bir alan ortaya çıkarılabilmektedir. Diğer bir ifadeyle kurum içi ağlar, işletmenin bilgi üretim sisteminin kalbidir. (Özdemirci ve Aydın, 2007: 170)

Teknoloji ile insan kaynaklarının bir araya gelmesinden ortaya çıkan ürün İnsan Kaynakları Bilgi Sistemleridir (HRIS-Human Resources Information Systems). HRIS, insan kaynakları işlevi için gerekli olan veri tabanları, bilgisayar uygulamaları ve donanım ile yazılımlardan oluşan, insan kaynakları ile ilgili olmak üzere verileri toplamak, kaydetmek, saklamak, yönetmek, dağıtmak ve sunmak amacıyla kullanılan bütünleşik bir sistemdir. (Shibly, 2011: 158)

HRIS ile uzun vadeli planlar, işgücü planlamaları ve arz ve talep tahminleri bilgi ile desteklenebilmektedir. İşe alım ve işten ayrılmalar, başvuru sahibinin nitelikleri hakkında bilgi sahibi personel desteği verebilmektedir. Ayrıca tazminat programları, maaş tahminleri, maaş bütçeleri ve toplu sözleşme müzakereleri hakkında bilgi sağlayabilmektedir. (Shibly, 2011: 158)

HRIS, yetenekli çalışanları çekmek, işe almak, korumak ve işten ayrılmamasını sağlamak, işgücü yönetimini desteklemek ve işgücü yönetimini optimize etmek için kullanılmaktadır. Kısaca HRIS, insan kaynaklarının sorumlu olduğu idari ve stratejik

değişkenlerin organize edilmesine yardımcı olmaktadır. Günümüzde HRIS adeta insan kaynaklarında bilgi teknolojilerinin kullanımına ve şirket stratejisinin geliştirilmesi ve uygulanmasına katılarak, değer yaratmanın anahtarı haline gelmiştir. (Barut, Değerlioğlu, 2010: 877)

HRIS'in faydalarını şu şekilde sıralamak mümkündür. (Jahan, 2014: 34)

- Verilerin alınması ve işlenmesinin daha hızlı olması.
- Maliyetlerin azaltılmasına olanak tanıyan verimsiz çabaların azaltılması,
- Verilerin sınıflandırılmasında ve tekrar sınıflandırılmasında kolaylık sağlanması.
- Daha etkili bir karar vermeye yol açan daha iyi analiz.
- Daha yüksek üretilen bilgi / raporun doğruluğu.
- Soruları cevaplamak için hızlı tepki.
- Geliştirilmiş rapor kalitesi.
- Daha iyi iş kültürünün olması.
- Akıcı ve sistematik prosedürün oluşturulması.
- Sistemde daha fazla şeffaflık.

3.1. Bilgi Güvenliği Farkındalığı Yaratma

Faydalı ve verimli çalışan bilgi güvenlik anlayışı ve farkındalığı yaratma prosesi ve eğitimi oluşturabilmek amacıyla bilgi güvenliğinden sorumlu olan yöneticilerin görev ve sorumlulukları açıkça belirlenmelidir. Süreç, kurum içindeki en üst seviyeden en alt seviyedeki çalışana kadar katılımı zorunlu kılmaktadır. Bilgi güvenliği farkındalığı yaratma sürecinden üst yönetim esas sorumludur. Üst yönetim, bu sorumluluğu yerine getirmek için bir bilgi güvenliği yöneticisi görevlendirmektedir. Bilgi güvenliği yöneticisi ise bilgi güvenliği bilinçlendirme süreci sorumlusu görevlendirerek taktik ve uygulama seviyesinde sürecin hayata geçirilmesinden sorumlu olmaktadır. Bölüm yöneticileri ise bilgi güvenliğinin farkındalığının yaratılması sürecine kendi bölümündeki personelinin katılımını ve uymasını sağlamaktadır. Nihai olarak çalışanlar ise bilgi güvenliği farkındalığı yaratma sürecinin hedef kitlesidir. (Önel, 2008: 6)

Bilgi güvenliği farkındalığının yaratılması üç temel aşamada gerçekleşmektedir. Bu aşamaları sürecin planlanması ve tasarlanması, bilinçlendirme ve eğitim materyalinin geliştirilmesi ve son olarak sürecin uygulanması olarak sıralamak mümkündür.

Farkındalık yaratma ve eğitim materyalinin geliştirilmesinde kurumun kendi imkanlarından faydalanılabildiği gibi diğer kurum ya da kuruluşların çalışmalarından da uyarlama yapılabilir. Ayrıca eğitim kuruluşlarından hazır olarak satın almak da mümkündür. Ne şekilde temin edildiğinden bağımsız olarak personele nasıl bir davranış şekli kazandırılacağı ve hedef kitleye kazandırılabilecek yetenekler göz önünde bulundurulmalıdır.

Farkındalık yaratabilmek için öncelikle hangi konularda farkındalık yaratılacağı belirlenmelidir. Parola kullanımı, virüs ve zararlı yazılımlardan korunma, acil durumlarda müdahale, bilgi sisteminin tanıtımı, yazılımların lisansları, kurum içinde izin verilen lisanslar vb. gibi konularda bilinçlendirme yaratılabilir. Bilinçlendirme materyalleri, sektör ile ilgili e-posta grupları, akademik makaleler, profesyonel bilgi güvenliği kuruluşları, bilgi güvenliğine yönelik web siteleri, süreli yayınlar ve konferanslardan faydalanılabilir.

3.2. Bilgi Güvenliği Teknik Eğitimlerinin Alınmasını Sağlamak

Sürecin uygulamaya konmasında yeterli desteği elde edebilmek için planın kurum çalışanlarına anlatılması gereklidir. Bu sürece neden ihtiyaç duyulduğu ve süreçten elde edilecek kazanımlar vurgulanmalıdır. Sürecin maliyetinin nasıl karşılanacağı belirlenmeli ve süreçte görev alacak personel net bir şekilde belirlenmelidir. Sürecin uygulanabilmesi için bilgi güvenliği bilinçlendirme ve eğitim materyalinin kurum çapında nasıl dağıtılacağı belirlenmelidir. Bu amaçla materyaller, kalem, not kağıdı, kahve fincanı, fare altlığı gibi nesnelere yazılabilecek uyarıcı mesajlar, uyarıcı ve bilgilendirici posterler, ekran koruyuculara yazılacak bilgi güvenliğine yönelik mesajlar, kurum gazetesi ya da dergisine yazılabilecek yaşanmış öyküler, belli aralıklarla kurum içi mesajlaşma sistemine ya da e-posta hesaplarına gönderilecek mesajlar, seminerler vb. kullanılabilir. Ayrıca eğitim materyallerinin sunumu için de interaktif video, web ve bilgisayar tabanlı eğitimler ile sınıf içi eğitmenler eşliğinde eğitimler uygulanabilmektedir.

Kurumun bilgi güvenliği politikasındaki eğitim ve bilinçlendirme programını ilgilendiren maddeler, programın kapsamı, programı geliştiren ve programın sunulacağı personelin görev ve sorumlulukları, hedef kitle, ulaşılmak istenen kurumsal hedefler, zorunlu ve isteğe bağlı kurs ve materyaller, eğitimler sonucunda ulaşılması istenen bilgi

ve farkındalık seviyesi ve programın hayata geçirilmesinde kullanılacak yöntemler programın ele alması gereken konulardır. (Önel, 2008: 15)

3.3. Bilgi Güvenliği Politikası Oluşturma

Bilgi güvenliği sistemi politikaları, kurum ya da kuruluşlardaki güvenlik seviyesinin tanımlanmasında kullanılmaktadır. Bu politikalar, kurum ve kuruluşlarda bilgi güvenliği için yapılması gereken tüm bilgi güvenliği ile ilgili faaliyetleri içeren talimat ve yönetmeliklerdir. İşletmenin bilgi – veri kaynaklarına ulaşabilme yetkisi olan tüm çalışanların uyması gereken kuralları içeren bu belge, her kuruluş için birbirinden farklı olmakla birlikte genel olarak çalışanların bilgi güvenliği konusundaki sorumluluklarının çerçevesini çizmektedir. (Baykara, vd, 2013: 237) Tablo 4'de Bilgi Güvenliği Sistemi Politikası görülmektedir.

Tablo 4: Bilgi Güvenliği Sistemi Politikası

Bölüm Adı	İçerik
Genel Açıklama	Politikayla ilgi gerekçeler ve buna bağlı risklerin tanımlanmasını kapsar
Amaç	Politikanın yazılımasındaki amaç ve neden böyle bir politikaya ihtiyaç duyulduğunu açıklar.
Kapsam	Politikaya uyması gereken çalışan gurupları(ilgili bir gurup veya kurumun tamamı) ve bilgi varlıklarını belirler.
Politika	Uygulanması ve uyulması gereken kuralları veya politikaları içerir.
Cezai Yaptırımlar	Politika ihlallerinde uygulanacak cezai yaptırımları açıklar.
Tanımlar	Teknik terimler ile açık olmayan ifadeler listelenerek açıklanır.
Düzeltme Tarihçesi	Politika içersinde yapılan değişiklikler,tarihlerve sebepleri yer alır.

Kaynak: Muhammet Baykara, Resul Daş, İsmail Karadoğan, "Bilgi Güvenliği Sistemlerinde Kullanılan Araçların İncelenmesi, ISDFS'13, Elazığ, 20-21 Mayıs, 2013, 238.

Bilgi güvenliği politikası, bir kurumun ürettiği ve kullandığı bilgilerin yönetimi ve korunmasını düzenleyen kurallar ve uygulamalardır. Bu kuralları içeren politikalar, çeşitli seviyelerde yazılabilmektedir. Örgütün her seviyesi için ayrı ayrı politikalar

oluşturmaktansa, tüm seviyeler için en üstte ve temel ilkelerden oluşan bir bilgi güvenliği politikası oluşturulabilir ve tüm seviyelerin ayrı ayrı politikaları, bu genel politika ile uyumlu hale getirilebilir.

Bilgi güvenliği politikası, kurumun bilgi güvenliği ihtiyacını çalışan herkese duyurabilmek için hazırlanmaktadır. Kurumdaki bilgi güvenliği ihtiyacı, kanuni düzenlemelerle de belirlenmiş olabilir. Bu gibi bir durumda yasal zorunluluklar kurumun bilgi güvenliği politikasında açıkça belirtilmelidir. (Öztürk, 2008: 6)

Genel olarak bilgi güvenliği politikası, ISO/IEC:27001 Standardı A5.1 maddesinde bir bilgi güvenliği politikasında asgari bulunması gereken konular şu şekilde sıralanmıştır:

- Bilgi güvenliğinin tanımı, kapsamı ve hedefleri,
- Bilgi güvenliğinin kurum açısından önemi,
- Bilgi güvenliğinin amacı ve güvenlik ilkeleri,
- Kontrol hedefleri için risk değerlendirme ve risk yönetimini de içeren bir genel çerçeve,
- Güvenlik politikası, ilkeleri, standartları ve uyum ihtiyaçlarının kısa bir özet açıklaması,
- Bilgi güvenliği ile ilgili tüm görev ve sorumlulukların tanımı,
- Kurum çalışanların uyması gereken kurallar,
- Alt dokümanlar için ayrıntılı politikalar ve prosedürler

Bu sıralama ışığında bilgi güvenliği politikasında yer alması gereken asgari nitelikleri ve şu şekilde açıklamak mümkündür. (Öztürk, 2008: 8)

Bilgi Güvenliğinin Tanımı: Bilgi güvenliği politikasının hedef kitlesi kurumun çalışanlarıdır. Bilgi güvenliğinin, kurum içerisinde farklı görevlerde birçok çalışan olmasından hareketle kimi çalışanlar için yabancı bir kavram olma ihtimali nedeniyle, herkesin anlayabileceği şekilde anlaşılabilir tanımının bulunması şarttır.

Bilgi Güvenlik Gereksinimi ve Bilgi Güvenlik İçeriği: Kurumda neden bilginin korunmasına ihtiyaç olduğunun açıklaması olan bu aşamada kurumun bilgi güvenliğine olan bağımlılığı vurgulanmaktadır. Bu kapsamda hangi yönetim birimlerinin ve aktivitelerinin bilgi güvenliği yapısında değerlendirileceği belirtilmektedir.

Bilgi Güvenliği Hedefleri: Ulaşılması istenen amaç ve bilgi güvenliğinin yönetimi konusunda kurum çalışanlarını bilgi vermek amacıyla kısaca tanımlanması gereken hedeflerdir. Belirlenen hedeflerin işletmenin çalışma hedefleri ile de ilişkilendirilmesi de gerekmektedir.

Risk Yönetim Sınırları: İşletmenin bilgi güvenliğine ilişkin riskleri ne şekilde yönetebildiğine ilişkin bir meydana çıkarıldığı bu aşamada bilgi güvenliğini sağlayabilmek için uygulanacak kontroller ve bu kontrollerin bağlantılı olduğu riskler tanımlanmaktadır.

Yönetimin Bilgi Güvenliğini Sağlama Sözü ve Politika Dokümanının Onayı: Kurum yönetiminin bilgi güvenliği politikasında, bu politikayı uygulamak konusunda kurumun kararlığını ortaya koyan onay imzası bulunmalıdır. Bu onay ile kurum çalışanlarının bilgi güvenliğine daha fazla önem vermesinin sağlanması amaçlanmaktadır. Onay imzası bulunmayan bir politika, kurum içerisinde çalışanlar tarafından yeterince dikkate alınmayabilir.

Bilgi Güvenliği İlkeleri: Bilgi güvenliği ilkeleri, kurum çalışanlarına çeşitli konu ve kavramlar ile ilgili olarak beklenen davranışları tanımlamaktadır.

Roller/Görevler ve Sorumluluklar: Bilgi güvenliği politikasının bu kısmı, kurumun bilgi kaynaklarını kullanan tüm paydaşların sorumluluklarını kapsamaktadır.

Politikaların İhlali ve Yaptırımlar: Bir paydaşın politikaya uymaması ya da politikaya aykırı hareket etmesi durumunda karşı karşıya kalabileceği yaptırımları belirten ifadedir. Kurumun genel disiplin politikası ile ilişkilendirilmelidir.

Diğer Kural, Yönerge, Standart ve Süreçlere Atıflar: Bilgi güvenliği politikası, tek başına değil, diğer tüm kural, yönerge, standart ve süreçler ile bir bütünü oluşturmaktadır. Paydaşların zihninde bu bütünü canlandırabilmeleri için diğer tüm dokümanlara atıf yapılmalıdır.

Bilgi Güvenliği Politikası Gözden Geçirme Kuralları: Kurumda bilgi güvenliğinin sağlanması için uygulanan kural ve alınan önlemlerin etkinliğinin kontrol edilmesi gereklidir. Bilgi güvenliği politikası da buna dahildir. Bu nedenle bilgi güvenliği politikasının etkinliğin kontrolünün de kim tarafından ne sıklıkla yapılacağı bilgi güvenliği politikası dokümanında yer almalıdır.

Tablo 5 de örnek bir bilgi güvenliği yönetimi politikası görülmektedir.

Tablo 5: Örnek Bir Bilgi Güvenliği Politikası

Bilgi Güvenliğinin tanımı	Bu politikada Bilgi Güvenliği kurumun bilgi varlıklarının aşağıdaki özelliklerinin lorunmasıolarak tanımlanır : a) Gizlilik : Bilginin sadece yetkili kişiler tarafından erişilebilir olması, b) Bütünlük : Bilginin yetkisiz değiştirmelerden korunması ve değiştirildiğinde farkına varılması, c) kullanılabilirlik : Bilginin yetkili kullanıcılar tarafından gerek duyulduğu an kullanılabilir olması,
Bilgi Güvenliği İhtiyacı ve Bilgi Güvenliği Kapsamı	Kurumumuz, satış hizmetlerinin tümünü elektronik ortamda gerçekleştirmektedir. Bu politika, kurum Bilgi İşlem altyapısını kullanmakata olan tüm birimleri,üçüncü taraf olarak bilgi sistemlerine erişen kullanıcıları ve bilgi sistemlerine teknik destek sağlamakta olan hizmet, yazılım veya donanım sağlayıcılarını kapsamaktadır.
Bilgi Güvenliği Hedefleri	Kurum yönetimi : * Kurumun güveniliriliğini ve temsil ettiği makamın imajını korumak, * Üçücü taraflarla yapılan sözleşmelerde belirlenmiş uygunluğu sağlamak, * Kurumun temel ve destekleyici iş faaliyetlerinin en az kesinti ile devam etmesini sağlamak, Amacıyla kurum bilişim hizmetlerinin gerçekleştirilmesinde kullanılana tüm fiziksel ve elektronik bilgi varlıklarının bilgi güvenliğini sağlamayı hedefler.
Risk Yönetim çercevesi	Kurumun risk yönetim çercevesi bilgi güvenliği risk/lerinin tanımlanmasını, değerlendirilmesini,işlenmesini kapsar. Risk değerlendirmesi, ugulanabilirlik bildirgesi ve risk işleme planı, bilgi güvenliği risklerinin nasıl kontrol edildiğini tanımlar.Bu planın yönetiminden ve gerçekleştirilmesinden Bili Güvenliği Koordinasyon Kurulu sorumludur.

Yönetim Bilgi Güvenliğini Sağlama Sözü ve politika Dokümanının Onayı	Kurum yönetimi olarak," Kurum Bilgi Güvenliği Politikası" nın uygulanmasının sağlanmasının ve kontrolünün yapılmasının, güvenlik ihlallerinde de gerekli yaptırımın icra edilmesinin yönetim tarafından desteklendiğini beyan ederim. Genel Müdür
Bilgi Güvenliği İlkeleri	Kurum bilgi işlem altyapısını kullanan ve bilgi kaynakalarına erişen herkes : * Kişisel ve elektronik iletişimde ve üçüncü taraflarla yapılan bilgi alışverişlerinde kuruma ait bilginin gizliliğini saplamalı, * kritiklik düzeylerine göre işlediği bilgiyi yedeklemeli, * Risk düzeylerine göre belirlenen güvenlik önlemlerini almalı, * Bilgi güvenliği ihlal olaylarını raporlamalı ve bilgi Güvenliği Birimin'ne bildirilmeli, bu ihlalleri engelleyecek önlemler almalıdır. Kurum içi bilgi kaynakları(duyur,döküman vb.) yetkisiz olarak 3. kişilere iletilemez kurum bilişim kaynakalrı,T:C. Yasalarına ve bunlara bağlı yönetmeliklere aykırı faaliyetler amacıyla kullanılamaz.
Roller/Görevler ve Sorumluluklar	Kurumun tüm çalışanları ve BGYS'de tanımlana dış taraflar,bu politikaya ve bupolitikayı uygulayan BGYS politika, prosedür ve talimatlarına uymakla yükümlüdür. Birimlerin güvenlik sorumlularından oluşan Güvenlik Koordinasyon Kurulu, BGYS altyapısını desteklemek ve işleyişini devam ettirmekle sorumludur.
Politikaların İhlali ve yaptırımlar	Bilgi güvenliği politika, prosedür ve talimatlarına uyulmaması halinde, kurum personel Yönetmeliği gereğince aşağıdaki yaptırımlardan bir ya da birden fazla maddesini uygulayabilir : * Uyarma, * Kınama, * Para cezası, * Sözleşme feshi.
Diğer Kural, Yönerge, Standart ve	İş Sürekliliği ve Acil Durum planları, Veri Yedekleme prosedürleri, Virüs ve Saldırganlardan Korunma, Sistemlere Erişim Kontrolü, Bigi Güvenliği Olayları Prosedürleri bu

Süreçlere Atıflar	politikayı destekler. Bu alanlarla ilgili işleyiş özel olarak dokümante edilmiş politika ve prosedürlerle tanımlanır.
Bilgi Güvenliği Politikası Gözden Geçirme Kuralları	Bu politika, Güvenlik Koordinasyon Kurulu tarafından periyodik olarak6 (altı) ayda bir gözden geçirilir. Yönetmeliklerde veya bilgi güvenliği uygulama süreçlerindeki değişiklikler politikanın gözden geçirilmesini gerektirir. Gözden geçirilen ve güncellenen politika Kurum Başkanı tarafından onaylanır. Onaylana politika kurum web sayfasında yayınlanır.

Kaynak: http://sonettelekom.com/sayfa=kalite

3.4. Bilgi Güvenliği Kültürü Yaratmak

Bilgisayarlarda ve bilgi teknolojisindeki hızlı değişimler, bilgi varlıklarının güvenliğinde sürekli olarak yeni riskler oluşturmaktadır. Buna ek olarak bilgi teknolojilerinin kullanılması, bilgi güvenliğinin ihlalini kolaylaştırmakta ve hatta kimi durumlarda tespit edilemez hale getirebilmektedir. Bu nedenle kurum ve kuruluşlar yeni zorluklara ve risklere yanıt vermek için bilgi güvenliği yeteneklerini sürekli olarak geliştirmek zorundadır.

Bilgi güvenliği kültürü, bilgi varlıklarının güvenliği açısından risk oluşturabilecek eylemlerden kaçınmak için bilgi teknolojilerinin kullanımı esnasında insan davranışına rehberlik etmektedir. Bilgi güvenliği, yalnızca çalışanlar gerekli önlemleri bildiklerinde, anladıklarında ve kabul ettiklerinde etkili olabilmektedir. Bu nedenle bilgi güvenliği kültürü, çalışanların günlük faaliyetlerinin doğal bir yönü haline getirmek için teknik güvenlik yöntemlerini destekleyen tüm sosyo-kültürel önlemleri içermektedir. Bilgi güvenliği kültürü bir organizasyonun güvenliğini ve çalışanların bilgi teknolojilerini kullanımları esnasında kabul edilebilir davranışlarda bulunmalarını etkilemektedir. Buna göre bilgi güvenliği kültürünü "Bilgi güvenliğini korumak için çalışanların güvenlik davranışlarını etkilemek amacıyla örgütte bilgi varlıklarıyla insan etkileşimini yönlendiren algı, tutum, değer, varsayımlar ve bilginin toplanması" olarak tanımlamak mümkündür. (Alhogail, 2015: 567)

Bilgi güvenliği kültürünü açıklayan bilgi güvenliği konuları asgari olarak şunları içermelidir: (Helokunnas ve Kuusisto , 2003: 191)

- Güvenliğin önemli olduğuna dair rasyonel inanç,
- Güvenli fiziksel ve mantıksal bir ortamın korunması ve yılda birkaç kez güvenlik denetimlerinin yapılması gibi uzun vadeli ve kısa vadeli bilgi güvenliği hedeflerinin iyi dengelenmesi,
- Güvenlik politikası, güvenlik prosedürleri ve süreçleri ve çalışanları motive etmek için güvenlik teşviki,
- Tehdit ve risk değerlendirmeleri yaparak güvenliği sürekli iyileştirme
- Güvenliğin, çalışanların günlük işleri üzerinde bir etkiye sahip olması
- Güvenlik politikası geliştirirken ve güvenliği yönetirken işbirliği
- İyi tanımlanmış güvenlik hedeflerinin kontrolü, koordinasyonu ve sorumluluğu,
- Güvenlik gereksinimleri, dış denetim ve hükümet gereksinimlerine uygundur.

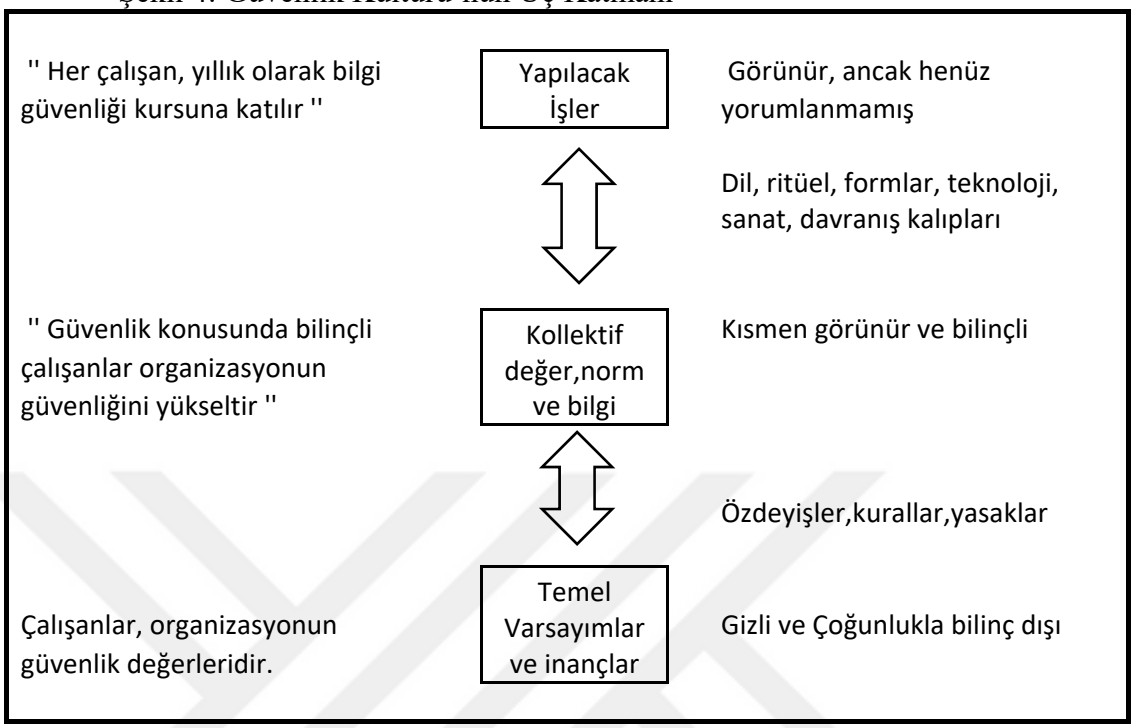
Bilgi güvenliği kültürü, genel olarak örgüt kültürünün çalışanların davranışlarından etkilenerek gelişmesi gibi, çalışanların bilgi güvenliği konusundaki davranışlarından gelişmektedir. Bu nedenle bilgi güvenliği kültürü, çalışanların bilgi varlıklarıyla olan etkileşimine ve örgütteki örgüt kültürü bağlamında sergilediği güvenlik davranışına dayanmaktadır. (Veiga ve Eloff, 2010: 198)

Örgüt kültüründe, işle ilgili bilgiler genel olarak göz ardı edilebilmektedir. Çünkü ortalama bir çalışanın işini yapmak için gerekli bilgiye sahip olduğu varsayılabilir. Bilgi güvenliğinde ise çalışanın normal iş işlevlerini yerine getirmek için gerekli bilgilerin bulunması zorunlu değildir. Bilgi güvenliği bilgisine, ancak ve ancak bilgi güvenliği uygulamaları ile normal iş işlevlerinin birbiriyle uyumlu olması halinde ihtiyaç duyulmaktadır. Ortalama çalışanının işini güvenli bir şekilde gerçekleştirmek için gerekli bilgiye sahip olduğu varsayılamaz. Bir organizasyon, bilgi güvenliği alt kültürü geliştirmeye çalışıyorsa, tüm faaliyetlerin iyi bilgi güvenliği uygulamaları ile uyumlu olacak şekilde yapması gerekmektedir. Bilgi güvenliğiyle ilgili yeterli bilgiye sahip olmak normal bir faaliyeti güvenli bir şekilde gerçekleştirmek için bir ön şarttır. (Niekerk, ve Solms, 2010: 478)

Bilgi Güvenliği Kültür, örgüt kültürünün bir parçasıdır. Örgüt kültürü, çalışanların kuruluşu nasıl gördüğünü tanımlamaktadır. Bu, zamanla büyüyen ve değişen ve bir dereceye kadar yönetim tarafından etkilenebilen veya hatta tasarlanabilen kolektif bir olgudur. (Schlienger ve Teufel, 2003: 1)

Şekil 4'te güvenlik kültürünün üç katmanı görülmektedir.

Şekil 4: Güvenlik Kültürü'nün Üç Katmanı



Kaynak: Thomas Schlienger, Stephanie Teufel, "Analyzing Information Security Culture: Increased Trust by an Appropriate Information Security Culture", Computer & Society, Proceedings of the 14th International Workshop on Database and Expert Systems Applications (DEXA'03), 2003, 1.

3.5. Bilgi Güvenliği Uygulamalarında Etik Davranış

Zamandan ve mekândan bağımsız olarak herkesin bilgi ile buluşabildiği internette, etik ve hukuksal sorumlulukları da kapsayarak bilgi güvenliğini sağlamak ve bu güvenliğin yeterli olabilmesi için gereken tedbirleri oluşturmak şarttır. Kurumların bilişim güvenliğinden sorumlu çalışanlar, bilişim teknolojilerini kullanarak vazifelerini en doğru şekilde yapmalı, bilgi güvenliğini içeren kurallar ve etik değerler çerçevesinde faaliyetlerini gerçekleştirmelidir. Bilgi işlem profesyonellerinin sorumluluklarının yalnızca bilginin düzenlenmesi, depolanması ve sunumu ile sınırlı olmadığı düşünüldüğünde, çalışanların ve müşterilerin kişisel bilgilerinin ve finansal bilgilerinin güvenli olarak muhafaza edilmesi ve meydana gelen bir suçun güvenlik birimlerine iletilmesi konusunda cezai sorumluluklara sahip olduğu bilinmelidir. Bilgi güvenliği hem

hukuki hem de bilişimin alanına girdiğinden, teknik önlemlerin yanı sıra hukuki açıdan da teminat altına alınmalıdır. (Avcıoğlu, 2015: 165)

Bilgi güvenliği ile ilgili olarak veri sızıntısını engelleyebilmek için bilgi güvenliği çalışmalarını üstlenecek profesyonellerin kişisel bilgilerinin yanı sıra sosyal medya hesapları dahi istenmeli ve gözden geçirilmelidir. Çünkü bilgi güvenliği ile ilgili olarak kişisel reklam amacıyla sosyal medya hesaplarında bilgi güvenliği profesyonellerinin sistemlerde buldukları açıkları ifşa ettikleri görülmektedir. Dolayısıyla etik açıdan bilgi güvenliğinde gizliliğe ve mahremiyete özel olarak önem verilmelidir. (Çelen ve Seferoğlu, 2016: 128)

Bir diğer etik konu, bilgi güvenliği çalışmalarında elde edilen bilgilerin, bilgi güvenliği çalışması tamamlandıktan sonra satışa çıkarılmamasıdır. Bilgi güvenliği uygulamaları ile elde edilen bilgilerin etik değerler hiçe sayılarak satışa çıkarılması, firmanın güvenilirliğini de sarsacaktır. Bir diğer risk ise bilgi güvenliği uygulamaları esnasında sistemde açık bulunması halinde bu açığı kapatmak için şantaj yapılmasıdır. İzin olmaksızın açıkları tespit eden kişilerin, bu açıkları şantaj malzemesi yapmadan önce kendi lehine nasıl kullandığını tespit etmek güçtür. Bu nedenle şantaj yapılması halinde doğrudan savcılığa suç duyurusunda bulunulması gereklidir. (Fidan, 2016: 1642)

4. BİLGİ GÜVENLİĞİNDE KURAMSAL YAKLAŞIMLAR

Son yıllarda Bilgi Güvenliği literatüründe 54 teori kullanıldığı görülmektedir. (Karjalaine ve Siponen, 2011: 520) kullanım sıklığına göre ilk 7 teori aşağıdaki tabloda belirlenmiştir.(Lebek, vd, 2013: 2980)

Tablo 6: En çok Kullanılan Teoriler

	Theory	%
Sebepli Davranış Teorisi / Planlı Davranış Teorisi	Theory of Reasoned Action - Theory of Planned Behavior	27
Genel caydırmazlık Teorisi	General Deterrence Theory	17
Korunma Motivasyon Teorisi	Protection Motvation Theory	10
Teknoloji kabul Modeli	Technology Acceptance Model	7
Sosyal Kavramsal Teori	Social Cognitive Theory	3
Yapılandırmacılık	Constructivism	3
Sosyal Öğrenme Teorisi	Social Leraning Theory	3

4.1. Planlı Davranış Teorisi

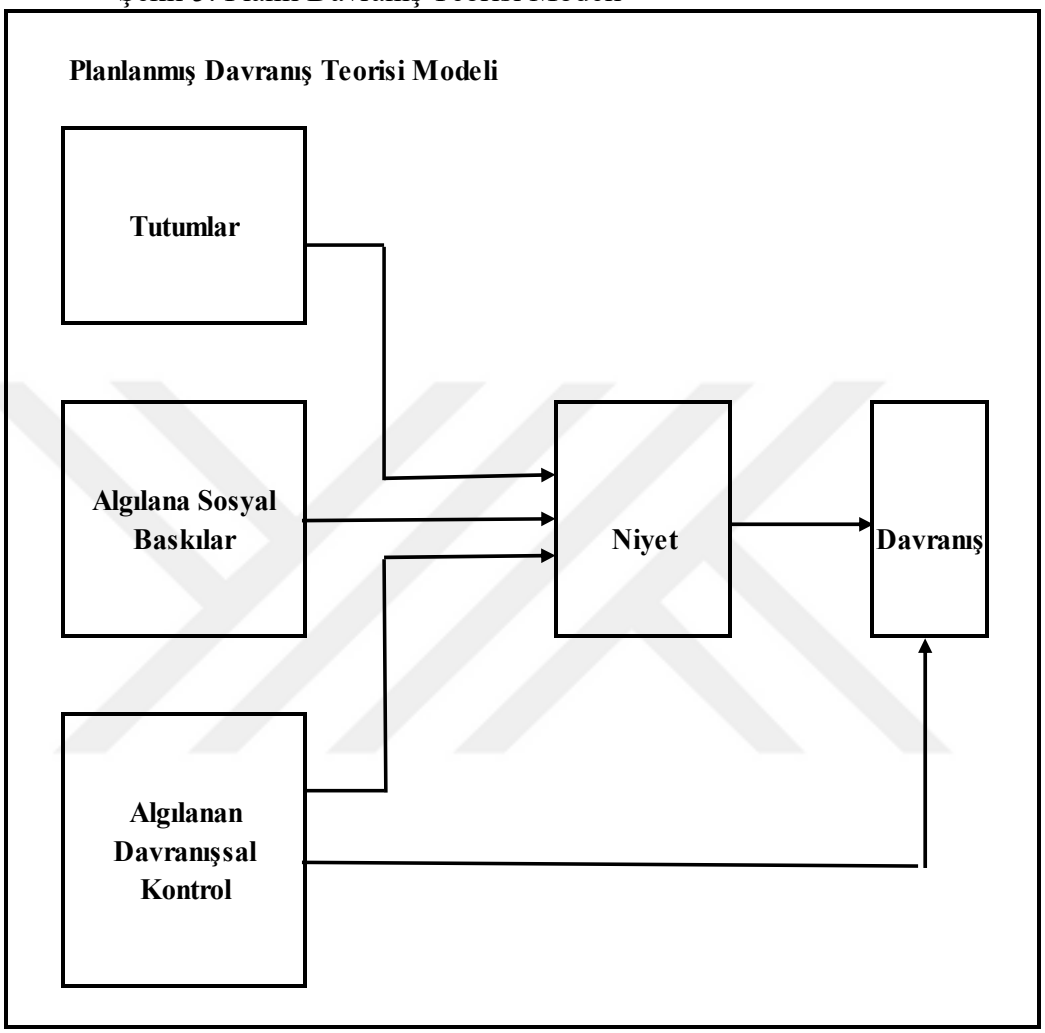
Bilgi güvenliği davranışı literatüründe bu çalışma ile bağlantılı iki teori öne çıkmaktadır. Bunlar; planlı davranış teorisi (planned behavior theory) ve kişi-çevre uyumu modeli (person-environment fit model) dir. Theory of reasoned action'ın (Ajzen ve Fishbein, 1980: 501) genişletilmiş versiyonu olarak planlı davranış teorisinin odağında, bir davranışa yönelimi sağlayan "niyet" bulunmaktadır. Bu bağlamda niyet, bir davranışı sergilemek için bireyin ne kadar istekli olduğunu ne kadarlık bir efor sarf etmeyi planladığını göstermektedir. Bir davranışa yönelik niyetin gücü bir anlamda sergilenecek performansın da bir göstergesidir. Planlı davranış teorisi, niyete etki eden üç değişkenin olduğunu ifade etmektedir. Bunlar; davranışa yönelik tutum, sübjektif normlar ve öz-yeterliliktir. (Ajzen ve Fishbein, 1991: 182)

Planlı Davranış Teorisi (Theory of Planned Behavior - TPB), Sebepli Davranışlar Teorisi' (Theory of Reasoned Action - TRA) temellidir. Azjen ve Fishbein, 1975 deki çalışmalarıyla gelişmiş olup, sosyol - psikolojik baza dayanan davranış teorisidir. Fakat, Kişilerin eylemlerinde kendi kontrolünde olmadığında, Sebepli Davranışlar Teorisi tam olarak yanıt verememiş ve zaman zaman sorunlara sebep olmuştur. (Chang, 1998: 1830). Bundan dolayı Azjen (1991) Algılanan Davranışsal Kontrol (Perceived Behavioral Control - PBC) değişkenini ilave ederek TRA'yı geliştirmiş ve TPB'yi meydana getirmiştir.

TPB'ın bazında kişilerin sistemli bir şekilde bilgiye erişerek, akılcı kararlar verdiği düşüncesi yatar. TPB kişilerin davranışlarının temel belirleyici faktörünün bilişsel sürecin mantıksal neticesi olduğu varsayımına dayanır. (Azjen ve Fishbein, 1975: 275). TPB üç ana unsurun kişi davranışlarını oluturduğunu varsayar. TPB, kişilerin gerçek manada davranışlarının (Actual Usage-AU), bireylerin davranışa dönük niyetlerinden (Behavioral Intention - BI) ve niyetlerinde bireyin tavrı (Attitude - A), yakınların etkisi (Subjective Norm - SN) ve algılanan davranışsal kontrol (Perceived Behavioral Control - PBC) değişkenlerinin etkisi ile belirlendiğini ve şekillendiğini savunur.TPB bireyin niyetinin, tavırlarının (Attitude) ve kişisel normlarının (Subjective Norm) etkisiyle şekillendiğini savunur. Sonraki çalışmalarda algılanan davranışsal kontrol (Perceived Behavior Control - PBC) değişkeni de TPB modeline eklenmiş ve bireylerin tam olarak

davranışlarını kontrol altında tutamadığı durumlarda modele entegre edilen bu değişken ile model geliştirilmiştir. (Azjen, 1991: 185).

Şekil 5: Planlı Davranış Teorisi Modeli



Kaynak: Icek AJZEN (2006).''Constructing a TpB Questionnaire: Conceptual and Methodological Considerations''
http://www.people.umass.edu/aizen/pdf/tpb.measurement.pdf.(Erişimtarihi:17/05/2018)

Planlı davranış teorisi çerçevesinde bu araştırma, bilgi güvenliğinde tutuma ettiği varsayılan iş engeli, gizlilik ihlali ve bilgi güvenliğinde stres değişkenleri üzerine odaklanmaktadır.

4.2. Birey – Çevre Uyum Modeli

Kişi-çevre uyumu ise bireysel karakteristikler (e.g., skills, abilities, needs, desires, values, goals, personality) ile çevre arasında uyumun derecesi olarak tanımlanmaktadır. (Kristof, 1996: 49) Bireysel beceriler, ihtiyaçlar, değerler vb. ile çevre arasındaki uyumun artması çalışanların iş tatmini ve performansını da artırmaktadır. (Ostroff ve Shulte, 1987: 69) Kavram zamanla, person-job, person-groups, person-supervisor ve person-organization uyumu biçiminde farklı düzeylerde ele alınmıştır. Bu çalışma, birey-organizasyon uyumu çerçevesinde, çalışanların bilgi güvenliği davranışları ile organizasyonun bilgi güvenliği hedefleri arasındaki uyuma odaklanmaktadır. Birey-çevre ya da daha spesifik düzeyde birey-organizasyon uyumsuzluğunun her iki taraf açısından stres yaratacağı (Edwards, vd, 1998: 28) savından hareket edilmektedir. Dolayısıyla, bireyin bilgi güvenliği davranışı ile organizasyonun bilgi güvenliği politikaları arasında uyum dengesi bozuldukça hem birey hem de örgüt açısından stres düzeyi artmaktadır. Bilgi güvenliği uygulamaları bazında gizlilik ihlali ve iş engelleri konusunda çalışanların örgütsel beklentilere cevap verememesi, çalışanların yetkinlik düzeylerinin organizasyonel gereklilikler ile uyumsuz olmasının bilgi güvenliği uygulamalarında stres yaratacağı varsayılmaktadır.

4.3. Koruma Motivasyon Teorisi

Koruma Motivasyonu Teorisi (Protection Motivation Theory), menfaat sahiplerinin kendilerini tehlikeli durumlara karşı korumaya yönelik motivasyonlarının ya da niyetlerinin, risklerin şiddeti, risklere karşı kişisel güvenlik açığı, riski azaltma için öz yeterlilikleri ve riski azaltma davranışı olmak üzere dört temel bilişsel ve algısal faktörden oluştuğunu belirten teoridir. Yine bu teoriye göre insanların kendilerini koruma niyetleri, risk azaltma davranışının maliyeti ve alternatif risk azaltma davranışlarının getirileri tarafından zayıflatılmaktadır.(Bender, vd, 2007: 890)

Korunma Motivasyonu Teorisi, insanların tehditleri değerlendirmede ve başa çıkma alternatifleri arasında seçim yapmaları arasında kullandıkları ara süreçtir. İlgililer, kendilerini riskten korumak için tehditlerin değerlendirilmesi ve başa çıkma faktörlerinin bir kombinasyonunu kullanmaktadır. İnsanlar, toplumsal ya da kişiler arası risklerden kaçınmak için motive olabildikleri gibi, işyerindeki hem iş sağlığı ve güvenliğini

sağlayacak, hem de bilgi güvenliğini sağlayacak risklerden kaçınmak için de motive olabilmektedir. (Bender, vd, 2007: 891)

Korunma Motivasyonu Teorisi, bireyin koruyucu eylemlerde bulunma niyetini öngören en güçlü açıklayıcı teorilerden biridir. Temel olarak hem tehdit değerlendirmesinden hem de başa çıkma değerlendirmesinden kaynaklanmaktadır. Tehdit değerlendirmesi, tehdit edici olayların meydana gelme olasılığına ilişkin algılanan güvenlik açığı ve olayın sonuçlarının ciddiyeti olmak üzere iki faktörün bileşkesidir. Tehditle başa çıkma değerlendirmeleri, üç faktörlü bir altyapıya sahiptir. Bunlar, bireyin önerilen davranışla başa çıkma ya da bunları yerine getirme yetenekleri olan öz yeterlilik; bireyin yaptığı eylemin algılanan faydası hakkındaki inancı olan tepki etkililiği ve algılanan fırsatın faydaları hakkındaki algılamalar olan tepki maliyetidir. (Ifinedo, 2012: 84)

Korunma Motivasyonu Teorisi, sağlık alanında daha sık kullanılan bir teori olmakla birlikte, bilgi güvenliği konusunda da kullanılmaktadır. Korunma Motivasyonu Teorisi, bir tehdide karşılık olarak uyarlanmış ya da uygunsuz olmak üzere iki tip davranıştan birini yapma ihtiyacını değerlendirmektedir. Uyarlanmış davranış, bir kişiyi tehdide karşı korumakta etkili bir davranış türüyken, uygunsuz bir davranış ise hiçbir şey yapmamak ya da riski artırabilecek davranışlarda bulunmaktır. Yapılan tehdit değerlendirmesinde bireyler tehdidin oluşma ihtimalini ve tehdidin ciddiyetini değerlendirmektedir. Ayrıca davranışın etkili bir tehdit caydırıcı olup olamayacağını da değerlendirmektedir. (Shillair, vd, 2015: 200)

Bu tip davranışları işyerinde bilgi güvenliğine uyarlarsak, kimi çalışanlar eposta hesaplarına gelen tüm spam sayılabilecek mailleri ve ekleri açarken, bazı çalışanlar ise bu tip mailleri açmadan, okumadan ve eklerini indirmeden silmektedir. Kimi çalışanlar tahmin edilmesi çok kolay şifreler kullanırken, kimi çalışanlar ise tahmin edilmesi çok daha zor ve uzun şifreler kullanmaktadır. Bazı çalışanlar anti virüs programlarını kurmazken, bazı çalışanlar ise sürekli olarak anti virüs programı kullanır ve düzenli aralıklarla tarama yaptırır. Dolayısıyla bir tehdide karşı kullanıcılar virüs olma ihtimalini düşünüp (tehdit değerlendirmesi), bu zararlı postayı açarsa neler olabileceğini (tehdidin ciddiyeti) ve sonuçlarını değerlendirmektedir.

Bu değerlendirmeler elbette tehdit hakkında bilgi sahibi olan ve tehdidi tanıyabilen kullanıcılar üzerine kuruludur. Bireyler, aynı zamanda tehditle baş etme yeteneklerini de düşünmektedir. Başa çıkma değerlendirmeleri, uyarlamalı yanıtların etkililiğine ilişkin etkililik inancı (örneğin bir bağlantının açılıp açılmamasının virüsü engellemeyeceği) ve kişinin uyarlamaları yanıtını başarıyla yerine getirebilme kabiliyetine yönelik kişisel inançları sonucunda yapılmaktadır. (Shillair, vd, 2015: 201)

5. BİLGİ GÜVENLİĞİ UYGULAMALARINDA ÇALIŞANLARA DÖNÜK RİSK ALANLARI

5.1. Psikolojik Risk

Çalışma hayatından dolayı meydana gelen stres ile oluşan sağlık problemlerinin düşündüğümüzde, psikolojik risk etmenleri, çalışanların verimliliğini doğrudan etkileyebilen, sigara, alkol, uyuşturucu madde gibi alışkanlıkların oluşmasına ya da kullanımının artmasına neden olabilmektedir. Bunun sonucunda da çalışanların yalnızca iş yaşamına tesir eden bir faktör oluşturmaktan daha fazla olarak iş görenin iş hayatı dışındaki özel hayatına, sosyal çevresine ve ailesini de olumsuz etkileyen bir faktör haline gelebilmektedir. Psikolojik risk faktörlerini işin mahiyeti, işin temposu, iş programları, kontrol, çevre, kişiler arası ilişkiler, işyerindeki vazifesi, mesleki gelişimi, çalışma hayatı ve iş harici hayat nedenleri gibi faktörler oluşturmaktadır. (Paşa ve Kaymaz, 2013: 18)

İşin Mahiyeti: İş için gereken vasıfların kullanılamaması, çeşitliliğin olmaması, tekrarlayıcı işlerde çalışma, öğrenme fırsatı bulamama gibi faktörler, özellikle teknolojinin gelişimi ile birlikte işlerin makineler tarafından yapılması gibi nedenlerle çalışanlar işyerinde kendilerini daha değersiz hissederek mevcut görevlerinden daha fazlasını yapabilmek için yetkisi olmayan ve bilmesi gerekmeyen bilgileri edinmeye çalışabilmektedir. Bu da bilgi güvenliğini tehlikeye düşürmektedir.

İş Yükü ve İş Temposu: Aşırı iş yükü ve zaman baskısı bir diğer psikolojik risk faktörüdür. Çalışanın, kendi niteliklerine uygun işi yapabilmek için yeterli zamana sahip olmaması ya da işin, çalışanın niteliklerinden fazlasını gerektirmesi durumunda oluşabilmektedir. Böyle bir durumda çalışanlar işi daha kısa sürede bitirebilmek için başkasından yardım isteyebilir ve ekstra bilgiye ihtiyaç duyabilir. Bu da bilgi güvenliğini tehlikeye düşürebilir. (Tutar, 2016: 155)

İş Programları: Vardiyalı çalışmak bir diğer psikolojik risk faktörüdür. Sürekli olarak gece vardiyasında çalışanlar bir süre sonra yalnızlaşabilmektedir. Ayrıca aşırı yorgunluk ve stres ortaya çıkabilmektedir. Bu da çalışanın yakınmalarının artmasına, bilgiyi paylaşma yoluna gitmesine neden olabilmektedir.

Kontrol: Çalışanların kararlara katılımını içermektedir. Bu durum çalışanların işi benimsemesi konusunda olumlu etki yaratmakla birlikte, kendilerini de işyerinde tehdit altında hissetmemelerini sağlamaktadır. Kararlara katılımın olmadığı işyerlerinde bilgi de tehdit altındadır. Çalışanlar, işyerindeki pozisyonlarını koruyabilmek için bilmeleri gerekenden fazla bilgiyi öğrenmek isteyebilir. (Çelik, 2010: 254)

Çevre ve Ekipman: Isı, nem, ışık gibi çevresel koşulların uygun olması ile işyerindeki düzen ve disiplinin sağlanması, huzursuzlukların azaltılması ve verimliliğin artırılması mümkün olmaktadır. Bu sayede çalışanlar yalnızca kendi işlerine odaklanacak, moral ve motivasyonları yüksek olacaktır. Rahat ve huzurlu bir ortamda çalışan çalışanlar, kendilerini ilgilendirmeyen bilgiler ile ilgilenmeyecektir.

Kişiler Arası İlişkiler: İşyerindeki liderlik stili, önemli bir psikolojik risk faktörüdür. Otoriter bir yönetsel ve idari yaklaşım anlayışı ile meydana getirilen iş yaşam alanı, gergin, tehdit, korku ve kaygı doğuracaktır. Bu da bilgiyi tehdit altına almaktadır.

İşyerindeki Görev: İşyerindeki rol çatışmaları, yöneticinin çalışanlardan tutarsız ve çelişkili beklentilerde bulunması ya da birden fazla yöneticinin bir çalışandan birbiriyle çatışan isteklerde bulunması ile ortaya çıkmaktadır. Bir çalışan, kendisinden istenen bir işi yapabilmek için ekstra bir bilgiye ihtiyaç duyup, o işi yerine getirmeye çalışırken, bir başka yöneticinin o işi yapmamasını istemesi ile yaşanan rol belirsizliği, çalışanın edinmemesi gereken bilgiyi edinmesini sağlayabilir. Bu da doğal olarak bilgiyi tehdit altına alacaktır.

Kariyer Gelişimi: Kişinin iş yaşamında belirli bir amaca erişmek, kariyerinde yükselmek ve bu sayede çok daha saygı görmek, güç sahibi olmak, ve para elde etmek isteğinin işyeri tarafından karşılanmaması durumunda çalışanlar başka işyerine transfer olmayı isteyebilmektedir. Bu da elde tutulamayan çalışan ile işyerindeki bilgilerin başka ve rakip bir işletmeye kaptırılması anlamına gelebilmektedir. (Altıntaş, 2014: 108)

İş ve İş Dışı Yaşam Etkileşimi: Bireyin iş yaşantısı ile iş dışındaki yaşantısı arasındaki denge, çalışanların yakındığı konuların başında gelmektedir. İş dışında

yaşadığı olumsuz hayat tecrübeleri, şiddetli geçimsizlik, yeni bir çocuğun doğumu, ekonomik sorunlar, hobilerinden mahrum kalmak vs. gibi olaylar, çalışanlarda strese neden olabilmektedir. Bu da hem iş yaşantısını, hem de özel hayatını etkileyebilmektedir.

Tablo 7'de psikolojik risk faktörleri görülmektedir.

Tablo 7: Psikolojik Risk Faktörleri

1- İşin Mahiyeti	İşte çeşitliliğin az olması İşin çok bölünmüş küçük bir parçasını yapma İşin çalışanın yeteneğine göre verilmemesi Belirsizliğin çok olması
2- İş yükü ve iş temposu	Fazla çalışma ya da atıl kalma Üretim hızının neden olduğu baskı Zaman baskısı İş bitim tarihlerinin baskısı
3- İş programlama	Vardiyalı çalışma Gece çalışması Esnek olmayan çalışma programları Son anda belli olan fazla mesai programları Uzun saatler boyunca tek başına çalışma
4- Kontrol	Çalışanların kararlara düşük katılımı Çalışanların iş programlan üzerinde kontrollerinin az olması
5- Çevre ve Kontrol	Yeterli ekipmanın olmaması Yetersiz mekân: aydınlatma ve gürültü gibi olumsuz fiziksel ortam
6- Kişiler arası ilişkiler	Sosyal ya da fiziksel olarak izolasvon Çalışanlarla ya da yöneticilerle olan ilişkiler Kişilerarası çatışmalar Sosyal desteğin azlığı
7- İşyerindeki Görev	Rol belirsizliği Rol çatışmaları İnsanlara ilişkin s olumluluklar
8- Kariyer Gelişimi	Terfilerin olmaması ya da belirsiz olması Düşük ücretler İş güvencesinin olmaması İşin sosyal değerinin düşük olması
9- İş ve İş Dışı Yaşam Etkileşimi	İş ve ev yaşamının birbiriyle çelişmesi Evdeki desteklerin azlığa Çift kariyer sorunları

Kaynak: T. C. Çalışma ve Sosyal Güvenlik Bakanlığı, Psikolojik Risk Faktörleri Bilgilendirme Rehberi, (Editörler: Fatma Nur Büyükkara, Mert Durşen, Erkan Serdar Serter, Ahmet Cankurtaran, Serra Ela), Ankara, 2016, 3.

5.2. Stres Yaratma

Bilgi güvenliğini sağlama alabilmek için kullanılan yazılımların sürekli olarak test edilmesi önem taşımaktadır. Yazılım testleri, kullanılan yazılımın beklenen kalitede olduğunu belirlemek, eğer beklenen kalitede değilse istenilen kaliteye ulaşabilmek için belli kural ve yöntemler ile yürütülmelidir. Çünkü yazılımlarda çıkan hataların geç fark edilmesi, maliyetlerin yükselmesine neden olacaktır. Yazılım geliştirme çabalarının ilk aşamasında ortaya çıkan hatalar projede daha fazla efor sarf edilmesini gerektirecek, sonlara doğru fark edilen hatalar ise müşterinin bilgisi dahilinde olacağından itibar kaybına yol açacaktır. Bu nedenle bilgi güvenliği açısından yazılım geliştirme sürecinin en başından itibaren birtakım testler yapılmak durumundadır. (Goldstein ve Sapra, 2013: 5)

Testlerin uygulanmasında test stratejinin belirlenmesi ve planlama aşamasıyla süreç başlamaktadır. Bir ürünün nasıl test edileceğinin belirlenmesiyle birlikte tüm test tipleri ve seviyeleri belirlenmektedir. Sonrasında testin amacı ve belirlenen ihtiyaçlar doğrultusunda testin analizi ve gerçekleştirilmesi aşamasına geçilmektedir. Test, analiz aşamasında edinilen bilgiler ve ihtiyaçlar doğrultusunda test senaryoları oluşturulduktan sonra gerçekleştirilmektedir. Son olarak testlerin gerçekleştirilmesinden ardından sonuçlar analiz edilerek test projesinin bitirilmesine karar verilmektedir. Biten testlerin çıktıları ise benzer testler için saklanmaktadır. (Vural ve Sağıroğlu, 2011: 94) Bu testlerden biri de yük ve stres testleridir.

Yük ve stres testleri, uygulamaların değişik senaryolarda ve değişik kullanıcı yükleri altında nasıl davrandığını görmek ve var olan altyapının kaldırabileceği maksimum yükü belirlemek amacıyla gerçekleştirilmektedir. Ayrıca uygulamanın en kırılgan noktalarını belirlemek, optimum performans değerini ortaya çıkartıp performans artırıcı önlemler almak da yük ve stres testlerinin amaçları arasındadır. Stres testleri ile bilgi teknolojilerinin altyapısının, kullanılan sunucuların, yazılımların ve uygulamaların performansı test edilmektedir. Böylece sistem üzerine binebilecek yükün ileride

doğurabileceği olumsuz sonuçların önceden kestirilmesi ve ileriye yönelik çözüm önerileri üretmek mümkün olacaktır. (Chandra ve Challa,Hussain, 2014: 7757)

5.3. Finansal Risk

Bilgi güvenliği konusundaki en önemli risklerden biri finansal risktir. Yeterli bilince sahip olmayan çalışanlar finansal risk altına girebilmektedir. Örneğin bir kullanıcının kendi kullandığı bilgisayarda eposta adresine gönderilen virüslü içerikleri bilinçsiz bir şekilde açması, epostanın eklerinde yer alan dosyaları indirmesi, resim ya da müzik dosyalarının beraberinde solucan, keylogger ya da trojan denilen virüsleri içermesi sonucunda hem kendisinin hem de çalıştığı firmanın zarar görmesi kaçınılmazdır. Özellikle keylogger denilen zararlı içerik, bilgisayarda klavyeyle yazılan tüm bilgileri kaydederek yetkisiz ve kötü niyetli kişilere göndermektedir. Ayrıca bu gibi zararlı içeriklerin, başka bir bilgisayarda indirilerek taşınabilir belleklere bulaşması ve bu belleklerin işyerinde de kullanılması nedeniyle çevrimiçi olmayan ortamda dahi virüsün bulaşması mümkün olmaktadır. Dolayısıyla bankacılık işlemleri, hassas ve ticari nitelikteki finansal bilgiler risk altına girmektedir.

5.4. Yaratıcılığı Engelleme – Sosyal Diyaloğu Engelleme

Sosyal diyalog, iş hayatı içindeki birbirinden değişik rollerdeki kişilerin hep beraber kararlar alabilmelerine imkan veren bir anlaşma mekanizmasıdır. Farklı bir açıdan bakıldığında yönetim karalarına ortak olabilmede denilebilir. Dolayısıyla tek seferlik bir olguyu değil, bir süreci ifade etmektedir. Yöneten ve yönetilen ilişkisinin olduğu her kurumda bir ast üst dolayısıyla bir güç ilişkisi söz konusudur. (Can, 2013: 28) Bilgi güvenliği uygulamaları ve performans yönetim sistemine entegrasyon ile birlikte düşünüldüğünde çalışanların yönetime katılmasından çok performanslarının esas ölçüt alınması, dolayısıyla çalışanları yönetime katılmak bakımından etken bir durumdan, yalnızca çalışan olarak edilgen bir yapıya indirgenmesi söz konusu olmaktadır. Sıkı bir bilgi güvenliği uygulaması ve etkin bir performans yönetim sisteminin olduğu işletmelerde çalışanlar, işletme içindeki bilgilere sınırlı bir erişime sahip olmaktadır. Bu da çalışanları adeta bir robota dönüştürerek yaratıcılıklarına ket vurulmasına neden olabilmektedir.

5.5. Risk Yönetim Süreci

Bilginin güvenliğinin tam anlamıyla sağlanabilmesi için alanında uzman olan kuruluşlardan danışmanlık almak, bilgi güvenliğinin sağlanabilmesi için önem taşımaktadır. Özellikle KOBİ'lerin bilgi güvenliği konusunda kaynak yetersizliğinden dolayı eksik kalabildiği göz önünde bulundurulduğunda, uzmanlık gerektiren bir konu olarak bilgi güvenliği için danışman firmalardan hizmet almak hem bilginin korunması, hem de kurum ve kuruluşların kaynaklarının etkin bir şekilde kullanılmasını sağlayacaktır. (Çetin, vd, 2013: 240)

Bilgi güvenliğinde danışmanlık almak, bilgi güvenliği yönetim sistemi standartlarına sahip olmanın anahtarlarından biridir. Ticari sürekliliği sağlayabilmek adına ihtiyaç duyulan süreçlerin tanımlanması ve uygulanması için sağlam bir temel olan bilgi güvenliği yönetim sistemleri standartlarına uyum sağlayan kurum ve kuruluşlar, bilginin kötü niyetli ellere geçmesini engelleyecek yönetim kabiliyetine erişebilmektedir. Ayrıca hem yerel hem de küresel pazarda çok daha saygın ve güvenilir bir kurum imajı çizmektedir. Bilgi güvenliği konusunda danışmanlık hizmeti alarak, bilgi güvenliği standartlarına erişebilmek için gereken stratejilerin ve prosedürlerin hazırlanması hızlandırılabilir. (Gülseçen, 2016: 114)

Bilgi güvenliğinde danışmanlık alma, çalışanların bilgi güvenliği farkındalığını artırma eğitimlerinden başlayarak tüm gerekli bilgi güvenliği araçlarının kullanımına kadar geniş bir yelpazeyi kapsamaktadır. Bilgi güvenliği danışmanlığı alarak gereksiz yatırımlar önlenebilmekte, öncelikli problemlere öncelikli çözümler sağlanabilmektedir. Bilgi güvenliğini sağlayabilmek için bilgi güvenliği uygulamasının kapsamı belirlenerek bilgi güvenliği stratejileri oluşturulmalı ve risk analizi yapılmalıdır. Bilgi güvenliği uygulamasının kapsamının belirlenmesi ile birlikte süreçler analiz edilerek bilgi varlıklarının üzerinde ne gibi risklerin olduğu ve ne gibi zayıf noktaların olduğu belirlenmeli ve risklerin sıralaması en acil ve en riskliden en az acil ve en az riskliye doğru yapılmalıdır. (Baykara, vd, 2013: 233)

Bilgi güvenliği konusunda danışmanlık alarak kurumda kendi kendini yöneten bir bilgi güvenliği yönetim sistemi kurulabilmekte, kontrol sistemi ile bilgi güvenliği yönetim sistemi geliştirilebilmekte ve hedeflenen bilgi güvenliği sertifikalarının alınması mümkün olmaktadır.

Bilgi güvenliği konusunda danışmanlık almak istendiğinde, danışmanlık alınacak firmanın seçiminde, firmanın bilgi güvenliği yönetim sistemi uygulama metodolojisi incelenmelidir. Danışman firmanın bilgi güvenliği yönetim sistemini uygularken ISO/IEC 27002:2013 Bilgi Güvenliği Yönetimi İçin Uygulama Prensipleri'ni eksiksiz uygulaması gereklidir. Bu prensipler;

1-Bilgi güvenliği yönetimini başlatmak,

2-Bilgi güvenliğini gerçekleştirmek,

3-Bilgi güvenliğini sürdürmek ve iyileştirmek için genel prensipleri ortaya koymaktadır. (Türk, 2003: 144)

Bilgi güvenliği yönetim sisteminin kapsam alanı, işletmenin belirlenen bir kısmı olabilir ya da işletmenin bütününü de kapsayabilir. Fakat, her iki seçenek de de, İşletmenin BGYS kapsam alanını ve oluşturduğu sınırları yanlışsız ve tam olarak tanımlaması gerekmektedir. BGYS kapsamı, kurum içi ve dışı hususlar, tepe yönetimin niyeti ve ilgili tarafların ihtiyaç ve beklentileri dikkate alınarak belirlenmelidir. Kapsam dışında bırakılanların hangi nedenlerle dışarıda bırakıldıklarını kurumun sağlam gerekçelerle açıklayabilmesi gerekmektedir. Bu adımın sonunda bir kapsam dokümanı yayınlanmalı ve üst yönetim tarafından onaylanmalıdır. (Peppard ve Ward, 2016: 354)

Risk yönetimi, riski belirlemek, değerlendirmek ve riski makul seviyeye indirmek için harekete geçme sürecidir. Bilgi güvenliğinde risk yönetimi, her biri kendi içerisinde büyük öneme sahip ve birbirini etkileyen beş temel fonksiyon ile yerine getirilmektedir: Riski belirleme, riskin analizi, riskin değerlendirilmesi, riske müdahale edilmesi ve risk yönetimini izleme. (Soomro, vd, 2016: 61)

Risk yönetim süreci, organizasyonel yapıya uygun, tekrar edilebilir, uluslararası standartlara ve uygulamalara uygun ve bu konularda deneyim sahibi iç ve dış birimler tarafından kontrol edilebilmelidir. Bilgi güvenliği açısından risk yönetiminde risk alanları şu şekilde belirtilebilir. (Emhan, 2009: 212)

Yönetim ve Strateji Riski: Bilgi güvenliği hedef ve süreçlerinin işletmenin hedef ve süreçleri ile uyumsuz olması sonucunda bilgi işlem teknoloji faaliyetlerinin işletme faaliyetleriyle ilişkili bir çalışma gurubu gibi çalışamaması riskidir.

Beceri ve Teknolojik Gelişme Riski: Bilgi teknolojilerinin iş ile ilgili birimleri, sektörün ileri gelen oyuncularından biri haline getirecek ve orda kalmasını sağlayacak iş yeteneklerini geliştirecek yenilikleri gerçekleştirmek konusunda başarısız olması riskidir.

Mimari Risk: İşletmenin tüm ünitelerinin gereksinimlerinin randımanlı, maliyet açısından etkin ve iyi kontrol edilebilir şekilde olmasını sağlayacak etkin ve sürdürülebilir alt yapının olmaması riskidir.

İş Sürekliliği Riski: Bilgi teknolojilerinin kritik operasyonel süreçleri devam ettirememesi riskidir.

Uyumluluk Riski: Bilgi teknolojilerinin yasal düzenleyicinin gerekliliklerini yerine getirecek desteği verememesi riskidir.

Kaynak Riski: Bilgi teknolojilerinin insan ve finansal kaynaklarını uygun hazırlık ve planlamayla yönetememesi riskidir.

Üçüncü Parti İlişkileri Riski: İş ortamının ve iş ortamında üretilen bilgilerin üçüncü parti kişi ya da kurumlarla paylaşılması ya da onlar tarafından öğrenilmesi riskidir.

Değişiklik Gerçekleştirme Riski: Teknolojik kaynakların uygun bir şekilde yenilenmemesi ya da yenilenememesi riskidir.

Bilgi Riski: Hassas bilgilerin saklanamaması riskidir.

Altyapı Riski: Bilgi teknolojileri altyapısının tehditlere açık olmasıdır.

Online Risk: Web sitesinin saldırılara açık olması riskidir.

Bu risklerin ortadan kaldırılabilmesi ya da minimize edilebilmesi için öncelikle ISO 27001 BGYS standardına göre bilgi güvenliği politikası temel alınarak sistematik bir risk yönetimi yaklaşımı belirlenmelidir. Kurum, kendisine yapısına göre belirlediği bir uygulamayı seçebilmekte özgürdür. Ancak nasıl bir yaklaşım seçilirse seçilsin, seçilen risk yönetimi yaklaşımı mukayese edilebilir ve tekrarlanabilir sonuçlar üretmeyi garanti etmesi gereklidir. Risk yönetimi bağlamında kabul edilebilecek risk düzeyleri tespit edilmeli ve bunlar için değerler geliştirilmelidir. Risk yönetimi anlayışı risklerin tespit

edilmesi, risklerin derecelendirilmesi, önceliklendirilmesi ve işlenmesi ile ilgili tüm kuralları içermelidir. (Webb, vd, 2016: 25)

Bilgi güvenliğinde risk yönetimi, bilgi varlıklarının tehlike analizini gerçekleştirerek, teknik, idari ve fiziksel açıdan bilgi varlıklarının ne ölçüde tehlikede olduğunu ortaya çıkarmak amacıyla yapılmaktadır. Şüphesiz bilginin olduğu her yerde her zaman risk vardır. Bu nedenle çok yönlü risk analizi çalışmaları ile kurum ve kuruluşların tüm bilgi varlıklarının envanteri ortaya çıkartılarak tüm bilgi varlığının kalem kalem güvenlik derecelendirmesi yapılmalıdır. (Alshaikh, vd, 2015: 3)

Risk belirlemesi yapılırken işletme envanterlerinde bulunan bilişim varlıklarının sahip oldukları açık noktalar ve bu zayıf noktaları kullanarak varlığa, dolayısı ile kuruma zarar verebilecek olan tehditler belirlenmektedir. Sonrasında risk yönetimi yaklaşımında belirlenen yönteme uygun olarak riskler ortaya konulmaktadır. Riskler belirlendikten sonra risklerin sınıflandırması yapılmalıdır. Risklerin sınıflandırılması şu şekilde yapılabilmektedir: (Yılmaz, 2014: 53)

Güvenlik Riski: Bilginin değiştirilmesi, bilgiye yetkisiz kişilerce erişilebilmesi ve kullanılması riskidir.

Erişebilirlik Riski: Bilgi ve/veya uygulamalara sistem kaybı, çökmesi, internet erişiminin olmaması, doğal felaketler gibi nedenlerle erişilememesi riskidir.

Geri Kazanılabilirlik: Bilgi ve/veya uygulamalara sistem kaybı, çökmesi, internet erişiminin olmaması, doğal felaketler gibi nedenlerle erişilemediği durumlarda bilginin tekrar geri getirilebilmesi için gereken sürenin uzaması riskidir.

Performans Riski: Sistemin, uygulamaların ya da personelin yetersiz performansı sonucu iş verimliliğinin düşmesi riskidir.

Ölçeklenebilirlik: Sistemin ve organizasyonun değişen bilgi ihtiyacını karşılayabilmesi için geliştirilmesi gerekmesine rağmen geliştirilememesidir.

Uyumluluk Riski: Bilgiye ulaşma, elde tutma ve bilgiyi işlemenin, iş politikalarına uygun şekilde yapılmaması riskidir.

Açık noktaların tespit edilmesi esnasında teknik zayıflıklarının, açık noktaların tespit çalışmaları da yapılmalıdır. Risk belirleme çalışmasına destek sağlamak amacı ile teknik açıklıkların tespit edilmesi için gerekli analiz faaliyetleri gerçekleştirilmelidir.

Bulgular risk yönetimi yaklaşımına uygun olarak belgelendirilmelidir. Kurumun bilgi varlıklarının taşıdığı riskler varlık sahipleri ile görüşmeler yapılarak toplanmalıdır. (Peltier, 2013: 59)

Risk yönetimi uygulamaları sonucunda belirlenen risk ve tehditleri baz alarak, bunlara karşı en etkin risk uygulama metotları tespit edilmelidir. Belirlenen risklere karşı dört farklı tavır alınabilmektedir. Bunlar; (Fenz, vd, 2014: 415)

1. En etkin kontrol yöntemleri ile oluşan riskleri bertaraf edilmesi ya da makul bir düzeye çekilmesi
2. Tehdit ve risklerin meydana gelmesine sebep olabilecek fonksiyon ve durumları baştan kaçınarak risklerden uzaklaşılması
3. Sigortalayarak ve veya satıcı – müşterilere oluşan riskleri işletmenin dışına yansıtılması
4. İşletme politikasına uygun olarak ve riskin makul düzeyde kalması koşuluyla oluşan riskleri bilinçli bir şekilde yönetimin onayı ile şirket bünyesine alınması

Tespit edilen işlemler neticesinde belirlenen risklerin risk uygulama-işlem planı meydana getirilmelidir. Risk işleme süreci sonrasında geriye kalan riske artık risk denir. Bunlar kabul edilen riskler veya tamamen ortadan kaldırılamayan riskler olabilir. Kurum üst yönetimi artık riskler için onay vermelidir. Bu adım sonunda artık risk onay belgesi oluşturulmalıdır.

6. BİLGİ GÜVENLİĞİNDE STRES FAKTÖRLERİ

6.1. Gizlilik İhlali

OECD tarafından yayımlanan "Kişisel Verilerin Korunması ve Sınır Ötesi Akımlarının Korunmasına İlişkin Kılavuz İlkeler", 1980'den beri kamu ve özel sektörde kişisel bilgilerin ele alınması konusunda uluslararası bir fikir birliğini temsil etmektedir. Bilgi güvenliği açıkları, sağlık hassasiyetleri gibi doğrudan insan hayatını tehdit etmese de, bireyler güvenli bir ortamda bilgi teknolojilerini kullanmayı tercih etmektedirler. İnsanlar, olası bilgi güvenliği tehditlerini fark etmiyor olsalar da kişisel bilgilerin çalışması, silinmesi, değiştirilmesi ya da kişisel bilgilere ulaşımın engellenmesi gibi risklerle her an karşı karşıyadırlar. (Siponen, 2000: 32) Bu bağlamda bakıldığında,

güvenlik ve gizlilik, bilişim teknolojilerinin kullanımında bireylerin en hassas oldukları iki noktayı oluşturmakta (Turn ve Ware, 1976: 140) ve bilgi teknolojilerinin gelişimine bağlı olarak evrim geçirmektedir. (Wieczorkowski ve Polak, 2017: 71)

Kişisel veri denince yalnızca isim, soy isim, doğduğu yer, doğduğu tarihi vb. bilgileri kapsamadığı ilave olarak da şahısların sahip oldukları sosyo - kültürel durumları, fiziki varlıkları, ruhsal ve maddi bütün tanımlayıcı bilgiyi içerdiği belirtilmiştir. Kişisel veriler çerçevesinde bireyin her türlü kimliklerinin bilgisine ilave, vergi, pasaport , sosyal güvenlik numaraları, sürücü belgesi bilgileri, araç plakası, ikamet, iş , elektronik-posta adresleri, sabit – mobil telefon numaraları, faks , CV si, kişisel fotoğrafları, videoları, sağlık bilgilerini kapsayan kan - genetik bilgileri, sabıka geçmişi ve adli sicil kayıtları benzeri bireyin tanımlı ya da tanımlanabilir durumunu ortaya çıkaran bütün bilgi ve veriler özel kişisel veri sayılabilmektedir. (Li, 2015: 44)

Daha geniş networklerin oluşması, internet kullanıcılarının sayısının artması, bilgi teknolojileri altyapılarının gelişmesi ve özel/kamu sektörlerinin temel faaliyetlerini yerine getirmeleri için bilgi teknolojilerine olan ihtiyaçlarının artması, bilgi güvenliği ve gizlilik unsurlarını zamanla daha fazla önemli hale getirmiştir (OTA, 1994). Buna karşın, bilgi güvenliği tehditleri ve buna bağlı oluşan kişisel düzeydeki gizlilik ihlalleri *(invasion of privacy*) aynı zamanda stres yaratan bir faktör olarak görülmektedir. (Lee vd. 2016: 63) tarafından, bilgi güvenliğinde stres faktörleri üzerine gerçekleştirilen bir araştırmanın bulguları, gizlilik ihlalinin, bilgi güvenliğinde stres yaratan bir değişken olduğunu doğrulamaktadır. Genel olarak ihlal, birçok araştırmada da (Wang vd, 2008; 3002; Shu vd, 2011:932; Tarafdar vd, 2007:315; Ragu-Nathan vd, 2008: 3005) bir tekno-stress kaynağı olarak değerlendirilmektedir.

Ülkemizde 07/Nisan/2016 tarihli resmi gazete ile yayınlanarak 6698 sayılı Kişisel Verilerin Korunması Kanun (KVKK) yürürlüğe girmiştir. Sorumluların üstleneceği temel ilkeler ve uygulama prensipleri belirlenmiştir. Kişisel veriler aşağıdaki prensiplere göre işlenmek zorundadır.

a) Hukuka ve dürüstlük kurallarına uygun olma,
b) Doğru ve gerektiğinde güncel olma,
c) Belirli, açık ve meşru amaçlar için işlenme,
d) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma,

e) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli süre kadar muhafaza edilme, KVKK-madde4 (http:/www.kisiselverilerinkorunması.org)

KVKK' ya göre kişisel veriler, kanunda belirlenen özel durumlar haricinde, ilgili kişinin açıkça onayı olmaksızın, kullanılamaz ve aktarılamaz.
(http:/www.kisiselverilerinkorunması.org)

Örneğin kurumlarda, video kamera uygulamaları hukuka ve dürüstlük kuralına uygun olmalı. Gizli kamera ile çekim yapılamaz. Belirli açık ve meşru amaç için kullanılmasına göre ise, ancak iş sağlığı ve güvenliği , genel güvenlikle ilgili olursa kabul edilebilir. İşçilerin soyunma odalarına konulamaz. Başka bir örnek vermek gerekirse, iş başvurularında adayın verdiği referansı haricinde, aday hakkında bilgi toplanması, Avrupa hukukunda kabul edilmeyen bir davranış olarak kabul edilmektedir. Ayrıca insan kaynakları uygulamalarında çok uluslu şirketler daha dikkatli olmak zorundalar, özellikle bulut sistemi ile çalışanların verileri kolayca aktarılabilmektedir.

Chunghun Lee, Choong Lee, Suhyunh Kim çalışmasında bazı önemli bulgular bulunmuştur. İlk olarak İş yükü ve Gizlilik ihlali Bilgi Güvenliği stresine neden olmaktadır. İkinci olarak İş Yükü, Bilgi Güvenliği Tekniği açısından daha büyük etkiye sahiptir. Son olarak, iş yükü bilgi güvenliği stresi üzerinde, gizliliğin ihlaline göre daha güçlü bir etkiye sahiptir. (Lee, vd, 2016: 64)

Chunghun Lee, Choong Lee, Suhyunh Kim çalışmasının çeşitli pratik sonuçları oluşmaktadır. Öncelikle gizliliğin ihlali Bilgi Güvenliği Stresi üzerinde önemli bir etkisi vardır. Çünkü Bilgi Güvenliği önlemek için izleme üzerine odaklanır. (Udo 2001: 168) Strese yol açan, şirketlerde çalışanların her hareketini gerçek zamanlı izleme gerçekleştirir. Önerimiz, şirketlerin güvenli yazılım kullanmaları ile yetkilendirme ve erişim haklarını uygularken Bilgi Güvenliğini sağlarken Stresi de azaltacaktır. (Chunghun Lee, vd, 2016: 63) ikinci olarak aşırı iş yükü Bilgi Güvenliği Stresi üzerinde önemli bir etkiye sahiptir. Bu teknik güvenlikli merkezlerde daha büyüktür. Normal görevlerine ilave olarak güvenlikle ilgili yükler ilave geldiğinden dolayı, teknik güvenlik talepler ve yönetsel güvenlik talepler fazladır. Bundan dolayı da Teknik Güvenlik talepler çalışanın verimliliğini düşürür. Çünkü birçok sıkı şifreleme, kısıtlamalar, limitli internet kullanımı gibi uygulamalar çalışanların normal iş yüklerine ilave yükler getirerek verimliliklerini düşürür. (Chunghun Lee, vd, 2016: 65)

Çalışanlarla iletişim çok önemli ve gereklidir. Bilgi güvenliği stresine uyumlu tutum oluşması, iş yükünün ve gizlilik ihlalini azaltır.

Ayrıca Bilgi Güvenli Stresinin hedefi hakkında bilgilendirme yapmak, çalışanların inanması bakımından çok önemlidir. Bilgi Güvenli Stresinin amacının onları izlemek değil işletme açısından kritik bilgileri korumak olduğunu anlatmak gerekir. (Bulgurcu, vd, 2010: 524). Eğitimler, kampanyalar, şirket içi Bilgi Güvenliği Politikalarına pozitif tutum oluşturabilir. (Hentea, 2005: 173).

Bilgi güvenliği politikasında, temel olarak Bilgi güvenliği eğitimi verilmesi, çalışanların bu konuya karşı dirençleri azaltır. Çünkü çoğu çalışan bilgi güvenliği koruma ile ilgilenmez. (Furnell, vd, 2002:15; Thomson ve von Solms,1998: 167 ; Udo, 2001: 166).

Ayrıca, Bilgi güvenliği uyum eğitimleri ile çalışanları motive etmeliler, bu eğitimlerle korsan saldırılar, hackerların tehditlerinden korunmalar tam olarak anlaşılması sağlanabilir. (Bulgurcu, vd, 2010: 524).

6.2. İş Engeli

(Bulgurcu, vd, 2010: 531) iş engelini, bir çalışanın bilgi güvenliği politikalarına uyum sağlamaya çalışırken günlük olarak işiyle ilgili görevleri yerine getirmesini engelleyen ya da zarar veren durum olarak tanımlamaktadır. Çalışmada iş engeli, çalışanlar tarafından bilgi güvenliği politikalarına uyumun getirdiği bir maliyet olarak değerlendirilmektedir. Aynı çalışmada, bilgi güvenliği gereksinimlerinin zaman kaybı yarattığı ve bu yönüyle bilgi güvenliği politikalarına uygun tutum geliştirme sürecine iş engellerinin negatif etkilerinin olduğu bulgulanmıştır. Diğer bir çalışmada (Li, 2015: 44) bilgi güvenliği politikalarının yarattığı iş engellerinin, kullanıcıların yararlı olabilecek güvenlik aksiyonları (IT support, monitoring) almalarını engelleyen ya da güçleştiren unsurlar olduğu ifade edilmektedir. Bilgi güvenliği politikaları, çalışanlar için belirli oranlarda iş yükü (workload) yaratmakta, iş yükü ise zaman kaybı yaratmaktadır. Söz konusu zaman kaybı ise iş engeli oluşturmaktadır. (Frangopoulos, 2013: 56) Bilgi güvenliği uygulamalarının yarattığı yüksek düzeyde iş yükü, bilgi güvenliği sisteminin fonksiyonel düzeyde zayıflamasına, insan kaynaklı hataların ortaya çıkmasına ve bir bütün olarak bilgi güvenliği sisteminin performansının düşmesine neden olmaktadır.

(Kraemer, vd, 2009: 510) Aşırı iş yükü aynı zamanda bilgisayar kullanıcılarının da performansını düşürecek etkiler yaratmaktadır.

İşletmeler teknik güvenlik sistemlerini adapte edebilirlerse, bilgi güvenliği stresine iş yükü daha fazla etki etmektedir, gizlilik ihlaline göre. İşletmler daha fazla yoğunlaşmak zorundalar fazla iş yüküne, çalışanların gizlilik ihlallerinden. Teknik güvenlik sistemleri, çalışanlara ilave görevler getireceği gibi onların rutin işlerinde zorunlu değişikliklere neden olabilir. (Chunghun Lee, vd, 2016: 65)

Bulgurcu'nun Bilgi Güvenliği Politikası farkındalığının, tutumlar üzerine etkisini aşağıdaki yapısal model testini görebiliriz. Bu çalışmada 3 çeşit inanç sınıfını görebiliriz. Uygunluğun faydası – uygunluğun maliyeti ve uyumsuzluk maliyeti olarak. (Bulgurcu, vd, 2010: 529)

Bilgi güvenliği farkındalığı ve genel farkındalık, çalışanın Bilgi güvenliğine uyma niyetine doğrudan veya dolaylı olarak, uyum sağlama davranışı olarak etkiler. Bizim daha çok üzerinde duracağımız konu ise iş engelinin uygunluk maliyetine direk etki ettiğini görülmektedir.

6.3. Bilgi Güvenliğinde Stres

Bilgi güvenliği politikalarına uyuma etki eden bir bileşen olarak stres de son yıllarda araştırmalara konu edilmektedir.(Lee, vd, 2016: 65), bilgi güvenliği stresini anlamak amacıyla bilgi güvenliği uyum aktivitelerinin türlerini araştırdığı çalışmasında, kişi-çevre uyum teorisine dayanarak çalışanların nasıl stres yüklendiği, bilgi güvenliği stresinin (ISS) arkasındaki faktörlerin neler olduğu ve yönetimsel ve teknik güvenlik odaklı organizasyonlar arasındaki farkları incelediği çalışmasında aşırı iş yükünün ve mahremiyet ihlalinin, bilgi güvenliği stres etmenleri olduğunu göstermiştir. (Chunghun Lee, vd, 2016: 68) Benzer şekilde Ament ve Haag (2016) da bilgi güvenliği bilincini artırmak amacıyla gerçekleştirilen faaliyetlerin çalışanlarda strese neden olduğunu ortaya koymuştur. (Ament, Haag, 2016: 14)

Bilgi güvenliğinde stres kavramı, tekno-stres olgusu ile doğrudan ilişkilidir. Tekno-stres kavramı, bilgi ve iletişim teknolojilerinin gelişimine paralel olarak, çoğunlukla yeni teknolojilere uyum sağlanmakta zorlanılan, çalışanların görevlerini yerine getirmeleri için gereken düzeyde beceriye ya da yetkinliğe sahip olmadığı

koşularda ortaya çıkan (Tarafdar vd., 2007: 312; Park ve Im, 2012: 69) teknoloji kaynaklı stres durumunu ifade etmek için kullanılmaktadır. Yoğun cep telefonu ve bilgisayar kullanımı, e-mail trafiği, elektronik mesajlaşma, gün içinde yoğun telefon görüşmeleri, devamlı surette şifre kullanma/güncelleme, yazılım güncelleme, siber ataklara maruz kalma vb. faktörler teknolojik bazlı strese neden olabilmektedir. Bilişim ortamında bilgiyi kaybetme korkusu, kişisel bilgilerin ihlali ve güvenlik sorunu, hızlı işlem yapmaya bağlı hata yapma korkusu, teknoloji temelli iş yükü artışı olası tekno-stres kaynakları arasında gösterilmektedir. (Mahboob ve Khan, 2016: 29; Salanova vd., 2013:28).

7. BİLGİ GÜVENLİĞİNDE STRES İŞ TATMİNİ İLİŞKİSİ

Bilgi güvenliğinde stresin iş tatmini ile ilişkisinin araştırıldığı çalışmalarda genellikle bilgi güvenliğinde stresin iş tatminini negatif etkilediğine ulaşılmaktadır. (Kumar, vd, 2013: 2), toplam 80 bilgi güvenliği profesyoneli ile gerçekleştirdiği çalışmasında, bilgi güvenliğindeki stres faktörünün iş tatminini ve bağımlılığını açıkça negatif etkilediğini ortaya koymuştur. Benzer şekilde (Khan, vd, 2013: 9) de Pakistan'da 148 kütüphane görevlisi ile gerçekleştirdikleri çalışmalarında bilgi güvenliğinde stresin iş tatminini olumsuz etkilediğini belirlemiştir. (Khan, vd, 2013: 10)

İlgili literatürde, tekno-stres ile iş tatmini arasındaki ilişkiyi irdeleyen araştırmalara rastlamak mümkündür. (Ragu-Rathan, vd, 2008: 418), yapısal eşitlik modellemesi ile 608 son kullanıcı üzerinde gerçekleştirdikleri bir araştırmanın sonuçlarına göre; tekno-stres yaratan faktörlerin (tekno-işyükü, tekno-ihlal, tekno-karmaşıklık, tekno-güvenlik ve tekno-belirsizlik) iş tatminini azalttığı yönünde bulgulara ulaşılmıştır. Bir başka araştırmada (Tarafdar vd, 2007: 320), tekno-stres faktörlerinin psikolojik ve davranışsal gerginlik üzerindeki etkileri incelenmiş, teknoloji temelli stres unsurlarının çalışanların iş tatminini azaltıcı etkilerinin olduğu bulgulanmıştır. Aynı araştırmada ayrıca tekno-stres faktörlerinin örgütsel bağlılık, yenilikçi davranış ve kullanıcı tatminini olumsuz yönde etkilediği de ifade edilmektedir. (Tarafdar, vd, 2007: 321) Benzer biçimde diğer araştırmalar da (Jena, 2015: 118; Kumar vd., 2013: 2), tekno-stresin iş tatmini üzerinde negatif etkiye sahip olduğu bulgusuna ulaşmışlardır. (Jena, 2015: 122) Tekno-stres sadece iş tatminini değil, benzer biçimde çalışanların verimini düşürecek etkiler de ortaya çıkarmaktadır. (Tu vd., 2005: 80).

Bilgi güvenliği, yönetsel, fiziksel ve teknolojik kontrol olmak üzere 3 boyutlu bir yapıyı gerekli kılmaktadır. Yönetsel güvenlik boyutu; bilgi koruma politikası oluşturmak, örgütsel yapı ve bağlantılı sorumlulukları tasarlamak, kritik bilgi varlıklarını tanımlamak, süreci yönetecek işgücünü istihdam etmek, gelecek kriz senaryoları oluşturmak ve sistematik denetimler yapmak olarak ifade edilebilecek faaliyetler içermektedir. Teknolojik kontrol boyutu; bilgisayarların ve networklerin yönetimi, sistem giriş kontrolleri, sistem geliştirme, bakım kontrolleri gibi çalışmaları gerekli kılmaktadır. Fiziksel kontrol boyutunda ise bilgisayar ünitelerinin ve gerekli malzeme ihtiyaçlarının yönetimi gündeme gelmektedir. (Jeong ve Jeong, 2011:74). Bu bağlamda, bir tekno-stres kaynağı olarak bilgi güvenliği uygulamalarının yarattığı sorumluluklar ve iş yükü çalışanlar nezdinde stres yaratabilmektedir ve bu stres faktörü çalışanların iş tatminini negatif yönde etkilemektedir (Park ve Cho, 2016: 70). Bulgurcu vd, (2010: 541), bilgi güvenliği uygulamalarının ortaya çıkardığı iş engellerinin çalışanlar nezdinde stres yarattığını bulgulamışlardır.

III. BÖLÜM
BİLGİ GÜVENLİĞİ UYGULAMALARININ BİREY DÜZEYİNDEKİ YANSIMALARI ÜZERİNE BİR ARAŞTIRMA

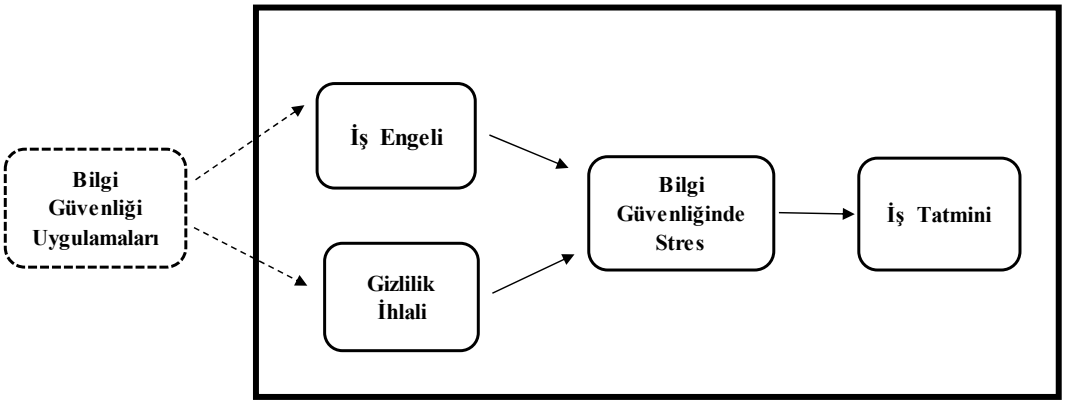
1. ARAŞTIRMANIN AMACI

İş tatmini işletmelerin en önemli sermayesi olan insan kaynaklarını elde tutabilmenin anahtarlarından biridir. Yüksek iş tatminine sahip olan çalışanların işletmeye daha fazla bağlanacağı ve ayrılmak istemeyeceği açıktır. Bu nedenle de işletmeler için çalışanların tatminini sağlamak ana hedeflerin başında gelmelidir. İş tatminini etkileyen birçok farklı unsur bulunuyorsa da bu çalışma iş tatmine farklı bir açıdan bakmayı amaç edinmiş ve Bursa orjinli Ar-Ge merkezi olan firmalar üzerinde bilgi güvenliği uygulamalarının yarattığı iş engeli, gizlilik ihlali ve stresin iş tatmini üzerindeki etkilerini araştırmak amacıyla gerçekleştirilmiştir.

2. MODEL VE HİPOTEZLER

Bilgi güvenliği uygulamalarının yarattığı iş engeli, gizlilik ihlali ve stresin iş tatmini üzerindeki etkilerini analiz etmek üzere Şekil 8'deki model esas alınmıştır. İş engeli, gizlilik ihlali ve stres bağımsız değişkenler olarak modele dahil edilirken, iş tatmini bağımlı değişken olarak esas alınmıştır. Bu kapsamda ilgili model ve hipotezler aşağıda ifade edilmektedir.

Şekil 6: Araştırmanın Modeli



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

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

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

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

3. ARAŞTIRMANIN METODU, ÖRNEKLEM VE ÖLÇME ARAÇLARI

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

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

politikalarıyla uyumlu süreçler geliştirmiş firmalar tercih edilmiştir. Bu kapsamda, otomotiv, tekstil, cam ve kablo endüstrilerinden olmak üzere toplam 215 çalışan üzerinde anket uygulaması gerçekleştirilmiştir.

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

İş Engeli Ölçeği: İş engeli ölçeği, (Bulgurcu, vd, 2010: 535) çalışmalarında yer alan 3 ifadeden oluşmaktadır. Araştırmada cronbach alpha değeri 0.92 olarak olarak tespit edilmiştir. Bu araştırmada ise iş engeli ölçeğinin cronbach alpha katsayısı 0.88 seviyesindedir. İş engeli ölçeğinde, Hiçbir Zaman (1) - Her Zaman (5) skalası kullanılmıştır.

Gizlilik İhlali Ölçeği: Gizlilik ihlali ölçeği, (Ayyagari, vd, 2011: 839) tarafından geliştirilen 4 ifadeden oluşmaktadır. Bu çalışma için sözkonusu ifadelerden 3 tanesi araştırmaya dahil edilmiştir. Sözkonusu ifadeler için orijinal kaynakta tespit edilen cronbach alpha değeri 0.88 değerinin üzerindedir. Bu araştırmada ise 3 ifadenin cronbach alpha katsayısı 0.87 olarak tespit edilmiştir. Ölçekte, Kesinlikle Katılmıyorum (1) - Kesinlikle Katılıyorum (5) skalası kullanılmıştır.

Bilgi Güvenliğinde Stres Ölçeği: Bilgi güvenliğinde stres ölçeği, (Ayyagari, vd, 2011: 839) tarafından geliştirilmiştir ve 8 ifadeden oluşmaktadır. Orijinal ölçekte cronbach alpha değeri 0.88 değerinin üzerinde tespit edilmiştir. Bu araştırmada ise stres ölçeği için belirlenen güvenilirlik katsayısı 0.93 düzeyindedir. Ölçekte, Kesinlikle Katılmıyorum (1) - Kesinlikle Katılıyorum (5) skalası kullanılmıştır.

İş Tatmini Ölçeği: İş tatminini ölçümlemek üzere (Cammann, vd, 1983: 130) tarafından kullanılan 2 ifadeye yer verilmiştir. Camman araştırmalarında iş tatmini ölçeğinin güvenilirlik katsayısını 0.90 olarak tespit etmişlerdir. Sözkonusu iki ifade için bu araştırmada cronbach alpha katsayısı ise 0.89 olarak bulgulanmıştır. Ölçekte, Kesinlikle Katılmıyorum (1) - Kesinlikle Katılıyorum (5) skalası kullanılmıştır.

Tüm ölçeğin güvenilirlik katsayısı 0.89 seviyesindedir.

Tablo 8**:** Modelde yer alan değişkenlere ait ölçekler, ifadeler ve kaynaklar

Değişkenler	İfadeler	Kaynak
İş Engeli	1. Bilgi güvenliği gerekliliklerini yerine getirirken günlük olarak yaptığım işi aksatabiliyorum. 2. Bilgi güvenliği gerekliliklerini yerine getirirken yöneticilerime, çalışma arkadaşlarıma ya da müşterilere zamanında geri dönemiyorum. 3. Bilgi güvenliği gerekliliklerini yerine getirmeye çalışırken işimdeki verimliliğin azaldığını düşünüyorum.	Bulgurcu vd, (2010)
Gizlilik İhlali	1. İletişim teknolojilerini (e-mail, skype, cep telefonu aplikasyonları vb.) kullanırken, bilgi güvenliği kapsamında bile olsa takip ediliyor olmam beni rahatsız ediyor. 2. Bilgi güvenliği faaliyetleri kapsamında izleniyor olmam dolayısıyla özel yaşantımın ihlal edildiğini düşünüyorum. 3. Bilgi güvenliği faaliyetleri neden gösterilerek işverenin çalışanları takip ettiğini düşünüyorum.	Ayyagari vd, (2011)
Bilgi Güvenliğinde Stres	1. Bilgi güvenliği politikalarının yarattığı gereklilikleri yerine getirirken yorulduğumu hissediyorum. 2. Tüm gün bilgi güvenliği gerekliliklerini yerine getirmek bende stres yaratıyor. 3. Bilgi güvenliği politikalarının yarattığı gereklilikleri yerine getirirken tükendiğimi hissediyorum. 4. Kurumumdaki bilgi güvenliği faaliyetleri kapsamında benden talep edilenler, işimi yaparken ilave yük yaratıyor. 5. Kurumumdaki bilgi güvenliği faaliyetleri kapsamında yürütülen işler problemler yaratabiliyor. 6. Kurumumdaki bilgi güvenliği faaliyetleri kapsamında yürütülen işlerle ilgili şikâyetler duyuyorum. 7. Bilgi güvenliğini ilgilendiren işler beni fazlasıyla meşgul ediyor, zaman kaybına neden oluyor. 8. Bilgi güvenliğini ilgilendiren işleri yaparken baskı altında hissediyorum.	Ayyagari vd, (2011)
İş Tatmini	1. İşimden genel olarak memnunum. 2. Genel olarak bu kurumda çalışmayı seviyorum.	Cammann vd, (1983)

4. BULGULAR

4.1. Tanımlayıcı İstatistik Verileri

Tablo 9'da ölçekte yer alan ifadelerin tanımlayıcı istatistikleri görülmektedir. Buna göre katılımcılar işlerinden genel olarak memnun (ortalama 4,02 ve standart sapma 0,80) ve genel olarak çalıştığı kurumda çalışmayı sevmektedir (ortalama 4,14 ve standart sapma 0,72).

Tablo 9: Tanımlayıcı İstatistikler

	Ortalama	Standart Sapma
İşimden genel olarak memnunum.	4,02	0,80
Genel olarak bu kurumda çalışmayı seviyorum.	4,14	0,72
Bilgi güvenliği gerekliliklerini yerine getirirken günlük olarak yaptığım işi aksatabiliyorum.	1,84	0,89
Bilgi güvenliği gerekliliklerini yerine getirirken yöneticilerime, çalışma arkadaşlarıma ya da müşterilere zamanında geri dönemiyorum.	1,75	0,84
Bilgi güvenliği gerekliliklerini yerine getirmeye çalışırken işimdeki verimliliğin azaldığını düşünüyorum.	1,74	0,84
İletişim teknolojilerini (e-mail, skype, cep telefonu aplikasyonları vb.) kullanırken, bilgi güvenliği kapsamında bile olsa takip ediliyor olmam beni rahatsız ediyor.	2,97	1,26
Bilgi güvenliği faaliyetleri kapsamında izleniyor olmam dolayısıyla özel yaşantımın ihlal edildiğini düşünüyorum.	2,85	1,20
Bilgi güvenliği faaliyetleri neden gösterilerek işverenin çalışanları takip ettiğini düşünüyorum.	2,70	1,13
Bilgi güvenliği politikalarının yarattığı gereklilikleri yerine getirirken yorulduğumu hissediyorum.	1,94	0,90
Tüm gün bilgi güvenliği gerekliliklerini yerine getirmek bende stres yaratıyor.	1,84	0,95
Bilgi güvenliği politikalarının yarattığı gereklilikleri yerine getirirken tükendiğimi hissediyorum.	1,64	0,84
Kurumumdaki bilgi güvenliği faaliyetleri kapsamında benden talep edilenler, işimi yaparken ilave yük yaratıyor.	1,90	0,90
Kurumumdaki bilgi güvenliği faaliyetleri kapsamında yürütülen işler problemler yaratabiliyor.	1,87	0,90
Kurumumdaki bilgi güvenliği faaliyetleri kapsamında yürütülen işlerle ilgili şikâyetler duyuyorum.	1,86	0,86
Bilgi güvenliğini ilgilendiren işler beni fazlasıyla meşgul ediyor, zaman kaybına neden oluyor.	1,78	0,86
Bilgi güvenliğini ilgilendiren işleri yaparken baskı altında hissediyorum.	1,65	0,89

4.2. Demografik Bulgular

Katılımcıların demografik özellikleri Tablo 10'da görülmektedir. Buna göre; Katılımcıların çoğunluğu erkek olup, katılımcıların çoğunluğu 31-40 yaş aralığında olduğu görülmektedir. Eğitim durumuna baktığımızda katılımcıların çoğunluğu lisans mezunudur. Kıdeme bakıldığında, katılımcıların çoğunluğu 1 ila 5 yıllık kıdeme sahiptir. Katılımcıların çoğunluğu Ar-Ge departmanında çalışmaktadır.

Tablo 10: Demografik Özellikler

		N	%			N	%
Cinsiyet	*Kadın*	81	37,7	**Kıdem**	*1 yıldan az*	27	12,6
	Erkek	134	67,3		*1-5 yıl*	74	34,4
Yaş	*20 yaşına kadar*	-	-		*6-10 yıl*	44	20,5
	21-30	68	31,6		*11-15 yıl*	24	11,2
	31-40	97	45,1		*16 yıl ve üstü*	46	21,4
	41-50	39	18,1	**Departman**	*Ar-Ge*	35	16,3
	51 ve üstü	11	5,1		*Finansman*	21	9,8
Eğitim	*İlköğretim*	-	-		*Muhasebe*	30	14
	Lise	8	3,7		*İnsan Kaynakları*	14	6,5
	Ön Lisans	5	2,3		*Satın Alma*	6	2,8
	Lisans	160	74,4		*Bilgi İşlem*	9	4,2
	Yüksek Lisans	39	18,1		*Pazarlama Satış*	24	11,2
	Doktora	3	1,4		*Lojistik*	28	13
					Üretim	21	9,8
					Diğer (Kalite, Dış Ticaret, İş Güvenliği)	27	12,6

4.3. Korelasyon Analizi

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

Tablo 11: İş engeli, gizlilik ihlali, bilgi güvenliğinde stres ve iş tatmini değişkenleri arasındaki korelasyonlar, ortalama, standart sapma ve cronbach alpha değerleri

Tablo 11: Korelasyon Analizi

	M	SD	Cronbach Alpha	İE	Gİ	BGS	İT
İş Engeli (İE)	1,78	0,77	0,88	1			
Gizlilik İhlali (Gİ)	2,84	1,07	0,87	,319**	1		
Bilgi Güvenliği Stresi (BGS)	1,81	0,73	0,93	,604**	,436**	1	
İş Tatmini (IT)	4,08	0,72	0,89	-0,075	,156*	,194**	1

**. Korelasyon 0,01 seviyesinde anlamlı.

*. Korelasyon 0,05 seviyesinde anlamlı.

4.4. Faktör Analizi

Araştırmada, yapısal eşitlik modellemesine alt yapı oluşturmak üzere Temel Bileşen Analizi (Principal Components Analysis-PCA) metodu ile faktör analizi uygulanmıştır. KMO ve Bartlett test sonucu (0.876, χ^2 =2516.882; *df*= 120; *p*=.000), verilerin bir faktör analizi için uygun olduğunu ortaya koymaktadır. Tüm ifadelerin öz değeri 1'den büyük 4 boyut altında toplandığı görülmüştür. 4 boyut için toplam açıklanan varyans %76.2 seviyesindedir. Faktörler ve faktör yükleri dağılımı Tablo 12'de görülmektedir.

Tablo 12: Faktör Analizi

	Faktör Yükleri				
	1	2	3	4	*Cronbach Alpha*
İş Engeli					**0,88**
Bilgi güvenliği gerekliliklerini yerine getirirken günlük olarak yaptığım işi aksatabiliyorum.	0,84				
Bilgi güvenliği gerekliliklerini yerine getirirken yöneticilerime, çalışma arkadaşlarıma ya da müşterilere zamanında geri dönemiyorum.	0,83				
Bilgi güvenliği gerekliliklerini yerine getirmeye çalışırken işimdeki verimliliğin azaldığını düşünüyorum.	0,78				
Gizlilik İhlali					**0,87**
İletişim teknolojilerini (e-mail, skype, cep telefonu aplikasyonları vb.) kullanırken, bilgi güvenliği kapsamında bile olsa takip ediliyor olmam beni rahatsız ediyor.		0,90			
Bilgi güvenliği faaliyetleri kapsamında izleniyor olmam dolayısıyla özel yaşantımın ihlal edildiğini düşünüyorum.		0,90			
Bilgi güvenliği faaliyetleri neden gösterilerek işverenin çalışanları takip ettiğini düşünüyorum.		0,76			
Bilgi Güvenliğinde Stres					**0,93**
Bilgi güvenliği politikalarının yarattığı gereklilikleri yerine getirirken yorulduğumu hissediyorum.			0,82		
Tüm gün bilgi güvenliği gerekliliklerini yerine getirmek bende stres yaratıyor.			0,81		
Bilgi güvenliği politikalarının yarattığı gereklilikleri yerine getirirken tükendiğimi hissediyorum.			0,78		
Kurumumdaki bilgi güvenliği faaliyetleri kapsamında benden talep edilenler, işimi yaparken ilave yük yaratıyor.			0,70		
Kurumumdaki bilgi güvenliği faaliyetleri kapsamında yürütülen işler problemler yaratabiliyor.			0,74		
Kurumumdaki bilgi güvenliği faaliyetleri kapsamında yürütülen işlerle ilgili şikâyetler duyuyorum.			0,69		
Bilgi güvenliğini ilgilendiren işler beni fazlasıyla meşgul ediyor, zaman kaybına neden oluyor.			0,80		
Bilgi güvenliğini ilgilendiren işleri yaparken baskı altında hissediyorum.			0,77		
İş Tatmini					**0,89**
İşimden genel olarak memnunum.				0,94	
Genel olarak bu kurumda çalışmayı seviyorum.				0,04	

4.5. Doğrulayıcı Faktör Analizi

Doğrulayıcı faktör analizi, belirlenen bir ölçme modelinin tutarlılığının istatistiksel olarak anlamlı olup olmadığını test etmek amacıyla yapılmaktadır.

Doğrulayıcı faktör analizi, geleneksel yöntemle yapılan faktör analizlerinden farklı olarak, daha önceden araştırmacı tarafından belirlenmiş bir faktöryel yapının doğrulanmasını test etmek amacıyla kullanılmaktadır. Bu tür çalışmalarda, ölçek maddeleri tarafından yapılandırıldığı düşünülen birden fazla örtük (latent) değişkenin, bir başka örtük değişken tarafından açıklandığı varsayılır ve bu varsayımın veriye uygunluğu test edilir (Gürbüz ve Şahin, 2015: 326).

Model uygunluğunun değerlendirilmesinde kullanılan birbirinden farklı uyum iyiliği indeksleri ve bu indekslerin sahip olduğu istatistiksel fonksiyonlar bulunmaktadır. Analizde, uyum iyiliği indeksi (goodness of fit index-GFI), standardize edilmiş kök ortalama kare artık (Standardized RMR) ve kök ortalama kare yaklaşım hatası (Root mean square error of approximation-RMSEA), Bentler karşılaştırmalı uyum indeksi (Bentler Comparative Fit Index-CFI) dikkate alınmaktadır. Sözkonusu modelin ölçme gücünün tespitinde yukarıda ifade edilen indekslerin belirli uyum değerlerine sahip olması beklenmektedir. Bu değerler Tablo 13'de yer almaktadır.

Tablo 13: Doğrulayıcı Faktör Analizi

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

Elde edilen veriler kapsamında, araştırma modelinin ölçme gücünü veya diğer bir deyimle ölçme aracının geçerliliğini sınamak amacıyla AMOS istatistiksel paket programı aracılığı ile doğrulayıcı faktör analizi yapılmıştır. Analiz çerçevesinde, iş engeli, gizlilik ihlali, bilgi güvenliğinde stres ölçekleri ve tüm model bazında indeks uyum değerleri hesaplanmıştır. Sonuçlar Tablo 14'de görülmektedir. Uyum iyiliği değerlerinin genel olarak kabul edilebilir limitler arasında olduğu ve dolayısıyla ölçme aracının geçerliliğinin bulunduğu tespit edilmiştir.

Tablo 14:Ölçme Aracının Geçerliliği

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

Normallik testi sonuçlarına bakıldığında, araştırmada kullanılan değişkenlerin çarpıklık ve basıklık değerlerinin genel olarak -1 ile +1 arasında yer aldığı görülmüştür. Skewness ve kurtosis değerlerinin, -1 ile +1 arasında yer alması halinde normallik varsayımının karşılandığı ifade edilmektedir (Kalaycı, 2005: 73).

4.6. Yapısal Eşitlik Modellemesi

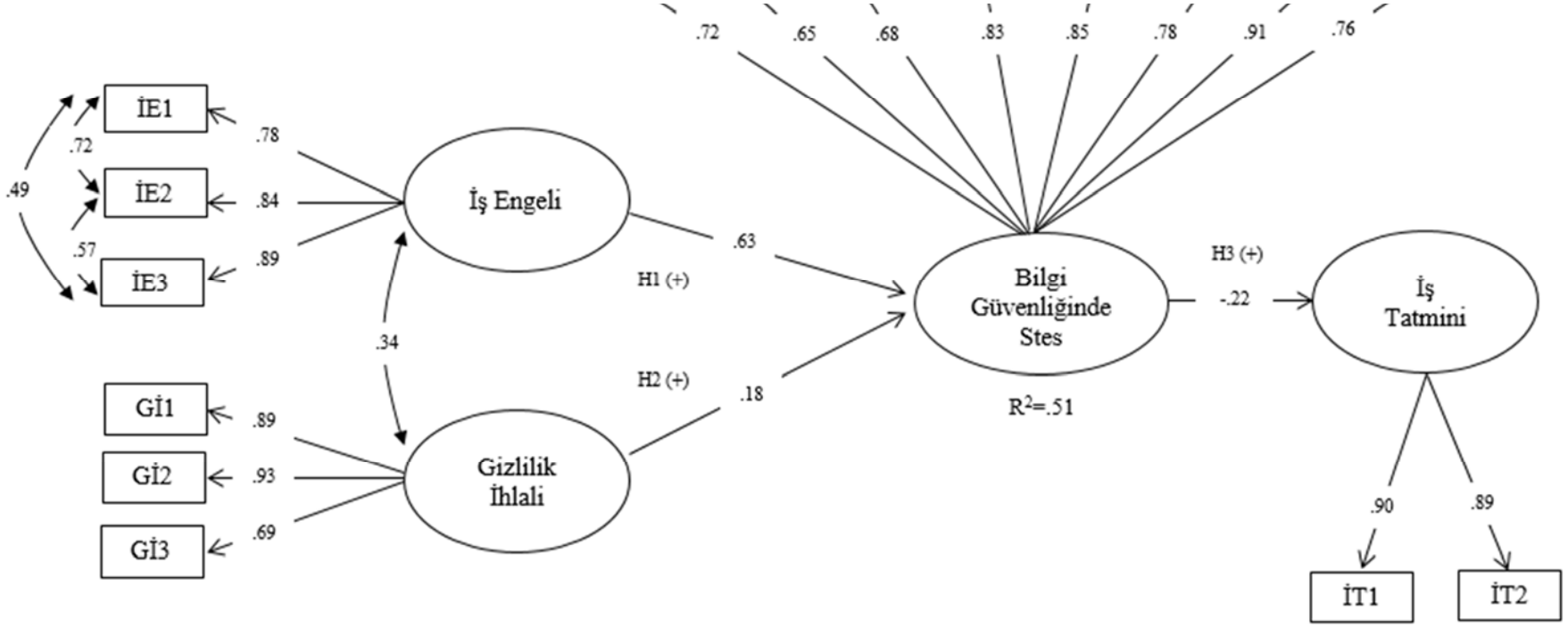
Modelde yer alan ifadelerin genel anlamda faktör yükleri ve bağımsız değişkenlerin bağımlı değişkeni açıklama düzeyi yüksektir. Bu kapsamda, iş engeli, gizlilik ihlali ve bilgi güvenliğinde stres bağımsız değişkenleri, iş tatmini bağımlı değişkeni (R^2= 0.51) düzeyinde açıklamaktadır.

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

Yapısal eşitlik modellemesi sonuçları incelendiğinde, iş engelinin, bilgi güvenliğinde stres değişkeni üzerinde pozitif bir etkiye sahip olduğu bulgulanmıştır (parametre tahmini=.618; p=.000). Bu bağlamda, "H1: Bilgi güvenliği uygulamalarının yarattığı iş engelleri, stres değişkeni üzerinde pozitif etkiye sahiptir." hipotezi kabul edilmiştir. Diğer taraftan, gizlilik ihlali değişkeninin de bilgi güvenliği değişkeni üzerinde pozitif bir etkiye sahip olduğu tespit edilmiştir (parametre tahmini=.153; p=.005). Dolayısıyla, "H2: Bilgi güvenliği uygulamalarının yarattığı gizlilik ihlali algısı, stres değişkeni üzerinde pozitif etkiye sahiptir." hipotezi de kabul edilmiştir. Son olarak, bilgi güvenliğinde stres değişkeninin, iş tatmini üzerindeki etkilerine bakılmıştır. Analiz sonuçları, bilgi güvenliğinde stres değişkeninin, iş tatmini değişkeni üzerinde negatif

etkiye sahip olduğunu doğrulamaktadır (parametre tahmini= -.203; p=.006). Bu çerçevede, “H3: Bilgi güvenliği uygulamalarının yarattığı stres, çalışan tatmini üzerinde negatif etkiye sahiptir.” hipotezi kabul edilmiştir. Genel olarak, araştırmanın tüm hipotezleri kabul edilmiştir. Yapısal eşitlik modellemesi analiz sonuçları toplu olarak Şekil 9’da görülmektedir.

Şekil 7. Şekil 7: Yapısal Eşitlik Modellemesi Sonuçları



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

SONUÇ VE ÖNERİLER

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

Bilgi güvenliği politikaları diğer taraftan çalışanları bireysel olarak etkileyecek sonuçlar da yaratmaktadır. Bilgi güvenliği politikalarının yarattığı iş engelleri, gizlilik ihlali oluşturacak takip mekanizmaları, bilgi güvenliği bazında stresin ortaya çıkmasına neden olmaktadır. Genel anlamda, örgütsel stres kaynakları arasında birçok faktör sayılabilmekle birlikte, son zamanlarda teknoloji bazlı stres unsurlarının da örgütsel stresin nedenleri arasında ön plana çıktığı görülmektedir. (Kinman ve Jones, 2005: 115) çalışmalarında, özellikle yeni teknoloji kullanımının hızlı olmayı gerektirdiğini, düşünmeye zaman kalmadığını ve her şeyin standartlaştığını belirtmekte, bu durumun ise çalışanların stres düzeylerini arttırdığı ifade edilmektedir.

Araştırmada karşımıza çıkan ilk bulgu, bilgi güvenliği uygulamaları kapsamında ortaya çıkan iş engellerinin, bilgi güvenliğinde stres değişkeni üzerinde etkili olduğu yönündedir. (Bulgurcu, vd, 2010: 529), araştırmalarında çalışanların bilgi güvenliği politikalarına uyumun belirli oranlarda iş engeli yarattığını, bilgi güvenliği gereklilikleri çerçevesinde çalışanların zaman ayırmaları gerektiğini, bunun da günlük işleri göreli olarak aksattığını bulgulamışlardır. Bu araştırmayla, Bulgurcu et al. bulgusunu

tamamlayacak şekilde, bilgi güvenliği politikalarının neden olduğu iş engellerinin bir stres faktörü olduğu ve çalışanları negatif yönde etkilediği ortaya çıkmaktadır. Bu kapsamda, uygulamanın yapıldığı işletmelerde bilgi güvenliği uygulamalarının çalışanların günlük olarak yaptıkları işleri aksatabileceği, zaman yönetimi açısından sorunlar oluşturabileceği, iş verimliliğini azaltacak (Tu vd., 2005) etkiler yaratabileceği ve söz konusu negatif etkilerin bilgi güvenliğinde stres yaratabileceği yönünde tespitlere ulaşılmıştır. Diğer taraftan (Lee, vd, 2016: 65) yürüttükleri çalışmalarında, bilgi güvenliği uygulamalarının belirli oranlarda iş yükünü artırdığını ve bunun da çalışanların bilgi güvenli uygulamaları bağlamında strese neden olduğunu doğrulamaktadır. Dolayısıyla araştırmamız Lee nin bulgularını destekler niteliktedir.

Araştırmada dikkati çeken diğer bir önemli bulgu da bilgi güvenliği uygulamalarının ortaya çıkardığı gizlilik ihlali algısının çalışanların stres düzeyini artırmasıdır. Çalışanların iletişim teknolojilerinin kullanıma bağlı olarak takip edildikleri hissine kapılıyor olmaları, özel yaşantılarının ihlal edildiğini düşünüyor olmaları ve işveren tarafından takip edildiklerine dair algının varlığı bilgi güvenliği kapsamında çalışanlarda stres oluşturmaktadır. Bu sonuç, (Ayyagari, vd, 2011: 838) çalışmaları ile uyum göstermektedir. Ayyagari vd'in tekno-stres üzerine gerçekleştirdikleri araştırmanın bulguları, gizliliğin ihlal edildiğine dair bireysel algı ile stres arasında pozitif yönlü ilişkinin olduğunu ispatlamaktadır. Bilgi güvenliğinde stres faktörlerinin belirlenmesine dönük diğer bir araştırmada ise (Lee, vd, 2016: 65), gizlilik ihlalinin önemli bir bilgi güvenliği stres unsuru olduğu bulgulanmıştır.

Bu yönüyle mevcut araştırma Lee vd lerinin bulguları ile de paralel sonuçlar yaratmıştır. Gizlilik ihlali, doğrudan internet kullanıcılarının da en fazla hassasiyet gösterdikleri konuların başında gelmektedir. (Udo, 2001: 170) tarafından, internet ortamında alışveriş yapan kullanıcılar üzerinde gerçekleştirilen bir araştırmada, gizlilik ihlali ve güvenlik açıklarının internette alışveriş yapmayı engelleyen en önemli faktörler olduğu tespit edilmiştir. Dolayısıyla, kişisel gizliliği tehdit eden koşulların bilişim alanında farklı boyutlarda bile olsa bireyleri tedirgin ettiğini söylemek mümkündür.

Araştırmanın en dikkat çekici bulgusu ise bilgi güvenliğinde stres faktörlerinin, çalışanların iş tatmini üzerinde etkisidir. Bu bağlamda, bilgi güvenliği gerekliliklerini yerine getirirken çalışanların yorgunluk, tükenme ve stres hissettikleri ve bunun da iş

tatminini negatif yönde etkilediği saptanmıştır. Bilgi güvenliği bağlamında ortaya çıkan stres faktörlerinin (tekno iş yükü ve gizlilik ihlali), teknoloji kaynaklı olduğu varsayımı altında, tekno-stress unsurlarının iş tatminin negatif yönlü etkilediğini ortaya koyan araştırmalara rastlamak mümkündür. (Jena, 2015: 120), Hindistanlı akademisyenler üzerinde gerçekleştirdiği araştırmasında, tekno-stress faktörlerinin iş tatmini üzerindeki olumsuz etkilerine dikkat çekmiştir. (Qiu, 2013: 69), tekno-stress ile iş tatmini arasındaki bağ üzerine gerçekleştirdiği çalışmasında, tekno-stress unsurlarının iş tatminini etkileyen önemli bir değişken olduğunu vurgulamaktadır. Benzer biçimde (Khan, vd, 2013: 10), yine tekno-stress faktörlerinin iş tatminini negatif yönde etkilediğine dair bulgulara ulaşmışlardır. Dolayısıyla, bu araştırmada ortaya çıkan tekno-stress iş tatmini ilişkisi, literatürdeki benzer çalışmalar ile paralellik göstermektedir.

Bilgi güvenliği uygulamalarının yarattığı gizlilik ihlali algısının çalışanlar üzerine stres etkisine neden olmaktadır. Dolayısıyla bilgi güvenliği uygulamaları nedeniyle mahremiyetlerinin zarar gördüğünü düşünen çalışanların stres düzeyleri artabilmektedir. Bu nedenle bilgi güvenliği uygulamaları mahremiyet ihlaline yol açmayacak şekilde düzenlenmelidir. Bu kapsamda bilgi güvenliği uygulamaları bahanesiyle çalışanların iletişimleri kontrol edilmemelidir. Bu durum, özel konuşmalarının bir gün karşılarına çıkabileceği düşüncesi doğurabileceğinden çalışanlarda strese neden olabilmektedir.

Bilgi Güvenliği Uygulamaları kişisel performans kriteri olarak belirlenebilir. Bilgi Güvenliği Yönetimi de en zayıf halka olan insanın farkındalığı için ve güncel bilgilerin paylaşmasını revize etmek için – siber saldırıları – zayıf noktaları paylaşmak için yılda en az 1 defa tüm çalışanları bilgilendirmelidir.

Gelecekte yapay zeka, sanal gerçeklik başta olmak üzere, Bilgi Teknolojileri kullanımımız artarak gelişimini sürdüreceği kaçınılmaz bir gerçektir. Bu bağlamda siber saldırılar, bilgi iletişiminden kaynaklı problemler kaçınılmaz olacaktır. Bu tür tehditlerden korunmak için bilgi güvenliğinden sorumlu departmanı çalışanların farkındalık düzeylerini geliştirmeli, eğitim çalışmaları ile teknik donanımlarını artırmalıdır. Eğitim çalışmaları ile çalışanların öz yeterliliklerinin artması, stres düzeyinin azalmasına katkıda bulunacaktır.

Stres genel anlamda, iş tatmini ile negatif yönlü bir ilişkiye sahiptir. Stres, hata yapma olasılığını artırmaktadır. Aynı zamanda stres iş tatminini düşürerek işden ayrılma

ile sonuçlanabilecek bir koşul oluşturabilmektedir. Bu nedenle işverenlerin bilgi işlem uygulamalarından kaynaklanan stres unsurlarını dikkatlice takip etmeleri çok yararlı sonuçlar doğuracaktır. Bilgi işlem ve bilgi güvenliğinden sorumlu çalışanlarının, konularına çok hakim olması ve kendilerini yenileyen olması önemlidir. Bunlar diğer çalışanlarla iyi bir iletişim-eğitimle konun üzerine giderek çalışanlara daha fazla bilgilendirdikçe – eğitim verdikçe, donanım sahibi personel tedirginliklerinden, korkularından ve stresinde uzaklaşacağı kanaatindeyim. Genel anlamda da çalışan stresini azaltmak için, işletmeler spor, yoga gibi aktivitelerle çalışanlarına katkıda bulunabilirler.

Genel olarak denilebilir ki, ilk etapta bilişim ana ekseni çerçevesinde düşünülen bilgi güvenliği uygulamalarının esasen beşeri yapı ile çok yakından ilişkisi bulunmaktadır. Bilgi güvenliği politikalarının etkinliği ciddi bir oranda çalışanların uyma davranışı göstermelerine bağlıdır. Çalışanların kişisel ihmali ile ortaya çıkabilecek çok sayıda bilgi güvenliği tehdidi bulunmaktadır. Bilgi güvenliği açıklarının işletmelere mali, yönetsel ve toplumsal düzeyde yük getirdiği düşünüldüğünde, çalışanların konuya hassasiyetle yaklaşmaları gereği ve önemi daha net ortaya çıkmaktadır.

ARAŞTIRMANIN KISITLARI VE GELECEK ARAŞTIRMALAR İÇİN ÖNERİLER

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

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

KAYNAKÇA

ACILAR, A. (2009) "İşletmelerde Bilgi Güvenliği ve Örgüt Kültürü", *Organizasyon ve Yönetim Bilimleri Dergisi*, C. 1, S. 1, ss. 25-33.

ADEYEKE, W. B. Adeoti, "The Importance of management information systems, Library Review, Vol. 46, No. 5, 1997, ss. 318-327.

AJZEN, I. (1991). "The Theory of Planned Behavior", Organizational Behavior and Human Decision Processes, Vol. 50, 179-211

AJZEN, I. ve FISHBEIN, M. (1980). Understanding Attitude and Predicting Social Behavior, Englewood Cliffs, NJ: Prentice-Hall.

AKGÜN, A. ve KESKİN, H. (2003) "Sosyal Bir Etkileşim Süreci Olarak Bilgi Yönetimi ve Bilgi Yönetimi Süreci", *Gazi Üniversitesi İİBF Dergisi*, Cilt 1, ss. 175-188.

AKGÜN, Ö. E. ve TOPAL, M. (2015) "Eğitim Fakültesi Son Sınıf Öğrencilerinin Bilişim Güvenliği Farkındalıkları: Sakarya Üniversitesi Eğitim Fakültesi Örneği", Sakarya University Journal of Education, Cilt: 5, Sayı: 2.

AKKAYA, M. U. (2014) "Siber Güvenlik Standartları ve Belgelendirmeleri", 2. Uluslararası İstanbul Akıllı Şebekeler Kongre ve Fuarı, İstanbul.

AKLEYLEK, S. ve YÜCE, Z. (2011). "Siber Güvenlikte Kriptoloji", Ankara: Siber Güvenlik Çalıştayı.

ALHOGAIL, A. (2015) "Design and Validation of Information Security Culture Framework", Computers in Human Behavior, No. 49.

ALSHAIKH, M., SEAN, B.M., ATIF,A. Ve SHANTON C.(2015), "Information Security Policy: A Management Practice Perspective", Australasian Conference on Information Systems, Adelaide,

ALTINTAŞ, E. (2014) Stres Yönetimi, 1. Baskı, Anı Yayıncılık, Ankara, 2014,

ANAMERİÇ, H. (2005) "Yönetim Bilgi Sistemlerinin Yönetim Fonksiyonları Üzerine Etkisi", *AÜ Dil Tarih Coğrafya Fakültesi Dergisi,* 42(2), ss. 25-43.

AMENT, C., ve HAAG, S. (2016) "How Information Security Requirements Stress Employees", *Thirty Seventh International Conference on Information Systems*, Dublin, P.13-15

ATEŞ, E.C., ve TOKAY, A. (2018) '' Online Journal of Technology Addiction & Cyberbullying, 5(1), 1-33.

ATILGAN, D. (2009) "Bilgi Yönetimi Kavramı ve Gelişimi", *Türk Kütüphaneciliği Dergisi*, 23(1), ss. 201-212.

ATLI, D. (2014) "Bilgi Çağında İşletmeler Açısından Bilgi Yönetimi ve Stratejik Önemi", *Akademik Bilişim* -, 5-6 , Mersin Üniversitesi, Mersin.

AYYAGARI, R., GROVER, V ve PURVİS, R. (2011). "Technostress: Technological Antecedents and Implications", MIS Quarterly, Vol. 35, No. 4, 831-858.

AVCIOĞLU, G. Ş. (2015) Küresel Bilgi Teknolojileri ve Toplumsal Değerler, Çizgi Kitabevi, İstanbul.

BARUT, O. ve DEĞERLİOĞLU, O,(2010) "Human Resources Information Systems: A Sociotechnical Perspective", Information Technology Journal, Volume: 9, Number: 5,

BAYKARA, M., DAŞ, R ve KARADOĞAN, İ, (2013) "Bilgi Güvenliği Sistemlerinde Kullanılan Araçların İncelenmesi", *1st International Symposium on Digital Forensics and Security (ISDFS'13)*, Elazığ, 231-239.

BENDER, H., MARTIN, I.M. ve RAİSH, C. (20017) "What Motivates Homeowners to Protect Themselves from Wildfire Risks in the WUI?" Risk Anlysis, Volume: 27, 23 Issue: 4,

BLAKLEY, B., MCDERMOTT, E. ve GEER, D. (2001) "Information Security is Information Risk Management", *NSPW*, 97-104.

BULGURCU, B., ÇAVUŞOĞLU, H. ve BENBASAT, I. (2010) "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness", MIS Quarterly, Vol. 34, No. 3, 523-548.

ÇAKAR, D., YILDIZ, S., ve DUR, S. (2010) "Bilgi Yönetimi ve Örgütsel Etkinlik İlişkisi: Örgüt Kültürü ve Örgüt Yapısının Temel Etkileri", *Ege Akademik Bakış Dergisi*, C. 10, S. 1, ss. 71-93.

CAMMANN, C., FICHMAN, M., JENKINS, D., ve Klesh, J. (1983) Assessing the attitudes and perceptions of organizational members. in Seashore, S., Lawler, E., Mirvis, P., and Cammann, C. (eds.), Assessing organizational change: A guide to methods, measures and practices. New York, NY: John Wiley, 71-138.

CAN, E. (2013), İşyerinde Sosyal Diyalog ve Demokrasi, TC Çalışma ve Sosyal Güvenlik Bakanlığı, Çalışma ve Sosyal Güvenlik Eğitim ve Araştırma Merkezi Yayınları, Yayın No: 40, Ankara,

ÇELEN, F. K., SEFEROĞLU, S. S. (2016) "Bilgi ve İletişim Teknolojilerinin Kullanımı ve Etik Olmayan Davranışlar: Sorunlar, Araştırmalar ve Değerlendirmeler, *Journal of Computer and Education Research*, Cilt: 4, Sayı: 8,

ÇELİK, A. (2010), Kriz ve Stres Yönetimi, 1. Baskı, Gazi Kitabevi, Ankara,

ÇETİN, C., ELMALI, E. D. ve ARSLAN, M.L. (2013) İnsan Kaynakları Yönetimi, 5. Basım, Beta Basım Yayın, İstanbul, s. 240.

CHAFFEY D. ve WOOD, S. (2005) *Business Information Management*, England: Prenctice Hall.

CHANDRA J.V., CHALLA, N. ve HUSSAIN, M.A. (2014), "Data and Information Storage Security from Advanced Persistent Attack in Cloud Computing", *International Journal of Applied Engineering Research,* Volume: 9, Number: 20,

DABAN, C. (2017) "Siber Güvenlik ve Uluslararası Güvenlik İlişkisi", Siber Politikalar Dergisi, Cilt: 1, Sayı: 1.

DARICILI, A. B. (2014) "Rusya Federasyonu Kaynaklı Olduğu İddia Edilen Siber Saldırıların Analizi", U. Ü. Sosyal Bilimler Enstitüsü Dergisi, Cilt: 7, Sayı: 2.

DAVIES, M.A.C., ve TITTERINGTON, A. J. (1991) "Marketing the concept of information management to top executives", *Journal of Information Science*, 17, 209-220.

DAWIS, R., ve LOFQUIST, L. H. (1987), "Measurement of Person–Environment Fit and Prediction of Satisfaction in the Theory of Work Adjustment", Journal of Vocational Behavior, Vol. 31, No. 3,

DEMİR, H., ve OKAN, T. (2009) "Teknoloji, Örgüt Yapısı ve Performans Arasındaki İlişkiler Üzerine Bir Araştırma", Doğuş Üniversitesi Dergisi, Cilt: 10, Sayı: 1,

DEMİRHAN, D. (2002) "İşletmelerde Stratejik Bilgi Sistemleri Yönetimi ve Rekabet Üstünlüğü Elde Edilmesindeki Rolü", *Ege Üniversitesi Akademik Bakış Dergisi*, S. 2,

DIAS, C. (2001) Corporate portals: a literature review of a new concept in Information Management, *International Journal of Information Management*, 21: 269–287.

DUBE D. P., ve GULATI, V. P. (2008) Information *System Audit and Assurance*, New Delhi: Tata McGraw Hill.

DURNA, U., ve DEMİREL, Y. (2008) "Bilgi Yönetiminde Bilgiyi Anlamak", *Erciyes Üniversitesi İİBF Dergisi*, Sayı 30: 129-156.

EDWARDS, J. R., CAPLAN, R. D., ve HARRİSON, R. V. (1998). "Person-Environment Fit Theory: Conceptual Foundations, Empirical Evidence, and Directions For Future Research", In C. L. Cooper (Ed.), Theories of Organizational Stress (28-67). Oxford: Oxford University Press.

EMİNAĞAOĞLU, M., ve GÖKŞEN, Y. (2009) "Bilgi Güvenliği Nedir, Ne Değildir, Türkiye'de Bilgi Güvenliği Sorunları ve Çözüm Önerileri", DEÜ SBE Dergisi, Cilt:11, Sayı: 4, s. 9.

EMHAN, A. (2009), "Risk Yönetim Süreci ve Risk Yönetim Teknikleri", Atatürk Üniversitesi İktisadi ve İdari Bilimler Dergisi, Cilt: 23, Sayı: 3, 212-215.

EREN, M. (2017) “Avrupa Birliği'nin Siber Güvenlik Stratejisi İçin Kuramsal Çerçeve ve Strateji Belgesi Öncesi AB'nin Eylemleri”, Siber Politikalar Dergisi, Cilt: 2, Sayı: 3

EROL, S. E., Ceyhan, E.B., ve Sağıroğlu, Ş. (2016) “Kişisel, Kurumsal ve Ulusal Bilgi Güvenliği Farkındalığı Üzerine Bir İnceleme”, Internatıonal Conference On Informatıon Securıty And Cryptology,

ERSOY, E.V. (2012) *ISO/IEC 27001 Bilgi Güvenliği Standardı*, Ankara: ODTÜ Geliştirme Vakfı Yayını.

EVRİN, V., ve DEMİRER, M.(2011) “Kurumsal Bilgi Güvenliği Süreç Çalışmaları: ISO/IEC-27001 Örneği”, IV. Ağ ve bilgi Güvenliği Sempozyumu 2011, Ankara, 25-26.

FERUZA Y., SATTAROVA, K., ve TAO-HOON (2007) “IT Security Review: Privacy, Protection, Access Control, Assurance and System Security”, *International Journal of Multimedia and Ubiquitous Engineering* 2(2): 17-32.

FENZ, S., HEURIX, J., NEUBAUER, T., ve PECHSTEIN, F. (2014), “Current challenges in information security risk management”, Information Management & Computer Security, Volume: 22, Issue: 5.

FFIEC (2016) *Information Security*, Virginia: FFIEC.

FFIEC (2010) *Information Security*, Virginia: FFIEC.

FİDAN, M. (2016) Bilişim Etiği Boyutlarına Göre Bilişim Teknolojileri ve Yazılım Dersi Öğretim Programı Kazanımlarının İncelenmesi, *Kastamonu Eğitim Dergisi*, Cilt: 24, Sayı: 4, s. 1642-1644.

FRANGOPOULOS, E.D., ELOFF, M.M ve VENTER, L.M. (2013). “Psychosocial Risks: Can Their Effects on the Security of Information Systems Really be Ignored?”, Information Management & Computer Security, Vol. 21, No. 1, 53-65.

GOLDSTEIN, I., SAPRA, H., (2014) “Should Banks' Stress Test Results be Disclosed? An Analysis of the Costs and Benefits”, Foundations and Trends in Finance, Volume: 8, Issue: 1,

GÖÇOĞLU, V. (2018) “Türkiye’nin Siber Güvelik Politikalarının kamu Politikası Analizi Çercevesinde Değerlendirilmesi ”, Ankara

GÜÇLÜ, N., ve SOTİROFSKİ, K. (2006) “Bilgi Yönetimi”, *Türk Eğitim Bilimleri Dergisi*, Güz , 4(4), 351-371.

GÜLDÜREN, C., ÇETİNKAYA, L., ve KESER, H. (2016) “Ortaöğretim Öğrencilerine Yönelik Bilgi Güvenliği Farkındalık Ölçeği (GBFÖ) Geliştirme Çalışması”, İlköğretim Online, Cilt: 15, Sayı: 2.

GÜLSEÇEN, S. (2016), Bilgi Yönetimi Bilgi Türeticileri, Büyük Veri, İnovasyon ve Kurumsal Zeka, Papatya Bilim Yayıncılık, 1. Basım,

GÜNTAY, V. (2016) “Ulusal Güvenlik Çerçevesinde Siber Güvenlik Yaklaşımı Oluşturma Sorunu” Siber Politikalar Dergisi, Cilt: 1, Sayı: 1.

GÜRBÜZ, S., ve ŞAHİN, F. (2015) “Sosyal Bilimlerde Araştırma Yöntemleri” Seçkin Yayıncılık, 2. Baskı,

HEKİM, H., ve BAŞIBÜYÜK, O. (2013) “Siber Suçlar ve Türkiye’nin Siber Güvenlik Politikaları”, *Uluslararası Güvenlik ve Terörizm Dergisi*, 4(2), s. 136.

HELOKUNNAS, T., ve KUUSİSTO, R. (2003) “Information Security Culture in a Value Net”, IEMC '03. Managing Technologically Driven Organizations: The Human Side of Innovation and Change.

HENTEA ,M. (2005),’’The Journal of Issues in Informing Science and Information Technology’’ , volüme 2, 169 -178

İLTER, H.K. (2007) “Bilgi Sistemleri Perspektifinden Kurumsal Kaynak Planlaması: Etkiler ve Değerler”, *İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi*, S. 11.

İPÇİOĞLU, İ., ve KÂHYA D. (2016) “Bilgi Yönetimi Sürecinin Örgütsel Performansa Etkisi ve Otomotiv Sektöründe Bir Araştırma”, “*Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 3(25)

IFINEDO, P. (2012)“Understanding information systems security policy compiance: An integration of the theory of planned behaviour and the protection motivation theory”, Computers & Security, No. 31, pp. 84.

JAHAN, S. (2014) “Human Resources Information System (HRIS): A Theoretical Perspective”, Journal of Human Resources and Sustainability Studies, Number:2,p. 34-35

JENA, R.K. (2015). “Impact of Technostress on Job Satisfaction: An Empirical Study among Indian Academician”, The International Technology Management Review, Vol. 5, No. 3, 117-124.

KARADAĞ, M., ve ABUHANOĞLU, H. (2015) “Sosyo-Kültürel Özelliklerin Bilgi Güvenliği Farkındalığı Üzerine Etkisi: Gülhane Askeri Tıp Fakültesi Eğitim Hastanesinde Bir Çalışma”, JASSS, Number: 36,

KARJALAINEN,M., ve SIPONEN, M. (2011)’’Toward a New Meta-Teory for Designing Information Systems (IS) Securyty Training Approaches’’, Journal of the Association for Information Syatems (JAIS), Vol.12,pp.518-555.

KESER, H., ve GÜLDÜREN, C. (2015) “Bilgi Güvenliği Farkındalık Ölçeği (BGFÖ) Geliştirme Çalışması”, K.Ü. Kastamonu Eğitim Dergisi, Cilt: 23, Sayı: 3.

KHAN, A., REHMAN, H., ve REHMAN, S. (2013). “An Empirical Analysis of Correlation Between Technostress and Job Satisfaction: A Case of KPK, Pakistan”, Pakistan *Journal Of Library and Information Science*; Issue:14,

KINMAN, G. ve JONES, F. (2005) “Lay representations of workplace stress: What do people really mean when they say they are stressed?”, Work & Stress, Vol. 19, No. 2, 101-120.

KÖK, B. (2006) “Bilişim Teknolojilerinin Yönetsel ve Örgütsel Etkileri”, *Ticaret ve Turizm Eğitim Fakültesi Dergisi*, Sayı 2.

KRAEMER, S., CARAYON, P., ve CLEM, J. (2009). “Human and Organizational Factors in Computer and Information Security: Pathways to Vulnerabilities”, Computers and Security, doi:10.1016/j.cose. 04.006, p.510

KRISTOF, A. L. (1996). "Person-Organization Fit: An Integrative Review of Its Conceptualizations, Measurement, and Implications", Personnel Psychology, Vol. 49, 1-49.

KUMAR, R., LAL, R., BANSAL, Y., ve SHARMA, S. K. (2013) "Technostress in Relation to Job Satisfcation and Organisational Commitment among IT professionals", International Journal of Scientific and Research Publications, Volume: 3, Issue: 12.

KURGUN, A., KURGUN H., ve AKİPEK, E. (2007) "Turizm Pazarlamasında Küresel Dağıtım Sisteminin Stratejik Rolü ve Önemi", *Dokuz Eylül Üniversitesi İİBF Dergisi*, C. 9, S. 1.

KURNAZ, İ. (2016) "Siber Güvenlik ve İlintili Kavramsal Çerçeve", Siber Politikalar Dergisi, Cilt: 1, Sayı: 1.

KURNAZ, N., ve DİNDAROĞLU, A. K. (2015) "İç Denetim ve Bilgi Güvenliği İlişkisi: Bölgesel Bir Araştırma", Bilgi Ekonomisi ve Yönetimi Dergisi, Cilt: X, Sayı: 1.

LEBEK, B., UFFEN, J., BREITNER, M.H., NEUMANN,M., ve HOHLER, B.(2013)''Employees' Information Security Awareness and Behavior:A Literature Review '', 46th Hawaii International Conferance on System Science,

LEE, C., LEE, C. C., ve KİM, S. (2016) "Understanding Information Security Stress: Focusing on the type of Information Security Compliance Activity", Computers & Science, Issue: 59, 60-70

LI, Y. (2015). "Users' Information Systems (IS) Security Behavior In Different Contexts", University of Oulu, Finland, ISBN 978-952-62-0938-8.

MARITZ,S. G.(2003)"Data Management: Managing Data As An Organizational Resource", Acta Commercii, Vol. 3,

ODABAŞ, H. (2008) "Bilgi Yönetimi ve Yüksek Öğrenim Kurumlarında Kurumsal Açık Erişim", *inet-tr'08 - XIII. Türkiye'de İnternet Konferansı Bildirileri 22-23* , Orta Doğu Teknik Üniversitesi, Ankara.

ODABAŞ, H. (2009) "Örgütlerde Enformasyon: Bilgi Yönetimi ve Süreci", *Information–Knowledge Management and Process in Organizations,* in: Tülin Aren Armağanı. Pamuk Yayıncılık.

OSTROFF, C., ve SCHULTE, M. (2007). Multiple Perspectives of Fit In Organizations Across Levels of Analysis. In C. Ostroff & T.Judge (Eds.), Perspectives on Organizational Fit (3–69). New York: Lawrence Erlbaum Associates.

ÖNEL, D. (2008) *Bilgi Güvenliği Bilinçlendirme Süreci Oluşturma Kılavuzu*, Kocaeli: TÜBİTAK.

ÖNOK M. (2013) "Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği", Marmara Üniversitesi Hukuk Araştırmaları Dergisi, Özel Sayı: Prof. Dr. Nur Centel'e Armağan

ÖZDEMİRCİ, F., AYDIN, C. (2008) "Kurumsal Bilgi Kaynakları ve Bilgi Yönetimi", *Türk Kütüphaneciliği*, 22(1): 59-81.

ÖZGÜR, S. (2012) "Bilgi Toplumu, Bilgi Yönetimi ve Halkla İlişkiler", *Gümüşhane Üniversitesi İletişim Fakültesi E-Dergisi*, 3: 191-214.

ÖZTÜRK, G. (2008) "Bilgi Güvenliği Politikası Oluşturma Kılavuzu", Tübitak Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü, Kocaeli, 6-7.

ÖZTÜRK, M. S. (2018) ''Siber Saldırılar, Siber Güvenlik Denetimleri ve Bütüncül Bir Denetim Modeli Önerisi '' Muhasebe ve Vergi Uygulamaları Dergisi ; Özel Sayı:208-232

PAŞA, M., ve KAYMAZ, K. (2013), Stres Yönetimi, 1. Baskı, Aktüel Yayınları, İstanbul, 2013, s. 18.

PELTIER, T. R. (2013), "Risk Management: The Faciliated Risk Analysis and Assessment Process", Information Security Fundamentals, Second Edition, CRC Press,

PEPPARD, J., ve Ward, J.(2016), The Strategic Management of Information Systems: Building a Digital Strategy, Fourth Edition, John Wiley & Sons,

PIETERS, W. (2011) "The (social) construction of information security", Inf. Soc. 27(5): 326-335.

SAFA, N. S., SOLMS, R.V., ve FURNELL, S. (2016) "Information security policy compliance model in organizations", *Computer and Security*, 56: 70-82.

SAĞSAN, M. (2002) "Bilgi Savaşı: Siperlerden Klavyelere Taşınan Bir Harekâtın Anatomisi", Avrasya Dosyası, İstihbarat Özel Sayısı, S. 2,

SAĞSAN, M. (2007) "Uygulamadan Disipline Bilgi Yönetimi ve Bir Alan Çalışması", *Amme İdaresi Dergisi*, 40(4)

SALDAMLI, A. (2008)"İnsan Kaynakları Yönetiminde Bilişim Teknolojilerinin Kullanımına Yönelik Bir Araştırma: Tekirdağ Örneği", İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi, Sayı: 13, s. 248.

SHIBLY, H. A. (2011) "Human Resources Information Systems Success Assetsment: An Integrative Model", Australian Journal of Basic and Applied Sciences, Volume: 5, Number: 5, p. 157.

SCHLIENGER, T., ve TEUFEL, S., (2003), "Analyzing Information Security Culture: Increased Trust by an Appropriate Information Security Culture", Computer & Society, Proceedings of the 14th International Workshop on Database and Expert Systems Applications (DEXA'03), p. 1.

SHILLAIR, R. (2015) "Online safety begins with you and me: Convincing internet users to protect themselves", Computers in Human Behavior, No. 48, pp. 200.

SINGH, A., VAİSH, A., ve KESERWANİ, K. P. (2014) "Information Security: Components and Techniques", *International Journal of Advanced Research in Computer Science and Software Engineering*, 4(1): 1072-1077.

SİPONEN, M. T. (2000). "A Conceptual Foundation for Organizational Information Security Awareness", Information Management & Computer Security, Vol. 8, No. 1, 31-41.

SİPONEN, M., MAHMOOD, M. A., ve PAHNİLA, S. (2014) "Employees' Adherence to Information Security Policies: An Exploratory Field Study", Information & Management, No 51,

SOOMRO, Z. A., SHAH, M. H., ve AHMED, J. (2016), "Information security management needs more holistic approach: A literature review" *International Journal of Information Management,* Volume: 36, Issue: 2.

STAIR, R., ve RAYNOLDS, G. (2008) *Fundamentals of Information Systems*, USA: Cengage Learning Inc.

SUNDGREN, B., ve STENESKOG, G. (2003), "Information Systems for Concerted Actions", *Exploring Patterns in Information Management*, Sundgren, Bo; Martensson, Por, MAHRING, Magnus; Nilsson, Kristina (ed), Stockholm: Stockholm Schools of Economics.

ŞAHİNASLAN, E., KANTÜRK, A., ŞAHİNASLAN, Ö., ve BORANDAĞ, E. (2009) "Kurumlarda Bilgi Güvenliği Farkındalığı, Önemi ve Oluşturma Yöntemleri", Akademik Bilişim '09 – XI. Akademik Bilişim Konferansı. Şanlıurfa.

ŞAHİNASLAN, Ö., ŞAHİNASLAN, E., BORANDAĞ, E., ve ŞAHİNASLAN, A. M. (2013) "Güvenli Bir Toplum İçin Son Kullanıcı Siber Güvenliği", Akademik Bilişim - XV. Akademik Bilişim Konferansı, Antalya.

QİU, W. (2013). "The Impact of Technostress on Job Satisfaction and Organizational Commitment", Master Thesis, Massey University. P.67-79

TAHİROV, A. (2009) "Bilgisayar Destekli Bilgi Sistemleri", *Journal of Qafqaz University*, S. 27.

TANILIR, M. N. (2002) İnternet Suçları ve Bireysel Mahremiyet. Ankara: Liberte Yayınları

TAŞÇI, U. C., ve CAN, A. (2015) "Türkiye'de Polisin Siber suçlarla Mücadele Politikası: 1997-2014", Fırat Üniversitesi Sosyal Bilimler Dergisi, Cilt: 25, Sayı: 2.

TONTA, Y. (2004) "Bilgi Yönetiminin Kavramsal Tanımı ve Uygulama Alanları", *Kütüphaneciliğin Destanı Sempozyumu*, 21-24 , Ankara. 3-7

TURN, R., ve WARE, W.H. (1976). "Privacy and Security Issues in Information Systems", IEEE Transactions on Computers, The Rand Paper Series. , p.133-147

TUTAR, H. (2016), Kriz ve Stres Yönetimi, 4. Basım, Seçkin Yayıncılık, Ankara,

TÜRK, M. (2003), Küreselleşme Sürecinde İşletmelerde Bilgi Yönetimi, 1. Baskı, Türkmen Kitabevi, İstanbul,

UDO, G.J. (2001). "Privacy and Security Concerns as Major Barriers For e-Commerce: A Survey Study", Information Management & Computer Security, 9(4), 165-174.

UZUN, H. ve DURNA, U. (2008) "İşletmelerde Rekabet Unsuru Olarak Bilgi Yönetimi", *Niğde Üniversitesi İİBF Dergisi*, 1(1). 33-40.

ÜNVER, M., ve CANBAY, C., (2010) "Ulusal ve Uluslararası Boyutlarıyla Siber Güvenlik", Elektrik Mühendisliği, Sayı: 436.

ÜNVER, M., CANBAY, C., ve MİRZAOĞLU, A. G. (2009) Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler, Ankara: Bilgi Teknolojileri ve İletişim Kurumu (BTK)

VAN NIEKERK, J. F., ve Von Solms, R.(2010) "Information Security Culture: A Management Perspective", Computers & Security, No. 29,

VEIGA; A. D., ve ELOFF, J. H. P. (2010) "A Fremework and Assessment Instrument for Information Security Culture", Computers & Security, No. 29, p. 198.

VURAL, Y., ve SAĞIROĞLU, Ş. (2007) "Kurumsal Bilgi Güvenliği: Güncel Gelişmeler", Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı, Ankara, 13-14 Aralık, s. 192.

VURAL, Y., ve SAĞIROĞLU, Ş. (2008), "Kurumsal Bilgi Güvenliği ve Standartları Üzerine Bir İnceleme", Gazi Üniv. Müh. Mim. Fak. Der. 23(2), s. 511

VURAL, Y., ve SAĞIROĞLU, Ş.(2011), "Kurumsal Bilgi Güvenliğinde Güvenlik Testleri ve Öneriler", Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi, Cilt: 26, Sayı: 1,

WEBB, J., MAYNARD, S.B., AHMAD, A., ve SHANKS, G. (2016) "Foundations for an Intelligence-driven Information Security Risk-management System", JITTA: Journal of Information Technology Theory and Application, Volume: 17, Issue: 3,

WİECZORKOWSKİ, J., ve POLAK, P. (2017). "Big Data and Privacy: The Study of Privacy Invasion Acceptance in the World of Big Data", Online Journal of Applied Knowledge Management, Vol. 5, No. 1, 57-71.

YILDIZ, S. (2007) "Suçta Araç Olarak İnternetin Teknik ve Hukuki Yönden İncelenmesi", Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, Sayı: 17.

YILMAZ, E., ŞAHİN, Y. L., ve AKBULUT, Y. (2016) "Öğretmenlerin Dijital Veri Güvenliği Farkındalığı" Sakarya University Journal of Education, Cilt: 6, Sayı: 2.

YILMAZ, E., Nurcan, U., ve GÖNEN, S. (2015) "Bilgi Toplumuna Geçiş ve Siber Güvenlik", Bilişim Teknolojileri Dergisi, Cilt: 8 Sayı: 3.

YILMAZ, H., (2014) TS ISO/IEC 27001 Bilgi Güvenliği Yönetimi Standardı Kapsamında Bilgi Güvenliği Yönetim Sisteminin Kurulması Ve Bilgi Güvenliği Risk Analizi", Denetişim, Sayı: 15.

YILMAZ, S., ve SAĞIROĞLU, Ş. (2013) "Siber Güvenlik Risk Analizi", 6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, Ankara, Proceeding: Bildiriler Kitabı, 20-21 Eylül.

YILMAZ, S., ve SAĞIROĞLU, Ş. (2013) "Siber Güvenlik Risk Analizi, Tehdit ve Hazırlık Seviyeleri", 6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, Ankara.

ZAİM H., ve SEÇGİN, G. (2012) "Bilgi Yönetiminde Bilgi Dönüştürme ve SECI Modeli: Hizmet Sektöründe Bir Alan Araştırması", *İstanbul Üniversitesi İşletme Fakültesi Dergisi*, 41(1)

ZAİM, H. (2010) "Bilgi Yönetiminin Alt Yapısı ve Bilgi Yönetim Performansı: Türkiye'de Bir Saha Çalışması", *Sosyal Siyaset Konferansları Dergisi*, Sayı 59: 51-67.

"Siber Güvenlik Geleceği Şekillendiriyor" Ekonomik Forum, Sayı: 251, 2015, s. 12-21. http://haber.tobb.org.tr/ekonomikforum/2015/251/012_021_KAPAK_KONUSU.pdf (Erişim Tarihi: 05.05.2018).

ARSLAN, M.E. (2017) “Siber Güvenlik ve Siber Saldırı Türleri” http://www.academia.edu/31827545/S%C4%B0BER_G%C3%9CVENL%C4%B0K_VE_S%C4%B0BER_SALDIRI_T%C3%9CRLER%C4%B0_CYBER_SECURITY_AND_CYBER_ATTACK_TYPES (Erişim Tarihi: 05.05.2018).

FORCEPOINT, www.infonet.com.tr , 2018 (Erişim tarihi :28/08/2018).

HTTPS:// siber.boun.edu.tr, 2018 (Erişim tarihi:28/08/2018)

ULUDAĞ ÜNİVERSİTESİ

TEZ ÇOĞALTMA VE ELEKTRONİK YAYIMLAMA İZİN FORMU

Yazar Adı Soyadı	**Halil ERBİ**
Tez Adı	**Bilgi Güvenliği Stres Faktörlerinin İş Tatmini Üzerindeki Etkileri : Ar-Ge Merkezi Olan İşletmeler Üzerine Bir Araştırma.**
Enstitü	**Sosyal Bilimler Enstitüsü**
Anabilim Dalı	**İşletme**
Bilim Dalı	**Yönetim ve Organizasyon**
Tez Türü	**Yüksek Lisans**
Tez Danışmanı	**Doç. Dr. Kurtuluş KAYMAZ**
Çoğaltma (Fotokopi Çekim) İzni	☐ Tezimden fotokopi çekilmesine izin veriyorum ☒ Tezimin sadece içindekiler, özet, kaynakça ve içeriğinin % 10 bölümünün fotokopi çekilmesine izin veriyorum ☐ Tezimden fotokopi çekilmesine izin vermiyorum
Yayımlama İzni	☒ Tezimin elektronik ortamda yayımlanmasına izin veriyorum ☐ Tezimin elektronik ortamda yayımlanmasının ertelenmesini istiyorum 1 yıl ☐ 2 yıl ☐ 3 yıl ☐ ☐ Tezimin elektronik ortamda yayımlanmasına izin vermiyorum

Hazırlamış olduğum tezimin yukarıda belirttiğim hususlar dikkate alınarak, fikri mülkiyet haklarım saklı kalmak üzere Uludağ Üniversitesi Kütüphane ve Dokümantasyon Daire Başkanlığı tarafından hizmete sunulmasına izin verdiğimi beyan ederim.

Tarih: 28.08.2018

İmza: