GÜVENLİK GÜÇLERİNİN BİLGİ GÜVENLİĞİ FARKINDALIĞINA YÖNELİK BİR BETİMLEME

YÜKSEK LİSANS TEZİ

Emre TANER

Danışman
Doç. Dr. İbrahim KILIÇ

İNTERNET VE BİLİŞİM TEKNOLOJİLERİ YÖNETİMİ
ANABİLİM DALI

Ocak, 2019

AFYON KOCATEPE ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ

GÜVENLİK GÜÇLERİNİN BİLGİ GÜVENLİĞİ FARKINDALIĞINA YÖNELİK BİR BETİMLEME

Emre TANER

Danışman
Doç. Dr. İbrahim KILIÇ

İNTERNET VE BİLİŞİM TEKNOLOJİLERİ YÖNETİMİ ANABİLİM DALI

OCAK 2019

TEZ ONAY SAYFASI

Emre TANER tarafından hazırlanan "Güvenlik Güçlerinin Bilgi Güvenliği Farkındalığına Yönelik Bir Betimleme" adlı tez çalışması lisansüstü eğitim ve öğretim yönetmeliğinin ilgili maddeleri uyarınca 03/01/2019 tarihinde aşağıdaki jüri tarafından **oy birliği** ile Afyon Kocatepe Üniversitesi Fen Bilimleri Enstitüsü **İnternet ve Bilişim Teknolojileri Yönetimi Anabilim Dalı'nda YÜKSEK LİSANS TEZİ** olarak kabul edilmiştir.

Danışman : Doç. Dr. İbrahim KILIÇ

Başkan : Doç. Dr. İbrahim KILIÇ
Afyon Kocatepe Üniversitesi,
Veteriner Fakültesi

Üye : Doç.Dr. Sinan SARAÇLI
Afyon Kocatepe Üniversitesi,
Fen Edebiyat Fakültesi

Üye : Dr. Öğr. Üyesi Cengiz GAZELOĞLU
Süleyman Demirel Üniversitesi,
Fen Edebiyat Fakültesi

Afyon Kocatepe Üniversitesi
Fen Bilimleri Enstitüsü Yönetim Kurulu'nun
...../...../..... tarih ve
..... sayılı kararıyla onaylanmıştır.

.....
Prof. Dr. İbrahim EROL
Enstitü Müdürü

BİLİMSEL ETİK BİLDİRİM SAYFASI
Afyon Kocatepe Üniversitesi

Fen Bilimleri Enstitüsü, tez yazım kurallarına uygun olarak hazırladığım bu tez çalışmasında;

- Tez içindeki bütün bilgi ve belgeleri akademik kurallar çerçevesinde elde ettiğimi,
- Görsel, işitsel ve yazılı tüm bilgi ve sonuçları bilimsel ahlak kurallarına uygun olarak sunduğumu,
- Başkalarının eserlerinden yararlanılması durumunda ilgili eserlere bilimsel normlara uygun olarak atıfta bulunduğumu,
- Atıfta bulunduğum eserlerin tümünü kaynak olarak gösterdiğimi,
- Kullanılan verilerde herhangi bir tahrifat yapmadığımı,
- Ve bu tezin herhangi bir bölümünü bu üniversite veya başka bir üniversitede başka bir tez çalışması olarak sunmadığımı

beyan ederim.

03/01/2019

Emre TANER

ÖZET
Yüksek Lisans Tezi

GÜVENLİK GÜÇLERİNİN BİLGİ GÜVENLİĞİ FARKINDALIĞINA YÖNELİK BİR BETİMLEME

Emre TANER
Afyon Kocatepe Üniversitesi
Fen Bilimleri Enstitüsü
İnternet ve Bilgi Teknolojileri Yönetimi Anabilim Dalı
Danışman: Doç. Dr. İbrahim KILIÇ

Bu araştırmanın amacı, emniyet ve asayiş ile kamu düzenini korumakla görevli olan emniyet personelinin bilgi güvenliği farkındalık düzeylerinin tespit edilmesidir. Çalışmaya, Siirt'te görev yapan 207 jandarma ve 197 polis olmak üzere toplam 404 personel katılmıştır. Veri toplama tekniği olarak anket kullanılmıştır. Verilerin analizinde, betimsel istatistiklerin (frekans, yüzde, ortalama, standart sapma) yanı sıra, bilgi güvenliği farkındalık düzeylerinin katılımcıların demografik özelliklerine göre karşılaştırılmasında t testi ve varyans analizi kullanılmıştır. Araştırma sonucunda, bilgi güvenliği farkındalık düzeyi ölçeğinin "saldırı ve tehditler" alt boyutuna ilişkin genel ortalama 2,32 ve "kişisel verileri koruma" alt boyutuna ilişkin genel ortalama ise 2,87 olarak hesaplanmıştır. Bu değerler emniyet personelinin bilgi güvenliği farkındalık düzeylerinin yüksek olmadığını hatta ortalamanın altında olduğunu göstermektedir. Diğer taraftan katılımcıların bilgi güvenliği farkındalık düzeylerinin bazı demografik özellik değişkenlerine göre farklılık gösterdiği tespit edilmiştir. Araştırma sonuçları, emniyet personelinin bilgi güvenliği farkındalık düzeylerinin artırılmasına yönelik önlem alınmasını ve gerekli çalışmalar yapılmasını ortaya koymuştur.

2019, ix + 73 sayfa

Anahtar Kelimeler: Bilgi, Bilgi Güvenliği, Bilgi Güvenliği Farkındalığı, Kişisel Bilgilerin Korunması,

ABSTRACT
M.Sc. Thesis

A DESCRIPTION RELATED TO INFORMATION SECURITY AWARENESS OF SECURITY PERSONAL

Emre TANER
Afyon Kocatepe University

Graduate School of Natural and Applied Sciences

Department of Internet and Information Technology Management

Supervisor: Assoc. Prof. İbrahim KILIÇ

The aim of this study is to determine the awareness levels of information security of the safety personnel who are responsible for protecting public order and security. A total of 404 personnel participated in the study, including 207 gendarme and 197 policemen, working in Siirt province of Turkey. Questionnaire was used as data collection technique. In the analysis of the data, in addition to descriptive statistics (frequency, percentage, mean, standard deviation), t test and variance analysis were used to compare the awareness levels of information security of the safety personnel according to the demographic characteristics of the participants. According to the results of the study, the overall average regarding the "attack and threats" sub-dimension of the awareness levels of information security calculated to be 2.32 and the overall average for the "personal data protection" sub-dimension has been calculated as 2.87. These values indicate that the awareness levels of information security of the safety personnel are not high and even below the average. On the other hand, it was determined that the awareness levels of information security of the participants varied according to some demographic characteristics. According to the results of the study, it was suggested that precautions should be taken to increase the awareness levels of the safety personnel about the information security and it has been revealed that studies should be carried out to increase the awareness levels of information security of safety personnel.

2019, ix + 73 pages

Keywords: Information, Information Security, Information Security Awareness, Protection of Personal Information,

TEŞEKKÜR

Bu araştırmanın konusu, deneysel çalışmaların yönlendirilmesi, sonuçların değerlendirilmesi ve yazımı aşamasında yapmış olduğu büyük katkılarından dolayı tez danışmanım Sayın Doç. Dr. İbrahim KILIÇ'a, anket çalışması sırasında yardımlarını esirgemeyen Siirt İl Emniyet Müdür Yrd. Sayın Nihat ÖZEN'e teşekkür ederim. Ayrıca, bu araştırma boyunca maddi ve manevi desteklerini esirgemeyen değerli eşim Hilal'e ve kızım Dilara'ya teşekkür ederim.

Emre TANER

AFYONKARAHİSAR, 2019

İÇİNDEKİLER DİZİNİ

Sayfa

SİMGELER ve KISALTMALAR DİZİNİ

Simgeler

f	Frekans
P	İstatistiksel Olasılık Değeri
SS	Standart Sapma
t	t-test İstatistiği
F	Varyans Analizi İstatistiği
$\bar{x}$	Aritmetik Ortalama

Kısaltmalar

BİAK	Bilişim ve İnternet Araştırma Komisyonu
CMK	Ceza Muhakemesi Kanunu
DNS	Domain Name Server, Bölge Ad Sunucusu
DOS	Denial Of Service, Servis Engelleme
GD	Güvenlik Duvarı
IEC	The International Electrotechnical Organization, Uluslararası Elektroteknik Komisyonu
ISO	International Organization for Standardization, Uluslararası Standardizasyon Kurumu
IP	Internet Protocol, İnternet Protokolü
TBMM	Türkiye Büyük Millet Meclisi
TCK	Türk Ceza Kanunu
TDK	Türk Dil Kurumu
TUBİTAK	Türkiye Bilimsel ve Teknik Araştırma Komisyonu
TÜİK	Türkiye İstatistik Kurumu
TSE	Türk Standartları Enstitüsü

ŞEKİLLER DİZİNİ

Sayfa

ÇİZELGELER DİZİNİ

Sayfa

1. GİRİŞ

Bilgi, insanoğlunun var olmasından itibaren düşüncesini, davranışını ve gelişim sürecini belirleyen en önemli faktörlerden biridir (Vural 2007). Tarih boyunca bilgi insanoğlunun sahip olduğu en önemli olgu olmasından dolayı bilgi kavramı aynı zamanda güç olarak algılanmaktadır (Güçlü ve Sotirofski 2006). Bilginin zaman içerisindeki yoğun artışı ve teknolojinin gelişmesi ile birlikte var olan bilgiler elektronik ortamlara taşınması gereğini doğurmuştur. Çok fonksiyonlu, boyut olarak çok az yer kaplayan büyük teknolojik cihazlar sayesinde daha fazla bilgi dijital ortama aktarılmakta, işlenmekte ve taşınabilmektedir.

Tüm bu teknolojik gelişmeler bireylerin günlük yaşantısında iletişim kurma ve bilgi paylaşmada sağladığı hız ve kolay erişilebilirlik vb. avantajları sebebiyle tercih edilmektedir (Erdoğmuş 2017). Ancak bu avantajların kullanılabilmesi için kişilerin, sürekli gelişen ve daha karmaşık bir hal alan teknolojik gelişmeleri yakından takip etmesi gerekmekte ve iletişim için gerekli akıllı cihazları ve içerdiği yazılımları kullanmak için gerekli teknolojik bilgiye sahip olması gerekmektedir. Yani bilgi ve iletişim için sadece okuma yazma bilgisi yetmemekte, bunun yanında bireylerin gerekli medya okur-yazarlığına da bilmesi gerekmektedir (Mart 2012).

Bilgi teknolojilerinin, bilgi kaynaklarına hızlı ulaşım sağlaması, ulaşılan bilginin hızlı bir şekilde aktarımı, sosyalleşme, çevrimiçi anlık iletişim kurma gibi faydalarının olmasının yanında birçok olumsuzluğu da beraberinde getirmektedir. Sanal ortamlarda bilgiye ulaşmanın kolay olması kadar zararlı içeriklere de erişimin kolay olması ve bu içeriklere daha fazla maruz kalınması bireylerin sosyal yaşantılarında olumsuz etkilere sebep olmaktadır.

Gerçek dünyadan farklı olan bu dijital dünyada kişiler arası ilişkiler değişmekte ve gerçek dünyada iletişim kurmada önemli olan yaş, cinsiyet, ırk, kültür vb. pek çok özellik sanal dünyada önemli olmamaktadır. Online alışveriş, bankacılık faaliyetleri, hatta direk internet üzerinden çalışma vb. kullanımlar insanın sosyal yaşamını etkileyecek unsurlardır (Ertuğrul ve Keskin 2012).

İnternetin hayatımızın her alanına nüfuz etmesi günümüzde, banka bilgileri, çalışma hayatı ile ilgili bilgiler, kişinin yaşantısını ilgilendiren tüm unsurlar, kısacası tüm kişisel veriler yeni nesil akıllı teknolojik cihazlar ile saklanmakta ve internet yardımı ile istenildiği zaman istenildiği yerde ulaşılmakta ve başka bir alıcıya gönderilmesini mümkün kılmaktadır (Çetin 2014). Yeni nesil akıllı cihazlar ve beraberinde geliştirilen tüm yardımcı uygulamalar hayatımızı kolaylaştırmasının yanında bazı güvenlik problemlerini ve yeni suçları da beraberinde getirmektedir (Gülmüş 2010). Özellikle mobil cihazlardaki gelişim ve akıllı telefonların hayatımıza girmesi ile birlikte internet, sosyal medya programları, bankacılık faaliyetleri vb. bilgisayar üzerinden yapılan birçok işlem artık cep telefonlarından yapılabilir olması internet kullanımında da artışa sebep olmakta ve artık mobil internete doğru bir eğilimin olduğu görülmektedir (Bolat vd. 2017).

İnternet ve çevrimiçi dünyanın giderek hayatımızı kuşatması ile birlikte kötü niyetli bilgisayar korsanları tarafından bir hedef haline gelmiş ve siber saldırı sayısı artmıştır. Bu durum sahip olunan bilginin korunmasını da sorun haline getirmiştir (Karaaslan 2013). Özellikle kritik sayılacak kurumlarda görev yapan personele ait kişisel veriler ile personelin iş yaşantısı ile alakalı elektronik ortamlarda tuttuğu kayıtlara kötü niyetli kişilerce erişilmesi, kurumun güvenliğini de tehlikeye atacağından, kişisel veri güvenliğinin kurumsal veri güvenliğini de etkilemesi söz konusu olacaktır.

Bilgi güvenliği risklerinden korunmak için kurumsal seviyede her ne kadar yüksek miktarda paralar harcansa da halen güvenlik seviyesi %100'lere ulaşamamaktadır. Bunun başlıca sebeplerinden birisi, kurumlarda bulunan bu bilgi teknolojisi ürünleri kullanan insan faktöründen kaynaklanmaktadır (Şahinaslan vd. 2009). İnsan kaynaklı bilgi güvenliği ihmallerini ve doğuracağı riskleri %0 seviyelerine indirmek imkânsız gibi görünse bile profesyonel bir ekip tarafından hazırlanmış farkındalık eğitimleri ile bilgi güvenliği zafiyetleri minimum seviyeye indirilebilir. Görüldüğü üzere bireylerde, bilişim teknolojileri alanında yapacağı tüm işlemlerde bilgi güvenliği farkındalığının oluşması gerek kişisel gerekse kurumsal, alanda önem arz etmektedir. Bir kurumun bilgi güvenliği seviyesi o kurumda çalışan bireylerin bilgi güvenliği farkındalık seviyesi ile doğrudan ilişkilidir.

Teknolojik gelişmelerle birlikte son yıllarda bilgi güvenliği konusuna olan ilgi tüm dünyada ve ülkemizde oldukça artmıştır. Bu konuda yapılan araştırmaların çoğu teknik altyapı ile ilgili olan; güvenlik duvarı, IP analizi, saldırı tespit/önleme sistemleri, anti virüs yazılımları, şifreleme programları, kimlik doğrulama, yetkilendirme vb. konularla ilgilidir. Oysa ki insan faktörünü göz ardı eden tüm bu çalışmalar tek başına yeterli olmamaktadır. Bir kurumda bilgi güvenliği konusu, teknik önlemlerin alınmasının yanında çalışanlarının da güvenlik bilincine ulaşması ile birlikte sağlanabilir (Keser ve Güldüren 2015).

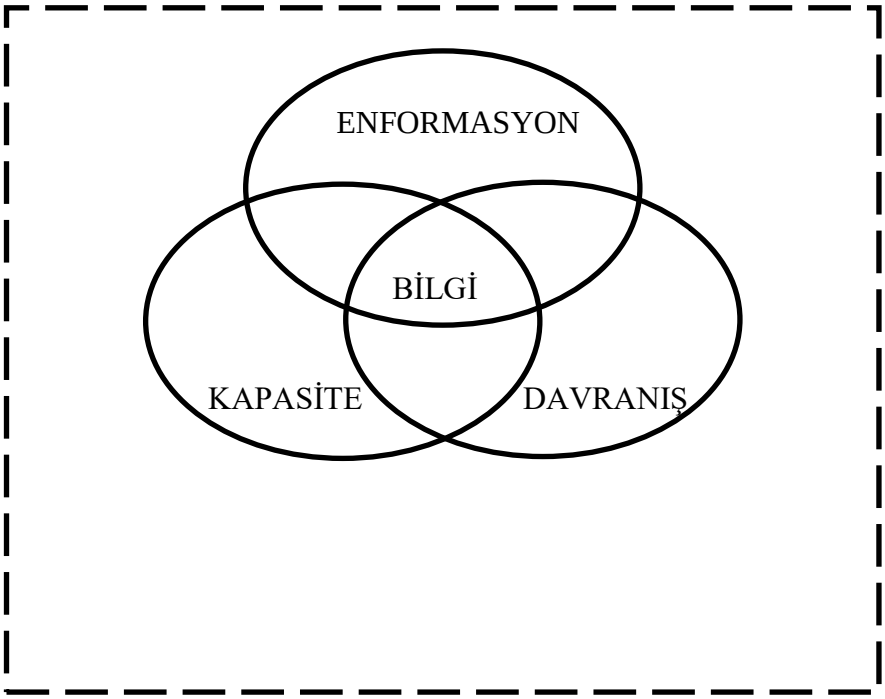
2. LİTERATÜR BİLGİLERİ

2.1 Bilgi Kavramı

Bilgi, ‘’İnsan aklının erebileceği olgu gerçek ve ilkelerin bütünü, insan zekasının çalışması sonucu ortaya çıkan düşünce ürünü’’ olarak tanımlanmaktadır. Bilgi kelimesi Yunan kökenli olmasının yanında manası şekil vermek anlamına gelen Latince bir sözcükten türetilmiştir.

Bilgi kavramı ile ilgili çok çeşitli tanımlar ve kavramlar ele alınmıştır. Case (2002)’ in Bateson (1972)’dan aktardığına göre ‘’bilgi insanın bilişsel yapısında değişiklik yaratan herhangi bir şeydir’’ tanımı yaygın olarak kabul edilen bir görüş olmaktadır. McCarthy (2002), bilgiyi ‘’bir veya daha fazla toplumsal grup ya da insan topluluğu tarafından kabul edilen her türlü fikir ve edim biçimleri; onların kendileri ve ötekiler için gerçek kabul ettikleri olgulara ilişkin fikirler ve edimler ‘’ olarak tanımlamış ve bilginin toplumsal bir olgu olduğu kısacası toplumsal olan her şeyle ilişki içerisinde olduğunu belirtmiştir (akt: Uçak 2010). McCarthy’e paralel olarak bilgi konusuna sosyolojik açıdan yaklaşan Aydın (2004) bilgiyi insanın kendini anlama ve yorumlayabilme biçimi olarak tanımlamaktadır. Irzık (2002) bir şeyin bilgi olabilmesi için doğru olması gerektiğinin öne sürmüştür. Özellikle teknoloji çağında görsel medya yoluyla alınan bilginin ne kadar doğru olacağı ve toplum yararına olan katkısını sorgulamıştır. Burada bilginin toplum ihtiyaçlarını ne denli karşıladığını ve toplum yararına ne denli katkıda bulunduğunun sorgulanması gerektiğine değinilmiştir.

Şekil-2.1’de gösterildiği üzere bilgi tek başına bir unsur olmasının yanında birçok değerin birleşmesi sonucu oluşmuştur. Bilgi, davranış, kapasite ve enformasyon unsurlarının birleşmesiyle meydana gelmiştir. Yani kısacası bilgi deneyim, kültür, huy, algılama ölçüsü, bakış açısı, kişilik gibi birçok faktörün bir araya gelmesi ile oluşmuştur (Türk 2003).



Şekil 2.1 Bilginin Tanımı (Türk 2003).

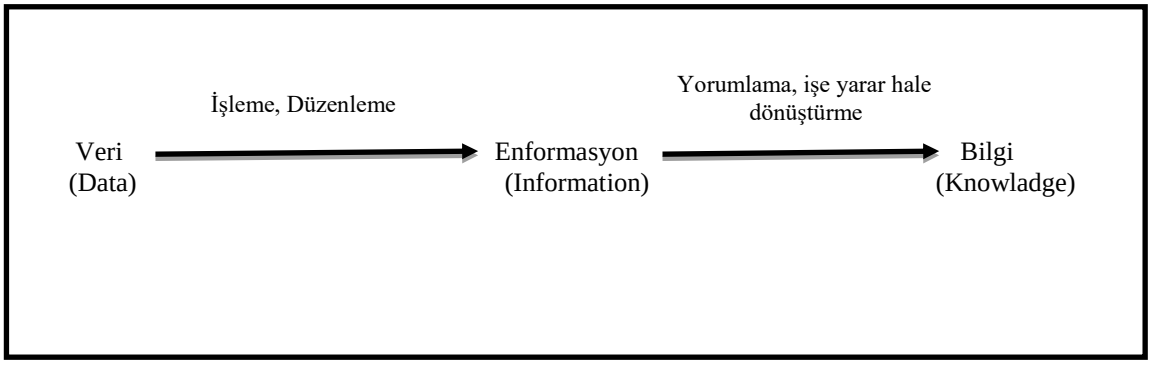
Mengüşoğlu (1988), bilginin nitelikleri üzerine yapmış olduğu incelemede bilgiyi: bilimsel bilgi, doğal bilgi, felsefi bilgi, sanatsal bilgi ve din bilgisi olmak üzere 5 temel tür üzerinde sınıflandırmıştır. Genel olarak kabul edilen bu türlere Aydın (2004), teknik ve politik bilgiyi de ekleyerek 7 temel tür altında toplamıştır. Yeniçeri ve İnce (2005), bilgiyi kullanım alanı, kaynağı, rekabet üstünlüğü ve niteliğine göre 4 ana unsurda birleştirmiş ve farklı türlere ayırmıştır. Ayrıca bir bilginin anlamlı olabilmesi ve değer taşıması için doğrululuk, olayla olan ilgisi, tam ve doğru zamanda olması, ihtiyaç halindeki ulaşılabilme ölçüsü, anlaşılırlık, güvenilir olması ve kabul edilebilir maliyet seviyesinde olması gibi birçok özelliğe sahip olması gerekmektedir. Aksi takdirde bilgi var olur ancak herhangi bir değer taşımaz.

2.1.1 Bilgiyi Oluşturan Temel Unsurlar

Bilginin anlamlı bir sonuca ulaşılabilmesi için onu oluşturan bazı unsurlar vardır. Konunun uzmanlarınca yapılan çalışmalar sonucunda bu unsurlar Veri ve Enformasyon olarak karşımıza çıkmaktadır. Bu iki kavaram bilginin oluşmasında ve kaybolmasında etkin rol oynayan unsurlardır. Bu unsurlar birbirleri ile doğrudan ilişkilidirler. Bilgi

kişisel bir oluşumdur. Bir kişiden diğerine doğrudan iletilmesi mümkün değildir. Bundan dolayı bilgiyi oluşturan temel unsurlarda en az bilgi kadar önem arz etmektedir. Türkçemizde günlük kullanım dilinde bilgi, veri ve enformasyon kavramları çokça birbirine karıştırılmaktadır. Bu kavramlar arasındaki anlam farklılıklarını doğru ayırabilmek, kavramlara sahip oldukları gerçek anlamları ile tanımlayabilmek doğru kullanım ve bilgiye ulaşmak açısından oldukça önemlidir (Odabaş 2003, Yılmaz 2009, Demirtaş 2013).

Bilgi ve onu oluşturan unsurlar arasındaki ilişki şekil 2.2' de gösterildiği gibidir. Buradan da anlaşılacağı üzere bilgiyi elde edebilmek için onu oluşturan unsurların birbirine dönüşmesi oldukça önemlidir. Bir başka deyişle veri işlenmesi sonucu enformasyonu, enformasyonda birtakım işlemlerden sonra bilgiyi oluşturur (Güçlü ve Sotirofski 2006).



Şekil 2.2 Bilgiyi Oluşturan Unsurlar (Güçlü ve Sotirofski 2006).

2.1.1.1 Veri

Veri, verilen şey anlamına gelen Latince datum ve İngilizce data sözcüğünden türetilerek dilimize girmiştir. Litaratür de İlk olarak M.Ö. 3000'li yıllarda ünlü bilim adamı Öklidin çalışmalarında geçmektedir. Türkçe sözlükte anlamı ''bir yargının temelini oluşturan ana öğe'' şeklinde tanımlanmaktadır. Tanımdan da anlaşılacağı gibi bilgiye giden yolda temel öğe veridir. Kısacası veri bilginin işlenmemiş halidir. Günümüzde bilişim alanında sıkça duyduğumuz verinin bu ortamlarda anlamı ise, elektronik ortamlarda yer alan ve aktarılan sinyaller olarak adlandırılmaktadır (Canbek ve Sağıroğlu 2006).

İnternet ve gelişen teknoloji ile birlikte hayatımızın vazgeçilmez unsurları olan cep telefonu, tablet, akıllı saatler vb. birçok teknolojik cihazlar veri üretir konuma gelmiştir. Verideki bu büyük artış büyük veri (Big Data) kavramını da ortaya çıkarmış ve yeni bir devrin başlangıcı olmuştur (Doğan ve Arslantekin 2016). Verinin giderek artan bu büyüklüğü verinin saklanmasında dijital platformların kullanılmasına yol açmış ve böylece kişisel veri kavramının ortaya çıkmasına neden olmuştur. Önem arz eden bu konuyu ayrıca açıklanmasının yararlı olacağı düşünülmektedir

- **Kişisel Veri**

Kişisel veri kısaca bir kişiye ait her türlü bilgi olarak tanımlanabilir. Kişinin sosyal, aile, özel hayatına, iş dünyasına ilişkin her türlü bilgi kişisel veridir. Kişisel veri konusu özellikle verideki artış ile birlikte çok önemli bir durum haline gelmiştir. Kişisel verilerin tamamı artık dijital platformlarda bulunmaktadır. Ve kişiler tamamen kendilerine ait olan bu verileri koruyabilmek için çeşitli önlemler almaktadır (Çetin 2014). Çok önemli bir konu olan kişisel verilerin korunması ile ilgili ülkemizde kişisel verileri koruma kurulu ve kişisel verilerin korunması kanunu oluşturulmuş ve kişiye özgü bu veriler koruma altına alınmaya çalışılmıştır. Bilgi güvenliği konusu ile kişisel veri kavramı birbiri ile tamamen ilişki içerisinde iki kavramdır.

2.1.1.2 Enformasyon

Sözlük anlamı danışma, tanıtma olan enformasyon sözcüğü verinin düzenlenmiş hali olarak karşımıza çıkmaktadır. Veri üzerinde yapılan düzelme çoğunlukla düzeltmeyi yapan kişi için bir anlam ifade etmektedir (Barutçugil 2002). Enformasyon verinin anlam kazanmış halidir. Davenport ve Prusak, (2001)'a göre enformasyon bir çeşit mesajdır ve bir belge olabileceği gibi görsel ve işitsel de olabilmektedir. Aynı zamanda mesajın alıcısına bir değer katmalı, bakış açısını farklı yönlere çekebilme özelliği yüklemelidir. Bu durum gösteriyor ki veriye katılan anlam ne kadar iyi olursa enformasyonun niteliği de o denli iyi olmaktadır ve ulaşılan bilginin değerini artırmaktadır. Bunun yanında enformasyonun taşıdığı anlam alıcı tarafından bakış açısına bağlı olarak veri niteliğine dönüşebilir. Yani enformasyon mesajı alan kişinin algı ve gereksinimlerini karşılarsa bir anlam ifade eder.

Türkçede çok sık birbirine karıştırılan ve aynı anlam ifade ettiği düşünülen veri, enformasyon ve bilgi kavramlarının birbirine çok yakın olduğu ancak aralarında büyük farklar olduğu görülmektedir. Doğru ve nitelikli bilgiye ulaşmanın yolu onu oluşturan unsurların doğru yorumlanmasından geçmektedir. Çapar (2005), bu kavramlar arasındaki bağı; ‘’bilgi, veri ve enformasyonu akıl süzgecinden geçirilip kişisel deneyimler, karar verme, tahmin etme vb. eylemlerde yeri geldiğinde kullanılan şeklidir’’ diye açıklamıştır.

2.2 Bilgi Güvenliği Kavramı

21. yüzyılın bilgi çağı olmasından dolayı, şirketler, devlet kurumları, sağlık, eğitim vb. tüm alanların ortak paydası bilgi çağında yaşıyor olmalarıdır. Bu kurumlar arasında ister üretim alanında ister tüketim tarafında ve ister hizmet alanında bulunun sahip olunan en önemli değer bilgidir. Kurumların veya şirketlerin rekabet edebilmesi ve gerçekleştireceği her türlü faaliyetlerinde bilgi unsuru kesinlikle yer alacaktır. Bu durum sahip olunan bilginin önemini de artırmaktadır. Bu kadar değerli ve vazgeçilmez olan bilginin uygun bir şekilde korunması da başlı başına bir iş ve alan olmuştur (Eminağaoğlu ve Gökşen 2009).

İnternet ve bilişim teknolojilerindeki gelişim ve bugün geldiği nokta itibarı ile tüm dünya üzerindeki ülkelerde olduğu gibi ülkemizde de gelişmesi ve kullanıcı sayısı hızla artmaktadır. Çizelge 2.1’de gösterildiği üzere TÜİK’in 2017 yılı hane halkı bilişim teknolojileri kullanımı araştırmasında; 2004 yılında hane halkı seviyesinde bilgisayar kullanımı %23,6 iken bu oran 2017 yılında %56,6’lara çıkmıştır. Yine internet kullanımı 2004 yılında %18,8 seviyesinde iken 2017 yılında %66,8 seviyelerine ulaşmıştır. Yine Deloitte şirketince yapılan 2015 global kullanıcı anketinde Türkiye, dinamik genç nüfusu nedeni ile dünyada cep telefonu bağımlılığının en yüksek olduğu ülkelerden biri olduğu ve bu kapsamda katılımcıların %82’si internet erişimi için akıllı telefonları tercih ettikleri görülmektedir (İnt.Kyn.1).

Çizelge 2.1 Girişimlerde ve hanelerde bilişim teknolojileri kullanımı (TÜİK 2017)

	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
Girişimlerde Bilişim Teknolojileri Kullanımı ICT Usage in Enterprises														
Bilgisayar kullanımı - Computer usage	-	87,8	-	88,7	90,6	90,7	92,3	94,0	93,5	92,0	94,4	95,2	95,9	97,2
İnternet erişimi - Internet access	-	80,4	-	85,4	89,2	88,8	90,9	92,4	92,5	90,8	89,9	92,5	93,7	95,9
Web sitesi sahipliği - Having website	-	48,2	-	63,1	62,4	58,7	52,5	55,4	58,0	53,8	56,6	65,5	66,0	72,9
Hanelerde Bilişim Teknolojileri Kullanımı ICT Usage in Households and Individuals														
Bilgisayar kullanımı (Toplam) - Computer usage (Total)	23,6	22,9	-	33,4	38,0	40,1	43,2	46,4	48,7	49,9	53,5	54,8	54,9	56,6
Erkek - Male	31,1	30,0	-	42,7	47,8	50,5	53,4	56,1	59,0	60,2	62,7	64,0	64,1	65,7
Kadın - Female	16,2	15,9	-	23,7	28,5	30,0	33,2	36,9	38,5	39,8	44,3	45,6	45,9	47,7
İnternet kullanımı (Toplam) - Internet usage (Total)	18,8	17,6	-	30,1	35,9	38,1	41,6	45,0	47,4	48,9	53,8	55,9	61,2	66,8
Erkek - Male	25,7	24,0	-	39,2	45,4	48,6	51,8	54,9	58,1	59,3	63,5	65,8	70,5	75,1
Kadın - Female	12,1	11,1	-	20,7	26,6	28,0	31,7	35,3	37,0	38,7	44,1	46,1	51,9	58,7
Hanelerde İnternet erişimi - Households with access to the Internet	7,0	8,7	-	19,7	25,4	30,0	41,6	42,9	47,2	49,1	60,2	69,5	76,3	80,7

Ülkemizde ve dünyada ki tüm bu teknolojik gelişmeler ve özelliklede internetin gelişmesi ile birlikte sahip olunan bilginin boyutları da artmıştır. Hayatımızın bir parçası haline gelen cep telefonu, tablet gibi çok yönlü küçük ancak marifeti büyük teknolojik cihazlar sayesinde bilgiye ulaşmak çok kolay bir hale gelmiş ve aynı zamanda bilginin işlenmesi, depolanması, aktarılması kolaylaşmıştır (Şahinaslan vd. 2009).

Dijital platformlarda tutulan kişisel ve kurumsal boyuttaki her türlü bilginin mutlak gizliliğinin sağlanması ve veri kaybının önlenmesi, ikinci şahısların eline geçmesini önlemek için güvenliğinin sağlanması zorunluluk haline gelmiştir. Sahip olunan bu bilginin korunması sadece bu işi profesyonel olarak yapan bilgi güvenliği uzmanlarının yanında doğrudan veya dolaylı olarak bilgiye nüfuz eden, kurumsal boyutta bilgi sistemlerini etkileyen tüm bireylerin de görevi haline gelmiştir (Vural 2007).

Bilginin bu denli gelişimi ve iletilmesinin kolaylaşmasının birçok yararının olması yanında en değerli kazanımlardan biri olan bu bilginin korunması da başlıca bir sorun haline gelmiştir. Kişisel ve kurumsal bazda sahip olunan bilginin boyutu ve dijital

ortamdaki hareketliliği çeşitli güvenlik risklerinin oluşmasına ve bilginin istem dışı olarak üçüncü şahısların eline geçmesine sebep olmaktadır. Önceleri sadece insan faktörüne dayalı yani fiziksel olarak oluşan bu tehditler elektronik bilgi sistemlerinin yaygınlaşması ile yazılım ve donanımsal tehditler başta olmak üzere çok çeşitli boyutlar kazanmıştır. Bu tehditlerden korunmak için kişisel ve kurumsal boyutta yüksek maliyetler ödenmek sureti ile önlem alınmaya çalışılmaktadır. Yazılımsal tehditlerden korunmak için çok çeşitli teknolojik altyapılar kurularak bu riskler en aza indirilmeye çalışılmakta ancak kullanıcı kaynaklı bilgi güvenliği açığında durumsal farkındalık oluşturmaktan ve oluşabilecek riskleri en aza indirmeye çalışmaktan başka çare bulunamamaktadır. Bu yüzden Bilgi güvenliği konusunda en zayıf halka olan insan faktörünün bilgi güvenliği risklerine karşı bilinçlendirmek ve oluşabilecek riskleri kabul edilebilir seviyeye indirmek önem arz etmektedir (Baykara vd. 2013, Şahinaslan vd. 2009, Çetin 2014).

Bilgi Teknolojileri Kurumu tarafından yapılan 2017 yılı elektronik haberleşme sektörüne ilişkin yıllık istatistik bültenin de özellikle 2016 yılında 4.5G teknolojisinin hızla yaygınlaşmaya başlamasından itibaren internet abone sayılarında ve veri iletişim trafiğinde önemli ölçüde artışlar kaydedilmiştir. İnternet abone sahipliği 2017 yılı itibarı ile 62,2 milyona yükselmiştir (Anonim 2018). Bu durum günümüzde birçok kişinin akıllı telefon, tablet, bilgisayar vb. çeşitli teknolojik cihazlar vasıtasıyla internet ortamını kullandığını göstermektedir. Günümüzde birçok bilgi bilgisayar akıllı telefon vb. elektronik ortamlarda tutulmaktadır. İnternete bağlı olan elektronik cihazlardaki bilgi, veya veri herhangi bir ağa bağlı olmayan bilgisayar, telefon vb. elektronik cihazlara göre daha fazla risk oluşturmaktadır ve bu durum internet kullanıcıların dikkat etmesi gereken bir husus olarak öne çıkmaktadır.

Bilgi Teknolojileri Kurumunca yayınlanan bülten de internet abone sayısında ki artış göz önünde bulundurulduğunda bu bilgiler bazen bilinçli olarak sosyal medya ortamlarında paylaşılmaktadır. Kişinin dini, etnik, siyasi, aile vb. birçok konuda fikir ve görüşlerini yansıtan bu bilgiler şahıs olarak çok önem arz etmese de bazı kötü niyetli kişilerin kullanabileceği bir ortam oluşturmaktadır. Bilgi güvenliği konusunda her ne

kadar çeşitli önlemler alınmaya çalışılsa da bilgi paylaşımında kullanılan sosyal medya ortamlarına da dikkat etmek gerekmektedir (Ertuğrul ve Keskin 2012).

Sayarı 2009'a göre elektronik ortamlarda tutulan bilginin güvenliğinin sağlanamaması durumunda genel anlamda şu gibi risklerin ortaya çıkmasına yol açmaktadır;

- Kurumların sahip oldukları ve özellikle gizli içerikli bilgiler üçüncü şahısların eline geçebilecektir.
- Sahip olduğu bilgiyi koruyamayan ve üçüncü şahısların eline geçmesini önleyemeyen kurumlar ciddi itibar kayıpları yaşayacaktır.
- Kamu kurumlarında kaybedilen hassa bilgiler ülke menfaatlerine zarar verebilecektir.
- Bilginin kaybedilmesi onu tekrara sağlayabilmek için belli bir süre iş ve zaman kaybına sebebiyet verecektir.
- Özellikle kamusal anlamda ve bazı önemli kurumlar yasal olarak ciddi yaptırımlara maruz kalabilecektir.

Bilgi çağı ve bilgi toplumunda yaşayan bireyler, şirketler ve kurumlar olarak bilgi güvenliği konusu sadece belli bir kesimin konusu olmaktan çıkmış ve bilgiye sahip olan herkesi ilgilendiren bir konu haline gelmiştir. Schmidt (2004)'e göre bilgi güvenliği kavramı, bilgiye istenildiği zaman erişilme imkânı olan elektronik platformlarda, bilginin gönderici ve alıcı arasındaki transfer sürecinde, bütünlüğünün sağlanması ve üçüncü şahısların nüfuz etmeden güvenli bir şekilde gönderilmesi şeklinde tanımlanmıştır (akt: Yılmaz vd. 2016). Kısacası bilgi güvenliği, elektronik ortamlarda bilgilerin depolanması ve iletimi esnasında bilgilerin içeriğinin bozulmadan, yetkisiz kişilerin erişiminden korunması için güvenli bir alan yaratma çalışmalarının tümü olarak tanımlanmaktadır (Canbek ve Sağıroğlu 2006). Bu tanımdan da anlaşılabileceği üzere bilgi güvenliği; bilgilerin yetkisiz kişilerin eline geçmesinin yanında gizlilik, bütünlük, erişilebilirlik (kullanılabilirlik) gibi onu oluşturan unsurların da yeterli düzeyde sağlanması ile mümkün olabilir.

2.2.1 Bilgi Güvenliğini Oluşturan Temel Unsurlar

Bilgi güvenliğinin tam manası ile anlaşılması ve uygulanabilmesi için onu oluşturan unsurların da iyi bilinmesi gerekmektedir. Bilgi güvenliği temel de üç unsuru içerir bunlar; Gizlilik, Bütünlük, Kullanılabilirlik (Erişebilirlik)' tir.

2.2.1.1 Gizlilik

Gizli sözcüğü literatür de sıkça karşılaşılan ve günlük hayatımızda sürekli kullandığımız bir kelimedir. Türk dil kurumunca başkalarından saklanan, duyurulmayan, saklı kalan, mahrem anlamlarına gelmektedir. Buradan anlaşılacağı üzere gizli kişiye ait olan her türlü bilgi, veri vb. edinimleri içerir. Bir güvenlik unsuru olarak baktığımız gizlilik sahip olunan bilgiye kişinin kendisinin veya kurumun sadece izin verildiği ölçüde üçüncü kişilerce ulaşılabilmesidir.

TSE ISO/IEC 27002: 2017 " Bilgi Güvenliği Yönetim Standardı'' gizliliği bilginin yalnızca yetkili kullanıcı veya kullanıcıların, erişebilir olmasının gerçekleştirilmesi olarak tanımlamaktadır. Kişisel ve kurumsal kullanıcılar olarak gizliliği temin için birçok yöntem uygulanabilir. Parola oluşturma, kilitleme vb. kontroller gizliliği sağlamak için örnek olarak verilebilir. Kurumsal bazda gizlilik niteliğinin sağlanması için kurum tarafından hazırlanan politika, sözleşme de belirli bir bilgi varlığının gizlilik seviyesi ve karşılıklı yapılması gereken işlemlerin tanımlanması gerekmektedir (Ganbat 2013).

2.2.1.2 Bütünlük

Bütünlük, bilginin depolandığı yerde veya başka bir ortama aktarıldığında, yetkisiz kişilerce içeriğinin bozulması, değiştirilmesi, silinmesi gibi tehditlere karşı korunması olarak tanımlanabilir. ''Bilgi Güvenliği Yönetim Standardı'' bütünlüğü, bilgi ve bilgi işlemleri ile veri içeriğinin bozulmadığının garanti altına alınması olarak tanımlamaktadır. Bilginin içeriğinde meydana gelecek olan bozulma kasıtlı veya kaza ile olması bütünlük tabirinde herhangi bir değişikliğe sebep olmaz (Özcan 2009). Özellikle kurumların verinin veya bilginin bütünlüğünün sağlanması ve korunması için

önlem almaları gerekmektedir. Kurumsal anlamda bir denetim mekanizması kurularak bilginin bütünlüğü, doğruluğu konusunda bazı stratejiler geliştirilmeli ve yapılacak kontrollerde bu durum sağlanmalıdır.

2.2.1.3 Erişebilirlik, Kullanılabilirlik

Erişebilirlik adından da anlaşılacağı üzere yetkili kişilerce sahip olunan bilgiye istenildiği zaman erişilebilmesinin sağlanmasıdır. Bilgi yönetim standardına göre Erişilebilirlik; yetkili kullanıcıların ihtiyaç duyulduğunda bilgi ve ilişkili varlıklara erişim hakkının olmasının temini olarak tanımlanmıştır. Kısacası bilgiye veya veriye kişinin istediği zaman ulaşabilmesinin bilgi sağlayıcıları tarafından sağlanmasıdır. Kurumlar bu konu ile ilgili erişim yetkilendirme etkinliğinin doğru ve güvenli bir şekilde sağlamalıdır (Ganbat 2013).

2.2.1.4 Diğer Unsurlar

Canbek ve Sağıroğlu (2006), bilgi, bilgi güvenliği ve süreçleri üzerine isimli makalesinde de belirttiği üzere bilgi güvenliğini sağlayan ve genel geçerlilik görmüş bu üç temel unsurun yanında bazı yan unsurlar da bulunmaktadır. Bunlar; sorumluluk, erişim denetimi, güvenilirlik, kimlik kanıtlama, inkâr edememe ve emniyettir. Bu kavramların anlamını kısaca açıklamak gerekirse;

- Kimlik kanıtlama, kullanıcıların sistem üzerinde erişim sağlayabileceği belirli tanımlama işlemleri neticesinde sisteme kimin girdiğinin belirlenmesi işlemidir.
- İnkâr edememe, herhangi bir bilgi veya veriye erişen kimsenin yada transfer sürecinde gönderen ve alan tarafların inkar edemeyecek şekilde kayıtların tutulması işlemidir.
- Sorumluluk, Sistem sorumlularını belirleme aşamasıdır. Çoğu bilgi sistemlerinde bulunan log kayıt sistemi bu unsura örnek olarak gösterilebilir.
- Erişim denetimi, sisteme erişmek için gerekli izinlerin verilmesidir.

- Güvenilirlik, bir elektronik sistemin gereksinimleri karşılayacak şekilde teknik şartnamede bahsedilen hususlar ile ilgili gerekli garantiyi sağlayabilme yeteneğidir.
- Emniyet, bir bilgisayar sisteminin başka bir çalışma ortamına entegre olduğu durumlarda entegre olduğu ortam için gelebilecek tehlikeleri önleme çalışmalarıdır.

2.3 Bilgi Güvenliğini Tehdit Eden Unsurlar

Tehdit; bilgisayar ve bilişim dünyasında bir sistemin veya sitemin bulunduğu kurumun zarar görmesine sebep olan bir saldırı durumunda, gerçekleşen olayın arka planında bulunan gizli sebepler olarak tanımlanabilir (Eken 2013). Yukarıdaki konu başlıklarında sıklıkla bahsedildiği üzere teknolojik gelişmelerde yaşanan yenilikler sahip olunan tüm bilgilerin dijital ortama taşınması ihtiyacını doğurmuş ve buna paralel olarak kötü niyetli kişiler için bilgilerin tutulduğu bu dijital platformlar hedef haline gelmiştir. Bilgiyi üretmek ve onu uygun şekilde depolamanın yanında bahse konu sistemlerin güvenliğini sağlamakta en az bilgiye sahip olmak kadar önemli bir konudur. Bilgi güvenliğinin tehdit eden unsurlar teknolojik gelişmelerden önce bilgilerin fiziki olarak güvenliğinin sağlanması şeklinde düşünülse de günümüzde dijital platformların kapasiteleri ve yetenekleri göz önüne alındığında bilgi güvenliği daha çok dijital veri güvenliği olarak anlaşılmaktadır (Yılmaz vd. 2016). Özellikle devlet kurumlarında, özel şirketlerde veya kişisel olarak bilginin tutulduğu bu dijital platformların internet ortamına bağlı olması oluşan riski de ciddi anlamda artırmaktadır.

Dijital veri güvenliğini tehdit eden birçok unsur bulunmaktadır. Bunlar kısaca yazılımsal, fiziksel ve kullanıcı kaynaklı tehditler olarak 3 temel konu başlığı altında toplamak mümkündür. Bu tehditlerin neler olduğunun bilinmesi ve farkındalık oluşturulması bilgi güvenliği risklerini kabul edilebilir seviyeye indirmek adına önemlidir.

2.3.1 Yazılım Kaynaklı Tehditler

Zararlı yazılımlar (malwere) günümüz bilgisayar ve teknoloji dünyasında karşılaşılan en büyük tehditlerden biridir. Zararlı yazılımlar sistemlere yetkisiz olarak giriş yaparak sahip olunan bilgilere nüfuz etmek, bilgilerin çalınması, yok edilmesi, değiştirilmesi vb. bilgisayara zarar vermek üzere tasarlanmış olan her türlü yazılımlardır (Kara 2015). Bu tip yazılımların ana amacı bilgi çalma ve sistemlere zarar vermektir. Günümüz de internet kullanan veya herhangi bir ağa bağlı olan birçok kişi doğrudan veya dolaylı olarak bu zararlı yazılımların etkisi altında kalmıştır. Dünyanın önde gelen siber güvenlik kuruluşlarından McAfee şirketinin yayınlamış olduğu McAfee Labs 2018 siber tehdit raporuna göre 2017 yılının 4'üncü çeyreğinde her saniye sekiz yeni virüsün ortaya çıkması ile zararlı yazılım sayısı en yüksek seviyelere ulaşmıştır. 2017 yılının 3'üncü çeyreğinde saldırganlar en çok bankacılık ve finans sektörünü hedef almalarına karşın 4'üncü çeyreğinde siber suçluların dosyasız zararlı yazılımlar, kripto para birimi madenciliği, gizli mesaj yerleştirme ve sağlık sistemlerine yönelik tehditlerinde rekor artışların olduğunu göz önüne sermektedir (İnt.Kyn.2). Bu durum göstermektedir ki her yeni gelişmeye karşın siber suçlularında farklı tür saldırı yöntemleri ve zararlı yazılımlar ile bilgi ve bilgi sistemlerimizi hedefleri haline getirmektedirler.

Özellikle herhangi bir ağa başlı bilgisayarlarda zararlı yazılımlara maruz kalma olasılığı çok daha artmaktadır. Bundan dolayı internet ortamına bağlı bulunan bilgisayarlarda bilgi güvenliğinin sağlanması için dikkatli olunması gerekmektedir. Güvenlik duvarı ve anti virüs programları zararlı yazılımlara karşı koruma sağlamanın en temel yollarından biridir. Zararlı yazılım türlerinin ve çalışma şekillerinin bilinmesi önlem alınması bakımından önem arz edeceğinden belli başlı zararlı yazılım türleri aşağıdaki gibidir (Arıcı 2018, Can ve Akbaş 2014, Yılmaz ve Sağıroğlu 2013, Bıçakçı 2014, Erdoğmuş 2017, Gülmüş 2010, Moody et. al. 2018, İnt.Kyn.3).

- **Virüsler:** Çalıştırılabilir dosya uzantılarına bulaşan bir yazılım türüdür. Virüsler, bulaştıkları diğer bilgisayarlardan sizin bilgisayarınıza CD, DVD, USB bellek veya ağ yoluyla erişebilirler. Aşağıda yaygın virüs türlerini görebilirsiniz:

1. **Dosya virüsleri:** Dosyalara bulaşan virüslerdir, .exe ve .com uzantılı çalıştırılabilir dosyalara bulaşır.
2. **Script virüsleri:** Script virüsleri, dosya virüslerinin çeşitli programlama dillerinde (VBS, JavaScript, BAT, PHP v.s) yazılmış bir alt türüdür. Bu virüs türleri diğer Windows veya Linux kodlarının scriptlerine kendi kodunu ekleyerek veya başka bir virüsün uzantısı şeklinde bulaşabilir.
3. **Boot virüsleri:** Boot virüsleri usb bellek gibi taşınabilir cihazların veya sabit disklerin boot sektörüne bulaşan ve bu aygıtlar her çalıştırıldığında otomatik olarak kendilerini çalıştıran virüs türleridir.
4. **Makro virüsleri:** Makro virüsleri zararlı virüs kodunu dökümanların içine enjekte edebilir. Bu virüs türleri genellikleri zararlı virüs kodunu kelime veya tablo işleme uygulamalarının (word, excel, v.s) dosyalarına enjekte eder. Bu şekilde virüslü döküman her çalıştırıldığında virüs de çalıştırılmış olur.

Virüsler ayrıca eylemi gerçekleştirme türlerine göre de sınıflandırılabilir. Direct action virüsleri çalışmak için kullanıcının bir eylem gerçekleştirmesini bekler. Resident(kalıcı) virüsler ise sürekli olarak bilgisayar belleğinde çalışmaya devam eder.

- **Solucanlar:** Bilgisayar solucanları virüslerin bir alt grubu olarak nitelendirilmektedir. Ağ sistemi üzerinde çalışırlar ve genellikle internet sayfaları arasında gezinirken ortaya çıkan istenmeyen sekmelere tıklanması sonucu bilgisayara bulaşırlar. Bilgisayarda oluşturduğumuz dosyaları silme, sistemi yavaşlatma, bazı sistem programlarına etki etme gibi özellikleri vardır.

- **Truva atları:** Virüs ve solucan gibi kendini kopyalayıp dosyalara bulaşamayan bir zararlı yazılım türüdür. Genellikle çalıştırılabilir dosya (exe, com) tipinde olur ve trojan kodu dışında farklı bir kodu bünyesinde bulundurmaz. Bundan dolayı tek çözüm yolu bilgisayara bulaşan trojan dosyasının bulunup silinmesidir. Trojanlar, keylogger(tüm klavye girişleri kaydeden program) işlevinden dosyaları silmeye veya disk biçimlendirmeye kadar çeşitli fonksiyonlara sahip olabilir. Bazı trojanlar saldırgana bir arka kapı açarak

sistemde bulunan şifre, e-posta, dosyalar, veriler vb. birçok önemli bilgiye erişebilirler. Genellikler lisanssız yazılımlarda, internette bulunan çeşitli film, müzik izleme sitelerinde, ücretsiz indirme imkânı sağlayan sitelerden bilgisayara bulaşırlar.

- **Adware:** Reklam destekli yazılım ifadesinin kısaltılmış halidir. Kullanıcıya reklam materyali gösterme amacı taşıyan yazılımlar bu kategoriye girer. Adware genellikle internete bağlandınız sırada reklam içerikli tarayıcı penceresi açarak, internet tarayıcı ana sayfasını değiştirerek veya bir windows uygulamasının penceresini açarak karşımıza çıkarlar.

- **Spyware**: Kullanıcıdan herhangi bir bilgi almaksızın çeşitli bilgileri toplayan bir zararlı yazılım türüdür. Bu Spyware yazılımları çalıştıkları ortamda sistem ile ilgili bilgileri, yüklü uygulamaları, internet geçmişi ile ilgili bilgileri, kayıtlı şifreler vb. önemli bilgileri almaya çalışırlar. Bunun yanında kredi kartı ve diğer hesap bilgileri gibi finans bilgileri ve kimlik hırsızlığı gibi tehlikeli amaçlar için oluşturulan Spyware türleri de vardır.

- **Riskware :** Çalıştığı zaman kullanıcı güvenliği için risk oluşturan tüm yazılımlar bu sınıfa girer. Spyware ve adware'de olduğu gibi riskware yazılımları da kullanıcının bilgisi dahilinde bilgisayara kurulabilir. Kullanıcıyı ödeme sayfasına yönlendiren "Dialer" isimli uygulamalar en tanınmış riskware tipine bir örnektir. Birçok program legal olarak kullanıcıyı ödeme sayfasına yönlendirebilir ancak bu gibi yazılımlar kullanıcıyı yanıltarak rızası olmadan bu sayfalara yönlendirir.

- **Tehlikeli olabilecek uygulamalar :** Özellikle akıllı telefonların gelişmesinden sonra, siber suçlular tarafından geliştirilen ve üçüncü parti uygulamalarına gömülen zararlı kodlar ile cihazlarda bulunan şifreler, bankacılık gibi finansal faaliyetler, kişinin özel hayatını ilgilendiren SMS'ler, sohbet geçmişi, resim, video kaydı vb. tüm bilgilerin üçüncü şahısların eline geçmesine imkan tanımaktadır. Bu tip programlar kullanıcı tarafından cihazlara kurulur.

Günümüzde cep telefonu kullanım oranı ve uygulama sayıları dikkate alındığında önlem alınmaması durumunda ciddi tehlike oluşturabilirler. Cep telefonlarına yüklenecek olan uygulamaları kurmadan önce içeriğine, kullanım izinlerine ve üretici firmaya dikkat etmek alınab ilecek en temel kullanıcı önlemidir Çeşitli güvenlik programları ve kullanıcı farkındalığı ile Keylogger, ekran kaydetme, uzaktan erişim araçları, şifre kırma ve güvenlik testi programları bu sınıfa giren programlara örnektir.

- **Hoax :** Kullanıcılara gönderilen ve kasıtlı olarak yanlış bilgilendirme amacı taşıyarak okuyan kişi tarafından yayılmasını amaçlar. Hoax genelde kullanıcının yapmaması gereken bir şeyi yaptırabilmek üzere yapılmıştır. Bu tip mesajlar bazen kullanıcılara sistem dosyalarından bazılarını silmelerini söyleyerek bilgisayar sistemlerine zarar vermeyi amaçlarlar.

- **Dos saldırıları :** Açık adı Denial of Service yani servis dışı bırakma saldırısı olan Dos saldırıları bir bilgisayarı veya ağı hedef alarak kullanımını yavaşlatmaya ve o ağı kullanılamaz hale getirmeyi hedefleyen saldırılardır. Kullanıcılar arasındaki iletişimi keser. Hizmet kesilmesine neden olan saldırı bilgisayarı birçok farklı yerlerde dağınık bulunması durumunda DDOS olarak adlandırılır. Bu tip saldırılar genellikle bilgisayarın yeniden başlatılması ile düzeltilir.

- **DNS Zehirleme:** bir bilgisayar sisteminin DNS sunucularını etki altına alır ve sunucunun ön belleğinde bulunan veri tabanındaki verileri değiştirerek veya veri ekleyerek sistemin başka bir sunucuya yönlendirilmesini sağlama işlemidir. Bunun sonucunda, istedikleri web sitesine ulaşmaya çalışan kullanıcılar gerçek sitenin yerine saldırganlar tarafından kontrol edilen başka bir web sitesine yönlendirilirler. Buradaki en büyük tehlike kullanıcıların web sitesine verdikleri bilgilerin kötü niyetli kişilerin eline geçmesidir.

2.3.2 Fiziksel Tehditler:

Deprem, sel, yangın gibi doğal afetler veya olası gelebilecek teknik arızalar bu

kategoriye girmektedir. Önceden tespit edilmesi zor olan bu tip tehditler karşısında önceden hareket tarzları belirlenerek afet durumunda uygulanması yaşanacak olan bilgi kaybını en aza indirebilir (Tekerek 2008). Kurumsal anlamda böyle bir olay karşısında olası senaryolar belirlenerek önemli bilgilerin tutulduğu sistemlerin ilk olarak kurtarılması sağlanabilir. Bunun yanında felaket sonrası en kısa sürede geriye nasıl dönüleceği ile ilgili önceden planlamalar yapılmalı ve hayati önem arz eden bilgilerin muhakkak bir yedeğinin bulunması sağlanmalıdır. Gülmüş (2010), yapmış olduğu çalışmada fiziksel güvenliğin sağlanabilmesi için standart hale gelen ve bilgi güvenliği açısından gerekli bazı işleri özetlemiştir. Bu işler aşağıda sıralanmıştır.

- Bilgi işleme servis merkezlerinin korumak amacıyla fiziksel bir sınır güvenliği tesisi (yetkili kontrollü kart sistemi, güvenlik görevlilerinin bulunduğu nizamiye vb.) kurulmuş olmalıdır.
- Bazı önemli yerlere sadece yetkili personelin girebilmesini sağlayabilecek parmak izi okuma vs. gibi tedbirler geliştirilmelidir.
- Birliğe veya kuruma gelen ziyaretçiler belli bölümlerde bekletilmeli ve muhakkak kayıt altına alınmalıdır.
- Kurum içerisinde çalışanlar kimliklerini belirleyebilecek şekilde tanıtım kartı taşımalıdır.
- Kişisel çalışma odalarında fiziki güvenlik tedbirlerine uyulmalıdır.
- Kritik tesis ve kurumlar herkes tarafından kolayca ulaşamayacağı yerlerde olmalıdır.
- Kurum içerisinde çalışanların güvenliğini sağlayacak yönetmelikler uygulanmalıdır
- Kritik bilgilerin bulunduğu sistem odalarına ait telefon rehberlerine herkesin ulaşamaması için tedbirler alınmalıdır.
- Doğal afetler sonucu olabilecek fiziki tahribata karşı tedbirler geliştirilmeli ve belli zamanlarda yapılacak tatbikatlarla herkes tarafından uygulanabilir seviyeye getirilmelidir.
- Kurumun yakınında bulunan ve tehlike oluşturabilecek tesislere karşı önlem geliştirilmelidir

- Herhangi bir olumsuz durumda sistemin tamamen durmaması için yedek sistemler oluşturulmalı ve bu sistem ana merkezden olabildiğince uzakta olmalıdır
- Tüm personel bilmesi gerektiği kadar bilgi prensibine uymalıdır.
- Ses ve görüntü kaydeden cihazlar önemli bölümlere sokulmaması için önlem geliştirilmelidir
- Kritik bölümlerde kimsenin olmadığı durumlarda kilit altında tutuluyor olmalıdır.
- Kritik bölümlerde yapılacak çalışmalarda dışarıdan gelen personele muhakkak nezaret ediliyor olmalıdır.
- Korunması gerektiren kritik ekipmanlar gerekli şekilde izole edilmiş olmalıdır
- Özelikle sistem odalarındaki bilgisayar sistemlerinin zarar görmemesi için sıcaklık, nem gibi etkileyebilecek parametreler kontrol altında tutulmalıdır.
- Bilgi sistemlerinin bulunduğu odalarda dışarıdan gelebilecek yangın vs. gibi tehlikelere karşı sigara içilmemesi vb. levhalar bulunmalıdır
- Acil durumlarda iletişime devam edebilmek için ana sistemden bağımsız hatlar oluşturulmalıdır.
- Kablolar yer altında olmalıdır.
- Kurumlar yasal yükümlülüklerini yerine getirmelidir.
- Ana sistemden çıkan hatların özellikle güç kabloları ile veri kablolarının birbirinden bağımsız şekilde ayrılmalıdır.
- Bakım onarım zamanlarında yanlış bağlantı olmaması veya herhangi bir arıza durumunda doğru müdahaleyi yapabilmek için kablolar etiketlenmiş olmalıdır.
- Çok hassas bilgiler için ayrıca önlemler geliştirilmeli ve koruma altına alınmalıdır.
- Alternatif yol ve iletişim kanalları mevcut olmalıdır.
- Ekipmanlar sigortalı olmalı ve sigortada yazan şartlara uygun olmalıdır.
- Alternatif yol ve iletişim kanalları mevcut olmalıdır.
- Özellikle bilgi sistemlerinde meydana gelen arızalarda dışarıdan yapılacak müdahalelerde mümkünse özel bilgiler yedeklenmeli ve silinmelidir. Gerekli önlemler alınmalıdır.

2.3.3 İnsan Kaynaklı Tehditler:

Daha önce belirtildiği üzere bilginin boyutundaki artış onu elektronik ortamlara taşınmasını sağlamış ve gelinen nokta itibarı ile elektronik ortamda bulunan bu bilgilerin boyutlarındaki inanılmaz artış bilgi güvenliğinin sağlanması ihtiyacını kişisel ve kurumsal bazda maksimum seviyeye çıkarmıştır. Bunun sebebi bilgilerin paylaşımlarının çok kolay olması, bilgiye bulunduğumuz her yerden ve her ortamdan erişilebilir olması bu paylaşımlar esnasında meydana gelen açıklar üzerinde veri kaybı yaşanma ihtimalinin yüksek olması olarak gösterilebilir (Vural ve Sağıroğlu 2008).

Herhangi bir sisteme erişme imkânı olan bir kullanıcının, bilgi sistemlerini bilinçsiz ve yeterli eğitim almadan kullanması sonucu erişilebilirlik, gizlilik, bütünlük gibi bilgiyi oluşturan unsurların bir veya birkaçının ihlal edilmesine sebep olan bilmeyerek veya ihmalkârlık sonucu yapılan kullanıcı davranışlarını insan faktöründen kaynaklanan istem dışı tehditler olarak tanımlayabiliriz (Vural 2007).

Bilginin bulunduğu elektronik ortamlarda güvenliğinin sağlanması için özellikle kurumsal anlamda alınan yazılımsal önlemlerin büyük önem taşıdığı düşünülmektedir. Ancak yapılan araştırmalar bize gösteriyor ki bilgi güvenliğini sağlamanın en iyi yolu bilgi teknolojilerine, onu oluşturan yazılımsal ve teknik altyapılarına çok para harcamanın yanında o sistemi kullanan kişilerin bilinçlenmesi ve sahip olunan yazılımsal ve teknik altyapıların doğru yer ve zamanda kullanılması ile mümkün olabilir (Keser ve Güldüren 2015).

Bilgi güvenliğini bilginin işlendiği, üretildiği, saklandığı her ortamda ve özelliklede kurumsal anlamda sağlamak bir zorunluluktur. Kişisel boyutta bilgi güvenliği önemli olduğu kadar kurumsal anlamda bu bilgi güvenliği çok daha önemlidir. Özellikle de toplumun ve ülkenin menfaatlerini doğrudan etkileyecek olan kritik kurumlarda bilgi güvenliği konusu hayati öneme sahiptir. Bu tip stratejik kamu kurumlarında veya özel şirketlerde çalışan ve özellikle bilginin bulunduğu platformlarda görev yapan personelin bilinçlenmesi kurum veya şirketin bilgi güvenliği konusunda ilerlemesini sağlayacaktır. (Vural ve Sağıroğlu 2008, Gülmüş 2010).

İnsan kaynaklı bilgi ihlallerini bilinçli ve bilinçsiz olarak iki ayrı gurupta incelendiğinde, bilgi ve eğitim eksikliğinden kaynaklı ihlallerin giderilmesi için yukarıda bahsedildiği gibi personelin bilinçlendirilmesi ve çeşitli eğitim programları ile bilgi güvenliği konusunun pekiştirilmesi kullanıcı bazda yeterli olacaktır. Bunun yanında personelin bilinçli olarak yaptığı bilgi ihlallerinin önüne geçilebilmesi için ise özellikle kritik kadrolarda çalıştırılan personelin işe alım sürecinde detaylı arşiv araştırmasının yapılması gerekmektedir. Ayrıca kurum veya şirket içerisinde kontrol mekanizmasının kurulması da önem arz etmektedir.

- **Açık Kaynak İstihbaratı:**

İstihbarat sözcüğü Arapçadaki haber ve bilgi alma anlamına gelen istihbar etme kelimesinden türemiştir. Türk Dil Kurumuna göre ‘‘Yeni öğrenilen bilgiler, haberler, duyumlar, bilgi toplama, haber alma’’ anlamlarına gelmektedir. İstihbarat kelimesinin İngilizce ve Fransızcadaki karşılıkları ise akıl manasına gelmektedir. Kısacası istihbarat alınan bir haber, duyum, ham bilginin çeşitli vasıtalar aracılığıyla işlenmesi, yorumlanması, kıymetlendirilmesi sonucunda ortaya çıkan ürün bilgi olarak tanımlanabilir (Güldiken 2006). İstihbarat her dönem varlığını korumuş ve dönemin teknoloji, şartlarına göre şekillenmiştir. Dünya üzerindeki tüm ülkelerin ekonomik, siyasi, askeri varlıklarını koruyabilmesi ve güçlü bir ülke olabilmesinin arkasındaki en önemli unsur sağlam bir istihbarat ağına sahip olmasına ve bu istihbaratı etkili bir şekilde kullanmasına bağlı olduğu düşünülmektedir (Gül 2015).

Gelişen teknoloji ile birlikte istihbarat faaliyetlerinin de büyük bir bölümü teknolojik alana taşınmıştır. Siber istihbarat olarak tanımlanan bu istihbarat yaklaşımı günümüzde çok önemli bir yer tutmaktadır. Açık kaynak istihbaratı içerisinde ise sosyal medya programlarının takibi bilgi edinme bağlamında en çok başvurulan alanların başında gelmektedir. Dünyada ve ülkemizde sosyal medya programlarını kullanan kişi sayısındaki ciddi artışla birlikte sosyal medya platformları birçok kişi ve kurum için ciddi tehlike oluşturmaktadır.

Küresel çapta araştırmalar yapan We Are Social 2018 raporuna göre dünya nüfusunun %42'si aktif sosyal medya kullanıcısı olduğu Türkiye'de ise nüfusun %63'ünün aktif sosyal medya kullanıcısı olduğu tespit edilen veriler arasındadır. Bu istatistiklerden de anlaşılacağı üzere ülkemizde yoğun bir biçimde kullanılan sosyal medya programları üzerinde yapılan her paylaşımın kişinin siyasi, kültürel, dini vb. görüşlerinin üçüncü şahıslar tarafından görülebileceği, kişinin adresi, çalıştığı kurum vb. alanlar hakkında bilgi sahibi olunabileceği ve açık bir hedef haline gelebileceği bir gerçektir. Bu bağlamda özellikle kritik kurumlarda görev yapan personelin günlük yaşantısı ve iş ortamı ile ilgili tehlike oluşturabilecek bilgileri sosyal medya ortamlarında herkese açık bir şekilde paylaşmaması kişinin ve çalıştığı kurumdaki bilgi güvenliği açısından uygun olacaktır.

2.3.4 Bilgi Güvenliğine Yönelik Tehditler:

Yukarıdaki konu başlıklarında bahsedildiği üzere bir kurum veya kuruluşun sahip olduğu en önemli değer bilgidir. Kurumlar ve hatta ülkeler için en önemli görevlerden biri sahip oldukları bilgiyi korumaktır. Bu anlamda Bilgi güvenliğine yönelik yazılımsal, fiziksel tehditlerin yanında direk bilgi güvenliği tehdidi konusu gündeme gelmiştir. Bu konu hakkında Ocak 2013 yılında TBMM bilişim ve internet araştırma komisyonu (BİAK) tarafından yayınlanan kılavuzda bu konu ayrı bir bölüm olarak incelenmiştir. Kılavuzun ilgili bölümünde anlatılan konu başlıkları özetle aşağıdaki gibidir.

Bilgi güvenliğine yönelik olarak yapılan en büyük tehditlerden biri ağ sistemlerine olan saldırıdır. Ağ sistemleri bilgisayarlar arası haberleşmeyi sağlayan ve genellikle ana bir server üzerinden bağlantılı olduğu bilgisayarlar arasındaki bilgi paylaşımının mümkün olduğu sistemlerdir. Özellikle kurumsal şirketlerde ve kamu kurumlarında dış ağa kapalı olması durumunda hem bilginin aktarımı hem de güvenli olması sebebiyle ağ sistemleri olmazsa olmaz sistemlerden biridir. Ancak bu sistem ağa bağlı durumdaki bir bilgisayara sızılması durumunda tüm bilgisayarlarında tehlike altında olacağından bilgi güvenliği konusunda en büyük tehditlerden biridir. Bu tehdidi "Siber Tehdit", bu alanda yapılan her türlü girişimde "Siber Saldırı", hedef ülke veya kurum için boyutta

ekonomik, psikolojik vb. eylemelerde yapılan her türlü saldırı "Siber Savaş" (Cyber Warfare) olarak adlandırılmaktadır.

Siber saldırılar kurumlara kişilere veya toplumun bir kesimine yönelik gerçekleştirilebilir. Bu tip saldırıların ana amacı hedefe yönelik değerli bilgileri ele geçirmek ve maddi, manevi kazanç sağlamaktır. Kısacası bu tip saldırılar kişisel bilginin gizliliğine yönelik bir tehdittir.

Siber savaş olarak adlandırılan saldırılarda ise hedef devletler veya hedef devlete ait kurumlardır. Genellikle hedef alınan ülkedeki enerji, sağlık, bankacılık faaliyetleri, su, elektrik, internet gibi kritik altyapılara yönelik saldırı gerçekleştirilir ve bu tip kritik altyapıların zarar görmesi hizmet aksaması başta olma üzere birçok felaket zincirini beraberinde getirmektedir. Genel bilgileri kısaca verilen siber saldırılar ve bilgi güvenliğine yönelik tehditleri "Siber Dünya'da Gerçekleşebilecek Saldırılar" ve "Siber Saldırı Çeşitleri" başlıkları altında değerlendirmek mümkündür'' şeklinde açıklanmıştır. Aşağıda bulunan Çizelge 2.2'de siber dünyada gerçekleşebilecek saldırılar ve etki alanları gösterilmiştir.

Çizelge 2.2 Siber Saldırı türleri, kullanım alanları ve sağladığı fayda

Saldırı Türleri	Motivasyon	Hedef Kitle	Metot
Siber Suçlar	Ekonomik Fayda	Kişisel Kullanıcılar, Firmalar	Kullanıcı Bilgilerini Çalma, Sahtekarlık, Şantaj, Saldırı, Güvenlik Açığı Kullanımı, Lisanssız Yazılım Kullanma,
Hactivizim (Siber Korsanlık)	Politik Amaçlar, Kişisel Tatmin	Kurumlar, Devletler	Siber Ortamdaki Saldırı Yöntemlerinin Kullanımı
Siber Casusluk	Ekonomik Fayda ve Kritik Bilgi Kazanımı	Kişisel Kullanıcılar, Kurumlar, Devletler	Güvenlik Açığı, Siber Ortamdaki Saldırı Yöntemlerinin Kullanımı
Siber Terör	Politik Değişiklikler	Devletler	Bilgisayar Tabanlı Şiddet ve Yıkım
Siber Savaş	Politik veya Askeri Fayda	Kişisel Bilgi ve Askeri Sistem Altyapıları,	Siber Ortamdaki Saldırı Yöntemleri

2.4 Bilgi Güvenliği Konusunda Alınabilecek Önlemler

Bilgi güvenliğinin sağlanması konusunda korunacak bilgi varlıklarının seçilmesi, sınıflandırılması ve uygun güvenlik önlemlerinin tespit edilmesi gibi işlemleri en önemli hususlardan biri olmasına rağmen, bu konunun çoğu zaman dikkate alınmadığı bilinmektedir (Henkoğlu 2017).

Bilgi teknolojileri ile bu teknolojileri meydana getiren unsurlar ile bilgiye sahip olmanın ve onu korumanın önemi tam olarak anlaşılmış değildir. Bilginin ne olduğu ona sahip olmanın getirdikleri ve yeterince korunmaması durumunda nasıl bir sonucun ortaya çıkacağı konuları yeterince anlaşılmadığından; bilişim teknolojileri ve bilgi güvenliği konusunda gereken önem gösterilememektedir. Gerekli olan bu özenin gösterilmemesi ilerleyen dönemlerde ciddi sorunlara sebep olabilecek bir durumla karşı karşıya kalınması riskini ortaya çıkaracaktır. Bilginin değerinin olması, bu değeri elde etmek için emek ve zamanın harcanması ve kazanılan bilginin fark yaratması nedeniyle bilgi, korunması gereken bir varlık olarak görülmektedir (Canbek ve Sağıroğlu 2006). Bu çerçeveden bakıldığında öneme sahip bilgilerin güvenliğine yönelik olarak bireysel ve kurumsal boyutta çeşitli önlem ve tedbirler alınması gerekli kılınmıştır.

Bilgi güvenliğinde ana gaye, mevcut bilgilerin izinsiz erişim sağlanmasından, kullanımından, yetkisiz ve ilgisiz kişilere paylaşılmasından, içeriğinde değişiklik yapılmasından, zarar verilmesinden ve yok edilmesinden korunmasıdır. Bilgi güvenliği; bilgilerin gizliliğini, bütünlüğünü ve erişilebilirliğini amaçlamaktadır.

Bilgilerinin bulunduğu dijital ortamlarda bilgi güvenliğinin oluşturulması için özellikle yazılımsal anlamda alınmış önlemlerin ciddi şekilde önem arz ettiği bilinmektedir. Ancak yapılan araştırmalar ve tespitlerin ortaya çıkardığı sonuçlara göre bilgi güvenliğini sağlamanın en doğru yolu bilgi teknolojilerine, onu oluşturan yazılımsal ve donanımsal altyapılarına yüksek maddi bütçe ayırmanın yanında o sistemi kullanan kişilerin farkındalığının oluşması, bilinçlenmesi ve sahip olunan yazılımsal ve donanımsal altyapıların doğru şekilde kullanılması ile mümkün olabilir (Keser ve Güldüren 2015).

2.4.1 Kişisel Boyutta Alınabilecek Önlemler

Bilgi güvenliği konusunda zafiyet oluşturabilecek en zayıf halka insan faktörüdür. Ve bu zafiyetin giderilmesi için ilk yapılması gereken bilgi güvenliği konusunda farkındalığı arttırmak olmalıdır. Kişisel gelişim sürecinde alınan kurs eğitim vb. programlara bilgi güvenliği konusu da eklenebilir. Ayrıca teknolojik gelişmeleri takip etmek ve yenilikler ile ilgili dergi, gazete, internet sayfaları, bloglar vs. takip etmek farkındalık seviyesini yeterli bir boyuta taşıyacaktır. Daha stratejik alanlarda çalışan personellerin ise profesyonel olarak yardım almaları gerekmektedir. Bu çerçevede farkındalık seviyesini arttırmak için çeşitli kavramlara detaya girmeden değineceğiz (Can ve Akbaş 2014, Yılmaz ve Sağıroğlu 2013, Uğuz 2018, Wong *et al.* 1993, Tatar 2011, Mody *et al*. 2018, Henkoğlu 2017, Yavanoğlu vd. 2012).

- **Sosyal Mühendislik**

Çağımızda bilişim ve bilgi güvenliğinin sağlanmasında akla gelen ilk konu olarak sosyal mühendislik kavramı gelmektedir. Bilişim ve bilgi güvenliğine yapılan tehditlerin başında sosyal mühendislik saldırıları mevcuttur. İnsanların çeşitli zafiyetlerinden faydalanılarak farklı ikna ve kandırma taktikleri ile ulaşılmaya çalışılan bilgiyi karşıdaki kişinin haberi olmadan ele geçirme tekniği olarak adlandırılan sosyal mühendislik saldırılarına karşı çok dikkatli olunmalıdır. Sahte hikayeler uydurularak güvenilir bir kişi izlenimi verilir ve hedef kişinin güveni kazanılıp istenilen bilgiye sahip olunur. Bazen çeşitli zararlı yazılımlar vasıtasıyla (Trojanlar/Truva atları) yapılabilir.

- **Oltalama(Phishing)**

Oltalama saldırılarında amaç bilgi elde edilmek istenen hedef kişiye çeşitli güvenilir kaynaklardan geliyormuş izlenimi verilmiş sahte e-postalar gönderilerek gövde metninde bulanan bağlantıya tıklanılması sonucu gerçek gibi gözüken sayfaya yönlendirmesi yapılarak kullanıcı giriş bilgilerinin çalınmasıdır.

Bu saldırıdan korunmanın en temel ilkesi bilinmeyen kaynaklardan gelen e-posta ve e-posta eklerini kesinlikle açmamaktır. Ayrıca yönlendirme yapılan sayfalarda hiçbir bankanın veya herhangi bir kurumun istemeyeceği bilgilerin girişi yapılmamalıdır. Çünkü bilinmelidir ki e-posta yoluyla kişisel bilgi talebi olmaz. Dikkat edilmesi gereken bir diğer husus da Web sayfalarının sol üst bölümünde yer alan kilit işaretinin mevcut olmasıdır. Bu işaret güvenli bir sayfada işlem yapıldığını belirtir.

- **Şifre/Parola Güvenliği**

Bilişim sistemlerindeki bilgi güvenliğinin en mühim konularından biri yüksek güvenlikli şifre/parola oluşturmaktır. Kimlik doğrulama yöntemlerinden en genel kullanım alanına sahip parolalar ne kadar güçlü olursa tahmin edilmesi ve deneme yanılma yoluyla tespit edilmesi imkânsız boyutlara ulaşabilir. Büyük ve küçük harfler, rakamlar ve aynı zamanda özel karakterler kullanılarak en az 8 adet karakterden oluşan parolalar güçlü olarak nitelenebilir. Fakat bir parolanın güçlü olması sadece onun karakter komplikesinden oluşmaz. Kullanıcının da bu parolayı kimseye söylememesi ve başka kişilerin ulaşabileceği yerlere yazılmamış olması gerekmektedir. Ayrıca tüm sistemlerden tek bir parola kullanmak yerine her bir sistem için farklı bir parola kullanmak daha etkili ve güvenlikli olacaktır.

- **Sosyal Medya Platformlarının Kullanımı**

İnternet alanında yaşanan gelişmeler ve etkileşimli web olarak adlandırılan web 2.0'ın gelişmesi ile birlikte Özellikle son dönemlerde mobil cihazlardaki imkân ve olanakların gelişim göstermesiyle birden fazla sosyal medya hesabına sahip kişi sayısı ciddi şeklide artış göstermiştir. Teknolojinin her alanında olduğu gibi sosyal medyada da artış gösteren kullanım beraberinde tehlikeli boyutları da taşımaktadır. İletişim kolaylığı sağlayan bu mecralar art niyetli kişilerin çeşitli yöntemleriyle kişisel bilgi güvenliğine tehditler barındırmaktadır. Özellikle kötü niyetli kişiler tarafından ilk bakışta hedef şahsa ait ad, soyad, yaşadığı şehir, cep telefonu numarası, anne kızlık soyadı gibi profil bilgilerine çok rahat ulaşabilmektedir. Bunun yanında gittiğimiz yerler ve konum bilgilerimizde kötü niyetli şahıslar tarafından ele geçirilebilecek bilgiler arasındadır.

Sosyal medya platformları güvenlik güçlerinde çalışan personel içinde ciddi tehlikeler oluşturmakta ve personel tespit edilmesi halinde direk hedef haline gelebilmektedir.

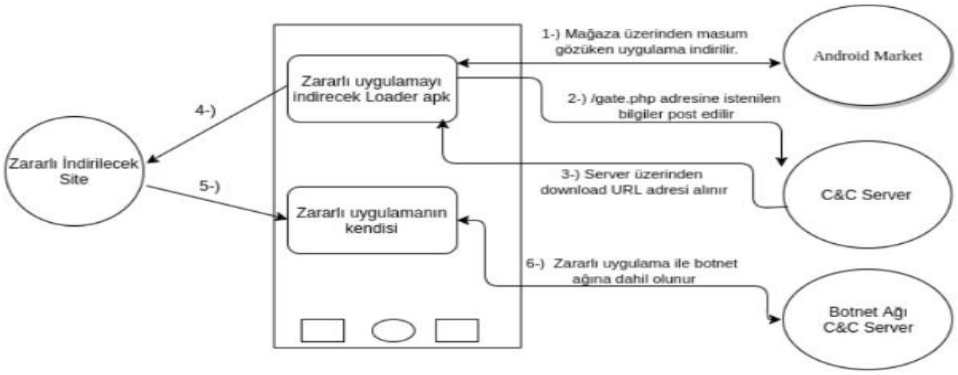
Sosyal medya platformlarının servis sağlayıcı şirketleri güvenlik politikalarını geliştirmeli ve bilgi güvenliği risklerine karşı kişisel verilerin korunmasına yönelikte yayın ve güvenlik politikalarını geliştirmeleri önem arz etmektedir. Ancak servis sağlayıcıların kişisel verileri koruma altına almasını beklemeden kişisel olarak bazı basit önlemlerle kişisel verilerini koruma altına alabilmesi mümkündür. Sosyal medya platformlarını kullananların kişisel boyutta alınabilecek önlemlerin başında güçlü parolalar, tanınmayan kişilerden gelen talepleri kabul etmeme, hesapların gizlilik ayarlarına önem gösterme, özellikle herkese açık paylaşımlarda gizlilik içeren bilgileri bulundurmama vb. gelmektedir. Güvenlik güçlerinde çalışan personel için üniformalı resimlerin paylaşılmaması, bulunduğu yerlerde konum bilgilerini paylaşmaması vb. önlemler alınabilir.

- **Cihaz Güvenliği (Bilgisayar/Telefon/Tablet)**

Teknolojik çağın büyümesiyle ve ucuzlamasıyla artık herkesin kişisel bilgisayarı, akıllı telefonu ya da tableti veya bunlardan birden fazlası bulunmaktadır. Kullanımı yaygınlaşan bu cihazlar dijital dünyanın tehlikesini de beraberinde getirmektedir. Bu cihazlar kişisel bilgiler barındırmaları sebebiyle ekstra güvenlik önlemi alınmasını gerekli kılmaktadır. İçerlerinde bulunan mevcut güvenlik yazılımları tek başlarına bilgi güvenliğini sağlamada yeterli değildir. Kullanıcılarında ilave önlemler alması gerekir.
Bunların başında cihazı açmak için kullanılan güçlü bir parola gelir. Kurulum ve diğer aşamalarda yapılması gereken temel güvenlik ayarlarının özenli yapılması da önem taşımaktadır. İndirilecek uygulamaların kaynağının güvenli olup olmadığına dikkat edilmelidir. Güvenlik güncellemeleri zamanında yapılmalıdır. Şifresiz ve herkesin kullanımına açık kablosuz ağlar tercih edilmemelidir.

Günümüzde mobil cihazların teknolojinin gelişimi ile birlikte göstermiş oldukları etkileşim ortadadır. Öyle ki akıllı telefonlardan her türlü işlemin yapılması ve uygulamalar üzerindeki kolaylıklar kişilerin internet, bankacılık, haberleşme, oyun vb.

işlemlerini yaparken akıllı telefonlarını daha çok tercih etmesine sebep olmaktadır. Mobil telefonlara yüklenen uygulamalar cep telefonundaki rehber, SMS, dosyalar, fotoğraflar, videolar vb. birçok alana ulaşım sağlamaktadır. Mobil cihazlara indirilen uygulamaların cep telefonu üzerinde birçok alana ulaşabilmesi kötü niyetli kişilerin iştahının kabartmıştır. Masum gibi görülen birçok uygulama arka planda barındırdıkları zararlı kodlarla mobil cihazlara nüfus etmekte ve kişilerin özel bilgilerini kayıtlı şifrelerini üçüncü şahısların eline geçmesine imkân tanımaktadır Aşağıdaki şekilde android tabanlı yazılan virüs ve benzeri zararlı yazılımların cihazlara bulaşma aşamaları gösterilmektedir.



Şekil 2.3 Android Tabanlı Zararlı Yazılımların Cihazlara Nüfus Etme Aşamaları (Ceylan 2018).

Android market üzerinde aynı zararlı yazılım bile farklı uygulamalar arkasına saklanarak ve yeni yöntemler geliştirerek mağaza üzerindeki yaşam döngüsüne devam edebilmektedir. 2017 yılında 700.000'den fazla android uygulama zararlı olduğu gerekçesi ile mağazadan kaldırılmıştır (Ceylan 2018). Durum böyle iken güvenilir olduğunu düşündüğümüz ve özellikle kurumsal şirketlere ait uygulamalar haricinde hiçbir uygulamayı mobil cihazımıza indirmemeli ve uygulamaların mobil cihaza inerken istemiş oldukları izinlere dikkat etmekte fayda vardır.

2.4.2 Kurumsal Boyutta Alınabilecek Önlemler

Kurumların sahip oldukları varlıklardan en önceliklisi bilgidir. Bilgi, sözlü, yazılı veya dijital ortamlarda bulunabilir. Çağımızdaki teknolojik gelişmeler sebebiyle sahip olunan

bilgilerin güvenliğinin sağlanması kurumun geleceği açısından artık ciddi manada stratejik önem arz etmektedir.

Günümüzde kurumların sistemlerinde barındırdıkları bilgilerinin dijital ortamlarda bulundurmaları, bu bilgilerin güvenliğini tehlikeli duruma düşürmüştür. Çeşitli siber saldırı teknikeriyle kurumlara ait bilgilerinin çalınması, yok edilmesi, ortaya çıkması ve kötü niyetli kişilerin eline geçmesi ne yazık ki artık çok daha kolay olabiliyor. Bu durum oluşabilecek kötü sonuçları itibariyle kurumlar için güvenlik zafiyeti oluşturabilir ve itibar kaybına sebep olabilir. Bu sebeple kurumların bilgi güvenliği konusuna ivedilikle önem vermeleri gerekmektedir. Ayrıca oluşabilecek sorunların önceden tespiti ve giderilmesi amacıyla ciddi önlemler almak ve yüksek miktarlarda bütçeler ayırmak zorundalar (Odabaş, 2003).

Kurumların bilgi güvenliği risklerini ortadan kaldırma bakımından yapacakları çalışma ilk olarak tutarlı bir politika geliştirilmesi olmalıdır. Bu politikanın, kurumun bilgi güvenliğini tüm detaylarıyla kapsayacak hususları içermesi ve özellikle yeni oluşabilecek tehditlere karşı sürekli güncellenebilir yapıda olması gerekir.

Kurum çalışanlarının ve ziyaretçilerinin kurumun hangi bölümlerine ulaşabileceğinin belirlenmesi, yetkisiz ve sorumsuz kişilerin bilişim ve bilgi sistemleri donanımlarının bulunduğu güvenlikli bölge olarak belirlenmiş alanlara ulaşmalarının ve erişimlerinin engellenmesi ya da çeşitli tedbirlerle kısıtlama getirilmesi ayrıca önem taşımaktadır. Özellikle bilişim konularında teknik destek hizmeti alınan kurum dışı ekiplere karşı dikkatli olunması gerekmektedir (Gülmüş, 2010).

Yetkisiz kişilerin kurum bilgilerine izinsiz erişimini önlemek bakımından kurum bilgisayar ağlarına kötü niyetli yazılımların (mallware/virüs) sokulmasını engelleyecek tedbirlerin alınması ve kurum personeli ya da başka kişilerin harici bellek, CD/DVD' ye kopyalama gibi yöntemlerle kurum bilgilerini dışarıya çıkarmasını önleyecek gerekli tedbirlerin oluşturulması ciddi önem arz etmektedir.

Kurum personelinin iş amaçlı kullanmakta olduğu her türlü dijital materyale erişiminde uygun şekilde oluşturulmuş kırılması ve tahmin edilmesi zor komplike şifreleri kullanabilecek ve bilgileri içeren sistemlere erişim yapan ve giriş sağlayan herkesin dijital ortamlarda izlenebildiği yazılımlar destek alınmalıdır. Bu sayede hangi personelin ne zaman hangi veriye ulaştığının tespiti yapılan kontroller ve incelemeler sonucu ortaya çıkar. Ayrıca tüm bilişim ve bilgi sistemlerinin belirli periyotlarla dışarıdan ve içerden sızma/güvenlik açığı yakalama testleriyle düzenli olarak denemelere tabi tutularak olası saldırı veya olumsuz durumların önüne geçilmesi amaçlanmalıdır.

Her ne kadar dijital tehlikeler olabileceği gibi fiziksel açıdan da bilgilerin güvenliğini tehlikeye düşürecek durumlar oluşabilir. Bunlara örnek deprem, yangın, su baskını, elektronik arıza sonucu sistemlerin tamiri mümkün olmayan bozulmaları vb. olarak verilebilir. Bu gibi durumların önceden öngörülerek çeşitli tedbirlerle zararlarını ortadan kaldırmaya ya da en aza indirmeye çalışılabilir. Bazı kamu kurumlarında uygulandığı gibi önemli bilgi ve belgelerin bulunduğu alanlar sınıflandırılarak belli bir yerde saklanmalı ve örneğin yangında ilk önce kurtarılacaktır vb. uyarılarla olağanüstü durumlarda kurtarma öncelikleri alınabilir (Özcan, 2009).

ISO/IEC 27002:2017 kalite standartlarında da yer alan temiz masa/ekran kuralına benzer politikalar oluşturulmalı, mesai saatleri dışında veya kullanıcının çalışma odasında bulunmadığı durumlarda masa üzerinde ve/veya bilgisayar ekranında bilgi güvenliğini ihlal edecek belge, doküman vb. materyalleri bırakmamalıdır. Personeller bu konuda bilinçlendirilmeli ve gerekli takibinin yapılması gerekmektedir (Akyol, 2013).

Kamu kurumlarında atılması gereken bir diğer adım ise günümüz dünyasında kabul edilmiş Bilgi Güvenliği Yönetim Standardı olan ISO (The International Organization for Standardization) ve IEC (The Electrotechnical Commission) kuruluşlarının ortak bir çalışması sonucu yayınlanan ISO/IEC 27002:2017 bilgi teknolojisi-güvenlik teknikleri-bilgi güvenliği kontrolleri için uygulama prensiplerine uyumluluğun sağlanması olmalıdır. Bu standart amacı itibariyle kurumlarda bilişim ve bilgi güvenliği yönetim

sisteminin oluşturulması ve bu yönetim sisteminin sağlıklı bir biçimde devamının sağlanması için kontrol maddelerinin verilmesidir. Bahse konu kontrol maddeleri sistemin işleyişi ile ilgili nasıl sorusuna fazla detaylandırmadan yanıtlar vermektedirler. Fakat kurumların hareket tarzları konusunda kendi kararlarını kendileri almaları için yönlendirme yapmamaktadır. Bu standardın en önemli avantajlarında biri de risk analizleri yapılarak eksikliklerin tespiti ve giderilmeleri aşamalarında sağladığı katkıdır (Aslandağ 2010).

2.5 Bilgi Güvenliğine Yönelik Yapılan Çalışmalar

Yılmaz ve Ezin (2017), Ebeveynlerin bilgi güvenliği farkındalıklarının incelenmesi üzerine yapmış oldukları çalışma neticesinde ebeveynlerin belli bir seviyede bilgi güvenliği farkındalığı olduğu fakat bazı spesifik (depolama yerleri, depolama süreleri vs.) konularda farkındalık seviyelerinin yetersiz olduğu sonucuna varmıştır. Ayrıca Ebeveynlerin çocuklarına bilgi güvenliği konusunda uyarıdan başka somut bir bilgi veremedikleri sonuçlarına ulaşmışlardır.

Çek (2017), kurumsal bilgi güvenliği ve bilgi güvenliğinde insan faktörünün önemi ile ilgili yapmış olduğu yüksek lisans tezinde bilgi ve bilgi güvenliği ile ilgili çeşitli kavramları açıklayarak kişisel boyutta bilgi güvenliğinin önemi ve bilgi güvenliğinin sağlanması için alınabilecek önlemleri sıralamıştır.

Erdoğmuş (2017), üniversite öğrencilerinin bilgi güvenliği kazanımlarının farkındalıkları üzerindeki etkilerini belirlemek amacıyla bir anket çalışması yapmış ve öğrencilerin bilgi güvenliği farkındalıkları, internet güvenliği, sosyal medya kullanımı, ağ güvenliği, şifre oluşturma ve sosyal medya tuzakları olmak üzere 5 alt boyutta çıktığı anlaşılmıştır.

Başdinkçi (2017), sağlık kurumlarında bilgi güvenliği risk değerlendirilmesi üzerine yapmış olduğu çalışmada, katılımcılara göre en önemli risk faktörlerinin hasta bilgilerinin sızdırılması, şifrenin paylaşılması, kötü niyet, veri güvenliğinin sağlanamaması ve lisanssız yazılım kullanımı olduğu sonucuna varılmıştır.

Henkoğlu (2017), Kişisel veri güvenliği ve bilgi güvenliği konusunda yapmış olduğu değerlendirme çalışmasında, bilgi güvenliği konusunda uygulamada yapılan yanlışlar ve bu konuda ki sorumlulukların neler olduğu, teknik ve hukuki boyutu, uygulamadaki risklerin neler olduğu konularında bir çalışma yapmıştır.

Yılmaz vd. (2016), öğretmenlerin dijital veri güvenliği farkındalığını ölçmek amacıyla bir çalışma yapmışlardır. Çalışma sonucunda öğretmenlerin dijital veri güvenliğinin çok yüksek seviyede olduğu, farkındalık değerlerinin cinsiyet, kullanım sıklığı, elektronik cihaz çeşitliliği durumlarına göre değiştiği görülmüştür.

Keser ve Güldüren (2015), yükseköğretim kurumlarında çalışan öğretim elemanlarının bilgi güvenliği farkındalığını belirlemek maksadıyla bir ölçek geliştirmişlerdir. Yapılan testler sonucunda yükseköğretim kurumlarında çalışan öğretim görevlilerinin bilgi güvenliği farkındalığını ortaya koyacak genel geçerlilik görmüş bir ölçek geliştirmişlerdir.

Karadağ ve Abuhanoğlu (2015), bilgi güvenliği farkındalık seviyesini belirlemek amacı ile Gülhane Askeri Tıp Fakültesi Eğitim Hastanesi çalışanlarına yönelik bir çalışma gerçekleştirmişlerdir. Çalışmada farkındalık düzeyi ile çeşitli değişkenler arasında anlamlı bir fark olup olmadığı araştırılmış olup sonucunda yaş ve unvan durumunun farkındalık seviyesi üzerinde anlamlı bir ilişki olduğunu ortaya koymuşlardır.

Akgün ve Topal (2015), eğitim fakültelerinde öğrenim gören öğrencilerin bilgi güvenliği seviyelerinin tespit etmek maksadıyla bir çalışma yapmışlardır. Çalışma sonucunda bilgi güvenliği seviyesinin yeterli olmadığı durumu ortaya çıkmıştır. Bilgi güvenliği ile ilgili eğitim alan katılımcılar ile almayanlar arasında ciddi bir fark olduğu sonuçlarına ulaşmışlardır.

Çetin (2014), kişisel bilgi güvenliği ile bilgi güvenliği farkındalık seviyelerini araştırmak maksadıyla literatür taraması ve yüz yüze görüşmeler sonucunda ‘’Kişisel Veri Güvenliği Farkındalığı’’ anketi geliştirmiştir. Anket uygulaması sonucunda katılımcıların kişisel bilgi güvenliği seviyelerinin ortalama seviyenin üzerinde olduğu

ve verilerin paylaşımı konusunun diğer ölçek maddeleri arasında en yüksek olduğu sonucuna ulaşmıştır.

Can ve Akbaş (2014), yapmış oldukları çalışmada kurumsal ağ ve sistem güvenlik politikalarının oluşturulması ve olası bir siber saldırı durumunda uygulanacak güvenlik politikalarının neler olabileceği konusunu açıklamışlardır.

Baykara vd. (2013) bilgi güvenliği sistemlerinde kullanılan araçların incelenmesi üzerine yapmış oldukları çalışmada NMAP, NESSUS, WİRESHARK, TCPDUMP, SNORT vb. bazı bilgi güvenliği sağlayan araçların işleyişleri üzerine bir çalışma yapmışlardır.

Yılmaz ve Sağıroğlu (2013), siber güvenlik alanında kullanılabilecek evrensel kaideler, siber kaynakların risk analizi, siber saldırı durumunda karşılık seviyesinin ne durumda olduğu ve saldırı araçları üzerine bir inceleme ve analiz sunmuşlardır.

Akyol (2013), COBİT gibi iç denetim sistemi uygulayan şirketlerdeki bilgi güvenliği politikalarının şirket, personel ve süreçlere olan etkilerinin araştırmak maksadıyla anket çalışması yapmıştır. Çalışan performansının bilgi, eğilim ve farkındalık kavramları ile pozitif bir ilişki içerisinde olduğu sonucuna ulaşılmıştır.

Demirtaş (2013), bilgi güvenliği yönetiminin gerekliliği üzerine yapmış olduğu çalışmada, bilgi güvenliği sisteminin başarı dayanaklarını değerlendirerek, bilgi güvenliği yönetiminin performansını etkileyen faktörleri ortaya çıkarmayı hedeflemiştir.

Henkoğlu ve Yılmaz (2013), Avrupa Birliği (AB) bilgi güvenliği politikaları ile ilgili yapmış oldukları çalışmada, AB bilgi güvenliği politikalarını belirleyen etmenlerin neler olduğu, nasıl uygulandıklarının değerlendirilmesini yapmışlardır.

Yavanoğlu vd. (2012), yapmış oldukları çalışmada sık kullanılan sosyal paylaşım sitelerini incelemiş, bu ortamlarda karşılaşılan güvenlik ihlallerini örneklendirerek bilgi güvenliği bağlamında alınabilecek önlemleri sıralamışlardır.

Şahinaslan vd. (2009), kurumlarda uygulanabilecek bilgi güvenliği eğitimi üzerine bir çalışma yapmışlardır. Çalışma sonucunda; çalışanları eğitmek maksadıyla etkili farkındalık programlarının oluşturulması, teknolojik önlemlerin alınması, kontrol mekanizmasının geliştirilmesi gibi sonuçlara ulaşmışlardır.

Eminağaoğlu ve Gökşen (2009), bilgi güvenliği alanında Türkiye'de ve dünyadaki mevcut durumu araştırmış ve bu alanda yapılan ortak yanlışları tespit ederek kısa ve uzun vadede kişisel ve kurumsal boyutta ne gibi önlemler alınabileceği üzerine bir çalışma yapmışlardır.

Yılmaz (2009), bilgi yönetimi ile enformasyon yönetimi kavramlarını içerik bakımından incelemiş ve bu iki kavram arasındaki farkları ortaya koymaya çalışmıştır.

Vural ve Sağıroğlu (2008), kurumsal anlamda oluşturulabilecek bilgi güvenliği alanında yapmış oldukları inceme çalışmasında, bilgi güvenliği seviyesinin en üst düzeye çıkarılabilmesi için bilgi güvenliği standartlarının ve bu alanlardaki güncel teknolojik gelişmelerin takip edilmesinin önemli olduğu ayrıca, bağımsız uzman kuruluşlarca denetlenmesi gerektiği, BGYS standartlarının uygulanması gerektiği sonuçlarına ulaşmışlardır.

Canbek ve Sağıroğlu (2006), bilgi güvenliği ve onu oluşturan unsurlar üzerine yapmış oldukları çalışmada, güvenlik unsurları, güvenlik süreçleri gibi 2 ana alt başlık altında bilgi güvenliği ve süreçlerinin incelemişlerdir.

Güçlü ve Sotirofski (2006), Bilgi yönetimi üzerine yapılmış olan bu çalışmada bilgi güvenliği konusunun temelini oluşturan bilgi kavramı ve bilgi çeşitleri incelenmiş, bilgi yönetimi süreci ve bu sürecin basamaklarını açıklanarak eğitim örgütlerine uygulanabilirliği araştırılmıştır.

2.6 Bilgi Güvenliği İle İlgili Yapılan Hukuki Düzenlemeler

Bilişim ve Bilgi Güvenliği kavramı genel anlamda sözlü ve yazılı bilgileri ya da dijital ve elektronik ortam gibi farklı mecralardaki bilgilerin gizlilik, erişebilirlik ve bütünlük açısından güvence altına alınması ve bu durumun devamında sürekliliğinin sağlanmasıdır.

Bilgi güvenliği; özellikle ellerinde veri bulunduran özel ya da resmi kurumlar veya kişisel anlamda her türlü bilgiye sahip kimseler açısından öncelikli korunması gereken bir alan oluşturmaktadır. Durmaksızın gelişen teknoloji ile birlikte kötü niyetli kişiler veya oluşumlar özellikle değerli bilgiye sahip kişi ya da kurumlara saldırarak bilgi hırsızlığı ile kendilerine fayda sağlamaya çalışmaktadırlar. Bu çerçevede kurumlar ya da kişiler ellerinden geldiğince mevcut tehlikeden kendilerini korumak için çeşitli önlemler almaktadırlar. Kişi ya da kurumların tek başlarına çabaları kötü niyetlilerin davranışlarını engellemeye yetebilir fakat yaptırım niteliği taşımaz ve tekrar oluşmasını engellemeye yetmez. Burada devreye Devletlerin kanunları ve düzenlemeleri girmektedir. Konu ile ilgili çeşitli kanun, yönetmelik ve diğer hukuki düzenlemeler ile bu alanda hizmet veren kurum ve kuruluşlar aşağıda sunulmuştur (Avşar ve Öngören 2010, Uçak ve Henkoğlu 2010, Koç ve Kaynak 2009, Dülger 2018, İnt.Kyn.4).

- **Türkiye Cumhuriyeti Anayasası**

Bilişim ve Bilgi Güvenliği konusunda hukuki manada bir değerlendirme yapıldığında Türkiye Cumhuriyeti Anayasası'nın bu konuya ana hatlarıyla değindiği görülmektedir.
T.C. Anayasası'nın 20. Maddesi (Ek fıkra: 12/9/2010-5982/2 md.) gereğince;
"Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir" şeklindedir.

- **5237 sayılı Türk Ceza Kanunu**

Türk Ceza Kanunu'nun onuncu bölümü bilişim alanında suçlar başlığı altında 243, 244 ve 245. maddeleri genel olarak bilgi güvenliğin sağlanması ve bu yollarla işlene suçlar ve yaptırımları ile ilgili konularda çeşitli düzenlemeler getirerek koruma altına almayı amaçlamıştır. TCK 243. madde ile bir bilişim sisteminin bütününe veya belli bir kısmına hukuka aykırı olarak giren ve orada kamaya devam eden ile bir bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakillerini sisteme girmeksizin teknik araçlar ile hukuka aykırı izleyen kişinin karşılaşacağı yaptırımlar, TCK 244. Madde ile bir bilişim sisteminin işleyişini engelleyen, sistemdeki verileri bozan yok eden, değiştiren, erişilmez kılan kişiler ile ilgili yaptırımlar, TCK madde 245 ile ise banka bilgileri ve kredi kartları ile ilgili sahibinin rızası olmaksızın ele geçiren ve kullanan kişilerin karşılaşacağı yaptırımlar ve cezanın arttırılma biçimlerini düzenlemektedir.

- **5070 sayılı Elektronik İmza Kanunu**

Elektronik imza 5070 sayılı kanunda belirtildiği üzere ''Başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veri'' diye tanımlanmaktadır. Tanımdan anlaşılacağı gibi elektronik imza bir nevi kişinin kimliği gibidir. Kanunun beşinci maddesinde bu durum '' elektronik imza el ile atılan imza gibidir'' şeklinde belirtilmiştir. Bu Kanun ile elektronik imzanın hukuki ve teknik yönleri ele alınarak kullanan ve sertifika sağlayıcıların durumları ile ihlal durumunda karşılaşacağı yaptırımlar ele alınmıştır.

- **5651 sayılı Internet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun**

Bu kanun ile Türk Ceza Kanunu'nda yer alan bilişim suçlarının yanı sıra internet ortamındaki içeriklerin düzenlenmelerine yer verilmiştir.5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun da yer verilmiştir. Bu kanun 2007 yılında

yasalaşmıştır. Kanunla ile ilk defa internetteki katalog suçlar kapsamındaki yasal olmayan içerik ile ilgili erişimin engellenmesi şeklindeki mücadele esas ve usulleri düzenlenmiş ve internet hizmeti veren internet hizmeti veren içerik, yer ve erişim sağlayıcılara da belli başlı yükümlülük ve sorumluluklar getirilmiştir.

Bu kanunda düzenlenmiş katalog suçlara ilişkin; "Bilgi Teknolojileri ve İletişim Kurumu Bilgi ve İhbar Merkezi"; vatandaşların bahse konu suçlara ilişkin şikâyetlerini iletebilecekleri müracaat merkezi olarak kurulmuştur. 23.11.2007 tarihinde faaliyete geçen bu merkeze "http://www.ihbarweb.org.tr" adlı web sitesinden yasal olmayan içeriğe ilişkin ihbarda bulunula bilinmektedir. Kanun kapsamında ayrıca vatandaşlara dijital ortamında özel hayatın gizliliği ve kişilik haklarının ihlali ile ilgili olarak başvuru hakları tanımlanmıştır.

- **6698 sayılı Kişisel Verilerin Korunması Kanunu**

24 Mart 2016 tarihinde yasalaşarak yürürlüğe giren bu kanunun en genel tanımlamada amacı kişisel verilerin işlenmesinde kişi haklarını güvence altına almaktır. Kişisel Verilerin Korunması Kanunu; kişisel veriler kayda alınırken Anayasa tarafından belirlenmiş temel hak ve özgürlükleri korumayı, özel hayatın gizliliğine riayet etmeyi ve ayrıca kişisel verileri kayda alan veya işleyen tüzel ve gerçek kişilerin uyacakları esas ve usullerle yükümlülüklerini belirlemeyi ve düzenlemeyi amaç edinmiştir.

- **5809 sayılı Elektronik Haberleşme Kanunu**

Bilgi güvenliği açısından değerlendirilmesi ve bahsedilmesi gereken bir diğer kanun 5809 sayılı Elektronik Haberleşme Kanunudur. Elektronik haberleşme sektörüne çeşitli bilgi güvenliği konusunda çeşitli düzenlemeler getirmiştir. 12.Madde kişisel verilerin gizliliği ve korunması, yetkisiz ve izinsiz erişimi engelleyici tedbirlerin alınması ile ilgili kurumların yükümlülüklerini içeren düzenlemelere değinmektedir. 51.Madde kişisel verilerin insan hakları evrensel değerlerine uygun bir şekilde; ihtiyaç hasıl olduğunda ulaşılabilir, güncel, doğru ve iyi niyetli amaçlar doğrultusunda işlenmesi, mevcut durumun gerektirdiği ölçüde sınırlı olacak biçimde kayda alınması ve

korunmasını gerektiriyor. Ayrıca özel hayatın gizliliğinde haberleşme hürriyetine dair bilgi güvenliği konusunda çeşitli düzenlemeleri de barındırmaktadır.

- **5411 sayılı Ulusal Bilişim Güvenliği Kanun Taslağı**

Amacı, Devletin bilgi güvenliği konusundaki faaliyetlerinin geliştirilmesi ve bunu gerçekleştirmeye yönelik her türlü çalışmaların yapılması, kritik bilişim sistemlerine yapılabilecek saldırılara karşı çeşitli güvenlik önlemlerini almak ve bu hususlardaki usul ve esasları belirlemek olan bu kanun taslağı çalışmaları 2012 yılının başından itibaren devam etmektedir.

- **5411 Sayılı Bankacılık Kanunu**

5411 sayılı Bankacılık Kanunu; Bankacılık sektörüne düzenlemeler getiren en önemli kanunlardan biridir. Bilgi güvenliği ile ilgili olarak Bankacılık Kanununun 73. Maddesi; banka müşterisi ve bankacılık sırrı kapsamında bulunan tüm bilgilerin bankalar tarafından korunması, ifşa edilmemesi, açıklanmaması ve saklanması konularını düzenlemektedir.

- **Avrupa Konseyi Siber Suç Sözleşmesi**

Avrupa'da siber suçlarla ilgili olarak düzenlenmiş ilk belge niteliğini taşıyan ve amacı uluslararası alanda siber suçlarla etkili bir biçimde mücadele etmek ve bu suçlara karşı ortak bir duruş göstermek olan Avrupa Konseyi Siber Suç Sözleşmesi'ni 39'u Avrupa Konseyi üyesi ve Avrupa Konseyi dışından Japonya, Kanada, ABD ve Güney Afrika olmak üzere toplamda 43 ülke birleşerek imzalamıştır. Türkiye de 10 Kasım 2010 tarihinde Dışişleri Bakanlığı seviyesinde imzalamıştır. Uluslararası bir antlaşma ve tüm kanunların üzerinde işlem görecek olan bu belgede; özellikle telif haklarının ihlalleri, bilgisayarlarla ilişkili sahtekârlık eylemleri ve network güvenliği ihlaline ilişkin suçlar tanımlanmakta, cezai soruşturma ve kovuşturma yöntemleri belirlenmektedir.

Türkiye'de Bilgi Güvenliğine Yönelik Oluşturulan Kurum ve Kuruluşlar

Ülkemizde bilgi güvenliğine yönelik yapılan hukuki düzenlemelerin yanında bilgi güvenliği konusunda toplumu ve kişileri bilinçlendirmeyi amaçlayan, ülke çıkarlarına yönelik çözüm önerileri sunan ve bilgi güvenliğini koruma altına almayı hedefleyen bazı çalışmalarda yapılmaktadır. Bunlardan bazıları aşağıda verilmiştir.

- **Siber Güvenlik Eğitim Portalı**

Siber güvenlik eğitim portalı olarak hizmet veren site, Kalkınma Bakanlığı işbirliği ile TÜBİTAK-BİLGEM Siber Güvenlik Enstitüsü bünyesinde Siber Güvenlik Eğitim ve Araştırma Merkezi Projesi, Siber Güvenlik Eğitim Altyapısı bölümlerinden oluşmaktadır. Siber Güvenlik Eğitim Portali ile; bireylerin bilgi güvenliğine yönelik farkındalıklarının oluşması, üniversite öğrencilerinin bu konuda gerekli teknik altyapıyı elde etmelerinin sağlanması, profesyonel olarak bilgi güvenliği ve siber güvenlik alanlarında faaliyet yürüten kişilerin ve kurumların yeteneklerinin arttırılması maksadıyla çevrimiçi eğitim sunulması gerçekleştirilmektedir.

- **TÜBİTAK – BİLGEM – Siber Güvenlik Enstitüsü (SGE)**

Bu enstitü siber güvenlik alanında gerekli gerekli bilimsel altyapının sağlanması ve araştırma alanlarının oluşturulmasını, ülke genelinde yürütülen siber güvenlik faaliyetlerde gerekli teknik altyapıyı oluşturma ve kurumlara destek olabilecek önerilerde bulunmayı, ülkemizde bulunan kritik tesis ve altyapılar ile ilgili siber güvenliğin sağlanmasında gerekli desteği sağlamak amaçlarında faaliyetlerine devam etmektedir.

- **Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE)**

TÜBİTAK tarafından oluşturulan ve gerekli çalışmaların bu kurum tarafından yürütüldüğü Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü ülkemizdeki kamu kurumlarının ve özellikle stratejik öneme sahip kurumların sahip oldukları bilgiyi

korumaya yönelik projeler geliştirerek bu projelerin hayata geçmesine destek sağlayan önemli bir kuruluştur. UEKAE aynı zamanda teknolojik olarak bilgi güvenliğini sağlayan tüm elektronik cihazların tasarlanması ve kurulumuna kadar geçen sürede çeşitli çalışmalar yürüten ve Türkiye'nin bu alandaki önemli bir AR-GE kuruluşudur.

- **TR-BOME Bilgisayar Olaylarına Müdahale Ekibi**

TÜBİTAK UEKAE bünyesinde faaliyet gösteren bilgisayar olaylarına müdahale ekipleri tüm Türkiye'de faaliyet yürütürler. Ülke genelinde özellikle kamu olmak üzere tüm kurum ve kuruluşlardaki bilgisayar olaylarına müdahale etmek ve müdahale edebilme yeteneği kazandırmak üzere kurulmuştur. Genel olarak kurumlarda siber olay durumunda müdahale yöntemlerini alınması gereken önlemleri vb. birçok konuda kamu kurum ve kuruluşlarını bilinçlendirmek amacıyla kurulmuştur.

3. MATERYAL ve METOT

Bu araştırmanın evreni, Siirt İl merkezindeki İl Jandarma Komutanlığı ve İl Emniyet Müdürlüğünde görev yapan jandarma ve polislerden oluşmaktadır. Çalışmada zaman ve maliyet vb. nedenlerden dolayı örneklem alınma yoluna gidilmiş olup tabakalı tesadüfi örnekleme yöntemi ile seçilen 207 jandarma ve 197 polis olmak üzere toplam 404 personel araştırmanın örneklem grubunu oluşturmaktadır.

Çalışmada veri toplama tekniği olarak anket kullanılmıştır. Söz konusu anket temel olarak 2 bölümden oluşmaktadır. Anketin birinci bölümünde emniyet personelinin sosyo-demografik ve diğer bazı bireysel özelliklerini belirlemek üzere 11 adet kapalı uçlu soruya (mesleği, cinsiyet, medeni durum, yaş, eğitim düzeyleri, kıdem, çalıştıkları birim, unvan, sahip oldukları cihazlar, internete bağlanılan cihazlar, bilgisayar ve bilgi güvenliği seviyeleri) yer verilmiş olup anketin ikinci bölümünde ise Keser ve Güldüren (2015) tarafından geliştirilen 2 boyut (saldırı ve tehditler; kişisel verileri koruma) ve 34 maddeden oluşan bilgi güvenliği farkındalığı ölçeğine yer verilmiştir (Ek-1). Ölçekte yer alan her bir madde 5'li Likert tipi derecelendirmeye tabi tutulmuş olup 1= Hiç katılmıyorum ve 5= Tamamen katılıyorum aralığında puanlandırılmıştır.

Veriler SPSS 18.0 for Windows paket programı ile analiz edilmiş olup emniyet personelinin sosyo-demografik ve diğer bazı bireysel özellikleri frekans ve yüzde dağılımı ile sunulmuştur. Diğer taraftan ölçekteki her bir madde frekans ve yüzde dağılımının yanı sıra aritmetik ortalama ve standart sapma değerleriyle betimlenmiştir. Ayrıca katılımcıların bilgi güvenliği farkındalığının bireysel özelliklere göre karşılaştırılmasında parametrik test varsayımları (verilerin normal dağılması, varyansların homojenliği, gruplardaki birey sayısı vb.) gerçekleştiği için iki grup için bağımsız örneklemler için t-testi, ikiden fazla grup için ise tek yönlü varyans analizi kullanılmıştır. Varyans analizi sonucunda farklılığın kaynağını ortaya koymak için Tukey testi uygulanmıştır. Bununla birlikte ölçeklerin güvenilirliği için Cronbach's Alpha değerleri hesaplanmıştır. Buna göre Cronbach's Alpha değerleri saldırı ve tehditler alt boyutu için 0,786; kişisel verileri koruma alt boyutu için 0,803 ve genel bilgi güvenliği farkındalığı ölçeği için ise 0,814 olarak hesaplanmıştır

4. BULGULAR

Katılımcıların mesleklerine göre dağılımı Çizelge 4.1'de verilmiştir. Çizelge 4.1'e göre katılımcıların %51,4'ü asker iken %48,6'sı ise polistir.

Çizelge 4.1 Katılımcıların mesleklerine göre dağılımı

Değişken	Grup	Sayı (f)	Yüzde (%)
Meslek	Asker	207	51,4
	Polis	196	48,6

Katılımcıların cinsiyetlerine göre dağılımı Çizelge 4.2'de sunulmuştur. Çizelge 4.2 incelendiğinde katılımcıların %14,9'u kadın ve %85,1'i erkeklerden oluşmaktadır.

Çizelge 4.2 Katılımcıların cinsiyetlerine göre dağılımı

Değişken	Grup	Sayı (f)	Yüzde (%)
Cinsiyet	Kadın	60	14,9
	Erkek	343	85,1

Katılımcıların medeni durumlarına göre dağılımı Çizelge 4.3'te gösterilmiştir. Çizelge 4.3'e bakıldığında ankete katılan bireylerin %70,5'i evli ve %29,5'i ise bekardır.

Çizelge 4.3 Katılımcıların medeni durumlarına göre dağılımı

Değişken	Grup	Sayı (f)	Yüzde (%)
Medeni Durum	Evli	284	70,5
	Bekar	119	29,5

Katılımcıların yaşlarına göre dağılımı Çizelge 4.4'te sunulmuştur. Çizelge 4.4 incelendiğinde katılımcıların, %4,2'si 18-22 yaş grubunda, %36,5'i 23-27 yaş grubunda, %28,5'i 28-32 yaş grubunda, %12,7'si 33-37 yaş grubunda, %12,2'si 38-43 yaş grubunda ve %6,0'sı ise 43 yaş ve üzeri yaş grubunda yer almaktadır.

Çizelge 4.4 Katılımcıların yaşlarına göre dağılımı

Değişken	**Grup**	**Sayı (f)**	**Yüzde (%)**
Yaş	18-22 yaş	17	4,2
	23-27 yaş	147	36,5
	28-32 yaş	115	28,5
	33-37 yaş	51	12,7
	38-42 yaş	49	12,2
	43 yaş ve üzeri	24	6,0

Katılımcıların eğitim düzeylerine göre dağılımı Çizelge 4.5'te sunulmuştur. Çizelge 4.5'e göre katılımcıların, %1,5'i ilkokul mezunu, %27,0'ı ortaöğretim ve lise mezunu, %26,6'sı ön lisans mezunu, %43,2'si lisans mezunu ve %1,7'si ise lisansüstü mezunu olduklarını belirtmişlerdir.

Çizelge 4.5 Katılımcıların eğitim düzeylerine göre dağılımı

Değişken	**Grup**	**Sayı (f)**	**Yüzde (%)**
Eğitim Düzeyi	Lise ve altı	115	28,5
	Ön lisans	107	26,6
	Lisans	181	44,9

Katılımcıların çalıştıkları birimlere göre dağılımı Çizelge 4.6'da sunulmuştur. Çizelge 4.6 incelendiğinde katılımcıların, %27,8'i asayiş biriminde, %7,9'u kaçakçılık ve organize suçlar biriminde, %12,9'u komando ve özel harekât, %3,5'i kriminal ve OYİ biriminde, %10,4'ü istihbarat biriminde, %9,9'u terörle mücadele biriminde, %4,5'i personel olarak ve %23,1'i diğer (çevik kuvvet, siber suçlar v.b) birimlerde çalıştıklarını bildirmişlerdir.

Çizelge 4.6 Katılımcıların çalıştıkları birimlere göre dağılımı

Değişken	**Grup**	**Sayı (f)**	**Yüzde (%)**
Çalışılan Birim	Asayiş	112	27,8
	Kaçakçılık ve Organize Suçlar	32	7,9
	Komando ve Özel Harekat	52	12,9
	Kriminal ve OYİ	14	3,5
	İstihbarat	42	10,4
	Terörle mücadele	40	9,9
	Personel	18	4,5
	Diğer (Trafik, Çevik kuvvet, Siber suçlar v.b)	93	23,1

Katılımcıların ünvanlarına göre dağılımı Çizelge 4.7'de sunulmuştur. Çizelge 4.7'ye göre katılımcıların, %24,5'i uzman erbaşlardan (onbaşı, çavuş vb.), %16,9'u subay-astsubay ve %48,6'sı polis memurlarından oluşmaktadır.

Çizelge 4.7 Katılımcıların ünvanlarına göre dağılımı

Değişken	**Grup**	**Sayı (f)**	**Yüzde (%)**
Ünvan	Uzman Erbaş (onbaşı, çavuş v.b)	139	34,5
	Subay-Astsubay	68	16,9
	Polis Memuru	196	48,6

Katılımcıların çalışma sürelerine göre dağılımı Çizelge 4.8'de sunulmuştur. Çizelge

4.8'e göre katılımcıların, %11,2'si 1 yıl ve daha az süredir çalıştıklarını, %31,8'i 2-4 yıl çalıştıklarını, %24,1'i 5-7 yıl çalıştıklarını, %11,4'ü 8-10 yıl çalıştıklarını ve %21,6'sı ise 11 yıl ve daha uzun süredir meslekte çalıştıklarını belirtmişlerdir.

Çizelge 4.8 Katılımcıların çalışma sürelerine göre dağılımı

Değişken	Grup	Sayı (f)	Yüzde (%)
Çalışma Süresi	1 yıl ve daha az	45	11,2
	2-4 yıl	128	31,8
	5-7 yıl	97	24,1
	8-10 yıl	46	11,4
	11 yıl ve daha fazla	87	21,6

Katılımcıların bilgisayar ve bilgi güvenliği seviyelerine göre dağılımı Çizelge 4.9'da sunulmuştur. Çizelge 4.9'a göre katılımcıların bilgisayar ve bilgi güvenliği seviyeleri %3,5'inde hiç olmadığı, %19,1'i az olduğu, %38,7'si orta düzeyde olduğu, %29,5'i iyi olduğu ve %9,2'sinin ise çok iyi olduğu belirtilmiştir.

Çizelge 4.9 Katılımcıların bilgisayar ve bilgi güvenliği seviyelerine göre dağılımı

Değişken	Grup	Sayı (f)	Yüzde (%)
Bilgisayar ve Bilgi Güvenliği Seviyesi	Hiç	14	3,5
	Az	77	19,1
	Orta	156	38,7
	İyi	119	29,5
	Çok İyi	37	9,2

Katılımcıların sahip olduğu cihazlara göre dağılımı Çizelge 4.10'da sunulmuştur. Çizelge 4.10'a göre katılımcıların %29,5'inde akıllı telefon olduğu, %9,2'sinde

bilgisayar olduğu, %2,7'sinde tablet olduğu, %36,7'sinde telefon ve bilgisayar olduğu, %21.1'inde telefon bilgisayar ve tablet olduğu ve %0,7'sinde ise hiçbir cihaz olmadığı belirtilmiştir.

Çizelge 4-10 Katılımcıların sahip oldukları cihazlara göre dağılımı

Değişken	Grup	Sayı (f)	Yüzde (%)
Sahip Olunan Cihaz	Akıllı Telefon	122	30,2
	Bilgisayar	37	9,2
	Tablet	11	2,7
	Telefon ve Bilgisayar	148	36,7
	Telefon, Bilgisayar ve tablet	85	21,1

Katılımcıların internete bağlanılan cihazlara göre dağılımı Çizelge 4.11'de sunulmuştur. Çizelge 4.11 incelendiğinde katılımcıların %31,8'inin akıllı telefon ile internete bağlandığı, %8,4'ünün bilgisayar ile internete bağlandığı, %2,7'sinin tablet ile internete bağlandığı, %35,5'inin telefon ve bilgisayar ile internete bağlandığı, %20,1'inin telefon, bilgisayar ve tablet ile internete bağlandığı ve %1,5'inin ise hiçbir cihaz ile internete bağlanmadığı belirtilmiştir.

Çizelge 4.11 Katılımcıların internete bağlanılan cihazlara göre dağılımı

Değişken	Grup	Sayı (f)	Yüzde (%)
İnternete Bağlanılan Cihaz	Akıllı Telefon	118	29,3
	Bilgisayar	34	8,4
	Tablet	11	2,7
	Telefon ve Bilgisayar	143	35,5
	Telefon, Bilgisayar ve tablet	81	20,1
	Hiçbiri	16	4,0

Bilgi güvenliği farkındalık düzeyi ölçeğinin saldırı ve tehditler alt boyutuna ilişkin betimsel istatistikler Çizelge 4.12'de sunulmuştur.

Çizelge 4.12 Bilgi güvenliği farkındalık düzeyi ölçeğinin "saldırı ve tehditler" alt boyutuna ilişkin betimsel istatistikler

Maddeler		**Hiç**	**Az**	**Orta**	**Çok**	**Tam**	$\overline{X}$	**SS**
Bilgisayarıma kötü niyetli kod (malicious code) bulaşıp bulaşmadığını anlayabilirim.	f	122	96	102	44	39	2,46	1,29
	%	30,3	23,8	25,3	10,9	9,7		
Kötü niyetli yazılımlara (malware) karşı alınması gereken güvenlik tedbirlerini biliyorum.	f	95	112	104	46	46	2,59	1,28
	%	23,6	27,8	25,8	11,4	11,4		
Aldatmaca (hoax) nedir biliyorum.	f	149	93	87	43	31	2,29	1,27
	%	37,0	23,1	21,6	10,7	7,7		
Zincir e-postalara (chain e-mail) karşı nasıl hareket etmem gerektiğini biliyorum.	f	126	116	80	49	32	2,37	1,26
	%	31,3	28,8	19,9	12,2	7,9		
Bilgisayarımda casus yazılım (spyware) olup olmadığını anlayabilirim.	f	134	106	84	45	34	2,35	1,28
	%	33,3	26,3	20,8	11,2	8,4		
Bilgisayarıma casus yazılım yüklenmesini engelleme yöntemlerini biliyorum.	f	148	84	78	56	37	2,38	1,34
	%	36,7	20,8	19,4	13,9	9,2		
Kimlik hırsızlığı (identity theft) nedir biliyorum.	f	134	93	92	46	38	2,41	1,31
	%	33,3	23,1	22,8	11,4	9,4		
Kimlik hırsızlığına karşı alınması gereken güvenlik tedbirlerini biliyorum.	f	138	90	94	47	34	2,38	1,29
	%	34,2	22,3	23,3	11,7	8,4		
Sahte virüs koruma yazılımının ne olduğunu biliyorum.	f	119	105	85	54	40	2,48	1,31
	%	29,5	26,1	21,1	13,4	9,9		
Hizmet aksatrma (Denial of Service - DoS) saldırısı nedir biliyorum.	f	194	77	72	37	23	2,05	1,24
	%	48,1	19,1	17,9	9,2	5,7		
Kimlik avı (phishing) saldırısı nedir biliyorum.	f	155	103	86	37	22	2,18	1,20
	%	38,5	25,6	21,3	9,2	5,5		
Sosyal mühendislik (social engineering) saldırısı nedir biliyorum.	f	175	86	78	41	23	2,13	1,24
	%	43,4	21,3	19,4	10,2	5,7		
Sosyal mühendislik saldırısına uğramamak için nasıl hareket etmem gerektiğini biliyorum.	f	170	84	83	41	25	2,17	1,25
	%	42,2	20,8	20,6	10,2	6,2		
Siber zorbalık (cyberbullying) nedir biliyorum.	f	148	95	80	52	28	2,30	1,27
	%	36,7	23,6	19,9	12,9	6,9		
Siber zorbalığa karşı kendimi nasıl koruyacağımı biliyorum.	f	157	86	81	48	31	2,28	1,30
	%	39,0	21,3	20,1	11,9	7,7		
Siber zorbalığa karşı çocuklarımı nasıl koruyacağımı biliyorum.	f	149	87	75	58	34	2,36	1,33
	%	37,0	21,6	18,6	14,4	8,4		

Çizelge 4.12 incelendiğinde, "kötü niyetli yazılımlara (malware) karşı alınması gereken güvenlik tedbirlerini biliyorum" maddesine katılımcıların %53,6'sı az ve orta seçenekleri ile, ($\bar{x}$=2,59), "sahte virüs koruma yazılımının ne olduğunu biliyorum" maddesine katılımcıların %47,2'sinin az ve orta seçenekleri ile ($\bar{x}$=2,48) ve "bilgisayarıma kötü niyetli kod (malicious code) bulaşıp bulaşmadığını anlayabilirim" maddesine katılımcıların %49,1'inin az ve orta ($\bar{x}$=2,46) seçenekleri ile yarı olumlu görüş belirtmişlerdir. Ayrıca katılımcıların %67,2'si "hizmet aksatma (Denial of Service - DoS) saldırısı nedir biliyorum" maddesine hiç ve az seçenekleri, ($\bar{x}$=2,05), "sosyal mühendislik (social engineering) saldırısı nedir biliyorum" maddesine katılımcıların %64,7'si ($\bar{x}$=2,13) hiç ve az seçenekleri ve "sosyal mühendislik saldırısına uğramamak için nasıl hareket etmem gerektiğini biliyorum" maddesine katılımcıların %63,0'ı hiç ve az ($\bar{x}$=2,17) seçenekleri ile olumsuz görüş bildirmişlerdir.

Katılımcıların bilgi güvenliği farkındalık düzeyi ölçeğinin "kişisel verileri koruma alt boyutu"na ilişkin betimsel istatistikler Çizelge 4.13'te sunulmuştur. Çizelge 4.13'e göre, "Kişisel mahremiyet nedir biliyorum." ($\bar{x}$=3,18) maddesine katılımcıların %43,9'u çok ile tam seçenekleri, "şüpheli veya bilinmeyen kaynaklardan gelen özellikle eklentisi olan e-postaları açmanın taşıdığı riski biliyorum" ($\bar{x}$=3,03) maddesine katılımcıların %38,2'si çok ile tam secenekleri ve "çevrimiçi güvenli alışveriş yapmak için gerekli olan güvenlik tedbirlerini biliyorum" ($\bar{x}$=3,01) maddesine katılımcıların %37,2'si çok ile tam seçenekleri ile olumlu görüş bildirmişlerdir. Bunun yanı sıra katılımcıların, %50,2'si "bilgi sistemlerinde kullanılan virüs koruma yazılımını nasıl kullanacağımı biliyorum" ($\bar{x}$=2,67) maddesine hiç ve az, %49,9'u "bilgisayarımdaki virüs koruma yazılımının gerçek zamanlı koruma (realtime protection) özelliğini kullanmaktayım" ($\bar{x}$=2,67) maddesine hiç ve az ve %48,1'i "kullandığım bilgi sistemlerinde tanımlanmış olan kuralları nasıl uygulayacağımı biliyorum" ($\bar{x}$=2,70) maddesine hiç ve az seçenekleri ile olumsuz görüş bildirmişlerdir.

Çizelge 4.13 Bilgi güvenliği farkındalık düzeyi ölçeğinin "kişisel verileri koruma" alt boyutuna ilişkin betimsel istatistikler

Maddeler		Hiç	Az	Orta	Çok	Tam	$\overline{X}$	SS
Bilgi güvenliğinin ne anlama geldiğini biliyorum.	f	85	93	96	71	58	2,81	1,34
	%	21,1	23,1	23,8	17,6	14,4		
Bilgi güvenliği ile ilgili sorumluluklarımın ne olduğunu biliyorum.	f	90	93	88	77	55	2,79	1,35
	%	22,3	23,1	21,8	19,1	13,6		
Kullandığım bilgi sistemlerinde tanımlanmış olan kuralları nasıl uygulayacağımı biliyorum.	f	98	96	91	66	52	2,70	1,34
	%	24,3	23,8	22,6	16,4	12,9		
Bilgi sistemlerinde kullanılan virüs koruma yazılımını nasıl kullanacağımı biliyorum.	f	103	99	83	64	54	2,67	1,36
	%	25,6	24,6	20,6	15,9	13,4		
Bilgisayarımdaki virüs koruma yazılımının gerçek zamanlı koruma (realtime protection) özelliğini kullanmaktayım.	f	106	95	89	52	61	2,67	1,38
	%	26,3	23,6	22,1	12,9	15,1		
Bilgisayarımdaki virüs koruma yazılımının otomatik güncelleştirme yapmasını sağlayabilirim.	f	93	84	87	63	76	2,86	1,42
	%	23,1	20,8	21,6	15,6	18,9		
Dijital imza (digital signature) nedir biliyorum.	f	95	69	94	76	69	2,89	1,41
	%	23,6	17,1	23,3	18,9	17,1		
Şüpheli veya bilinmeyen kaynaklardan gelen özellikle eklentisi olan e-postaları açmanın taşıdığı riski biliyorum.	f	81	69	99	66	88	3,03	1,42
	%	20,1	17,1	24,6	16,4	21,8		
E-posta gönderirken "Gizli" (BCC) alanının sağladığı avantajları biliyorum.	f	102	82	99	59	61	2,74	1,38
	%	25,3	20,3	24,6	14,6	15,1		
İstenmeyen elektronik posta (spam) nedir biliyorum.	f	84	77	104	52	86	2,95	1,42
	%	20,8	19,1	25,8	12,9	21,3		
İstenmeyen elektronik posta miktarını azaltmak için gerekli bilgiye sahibim.	f	111	88	78	51	75	2,73	1,46
	%	27,5	21,8	19,4	12,7	18,6		
Sosyal ağ sitelerini (social networking sites) güvenli olarak nasıl kullanacağımı biliyorum.	f	97	85	101	52	68	2,77	1,39
	%	24,1	21,1	25,1	12,9	16,9		
USB sürücülerini (USB drives) kullanırken dikkat edilmesi gereken hususları biliyorum.	f	78	83	90	63	89	3,00	1,42
	%	19,4	20,6	22,3	15,6	22,1		
Taşınabilir cihazlara (portable devices) yönelik fiziksel güvenliği sağlamak ile ilgili dikkat edilmesi gereken konuları biliyorum.	f	85	78	103	57	80	2,92	1,40
	%	21,1	19,4	25,6	14	19,9		
Taşınabilir cihazlara yönelik veri güvenliği ile ilgili dikkat edilmesi gereken konuları biliyorum.	f	81	92	93	60	77	2,90	1,39
	%	20,1	22,8	23,1	14,9	19,1		
Kişisel mahremiyet nedir biliyorum.	f	72	65	89	73	104	3,18	1,44
	%	17,9	16,1	22,1	18,1	25,8		
Çevrimiçi güvenli alışveriş yapmak için gerekli olan güvenlik tedbirlerini biliyorum.	f	71	91	91	64	86	3,01	1,40
	%	17,6	22,6	22,6	15,9	21,3		
Mavidiş (Bluetooth) teknolojisi ile veri aktarımı konusunda bilgi sahibiyim.	f	95	73	78	69	88	2,96	1,47
	%	23,6	18,1	19,4	17,1	21,8		

Katılımcıların bilgi güvenliği farkındalığı ölçek ve alt ölçeklerinin mesleğe göre karşılaştırmasına yönelik *t*-testi sonuçları Çizelge 4.14'te sunulmuştur. Çizelge 4.14 incelendiğine, katılımcıların bilgi güvenliği farkındalığı ölçek ve alt ölçeklerinin meslek gruplarına göre farklılık göstermediği tespit edilmiştir (p>0,05).

Çizelge 4.14 Katılımcıların bilgi güvenliği farkındalığı ölçek ve alt ölçeklerinin mesleğe göre karşılaştırmasına yönelik bulgular

Ölçekler	**Grup**	$\overline{X}$	**SS**	***t***	**p**
Saldırı ve Tehditler	Asker	2,26	1,06	-1,303	0,193
	Polis	2,39	1,05		
Kişisel Verileri Koruma	Asker	2,78	1,28	-1,470	0,144
	Polis	2,95	1,07		
Genel Bilgi Güvenliği Farkındalığı	Asker	2,54	1,12	-1,475	0,141
	Polis	2,69	1,00		

Katılımcıların bilgi güvenliği farkındalığı ölçek ve alt ölçeklerinin cinsiyete göre karşılaştırmasına yönelik *t*-testi sonuçları Çizelge 4.15'te sunulmuştur. Çizelge 4.15 incelendiğinde katılımcıların bilgi güvenliği farkındalığı, saldırı ve tehditler algısı ve kişisel verilerin korunması algılarının katılımcıların cinsiyetlerine göre anlamlı bir farklılık göstermediği istatistiksel olarak %95 güvenilirlikle söylenebilir (p>0,05).

Çizelge 4.15 Katılımcıların bilgi güvenliği farkındalığı ölçek ve alt ölçeklerinin cinsiyete göre karşılaştırmasına yönelik bulgular

Ölçekler	**Grup**	$\overline{X}$	**SS**	***t***	**p**
Saldırı ve Tehditler	Kadın	2,15	1,03	-1,398	0,163
	Erkek	2,36	1,06		
Kişisel Verileri Koruma	Kadın	2,61	1,03	-1,802	0,072
	Erkek	2,91	1,20		
Genel Bilgi Güvenliği Farkındalığı	Kadın	2,39	0,98	-1,720	0,084
	Erkek	2,65	1,07		

Katılımcıların bilgi güvenliği farkındalığı ölçek ve alt ölçeklerinin medeni durumlarına göre karşılaştırmasına yönelik *t*-testi sonuçları Çizelge 4.16'da sunulmuştur. Çizelge 4.16'ya göre, bilgi güvenliği farkındalığı ölçek ve alt ölçeklerinin katılımcıların medeni durumlarına göre fark göstermediği saptanmıştır (p>0,05).

Çizelge 4.16 Katılımcıların bilgi güvenliği farkındalığı ölçek ve alt ölçeklerinin medeni duruma göre karşılaştırmasına yönelik bulgular

Ölçekler	**Grup**	$\overline{X}$	**SS**	**t**	**p**
Saldırı ve Tehditler	Evli	2,29	1,07	-1,114	0,266
	Bekar	2,41	1,01		
Kişisel Verileri Koruma	Evli	2,89	1,22	0,700	0,485
	Bekar	2,80	1,10		
Genel Bilgi Güvenliği Farkındalığı	Evli	2,61	1,08	-0,108	0,914
	Bekar	2,62	1,01		

Katılımcıların bilgi güvenliği farkındalığı ölçek ve alt ölçeklerinin yaşa göre karşılaştırmasına yönelik varyans analizi sonuçları Çizelge 4.17'de sunulmuştur.

Çizelge 4.17 incelendiğinde, saldırı ve tehditler algısı yaşa göre farkındalık göstermezken (p>0,05), kişisel verileri koruma algısının ve genel bilgi güvenliği farkındalığı yaşa göre anlamlı bir farklılık göstermektedir (p<0,05). Aritmetik ortalamalar incelendiğinde, 28 yaş ve üzeri gruplarda kişisel verilerin korunması algısının diğer yaş gruplarına nispeten daha yüksek olduğu saptanmıştır. Ayrıca genel bilgi güvenliği farkındalığının ise 28-32 yaş gruplarında daha fazla olduğu tespit edilmiştir.

Çizelge 4.17 Katılımcıların bilgi güvenliği farkındalığı ölçek ve alt ölçeklerinin yaşa göre karşılaştırmasına yönelik bulgular

Ölçekler	**Grup**	$\overline{X}$	**SS**	**F**	**p**
Saldırı ve Tehditler	18-22 yaş	2,26	0,93	1,484	0,194
	23-27 yaş	2,21	0,96		
	28-32 yaş	2,53	1,08		
	33-37 yaş	2,22	0,99		
	38-42 yaş	2,38	1,29		
	43 yaş ve üzeri	2,17	1,13		
Kişisel Verileri Koruma	18-22 yaş	2,70[ab]	0,81	5,029	0,000*
	23-27 yaş	2,52[b]	1,12		
	28-32 yaş	3,19[a]	1,13		
	33-37 yaş	3,08[a]	1,18		
	38-42 yaş	2,96[a]	1,32		
	43 yaş ve üzeri	2,91[ab]	1,27		
Genel Bilgi Güvenliği Farkındalığı	18-22 yaş	2,49[ab]	0,76	3,218	0,007*
	23-27 yaş	2,37[b]	1,01		
	28-32 yaş	2,88[a]	1,04		
	33-37 yaş	2,68[ab]	0,97		
	38-42 yaş	2,69[ab]	1,25		
	43 yaş ve üzeri	2,56[ab]	1,15		

**p<0,05; a,b:aynı sütunda farklı harfleri içeren gruplar arasındaki farklar önemlidir.*

Katılımcıların bilgi güvenliği farkındalığı ölçek ve alt ölçeklerinin eğitim düzeyine göre karşılaştırmasına yönelik varyans analizi sonuçları Çizelge 4.18'de sunulmuştur. Çizelge 4.18'e göre saldırı ve tehditler algısı katılımcıların eğitim düzeylerine göre farkındalık göstermezken (p>0,05), kişisel verileri koruma algısı ve genel bilgi

güvenliği farkındalığı eğitim düzeylerine göre anlamlı bir farklılık gösterdiği istatistiksel olarak %95 güvenilirlikle söylenebilir (p<0,05). Ortalamalar incelendiğinde gerek kişisel verileri koruma algısının gerekse genel bilgi farkındalığının lisans ve lisansüstü eğitim alanlarda diğer gruplara göre daha yüksek olduğu saptanmıştır.

Çizelge 4.18 Katılımcıların bilgi güvenliği farkındalığı ölçek ve alt ölçeklerinin eğitim düzeyine göre karşılaştırmasına yönelik bulgular

Ölçekler	**Grup**	$\overline{X}$	**SS**	**F**	**p**
Saldırı ve Tehditler	Lise ve altı	2,14	1,02		
	Ön lisans	2,32	0,95	2,122	0,077
	Lisans	2,45	1,12		
Kişisel Verileri Koruma	Lise ve altı	2,39[c]	1,19		
	Ön lisans	2,80[b]	1,09	8,689	0,000*
	Lisans	3,19[a]	1,14		
Genel Bilgi Güvenliği Farkındalığı	Lise ve altı	2,27[c]	1,07		
	Ön lisans	2,58[b]	0,96	5,588	0,000*
	Lisans	2,84[a]	1,06		

**p<0,05; a,b,c:aynı sütunda farklı harfleri içeren gruplar arasındaki farklar önemlidir.*

Katılımcıların bilgi güvenliği farkındalığı ölçek ve alt ölçeklerinin çalışılan birime göre karşılaştırmasına yönelik varyans analizi sonuçları Çizelge 4.19'da sunulmuştur. Çizelge 4.19 incelendiğinde saldırı ve tehditler alt ölçeği, kişisel verileri koruma alt ölçeği ve genel bilgi farkındalığı katılımcıların çalıştıkları birimlere göre istatistiksel olarak anlamlı bir fark gösterdiği (p<0,05) tespit edilmiştir. Bu bağlamda katılımcıların saldırı ve tehditler algısı, kişisel verileri koruması ve genel bilgi farkındalığı kriminal ve OYİ biriminde çalışanlarda diğer birimlere göre daha yüksek olduğu saptanmıştır.

Çizelge 4.19 Katılımcıların bilgi güvenliği farkındalığı ölçek ve alt ölçeklerinin çalışılan birime göre karşılaştırmasına yönelik bulgular

Ölçekler	Grup	$\overline{X}$	SS	F	p
Saldırı ve Tehditler	Asayiş	2,13[c]	1,04	3,324	0,002*
	Kaçakçılık ve Organize Suçlar	2,13[c]	0,74		
	Komando ve Özel Harekat	2,42[b]	0,90		
	Kriminal ve OYİ	3,37[a]	1,41		
	İstihbarat	2,44[b]	0,96		
	Tem	2,53[b]	1,07		
	Personel	2,03[c]	1,24		
	Diğer	2,33[bc]	1,10		
Kişisel Verileri Koruma	Asayiş	2,47[d]	1,21	5,871	0,000*
	Kaçakçılık ve Organize Suçlar	2,66[cd]	1,06		
	Komando ve Özel Harekat	2,82[c]	0,99		
	Kriminal ve OYİ	3,83[a]	1,19		
	İstihbarat	3,39[b]	1,23		
	Tem	3,23[b]	1,07		
	Personel	2,48[d]	1,22		
	Diğer	2,98[c]	1,10		
Genel Bilgi Güvenliği Farkındalığı	Asayiş	2,31[c]	1,09	4,886	0,000*
	Kaçakçılık ve Organize Suçlar	2,41[c]	,83		
	Komando ve Özel Harekat	2,63[b]	,89		
	Kriminal ve OYİ	3,61[a]	1,25		
	İstihbarat	2,94[b]	1,02		
	Tem	2,90[b]	,99		
	Personel	2,27[c]	1,15		
	Diğer	2,67[b]	1,03		

$p<0,05$; a,b,c,d:aynı sütunda farklı harfleri içeren gruplar arasındaki farklar önemlidir.

Katılımcıların bilgi güvenliği farkındalığı ölçek ve alt ölçeklerinin ünvana göre karşılaştırmasına yönelik varyans analizi sonuçları Çizelge 4.20'de sunulmuştur. Çizelge 4.20 incelendiğinde bilgi güvenliği farkındalığı ölçek ve alt ölçeklerinin katılımcıların ünvanlarına göre anlamlı bir farklılık gösterdiği istatistiksel olarak söylenebilir (p<0,05). Aritmetik ortalamalar incelendiğinde, subay-astsubay ve polis memurlarının uzman erbaşlara göre saldırı ve tehditler algısı, kişisel verileri koruması ve genel bilgi farkındalığının daha yüksek olduğu farklılığından bundan kaynaklandığı tespit edilmiştir.

Çizelge 4.20 Katılımcıların bilgi güvenliği farkındalığı ölçek ve alt ölçeklerinin ünvana göre karşılaştırmasına yönelik bulgular

Ölçekler	Grup	$\overline{X}$	SS	F	p
Saldırı ve Tehditler	Uzman Erbaş (onbaşı ve çavuş)	2,13[b]	1,02	4,222	0,015*
	Subay-Astsubay	2,53[a]	1,10		
	Polis Memuru	2,39[ab]	1,05		
Kişisel Verileri Koruma	Uzman Erbaş (onbaşı ve çavuş)	2,56[b]	1,26	8,906	0,000*
	Subay-Astsubay	3,24[a]	1,20		
	Polis Memuru	2,95[ab]	1,07		
Genel Bilgi Güvenliği Farkındalığı	Uzman Erbaş (onbaşı ve çavuş)	2,36[b]	1,09	7,413	0,001*
	Subay-Astsubay	2,90[a]	1,08		
	Polis Memuru	2,69[ab]	1,00		

**p<0,05; a,b:aynı sütunda farklı harfleri içeren gruplar arasındaki farklar önemlidir.*

Katılımcıların bilgi güvenliği farkındalığı ölçek ve alt ölçeklerinin çalışma süresine göre karşılaştırmasına yönelik analiz sonuçları Çizelge 4.21'de sunulmuştur.

Çizelge 4.21 Katılımcıların bilgi güvenliği farkındalığı ölçek ve alt ölçeklerinin çalışma süresine göre karşılaştırmasına yönelik bulgular

Ölçekler	Grup	$\overline{X}$	SS	F	p
Saldırı ve Tehditler	1 yıl ve daha az	2,39	1,12	0,309	0,872
	2-4 yıl	2,30	1,01		
	5-7 yıl	2,34	0,96		
	8-10 yıl	2,43	1,26		
	11 yıl ve daha fazla	2,25	1,09		
Kişisel Verileri Koruma	1 yıl ve daha az	2,82[ab]	1,09	2,548	0,039*
	2-4 yıl	2,67[b]	1,18		
	5-7 yıl	2,80[ab]	1,04		
	8-10 yıl	3,21[a]	1,36		
	11 yıl ve daha fazla	3,06[a]	1,23		
Genel Bilgi Güvenliği Farkındalığı	1 yıl ve daha az	2,62	1,06	1,018	0,398
	2-4 yıl	2,50	1,06		
	5-7 yıl	2,59	,94		
	8-10 yıl	2,84	1,23		
	11 yıl ve daha fazla	2,68	1,10		

**p<0,05; a,b:aynı sütunda farklı harfleri içeren gruplar arasındaki farklar önemlidir.*

Çizelge 4.21'e göre saldırı ve tehditler algısının ve genel bilgi güvenliği farkındalığının katılımcıların meslekte çalışma sürelerine göre anlamlı bir farklılık göstermediği tespit edilirken (p>0,05), kişisel verileri koruma algısı katılımcıların meslekte çalışma süresine göre anlamlı bir farklılık göstermiştir (p<0,05). Bu bilgiler ışığında kişisel verileri koruma algısının 8 ve daha fazla yıldır meslekte görev yapanlarda diğer gruplara göre daha yüksek olduğu söylenebilir.

Katılımcıların bilgi güvenliği farkındalığı ölçek ve alt ölçeklerinin bilgisayar ve bilgi güvenliği seviyelerine göre karşılaştırmasına yönelik varyans analizi sonuçları Çizelge 4.22'de sunulmuştur.

Çizelge 4.22 Katılımcıların bilgi güvenliği farkındalığı ölçek ve alt ölçeklerinin bilgisayar ve bilgi güvenliği seviyelerine göre karşılaştırmasına yönelik bulgular

Ölçekler	**Grup**	$\overline{X}$	**SS**	**F**	**p**
Saldırı ve Tehditler	Hiç	1,86[d]	1,01		
	Az	1,77[d]	0,74		
	Orta	2,08[c]	0,84	32,084	0,000*
	İyi	2,67[b]	1,01		
	Çok İyi	3,58[a]	1,22		
Kişisel Verileri Koruma	Hiç	2,13[d]	1,19		
	Az	2,23[d]	1,02		
	Orta	2,67[c]	1,06	22,820	0,000*
	İyi	3,31[b]	1,08		
	Çok İyi	3,87[a]	1,15		
Genel Bilgi Güvenliği Farkındalığı	Hiç	2,00[d]	1,08		
	Az	2,01[d]	0,84		
	Orta	2,39[c]	0,89	30,326	0,000*
	İyi	3,01[b]	0,96		
	Çok İyi	3,73[a]	1,15		

p<0,05; a,b,c,d:aynı sütunda farklı harfleri içeren gruplar arasındaki farklar önemlidir.

Çizelge 4.22'ye göre bilgi güvenliği farkındalığı ölçek ve alt ölçeklerinin katılımcıların bilgisayar ve bilgi güvenliği seviyelerine göre anlamlı bir farklılık gösterdiği istatistiksel olarak %95 güvenilirlikle söylenebilir (p<0,05). Aritmetik ortalamalar incelendiğinde katılımcıların, saldırı ve tehdit algılarının, kişisel verileri koruma algılarının ve genel bilgi güvenliği farkındalığının bilgisayar ve bilgi güvenliğini çok iyi bilenlerde daha yüksek olduğu tespit edilmiştir.

Katılımcıların bilgi güvenliği farkındalığı ölçek ve alt ölçeklerinin sahip olunan cihazlara göre karşılaştırmasına yönelik varyans analizi sonuçları Çizelge 4.23'te sunulmuştur.

Çizelge 4.23 Katılımcıların bilgi güvenliği farkındalığı ölçek ve alt ölçeklerinin sahip olunan cihazlara göre karşılaştırmasına yönelik bulgular

Ölçekler	**Grup**	$\overline{X}$	**SS**	**F**	**p**
Saldırı ve Tehditler	Akıllı Telefon	2,02[c]	0,89		
	Bilgisayar	2,38[b]	0,95		
	Tablet	2,17[c]	0,42	3,888	0,002*
	Telefon ve Bilgisayar	2,38[b]	1,12		
	Telefon, Bilgisayar ve tablet	2,64[a]	1,16		
Kişisel Verileri Koruma	Akıllı Telefon	2,48[b]	1,01		
	Bilgisayar	2,53[b]	1,02		
	Tablet	2,33[b]	0,79	6,984	0,000*
	Telefon ve Bilgisayar	3,05[a]	1,20		
	Telefon, Bilgisayar ve tablet	3,27[a]	1,29		
Genel Bilgi Güvenliği Farkındalığı	Akıllı Telefon	2,26[b]	0,89		
	Bilgisayar	2,46[b]	0,96		
	Tablet	2,25[b]	0,58	5,863	0,000*
	Telefon ve Bilgisayar	2,74[a]	1,10		
	Telefon, Bilgisayar ve tablet	2,97[a]	1,15		

*$p<0,05$; *a,b:aynı sütunda farklı harfleri içeren gruplar arasındaki farklar önemlidir.*

Çizelge 4.23'e göre, saldırı ve tehditler algıları, kişisel verileri koruma algıları ve genel bilgi farkındalığı katılımcıların sahip oldukları cihazlara göre istatistiksel olarak anlamlı bir farklılık göstermektedir ($p<0,05$). Aritmetik ortalamalar incelendiğinde telefon, bilgisayar ve tablete sahip katılımcıların saldırı ve tehditler algıları, kişisel verileri koruma algıları ve genel bilgi farkındalığı diğer gruplara göre daha yüksek olduğu tespit edilmiş olup bunun yanı sıra takılı telefon ve tablete sahip katılımcıların saldırı ve tehditler algıları, kişisel verileri koruma algıları ve genel bilgi farkındalığı diğer gruplara nispeten çok daha düşüktür.

Katılımcıların bilgi güvenliği farkındalığı ölçek ve alt ölçeklerinin internete girilen cihazlara göre karşılaştırmasına yönelik analiz sonuçları Çizelge 4.24'te sunulmuştur. Çizelge 4.24 incelendiğinde, saldırı ve tehditler algıları, kişisel verileri koruma algıları ve genel bilgi farkındalığı katılımcıların internete bağlandıkları cihazlara göre anlamlı bir farklılık gösterdiği saptanmıştır (p<0,05). Ortalamalara göre telefon ve bilgisayar ile telefon, bilgisayar ve tablete sahip katılımcıların saldırı ve tehditler algıları, kişisel verileri koruma algıları ve genel bilgi farkındalığı diğer gruplara göre daha yüksek olduğu saptanmıştır. Ayrıca yalnız akıllı telefonundan, bilgisayardan ve tabletten internete bağlanan katılımcıların saldırı ve tehditler algıları, kişisel verileri koruma algıları ve genel bilgi farkındalığı diğer gruplara nispeten çok daha düşüktür.

Çizelge 4.24 Katılımcıların bilgi güvenliği farkındalığı ölçek ve alt ölçeklerinin internete girilen cihazlara göre karşılaştırmasına yönelik bulgular

Ölçekler	**Grup**	$\overline{X}$	**SS**	**F**	**P**
Saldırı ve Tehditler	Akıllı Telefon	2,07^{c}	0,92	3,758	0,002*
	Bilgisayar	2,15^{c}	0,85		
	Tablet	2,15^{c}	0,84		
	Telefon ve Bilgisayar	2,41^{b}	1,14		
	Telefon, Bilgisayar ve tablet	2,67^{a}	1,13		
	Hiçbiri	2,35^{b}	0,89		
Kişisel Verileri Koruma	Akıllı Telefon	2,50^{b}	0,95	8,112	0,000*
	Bilgisayar	2,37^{b}	0,95		
	Tablet	2,31^{b}	0,86		
	Telefon ve Bilgisayar	3,13^{a}	1,25		
	Telefon, Bilgisayar ve tablet	3,26^{a}	1,28		
	Hiçbiri	2,76^{ab}	1,29		
Genel Bilgi Güvenliği Farkındalığı	Akıllı Telefon	2,30^{b}	0,87	6,490	0,000*
	Bilgisayar	2,27^{b}	0,85		
	Tablet	2,24^{b}	0,82		
	Telefon ve Bilgisayar	2,79^{a}	1,13		
	Telefon, Bilgisayar ve tablet	2,98^{a}	1,13		
	Hiçbiri	2,57^{ab}	1,03		

$^{*}p$<0,05; a,b.c:aynı sütunda farklı harfleri içeren gruplar arasındaki farklar önemlidir.

5. TARTIŞMA ve SONUÇ

Bilgi çağı olarak adlandırılan günümüz dünyasında kişisel ve kurumsal anlamda sahip olduğumuz en önemli değer hiç şüphesiz bilgidir. Bilgi insanın sahip olduğu tüm kazanımlardır. Buradan da anlaşılacağı üzere kişinin bireysel gelişimine ve kariyerine etki eden en önemli etken sahip olduğu bilginin değeridir. Kişinin yaşadığı toplumda diğer insanlardan ayrılabilmesi de tamamen bilgi seviyesi ile doğru orantılı bir konudur. Teknolojik gelişmeler ve özellikle de internetin hayatımıza girmesinden sonra bilgi ulaşması daha kolay bir hal almış ve bu durum bilginin boyutunda büyük bir artışa yol açmıştır.

Bilgi iş dünyasını oluşturan şirketler için de vazgeçilmez bir unsur ve rekabet olgusudur. Şirketlerin var olmasından itibaren üretim, tüketim vb. tüm faaliyet alanlarında kendisini eş değer şirketlerden ayıran en önemli özelliği de sahip olduğu bilginin ölçüsüdür. Kamu kurum ve kuruluşlarda da bu durum böyledir. Kurumların sahip oldukları bilgi seviyesi ve bilginin değerindeki kalite arttıkça kurumun değeri de artar ve ülkenin gelişmesinde önemli katkı sağlar. Kurumlarda çalışan personellerin sahip oldukları bilgi seviyesi kurumsal anlamda sahip olunan toplam bilgi ile doğru orantılı olarak gelişmektedir. Kurumlarda çalışan personelin değişmesi kurumun sahip olduğu toplam bilgi seviyesinde herhangi bir değişime yol açmaması için kurumsal hafızanın son derece sağlam bir zemin üzerine inşa edilmiş olması gerekmektedir.

Kişisel ve özelliklede kurumsal anlamda sahip olunan bilgideki yoğun artış ile bilgiye başka yer, mekân ve platformlardan ulaşılabilme gereksinimi bilginin dijital ortamlara aktarılmasına yol açmıştır. Teknolojik gelişmelerin ışığında bilginin depolanması iletimi ve ulaşılması daha kolay ve daha hızlı olmuştur. Bu durum kurumun faaliyet gösterdiği her bölgede aynı bilgi seviyesi ile hizmet vermesini ve kurumsal hafızanın oluşmasını sağlamıştır. Dijital ortamlara aktarılan bu bilginin korunması kişisel ve kurumsal anlamda hayati önem arz eden bir konu haline gelmiştir.

Teknolojik gelişmelere paralel olarak bilgi güvenliğini sağlayan teknik detaylar da gelişmiş ve her geçen gün yapılan yeni güncellemelerle elektronik ortamlardaki

açıklıklar giderilmektedir. Bu durum kötü niyetli şahısların bilginin kontrolünün ele geçirebilmek için kurumlardaki bu bilgi teknolojilerini kullanan insan faktörü üzerinde yoğunlaşmasına yol açmıştır. Bu yüzden bir kurumdaki güvenlik seviyesinin en zayıf halkası kuşkusuz insan unsurudur. Kritik kamu kurumlarında çalışan ve ülke menfaatlerinin tehlikeye atabilecek bilgiye ulaşan personel bilinçli veya bilinçsiz yaptığı her türlü ihlal ülke güvenliği açısından tehlikeli boyutlara varabilmektedir. Bilinçli yapılan bilgi güvenliği ihlallerine karşı personel alım sürecindeki arşiv ve güvenlik araştırmaları yeterli olabilecekken personelin bilinç dışı yaptığı ihlaller ancak kişilerin bilinçlendirilmesi ve bilgi güvenliği altyapısının oluşturulabilmesi ile mümkün olabilecektir.

Yukarıdaki bilgiler çerçevesinde, emniyet ve asayiş ile kamu düzenini korumakla görevli olan, toplum huzuru ve ülke menfaatleri çerçevesinde suç önleyici çalışma yürüten ve bu çalışmaları yürütürken birçok gizli bilgiyi de bünyesinde barındıran güvenlik (polis, jandarma) personelinin bilgi güvenliği farkındalık düzeylerinin tespit edilmesi amacıyla yapılan bu çalışmaya 207 jandarma ve 197 polis olmak üzere toplam 404 personel katılmıştır. Araştırma sonucunda, bilgi güvenliği farkındalık düzeyi ölçeğinin "saldırı ve tehditler" alt boyutuna ilişkin genel ortalama 2,32 ve "kişisel verileri koruma" alt boyutuna ilişkin genel ortalama ise 2,87 olarak hesaplanmıştır. Bu değerler Likert tipi ölçekte orta düzeyi gösteren 3 puanın altındadır ve emniyet personelinin (polis, jandarma) bilgi güvenliği farkındalık düzeylerinin düşük olduğunu göstermektedir. Özellikle emniyet personelinin "saldırı ve tehditler" alt boyutundaki bilgi güvenliği farkındalık düzeylerinin düşük olması dikkat çeken bir sonuç olmuştur. Bunu nedeni, saldırı ve tehdit konusunun diğer konulara oranla daha spesifik ve ilgi gerektiren bir konu olması olabileceği, ancak kurumsal bilgisayar kullanan personelin asgari düzeyde bu konularla içli dışlı olması kurumun siber saldırılara ve kurumun sahip olduğu bilginin yetkisiz kişilerin eline geçmesine karşı almış olacağı ilk önlem olabilecektir. Bilgi güvenliği farkındalık düzeyinin genel olarak düşük olmasının sebebi ise, kurum içi eğitimlerin alım süreci, oryantasyon eğitimi, hizmet içi eğitim süreçlerinde yetersiz seviyede olması gösterilebilir. Kurum içerisinde çalışan tüm personelin bilgi güvenliği konusunda asgari seviyeye gelebilmesi için eğitim faktörü öne çıkan ilk seçenektir.

Bilgi güvenliği farkındalık ölçeğinin "saldırı ve tehditler" alt boyutu incelendiğinde; güvenlik personelinin, kötü niyetli yazılımlara karşı alınması gereken güvenlik tedbirleri, sahte virüs koruma yazılımının ne olduğu, bilgisayara kötü niyetli kod bulaşıp bulaşmadığının anlaşılması konularında diğer ölçek maddelerine oranla daha iyi seviyede olması ile birlikte, hizmet aksatma saldırıları, sosyal mühendislik saldırıları ve sosyal mühendislik saldırılarına uğramamak için nasıl hareket etmesi konularında diğer ölçek maddelerine oranla daha düşük seviyede olduğu görülmüştür. Yine Bilgi güvenliği farkındalık ölçeğinin "kişisel verileri koruma" alt boyutuna ilişkin veriler incelendiğinde; Kişisel mahremiyetin ne olduğu, şüpheli veya bilinmeyen kaynaklardan gelen e-postaları açmanın taşıdığı risk, çevrim içi güvenli alışveriş yapmak için alınması gereken güvenlik tedbirleri alt boyutlarında güvenlik personelinin diğer ölçek alt boyutlarına oranla daha iyi seviyede oldukları ancak, virüs koruma yazılımını nasıl kullanması gerektiği, virüs koruma yazılımının gerçek zamanlı koruma özelliğinin kullanılması, bilgi sistemlerindeki tanımlanmış olan kuralları nasıl uygulayacağı konularında diğer ölçek boyutlarına oranla daha düşük seviyede oldukları görülmüştür.

Araştırma sonucunda güvenlik personelinin bilgi güvenliği ölçek ve alt ölçeklerine ilişkin farkındalık düzeyinin; cinsiyet, meslek ve medeni duruma göre anlamlı farklılıklar göstermemiştir. Buna karşılık kişisel verileri koruma ve genel bilgi güvenliği farkındalığı yaşa ve eğitime göre; tüm ölçek ve alt ölçeklerde çalışılan birim, unvan, bilgisayar ve bilgi güvenliği seviyesi, sahip olunan cihaz ve internete girilen cihaz değişkenlerine göre anlamlı farklılıklar göstermektedir. Buna göre yaşı ve eğitimi yüksek olan kriminal ve olay yeri inceleme, istihbarat ve Terörle Mücadele birimlerinde çalışan subay-astsubay unvanına sahip kıdemi yüksek, bilgisayar ve bilgi güvenliği seviyesi yüksek, telefon, bilgisayar ve tablet kullanan ve bu cihazlar ile internete bağlanan personelin bilgi güvenliği farkındalık düzeyinin yüksek olduğu görülmüştür.

Bu durum, kriminal, olay yeri ve siber suçlar bölümlerinde çalışan personelin bilgisayar konusunda daha çok bilgiye sahip olmasından, daha özel ve uzmanlık gerektiren işler ile uğraşmasından kaynaklanabildiği değerlendirilmektedir.

Yılmaz vd. (2016)'nin öğretmenlerin dijital veri güvenliğini ölçmek amacıyla yapmış oldukları çalışmada farkındalık düzeyinin yaş ve kullanım sıklığı ile anlamlı farklılık olduğu sonucu ile Karadağ ve Abuhanoğlu, (2015)'nun Gülhane Askeri Tıp akademisi çalışanlarının bilgi güvenliği farkındalık seviyesini belirlemek üzere yapmış oldukları çalışmada farkındalık düzeyinin yaş ve unvan faktörleri üzerinde anlamlı farklılıklar oluşturduğu sonuçları yapmış olduğumuz çalışma ile benzer sonuçlara ulaşmıştır. Ayrıca Akgün ve Topal (2005)'ın eğitim fakültelerinde eğitim gören öğrencilerin bilgi güvenliği seviyelerini araştırmak üzere yapmış oldukları çalışmada bilgi güvenliği konusunda eğitim alan personel ile almayan personel arasında ciddi bir fark olduğu sonucu ile yapmış olduğumuz çalışmada ki kriminal, olay yeri inceleme ve istihbarat birimlerinin siber bölümlerinde çalışan personelin bilgisayar konusunda eğitim aldığı göz önüne alındığında benzer sonuca ulaşmıştır.

Yukarıdaki sonuçlar çerçevesinde konu ile ilgili farklı çalışmaların farklı illerde farklı örneklem gruplarda yapılması bilgi güvenliği farkındalık düzeyinin mevcut durumunu betimleyecek, literatüre önemli katkılar sunacak ve ilgili birimlerin önlem alması konusunda yöneticilere önemli veri kaynağı oluşturacaktır. Bu anlamda çalışmanın sonuçlarından hareketle; Güvenlik personelinin (polis, jandarma) mesleğe başlamadan önceki eğitim ve oryantasyon eğitimi aşamalarında temel bilgisayar eğitiminin yanında bilgi güvenliği ve farkındalık konularında gerekli ders ve sınavlar ile farkındalığın oluşturulması personelin meslek hayatı boyunca bu konuda belli bir seviyeye gelmesi açısından son derece önemli olduğu değerlendirilmektedir. Ayrıca bilgi güvenliği üzerinde uzmanlaşmış kişi ve kuruluşlar yardımı ile meslek içi eğitim ve seminerler düzenlenerek konunun pekiştirilmesi ve yeni teknolojik gelişmelerin takip edilmesi açısından gerekli olduğu değerlendirilmektedir.

6. KAYNAKLAR

Akgün, Ö. E. ve Topal, M. (2015). Eğitim Fakültesi Son Sınıf Öğrencilerinin Bilişim Güvenliği Farkındalıkları: Sakarya Üniversitesi Eğitim Fakültesi Örneği. 8. Uluslararası Bilgisayar ve Öğretim Teknolojileri Sempozyumu, Sakarya Üniversitesi, Sakarya, 19 Eylül 2014, 98-121.

Akyol, F. (2013). COBİT uygulayan Şirketlerdeki Bilgi Güvenliği Politikalarının Şirket Personel ve Süreçlere Etkileri. Yüksek Lisans Tezi, Beykent Üniversitesi, Sosyal Bilimler Enstitüsü, İstanbul.

Anonim. (2018). Elektronik Haberleşme Sektörüne İlişkin İl Bazında Yıllık İstatistik Bülteni. Bilgi Teknolojileri ve İletişim Kurumu Sektörel Araştırma ve Strateji Geliştirme Dairesi Başkanlığı.

Anonim. (2017). TÜİK, Girişimlerde Bilişim Teknolojileri Kullanımı Araştırması, Hanelerde Bilişim Teknolojileri Kullanımı Araştırması, Türkiye İstatistik Kurumu, Ankara

Aslandağ, K. (2010). Bilgi Güvenliği Kavramı ve bilgi Güvenliği Yönetim Sistemleri ile Şirket Performansı ilişkisine Dair Bir Uygulama. Yüksek Lisans Tezi, Gebze Yüksek Teknoloji Enstitüsü, Sosyal Bilimler Enstitüsü, Gebze.

Avşar, Z. ve Öngören, G. (2010). Bilişim Hukuku. Türkiye Bankalar Birliği Yayın No: 270.

Awad, E., and Ghaziri, H. (2004). Knowledge Management. New Jersey: Prentice Hall Publishing.

Aydın, M. (2004). Bilgi sosyolojisi. Açılım Kitap, 3. Baskı, İstanbul, Türkiye.

Arıcı, H.Y. (2018), Adli Bilişim. Seçkin Yayıncılık, 1. Baskı, Ankara, Türkiye.

Barutçugil, İ. (2002). Bilgi Yönetimi. Kariyer Yayıncılık, 1. Baskı, İstanbul, Türkiye.

Başdinkçi, N. (2017). Sağlık Kurumlarında Bilgi Güvenliği Risk Değerlendirilmesi ve

Kullanıcıların Bilgi Güvenliği Farkındalık Düzeyinin Ölçülmesi . Yüksek Lisans Tezi, Çukurova Üniversitesi, Fen bilimleri Enstitüsü, Adana.

Baykara, M., Daş, R., ve Karadoğan, İ. (2013). Bilgi Güvenliği Sistemlerinde Kullanılan Araçların İncelenmesi. 1st International Symposium on Digital Forensics and Security, Elazığ, Türkiye 20-21 Mayıs 231-239.

Bıçakcı, S. (2014). NATO'nun gelişen tehdit algısı: 21. yüzyılda siber güvenlik. Kadir Has Üniversitesi, *Uluslararası İlişkiler Akademik Dergisi*, **10:** 101-130.

Bolat, Y. İ., Aydemir, M., ve Karaman, S. (2017). Uzaktan eğitim öğrencilerinin öğretimsel etkinliklerde mobil internet kullanımlarının teknoloji kabul modeline göre incelenmesi. Gazi Üniversitesi *Gazi Eğitim Fakültesi Dergisi*, **37:** 63-91.

Can, Ö. ve Akbaş, M.F. (2014), Kurumsal Ağ ve Sistem Güvenliği Politikalarının Önemi ve Bir Durum Çalışması. *Türk Bilim Araştırma Vakfı Dergisi*, **7:** 16-31.

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

Canbek, G., ve Sağıroğlu, Ş. (2006). Kötücül ve Casus Yazılımlar: Kapsamlı Bir Araştırma. *Gazi Mühendislik ve Mimarlık dergisi*.

Ceylan, M. (2018). Android Zararlı Yazılım Analizi ve Güvenlik Yaklaşımları. Bilgi Güvenliği Akademisi A.Ş 21-57.

Çapar, B. (2005). Bilgi Yönetimi. Bilgi Çağı Bilgi Yönetimi ve Bilgi Sistemleri İçinde. Çizgi Kitapevi, 1. Baskı, Konya, Türkiye.

Çek, E. (2017). Kurumsal Bilgi Güvenliği ve Bilgi Güvenliği İçin İnsan Faktörünün Önemi. Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi, Sosyal Bilimler Enstitüsü, İstanbul.

Çetin, H. (2014). Kişisel Veri Güvenliği Ve Kullanıcıların Farkındalık Düzeylerinin İncelenmesİ. A*kdeniz Üniversitesi İktisadi ve İdari Birimler Fakültesi Dergisi*, **(29):** 86-105.

Costa, R. at. all. (2010). Knowledge Management Capabilities Supporting Collaborative Working. Proceedings of the 2nd European Conference on Information Warfare and Security, 29-30 March 201-207.

Davenport, T., and Prusak, L. (2001). İş Dünyasında Bilgi Yönetimi. Rota Yayınları, 2. Baskı, İstanbul, Türkiye, Çevirmen :Günhan GÜNAY

Demirtaş, H. (2013). Bilgi Güvenliği Yönetiminin Gerekleri Ve Başarı Dayanakları: Bir Uygulama Örneği. Yüksek Lisans Tezi, Sakarya Üniversitesi, Sosyal Bilimler Enstitüsü, Sakarya.

Doğan, K., ve Arslantekin, S. (2016). Büyük Veri: Önemi, Yapısı ve Günümüzdeki Durum. *DTCF Journal Dergisi,* 15-36, DOI: 10.1501/Dtcfder_0000001461.

Dülger, M.V. (2018). Bilişim, Kişisel Verilerin Korunması ve İnternet İletişimi Mevzuatı. Seçkin Yayıncılık, 4. Baskı, Ankara, Türkiye.

Eken, H. (2013). Mobil ve Web uygulamalarının Yazılım Güvenliği. 15. Akademik Bilişim Konferansı, Akdeniz Üniversitesi, Antalya, Türkiye 23-25 Ocak 2013, 513-518.

Eminağaoğlu, M., ve Gökşen, Y. (2009). Bilgi Güvenliği Nedir, Ne Değildir, Türkiye' de Bilgi Güvenliği Sorunları ve Çözüm Önerileri . *Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi ,* **11:** 01-15.

Erdoğmuş, A. (2017). Üniversite Öğrencilerinin Bilgi Güvenliği Kazanimlarinin, Farkindaliklari Üzerindeki Etkilerinin Analizi: Afyon Kocatepe Üniversitesi Örneği. Yüksek Lisans Tezi, Afyon Kocatepe Üniversitesi, Fenbilimleri Enstitiüsü, Afyon.

Ertuğrul, İ., ve Keskin, N. (2012). İnternet'İn Türkçenin Kullanımında Ve Toplum-Birey Yapısının Değişimindeki Rolü. Doğu Akdeniz Üniversitesi, Bilgisayar ve Teknoloji Yüksek Okulu, Mesleki Eğitim Sempozyumu, **3:** 80-88.

Ganbat, O. (2013). Bilgi Güvenliği Yönetim Sistemi ISO/IEC 27001 ve Bilgi Güvenliği Risk Yönetimi ISO/LEC 27005 Standartlarının Uygulanması. Yüksek Lisans Tezi, Ege Üniversitesi, fen Bilimleri Enstitüsü, İzmir.

Gül, Z. (2015). Stratejik İstihbarat ve Genel Yanılgılar. *Güvenlik Bilimleri Dergisi,* **4:** 111-132.

Güldiken, N. (2006). Bilginin Elde Edilmesi ve korunmasında Ekonomik İstihbarat Sistemlerinin Rolü. C*umhuriyet Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi,* **7:** 169-182.

Güçlü, N., ve Sotırofskı, K. (2006). Bilgi Yönetimi. *Türk Eğitim Bilimleri Dergisi,* **4:**351-371.

Gülmüş, M. (2010). Kurumsal Bilgi Güvenliği Yönetim Sistemleri ve Güvenliği. Yüksek Lisans Tezi, Yıldız Teknik Üniversitesi, Elektrik Mühendisliği Anabilim Dalı, İstanbul.

Henkoğlu, T. ve Yılmaz, B. (2013). Avrupa Birliği (AB) Bilgi Güvenliği Politikaları, *Türk Kütüphaneciliği,* **27:** 451-471.

Henkoğlu, T. (2017). Kişisel Verilerimiz Ne Kadar Güvende: Bilgi Güvenliği Kapsamında Bir Değerlendirme. *Arşiv Dünyası Dergisi,* **17:** 46-56.

Irzık, G. (2002). Bilgi Toplumuna Geçiş: Sorunsallar, Görüşler, Yorumlar, Eleştiriler ve Tartışmalar. *Türkiye Bilimler Akademisi Yayınları*, **3:** 57-62.

Kara, İ. (2015). Türkiye'de Zararlı Yazılımlarla Mücadelenin Uygulama ve Hukuki Boyutunun Değerlendirilmesi. *Akademik Bakış Dergisi,* **52:** 87-98.

Karaaslan, E. (2013). Siber Güvenlik Deneyleri için Ağ Benzetici ve Ağ Sınama Ortamlarının Kullanımına Dair Ön İnceleme . *Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi,* 1-7.

Karadağ, M., ve Abuhanoğlu, H. (2015). Sosyo-Kültürel Özelliklerin Bilgi Güvenliği

Farkındalığı Üzerine Etkisi: Gülhane Askeri Tıp Fakültesi Eğitim Hastanesinde Bir Çalışma. *International Journal of Social Science*, Doi : 10.9761/ JASSS288436, **36:** 379-386.

Keser, H., ve Güldüren, C. (2015). Bilgi Güvenliği Farkındalık Ölçeği Geliştirme Çalışması. Kastamonu Üniversitesi, *Eğitim Dergisi,* **23:** 1167-1184.

Koç, S. ve Kaynak, S. (2009). Yeni Medya Olarak İnternet ve Hukuki Kişisel Güvenlik. 14. Türkiye'de İnternet Konferansı Bildirileri, İstanbul Bilgi Üniversitesi, Türkiye, 12-13 Aralık, 89-96.

Mart, İ. (2012). Bilişim Kültüründe Bilgi Güvenliği Farkındalığı. Yayınlanmamış Yüksek Lisans Tezi, Kahramanmaraş Sütçü İmam Üniversitesi, Fen Bilimleri Enstitüsü, Kahramanmaraş.

McCarthy, E. D. (2002). Bilgi Kültürü Yeni Bilgi Sosyolojisi. Chivi Yazıları Yayınevi, İstanbul, Çev: A. Figen YILMAZ.

Moody, G.D., Siponene, M., and Pahnila, S. (2018). Toward A Unifield Model Of Information Security Policy Compliance, *MIS Quarterly*, **42:** 285-A22.

Mell, P. and Grance, T. (2011). The Economics of Information Security Investment, Universty of Maryland Institute for Advenced Computer Studies, **5:** 438-457.

Mengüşoğlu, T. (1988). İnsan Felsefesi. Remzi Yayınevi, İstanbul, Türkiye.

Odabaş, H. (2003). Kurumsal Bilgi Yönetimi. *Türk Kütüphaneciliği,* **17:** 357-368.

Özcan, B. (2009). Kurumsal Bilgi Güvenliği ve Cobit. Yüksek Lisans Tezi, Haliç Üniversitesi, Fen Bilimleri Enstitüsü, İstanbul.

Sayarı, N. (2009). Bilgi Güvenliği ve Yönetimi. Türkiye Bilişim Derneği Ankara Şubesi Eğitim Etkinliği. Ankara.

Schmidt, A. H. (2004). Building a mosaic of security for a better world, security matters. USA: Aspatore Books.

Şahinaslan, E., Kantürk, A., Şahinaslan, Ö., ve Borandağ, E. (2009). Kurmlarda Bilgi Güvenliği Farkındalığı, Önemi ve Oluşturma Yöntemleri. 11. Akademik Bilişim Konferansı. Harran Üniversitesi, Şanlıurfa, 11-13 Şubat, 597-602

Tatar, Ü. (2011). Sosyal Mühendislik Saldırıları. 4. Ağ ve Bilgi Güvenliği Sempozyumu TUBİTAK Bilgem, Ankara, 25-26 Kasım.

Tekerek, M. (2008). Bilgi Güvenliği Yönetimi. *KSÜ Fen ve Mühendislik Fakültesi Dergisi* **11:** 132-137

Türk, M. (2003). Küreselleşme sürecinde İşletmelerde Bilgi Yönetimi. Türkmen Kitabevi, 1. Baskı, İstanbul, Türkiye.

Uçak, N. Ö. (2010). Bilgi: Çok Yüzlü Bir Kavram. *Türk kütüphaneciliği,* **24:** 705-722.

Uçak, N.Ö. ve Henkoğlu, T. (2012). Elektronik Bilgi Güvenliğinin Sağlanması İle İlgili Hukuki ve Etik Sorunluluklar. *Bilgi Dünyası Dergisi,* **13:** 377-396.

Uğuz, S., (2018). Kurumsal Bilgi Güvenliği Yönetim Sistemi Yazılımları: Örnek Bir Yazılım Geliştirilmesi. *Uluslararası Yönetim Bilişim Sistemleri ve bilgisayar Bilimleri Dergisi,* **2:** 1-11

Vural, Y. (2007). Kurumsal Bilgi Güvenliği ve Sızma Testleri. Yüksek Lisans Tezi, Gazi Üniversitesi, Fen Bilimleri Enstitüsü, Ankara.

Vural, Y., ve Sağıroğlu, Ş. (2008). Kurumsal Bilgi Güvenliği Ve Standartları Üzerine Bir İnceleme. *Gazi Üniversitesi Mühendislik Fakültesi Dergisi,* **23:** 507-522.

Yavanoğlu, U., Sağıroğlu, Ş. ve Çolak, i. (2012). Sosyal Ağlarda Bilgi Güvenliği Tehditleri ve Alınması Gereken Önlemler. *Politeknik dergisi,* **15:** 15-27.

Yeniçeri, Ö., ve İnce, M. (2005). Bilgi Yönetim Stratejileri ve Girişimcilik. IQ Kültür Sanat Yayıncılık, 1. Baskı, İstanbul, Türkiye.

Yılmaz, E., Şahin, Y. L., ve Akbulut, Y. (2016). Öğretmenlerin Dijital Veri Güvenliği Farkındalığı. *Sakarya Üniversitesi Eğitim Bilimleri Dergisi,* **6:** 26-45.

Yılmaz, F. G., ve Ezin, Ç. Ç. (2017). Ebeveynlerin Bilgi Güvenliği Farkındalıklarının İncelenmesi. *Eğitim Teknolojisi Kuram ve Uygulama Dergisi,* **7:** 41-57.

Yılmaz, M. (2009). Enformasyon ve Bilgi Kavramları Bağlamında Enformasyon Yönetimi ve Bilgi Yönetimi. *Ankara Üniversitesi Dil ve Tarih Coğrafya Fakültesi Dergisi,* **49:** 95-118.

Yılmaz, S., ve Sağıroğlu, Ş. (2013). Siber Güvenlik Risk Analizi, Tehdit ve Hazırlık Seviyeleri. 6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, Ankara, 20-21 Eylül, 158-166.

İnternet Kaynakları

1) https://www2.deloitte.com/content/dam/Deloitte/tr/Documents/technology-media-telecommunications/deloitte-global-mobil-kullanici-anketi-2015-f.pdf, 12.07.2018
2) https://www.chip.com.tr/haber/mcafee-siber-tehdit-raporunu-acikladi_74861.html, 22.08.2018
3) https://www.eset.com/tr/malware, 01.09.2018
4) http://www.guvenliweb.org.tr, 17.10.2018

ÖZGEÇMİŞ

Adı Soyadı	:	Emre TANER
Doğum Yeri ve Tarihi	:	İstanbul, 30.07.1987
Yabancı Dili	:	İngilizce
İletişim (Telefon/e-posta)	:	(0507) 954 6310, emretaner@jandarma.gov.tr

Eğitim Durumu (Kurum ve Yıl)

Lise	:	Süleyman Nazif Lisesi, (1994-2003)
Lisans	:	Konya Selçuk Üniversitesi, Teknik Eğitim Fakültesi, Makine Bölümü, (2004-2007) Anadolu Üniversitesi, İşletme Fakültesi, (2009-2014)

Çalıştığı Kurum/Kurumlar ve Yıl : Jandarma Genel Komutanlığı (2009-Devam)

EKLER

EK 1. Bilgi Güvenliği Farkındalık Düzeyi Belirleme Anketi

I. BÖLÜM

1. Cinsiyetiniz:
( ) Kadın **( )** Erkek

2. Medeni Durumunuz:
( ) Evli ( ) Bekar

3. Yaşınız:
( ) 18-22 yaş **( )** 23-27 yaş **( )** 28-32 yaş **( )** 33-37 yaş
( ) 38-42 yaş **( )** 43 ve/veya yukarısı yaş

4. Eğitim Durumunuz:
( ) İlköğretim **( )** Ortaöğretim (Lise) **( )** Önlisans **( )** Lisans **( )** Lisansüstü

5. Çalıştığınız Birim:
( ) Asayiş **( )** KOM **( )** İstihbarat **( )** Siber Suçlar **( )** Personel

( ) MEBS **( )** Komando-Özel Harekat **( )** TEM
( ) Trafik **( )** Kriminal-OYİ **( )** Diğer (Lütfen Belirtiniz) ……

6. Ünvanınız:

7. Bulunduğunuz Meslekte Ne Kadar Süredir Çalışıyorsunuz?
( ) 1 yıl veya daha az **( )** 2-4 yıl **( )** 5-7 yıl **( )** 8-10 yıl **( )** 11 ve/veya daha fazla yıl

8. Bilgisayar ve Bilgi Güvenliği Seviyeniz?
( ) Hiç **( )** Az **( )** Orta **( )** İyi **( )** Çokiyi

9. Aşağıdaki Cihazlardan Hangisine sahipsiniz?
( ) Akıllı Telefon **( )** Bilgisayar **( )** Tablet PC **( )**E-Book **( )** Hiçbiri

10. Aşağıdaki Cihazlardan Hangisi ile İnternete Bağlanırsınız?
( ) Akıllı Telefon **( )** Bilgisayar **( )** Tablet PC **( )**E-Book **( )** Hiçbiri

II. BÖLÜM

Lütfen aşağıdaki ifadelere ilişkin katılım düzeyinizi ilgili ifadeye ilişkin seçeneğin karşısına "**X**" işareti koymak suretiyle belirtiniz.	**HİÇ KATILMIYORUM**	**AZ KATILIYORUM**	**ORTA DÜZEYDE KATILIYORUM**	**ÇOK KATILIYORUM**	**TAMAMEN KATILIYORUM**
1- Bilgisayarıma kötü niyetli kod (malicious code) bulaşıp bulaşmadığını anlayabilirim.					
2- Kötü niyetli yazılımlara (malware) karşı alınması gereken güvenlik tedbirlerini biliyorum.					
3- Aldatmaca (hoax) nedir biliyorum.					
4- Zincir e-postalara (chain e-mail) karşı nasıl hareket etmem gerektiğini biliyorum.					
5- Bilgisayarımda casus yazılım (spyware) olup olmadığını anlayabilirim.					
6- Bilgisayarıma casus yazılım yüklenmesini engelleme yöntemlerini biliyorum.					
7- Kimlik hırsızlığı (identity theft) nedir biliyorum.					
8- Kimlik hırsızlığına karşı alınması gereken güvenlik tedbirlerini biliyorum.					

9- Sahte virüs koruma yazılımının ne olduğunu biliyorum.					
10- Hizmet aksatrma (Denial of Service - DoS) saldırısı nedir biliyorum.					
11- Kimlik avı (phishing) saldırısı nedir biliyorum.					
12- Sosyal mühendislik (social engineering) saldırısı nedir biliyorum					
13- Sosyal mühendislik saldırısına uğramamak için nasıl hareket etmem gerektiğini biliyorum.					
14- Siber zorbalık (cyberbullying) nedir biliyorum.					
15- Siber zorbalığa karşı kendimi nasıl koruyacağımı biliyorum.					
16- Siber zorbalığa karşı çocuklarımı nasıl koruyacağımı biliyorum.					
17- Bilgi güvenliğinin ne anlama geldiğini biliyorum.					
18- Bilgi güvenliği ile ilgili sorumluluklarımın ne olduğunu biliyorum.					
19- Kullandığım bilgi sistemlerinde tanımlanmış olan kuralları nasıl uygulayacağımı biliyorum.					
20- Bilgi sistemlerinde kullanılan virüs koruma yazılımını nasıl kullanacağımı biliyorum.					
21- Bilgisayarımdaki virüs koruma yazılımının gerçek zamanlı koruma (realtime protection) özelliğini kullanmaktayım.					
22- Bilgisayarımdaki virüs koruma yazılımının otomatik güncelleştirme yapmasını sağlayabilirim.					
23- Dijital imza (digital signature) nedir biliyorum.					
24- Şüpheli veya bilinmeyen kaynaklardan gelen özellikle eklentisi olan e-postaları açmanın taşıdığı riski biliyorum.					
25- E-posta gönderirken "Gizli" (BCC) alanının sağladığı avantajları biliyorum.					
26- İstenmeyen elektronik posta (spam) nedir biliyorum.					
27- İstenmeyen elektronik posta miktarını azaltmak için gerekli bilgiye sahibim.					
28- Sosyal ağ sitelerini (social networking sites) güvenli olarak nasıl kullanacağımı biliyorum.					
29- USB sürücülerini (USB drives) kullanırken dikkat edilmesi gereken hususları biliyorum.					
30- Taşınabilir cihazlara (portable devices) yönelik fiziksel güvenliği sağlamak ile ilgili dikkat edilmesi gereken konuları biliyorum.					
31- Taşınabilir cihazlara yönelik veri güvenliği ile ilgili dikkat edilmesi gereken konuları biliyorum.					
32- Kişisel mahremiyet nedir biliyorum.					
33- Çevrimiçi güvenli alışveriş yapmak için gerekli olan güvenlik tedbirlerini biliyorum.					
34- Mavidiş (Bluetooth) teknolojisi ile veri aktarımı konusunda bilgi sahibiyim.					