T.C.
HASAN KALYONCU ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
İŞLETME ANABİLİM DALI
İŞLETME DOKTORA PROGRAMI

SİBER RİSKLER KARŞISINDA KOBİ'LERİN BİLGİ GÜVENLİĞİ FARKINDALIKLARINI ÖLÇEN BİR ÖLÇEK GELİŞTİRME: GAZİANTEP ÖRNEKLEMİ

DOKTORA TEZİ

HAZIRLAYAN
CÜNEYT ÇATUK

GAZİANTEP - 2018

T.C.
HASAN KALYONCU ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
İŞLETME ANABİLİM DALI
İŞLETME DOKTORA PROGRAMI

SİBER RİSKLER KARŞISINDA KOBİ'LERİN BİLGİ GÜVENLİĞİ FARKINDALIKLARINI ÖLÇEN BİR ÖLÇEK GELİŞTİRME: GAZİANTEP ÖRNEKLEMİ

DOKTORA TEZİ

HAZIRLAYAN
CÜNEYT ÇATUK

TEZ DANIŞMANI
PROF.DR.GÜLÇİMEN YURTSEVER

GAZİANTEP – 2018

KABUL VE ONAY

Cüneyt ÇATUK tarafından hazırlanan **"Siber Riskler Karşısında Kobilerin Bilgi Güvenliği Farkındalıklarını Ölçen Bir Ölçek Geliştirme: Gaziantep Örneklemi"** başlıklı bu çalışma **10/04/2018** tarihinde yapılan savunma sınavı sonucu **başarılı** bulunarak jürimiz tarafından **Doktora Tezi** olarak kabul edilmiştir.

Prof. Dr. Gülçimen YURTSEVER ÇAVAŞ
(Başkan)

Prof. Dr. İbrahim ARSLAN
(Üye)

Dr. Öğr. Üye İbrahim ÇÜTCÜ
(Üye)

Dr. Öğr. Üye Mehmet AYTEKİN
(Üye)

Dr. Öğr. Üye İbrahim AKBEN
(Üye)

Onay
Yukarıdaki imzaların, adı geçen öğretim üyelerine ait olduğunu onaylarım. 10.04.2018

Doç. Dr. Mazlum ÇELİK
Enstitü Müdürü

TEZ ETİK VE BİLDİRİM SAYFASI

Doktora Tezi olarak sunduğum **"**Siber Riskler Karşısında Kobi'lerin Bilgi Güvenliği farkındalıklarını ölçen bir ölçek geliştirme: Gaziantep örneklemi**"** başlıklı çalışmanın tarafımca, bilimsel ahlak ve geleneklere aykırı düşecek bir yardıma başvurmaksızın yazıldığını ve yararlandığım eserlerin kaynakçada gösterilenlerden oluştuğunu ve bunlara atıf yapılarak yararlanmış olduğumu belirtir ve onurumla doğrularım. 10/04/2018

Cüneyt ÇATUK

ÖNSÖZ

Günümüz bilgi dünyasında görülen iletişim teknolojilerindeki hızlı gelişmeler ve değişimler uluslararası alanda ticari ilişkilerin de hızla gelişmesini sağlamaktadır. Kobilerin her geçen gün değişen ve gelişen iletişim araçlarını kulanırken karşılaşabilecekleri sorunlar da bu oranda artmıştır. Bu çalışmada geliştirilen ölçekle Kobilerin karşılaşabilecekleri bilgi güvenliği tehditlerine karşı farkındalıkları ölçülmeye çalışılmıştır. Bu çalışmayı sonuçlandırmamda görüşleri ile katkıda bulunan değerli hocam Prof. Dr. Gülçimen Yurtsever'e, bütün eğitim hayatım boyunca arkamda duran değerli annem Münevver ÇATUĞ'a sonsuz teşekkür eder, çalışmanın tüm ilgililere yararlı olmasını dilerim.

Gaziantep, 2018 Cüneyt Çatuk

ÖZET

Globalleşen dünya ve İnternet teknolojisinin sağladığı avantajlardan sonra KOBİ'ler bölgesel şirketler olmaktan çıkıp global firmalar haline geldiler. İnternetin ve globalleşmenin sağladığı bu avantajlar aynı zaman da KOBİ'ler için yeni tehditlerin oluşmasına neden oldu. Bu nedenle, bu çalışma KOBİ'lerin bilgi güvenliği farkındalıklarını ölçmek için bir ölçek geliştirilmesi amacıyla yürütülmüştür.

Bu ölçeğin İçerik/Kapsam geçerliği, Ölçüt-Bağımlı Geçerliliği ve Yapı Geçerliliği ispatlanmıştır. İç tutarlık Güvenirliği için Cronbach alfa katsayısı kullanılmıştır. Keşfedici ve Doğrulayıcı Faktör analizi yapılmıştır.

Ölçekte 37 madde bulunmaktadır. Veriler Gaziantep'te farklı sektörlerde faaliyet gösteren 800 KOBİ çalışanın anket sorularına verdikleri cevaplardan elde edilmiştir.. Araştırma sonuçlarına göre bu ölçeğin dört alt boyutu vardır. Dört alt boyutun toplam varyansın %67,33'ünü açıklamıştır.

Çalışmanın önemi KOBİ çalışanlarının çalıştıkları firmalarda bilgi güvenliği ile ilgili farkındalığın algılanmasını ölçmeye yönelik yeni, geçerli ve güvenirliği olan bir ölçek olmasıdır. Bu ölçek KOBİ'lerin bilgi güvenliği ile ilgili üzerinde durulması gereken hususlara yardımcı olabilir.

Anahtar sözcükler: Farkındalık, bilgi güvenliği, KOBİ, ölçek

ABSTRACT

After the advantages provided by the globalizing world and Internet technology, the Small and Medium Enterprises(SMEs) have become global companies from being regional companies. In addition to this advantage provided by the Internet and globalization, it also caused some risks for SMEs. For this reason, this study was conducted to develop a scale to measure the awareness of information security of SMEs.

Content / Scope validity, criterion / related validity and construct validity of this scale have been proven. Exploratory factor analysis and confirmatory factor analysis were utilized for the construct validity, and Cronbach's alpha coefficient was used for internal consistency reliability.

There are 37 items on the scale. The data were obtained from the answers of 800 SMEs employees working in different sectors in Gaziantep to the questionnaire survey. According to the results of the research, this scale has four sub dimensions. Four sub-dimensions explain 67.33% of the total variance.

The importance of the study constucted a new, valid and reliable scale to measure the perception of information security awareness in firms where SMEs employees are working. The result of this study may help to develop a better understanding of where SMEs need to focus information security concerns.

Key words: Awareness, information securities, SMEs, scale

İÇİNDEKİLER

TABLOLAR LİSTESİ

Sayfa No.

ŞEKİLLER LİSTESİ

Sayfa No.

KISALTMALAR LİSTESİ

ABD	**:**	Amerika Birleşik Devletleri
AFA	**:**	Açıklayıcı Faktör Analizi
DFA	**:**	Doğrulayıcı Faktör Analizi
E-Ticaret	**:**	Elektronik Ticaret
KMO	:	Kaiser-Meyer-Olkin Katsayı Değeri
KOBİ	**:**	Küçük ve Orta Büyüklükteki İşletmeler
NRD	**:**	Teslimatin Reddedilmemesi
NRR	**:**	Makbuzun Reddedilmemesi
OECD	**:**	Ekonomi Kalkınma ve İşbirliği Örgütü
RMIAS	**:**	Reference Model of Information Assurance and Security

BİRİNCİ BÖLÜM

GİRİŞ

Küreselleşme ve internetin sağladığı avantajlar sayesinde, küçük ve orta büyüklükteki işletmeler (KOBİ)'ler bölgesel firma olmaktan çıkıp, uluslararası pazarda faaliyet gösteren firmalar haline gelmiştir (Boateng ve Osei, 2013: 1). KOBİ'ler küreselleşmenin sunduğu üstünlükle stratejik pazarlarda faaliyet göstermek için teknolojiyi çok iyi kullanmaktadır. Bu eğilim birçok fırsatla birlikte bazı riskleri de beraberinde getirmiştir. Bu risklerden en önemlisi de siber tehlikedir (Duda, 2016: 16).

Siber güvenlik açıkları iş dünyasında çok ciddi boyutlarda tehdit oluştururken, KOBİ'ler genellikle bu saldırıların en büyük mağdurları olmaktadır. Yaşanan saldırılar KOBİ'lerde gelir kaybına, müşteri güven kaybına ve yatırımcı güveninin azalmasına neden olmaktadır. Bunun yanı sıra Firrma çalışanlarının yeterli farkındalığa sahip olmadığı, farkına varmadan verebilecekleri güvenlik açıkları çalıştığı kurumları istemedikleri halde büyük tehditlerle karşı karşıya getirebilmektedir (TÜSİAD, 2017). Bunun sonucunda ise yapılan saldırıların büyüklüklerine göre de KOBİ'ler iflas etme olasılığıyla karşı karşıya kalmaktadır (Boateng ve Osei, 2013: 23). Firmalar her ne kadar siber tehditler karşısında önlem alıp savunma sistemlerini geliştirmiş olsalar da, hiçbir zaman karışılacakları tehditlerin tamamını ortadan kaldıramamaktadırlar (Charney, 2010: 12).

Her dönemde Türkiye ekonomisi üzerinde etkisini sürdüren KOBİ'lerin etkisinin 1950'li yıllara kadar ekonomide fazla bir etkiye sahip olmadığı ve sadece tüketici ihtiyaçlarını karşılayabilecek durumda oldukları görülmektedir. 80'li yıllara kadar bu durum bu şekilde devam etmiştir. Ancak 80'lerden sonraki dönemde özellikle Avrupa Birliği'ne uyum sürecinde yaşanan gelişmeler KOBİ'lerin küreselleşen dünyada ve diğer rekabet

ekonomilerinde önemli bir yere sahip olduğunu hissettirmiştir (Küçük, 2005: 12). Türkiye Cumhuriyet Kalkınma Bakanlığı tarafından, ilki 1963'te daha sonra da her beş yılda bir yapılan ve hala günümüzde devam eden kalkınma programları, Türkiye'de sanayiyi geliştirmek ve desteklemek için çeşitli yapılar oluşturmuştur. Bu kalkınma programları sonucunda Küçük Sanayi Geliştirme Merkezi Genel Müdürlüğü, Küçük ve Orta Ölçekli İşletmeleri Geliştirme ve Destekleme İdaresi Başkanlığı , Küçük Sanayi Geliştirme Teşkilatı Genel Müdürlüğü adında yeni kurumlar kurulmuştur. Bu kurumlar KOBİ'leri ekonomik, teknolojik ve idari anlamda desteklemeyi amaçlamıştır.

Dünya Bankası tarafından hazırlanan "Türkiye'de KOBİ'lerin Önemi ve Emeği" adlı araştırmada, KOBİ'lerin Türkiye'nin GSYH'nin %85'ini oluşturduğu; Türkiye'de artan KOBİ yatırımlarının yeni iş fırsatları oluşturulmasında önemli bir etkiye sahip olduğu belirtilmektedir. Bundan dolayı da KOBİ'ler, Türkiye'de oluşturduğu üçte ikilik oranındaki iş imkanıyla, işsizdik oranın azalmasına neden olmuştur (Apak ve Atay, 2014: 150).

Sayısal verilere dayandırıldığında KOBİ'lerin Türk ekonomisi açısından önemi daha da belirgin hale gelmektedir. Türkiye'deki işletmelerin %99.77'u KOBİ'ler tarafından oluşturulmaktadır (Bilim, Sanayi ve Teknoloji Bakanlığı, 2016). Toplam istihdamın %78'i, toplam satışların %65'i ve aynı zamanda ekonomik katma değerin %55'i KOBİ'ler tarafından oluşturulan girişimler sayesinde gerçekleşmektedir (Bilim, Sanayi ve Teknoloji Bakanlığı, 2016). Bu nedenle KOBİ'ler, Türkiye ekonomisinin lokomotifi olarak görülebilir.

1.1. Problemin Tanımı ve Tarihçesi

Kuzey Atlantik Antlaşma Örgütü dergisi (2006) tarafından yapılan araştırmaya gore, ilk önemli siber saldırı, 1988 yılında Morris solucanı olarak adlandırılan virus tarafından gerçekleştirilmiştir. Bu virüs Unix işletim sistemindeki açığı kullanarak bilgisayarların yavaşlamasına neden olduktan sonra sistemi kullanılamaz hale getirmiştir.

Firmalara ve bilgisayar kullanıcılarına yönelik önemli siber saldırıların bazılarının kronolojik sıralaması aşağıda verilmiştir:

2001 yılında ilk ortaya çıktığında Codered solucan yazılımı her 37 dakikada çoğaltılarak toplamda 2 milyar dolar ($) zarara yol açmıştır (Hovay ve D'Arcy, 2004: 97).

2003'te ilk kez ortaya çıkan Blaster solucanı ilk başlarda yarım milyon bilgisayara zarar vermiş ve işletme başına 475 bin dolar kayıp verdiği açıklanmıştır (Hovay ve D'Arcy, 2004: 121).

2007 yılında Estonya' da yapılan siber saldırı sonucu bankacılık işlemleri, devlete ait internet siteleri ve haber portalları gibi başlıca internet hizmetleri kullanılamaz hale gelmişti (TÜSİAD, 2017).

Amerika'nın perakende devi Target firmasına 2013 yılında yapılan hacking saldırısı şu ana kadar yapılan en büyük siber saldırı olarak tarihe geçmiştir ve 40 milyon müşterinin kredi kartı bilgileri çalınmıştır. Bu olay sonucunda Target ve Visa firmaları zarar gören müşterilerine 67 milyon dolar verme taahhüdünde bulunmuştur (Isidore, 2015).

Büyük firmalar son yıllarda karşılaşabilecekleri saldırılardan korunmak için, güvenlik sistemlerini daha güçlü hale getirmektedirler. Küçük firmalar ise sahip oldukları bütçe darlıklarından dolayı gerekli tedbirleri almadıkları için büyük firmalara kıyasla daha kolay hedef haline gelmektedir. Pierre'e (2008) göre, KOBİ'lerin çoğu altyapılarında barındırdıkları bilgilerin, siber suçluların ilgi alanlarını kapsadığının farkında değillerdir. Firmaların;

çalışanları, kendi müşterileri ve satıcılarla ilgili topladığı bilgiler, siber suçluların ilgi alanına girmektedir. Siber saldırılarla ilgili olarak E-Ticaret müşterilerinin internet üzerinden yaptıkları işlemlerde siber saldırılara karşılaşma ihtimallerinin olduğu belirtilmektedir (Pierre, 2008). KOBİ'ler bu sitelere detaylı kişisel bilgileri verdikleri için bu durum siber tehdit oluşturabilmektedir. E-Ticaretin hızlı yayılması ve bağlantı ağlarının artması sonucunda karşılaşılabilecek olası saldırı oranı da artmaktadır (Sharma, Kunal, Singh ve Prakash, 2009: 39). Yapılan bir araştırmada 2014 yılında küçük işletmelerin % 60 'ı siber saldırılarla karşı karşıya kaldığı belirtilmektedir. (Government UK, 2015: 3) . Başka bir çalışmada ise Siber saldırıların %71'i çalışan sayısı 100'ün altında olan küçük işletmelerin başına geldiği ifade edilmektedir (Sorrentino, 2015).

Planque'a (1988) göre, bilgi edinme araçları, kişilerin, resmi olmayan ilişkileriyle kurumsallaşmadan, piyasada olan olayları bilgi edinme şeklidir. Günümüzde KOBİ'ler iletişim kurmak için, standart ve belirlenmiş iletişim kaynaklarını kullanmaya başlamışlardır. Fatura ve hassas dokümanlar e-mailler tarafından gönderilmekte, görüşmeler Skype üzerinden yapılmakta, resmi ve resmi olmayan görüşmeler Messenger vs. üzerinden yürütülmektedir. Önemli iş görüşmelerinin elektronik ortamda görüşmeye başlanmasından itibaren, bilgilerin gizliliği ya da bilginin korunması, bütünlüğün ve sürekliliğin sağlanması gerekmektedir (Planque, 1988). Bu tehditler her geçen gün daha artmakta ve durum daha karmaşık hale gelmektedir. Siber tehditler karşısında oluşacak olayların önüne geçmek için anında önlem alınması gerekmektedir. Bunun içinde çalışanların karşı karşıya kaldıkları bu tehditlerin farkında olması gerekmektedir (LeClair ve Keeley, 2015: 38).

Siber saldırılar ile ilgililerin farkındalıkların ölçülmesi çok önem arz etmektedir. Leclair ve Keeley'e (2015) göre, doğrudan güvenliğin geleceğini etkileyen alanlarda, bilinci geliştirmek ve farkındalığı arttırmak önemlidir. Geliştirilen bu farkındalık ölçeği ile siber

saldırılara karşı yapılacak eğitimde, çalışanların konu ile ilgili farkındalığını ölçmeye yardımcı olmakta ve eğitimin amacına ulaşılmasını kolaylaştırmaktadır.

Çalışmada öncelikle KOBİ'lerin tanımı, genel yapısı ve önemiyle ilgili bilgi verilecek ve Siber Tehditler ve Siber tehditlerin boyutları konusuna değinildikten sonra da KOBİ'lerin Siber saldırılarla ilgili farkındalıklarını ölçebilmek için Gaziantep ilinde faaliyet gösteren KOBİ'lere anket yapılacaktır. Sonuç bölümünde de KOBİ'lere önerilerde bulunulacaktır.

1.2. Araştırmanın Konusu

Bu çalışmada, Türkiye'de faaliyet gösteren KOBİ'ler üzerinde odaklanıp firmaların bilgi güvenliği farkındalıklarını ölçebilmek için Gaziantep ilinde faaliyet gösteren KOBİ'lerden elde edilen veriler kullanılarak ölçek geliştirilecektir.

1.3. Araştırmanın Amaçları

Bu araştırmanın üç amacı bulunmaktadır:

i. KOBİ'lerin karşılaşabilecekleri siber tehditlerle ilgili bilgi farkındalıkları araştırmak.

ii. Bu farkındalığı ölçmek için ölçek geliştirmek.

iii. KOBİ'lerin bilgi güvenliği farkındalıklarıyla ilgili zayıf ve güçlü noktalarını görebilmelerini sağlamak için ölçek geliştirmek

1.4. Araştırmanın Önemi

Hewlett Packard Entreprise (2016) tarafından 2012 yılından itibaren yapılan çalışmada, son üç yılda haftalık başarılı siber saldırı sayısı ortalamasının 50'den 102'ye çıktığı, ortalama saldırılardan kurtarma süresinin 14 günden 24 güne çıktığı, yıllık ortalama kayıp maliyetinin ise 6,5 milyon dolardan 8,9 milyon dolara çıktığı belirtilmiştir. Bu tehditler ile mücadele etmek işletmelerin günlük sorumlulukları arasında yer almaktadır. Genellikle küçük kuruluşlar kaynak yetersizliği ya da farkındalık eksikliği nedenlerinden dolayı kendilerini güvence altına almaları çok zordur (Sorrentino, 2015). Bu etkenlerden içerisinde farkındalık her zaman daha etkin ve erken tedbir alınması konusunda ön plana çıkmaktadır (Wilson veHash, 2003: 9). Farkındalığın belirsizliği azaltması nedeniyle örgütlerin gerek ağ gerekse kullanımlar ilgili çalışanları bilgilendirmesi önemlidir (Bisson, 2015: 8) .

KOBİ'lerin yaşanan saldırılar sonucunda gelir kaybına, müşteri güven kaybına, yatırımcı güveninin azalmasının yanı sıra yapılan saldırıların büyüklüklerine göre de iflas etmeye kadar gidebilmektedir (Boateng ve Osei, 2013: 115). Bu düzeyde önemli bir konu üzerinde KOBİ'lerin karşılaşabilecekleri siber tehditlerle ilgili farkındalıkları araştırması bakımından bu çalışma önem taşımaktadır.

1.5. Araştırmanın Kapsamı

Bu çalışmanın kapsamı Gaziantep ilinde faaliyet gösteren firmaların Siber tehditlere karşı farkındalıklarını ölçmeye yönelik geçerliliği ve güvenirliliği olan bir ölçek geliştirmektir. Bu ölçek Kobilerin bilgi güvenliği farkındalıklarını ölçebilmek için aşağıdaki başlıca boyutları kapsayacaktır:

i. Erişebilirlik
ii. İzlenebilirlik ya da Kayıt Tutma
iii. Kimlik Sınaması
iv. Bilginin Erişebilirliği
v. Bilgi Bütünlüğü
vi. Gizlilik
vii. İnkar Edememe
viii. Mahremiyet

1.6. Araştırmanın Yöntemi

Araştırmada KOBİ'lerin siber riskler karşısında farkındalıklarını ölçebilmek için ölçek geliştirilecektir. Bu araştırmanın Gaziantep ilinde yapılmasının nedeni kolay örneklemenin yanında Gaziantep'te faaliyet gösteren KOBİ'lerin Türkiye ekonomisinde büyük bir öneme sahip olmasıdır. Veriler ölçek geliştirmeye esas olarak güvenilirlik, geçerlilik ve kapsam doğrultusunda özenle toplanacaktır. Ayrıca, teorik ve kurumsal bilgilere ulaşmak için kaynak tarama yönteminden de faydalanılacaktır.

1.7.Tanımlar

Araştırma konusuyla ilgili araştırmada kullanılan ve araştırma içeriğini açıkça yansıtan anahtar niteliğindeki kavramlar aşağıda tanımlanmıştır.

KOBİ: Mikro işletmeler çalışan sayısı 9'dan az Yıllık net Satış hasılatı ve Yıllık Mali bilanço değeri 1 milyon TL'den az, Küçük işletmeler çalışan sayısı 10 ile 49 arasında değişen, Yıllık Net Satış Hasılatı ve Yıllık Mali Bilanço Değeri 5 milyon TL'den az olan ve son

olarak Orta ölçekli işletmeleri çalışan sayısı 50 ile 249 arasında olan yıllık net satış hasılatı ve yıllık mali bilanço değeri 40 milyon TL'den az olan firmalardır (KOSGEB, 2012).

Rekabet: Belli bir alanda faaliyet gösteren farklı kişi veya kuruluşların karşılıklı mücadeleleridir (Şağbanşua, 2006: 2).

Siber Tehdit: Firmaların varlıklarının ya da önemli bilgilerinin zarar görmesiyle sonuçlanabilecek herhangi bir tehdittir (Boateng ve Osei, 2013: 9).

Tehdit: "Bir sistemin veya kurumun zarar görmesine neden olan istenmeyen bir olayın arkasındaki gizli neden" olarak tanımlanabilir (Anonim, 2003). Tehditler sistemlerdeki güvenlik açıklarından doğar. Bu nedenle kurumlar sistemlerine yönelik tehditerin neler olduğunu bilmelidirler (Tekerek, 2008).

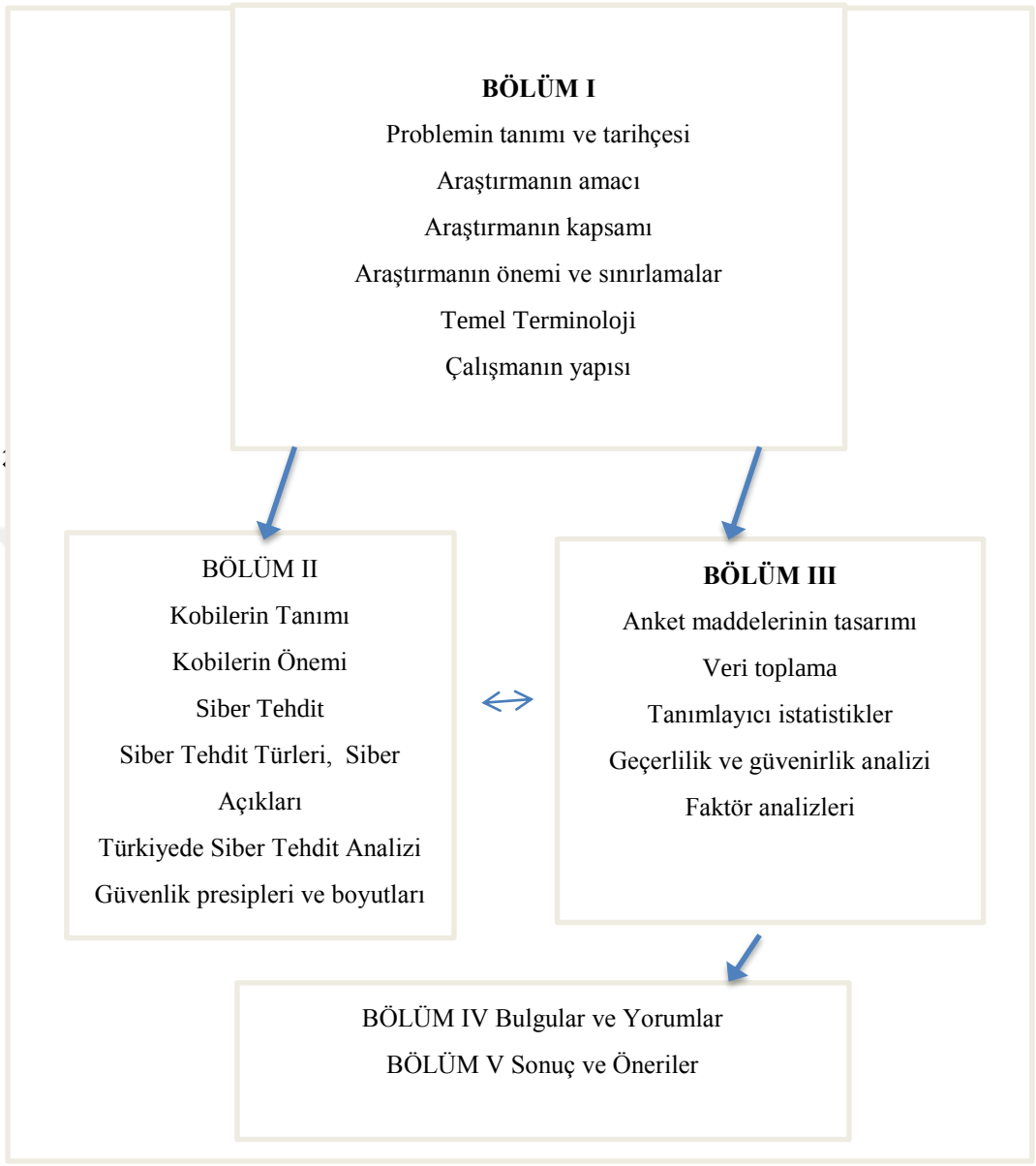
Siber Güvenlik: Siber ortamda, kurum, kuruluş ve kullanıcıların varlıklarını korumak amacıyla kullanılan araçlar, politikalar, güvenlik kavramları , güvenlik teminatlari, kılavuzlar, risk yönetimi yaklaşımları, faaliyetler, eğitimler, en iyi uygulamalar ve teknolojiler bütünüdür (Atalay, 2014).

Varlık: Varlık bir kişi veya kurumun sahip olduğu madi veya manevi değer içeren ve bu nedenle de korunması gereken tüm öğeler olarak tanımlanır (Örnek kurumdaki bilgisayarlar, tabletler, evraklar, personeller vb.).

Bilgi Güvenliği: "Bilginin bir varlık olarak hasarlardan korunması, doğru teknolojinin, doğru amaçla ve doğru şekilde kullanılarak bilginin her türlü ortamda, istenmeyen kişiler tarafından elde edilmesi olarak" tanımlamaktadır (Canberk ve Sagıroglu, 2006: 165) .

1.8. Çalışmanın yapısı

Tez dört bölüme ayrılmıştır. Bölümde I'de problemin tanımı, amacı, kapsamı, önemi sınırlılıkları ve araştırmanın temel terminolojisi açıklanmıştır. Bu bölüm tezin bundan sonraki bölümlerine esas oluşturmuştur. Bölüm II'de KOBİ'ler ve siber saldırılar ile ilgili teori ve uygulamalar tartışılmıştır. Bölüm III'te örnekleme yöntemi ve ölçeğin geliştirilme süreci açıklanmıştır. Faktör analizleri ve hipotez testlerinin sonuçları tartışılmıştır. Bölüm IV'te ise Bulgular ve Yorumlar Bölüm V'de Sonuç ve Öneriler tartışılmıştır.



Şekil 1. Çalışma Olgusunun Temel Bölümleri

İKİNCİ BÖLÜM

LİTERATÜR TARAMASI

2.1. KOBİ'lerin Tanımı

İşletmelerin sınıflandırılması bir çok dayanak esas alınarak yapılmaktadır. KOBİ'ler ise genellikle çalışan kişi sayısına, yıllık gelirine ya da varlık değerlerine göre sınıflandırılmaktadır. Ohalde KOBİ'ler kimlerdir? Ne yaparlar? şeklinde sorularla karşılaşılmakta ve KOBİ'lerin sınıflandırıldığı farklı parametreler olduğu için farklı tanımlar ortaya çıkmaktadır.

İngiltere'de Bolton Konseyi (1971) ekonomik ve istatistiksel olarak KOBİ'leri iki başlık altında toplamıştır. Bolton Konseyi (1971) KOBİ'leri bazı sektörlerde çalışan kişi sayısına, diğer sektörlerde ise yıllık gelirlerine göre sınıflandırmıştır.

Kanada hükümeti, küçük firmalar İstatistiksel raporunda (2013) 1-99 arasında çalışanı olan firmaları Küçük ölçekte firmalar, 100–499 arasında çalışanı olan firmaları ise Orta büyüklükte firmalar olarak kategorize etmektedir.

Avrupa Birliği (2009) ise KOBİ'leri çalışan sayısıyla birlikte gelir ve varlıklarına göre de sınıflandırmaktadır. Küçük firmaları, 50 kişiden az, gelirinin ve bilanço toplamının 10 milyon dolara eşit ve daha az olarak tanımlarken; orta büyüklükteki firmaları, çalışanı 250 kişiden az, gelirinin 50 milyon dolara eşit ya da daha az ve bilanço toplamlarının 43 milyon dolardan az olan firmalar olarak tanımlamaktadır. Mikro büyüklükteki firmaları da çalışanı 10 kişiden az, gelirlerinin ve bilanço toplamlarının 2 milyon dolara eşit ya da daha az olan firmalar olarak tanımlamaktadır.

KOBİ'ler, gerek oluşturdukları iş hacimleri, gerekse ekonomiye yaptıkları katkılardan dolayı ülke ekonomilerinde lokomotif görevi yapmaktadır. Bünyesinde 34 ülkeyi barındıran Ekonomi Kalkınma ve İşbirliği Örgütü (OECD) tarafından yayınlanan raporda (2014), OECD ülkelerinde iş imkanlarının %60-%70 oranında KOBİ'ler tarafından oluşturulduğu belirtilmektedir. Özellikle Amerika Birleşik Devletleri (ABD) ve İsveç gibi ülkelerde, iş imkanlarının büyük bir kısmı KOBİ'ler tarafından sağlanmaktadır (OECD, 2014).

Gelişmekte olan ülkelerde, tarım sektöründe faaliyet gösteren firmaların %90'dan fazlasını KOBİ'ler oluşturmaktadır. Bu firmalar Gayri Safi Milli Hasıla'nın önemli bir kısmını oluşturmaktadır. Makro firmalara örnek verecek olursak, Endüstriyel sektörde faaliyet gösteren firmaların %93'ü, Üretim firmalarının %38'i yatırım firmalarının %33'ü ve ihracat şirketlerinin %30'u Kobi'ler tarafından oluşturulmaktadır. Güney Afrika'da KOBİ'lerin ekonomiye desteği önemli ölçüde daha fazladır. Çünkü bu bölgede faaliyet gösteren işletmelerin %91'i ve Gayri Safi Milli Hasıla'nın %57'sini KOBİ'ler oluşturmaktadır. Gana'nın Gayri Safi Milli Hasıla'sının %70'i ve yerli ekonomiye fayda sağlayan firmaların %91'i KOBİ'lerin oluşturması buna örnek olarak verilebilir (Edinburg Grup, 2010: 7).

Türkiye'nin her döneminde KOBİ'lerin etkisini görmek mümkündür. Ancak KOBİ'ler, 1950'li yıllara kadar ekonomide fazla bir etkiye sahip değilken sadece tüketici ihtiyaçlarını karşılayabilecek durumdalardı. 1980'li yıllara kadar bu durum bu şekilde devam etmiş ve 1980'lerden sonraki dönemde özellikle Avrupa Birliği'ne uyum sürecinde yaşanan gelişmeler, KOBİ'lerin globalleşen dünyada ve diğer rekabet ekonomilerinde önemli bir yere sahip olduğunu hissettirmiştir(Küçük, 2005: 199).

Türkiye Cumhuriyeti Kalkınma Bakanlığı tarafından ilki 1963'te yapılan ve daha sonra her beş yılda bir planlanan ve hala günümüzde planlanması ve uygulanmasına devam edilen kalkınma programları, Türkiye'de sanayiyi geliştirmek ve desteklemek için çeşitli

yapılar da meydana getirmiştir. Programların sonucunda Küçük Sanayi Geliştirme Merkez Küçük Sanayi Geliştirme Teşkilatı, Küçük ve Orta Ölçekli İşletmeleri Geliştirme İdaresi Başkanlığı vb. kurumlar oluşturulmuştur. KOBİ'ler de ekonomik, teknolojik ve idari anlamda bu kurumları desteklemeyi amaçlamıştır. Kurumlarla ilgili genel olarak şu bilgi verilebilir:

KÜSGEM, 1973 yılında Gaziantep'te pilot proje niteliğinde küçük ölçekli sanayi işletmelerine ortak kolaylık atölyeleri ile destek vermeye çalışmıştır (KOSGEB, 2008).

KUŞET, Küçük ve Orta Ölçekli İşletmeleri Geliştirme Merkezleri, teknolojiyle üretimin artırılması, işsizlik oranlarının azaltılması, teknik danışmanlık verilmesi ve yönetim becerilerinin arttırılması gibi önemli unsurlar üzerinde durmuştur (KOSGEB, 2008).

SEGEM, KOBİ'lerde yönetici ve çalışanların eğitim ihtiyaçlarını karşılamak için kurulan kuruluştur (KOSGEB, 2008).

Dünya Bankası tarafından hazırlanan Türkiye'de KOBİ'lerin önemi ve Emeği adlı araştırmada, Türkiye'de artan KOBİ yatırımlarının yeni iş fırsatları oluşturulmasında önemli bir payının olduğu belirtilmektedir. Bunun yanı sıra KOBİ'lerin Türkiye'de oluşturduğu üçte iki iş imkanıyla, işsizliğin önüne çekilen en büyük set olarak görebilmektedir. KOBİ'ler aynı zamanda Türkiye GSYİH'nin %85'ini oluşturmaktadır (Apak ve Atay, 2014: 14).

KOBİ'lerin önemi sayısal verilere dayandırıldığında, Türkiye'deki işletmelerin %99.77'si KOBİ'ler tarafından oluşturulmaktadır. Toplam istihdamın %78'i ve aynı zamanda ekonomik katma değerin %55'ini oluşturmaktalar. KOBİ'ler Türk ekonomisinin lokomotifi olarak kabul edilebilir (Bilim, Sanayi ve Teknoloji Bakanlığı, 2016).

2. 2. Siber Tehdit ve Kobiler

Globalleşen dünya ve İnternet teknolojisinin sağladığı avantajlardan sonra, KOBİ'ler bölgesel şirketler olmaktan çıkıp global firmalar haline gelmiştir. İnternetin ve

globalleşmenin sağladığı bu avantajın yanısıra KOBİ'ler için de bazı risklerin oluşmasına neden olmaktadır.

Sharma, Kunal ve Sing'e (2009: 39) göre, Siber saldırılarla ilgili, E-Ticaret müşterilerinin internet üzerinden yaptıkları işlemlerde siber saldırılarla karşılaşma ihtimallerinin olduğu belirtilmektedir. Detaylı kişisel bilgiler verildiği için KOBİ'ler için siber tehdit oluşturabilmektedir. E-Ticaretin hızlı yayılması ve bağlantı ağlarının artması karşılaşılabilecek olası saldırı oranı artırmaktadır. Günümüzde KOBİ'ler İletişim kurmak için, e-mail gibi standart ve belirlenmiş iletişim kaynaklarını kullanmaya başladılar. Fatura ve hassas dokümanlar e-mailler aracılığıyla gönderilmekte, görüşmeler Skype üzerinden yapılmakta, resmi ve resmi olmayan görüşmeler Messenger vs. kullanılarak yapılmaktadır. Önemli iş görüşmelerin elektronik ortamda görüşmeye başlanmasından itibaren, bilgilerin gizliliği ya da korunması, bütünlüğün ve sürekliliğin sağlanması gerekmektedir.

Siber güvenlik açıkları iş dünyasına çok ciddi boyutlarda tehdit oluşturuyorken, KOBI'ler genellikle bu saldırıların en büyük mağdurları olmaktadır ve uğradıkları saldırılar sonucunda kayıplarını geri getirmede çok zorluk çekmektedir. Küçük firmalar büyük firmalardan daha kolay hedef haline gelmektedir. Büyük firmalar, son yıllarda karşılaşabilecekleri saldırılardan korunmak için, güvenlik sistemlerini güçlü hale getirmektedirler.

Pierre (2008) çoğu KOBİ'nin altyapılarında barındırdıkları bilgilerin, siber suçlularının ilgi alanlarını kapsadığının farkında olmamaktadır. Firmaların çalışanları, müşterileri ve satıcılarla ilgili topladığı bilgiler siber suçluların ilgi alanına girmektedir.

Günümüzde ise, işletmeler Siber güvenliğin sağlanmamasının önemi, bu durumun teknik, organizasyonel, ekonomik ve profesyonel maliyeti daha iyi anlaşılmakta ve bir çok yönetici de çok yönlü siber tehditlere karşı kendi şirketlerini korumak için ne yapabileceklerini düşünmektedir (Shackelford, 2016: 5). Siber saldırıların küresel maliyeti

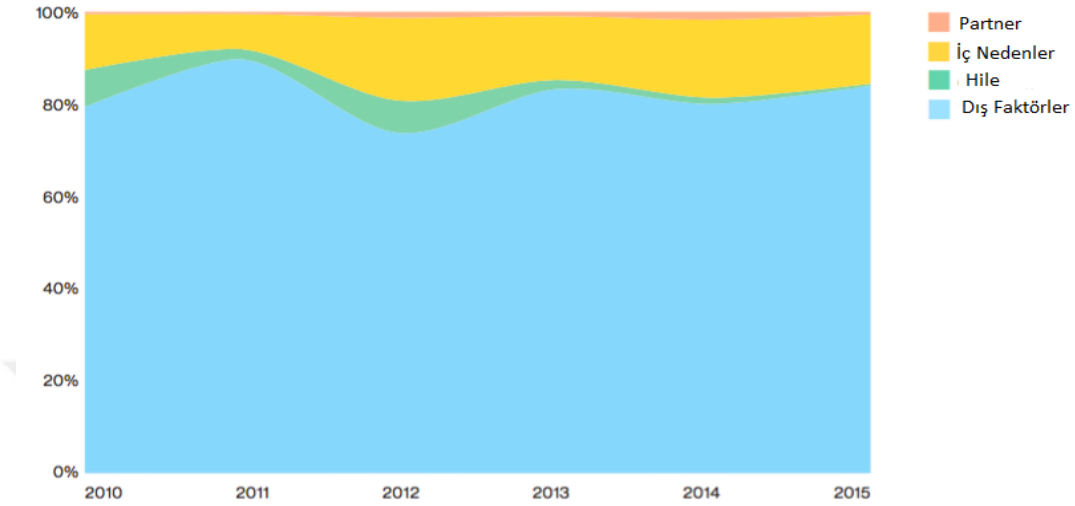
400 milyar dolar ile 2 trilyon dolar arasında değişmekte ve bu oran küresel yasadışı uyuşturucu sektöründen daha büyük maliyet oluşturmaktadır (Studies, 2014: 12). Bu örnek ne kadar büyük bir sorunla karşı karşıya kalındığını göstermektedir. Siber tehdit, bireysel kullanıcılardan organizasyonlara, Michelle Obama'dan Gana'daki bir vatandaşa kadar herkes için problem teşkil etmektedir (Baumhof, 2012). Hissedarlar ya da 3 milyara yakın internet kullanıcısı aynı siber tehdit unsurlarıyla karşı karşıya kalmaktadır (Shackelford, 2016: 5). Değerli fikri mülkiyete sahip firmaların sahip olduğu bu değerlerin her zaman tehdit altında olması buna örnek olarak verilebilir (Mcafee Labs ve Mcafee Fundstone Professional Service, 2010).

2015 yılında yayınlanan Symantec İnternet Güvenlik Tehdidi Raporu verilerine göre, 2014'te yapılan saldırıların %60'ının Kobiler üzerinde yapıldığı belirlenmiştir. 2014 yılında 317 milyon tutarında zararlı yazılım bulunmuş ve bir önceki yıla göre de bu rakamın fidye yazılımlarında %113 gibi bir artış olduğu tespit edilmiştir (Symantec, 2015: 48). Üretim sektörü ise son yıllarda yeni saldırıların hedef noktası haline gelmiştir. Bu yükselişte en önemli unsur üretim tedarik zincirinde yer alan üstlenici ve taşeron firmaların artması gösterilmektedir. Tedarik zincirindeki üstlenici ve taşeron firmalara yapılan saldırılarla ana hedefteki büyük işletmelere ulaşılması amaçlanmaktadır.

2.2.1. Siber Tehdit Açıkları

2016 Verizon tarafından yayınlanan ''Veri ihlalleri Araştırma Raporu''nda, 100.000 üzerinde olay incelendikten sonra veri ihlalleri araştırma raporu yayınlanmıştır. Veri kümesinde 64199 sızma tespit edilmiş ve bu sızmalar incelenerek analiz raporu oluşturulmuştur. Rapor 82 ülkede farklı sektörlerde faaliyet gösteren firmalar üzerinde düzenlenmiştir (Verizon, 2016: 3).

Yayınlanan rapor sonucunda firmalara yapılan saldırılar yıllara göre değişkenlik göstermiş olsa da, saldırıların en çok şirket dışı unsurlardan geldiği tespit edilmiştir (Verizon, 2016: 7).



Şekil 2. Veri İhlallerine Neden Olan Aktörler

Kaynak: Verizon, 2016: 7

2.2.2. Siber Tehdit Kategorileri

Yapılan siber saldırıların çok yönlü olması, bu saldırıların fiziksel olarak yıkıcı bir etki oluşturması şirketler için önemli kayıplara neden olmaktadır (Piggin, 2016: 37). İşletme veya herhangi bir kuruma yönelik oluşabilecek siber tehditler, sisteme yetkisiz erişim, sistemin bozulması veya engellenmesi, bilgilerin değiştirilmesi, yok edilmesi, ifşa edilmesi ve çalınması başlıkları altında toplanabilmektedir (Atalay, 2014).

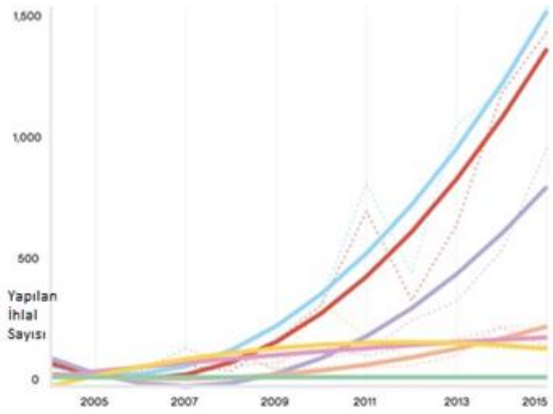
En son ihlallerin saldırganlar tarafından kötü amaçlı yazılımlarla, şirketlerin kontrol sistem yazılımlarına ve endüstriyel yazılımlara ve sistem davranışlarını öğrenmek için protokollere sızdığı görülmektedir. Aynı zamanda araştırmalar, saldırıların kurumsal itibarla birlikte markaya büyük oranda zarar verdiğini göstermektedir (Piggin, 2016: 37).

Ponemon kurumu tarafında 2014 temmuz ayında yapılan Kurumların kritik altyapıları adlı raporda, yapılan saldırıların %39'unun endüstriyel kontrol ağlarına yapıldığı tespit edilmiştir (Ponemon, 2014: 6).

Amerikan Siber Acil Müdahale ekibi (2015) yayınladığı raporda yapılan saldırıların çeşitliliğinin de artığı sıranlamaktadır:

i. Endüstriyel kontrol sistemine girilen yetkisiz kişi girişi
ii. Kontrol araçları ve yazılımlarda kullanılan zero-day cihaz ihlalleri
iii. Network ağlarında bulunana zararlı yazılımlar
iv. Ağ bölgeleri arasındaki yanal hareketler

Verizon (2016) yayınladığı raporda, yıllara göre yapılan saldırı kategorilerinde ise en fazla saldırıların Hackleme ve daha sonra sistemlere sokulan zararlı yazılımlar olduğu ortaya konulmuştur.



Şekil 3. Eylem Kategorilerine Göre Yapılan Saldırı Sayısı

Kaynak: Verizon, 2016: 8

Symantec İnternet Güvenlik Tehdidi Raporu'nda (2016) dünyada siber suç sıralaması belirlenirken kullanılan yöntemler altı başlıkta toplanmaktadır:

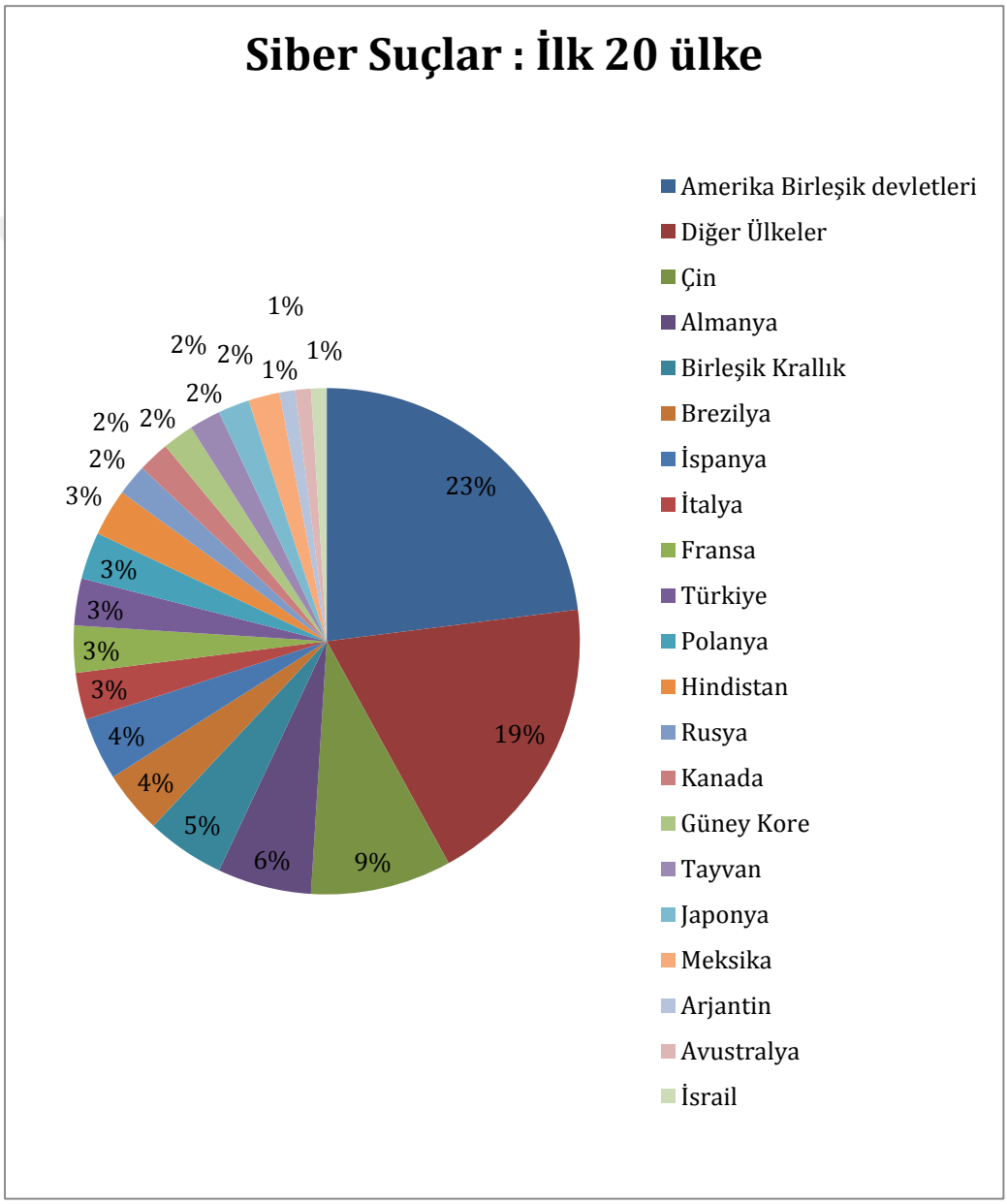
i. Kötü niyetli bilgisayar aktivetesi
ii. Spam zomba

iii. Oltalama website

iv. Bot

v. Saldırı başlangıcı

Şekil 4'de anlaşılacağı üzere Dünyada en çok saldırıya uğrayan ülkeler sıralamasında en başta Amerika Birleşik Devletleri olurken, ikinci sırada Çin yer almaktadır.



Şekil 4. Siber Saldırıların Yapıldığı Ülkeler

Kaynak: Enigma, 2016

2.2.3. Türkiye'de Siber Tehditlerinin Analizi

Symantec İnternet Güvenlik Tehdidi Raporu (2016) zararlı botların ülkelere saldırı sıralamasında Tablo 1'de görüldüğü gibi Çin %46.1 oranla ilk sırada yer almaktadır. Raporda Çin'in gelişen ekonomisinin hedef sıralamasında üst sıralara çıkmasına neden olduğu belirtilmektedir (Symantec, 2016: 60). Türkiye her geçen yıl tehdit sıralamasında üst sıralara çıkmaktadır. Tablo 1'de görüldüğü gibi 2014 yılında Türkiye yapılan bot saldırılarında ilk onda yer almazken, 2015 yılında %29,2 değişkenle dördüncü sırada yer almaktadır (Symantec, 2016: 60). Bu tablodan anlaşılacağı üzere Türkiye'deki firmaların her geçen yıl siber saldırılara maruz kalma riskinin artığı görülmektedir.

Tablo 1. 2015 ve 2014 Yıllarına Göre Ülkelere Yapılan Bot Saldırıları

	2015 Ülke / Bölge	2015 Bot Saldırıları	Bir önceki yıla göre değişkenlik	2014 Ülke / Bölge	2015 Bot Saldırıları
1	Çin	46,10%	84%	Çin	16,50%
2	Amerika Birleşik Devletleri	8%	-64,40%	Amerika Birleşik Devletleri	16%
3	Tayvan	5,80%	-54,80%	Tayvan	8,50%
4	Türkiye	4,50%	29,20%	İtalya	5,50%
5	İtalya	2,40%	-71,20%	Macaristan	4,90%
6	Macaristan	2,20%	-69,70%	Brezilya	4,30%
7	Almanya	2%	-58%	Japonya	3,40%
8	Brezilya	2%	-70,10%	Almanya	3,10%
9	Fransa	1,70%	-57,90%	Kanada	3%
10	İspanya	1,70%	-44,50%	Polonya	2,80%

Kaynak: Symantec, 2016: 60

Enigma Software tarafından yapılan analizde (2016), Türkiye'nin dünyada siber suç sıralaması belirlenirken kullanılan başlıkların sıralamaları Tablo 2'de verilmiştir. Türkiye'nin siber suçların gerçekleştirildiği yöntemlerde Spam ve Zombi sıralamasında ilk beşe girdiği görülmektedir.

Tablo 2. Türkiye Siber Suç Sıralaması

Kötü Niyetli Bilgisayar Aktivitesi	3
Kötü Niyetli Kod Sıralaması	15
Spam Zombi Sıralaması	5
Oltalama Web Site Sıralaması	24
Bot Sıralaması	8
Saldırı Başlangıç noktası	12

Kaynak: Enigma, 2016

Trend Micro şirketinin 2016'nın ilk yarısında gerçekleşen veri güvenliği olaylarını incelediği güvenlik raporunda; fidye yazılımın ülkelere göre dağılımında Türkiye, Avrupa bölgesinde ransomware adı verilen fidye yazılım saldırılarını yaşayan en faza ülke olurken, dünyada sıralamasında üçüncü sırada yer almaktadır.

Bütün bu analizler göz önünde bulundurulduğunda Türkiye'deki firmalar her geçen gün daha fazla riskle karşı karşıya geldiği ifade edilebilir.

2.3. Bilgi Güvenliği

Bilgi güvenliği; verilerin ya da bilgilerin, saklanması ve taşınması sırasında, bütünlüğünün bozulmadan, izinsiz erişimlerden korunması için gösterilen çabaların tümü ya

da bilginin bir varlık olarak hasarlardan korunması, doğru teknolojinin, doğru amaç ile ve doğru şekilde kullanılarak, her türlü ortamda istenmeyen kişiler tarafından elde edilmesinin önlemesi olarak da tanımlanabilir (Canberk ve Sarıoğlu: 174).

Kurumlar bilgi güvenliğinin çözülmesi gereken bir problemden çok yönetilmesi gereken bir işletme riski olduğunu anladılar (Sharma R., 2015: 12). Bu ihtiyaç döngüsü hiç bitmeyen bir iyileştirme olup değişen tehditlere karşı sürekli yenilenmesi gerekmektedir (Sharma R., 2015: 12).

Stratejik yönetim literatürüne göre, bilgi güvenliği e-ticaret için 'değer yaratan' bir olgu olarak görülmektedir (Cavusoglu, 2004: 71). İşletmeler kendi güvenliklerini sağlayabilmelerinin bir çok yolu var. Shackelforda (2016) göre işletmeler riske maruz kalmamak için siber güvenliklerini üç aşamada sağlayabilmektedir:

i. Firmalar sürekli siber riskleri değerlendirmeli ve risk durumlarına göre güvenliklerini tutarlı bir şekilde artırmalı.
ii. İşletmeler fayda maliyet analizi yaptıktan sonra kapsamlı risk azaltma çabasının bir parçası olarak sigorta kapsamını değerlendirmeli.
iii. Firmalar siber güvenlik organizasyonunu diğer firmalarla istişare yaparak analiz etmeli.

Shackhelford (2016) ayrıca şirketlerin en iyi dokuz uygulama ile kendi güvenliklerini sağlayabildikleri belirtilmektedir:

i. Bölüm ağları ve kamu internetinde kısıtlamalar yapılması
ii. NIST Framework kullanılması: 2013 şubat ayında Obama tarafından, kamu ve özel sektörün bilgi paylaşımıyla, uluslararası teknoloji standart kurumu (NIST) firmaların kendi altyapılarını korumaları için en iyi uygulamaları oluşturdu.
iii. Özel ya da kamuya ait siber güvenlik organizasyonlarıyla iletişimde olunması
iv. Yönetici oturum açma şifre vs. daha zorlu hale getirilmesi.

v. Yazılımların otomatik güncellendiğinden emin olunması.

vi. Oluşabilecek tehditlere karşı tedarik zincirindeki unsurların kontrol edilmesi.

vii. Oluşabilecek herhangi bir zarara karşı acil önlem planı ve hukuki boyutlarının göz önünde bulundurulması

viii. Yeni siber güvenlik pratikleriyle ilgili aktif olunması.

Sharma (2015) yönetim kurulu üyelerinin siber riskler karşısında 5 yol ile bilgi güvenliklerini iyileştirebileceklerini belirtilmektedir:

i. ***Siber güvenliğin gündem maddesi olarak oluşturulması:*** Bilgi güvenlik riskinin bütün operasyonel süreci etkilemesinden dolayı, her yönetim toplantısında gündem maddesi olmalıdır. Bu şekilde yöneticilerin desteklendiği görülmektedir.

ii. ***Yönetim yapısının Kontrolü:*** Etkili yönetim, yöneticilerin sahip olduğu deneyim ve yeteneklerden haberdar olmalı, bu sayede yönetim şirketin risk profiliyle orantılı olup olmadığının görülebilmesi, ilerde olası tehditlere karşı, yöneticilerin yeterli gerekliliklere sahip olup olmadığını görmesi açısından önem arzetmektedir.

iii. ***Organize ol, saray mücevherlerini koru:*** Yapılan anketler sonucunda saldırılar, finansal bilgilerin çalınması, fikri mülkiyet ve sahtekarlık ile ilgili şirketin sahip olduğu değerlere karşı yapılmıştır. Kurumlar kendileri için önemli olan varlıkları korumalı (saray mücevherleri). Aşağıdaki soruların şirketler tarafından net cevaplandırılması gerekiyor.

   a. Saray mücevherleri nerede tutuluyor?

   b. Bu bilgiler Çalınırsa ne olur?

   c. İşletmeler kanamayı ne kadar hızlı durdurabilir?

iv. ***Tedbir Etkinliği:*** Uyum, etkili siber güvenliğe denk değildir. Saldırılarla ilgili veriler, yönetim üyelerinin yaşanan tecrübelerden ders çıkartılıp çıkartılmadığına yardımcı olmaktadır. Bunun için aşağıdaki soruların cevaplandırılması gerekmektedir:

   a. İhtiyaç duyulduğunda gerekli kaynaklar kullanılıyor mu?
   b. Zor kararlar ihtiyaç duyulmadan önce alınıyor mu?

   Saldırılarla ilgili veriler aşağıdaki gibi gözlemlenmelidir:

   - Ne kadar saldırı yapıldı?
   - Saldırganlar sistemin hangi kısımlarına ulaşabildi mi?
   - Yönetim yapılan saldırılara ne kadar hızlı reaksiyon gösterdi? Reaksiyon süresi yeterli mi ?
   - Üçüncü şahıslar üzerinde gizli giriş testinin sonuçları nelerdir ?

v. ***İşbirliği yapmanın yolunu bulmak:*** Hükümet ajansları sistemleri sürekli gözetledikleri için, oluşabilen herhangi bir riski organizasyonlara ilk onlar bildirir ya da uyarıda bulunur. Yaşanan sorunları ya da tehditleri, daha büyük işletme topluluklarında dile getirilmesi, bilgi alışverişinde bulunulması işletmelere fayda sağlayabilmektedir.

2.3.1. Bilgi Güvenliği Tehditleri

ISO standartlarına göre işletmelerdeki bilgi güvenliği tehditleri aşağıdaki gibi sıralanmıştır(“The Security Risk Management Guide”, ISO/IEC 27002: 2005, NIST SP 800-30).

i. Sistem Odası:

Şifreli Kapı Girişi: Sunucu sistem odalarında sadece yetkili personelin giriş yapabilmesi

ii. Veritabanı:

a) *Yetkilendirme (Authorization):* Kişilere veritabanı ile ilgili geniş yetki verilmesi (silme, güncelleme vb.),

b) *Veri Girişi* : Yanlış veri girilmesi

c) *Yedekleme (Backup Recovery):* Veritabanı yedeklerinin düzenli alınmaması , olası bir sıkıntıda veri kaybı yaşanma ihtimali

d) *Veri Güvenliği :* Verilerin 3. şahısların eline geçmesi,

e) *Kimlik Tespiti (Authentication):* Hizmeti alan kişinin söylenilen kişi olmaması

f) *Şifre:* Şifrenin 3. kişilerle paylaşılması

g) *Lisansız Yazılım :* Yazılımların lisansız olması ve güncelleme yamalarını almaması

iii. Kullanıcı

a) Kötü Niyet (Sabotaj)

b) *Eğitimsizlik :* Eğitimsiz ve bilinçsiz kullanıcı

c) Şifrenin Paylaşılması

iv. Dış Etkenler

1) Kontrol Edilemeyen

(a) Deprem, Yıldırım, Fırtına, Çığ

(b) Afetler

(c) Terörist Sadırılar

2) Kontrol edilebilir

(a) Hırsızlık

(b) Yangın

(c) Sel

v. Dış Kaynaklar (Outsource)

(a) *Gizlilik :* Hizmet alımı yapılan firmalar ile gizlilik sözleşmelerinin olmaması

vi. Uygulama Yazılımı

a) *İhtiyaçların Eksik Belirlenmesi*

b) *Yavaşlık*

c) *Yama Yönetimi Eksikliği*

d) *Hata ve Uyarı Sistemi Eksikliği*

e) *Kötü Uygulama Yazılımı*

vii. Donanım

a) *Bilgisayarlar*

b) *Bakım Hataları*

c) *Fiziksel Güvenlik Eksikliği*

d) *Sunucular*

e) *Storage (Veri Depolama Ünitesi)*

f) *Yedek Donanımlardaki Eksiklik*

viii. Ağ (Network)

a) *Network Sistem Uzmanı Yetersizliği:* Konunun uzmanı kişilerin kurumlarda istihdam edilmemesi

b) *Yazılım:* Yazılım hataları, yetersizliği

c) *Firewall (Güvenlik Duvarı):* Kurumlarda internet çıkışlarını filtreleyen güvenlik duvarının olmaması, lisansız olması

d) *Intranet:* İç ağdaki, kurum içindeki güvenlik açıklıkları

e) *Altyapı Eksiklikleri*

f) *Donanım:* Yetersiz donanım kullanılması

g) *Şifre:* Şifrenin 3. şahıslar ile paylaşılması

ix. Sistem Yazılımı

a) Lisansız Yazılım

b) *Şifre:* Şifrenin 3. şahıslar ile paylaşılması

c) *Yama Yönetimi Eksikliği:* Güncellemelerin alınamaması

d) *Etki Alanı (Active Directory):* Kullanıcıların bilgisayarlarını kendi kullanıcı adı ve şifreleri ile açmamaları.

Bilgi Güvenliği Yönetim Sistemi‘nde güvenlik planlamasının ilk aşaması risk analizi ile başlar. Risk analizi sistemdeki eksikliklerin ve zayıflıkların tespit edilmesi ve bu nedenle meydana gelebilecek zararların hesaplanması işlemidir. Risk değerlendirmesi ise varlıkların karşısındaki olası tehditler, zayıflıklar, bunların etkileri, olasılıklar ve sonuçta olası risklerin derecesinin veya miktarının belirlenmesidir. Riske değer biçme veya risk değerlendirmesi, belirli bir riskin diğer risklere göre derecesinin ve önceliğinin saptanmasıdır. Risk değerlendirmesi, analiz ve değer biçmenin tamamından oluşan bir süreç olarak tanımlanmaktadır (Peltier, 2001).

2.3.2. Bilgi Güvenliği Farkındalığı

Firmalar bilgi güvenliği riskini minimize etmek istiyorsa, bilgi teknojilerine para harcamadan önce çalışanlarını bilinçlendirmeleri gerekmektedir (Puhakainen, 2006:83).

İnsan faktörüyle ilişkili bilgi güvenlik risklerini tamamen ortadan kaldırmak mümkün olmasa da, iyi organize edilmiş bir farkındalık etkinliği ile güvenlik riskleri minimize edilebilmektedir (Şahinaslan, Kandemir: 2009: 189).

Bilgi ve iletişim teknolojileri ile birlikte gelişen elektronik uygulamalar, iş dünyasında işleyişi kolaylaştırırken yeni güvenlik tehditlerini ve yeni suç tiplerini de beraberinde getirmektedir (Gülmüş, 2010: 99). Son yıllarda bilgi güvenliğine olan ilgi, dünyada olduğu gibi Türkiye’de talep görmekte ve bunla birlikte yapılan araştırmalar da artmaktadır (Keser ve Güldüren, 2015: 1169).

Bilgi güvenliği konusundaki araştırmalar, problemleri ve insan faktörünü göz ardı ederek daha çok teknik yönden ele almaktadır (Chen, Shaw ve Yang, 2006; Kjorvik, 2010; Rezgui ve Marks, 2008). Kurumsal ve kişisel bilgilerin güvenliğini sadece teknik ve güvenlik önlemleriyle (güvenlik duvarı, sanal özel tespit, önleme sistemi, anti virüs, içerik kontrolü

yazılımı, veri şifreleme, kimlik doğrulama, yetkilendirme vb.) sağlamak mümkün değildir (Rezgui ve Marks, 2008). Bunun yanı sıra kurum ve çalışanların güvenlik bilincine sahip olması gerekmektedir. (Keser, Güldüren, 2015: 1170).

Güvenlik teknolojilerinde yaşanan gelişmeler, teknik bakımdan oluşabilecek açıkları minimize ettiğinden dolayı saldırganlar insan unsuru odaklı saldırılar geliştirmeye başlamıştır (Keser ve Gldüren, 2015: 1168). Bundan dolayı kurumlarda güvenliğin en zayıf halkasını insan unsuru oluşturmaktadır (Kritzinger, Smith, 2008: 225). Genel bir söylem olarak "bir zincir, en zayıf halkası kadar güçlüdür" sözü bilgi güvenliği için de geçerlidir (Keser, Güldüren, 2015: 1169).

2.3.3. Bilgi Güvenliği Modellerinin Tarihçesi

Bilgi güvenliği kavramı, bilginin tehditlere karşı uygun şekillerde korunması anlamına gelmektedir (Canberk ve Sagıroglu, 2006: 174). Bilgi güvenliğini "Bilginin bir varlık olarak hasarlardan korunması, doğru teknolojinin, doğru amaçla ve doğru şekilde kullanılarak bilginin her türlü ortamda, istenmeyen kişiler tarafından elde edilmesi olarak" tanımlamaktadır (Canberk ve Sagıroglu, 2006: 175) .

Gizlilik, veri bütünlüğü, erişebilirlik (CIA) onlarca yıl bilgisayar güvenliğinin ve bilgi güvenliğinin modeli olarak kullanılmıştır (Whitman ve Mattord, 2012). CIA modelini ilk olarak 1975 yılında Saltzer ve Shroeder (1975) tarafından bilgiyi tehdit eden üç unsur olduğunu ortaya çıkarmıştır;

i. Yetkisiz kişilerin bilgiye ulaşamaması (Gizlilik)
ii. Yetkisiz kişilerin bilgiyi değiştirememesi (Bütünlük)
iii. Bilgiye ulaşılabilirlik (Erişebilirlik)

CIA modeli ilk olarak 1986-1987 yıllarında Johnson Space Center (2010) ve National Aeronautics ve Space Administration (NASA) tarafından ‘’Bilgi Güvenlik Planı’’ olarak kullanılmıştır. Bu tarihten itibaren CIA modeli popülerliğini artırdı ve günümüzdeki bir çok güvenlik modeli bu temel üzerine oluşturulmuştur (Whitman ve Mattord, 2012) .

CIA’ya alternatif olarak ilk kapsamlı model 1991 yılında Mccumber (1991) tarafından geliştirilmiştir. Bu model Mccumber’in Küpü olarak bilinmektedir. Bu model Milli Eğitim Standardı Bilgi Sistemleri Güvenliği Uzmanları (CNSS 4011) programının bir parçası olarak kullanılmaktadır (CNSS, Committee on National Security Systems: National In- formation Assurance (IA) Glossary, 2010).

Şekil 5. McCumber’in Küpü

Kaynak: Mccumber, 1991

McCumber’in Küpü üç bölümden oluşuyor;

i. Bilginin Durumu (Bilginin Tra, Depolama, İşleme)
ii. Bilginin Karakteristiği (Gizlilik, Bütünlük, Kullanılabirlik)
iii. Güvenlik önlemleri (Teknoloji, Politika ve Pratikler, Eğitim, Farkındalık ve Uygulama).

Maconach (2001) McCumber'in küpüne zaman boyutunu ve güvenlik önlemlerine kimlik doğrulama ve inkar edememeyi de ekleyerek geliştirmiştir.

Parker (1998) Bilgi güvenlik literatürüne altı elementten oluşan yeni bir model önermiştir;

- Kullanılabilirlik (Availability)
- Orijinallik (Authenticity)
- Gizlilik (Confidentiality)
- Tamlık (Integrity)
- İşe yararlık (Utility)
- Sahip olma (Possession)

Parker (1998) CIA modelinin sınırlılığının işaret ederek kendi modelini geliştirdiğini savunmaktadır. Model üç boyuttan oluşmaktadır:

i. Bilgi riskine neden olan eylemler
ii. Bilginin korunması için yapılması gereken kontroller ve pratikler
iii. Bilgi güvenliğinin elementleri

Bilgi sistemleri denetim ve kontrol birliği (ISACA) (2009) bilgi güvenirliği için önerdiği iş modelini dört bölümden oluşturmaktadır;

i. Organizasyon tasarımı ve strateji öğesi
ii. İnsan faktörü
iii. İşlem elementleri
iv. Teknoloji faktörü

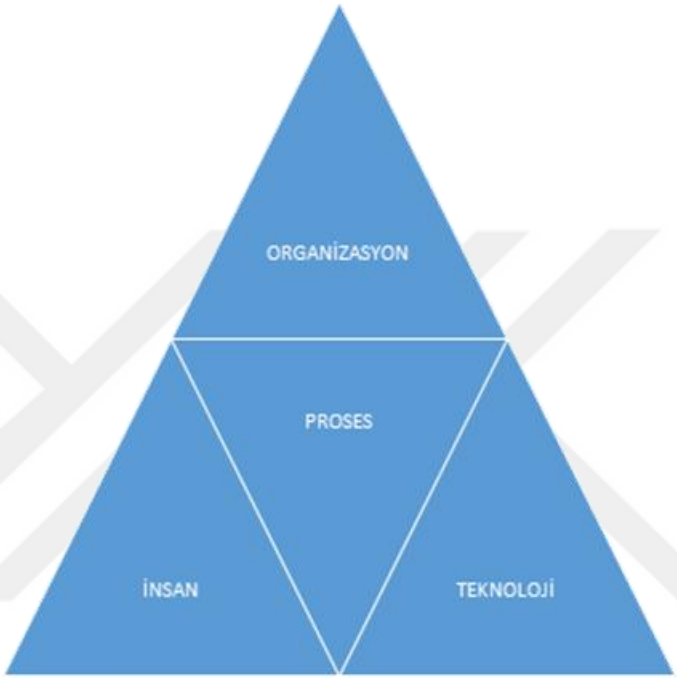
Belirtilen dört maddeyi altı dinamiğe bağlamaktadır;

i. Yönetim,
ii. Kültür,
iii. Etkinleştirme ve destek,

iv. Ortaya çıkışı,

v. İnsan faktörleri,

vi. İnsan faktörü mimarisi.



Şekil 6. Bilgi güvenirliği iş modeli

Kaynak: Jonsson, 2006: 58

Jonsson (2006) güvenlik sistemi giriş ve çıkış açısından kabul edilir bir kavramsal güvenlik modeli sunmaktadır. Jonsson güvenliği ve güvenilirliği entegre bir model önermektedir. Modelin temel amacı, güvenlik konusunda akıl ile yardımcı olmaktır. Yulia ve Jeremy (2013) ‘’Reference Model of Information Assurance & Security’’ adlı modelini oluşturmuştur. RMIAS dört bölümden oluşmaktadır.

i. Bilgi sistem güvenliği yaşam döngüsü

ii. Bilgi taksonomisi boyutları

iii. Bilgi güvenlik boyutları

iv. Karşı güvenlik boyutu

Ölçeğin amacı KOBİ'lerin siber riskler karşısında bilgi güvenliği farkındalıklarını ölçmek olduğundan dolayı, bilgi güvenlik boyutları üzerinde duralmaktadır. Daha önce bahsedildiği üzere CIA güvenlik prensiplerinin temelini oluşturuyordu. Oysa günümüzde CIA gelişen yeni tehditleri kapsayamamaktadır (Cherdantseva, Hilton, Rana ve Ivins, 2013: 57). Güvenlik prensiplerinin boyutlarının geliştirilmesi için Bilgi Güvenliği Literatürü ve Sistem Mühendisliği literatürüyle ilgili yaptıkları araştırmalar sonucunda, günümüz tehditlerini de kapsayan Reference Model of Information Assurance & Security (RMIAS) modelini geliştirmiştir. Güvenlik prensipleri Tablo 15'te detaylı anlatılmaktadır. Yapılan analiz sonuçları literatürde güvenlik prensipleriyle ilgili ortak bir sonuca varılamadığı belirtilmekte ve bu da dört nedene bağlanılmaktadır (Cherdantseva, Hilton, Rana ve Ivins, 2013: 58).

i. Aynı konuların farklı başlıklar altında sınıflandırılması

ii. Aynı isimle tanımlanmış güvenlik prensiplerinin farklı şekilde açıklanması

iii. Güvenlik prensiplerinin ayırt edici özelliklerinin olmaması

iv. Güvenlik prensipleriyle ilgili verilen maddelerin nitelik eksikleri (Bütünlük, sistem bütünlüğü ya da bilgi bütünlüğünü kapsayabilmektedir)

Yukarda bahsedilen nedenlerden dolayı güvenlik prensipleriyle ilgili literatürde ortak bir görüş olmadığından dolayı, Yulia ve Jeremy (2013) tarafından aşağıda belirtilen yol haritası sonucunda güvenlik prensiplerini yeniden tanımlandırılmıştır:

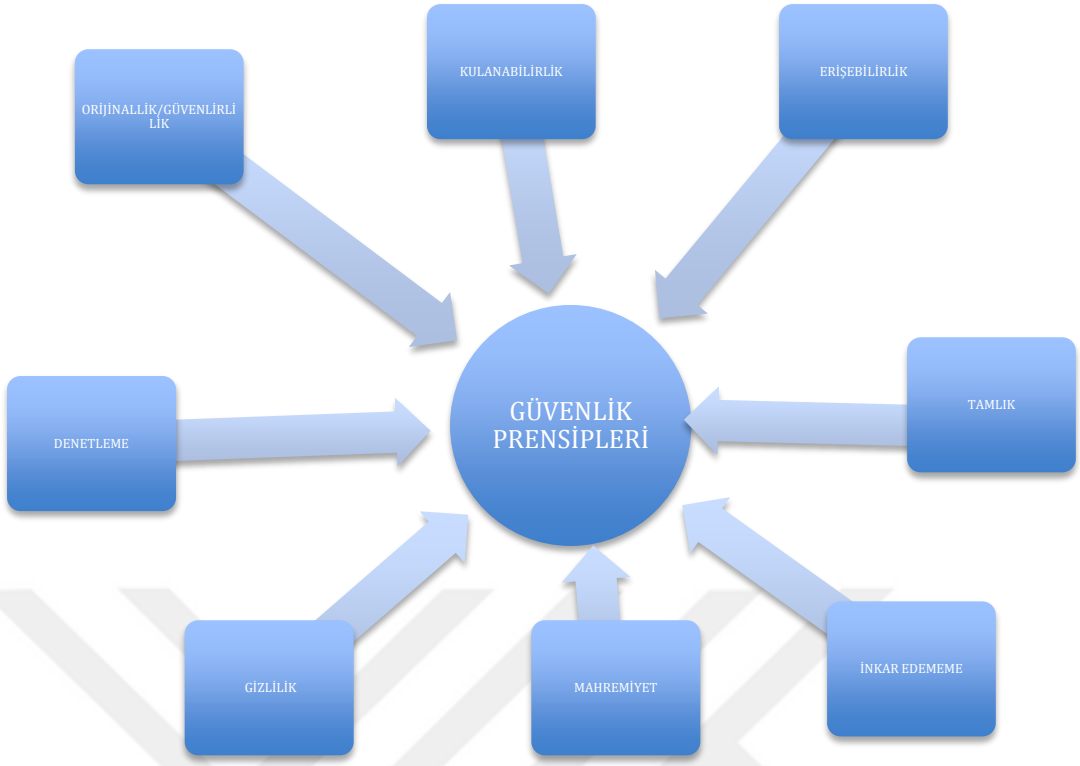
- Literatür taranarak güvenlik prensipleri kapsayıcı maddeler halinde listelendi.
- Bütün güvenlik prensipleri ayrıntılı ele alındı.
- İki anlamlı güvenlik prensipleri tek bir başlık altında toplanıp geliştirildi.

Önlemler listeden çıkarıldı (Güvenlik prensipleri, tüm olası alternatiflerin çözülmesine ilişkin problem ve teşvik dikkatle özetlenmektedir. Bunun sonunda daha verimli ve uygun maliyetli güvenlik çözümleri ortaya çıkmaktadır.)

- Güvenlik prensipler aşağıda belirtilen kriterler sonucunda yeniden tanımlanmaktadır:
- Her güvenlik prensibi yeniden adlandırıldı
- Her güvenlik prensibi sınırlandırılarak benzerlikler ortadan kaldırıldı
- Her hedef sistem mühendisliğiyle bütünleştirildi

Tablo 3'te güvenlik prensiplerinin tanımlarıyla birlikte analiz edilen literatüre atıfta bulanarak son hali oluşturulmuştur (Cherdantseva, Hilton, Rana ve Ivins, 2013: 50).

Science ve Direct (2016) dergisi tarafından yayınlanan makalede Bilgi güvenliğine ilişkin günümüze kadar gelen modellerin kapsamıyla ilgili inceleme yapılmıştır. Yapılan analiz sonucunda RMIAS modeli günümüze kadar yapılan en kapsayıcı model olduğu sonucuna varılmıştır (Cherdantseva, Rana, Ivins ve Hilton, 2016: 52). Bütün bu analizler sonucunda, RMIAS modelinde baz alınan güvenlik prensipleri maddelerine ilişkin anket soruları hazırlanmıştır.



Şekil 7. Rmias Modeli-Güvenlik Prensipleri

Kaynak: Cherdantseva, Rana, Ivins and Hilton, 2016: 50

Bilgi Güvenliği ile ilgili geliştirilen bütün modellerin Bilgi, İnsanlar, Proses, Donanım ve Ağ kriterleri karlılaştırılmış ve en kapsamlı modelin RMIAS olduğu sonucuna varılmıştır (Cherdantseva, Rana, Ivins and Hilton, 2016: 50).

Tablo 3. Güvenlik Prensiplerinin Son Hali

Güvenlik Prensipleri	Tanım	Analiz Edilen Literatür	Bilgi	İnsanlar	Proses	Donanım	Ağ
İzlenebilirlik ya da Kayıt Tutma(Accountability)	Sistemin kullanıcılarının yaptığı eylemlerden sorumlu tutulabilmesi için kaydını tutması	(CNSS, Committee on National Security Systems: National Information Assurance (IA) Glossary, 2010), (ISO/IEC 2700:2009, 2009), (Weitzner, Abelson, Berners-Lee, Feigenbaum, Hendler, ve Sussman, 2008)		x			
Denetleme(Auditability)	Sistemin insan veya makineler tarafından yapılan tüm eylemlerin izlenebilirliğini sağlayabilmesi	(Financial Reporting Council (FRC), 2005) (Sarbanes-Oxley, 2002), (Neumann , 1995)		x			
Orijinallik/Güvenirlilik(Authenticity/Trustworthiness)	Kimlik doğrulamanın yapılabilmesi için üçüncü bir taraf güvenlik	(D., Fighting Computer Crime, 1998), (CNSS, Committee on National Security	x	x	x	x	x

	sisteminin oluşturulabilmesi	Systems: National Information Assurance (IA) Glossary, 2010), (Ware ve Pfleeger, 2006), (ISO/IEC 2700:2009, 2009), (Anderson, 2001), (Neumann , 1995)					
Kullanılabilirlik (Availability)	Sistemin yetkili kullanıcılar tarafından gerekli olduğunda tüm sistem bileşenleri mevcut ve çalışır durumda olduğundan emin olmalıdır	(McCumber, 1991) (Maconanchy, Schou, Ragdale, ve Welch, 2001), (D., Fighting Computer Crime, 1998), (CNSS, Committee on National Security Systems: National Information Assurance (IA) Glossary, 2010), (ISO/IEC 2700:2009, 2009), (Neumann , 1995)	x	x	x	x	x
Gizlilik (Confidentiality)	Sisteme yalnızca yetkili kullanıcıların	(McCumber, 1991), (Maconanchy, Schou, Ragdale, ve Welch,	x				

	bilgiye erişiminin sağlanabilmesi	2001), (D., Fighting Computer Crime, 1998), (ISO/IEC 2700:2009, 2009) (Anderson, 2001)					
Tamlık (Integrity)	Bir sistem tüm bileşenlerinin de tamlık, doğruluk sağlamalı ve aynı zamanda yetkisiz değişiklikleri engeleyebilmelidir.	(McCumber, 1991), (D., Fighting Computer Crime, 1998), (CNSS, Committee on National Security Systems: National Information Assurance (IA) Glossary , 2010), (ISO/IEC 2700:2009, 2009), (Neumann , 1995)	x	x	x	x	x
İnkar Edememe(Non-repudition)	Sistemin yapılan bir eylemin gerçekleşip gerçekleşmediğini kanıtlayabilmesi	(CNSS, Committee on National Security Systems: National Information Assurance (IA) Glossary, 2010), (ISO/IEC 2700:2009, 2009), (Neumann , 1995), (Anderson,	x		x		

		2001)					
Mahremiyet	Bir sistemin gizlilik mevzuatına uyması gerekir, kişisel bilgilerini (kullanıcı katılımı)bireyler in kontrolü sağlayabilmesini mümkün kılmalı	(Weitzner, Abelson, Berners-Lee, Feigenbaum, Hendler, ve Sussman, 2008), (Smith ve Shao, 2007), (Report of the Secretary's Advisory Committee on Au, 1973), (OECD, Guidelines on the Protection of Privacy and Trans- border Flows of Personal Data , 1980), (Almagwashi ve Gray, 2012)	x	x			

Kaynak: Cherdantseva, Rana, Ivins ve Hilton, 2016: 50

2.4. Güvenlik Prensipleri

Bilgi güvenliği modelinden belirtilen 8 aşama başlıklar altında açıklanmıştır.

2.4.1. Gizlilik (Confidentiality)

Gizlilik, giriş yetkisi olmayan kullanıcıların, izinsiz girişlerin engellenmesi olarak tanımlanabilir (Yıldız, 2014: 58). Gizlilik, veri ağınızda bulunan bilgiler (disk, tape vb.) ve ağ üzerinde gönderici ve alıcı arasında bilgi alışverişini kapsamaktadır (Yıldız, 2014: 58). Saldırganlar talep ettikleri takdirde, parola dosyalarının çalınması, sosyal mühendislik ya da kullanıcının şifreyi girerken gözetlenmesi gibi bir çok yolla, gizliliği ihlal ederek bilgisayardaki verileri ele geçirebilmektedir (Yıldız, 2014: 59).

Bir başka tanımda ise gizlilik, bilgilerin yetkisiz kişilerden korunması olarak tanımlanmaktadır. Gizlilik ihlalini ise iletişim ya da bir dosyanın ifşa edilmesi sonucu oluştuğu belirtilmiştir (Knorr ve Rohrig 2015: 76).

Adalet Bakanlığınca hazırlanan Bilgi Güvenliği ve Kullanıcı Sorumluluğu ile ilgili raporda ise gizliliği kısaca bilginin yetkisiz kişilerin eline geçmemesi olarak tanımlanmaktadır(Adalet Bakanlığı, 2012: 12)

Uluslararası Standartlar Örgütü (ISO) tarafından "Bilginin sadece yetkilendirilmiş kişilerce erişilebilmesi " olarak tanımlanır ve Gizliliğin değer tanımı beş aşamada belirtilmektedir:

i. Varlık erişimi olan herkes tarafından ulaşılabilir
ii. Varlık işletmedeki herkes tarafından görülebilir, kullanılabilir
iii. Varlık sadece departmanlardaki kullanıcılar tarafından görülebilir
iv. Varlık doğrudan erişimi olan kişiler ve üstleri tarafından kullanabilir
v. Varlık yetkili amir tarafından görülebilir

2.4.1.2. Gizliliğin Sınıflandırılması

Sınav (2014) makalesinde Gizliliğin, bilgilerin depoda korunmasını sağladığını, aynı zamanda yetkisiz kişilerin girişlerini ya da bilgilere ulaşmaya çalışan grup ya da toplulukların, bilgilere ulaşmasını engellediğine değinmektedir. Bu engelleme fiziksel ya da elektronik olabilmektedir (Sınav, 2014: 59).

Elektronik gizleme, son kullanıcıların bilgi, veri ya da kaynaklara ulaşamamaları demektir. Örnek verecek olursak, birileri başkasının maillerini kişinin onayı olmadan ulaşabilirse, gizlilik ihlal edilmiş sayılmaktadır (Knorr ve Rohrig, 2015: 76).

Fiziksel gizlilik ihlalleri ise gizli ibaresi olan bilgisayarların okunması ya da gizli bilgilerin sözlü söylenmesi durumunda bilmemesi gereken kişilerin duymasını kapsamaktadır (Knorr ve Rohrig, 2015: 77).

Whitman ve Mattord (2014) ise makalesinde, bilginin gizliliğinin korunabilmesini aşağıda belirtilen önlemlerle sağlanabileceğini açıklamaktadır:

- Bilgi sınıflandırması
- Güvenli belge deposu
- Genel güvenlik politikalarının uygulanması
- Bilgi saklama görevlileri ve son kullanıcıların eğitimi

Avustralya Devleti (2012) tarafından yapılan araştırmada gizliliğinin korunabilesi için izinsiz erişimi engelemek adına firmaların mutlaka önlemler alması gerektiğini belirtmektedir.

2.4.1.3. Gizliliği Önemi

Bilginin gizliliği çalışanların, müşterilerin ya da hastaların kişisel bilgileri söz konusu olduğu zaman çok önemlidir (Whitman ve Mattord, 2014: 13). Bir kuruluşta işlem yapan kişiler, kuruluşun İç Gelir Hizmeti gibi federal bir kuruluş ya da bir işletme olması durumunda kişisel bilgilerin gizli kalmasını beklemektedir. Şirketler, gizli bilgileri ifşa ettiğinde problem ortaya çıkmaktadır. Bazen bu açıklama kasıtlı olsa da, gizli bilgilerin ifşa edilmesi, örneğin gizli bilgiler yanlışlıkla organizasyonun dışındaki birine e-postayla gönderildiğinde, gizlilik ihlali gerçekleşmiş olmaktadır. Konuya örnek olarak Şubat 2005'te veri toplama ve komisyonculuk şirketi ChoicePoint, 2004 yılında 145.000 kişinin kişisel bilgilerinin kimlik hırsızları tarafından çalındığını açıklamıştı (Whitman ve Mattord, 2014: 14). Gizlilik ihlallerine ilişkin diğer bir örnek ise, kritik bilgilerin olduğu dökümanların çalışanlar tarafından yanlışlıkla başka birine gönderilmesi ya da veri tabanına hackerların sızarak adres ya da buna benzer kişisel bilgilerin çalınması olarak gösterilebilir (Whitman ve Mattord, 2014: 14).

Tüketici olarak, "üyelere özel" kartlar kullandırılarak, harcama alışkanlıklarının bazıları ifşa edebilmektedir. Bir çevrimiçi anketi doldurulduğunda, çevrimiçi ayrıcalıklara erişmek için kişilerin kişisel geçmişinizi ifşa edebilmektedir. Açıklanan bilgiler kopyalanmakta, satılmakta, dağıtılmakta ve nihayetinde profiller halinde birleştirimektedir.

'Salam hırsızlığı' adı verilen bir suç teşebbüsünde de benzer bir teknik kullanılmaktadır (Whitman ve Mattord, 2014: 95). Şarküteri, bütün bir salamı çalamayacağınızı bilmektedir, ancak birkaç dilim salam haber verilmeksizin çalındığında kimse farkına varmamaktadır. Belli bir süre sonra salamın tamamı çalınmış olacaktır. Bilgi güvenliğinde salam hırsızlığı, bir çalışanın bir anda birkaç parça bilgi çalıp, daha fazla

almanın fark edileceğini bildiğinde ortaya çıkmaktadır. Ancak sonunda çalışan, eksiksiz veya kullanışlı bir şey almaktadır (Whitman ve Mattord, 2014: 95).

Gizlilik, firmaların önemli bilgilerinin ifşa edilmemesi, önemli evrakların yetkisiz kişilerce ele geçirilmemesi, firmanın prestiji ve geleceği açısında çok önem arz etmektedir. Firmalar genellikle yetkisiz kişilerin erişimini engelemek için bilgi sınıflandırması yaparak her departmana farklı saklama alanları oluşturarak departman arası bilgi sınıflandırması yapmaktadır. Satış fiyatları ya da maliyet gibi firmalar için çok önem arz eden kalemlerde ise sınırlı kişilere değiştirme yetkisi ya da görüntüleme yetkisi vermektedir.

2.4.2.Tamlık-Bütünlük (Data Integrity)

Tamlık-Bütünlükten kastedilen, bilginin göndericiden çıktığı halde, tahribata uğramadan alıcıya ulaşmasıdır (Sınav, 2014: 59). Bu sayede veri aktarımı yapılırken takip ettiği yollarda tahribata uğramadan ya da verisi ve sırası değiştirilmeden verinin alıcıya ulaşmasını sağlamaktır (Yıldız, 2014: 59). Bir başka tanımda ise veri bütünlüğü, bilginin yetkisiz kişiler tarafından değiştirilmemesi olarak tanımlanmaktadır Adalet Bakanlığı, 2012: 12). Knorr ve Rohrig'e (2015) göre veri bütünlüğü, istenmeden bilginin değiştirilmemesi ya da zarar görmemesi olarak tanımlanmaktadır.

ISO27001'de bütünlük ilkeleri aşağıdaki gibi sıralanmaktadır:

- Varlığın erişimi olmayan kişiler tarafından değiştirilmesi veya ortadan kaldırılması kurumu etkilememektedir.
- Varlığın erişimi olmayan kişilerce değiştirilmesi veya ortadan kaldırılması kurumu çok fazla etkilememekte ve kısa bir sürede veriler yeniden sağlanmaktadır.

- Varlığın erişimi olmayan kişilerce değiştirilmesi veya ortadan kaldırılması kurumu sınırlı bir şekilde etkilemekte ve durum orta bir sürede telafi edilmektedir.
- Varlığın erişimi olmayan kişilerce değiştirilmesi veya ortadan kaldırılması kurumu ciddi bir şekilde etkilemekte ve zarar orta vadede kaldırılmaktadır.
- Varlığın erişimi olmayan kişilerce değiştirilmesi veya ortadan kaldırılması kurumu çok ciddi etkilemekte ve etki telafi edilememekte yada çok uzun sürede düzeltilmektedir.

Bütünlüğün ihlal edilmesi, yetkili kişinin onayı olmadan bilgilerin değiştirilmesidir ve bu ihlal, yetkisi olan yada olmayan kişiler tarafından yapılmaktadır (Knorr, Rohrig, 2015: 77). Bütünlükten ödün verilmesi tesadüf, kasıtlı ve kötü niyetli kişilerce yapılabilmektedir. Kötü niyetli kişilerce bütünlüğün bozulması, bir işletmenin veri tabanın kasıtlı olarak değiştirilmesi, yeni eklerin yapılması ya da silinmesi olarak yapılabilir ve bu eylem yetkisi olmayan kişilerce ya da yetkisi olan kişilerce yapılabilmektedir (Knorr ve Rohrig, 2015: 77).

Yanlışlıkla bütünlüğün ihlal edilmesi, sistem değişikliğinde silinmemesi gereken kayıtların silinmesi sonucu oluşmaktadır. Bu eylem sisteme virüs bulaşması sonucu ya da kullanıcıların yanlışlıkla bazı şeyleri silmesi sonucu olabilmektedir. Sistemin bir şey silinmeden önce doğruluğu için sık sık sormasının nedeni budur. Bütünlük bilgi kaynaklarının güvenliği anlamına gelmektedir (Knorr ve Rohrig, 2015: 81).

Verinin bütünlüğü işletmeler ve müşteriler için çok önemli bir husustur. Firma tarafından hazırlanan proformanın üzerinde bulunan banka bilgilerinin hackerlar tarafından değiştirilmesi örnek olarak verilebilir. Bunun sonucunda müşteri yanlış kişilere proformada belirtilen meblağı ödeyebilmektedir. Bunlar göz önünde bulundurulduğunda veri bütünlüğü sorununun iki boyutu ortaya çıkmaktadır. Birincisi, müşteri firmadan bir kayıt aldığında, müşteri kayıt bütünlüğünü nasıl sağlayabilir? Yani, müşteri verilerin yetkisiz bir şekilde

değiştirilmediğini nasıl doğrulayabilir? İkincisi, müşteri yapılan ticaretle ilgili sorgu yaptığında doğru bilgilerin eksiksiz karşı tarafa ulaşabilidiğinde nasıl emin olunabilir? Hacigümüş, Iyer ve Mehrota, 2007: 166).

Bilgi bütünlüğü aşağıda verilen nedenlerden dolayı zarar görmüş olabilir (Tsai vd., 2007: 227);

- Kaynaklardaki tutarsızlık ve verilerin nasıl türetildiğinine ilişkin bilgi eksikliği
- Verilere uygulanan kurallarda tutarsızlık
- Birden fazla bakım noktası
- Kötü amaçlı değiştirme (bilgisayar korsanları saldırısı, kimlik belgesinin değiştirilmesi)
- Kazara değişen (İletişim hataları, sabit disk çökmesi, veri tabanı çökmesi).

2.4.3. Erişebilirlik(Availability)

Erişebilirlikten kastedilen, Bilişim sistemlerinin içeriden ya da dışarıdan, sistemi yavaşlatmaya yönelik saldırıların engellenmesidir (Yıldız, 2014: 60). Bunun sonucunda kullanıcılar, ulaşmaya çalıştıkları verilere zamanında ve güvenilir bir şekilde ulaşmalarını sağlamaktadır (Yıldız, 2014: 60). Sistemde Erişeblirliği etkileyecek saldırılar sadece hackerler tarafından yapılmamaktadır. Yazılımdaki hatalar, verilerin ısı topraklama etkisi gibi şartlardan dolayı da sürekliliğini etkiyebilmektedir (Yıldız, 2014: 60).

Diğer bir adıyla erişebilirlik kısaca kullanıcının bilgiyi talep ettiği zamanda ulaşabilir ve kullanabilir olması olarak tanımlanmaktadır (Adalet Bakanlığı, 2012: 22). Knorr ve Rohrig ise Sürekliliği, yetkili kişinin bilgi ve sisteme uygun zaman diliminde ulaşabilmesidir (Knorr, Rohrig, 2015: 76). Saldırı ya da sisteme girilmesi sonucunda yetkili kişi erişebilirliği kaybedebilmektedir (Knorr ve Rohrig, 2015: 76).

ISO 27001'de Süreklilik bir diğer adıyla Erişebilirlikten ilkeleri şunlardır:

- Varlığa erişimin ortadan kaybolması departmanı ya da şirketi hiç bir şekilde etkilemez.
- Varlığa erişimin ortadan kaybolması departmanı yada şirketi çok az etkiler ve en kısa sürede sorun çözülür.
- Varlığa erişimin ortadan kaybolması departmanı yada şirketi sınırlı şekilde etkiler ve hasar orta sürede tekrar düzeltilir.
- Varlığa erişimin ortadan kaybolması departmanı yada şirketi ciddi oranda etkiler ve orta vadede sorun çözülmüş olur.
- Varlığa erişimin ortadan kaybolması departmanı yada şirketi çok ciddi etkiler ve yaşanan hasar telafi edilemez yada çok uzun süre alır.

Erişilebilirlik, bilgi varlıklarının talep edildiğinde ulaşılabilir olmasını sağlamaktır. Servis ağındaki herhangi bir aksaklığın Kobilerdeki operasyonel süreci etkileyeceğinden dolayı çok önemli bir özellik haline gelmektedir.

Erişilebilirlik, yetkili kişinin sistemdeki kaynağa talep ettiğinde ulaşabilmesidir. Eğer kaynak önemli bir varlık ise erişebilirliği garanti altına almak için yedeklenmesinin mutlaka olması gerekmektedir.

Erişebilirlik üç başlık altında sınıflandırılmaktadır (Suhail, Quadri, 2016: 189);

i. Yazılım
ii. Donanım
iii. Ağ

2.4.3.1. Yazılım

Yazılım diğer iki unsura kıyasla en kritik faktördür (Suhail ve Quadri, 2016: 189). Tüm güvenlik saldırıları ve bunlarla ilgili çözüm yolları, yazılım veya işletim kodu ile birlikte ele alınmaktadır (Suhail ve Quadri, 2016: 189). Yazılım üç başlık altında sınıflandırılmaktadır (Brown, Johnston ve Kelly, 2002: 6);

i. Hizmet seviyesi
ii. Bileşen seviyesi/nesne
iii. Sınıf seviyesi

2.4.3.1.1. Hizmet Seviyesi

Yazılım mimarisinde en üst seviyedeki unsur hizmet seviyesidir. Saldırganlar ya da hackerler sisteme giriş yaparken ilk baktıkları yer burasıdır (Suhail ve Quadri, 2016: 190). Güvenlik açısından bakıldığında, bir uygulama programında daha fazla güvenlik açığı bulunan sistem, diğer arama programlarından kaynaklanan risklere/tehditlere karşı daha savunmasızdır. Çünkü kötü niyetli bir kullanıcının meşru bir yol ile bir uygulama programının hizmetlerini alması o kadar da zor değildir ve daha sonra programa eriştikten sonra onu gayri meşru yollarla kötüye kullanabilmektedir. Dolayısıyla, sürdürülebilir bir varlık durumunu korumak için bilgi sistemi farklı programlar tarafından kontrol edilebilmelidir (Suhail ve Quadri, 2016: 189).

2.4.3.1.2. Bileşen Seviyesi/Nesne

Buraya güvenlik açısından bakıldığında önemli olan şey istemci programların bileşene erişim için gerekli arabirime sahip olması durumunda belirli bir bileşene kimin erişebileceğidir (Suhail ve Quadri, 2016: 189). Yani yetkilendirme yapılırken kimin verilere ulaşabileceğini sınırlamak gerekmektedir. Çeşitli etkileşimli bileşenler arasında güçlü bir kimlik doğrulama ve erişim denetimi mekanizmasına ihtiyaç duyulmaktadır. Böylece yalnızca yetkili istemci programları kendi ilgili bölümlerine erişebilmektedir (Suhail ve Quadri, 2016: 189).

2.4.3.1.3. Sınıf Seviyesi

Bu yazılım mimarisinin en düşük düzeyidir. Nesne Odaklı Paradigma yani kapsülleme, bilgi gizleme, sınıflar ve nesneler vb. kavramlarını, etkin bir performansa ve yazılım sisteminin güvenli bir şekilde çalışmasına neden olacak şekilde kapsamaktadır. Tüm bu katmanlar arasında bir bağımlılık ve ilişki olduğu için, tasarımda kötü bir tasarım mevcutsa ya da en düşük düzeyde mantıksal bir kaçamak var ise, yukarıdaki katmanlardan erişerek adım adım hedefe ulaşılmaktadır. Bu nedenle, etkin ve güvenli bir yazılım sistemi, tasarımın en alt düzeylerinden var olan tüm katmanlara kadar özenle ele alınması gerekmektedir (Suhail ve Quadri, 2016: 190).

2.4.3.2. Donanım

Uygulama yazılımı tehlikeye girdiğinde, saldırganın/bilgisayar korsanının nihai hedefi, alıcı bilgi sistemine hasar getirmek ve bilgi sistemini bozmak olduğundan, bilgi sisteminin işletim sistemi veya sistem yazılımı üzerinde olumsuz etkilere neden olabilmektedir. Saldırganın nihai amacı alıcı sistemin kaynaklarını tüketmektir. Diğer bir deyişle, sistemin işlem kapasiteleri, hem Mikroişlemci hem de RAM üstesinden gelemeyecek kadar büyük miktarda gereksiz işler verilerek bitkinleşebilmektedir. Bu tür işler saldırganların hedef makinelere kurduğu kötü niyetli programlar tarafından oluşturulabilmekte veya ağ üzerinden canlı bir şekilde yapılabilmektedir. Yani Sockstress adlı bir aracı kullanarak DOS saldırısı bir servisi çökertmek için kaynakları tüketebilmektedir (Harris, 2002).

2.4.3.3. Ağ

Bir saldırgan hedef makineye izinsiz girdiğinde, hedef makinenin hizmetlerini erişilebilir kılmak için yapılabilecek en basit şey hedef sistemin bağlı olduğu ağa saldırmaktır. En yaygın ağ saldırısı, şuan ölümcül DDOS saldırısı olan ve 400 Gbps büyüklüğünde veri üretebilen ölümcül trafikle ağın sızmasıdır (Harris, 2002). Ayrıca bir saldırgan, ağ hizmetlerine geçersiz bir veri gönderebilmekte ve bu da hizmetlerin veya uygulamaların anormal davranışa neden olabilmektedir. Ayrıca bir saldırgan, meşru kullanıcılara ağa dayalı kaynağa erişim kaybına neden olan tüm trafiği engelleyebilmektedir. Ağ yığını yani TCP/IP modeli Şekil 4'te gösterildiği gibi 4 katmana sahiptir. Bir saldırgan, ağdaki herhangi bir seviyedeki protokollerden (ağ donanımındaki ve yazılımdaki güvenlik açıklarından) istifade edebilmekte ve bu nedenle hizmetleri meşru kullanıcılar için kullanılamaz hale getirebilmektedir. Örneğin, internet protokolü (IP) paketindeki bir Logic DoS saldırısı,

Payload veri boyutunu değiştirebilmekte ve bu da OS yazılımındaki bir arıza nedeniyle hedef işletim sisteminin çökmesine neden olabilmektedir.

Firmadaki çalışanlar ulaşmak istedikleri evrak ya da şirket ile ilgili bilgilere ulaşabilirliğiyle ilgili herhangi bir sorun yaşamamaları gerekmektedir. Çünkü günümüz rekabet ortamında hızlı bilgi alışverişi müşteriler için çok önem arz etmektedir. Bunun için de işletmeler gerekli önlemleri alarak çalışanlarına bu hizmet sunmak zorundadır.

2.4.4. İzlenebilirlik ya da Kayıt Tutma (Accountability)

Alan Westin (1967) Gizlilik ve Özgürlük adlı kitabında, gizliliğin tanımını bireylerin kendileriyle ilgili kişisel bilgilerin başkalarına iletilmesiyle ilgili sahip oldukları haklar olarak tanımlamaktadır. Bu tanım izlenebilirliğin temelini oluşturmakta ve bütün bilgileri kapsayacak şekilde açıklanmaktadır.

İzlenebilirlik ya da kayıt tutma kısaca sistemin kullanıcıların yaptığı eylemlerden sorumlu tutulabilmesi için kaydını tutması olarak tanımlanmaktadır (Weitzner vd., 2008: 83).

Bir başka tanımda ise izlenebilirlik ya da kayıt tutma, "kişinin inanç ve davranışlarını başkalarına haklı kılmak için örtülü veya açık baskı yapılması" olarak tanımlanmaktadır (Tadmor & Tetlock, 2009: 8). Hesap verme sorumluluğu kendi imajıyla da bağlantılıdır. Bu nedenle insanları bilinçli ve stratejik olarak davranışların, standartların ve hareketlerin nasıl olması gerektiği beklentilere uyacak şekilde değiştirmeye motive etmektedir (Gelfe ve Realo, 1999). Bu nedenle, hesap verebilirlik bir norm uygulama mekanizması olarak kabul edilmektedir (Tadmor ve Tetlock, 2009: 8). Hesap verebilirlik teorisinin benimsenmesi davranışsal güvenlik araştırmaları için nispeten yeni olup, planlı davranış teorisi ve diğerleri ile karşılaştırılmaktadır (Duy Dang, Siddhi ve Vince, 2006: 204). Hesap verebilirlik teorisini davranışsal güvenlik alanına tanıtan seminer kağıtlarından biri, 2015 yılında Vance, Lowry ve

Eggett (2015) tarafından yayınlanmıştır (Duy Dang, Siddhi ve Vince, 2006: 205). Bu araştırmacılar, örgütsel güvenlik için hesap verebilirlik algılamasının güvenlik eserleriyle arttırabileceği ve güvenlik politikasını ihlal etme niyetini azalttığı sonucuna ulaşmıştır (Duy Dang, Siddhi ve Vince, 2006: 204).

Sistemde yapılan işlemlerin daha sonra izlenebilmesi için kayıt altına alınması gerekmektedir. İşlemlerden kastedilen e-posta göndermek, herhangi bir sosyal medyadan mesaj gönderilmesi gibi hareketlerden bahsedebilmektedir. Toplanan bilgiler sayesinde bilinen saldırı türlerine rastlanması durumunda sistem otomatik olarak uyarı vermektedir (Yıldız, 2014: 60). Sistemin izlenebilirliği ya da kayıt tutulması garanti altına alınması, iletişimdeki kişilerin doğru kişilerle iletişimde olduklarından emin olunduğunu göstermektedir (Knorr ve Rohrig, 2015: 77).

Guangwu Hu, Wenlong Chen, Qi Li, Yong Jiang ve Ke Xu (2016) tarafından yapılan çalışmada, TRUEID şeması oluşturmuştur. Araştırmada günümüzde kritik internet güvensizliği durumu göz önünde bulundurulduğunda, internet izlenebilirliğini artırma ve muhtemel siber saldırıları önlemeye ışık tutabilmesi amaçlanmaktadır.

2.4.4.1. İzlenebilirlik- Kayıt Tutma ve Bilgi Iletişim Tekonlojisi (BİT)

Kayıt tutma ve BİT arasında birkaç olası bağlantı vardır. Önemli olan izlenebilirliğini sağlamak amacıyla BİT'in kullanılmasıdır. BİT, teknolojinin sorumluluk nesneleri ve nesneler arasındaki ilişkiyi tanımlamasına yardımcı olduğu hesap verebilirliği sağlamak için kullanılmaktadır. Buradaki temel fikir hesap verebilirliğin önemli bir bölümünün bilgi ve ilgili paydaşlara bilgi dağıtımı olmasıdır. BİT bilgi yakalamak ve yaymak için tasarlandığından, bu tür süreçleri kolayca destekleyebilmektedir.

Ticari organizasyonlarda, para veya maddenin hareketlerini yansıtmak için BİT kullanılarak yapılabilmektedir (Stahl, 2006: 56). Örneğin, ERP sistemlerinin içerdiği detaylı envanter takip sistemleri, bireysel kişilerin yaptıkları eylemlerden sorumlu tutulabilmelerini kolaylaştırmaktadır. Benzer şekilde, finansal bilgi sistemleri para hareketlerinin bireysel eylemlere bağlanmasına izin vermektedir. Hesap verebilirlik oluşturma yolları yeni değildir (aslında en azından muhasebe alanı kadar eskidirler). Ancak BİT kullanımıyla büyük ölçüde yardım edilebilmekte ve geliştirilebilmektedir. Daha genel olarak, BİT'in her tür varlığın davranışını izlemesine yardımcı olabileceği ve böylece sorun yaşandığı zaman sorumlu kişi tespit edilebilmektedir (Skovira, 2003:165).

Bu tür izlenebilirliği artıran BİT kullanımı için sayısız örnek bulabilmektedir. Bir şekilde elektronik olarak en çok yaratılan dosyalar bu şekilde yorumlanabilmektedir. Bu, yukarıda belirtilen işletme kayıtları için geçerlidir, ancak sağlık hizmetleri ve ilgili kayıtlar gibi diğer alanlarda da en az geçerlidir (Yakel, 2001: 243). Başka örnekler de kamu idaresi ve siyasettir.

Siyasi olarak sorumlu olmak için nedensel bir rol oynamak gerekli değildir. Çünkü siyasi sistemler oldukça karmaşık olma eğilimindedir. Bu da söylemin söylemsel süreçleri ve asimilasyonun anlaşılmasını zorlaştırmaktadır. Her hükümet ya da en azından her demokratik hükümet, vatandaşları için hesap verebilir olmalıdır. Bu hesap verebilirlik, yaratma araçlarını aramak için bir başka sebep ve BİT'in tek olmasından kaynaklanmaktadır. BİT, vatandaş fonlarının kamusal kullanımını inceleyebilmelerini ve böylece iyi politikaları belirlemelerini ve yolsuzluğun önlenmesini sağlayan bilgileri yayınlamak için kullanılabilmesidir (Barata ve Cain, 2001: 247).

2.4.4.2. İzlenebilirlik- Kayıt Tutma Ve Bilgi Iletişim Tekonlojisi Sorunları (BİT)

BİT, hesap verebilirlik sağlamak açısından çok değerli olabilmesine karşın, bunun tersini de beraberinde getirebilmektedir. Nissenbaum (1995), bilgisayarların hesap verebilirliğin dağılmasına veya dağılmasına neden olabilecek dört alanını tanımlamaktadır. Bunlar, bilgisayarların çoğu zaman bir bilgisayarın bireyleri ve işlevleri arasında bir bağlantı kurmayı pratik olarak imkansız kılan bir yazılım ve donanımdan oluşan karmaşık makineler olmasıdır(Johnson, Mulvey,1995: 58). Bu sorunların bir kısmı, genellikle kaçınılmaz olarak kabul edilen, ancak yine de özneyi ve nesneyi özniyete koymayı zorlaştıran yazılım arızaları veya "böcek" lerdir. Sık karşılaşılan bir sorun, bilgisayarın günah keçisi olarak kullanılması ve burada teknolojinin hesap verebilirliği ve sorumluluğun saptırılması amacıyla ifade edilmesi amaçlanmaktadır.

İlgili başka bir problem, hesap verebilirliğin basit bir şekilde anlaşılması için BİT'in oluşturulmasıdır. Genellikle, veri veya bilgiyi örneğin İnternet aracılığıyla erişilebilir hale getiren şeffaflığın hesap verebilirliğe yol açacağı düşünülmektedir. Barat ve Cain (2001), bu sorunu kamu mali hesap verebilirliği açısından tartışmaktadır. Hesap verebilirlik ve BİT arasındaki ilişkinin aşırı basitleştirildiğini ve bunun da bir artıştan ziyade hesap verebilirliğin azalmasına neden olabileceği belirtilmektedir.

2.4.5. Orijinallik-Güvenirlik (Authenticity/Trustworthiness)

Ağ güvenliği için kimlik sorgulanması, göndericinin ve alıcının doğru kişi olup olmadığını sorgulamasıdır (Yıldız, 2014: 60). Alıcının ve göndericinin iddia ettiği kişi olduğundan emin olunması gerekmektedir. Bunun yanı sıra, bilgisayara giriş yaparken girilen parola da kimlik sınaması olarak adlandırılabilmektedir.

Uluslararası Standartlar Organizasyonu (ISO) ise kimlik sorgulamasını, bir varlığın iddia edilen bir özelliğinin doğru olduğuna dair güvencenin sağlanması (ISO / IEC 27000, 2013) olarak tanımlanmaktadir. Başka bir deyişle, kimlik doğrulama, bilgisayar sistemine giriş yapan kişinin iddia edilen kişi olup olmadığını doğrulamaktadır.

Bilgi güvenliğinde kimlik sınaması kullanıcı adı ve şifreyle doğrulanabilmektedir. Şifre sistemde kayıtlı kullanıcı adıyla eşleşirse kullanıcının girişi yetkisi onaylanmaktadır (Karsten, 2011: 5).

Tanımlama ve kimlik doğrulaması için bir başka method ise biyometrik bilgilerdir. Örneğin Parmak izi veya RFID belirteçleri veya akıllı kartlar gibi elektronik sistemler farklı tanımlama yöntem çabaları, güvenilirlik ve güvenlik açısından birbirinden ayrılmaktadır. Kombinasyonu çeşitli yöntemler (çok faktörlü kimlik doğrulama) güvenliği artırabilmekte ve kimlik hırsızını engeleyebilmektedir. Örneğin, bir RFID simgesinin kaybolması tüm kapıları açabilmekte, bununla birlikte Ek PIN kodu (Kişisel Kimlik Numarası) yine de yetkisiz kişilerin erişimini (iki faktörlü kimlik doğrulama) engeleyebilmektedir (Karsten, 2011: 5).

Kimlik sınaması için genellikle kullanılan üç faktör aşağıdaki gibidir (Harris, 2002):

i. Kullanıcının sahip olduğu bir şey (simge veya akıllı kart gibi)
ii. Kullanıcının bildiği bir şey (bir parola veya PIN)
iii. Sadece kullanıcının sunabileceği bir şey (örneğin biyometrik tanımlama)

Ek faktör olarak kullanıcının bulunduğu yer (örneğin belirli bir terminal veya iş istasyonu kullanarak) sınamada kullanabilmektedir (Bishop, 2004). Temel olarak, tüm tanımlama yöntemleri, girilen veya okunan verileri depolanan bir kullanıcının kendisinin olduğu iddia ettiğinden emin olmak için kullanılmaktadır. Sonuç olarak, veri olmalı, iletişim ve saklama alanlarının da bulunduğu veritabanları veya dizinler gizli olarak kabul edilmeli ve korunmalıdır (Karsten, 2011: 5).

2.4.5.1. Yetkilendirme

Yetkilendirme, kimliği doğrulanmış erişim için hizmetin ayrıcalıklarını belirleyen ve onaylayan işlemdir (Bhattacharya, Kumar, 2015: 125). Bir başka deyişle, tanımlanmış ve doğrulanmış bir kişi, sistemde hangibir veriye erişmine izin verileceğini ve hangi eylemleri gerçekleştirmesine izin verildiğini belirtmektedir.

2.4.5.1.1. Erişim Kontrol Modelleri

Erişim kontrol modelleri, güvenlik politikası ve konular nesnelere erişimin nasıl sağlanacağıyla kurulan kuralları ve hedefleri uygulamak için kullanılmaktadır. Bugün kullanılan erişim kontrol modelleri aşağıda kısaca açıklanmıştır (Vacca, 2009: 515)

Daha az kullanışlı ama popüler olan erişim kontrol modelinden biri İdari Erişim Kontrolüdür (DAC). Bu model, bir nesne sahibinin, dosyaya kimin erişip erişemeyeceğini belirlemektedir. Bu nedenle DAC bazen de Kimlik Tabanlı Erişim Kontrolü (IBAC) olarak tanımlanmaktadır.

Zorunlu Erişim Kontrolü (MAC), konu olan tüm nesnelere (veri veya bilgi), izin seviyesinin, nesnenin sınıflandırmasında daha yüksek veya eşit olduğu durumda kullanılmaktadır. Yani her kullanıcı belirli seviyelerde verilere ulaşabilmekte ya da ulaşamamaktadır. Bu erişim kontrol modeli bazen kural tabanlı erişim kontrolü olarak da tanımlanmaktadır.

En yaygın model olan Rol Tabanlı Erişim Kontrolü (RBAC), rolleri veya bir konuyla ilgili izinleri gruplar halinde erişimine izin vermektedir. Örneğin, bir yönetici bir iş yaratabilir, pozisyon veya departmanla ilgili izinleri grup olarak atamayabilir ve her departman kendisiyle ilgili verilerin girişini yapabilmektedir. En önemli faydası kullanıcıların veri girişi

yaparken idari çabalarının azalmasıdır. Tüm erişim kontrol modelleri, kuruluşun güvenlik gereksinimlerine göre ayrı ya da hepsi birlikte kullanılabilmektedir (Harris 2002).

2.4.5.2. Erişim Kontrol teknikleri

Erişim kontrol matrisi, bir konunun erişim izinlerini ilişkilendiren bir mekanizmadır. Erişim açısından daha sık kullanılan tekniklerden biridir. Satırlar kullanıcının yetenek tablosundan oluşmaktadır. Öte yandan sütunları, kaynağın Erişim Kontrol Listesi'ni (ACL) yansıtmaktadır. Erişim kontrol listesi, kullanıcının kaynaklara bireysel erişim haklarını ve ayrıcalıkları belirleme metodudur. Bir işletim sistemindeki ve dosya içindeki ortak ayrıcalıklar sistem bağlamı şunlardır (Gattiker, 2004):

- Oku - bir dosyayı veya bir dizinin içeriğini okumak için
- Yaz - dosyaları / dizinleri oluşturmak veya güncellemek için
- Dosya Çalıştırmak - bir dosyayı çalıştırmak için, örneğin bir program

İçerik Bağımlı Erişim Kontrolü, kullanılan bir başka erişim kontrolü tekniğidir. Farklı erişim izni olan kullanıcıların erişim içeriğine bağlı olarak kontrol edilecek bilgiler, kullanıcıların sahip oldukları erişim iznine göre değişmektedir. Örneğin, bir bankadaki resepsiyonist, müşterinin adını ve hesap numarasını göremez ama banka çalışanı erişim izni olduğu için bu bilgileri kontrol edebilmektedir. Bununla birlikte, banka müdürü ayrıca geçen yılın banka hesap dökümlerine bakabilmekte ancak banka çalışanı bu verilere ulaşammaktadır. Bu yaygın olarak kullanılan bir yaklaşımdır. Belirli derecede gizlilik ihtiyacı duyan kurum veya kuruluşlar tarafından kullanılmaktadır Karsten, 2011: 5).

Kullanılan teknikler aşağıda sıralanmıştır Karsten, 2011: 5).

- Günün saati (yalnızca belirli saatlerde, sonuna kadar erişime izin verilmesi)
- İşlem türü (hangi işleme izin verildiğinin belirtilmesi)

- Mantıksal konum (IP adresi)
- Fiziksel yer (terminal).

Bilgi güvenliğinin korunabilmesi için yetkisiz kişilerinin erişimini engelemenin başka bir yolu da bilginin güvenirliliğini sağlayabilmektir. Bunun da en basit yolu dosya ya da bilgisayar erişimine şifreleme ya da farklı tekniler kulanarak yetkisiz kişilerin erişimlerini engeleyebilmektir.

2.4.6. Denetleme (Auditability)

Denetlemeden kastedilen "sistemin insan veya makineler tarafından yapılan tüm eylemlerin izlenebilirliğinin sağlanabilmesi" olarak tanımlanmaktadır(Cherdantseva, Hilton, Rana ve Ivins, 2013: 57). Bir diğer deyişle denetlenebilirlilik, veri tabanındaki öğelere erişen veya değiştiren kişileri takip edebilme eylemedir (Fariborz, Farahmand, Sharp, Enslow: 2005: 204).

Bir başka deyişle denetlenebilirlik, sistem davranışının tüm geçmişi üzerine uygulanan tüm ilgili eylemlerin tarihsel kayıtlardan yeniden oluşturabilmesiyle ilgilidir (Yan, Qian, Sharif, Tipper, 2012: 1002). Bu güvenlik amacı çoğunlukla olaydan sonra sistemdeki arızaların keşfedilmesi ve sebeplerinin bulunması ve bir güvenlik olayı arızasının veya sonuçlarının kapsamını belirlemekle ilgilidir. (Yan, Qian, Sharif, Tipper, 2012: 1002).

Üst düzey yöneticiler için denetlenebilirlik, sonuçların dayandığı herhangi bir sistem için merkezi bir kavramdır. Sistemin denetlenebilir olduğuna dair güvence sağlamak için sistem, sonuçlarının güvenilir olduğunun kanıtını sağlamalı ve işlemlerin, depolanmış verilerin ve çıktıların bağımsız, nesnel bir şekilde incelenmesinin yeterli güvenilirliği belirleyebileceği özelliklere sahip olmalıdır. Güvence, gizlilik ve bilginin varlığı ile ilgili kanıtların sunulması gerekmektedir. Sistemin denetlenebilirlik özelliklerinin kuruluştaki tüm

düzeylerde ve kuruluş sınırları boyunca gerekli olması çok önemlidir. Bu sıklıkla denetimler, bozulan ya da çoğaltılan bölümler arasındaki arabirimdedir(Hinde, 1996: 25).

Sistemlerin kapsamı değiştikçe ve sistemde yeni teknolojiler kullandıkça, kontrollerin yeri ve amaçları yeni sistem unsurlarına geçme eğilimi göstermektedir. Bir sisteme eklenen her yeni eleman, önemli kontrollerin yerini değiştirme ve değişen derecelerde güvenilirliğe tabi tutma potansiyeline sahiptir. İşletim sistemlerinin, ağların veya hatta uygulama sistemlerinin özelliklerinden daha önemli olanı, yönetimin kuruluş politikaları ve güvenlik ve kontrolle ilgili tutumlarıdır. Doğal olarak güvensiz bir sistem etkili kontrollerin bulunduğu bir ortamda güvence altına alınabilmektedir. Tersine en güvenli sistemler, çevre kontrol sistemlerinin etkisiz uygulamasıyla tehlikeye girebilmektedir. Denetlenebilirlik hedefleri, belirli sorumlulukları tanımlamış olan yönetim tarafından formüle edilmeli ve yayınlanmalıdır (Hinde, 1996: 25).

2.4.6.1. Bilgi denetimi

Bilgi denetimi (IA), Buchanan ve Gibb (2007) tarafından "bir organizasyonun bilgi kaynaklarını ve bilgi akışını, etkin ve verimli bilgi sistemlerini kolaylaştırmak ve değerlendirmek için için tanımlamak ve değerlendirmek " olarak tanımlanmaktadır. Buchanan ve Gibb (2008), 1990'ların sonunda ve 2000'lerin başında kurulan ortak IA metodolojilerinin karşılaştırmalı analizinde, IA için yedi basamaklı bir metodolojik taban çizgisi önermektedir.

i. Denetimin amaçlarını, projenin kapsamını belirleyerek, seçilen metadolojiyle iletişim ve iş stratejilerini geliştirirek planlama
ii. Bilgi kaynakları veri tabanında veri toplama, anket tasarımı ve dağıtımı, odak grupları tutma ve kişisel mülakatlar yapma
iii. Toplanan verilerin ve araştırmaların incelenmesi

iv. Tavsiyeleri formüle etme, ve bir değişim yönetim planı geliştirilmesi

v. Yazılı raporlar, sunumlar ve seminerler, web sayfaları ile ilgili kişilere tavyiselerde bulunma

vi. Uygulama yoluyla tavsiyelerin uygulanması önerilen programlar, resmi değişim planları, uygulama sonrası stratejiler, ve bilgi politikaları.

vii. Sürekli bilgi servis yönetimini ölçmek ve değişiklikleri düzenli bir bilgi denetimi ve hizmet değerlendirmesi döngüsüyle değerlendirmek.

Robert ve Chun (2016) tarafından 2011 ve 2016 yıllar arsında bilgi denetimiyle ilgili yazılan makalelerde, bilgi denetimiyle ilgili yapılmış araştırmalara olan ilginin çok olduğu ve 2011 yılından bu yana istikrarlı bir şekilde bu ilginin devam ettiği ortaya koyulmuştur. Ancak hem bilgi denetimi araştırmacıları hem de uygulayıcılar uygulamanın daha yaygın şekilde kullanılması için daha çok iş olduğunu belirtmiştir. Bilgi yönetiminin hemen hemen her sektörde bir zorunluluk haline geldiği böyle bir dönemde, bilgi denetimiyle ilgili araştırma ve uygulamaların diğer yönlerden bilgi yönetiminin gerisinde kalmış olmasını talihsizlik olarak görüldüğü belirtilmiştir (Robert ve Chun, 2017: 1385).

Yetkili kişilerin gün içerisinde yaptıkları eylemler, şirketin bilgi güvenliğinin sağlanabilmesi açısından önem arz etmektedir. Bir çok site, bilgisiyarınıza sızabilen, zarar verebilen virüsler ya da solucanlar içermektedir. Bütün bunların önüne geçebilmek için kulanıcıların denetlenebilirliği önem arz etmektedir.

2.4.7. İnkar Edememe (Non-repudition)

Bu veri sayesinde alıcı ve gönderici aldıkları mesajları gizleyememektedir. Özellikle gerçek zamanlı işlem gerektiren finansal sistemlerde işlem görmektedir. Bunun yanı sıra belli

bir potansiyel saldırıya karşı sistemi korumaya yönelik olduğu söylebilmektedir (Cherdantseva, Rana, Ivins ve Hilton, 2016: 50).

İnkar edememe, bir davada tarafları diğer tarafa karşı korumak ve belirli bir olay veya eylemin veriler üzerinden değişiklik yapılmadan, eylemin gerçekleşip gerçekleşmediğini kanıtlamak için önemli verilerdir (Zhou ve Gollman, 1997: 270). Bu anlaşmazlıkların çözümünü desteklemek için karşı konulmaz kanıtlar toplanmaktadır. İnkar edememeyle ilgili uluslararası iki standart vardır: ISO / IEC 10181-4 [3] ve ISO / IEC 13888 . ISO / IEC 10181-4. ISO 7498-2'de tarif edildiği gibi reddetme ve reddetme hizmetleri kavramını genişletmekte ve bu hizmetlerin geliştirilmesi ve sağlanması için bir çerçeve sağlamaktadır.

ISO / IEC 13888 (2010) üç bölümden oluşmaktadır. Genel bir inkar edilme modeli (ISO/IEC DIS 13888-2010. tarih yok) simetrik ve asimetrik şifreleme tekniklerine dayanan bir dizi inkar edilemez mekanizma sağlamaktadır.

ISO / IEC 13888-1'de, reddedilememe tanımı şu şekilde analiz edilmiştir:

i. Yaratılmamaya itiraz etme.
ii. Teslimatın reddedilmesi.
iii. Bilgi reddedilmesi.
iv. Menşe feragat etmeme.
v. Makbuza itiraz edilmemesi.
vi. Göndermenin reddedilmesi.
vii. Sunulamayın reddedilmesi.
viii. Ulaştırmayı reddedilme.

Bu çalışmada bilginin reddedilmesiyle üzerinde durulmaktadır. Günümüzde reddedilmeyen hizmetler çoğunlukla ileti taşıma sistemlerinde ve elektronik ticarette yer almaktadır(Zhou, Gollman, 1997: 270). Yaygın olarak kullanılan iki ileti gönderme sistemi İnternet e-posta sistemidir Borenstein ve Freed, 1993) ve (Crocker 1982). Bir ileti taşıma

sisteminde üç taraf vardır: Gönderen, alıcılar ve teslimat ajanı. Reddedilmemeyle ilgili üç güvenlik unsuru X.400 (CCITT 1988) aşağıda tanımlanmaktadır:

- Menşe Reddedilme Yasağı (NRO) mesajın orijinalinin kanıtı olan bir alıcıya mesajı gönderen kişiye mesaj gönderilmesini yanlışlıkla reddetme girişimine karşı koruma sağlamaktadır. Bu, hizmetin sağlayıcı yaratıcısıdır.
- Teslimatın reddedilmemesi, mesajın göndericisi tarafından, mesajın teslim edilmesinin kanıtıyla, alıcılar tarafından mesajın kabul edilmesini yanlışlıkla reddetme girişimine karşı koruma sağlamaktadır. Bu, hizmetin sağlayıcısı alıcıdır.
- Göndermeyi reddetme (NRS), iletiyi gönderenin kimliğini gösteren bir ileti gönderen kişiye, iletim aracısı tarafından iletinin orijinal olarak belirtilen alıcılara teslim edilmek üzere gönderildiğini yanlış şekilde reddetme girişimine karşı önlem almaktır. Bu, hizmetin sağlayıcı teslimat ajanıdır.

Teslimatın reddedilmesi için yukarıdaki tanımlama kafa karıştırıcıdır. Bunun yerine aşağıda belirtilen unsurlar daha açıklayıcıdır (Zhou ve Gollman, 1997: 270).

Teslimatın reddedilmemesi (NRD), gönderenin orijinal olarak belirtilen alıcılara teslim edildiğinin kanıtı olan bir mesajın yaratıcısı olmasını sağlamaktadır. Bu, hizmetin sağlayıcı teslimat ajanıdır.

Makbuzun reddedilmemesi (NRR), alıcıyı yanlışlıkla mesajı kabul etmeyi reddetme girişimini engelleyecek bir mesajın göndericisi tarafından gönderilmektedir. Bu, hizmetin sağlayıcısı alıcıdır.

Elektronik ticarette ana konu, ödeme ve mal teslimatının verimli, güvenilir ve güvenle nasıl başarılacağı ve muhtemel anlaşmazlıkları gidermek için ödeme ve mal teslimi hakkında uygun kanıt sağlamaktır (Bellare, Garay ve Hauser, 1995: 2). NetBill sistemi, ödeme ve mal teslimatını atomik sertifikalı teslimat adı verilen tek bir operasyona bağlayarak adil değişim sağlamaktadır. Tüketiciye ödeme yapılmadan önce malların teslimatından garanti verilmekte

ve tüccar, ödeme yapılana kadar tüketicinin mallara erişemeyeceğini garantilemektedir Cox, Tygar ve Sirbu, 1995: 11).

2.4.7.1. Dijital İmza

Özel anahtarın yetkisiz kullanımı: Diğer bölümlerde belirtildiği gibi, özel anahtar bir bilgisayarda veya bir aygıta kaydedilmektedir. Kullanıcı, özel anahtar için güvenli depolama alanı sağlamakla yükümlüdür. Kullanıcı, özel anahtardan yeterli derecede koruma sağlamazsa, PKI güvenliği ihlal edilmektedir (Perez ve Laurie, 2000: 257).

2.4.8. Mahremiyet

En geniş düzeyde, özellikle Avrupa açısından, mahremiyet, Birleşmiş Milletler İnsan Hakları Evrensel Beyannamesi'nde (1948) ve daha sonra Avrupa İnsan Hakları Sözleşmesi'nde ve ulusal anayasalarda ve hak tarikatlarında yer alan temel bir insan haktır. 'Yalnız kalma hakkı' 'kendimiz hakkında bilgi kontrolü' 'bireylerin ve kuruluşların, toplama, kullanma, ifşa etme'yle ilgili hak ve yükümlülükleri arasında değişen çeşitli gizlilik biçimleri vardır (Warren & Brandeis, 1980). Kişisel tanımlanabilir bilgilerin toplanması, kullanılması, ifşa edilmesi ve tutulması ile ilgili, bireylerin ve kuruluşların hak ve yükümlülükleri gizlilik ihlali ve bağlamsal bütünlükten kaynaklanan zararları ele almaktadır (Nissenbaum 2004)

Ticari tüketici bağlamında mahremiyet, müşterilerin kişisel bilgilerinin korunması ve uygun şekilde kullanılması ve müşterilerin kullanımıyla ilgili beklentilerini karşılamasını gerektirmektedir (Perason, 2012: 220). Uygun olan yasalar, yürürlükteki kanunlara, kişisel bilgilerin toplanması, kullanılması ve ifşa edilmesine ilişkin beklentilerin ve diğer bağlamsal

bilgilerin köklü olmasına bağlıdır. Bu nedenle mahremiyet, koşullar altında kişisel bilgilerin uygun şekilde kullanılması gerekmektedir.

Veri koruması kişisel bilgilerin yönetimidir ve gizlilikle ilgili kanun ve yönetmeliklerle bağlantılı olarak Avrupa Birliği'nde sıklıkla kullanılmakta, ancak ABD'de bu terimin kullanımı güvenlik üzerinde yoğunlaşılmaktadır.

"Kişisel bilgiler" ve "kişisel veriler" terimleri genel olarak Avrupa'da ve Asya'da kullanılırken, ABD'de "Kişisel Tanıtıcı Bilgi" (PII) terimi normal olarak kullanılmaktadır. Ancak genellikle aynı kavramı belirtmek için kullanılmaktadır. Bu, belirli bir kişiye izlenebilecek bilgiler olarak tanımlanmakta ve ad, adres, telefon numarası, sosyal güvenlik veya ulusal kimlik numarası, kredi kartı numarası, e-posta adresi, şifreler, doğum tarihi gibi bilgileri içermektedir. Mevcut Avrupa Birliği (AB) Kişisel verilerin tanımı şudur:

'Kişisel veriler', tanımlanmış veya tanımlanabilir doğal bir kişiyle veri konusuyla ilgili herhangi bir bilgiyi ifade etmektedir. Tanımlanabilir bir kimse, doğrudan veya dolaylı olarak, özellikle bir kimlik numarasına veya onun fiziksel, fizyolojik, zihinsel, ekonomik, kültürel veya sosyal kimliğine özgü bir veya daha fazla faktöre referans olarak tanımlanabilen verilerdir (European Commision, 1995).

Hassas kişisel bilgiler olarak kabul edilen bilgilerin tanımı, yargı alanına ve hatta belirli düzenlemelere göre değişiklik gösterse de, bazı kişisel veri öğeleri diğerlerinden daha duyarlı kabul edilmektedir. Mahremiyet, bir güvenlik unsuru olmasına rağmen, kişisel bilgiler için mahremiyet mekanizmalar ile ilgilidir ve güvenlikten farklıdır. Diğer yandan, güvenlik mekanizmaları, kimlik doğrulama, erişim denetimleri, kullanılabilirlik, gizlilik, bütünlük, saklama, depolama, yedekleme, olay tepkisi ve kurtarma gibi koruma mekanizmalarının sağlanmasına odaklanmaktadır. Gizlilik, yalnızca kişisel bilgilerle ilgiliyken, güvenlik ve gizlilik tüm bilgilere ilişkin olabilmektedir (Perason, 2012: 220).

Mahremiyet, Avrupa'da bir insan hakkı olarak görülürken, Amerika'da geleneksel olarak belirli bağlamlarda insanlara zarar vermemek için mahremiyet bir insan hakkından daha fazla bir öneme sahiptir. Mahremiyet, karmaşık ama önemli bir kavramdır ve buna karşılık kişisel bilgilerin toplanması ve işlenmesi, dünyanın birçok ülkesinde düzenlemeye tabidir (Perason, 2012: 220).

2.4.8.1. Kurumlar için Mahremiyet

Kuruluşlar için mahremiyet, kişisel bilgilerin yönetildiği yasalar, politikalar, standartlar ve süreçlerin uygulanmasını gerektirmektedir. 1970'lerde ABD'de geliştirilen ve daha sonra Ekonomik İşbirliği ve Kalkınma Teşkilatı (OECD) ve Avrupa Konseyitarafından ilkeler olarak benimsenen ve ilan edilen adil bilgi uygulamaları, dünya çapında çoğu veri koruma ve gizlilik yasalarının temelini oluşturmaktadır. Bu ilkeler genel olarak aşağıdaki şekilde tanımlanmaktadır (Perason, 2012: 220);

i. Veri toplamanın sınırlandırması: Veriler uygun olduğunda, veri konusunun onayı ile yasal olarak toplanmalı ve gerekli verilerle sınırlandırılmalıdır.
ii. Veri kalitesi: Veriler ilgili olmalı ve doğru tutulmalıdır.
iii. Amaç spesifikasyonu: Amaç veri toplama sırasında belirtilmelidir.
iv. Kullanım sınırlamaları: Bireyin onayı olmadan kişisel veriler başka amaçlarla kullanılmamalıdır.
v. Güvenlik: Kişisel veriler makul derecede güvenlikle korunmalıdır.
vi. Açıklık: Bireyler, kişisel verilerin neler olduğunu bulabilmeli ve bir kuruluş tarafından nasıl kullanılacağı bildirilmelidir.

vii. Bireysel katılım: Bir birey ve bir veri denetleyicisi tarafından tutulan tüm bilgilerin ayrıntılarını elde edebilmeli ve yanlış olması durumunda itiraz etmelidir.

viii. Hesap verebilirlik: Veri denetleyicisi bu ilkelere uymaktan sorumlu olmalıdır.

Bu çerçeve, bireysel sözleşmelere ihtiyaç duymadan katılımcı ülkelerde, kişisel bilgilerin paylaşılmasını sağlayabilmektedir. Veri toplama, konu erişim hakları ve veri akışı kısıtlamaları da dahil olmak üzere kuruluşlara gereksinim duyulmaktadır (Pearson 2012).

Gizlilik meseleleri şirketin rolüne bağlıdır. Bir kuruluş, kişisel verilerin bir nöbetçisi olabilmekte, son kullanıcı ise kişisel bilgilerini toplayabilmekte veya sadece başka bir kuruluş için dış kaynak hizmetleri sağlayabilmektedir. Yasal olarak, kuruluşun bu durumda bir veri denetleyicisi veya veri işlemcisi olup olmadığına bağlı olarak gereksinimler tamamen değişmektedir (Perason, 2012: 221);

Şirketler gizlilikle başa çıkmak için elinde bulundurdukları kaynaklar bakımından farklılık göstermektedir. Birçok büyük kurum ve kuruluşlarda uyumluluk sağlamak için bir Baş Gizlilik Görevlisi ve gizlilik personeli bulunmaktadır. Daha küçük organizasyonlar, çoğunlukla kalifiye mahremiyet uzmanları seçmek için kaynakları ve bunun yerine sorumlu kimseyi atayan uzmanlara sahip değildir (Perason, 2012: 221);

Bazı şirketler, herhangi bir ihlal yaptıkları tespit edilirse, konuyu görmezden gelmeyi ve cezaları ödemeyi seçebilmektedir. Ancak yazılıma geldiğinde düzenlemeler, uygulama faaliyetleri ve yaptırımlar şu anda dünyada artmaktadır. ABD, bir Tüketici Gizlilik Hakları Sözleşmesi getirmekte ve AB Veri Koruma Yönergesi ve Yönetmeliğini revize etmektedir. (WhiteHouse,2012)

2.5. Konuyla Ilgili Daha Önce Yapılan Çalışmalar

Karabacak (2003) tarafından yapılan çalışmada Bilgi Güvenliği Risk Analizi olarak adlandırdığı, günümüz teknolojisi ile örtüşen ve kurumların gereksinimlerini karşılayacak bir bilgi güvenliği risk analizi yöntemi önermiştir. Bu çalışmanın sonucunda BİGRA yöntemi ile standart diğer yöntemler karşılaştırılmıştır.

Zeydan (2006) yılında yaptığı çalışmada, kullanıcıların internete bağlıyken bir çok tehditle karşı karşıya olduğunu gözlemlemiştir. Bu saldırılar karşısında önlem alabilmek için antivirüs, güvenlik duvarı, anticasus gibi yazımların bilgisayarda yüklü olmasını ve kullanıcıların bu tarz programların güncel tutulması gerektiğini vurgulamıştır.

Erkan (2006) çalışmasında. ISO/IEC 27001: 2005 ve ISO/IEC 17799:2005 standartlarını inceleyerek Bilgi Güvenliği Yönetim Sistemleri ile ilgili aşamalara değinmiştir.

Öğüt (2006) yapmış olduğu çalışmada Türkiye'de ve dünyada ki bilgi güvenliği ile ilgili kanunları ve bilişim altyapısından bahsetmiştir.

Canberk ve Sağıroğlu (2006) çalışmalarında bilgi güvenliği ile ilgili temel kavramlardan yer vermiş ve bilgi güvenliğini oluşturabilmek için gerekli güvenlik süreçlerinden bahsetmiştir. Sonuç olarak kurumlar bütün güvenlik önemlerini alsa dahai, insan kaynaklı tehditlerden dolayı, kurumların bilgi güvenliğini %100 oluşturamayacağı sonucuna varmıştır.

Albreschtsen (2007) çalışmasında, Norveç'teki banka ve bilişim teknoloji şirketlerindeki çalışanlar üzerinde yapmış olduğu araştırmada çalışanların bilgi güvenliği deneyimlerini, farkındalık sevkiyerini ve kullanıcı davranışlarını incelemiştir. Bilgi güvenliğinde yaşanan sıkıntıların kaynağının, çalışanların bilgi güvenliği farkındalıklarının eksik olmasından kaynaklandığını belirtmiştir.

Tekerek (2008) çalışmasında, Bilişim sektöründe yaşanan gelişmeler sonucunda e-

kavramların (e-ticaret, e-rezervasyon, e-okul vb.) günlük yaşamda kullanımının giderek yaygınlaştığından dolayı bilgi güvenliği risk ve tehditlerinin de artığından bahsetmiştir.

Çetinkaya (2008) yapmış olduğu çalışmada, işletmelerin bilgi güvenliği başarı seviyesini ölçebilmek için ISO/IEC 27001: 2007 Bilgi Güvenliği Yönetim Sistemi standartların da web tabanlı bir test aracı geliştirilmiştir. Test aracında bilgi güvenliği altyapısının değerlendirilmesini ölçmek için 23 firmaya kurumda bilgi güvenliği politikası var mı, çalışanlar ile paylaşıldı mı, farkındalık yaratıldı mı, çalışanlara gerekli eğitimler verildi mi, kurallara uyulmama durumunda yazılı bir disiplin süreci var mı gibi sorular yöneltilmiştir. Araştırma sonucunda firmaların uyum, iş sürekliliği yönetimi, bilgi güvenliği ihlal olay yönetimi konularında uygulama eksikliği olduğu tespit edilmiştir.

Şahinaslan vd. (2009) yaptığı çalışmada bilgi güvenliğinin virüs programları, güvenlik duvarı gibi önlemlerin alınmasının yeterli olmadığını aynı zamanda kullanıcıların farkındalık düzeyinin artırılması gerektiğini vurgulamıştır.

Türkiye'de bilgi güvenliği sorunları ve çözüm önerileri üzerine Eminağaoğlu ve Gökşen'in (2009) yapmış oldukları çalışmada, bilgi güvenliğinde yapılan en yaygın hatalar ortaya konulmuş ve hatalara karşı alınabilecek önlemler ile çözüm önerileri üzerinde durulmuştur.

Adıgüzel (2009) yapmış olduğu çalışmada, internet bankacılığının müşterilere sağladığı kolaylıklardan bahsetmiştir. Müşterilerin güvenlik korkularından dolayından internet bankacılığı kullanımının azaldığı sonucuna varmıştır.

İnsan unsurunun göz önünde bulundurulmaması, bilginin güvenliğini riske atacağı gibi uygun bir şekilde korunamamasına neden olacaktır. Bilgilerin koruması için önlem alınmaması durumunda aşağıdaki riskler oluşmaktadır (Sayarı, 2009):

- Kuruma ait gizli ve hassas bilgiler ile kurumun işlerliğini sağlayan bilgi ve süreçler başka rakiplerin eline geçebilmesi

- Kurumun ismi, güvenilirliği ve itibarı toplum gözünde zarar görebilmesi
- Ülke çıkarının zarar görmesi söz konusu olabilmesi
- İş sürekliliğinin aksamasına sebebiyet verebilmesi
- Müşteri mağduriyeti ve memnuniyetsizliğine sebep olabilmesi
- Yasal yaptırımlara ve tazminatlara maruz kalması

2011 yılında Eurobarometer tarafından Avrupa Birliğinde ülkelerinde yapılan araştırma sonucunda, %10'luk dilimininin günlük hayatta kimlik bilgilerini, %50'lik kısmı sosyal bilgilerini, %90 kısmı ise sahip olduğu önemli bilgilerini paylaşmadıklarını belirtmiştir.

Eminağaoğlu (2011) yapılan çalışmada bir sağlık tesisinde özel bir bilgi güvenliği risk anketi hazırlanmış, kurumda anket uygulanmış ve elde edilen sonuçları değerlendirmiştir. Bu sonuçlara göre, hastanede hangi risklerin daha yüksek düzeyde / daha öncelikli oldukları belirlenmiş ve listelenmiştir. Buna göre en önemli tehditler kötü niyet, veri kaybı, izinsiz erişim,tahribata uğramış veri, bilgisayar virüsleri, deprem, sel, doğal afetler sonuçlarına ulaşılmıştır.

2012 yılında Milli Eğitim Bakanlığı 784 çalışanına uyguladığı çalışmada, bilgi güvenliği farkındalık anketi uygulanmıştır. Bu anketle çalışanların bilgi ve sistem güvenliğine önem verdikleri görülmüştür. Anketi yanıtlayan kişilerin %42,22'si şifre güvenliği için gerekli önlemi almadıkları ve %15,71'i unutmamak için tüm şifreleri aynı yaptıkları tespit edilmiştir. %65,37'si şifrelerini kimseye söylemediklerini belirtmiştir. Çalışanların %67,92'si anti virüs yazılımı bulundurmadığını ve %7,91'i nereden geldiği belli olmanyan e-posta ekinde gelen dosyaları kesinlikle açmadığını ve hemen sildiğini belirtmiştir (MEB, 2013).

Ketizmen ve Ülküderner (2012) kamu ve özel sektörün belirlenen şartlar dahilinde kamu ve özel sektörde çalışanların kişisel verilerin kaydetmesi gerektiğini ve bu verilerin

başka kişilerce ele geçirilmesini önlemek için devletin gerekli çalışamalar yapması gerektiğini belirtmiştir.

Haklı (2012) çalışmasında bilgi güvenliği ile ilgili kriterlerin incelenmiş ve kriterlerin öneminden bahsetmiştir. Kurumların bilgi güvenliklerin nasıl sağlanacağıyla ilgili önerilerde bulunmuştur.

Mart (2012) Türkiye'nin farklı illerinde bulunan 501 kişiyle yaptığı araştırmada, katılımcıların bilişim kültüründen ne şekilde faydalandığını tespit etmek istemiş ve bu kültürde yaşın cinsiyetin ve eğitim durumunun etkisini ölçmeye çalışmıştır. 45 yaş üzeri katılımcıların teknolijiden diğer yaş grubundanki katılımcılara göre daha fazla yararlandığını tespit etmiştir. Bunla birlikte teknoloji kullanımının cinsiyet eğitim ve mesleklere göre anlamlı bir fark olmadığı sonucuna varmıştır.

İnternet dünyasında oluşan ilerlemeler insanların hayatlarını daha kolay hale getirmektedir. Bütün bunlar sonucunda, şirketler erişmek istedikleri hedef kitlesine daha kolay ulaşabilir hale gelmektedir. Ancak bütün bu erişebilirlik, aynı zamanda firmalara bir çok tehditi de beraberinde getirmekte ve hırsızlık saldırıları, savunnma tekniklerini de berarberinde getirmektedir. Bu noktada bilgi güvenliği ve iletişim teknolojileri bir bütün olarak düşünülmeye başlanmıştır. Bilişim teknolojilerini uygunsuz kullanma, bireylerdeki risk algısının zafiyeti, bilgi güvenliği tehditlerinden habersizlik gibi bir takım olumsuzlukları ve telafisi güç bilgi güvenliği risklerini de bünyesinde barındırmaktadır. İnsan faktörü gözardı edilmesi durumunda bilgi güvenliği riskini gidermeye çalışmanın çok faydalı ve etkili olmadığı tespit edilmiştir (Mart 2012).

Keser ve Güldüren (2015) geliştirdikleri Bilgi Güvenliği Farkındalık Ölçeğiyle, yükseköğretim kurumlarında çalışan 363 öğretim üyesi üzerinde yaptıkları anket çalışması sonucunda öğretim elemanlarının bilgi güvenliği farkındalık düzeylerini belirlemeye çalışmıştır.

Kapanoğlu (2016) Öğretmenlerin interneti güvenli kullanım durumlarını ve bilgi güvenliği farkındalık düzeylerini tespit etmeye yönelik çalışma yapmıştır. Bilgi güvenliği farkındalıklarının branşlara, alınana bilgi güvenliği eğitimine öğrenim durumuna, yaşnılan bölgeye internet kullanım süresine ve yaşa göre anlamlı farklılıklar gösterdiğini tespit etmiştir.

Başdandikçi (2017) Adana ilinde sağlık tesisinde bilgi güvenliği risk değerlendirmesi yapma ve kullanıcıların bilgi güvenliği farkındalık düzeyini ölçmeyi amaçlamiştir. Çalışanlar ve özellikle yöneticilerin için bilgi güvenliğinin kritik bir konu olduğunu, bu nedenle kurumlarda bilgi güvenliği politikarlı geliştirilmesi ve bu politikaların tüm çalışanlar ile paylaşılması ve kullanıcılara bilgi güvenliği farkındalıkğı eğitimi verilmesi sonucuna varmıştır.

Tezin modelini oluşturan maddeler daha önce Türkiye'de gerçekleştirilen bazı çalışmalarda model olarak kullanılmıştır. Modelde kullanılan maddeler bir bütün olduğu için daha önce yapılan çalışmalara bu kısımda değinilmiştir. Türkiye'de yapılan çalışmaların CIA ve diğer modeller üzerinden yapılan çalışmalar olduğu görülmektedir. Ancak yapılan taramada, hiç bir çalışmada RMIAS modelinin kullanılmadığı tespit edilmiş

ÜÇÜNCÜ BÖLÜM

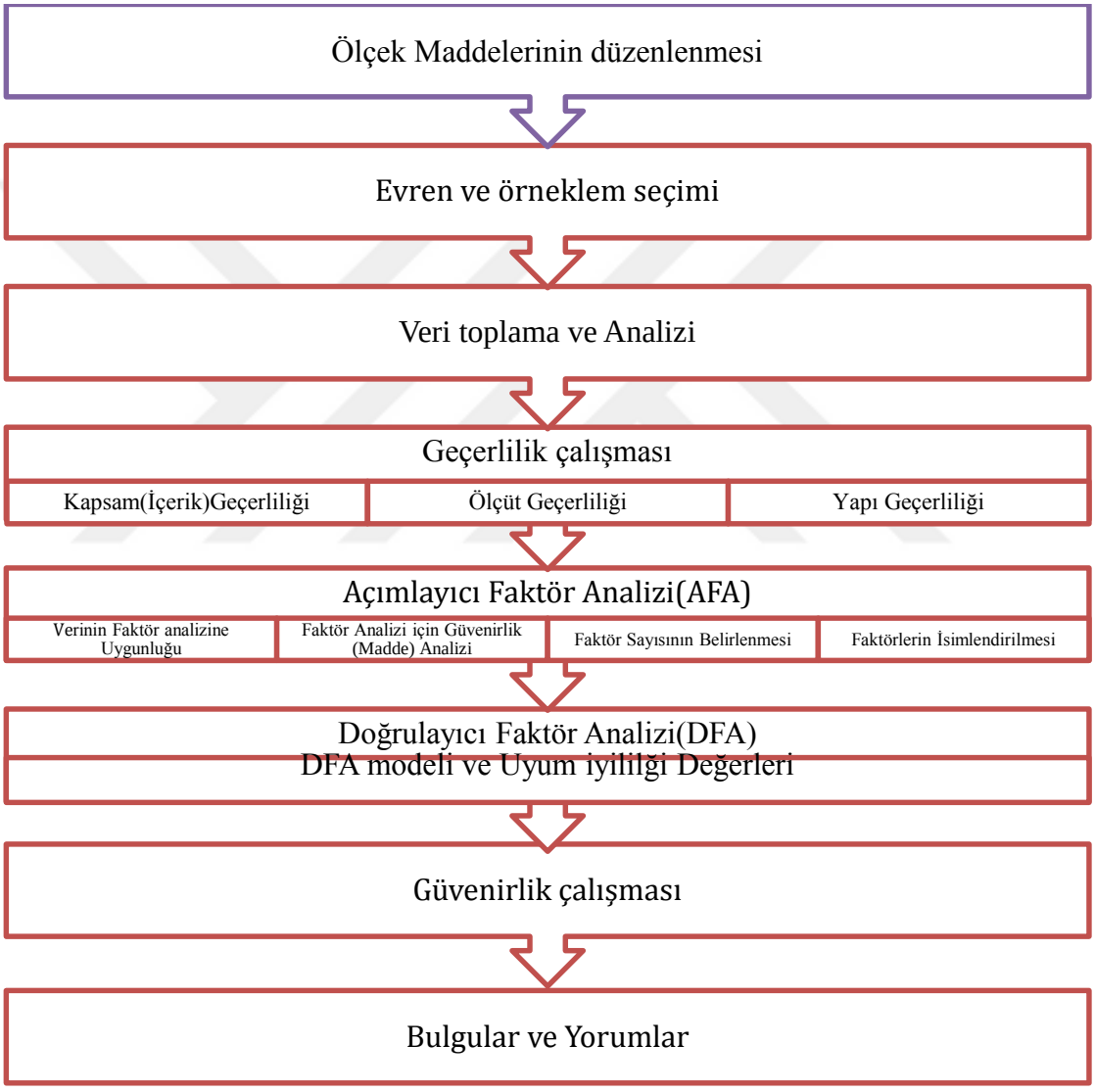
ARAŞTIRMA YÖNTEMI, SONUÇLARI VE YORUMLAMASI

Bu bölümde ölçek maddeleri açıklanarak geliştirilen ölçeğe ait verilerin analizi yapılmıştır. Cherdantseva ve Hilton (2013) Geliştirilen RMIAS modelindeki bilgi güvenliği amacıyla ilgili model temel alınarak literatür taramasına dayalı Likert tipi bir ölçek geliştirilmiştir. Geçerlilik çalışması, Açımlayıcı faktör analizi, Doğrulayıcı faktör analizi ve güvenirlik çalışması yapılmıştır. Şekil 8'da Araştırma basamakları açıklanmıştır.

3.1. Çalışmanın Evreni ve Örneklemi

Araştırmanın amacına ulaşması için kobi çalışanlarının görüşüne başvurulmuştur. Bu amaçla hazırlanan ölçeğin uygulanması için 2017 yılında Türkiye'nin Gaziantep ili sınırlarında faaliyet gösteren tüm kobi çalışanları evren olarak belirlenmiştir. Evren büyük olmasından dolayı örneklem alma yoluna gidilmiştir. Kolayda örnekleme yöntemi tercih edilmiş ve örneklemin ana kütleyi daha iyi temsil edebilmesi için farklı sektörlerde faaliyet gösteren küçük ve orta büyüklükteteki işletmelerde çalışan bireylere ulaşılmaya çalışılmıştır. Yapılan bu araştırma, kullanılacak istatistiksel yöntemlerin sonuçlarına göre değerlendirilecek ve araştırmada iddia edilen hipotezler sınanacaksa araştırmada kullanılacak örneklemin büyüklüğü çalışmanın geçerliliği yönünde önemli olmaktadır. Ölçek geliştirme çalışmaları incelendiğinde Comrey ve Lee (1992), örneklem büyüklüğü olarak 100'ü zayıf, 200'ü orta, 300'ü iyi, 500'ü çok iyi ve 1000'i mükemmel olarak değerlendirmektedir. Guilford (1954) örneklem sayısının en az 200; Aleamoni (1976) ise örneklem sayısının en az 400 olması

gerektiğini belirtmektedir. Bu çalışmalarla birlikte örneklem sayısını, analize dâhil edilen madde sayısına göre belirlenmesi gerektiği görüşünü de öne süren çalışmalar da bulunmaktadır. Nunually (1978), faktör analizinin kullanıldığı bir araştırmada örneklem sayısının madde sayısının 10 katı; Gorusch (1983) 15 katı ve Tavşancıl (2002) ise en az beş katı olması gerektiğini belirtmektedir.



Şekil 8. Araştırma Yönteminin Basamakları

3.2. Veri Toplama Aracının Uygulanması ve Verilerin Toplanması

Bu çalışmada verilerin toplanması için ölçek formu oluşturulmuştur. Ölçek formu iki kısımdan oluşmaktadır. Birinci kısımda katılımcıların özelliklerini belirlemeye yönelik demografik sorularla birlikte kobilerin bilgi güvenliğine yönelik siber risklere karşı aldıkları yöntem ve uyguladıkları teknikleri belirleme yönelik sorulardan oluşmaktadır. Ölçeğin ikinci kısmında ise uzman görüşleri sonunda oluşturulan firmaların bilgi güvenliği ve farkındalığını belirlemeye yönelik 37 madde yer almaktadır. Hazırlanan bu form 800 kişiye uygulanmıştır.

İstatistiksel analizler yapılmadan önce, ölçeğin kobi çalışanları tarafından tam olarak doldurulup doldurulmadığını, bilinçli bir şekilde sorulara cevap verilip verilmediğini belirlemek amacıyla uygulanan ölçek formları incelenmiştir. Bu inceleme sonucunda bazı ölçek formlarının rastgele ve eksik doldurulduğu fark edilmiştir. Bunun sonucunda rastgele ve eksik doldurulan ölçek formları araştırmaya dahil edilmemiştir. Analizler için kullanılacak ölçek form sayısı *756* olarak belirlenmiştir. Analizler bu ölçek formları üzerinde gerçekleştirilmiştir.

3.3. Verilerin Analizinde Kullanılan İstatistiksel Yöntemler

Araştırma için elde edilen verilerin analizi *SPSS 21* istatistik paket programı kullanılarak yapılmıştır. Bağımlı ve Bağımsız gruplarda ikili karşılaştırma için t Testi, Korelâsyon Analizi, Madde Analizi, Faktör Analizi ve iç tutarlılığı belirlemek için Concbach Alfa katsayısı bu program paket programı kullanılarak hesaplanmıştır. Doğrulayıcı faktör analizi ve 5'li model uygunluğu indeks değerleri de AMOS 21 programı yardımıyla hesaplanmıştır. Beşli Likert Tipi ölçeği kullanılmıştır. Ölçeğin ikinci kısmında yer alan

sorular “Kesinlikle katılmıyorum” ile “kesinlikle katılıyorum” arasında değişmekte ve ifadelerde bu derecelendirmeye göre değerlendirilmiştir.

3.4. Kobilerin Bilgi Güvenliği Farkındalığı Ölçeği’nin Geçerlilik Analizi

Geçerlilik ‘bir ölçme aracının ölçülmek üzere hazırandığı amacı, değişkeni ölçmek derecesidir. Bir ölçeğin ‘neyi ne denli ‘isabetli/doğru’ olarak ölçtüğüyle ilgili bir kavramdır (Kurasar, 1995; Öner 1997; Özgüven, 2000; Peirce, 1995; Tezbaşaran, 1996).

Bir ölçme aracının geçerliliğini sınamaya yönelik birçok ölçüt bulunmakla birlikte, bunlar genel olarak üç başlık altında toplanmaktadır (Karasar, 1995; Özgüven, 2000; Polit, Hungler, 1997; Tezbaşaran, 1996):

i. İçerik/Kapsam geçerliği (content validity)
ii. Ölçüt-bağımı geçerliği (criterion-related validity)
iii. Yapı geçerliği (construct validity)

Bu çalışmada geliştirilen ölçek için kapsam, ölçüt ve yapı geçerliliği ayrı ayrı incelenmiştir.

3.4.1. Kapsam/İçerik Geçerliği

Kapsam geçerliğinin amacı, ölçme aracında bulunan maddelerin ölçülmek istenen alanı temsil edip etmediğini bir uzman gruba inceleterek anlamlı maddelerden oluşan bütün oluşturmaktır. Burada sözü edilen uzman kişi hem ölçeğin hazırlandığı bilm alanın iyi bilen hem de ölçek sorusu hazırlama teknik ve yöntemlerini bilen bir kişidir. Uzmanların öneri ve eleştirileri doğrultusunda ölçek yeniden yapılandırılmaktadır(Karasar, 1995; Özgüven 2000; Polit Hungler 1997; Tezbaşaran, 1996).

İçerik geçerliliği uzmanların yargılarına dayanan bir ölçüttür. Ölçeğin içeriğinin yeterli olduğunun garanti altına alacak objektif kriterleri yoktur. Uzmanların çoğunluğnun aynı fikirde olması bir gösterge olabilmektedir (Polit, Hungler 1997; Portney Watkin 1993). Bu kapsamda Kobi Çalışanlarının çalıştıkları firmanın bilgi güvenliği farkındalığını ölçmek için danışman Prof. Dr. Gülçimen Yurtsever ve bir araştırmacının görüşleri alınmış ve bu görüşler literatür araştırmasına da dayandırılarak ölçek geliştirilmiştir.

İkinci Bölümde açıklanan ve Cherdantseva, Rana, Ivins, ve Hilton (2016) tarafından geliştirilen "RMIAS" modeli araştırmanın modeli olarak kullanılmıştır İçeriğin boyutlarının belirlenmesi ölçek geliştirmedeki en zor kısımdır. Bu amaçla bir uzmanlar grubundan yararlanılmasına ve literatür desteğine ihtiyaç duyulmaktadır. Bu amaçla alanında uzman 3 bilişim sistem uzmanı, 2 öğretim görevlisi ve 1 araştırma görevlisiyle birlikte ölçek madeleri geliştirilmiştir. Yapılan görüşmeler sonucunda 41 olan taslak ölçek maddeleri 37 maddeye indirilmiştir. Katılımcıların ölçekte yer alan olumlu ifade içeren maddelere ait cevap puanları 1 ile 5 arasında değerler almış ve cevaplayıcıların ifadeleri 5'e yaklaştıkça önermeye katıldıklarını; 1'e yaklaştıkça ise maddeki ifadeye karşı olumsuz görüşe sahip olduklarını göstermektedir. Katılımcıların olumsuz ifade içeren maddere ait cevap puanları 5 ile 1 arasında tersten değerler almış ve katılımcıların ifadeleri 1'e yaklaştıkça önermeye katıldıklarını; 5'e yaklaştıkça ise önermeye katılmadıklarını göstermektedir.

Tablo 4. Ölçek Maddeleri

Kobilerin Bilgi Güvenliğiyle ilgili Farkındalıkları		
Gizlilik		
1	Knorr ve Rohrig (2015)	Firmamız, yetkimizin olmadığı dosyalara girişlerimizi engeller.
2	Australian Government Department of Defance Intelligence ve Security (2012)	Firmamızda, teknolojik cihazlarda (makina, bilgisayar ve benzeri) izinsiz erişimi engellemek adına gerekli önlemler bulunur.
3	Whitman ve Mattord (2014)	Firmamızda önemli bilgilerin gizliliğinin korunabilmesi için ‘’Bilgi sınıflandırması’’ kullanılır.
4	Whitman ve Mattord (2014)	Firmamızda, önemli bilgilerin gizliliğinin korunabilmesi için ‘’Güvenli belge deposu’’ na benzer önlemler bulunur.
5	Whitman ve Mattord (2014)	Firmamızda önemli bilgilerin gizliliğinin korunabilmesi için ‘’Genel güvenlik politikaları’’ uygulanır.
6	Whitman ve Mattord (2014)	Firmamızda, önemli bilgilerin gizliliğini korunabilmesi için ‘’Bilgi saklama alanı’’ kullanılır.
7	Whitman ve Mattord (2014)	Firmamızda, önemli bilgilerin gizliliğinin korunabilmesi için ‘’son kullanıcıların eğitimine‘’ önem verilir.
Tamlık		
8	Boateng ve OSEİ (2013)	Firmamız, internetten yüklenen bütün dosyaların

		virüs programıyla taranmasına önem verir.
9	Knorr ve Rohrig, 2015)	Firmamızda, müşterilerimle olan iletişimimde, herhangi bir verinin değiştirilmesi olasılığına karşı önlem alınır.
10	Australian Government Department of Defance Intelligence ve Security(2012)	Ciddi bir siber saldırı ile bilgilerimizin zarar görmesi durumunda firmamız önemli derecede etkileneceğini düşünürüm.
11	Jeucken (2005)	Firmamızda, verilerin izinsiz değiştirlmesi konusunda önlem alınır.
Erişebilirlik		
12	Chaptered Proffessional account's canada (2014)	Kullandığımız bilişim sistemlerinin herhangi bir unsurunun (yazılım veya donanım vb.) kendisinden beklenildiği şekilde çalışmaması işlerimizi önemli ölçüde yavaşlatır.
13	Boateng ve OSEI (2013)	Şirketimiz,mail aracılığıyla gelebilecek olan virüslerin sistemimize girmemesi için önlemler alır.
14	Knorr ve Rohrig (2015)	Şirketimiz, dosya erişimlerine ulaşma hızımız yavaşladığında önlem alır.
15	Boateng ve OSEI (2013)	Şirketimiz, mail aracılığıyla zararlı dosyaların sistememize girmemesi için önlemleri göz ardı eder.
İzlenebilirlik Yada Kayıt tutma		
16	Yildirim, Akalp, Aytaç, Bayram (2011)	Firmamızda bilgi sistemlerine üçüncü taraf (dışarıdan) erişim, üst düzey bir yöneticinin onayını gerektirir.

17	Boateng ve OSEI (2013)	Firmamızda evrakların imha işlemi verinin izlenebilirliğini azaltmak için kullanılır.
18	Boateng ve OSEI (2013)	Firmamız verilerin kopyalamasını engeller.
19	Yan, Qian, Sharif ve Tipper, (2012)	Firmamız, dosya yada önemli bir evrak değiştirildiği zaman, değişiklik yapan kullanıcıyı görebilir.
Orijinallik-Güvenirlik		
20	Keller, Powell, Horstmann, Predmore ve Crawford (2005)	Firmamız, siber güvenlik açısından belirlenmiş riskler olduğunu düşünür ve bunlara karşı önlem alır.
21	Chaptered Proffessional account's canada (2014)	Firmamız, önemli evrakların değiştirilme ihtimaline karşı önlem alınır.
22	Kese ve Güldüren (2015)	Firmamız, bilgisayarımıza casus yazılım yüklenmesini engellemek için önlem alır.
23	Meb (2013)	Kimlik hırsızlığına karşı alınması gereken güvenlik tedbirlerini biliyorum.
Denetleme		
24	Yan, Qian, Sharif ve Tipper, (2012)	Firmamız, sistemdeki arızanın kaynağını tarihsel kayıtlardan çıkartabilir.
25	Yan, Qian, Sharif ve Tipper, (2012)	Firmamız sistemde ki değişikliklerden dolayı doğabilecek sorunları engellemek için önlem alır.
26	Yildirim, Akalp, Aytac ve Bayram (2011)	Firmamızda, güvenlik politikalarımızı ihlal eden çalışanlar için resmi bir disiplin süreci vardır.
27	Boateng ve OSEI (2013)	Firmadaki bilgisayarıma Mp3, video benzeri dosyaları indirebilirim.

İnkar Edememe		
28	Cherdantseva, Rana, Ivins ve Hilton (2016)	Firmamız, önemli bilgiler paylaştığımızda karşıdan yazılı onay almamızı ister.
29	Zhou ve Gollmann (1997)	Yazılı onayların, ileride doğabilecek hukuksal problemleri engelleyeceğinin farkındayım.
30	Lagou ve Chondrokoukis (2009)	Firmamızda, Dijital imzaya önem gösterilir.
31	(Zhou ve Gollmann, 1997)	Firmamız, önemli bir evrak silindiği zaman, işlemi yapan kullanıcıyı kayıtlardan bulamaz.
Mahremiyet		
32	Ekonomik İşbirliği ve Kalkınma Teşkilatı (OECD) ve Avrupa Konseyi (1980)	Firmamız, müşterilerimizin rızası olmadan bilgilerini başka amaçlarla kullanmaz.
33	Ekonomik İşbirliği ve Kalkınma Teşkilatı (OECD) ve Avrupa Konseyi (1980)	Firmamız, müşterilerimin bilgilerini başka kurumlarla paylaşmadan önce ilgili kişiye bilgi verir.
34	Chaptered Proffessional account's canada (2014)	Firmamız, müşterilerimizin kişisel bilgilerini olası tehditlere karşı korur.
35	Keser, Güldüren (2015)	Kişisel mahremiyetin ne olduğunu biliyorum.
36	Ekonomik İşbirliği ve Kalkınma Teşkilatı (OECD) ve Avrupa Konseyi (1980)	Müşterimle olan ilişkilerimde kişisel mahremiyete göre hareket ederim.
37	Ekonomik İşbirliği ve Kalkınma Teşkilatı (OECD) ve Avrupa Konseyi (1980)	Firmamız, müşterilerimin bilgilerini başka kurumlarla paylaşmadan önce ilgili kişiye bilgi verir.

3.4.2. Ölçüt Geçerliği

En objektif ve en pratik olan bu geçerlik sınamasında ölçek puanlarının bazı dış ölçütlerle ilişkisi aranır (Gözüm, Aksayan, 2003: 10). Bir testin diğer bir testle edilen sonuçları verme yeteniğidir (Pierce, 1995; Portney, 1993; Wood, 1994). Ölçüt bağımlı geçerliğinin yüksek olma eğilimi olması gerektiğinden dolayı ölçeğin kulanımında öncelikle sonuçları gözden geçirmelidir (Gözüm ve Aksayan, 2003: 10). Bu geçerlik sınamasında en önemli faktör, örneklemin temsil yeteneğidir (Gözüm ve Aksayan, 2003: 10). Temsil yeteneği ne kadar az ise, ölçüt geçerliliği o kadar problemli olur (Peirce, 1995). Bu geçerlik ölçütünü değerlendirmek üzere iki yaklaşım vardır (Gözüm ve Aksayan, 2003: 10);

- **Yordama-Kestirim Geçerliliği(predictive validity):** Ölçekten elde edilen bir ‘’yordayıcı puan’’ ile gelecekteki durumlarla ilgili bir ‘’ölçüt’’e ilişkin değerler arasındaki korelasyon katsayısı belirlenir /Öner, 1997; Özgüven, 2000; Peirce, 1995; Portney, Watkins, 1993; Tezbaşaran, 1996). Bu bir anlamda, yapılan ölçme ile ölçülmeye çalışılan şeyin gerçek hayattaki yansımalarının karşılaştırılmasındaki uyumu gösteren uygulama geçerliliğidir (Karasar, 1995). Ancak bu yöntemde bazı güçlüklerle karşılaşılır (Gözüm,Aksayan,2003: 10). Bunlardan en önemlisi uygulamadaki beklentilerin, ölçütlerin ve kavramların, gözlenebilir değişkenlerle ifade edilmesindeki güçlüktür (Karasar 1995, Portney ve Watkins, 1993).
- **Hemzaman/eşzaman geçerliliği(concurrent validity):** Ölçek puanları ölçüm anında var olan bir ölçütle karşılaştırılır (Gözüm,Aksayan,2003: 11). Benzer ölçek geçerliği olarak da bilinen bu yöntemde, daha önceden geçerliliği saptanmış olan bir ölçeğe gereksinim vardır (Gözüm, Aksayan 2003: 11). Yeni

uyarlanan ölçeğin geçerliğini bulmak için yeni test ve geçerliği yüksek' olduğu bilinen önceki test birlikte uygulanır; bireylerin yeni ve eski testten aldıkları puanlar arasındaki korelasyon hesaplanır ve bu koreleasyon katsayısının yüksek olması beklenir (Özgüven, 2000).

Bu kapsamda Hemzaman/eşzaman geçerliliği yöntemi kullanılmıştır. Bu çalışmada 50 kişilik örneklem grubu üzerinde, 2014 yılında Akademisyenler üzerinde Bilgi güvenliği farkındalığı ölçeği (ABGFÖ) ile Bilgi güvenliği farkındalığı ölçeği aynı anda uygulanmış ve elde edilen sonuçlar arasında korelasyon hesaplanmıştır. Koreleason değeri r = 0,407 olup istatistiksel olarak anlamlıdır (p=0,003<0,05). Elde edilen bu korelasyon değerine göre geliştirilen ölçek ile daha önceki ölçek arasında pozitif yönde ve orta düzeyde bir ilişki olduğu söylenebilir. Bu iki ölçek arasındaki korelasyon değerleri Tablo 7'de verilmiştir.

Tablo 5. Ölçüt geçerliliği korelasyon analizi sonuçları

		KBGFÖ	ABGFÖ
KBGFÖ	Pearson Korelasyon	1	
	N	50	
ABGFÖ	Pearson Korelasyon	,407**	1
	P	,003	
	N	50	50

**. Korelasyon değeri %1 önem seviyesinde anlamlıdır.

3.4.3.Yapı Geçerliliği

Yapı geçerliliği, ölçeğin ilgili kavram ya da kavramsal yapının tümünü ölçme yeteneğini göstermektedir (Portney, Watkins, 1993). Bir ölçeğin ve ondan elde edilen puanın gerçekte ne anlama geldiğini araştırma sürecidir. Bu süreç, ölçeğin ölçtüğü faktörler incelenerek ya da geçerliği araştırılan ölçeğin diğer ölçek ve ölçülerle olan ilişkisini araştırarak gerçekleştirilir. Her defasında ölçekle ilgili yeni bir parça bilgi elde edilerek, yığılmalı bir şekilde ölçeğin yapısı ve puanın anlamı hakkında bilgiler elde edilmektedir (Özgüven,2000). Bir ölçeğin yapı geçerliğini değerlendirmek üzere faktör analizi uygulanmaktadır (Karasar, 1995: Pcircc, 1995;Polit, Hungler, 1997; Portney, Watkins, 1993).

Bu çalışmada da geliştirilen ölçeğinin yapı geçerliği, literatürde en fazla kullanılan Faktör analizi Yöntemi ile incelenmiştir. Faktör analizi, ölçeğin ilgili kavram ya da kavramsal yapının tümünü ölçme yeteneğini göstermektedir. Faktör analizi ölçekteki maddelerin farklı boyutlar altında toplanıp toplanamayacağını değerlendirmek üzere yapılan bir işlemdir. Faktör analizinde amaç, çok sayıdaki maddelerin daha az sayıda faktörlerle ifade edilmesidir. Kendi aralarında yüksek ilişki gösteren maddeler faktörleri oluşturur ve bu faktörlerden her biri ölçmedeki kuramsal yapıyı ifade etmektedir (Eryılmaz 1999; Gözüm, Aksayan 2003; Karasar 1995; Tezbaşaran 1996; Yılmaz, Eryılmaz 2004). Faktör analizi Açımlayıcı (AFA) ve Doğrulayıcı Faktör Analizi (DFA) olmak üzere ikiye ayrılır. Bu çalışmada da geliştirinen ölçeğinin yapı geçerlililiği için hem AFA hemde DFA incelenmiştir. Çakmak ve diğerleri (2014), ölçek geliştirme çalışmalarında ideal durumun Açımlayıcı faktör Analizi (AFA) ve Doğrulayıcı Faktör analizlerinin (DFA) farklı örneklem gruplarından elde edilen veriler üzerinden yapılması gerektiğini ifade etmektedir. Bu çalışmada geçerli sayılan 756 ölçek formu rastgele ikiye bölünerek AFA ve DFA yapılmıştır.(n1=378, n2=378) ilk grup üzerinde AFA, diğer grup üzerinde ise DFA yapılmıştır.

3.4.3.1. Açımlayıcı Faktör Analizi (AFA)

Açımlayıcı Faktör Analizi uygulamayabilmek için iki ön koşul bulunmaktadır: Örneklem büyüklüğünün yeterli olması ve verinin Çok değişkenli Normal dağılımlı olmasıdır. Bu koşulları sınamak amacıyla örneklem büyüklüğünün yeterliği için Kaiser Meyer Olkin (KMO) katsayı değeri hesaplanırken, normallik şartı için Barlett Küresellik testinin manidar olup olmadığı araştırılmaktadır. Örneklem büyüklüğünün yeterliliği için KMO değerinin en az 0.60 olması gerekmektedir (Büyüköztürk, 2003: 120). KMO değeri bu sayıdan küçük ise analize devam edilmemelidir. Ancak KMO değeri 0,90 ve üzeri ise örneklem büyüklüğünün faktör analizi için mükemmel olduğu yorumlanmaktadır (Tavşancıl, 2005; Çokluk ve ark., 2010).

Ölçeğin deneme çalışmasında Tablo 6'da görüleceği üzere KMO değeri 0,942 olarak tespit edilmiştir. Barlett küresellik testi sonucu manidar olarak bulunmuştur ($\chi^2 = 12536{,}497$ sd=666; p=0,00<0,01). Bu sonuçlar, pilot çalışması için elde edilen örneklem verisinin büyüklüğünün faktör analizi için mükemmel ve örneklem verisinin dağılımın çok değişkenli normal dağılımlı olduğu sonucuna ulaşılmıştır.

Tablo 6. KMO ve Bartlett Testi Sonucları

Kaiser-Meyer-Olkin Örneklem Yeterliliği Ölçüsü		,942
Bartlett Küresellik Testi	Ki-Kare Değeri	12536,497
	sd	666
	p	,000

Ölçek geliştirme aşaması öncesinde araştırmacılar tarafından belirlenen tek faktörlü (genel görüş) yapıya uygun olarak geliştirilmek istenmiş ve bu sebeple öncelikle madde analizi birinci örneklem grubuna uygulanmıştır. Madde-toplam puan korelasyonu, ölçek maddelerinden alınan puan ile bütün test puanı arasındaki ilişkinin incelenmesine dayanan

tutarlılık hesaplama yöntemidir (Tezbaşaran, 1996). Madde toplam test korelasyonu, test maddelerinden alınan puanlar ile testin toplam puanı arasındaki ilişkiyi açıklamaktadır (Büyüköztürk, 2004). Bu değerin yüksek olması, ölçme aracının iç tutarlılığının yüksek olduğu anlamına gelmektedir. Ölçeğe ilişkin madde analizi sürecinde madde-toplam korelasyonu 0,30 ve altındaki maddelerin ölçekten atılması uygun görülmektedir (Geuens and Pelsmacker, 2002). Bunun yanında, Büyüköztürk (2002) madde analizi ile madde belirlenmesinde madde-toplam korelasyon katsayısı $r \geq 0,40$ değerinin çok iyi maddelere ve $0,30 \geq r \geq 0,39$ iyi maddelere ait olacağını ifade etmektedir. Bu ölçek için yapılan madde analizi sürecinde, bu düzey "0,40" olarak belirlendiğinden, bu koşulu sağlamayan 4 maddenin (S2, S14, S17 VE S18), ölçeğin ölçmesi istenen durumu ölçmeye olan katkısının az olduğu düşünüldüğünden ölçekten çıkarılmasına karar verilmiştir. Kalan 33 maddenin madde-toplam korelasyonları $0,50 \leq r \leq 0,81$ arasında değişmektedir. Daha sonra ölçeğin ön uygulama verilerinden elde edilen toplam puanlar hesaplanmıştır. Ölçek maddelerinin % 27 alt-üst gruplar arası (N1-n1 =102, N1-n2 =102) ayırt ediciliğine, bağımsız gruplar için t testi yardımıyla bakılmıştır. Yapılan analiz sonucunda 37 maddenin her birinin t testi sonuçlarına göre istenilen düzeyde ($p<0,01$) ayırt edici olduğu görülmüştür. Madde analizi sonucunda ölçekte yer alan 37 maddenin analiz sonuçları Tablo 7'de sunulmaktadır.

Tablo 7. Madde Analizi

Madde	Grup	N	Ortalama	Standart Sapma	t-değeri	p	Madde Toplam Korelasyonu
S1	Alt	102	2,4216	1,26206	-12,167	0,000	,595
	üst	102	4,2059	,77509			
S2	Alt	102	2,1863	,93056	-19,152	0,000	,232
	üst	102	4,3627	,67177			
S3	Alt	102	2,5294	,95135	-15,223	0,000	,648
	üst	102	4,1961	,56357			
S4	Alt	102	2,1667	1,04439	-20,233	0,000	,756
	üst	102	4,5686	,58884			
S5	Alt	102	2,5784	1,06647	-10,991	0,000	,583
	üst	102	4,0686	,85896			
S6	Alt	102	2,1078	,75658	-23,179	0,000	,812
	üst	102	4,3235	,59970			
S7	Alt	102	2,3725	1,06168	-16,232	0,000	,718
	üst	102	4,3824	,66069			
S8	Alt	102	2,7549	1,14698	-10,923	0,000	,504
	üst	102	4,2353	,74696			
S9	Alt	102	2,6765	,93514	-14,084	0,000	,634
	üst	102	4,2745	,66238			
S10	Alt	102	2,5392	1,06865	-13,736	0,000	,621
	üst	102	4,2549	,67025			
	üst	102	4,1863	,90903			

Madde	Grup	N	Ortalama	Standart Sapma	t-değeri	p	Madde Toplam Korelasyonu
S11	Alt	102	2,5294	1,01187	-13,842	0,000	,628
	üst	102	4,3039	,65686			
S12	Alt	102	2,7157	,82507	-14,856	0,000	,622
	üst	102	3,9608	,85506			
S13	Alt	102	2,8529	,89439	-10,583	0,000	,717
	üst	102	3,8922	,96377			
S14	Alt	102	2,1078	,75658	-7,982	0,000	,248
	üst	102	4,2157	,63911			
S15	Alt	102	2,8529	1,00884	-21,495	0,000	,630
	üst	102	3,8333	,89091			
S16	Alt	102	2,8431	,79285	-7,357	0,000	,796
	üst	102	4,0098	,94915			
S17	Alt	102	2,1176	1,01761	-9,527	0,000	,292
	üst	102	4,1569	1,06933			
S18	Alt	102	2,3431	1,04829	-13,952	0,000	,257

Madde	Grup	N	Ortalama	Standart Sapma	t- değeri	p	Madde Toplam Korelasyonu
S19	Alt	102	2,1765	,96894	-13,416	0,000	,588
	üst	102	3,8137	,78008			
S20	Alt	102	2,3922	,86924	-13,293	0,000	,746
	üst	102	4,3627	,71462			
S21	Alt	102	2,3725	1,07096	-17,686	0,000	,710
	üst	102	4,3529	,66967			
S22	Alt	102	2,5098	,94130	-15,835	0,000	,700
	üst	102	4,5784	,62038			
S23	Alt	102	2,0098	,93866	-18,532	0,000	,729
	üst	102	4,3529	,69861			
S24	Alt	102	2,6275	1,16824	-20,224	0,000	,626
	üst	102	4,4020	,60132			
S25	Alt	102	2,2549	,87525	-13,640	0,000	,666
	üst	102	4,3627	,89873			
S26	Alt	102	2,5196	1,03149	-16,969	0,000	,688
	üst	102	4,4510	,60734			
S27	Alt	102	1,9902	,88435	-16,296	0,000	,720
	üst	102	4,3333	,80016			
S28	Alt	102	2,5686	,91748	-19,842	0,000	,677
	üst	102	4,3333	,74904			
S29	Alt	102	2,7843	1,21564	-15,048	0,000	,473
	üst	102	4,1471	,69506			
	üst	102	4,7059	,45790			

Madde	Grup	N	Ortalama	Standart Sapma	t-değeri	p	Madde Toplam Korelasyonu
S30	Alt	102	2,8431	1,08769	-9,829	0,000	,574
	üst	102	4,3431	,66742			
S31	Alt	102	2,6569	1,08541	-11,871	0,000	,525
	üst	102	4,2157	,75291			
S32	Alt	102	2,9118	1,08183	-12,384	0,000	,623
	üst	102	4,5196	,74102			
S33	Alt	102	2,6569	1,05769	-15,213	0,000	,657
	üst	102	4,5196	,64070			
S34	Alt	102	2,7353	1,09839	-11,891	0,000	,584
	üst	102	4,2941	,73912			
S35	Alt	102	2,6765	1,03562	-15,851	0,000	,692
	üst	102	4,5098	,54035			
S36	Alt	102	2,7745	1,06154	-12,443	0,000	,597
	üst	102	4,3922	,77276			
S37	Alt	102	3,0392	1,04286	-14,779	0,000	,614

Maddeler arasındaki ilişkileri az sayıda ve en etkin şekilde ortaya koyabilecek faktör sayısını belirlemek için iki kriterden yararlanılmıştır. Bunlar, faktör özdeğerlerine dayalı olarak faktör özdeğer büyüklüğü ve birikimli çizgi grafiği kriterleridir. Bryman ve Cramer (1999), özdeğeri 1 veya 1'den büyük olan faktörlerin önemli faktör olarak nitelendirilmesi

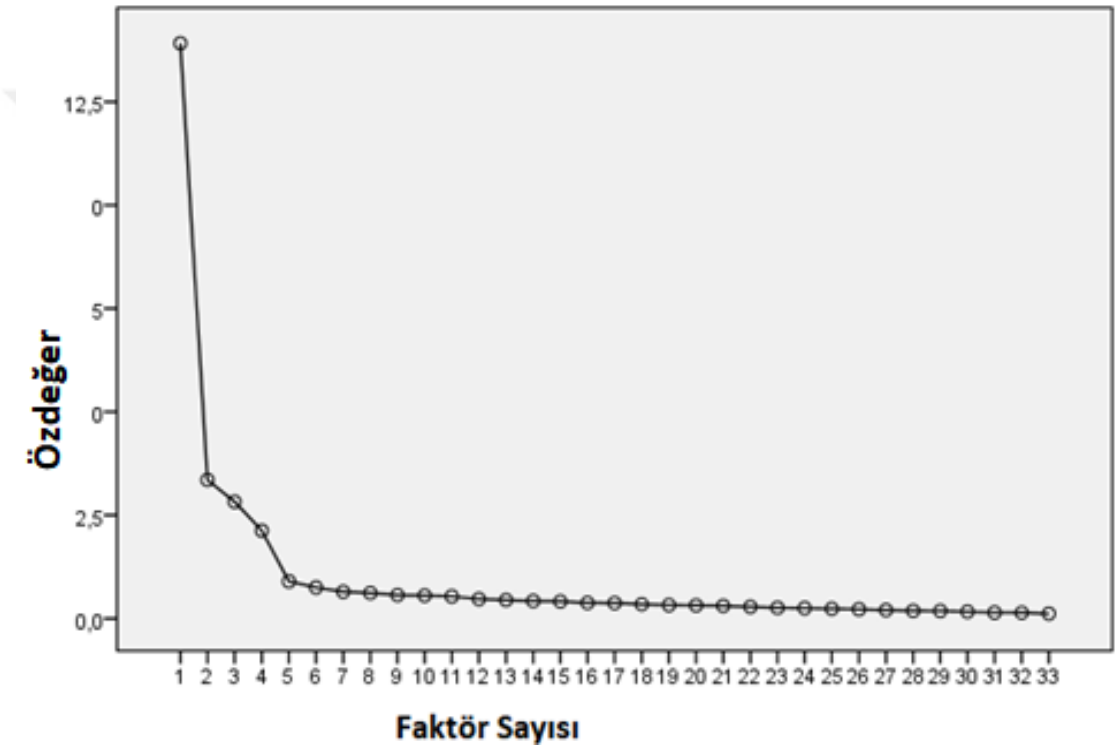
gerektiğini belirtmiştir. Bununla birlikte Büyüköztürk (2007) çizgi grafiğin maddelerin özdeğerlerinin birleştirilmesi sonucunda elde edildiğini, bu nedenle grafikte görülebilecek hızlı düşüşlerin (kırılma noktalarının) faktör sayısını vereceğini belirtmektedir.

Tablo 8. Faktör Toplam Varyansı

Bileşen	Başlangıç Özdeğerleri			Kareler Toplam Rotasyonu		
	Toplam	Açıklanan Varyans Yüzdesi	Birikimli Varyans Yüzdesi %	Toplam	Açıklanan Varyans Yüzdesi	Birikimli Varyans Yüzdesi %
1	13,917	42,172	42,172	8,458	25,630	25,630
2	3,353	10,159	52,332	5,789	17,542	43,172
3	2,825	8,562	60,894	4,565	13,834	57,006
4	2,127	6,444	67,337	3,409	10,331	67,337
5	,900	2,726	70,063			
32	,140	,423	99,640			
33	,119	,360	100,000			

Açımlayıcı faktör analizinde temel bileşenler yöntemi ve dik döndürme sonunda faktör özdeğerleri ve faktörlerin toplam varyansı açıklama oranları Tablo 8 ile verilmiştir. Tablo 12 incelendiğinde özdeğeri birden büyük dört faktörlü yapının olduğu tespit edilmiştir. Bu yapı toplam varyansın %67,33'nü açıklamaktadır. Sosyal bilimlerde yürütülen çalışmalarda toplam varyans oranının % 40 ile % 60 arasında değer alması ölçeğin faktör yapısının güçlülüğüne işaret etmektedir (Tavşancıl, 2002). Bu durum ölçeğin toplam varyans oranının yeterli bir değere sahip olduğunu göstermektedir. Bu çalışmada elde edilen %67,33'lük toplam varyans oranının %42'si Faktör 1, %10'16'sı Faktör 2, %8,56'sı

Faktör 3 ve %6,44'ü Faktör 4 tarafından açıklanmaktadır. Faktör sayısını belirleme için ayrıca çizgi grafiği incelemesi de yapılmıştır. Araştırmada geliştirilen ölçeğe ait çizgi grafiği şekil 10 ile verilmiştir. Şekil 10 incelendiğinde çizgi grafiğinde yüksek ivmeli hızlı düşüşlerin yaşandığı bileşenlerin 1, 2, 3 ve 4 numaralı faktörler olduğu, 5 numaralı faktörden itibaren grafiğin yatay bir görünüm aldığı anlaşılmaktadır. Buna göre ölçeğin içerdiği anlamlı faktör sayısının dört olduğu görülmektedir.



Şekil 9. Çizgi Grafiği

Faktör analizinde maddelerin en yüksek faktör yükü 0,45'den küçük ve birden fazla faktörde yer alıp birbirinden ayırt edilemeyecek kadar yakın (en yüksek iki faktördeki madde yükü arasındaki fark 0,10'dan küçük) olan maddeler varsa ölçekten çıkarılması önerilmiştir (Büyüköztürk, 2002: 474-479). Bununla birlikte bu aşamada aynı zamanda maddelerin ortak faktör varyans değerleri de incelenmelidir. Ortak varyans, ölçek içerisindeki bir maddenin diğer maddelerle paylaştığı varyans miktarıdır (Hair ve ark, 1998: 365). Ölçekte yer alan her

bir madde için hesaplanan bu değerin 0,50'inin altında olması durumunda o maddenin ölçekten çıkarılması önerilmektedir (Kalaycı, 2010: 342; Çokluk ve diğ., 2010: 194). Geliştirilen ölçekteki maddelerin faktör yükleri ve ortak faktör varyans değerleri Tablo 9 ile verilmiştir.

Tablo 9. Faktör Yükleri ve Ortak Faktör Varyansı

	Rotasyonlu Bileşen Matrisi					
	Madde	**Faktör Yükleri**				**Ortak Faktör Varyansı**
		1	**2**	**3**	**4**	
FAKTÖR 1	S3	,764	,075	,130	,109	,507
	S20	,763	,173	,206	,140	,618
	S6	,763	,328	,197	,095	,643
	S7	,761	,152	,169	,148	,589
	S5	,758	,066	,016	,100	,737
	S24	,756	,087	,081	,113	,653
	S23	,735	,266	,227	,001	,627
	S4	,734	,217	,207	,117	,700
	S25	,699	,238	,110	,114	,733
	SS1	,696	,100	,110	,028	,679
	S19	,675	,064	,229	-,051	,821
	S21	,664	,221	,314	,061	,793
	S27	,658	,199	,264	,211	,767
	S26	,635	,261	,308	,022	,851
	S22	,577	,371	,267	,074	,515
FAKTOR 2	S10	,084	,861	,080	,015	,674
	S29	,209	,794	,215	,111	,592
	S8	,120	,761	,161	,084	,547

	S9	,277	,759	,159	,149	,663
	S31	,215	,748	,139	-,042	,599
	S11	,227	,742	,179	,211	,571
	S30	,206	,739	,220	,035	,567
	S28	,259	,736	,303	,156	,586

	Madde	**Faktör Yükleri**				**Ortak Faktör Varyansı**
		1	**2**	**3**	**4**	
FAKTÖR 3	S34	,225	,143	,808	,143	,725
	S32	,251	,221	,807	,088	,755
	S33	,330	,164	,785	,137	,639
	S36	,186	,246	,781	,149	,626
	S37	,241	,282	,722	,136	,772
	S35	,342	,340	,721	,025	,770
FAKTÖR 4	S12	,127	,140	,128	,894	,744
	S13	,150	,048	,119	,868	,753
	S16	,205	,137	,091	,867	,727
	S15	,052	,101	,145	,856	,677

Tablo 8 incelendiğinde, Temel Bilşenler Yöntemi ve Dik döndürme (orthogonal) sonrası ölçek maddelerinin 4 faktörde, 0,577 ile 0,894 faktör yükleri aralığında toplandığı görülmektedir. Ölçekte yer alan 33 maddenin en yüksek faktör yük değerleri 0,45'in altında olan madde tespit edilememiştir. Bu maddelerin faktör yükleri bakımından en yüksek iki

faktördeki faktör yükleri arasındaki fark 0,1'den büyüktür. Ayrıca maddelerin ortak varyans değeri 0,507 ile 0,851 arasında olduğu hesaplanmıştır. Bu aşamada ölçekten herhangi bir maddenin çıkarılması gerekmemektedir. Analiz sonucunda Faktör 1'in 15 maddeden, Faktör 2'nin 8 maddeden, Faktör 3'ün 6 maddeden, ve Faktör 4'ün 4 maddeden, oluştuğu tespit edilmiştir.

Faktörlerin içindeki maddelere bakıldığında en fazla maddeye sahip olan faktör, faktör adları olarak kullanılmıştır. Faktör I'de en fazla faktör yük değerine sahip olan madde 3'ün içeriği "Firmamızda, önemli bilgilerin gizliliğinin korunabilmesi için Güvenli belge deposu'na benzer önlemler bulunur" olduğundan dolayı Faktör 1 "Gizlilik"; Faktör II'de en fazla faktör yük değerine sahip olan madde 10 olup içeriği "Ciddi bir siber saldırı ile bilgilerimizin zarar görmesi durumunda firmamızın önemli derecede etkileneceğini düşünmekteyim." olduğundan dolayı bu faktör "Bütünlük-Tamlık"; Faktör III'de ise en büyük faktör yük değerine sahip olan madde 34'ün içeriği "Firmamız, müşterilerimizin bilgilerini başka kurumlarla paylaşmadan önce ilgili kişiye bilgi verir" olduğundan dolayı "Mahremiyet"; Faktör IV'de de en büyük faktör yük değerine sahip olan madde 12'nin içeriği "Kullandığımız bilişim sistemlerinin herhangi bir unsurunun (yazılım veya donanım vb.) kendisinden beklenildiği şekilde çalışmaması işlerimizi önemli ölçüde yavaşlatır" ifadesinden oluştuğundan dolayı "Kullanılabilirlik ve Süreklilik" olarak isimlendirilmiştir. Faktörlerin isimlendirilmesi ve içerdikleri madde sayısı Tablo 10'da verilmiştir.

Tablo 10. Faktörler ve İçerdikleri Madde Sayıları

Faktörler	İsimleri	İçerdikleri Madde sayıları
Faktör 1	Gizlilik	15
Faktör 2	Bütünlük	8
Faktör 3	Mahremiyet	6
Faktör 4	Erişebilirlik	4

Araştırmaya esas aldığımız ve Cherdantseva, Rana, Ivins, & Hilton (2013) tarafından geliştirilen "RMIAS" modeli, araştırmanın modeli olarak kullanılmıştır. Bu araştırma modeli sekiz bölümden oluşmaktadır. Ancak araştırmada kullanılan ölçeğe Faktör analizinin uygulanması sonucunda ölçekteki maddelerin dört factor altında toplandığı tespit edilmiştir: Gizlilik, Bütünlük-Tamlık, Erişebilirlik ve Mahremiyet. Orijnallik-Güvenirlilik ile ilgili maddelerin "Gizlilik" adını verdiğimiz faktör yüklenmiştir. Bunun nedeni literatürde Orijnallik güvenirlilik Başka bir deyişle, kimlik doğrulama bilgisayar sistemine giriş yapan kişinin iddia edilen kişi olup olmadığını doğrulamaktadır (Karsten, 2011). Bu noktada tanımların birbirine yakın olmasından dolayı katılımcılar Orjinallik ve güverliliği Gizlilik ile aynı faktör olarak algılamış olabilecekleri ifade edilebilir.

Gizlilik faktörünün altında toplanan bir başka faktör ise İzlenebilirilik'tir. Alan Westin (1967) tarafından gizliliğin tanımı; bireylerin kendileriyle ilgili kişisel bilgilerin başkalarına iletilmesiyle ilgili sahip oldukları haklar olarak tanımlanmaktadır ve bu tanım izlenebilirliğin temelini oluşturmaktadır. Westin (1967) gizliliği bütün bilgileri kapsayacak şekilde açıklamıştır ve bundan dolayı da katılımcıların İzlenebilrililik ile ilgili maddeleri gizlilik maddeleri olarak algıladıkları ifade edilebilir.

Gizlilik fatktörünün altında toplanan bir başka faktör ise denetlenebilirililik'tir. Denetlenebilirlilik literatürde "veritabanındaki öğelere erişen (veya değiştiren) kişileri takip edebilme eylemi" (Fariborz Farahmand, Sharp, & Enslow, 2005) ve gizlilikte yetkisi olmayan kişilerin girişlerinin engelenmesi olarak tanımlanmıştır. Bu nedenle katılımcıların izinsiz girişlerin engelenmesini, denetlenebirlilik olarak algılamış olabilecekleri söylenebilir.

İkinci faktörün Bütünlük-Tamlık başlığı altında toplandığı görülmektedir. İnkar edememeyle ilgili maddeler bu başlık altında toplanmıştır. Literatürde Tamlık-Bütünlük veri bütünlüğü, istenmeden bilginin değiştirilmemesi ya da zarar görmemesi olarak tanımlanmaktadır (Knorr, Rohrig, 2015). İnkar edememe ise bir davada tarafları diğer tarafa karşı korumak ve belirli bir eylemin veriler üzerinden değişiklik yapılmadan eylemin gerçekleşip gerçekleşmediğini kanıtlamak için önemli veriler olarak tanımlanmaktadır (Zhou ve Gollmann, 1997). Bu yüzden katılımcılar inkar edememe ile ilgili verileri Tamlık-Bütünlük olarak algılamış olabilecekleri ifade edilebilir.

3.4.3.2. Doğrulayıcı Faktör Analizi (DFA)

DFA Önceden oluşturulan bir model aracılığıyla gözlenen değişkenlerden yola çıkarak gizli değişken (faktör) oluşturmaya yönelik bir işlemdir. Genellikle ölçek geliştirme ve geçerlilik analizlerinde kullanılmakta veya önceden belirlenmiş bir yapının doğrulanmasını amaçlamaktadır. Çok sayıda gözlenen veya ölçülen değişken tarafından temsil edilen ve gizli yapıları içeren çok değişkenli istatistiksel analizleri tanımlamak amacıyla kullanılmaktadır. Doğrulayıcı faktör analizi, açıklayıcı faktör analizi ile belirlenen faktörlerin, hipotez ile belirlenen faktör yapılarına uygunluğunu test etmek üzere yararlanılan faktör analizidir. Açıklayıcı faktör analizi, hangi değişken gruplarının hangi faktör ile yüksek düzeyde ilişkili olduğunu test etmek için kullanılırken, belirlenen sayıda faktöre katkıda bulunan değişken

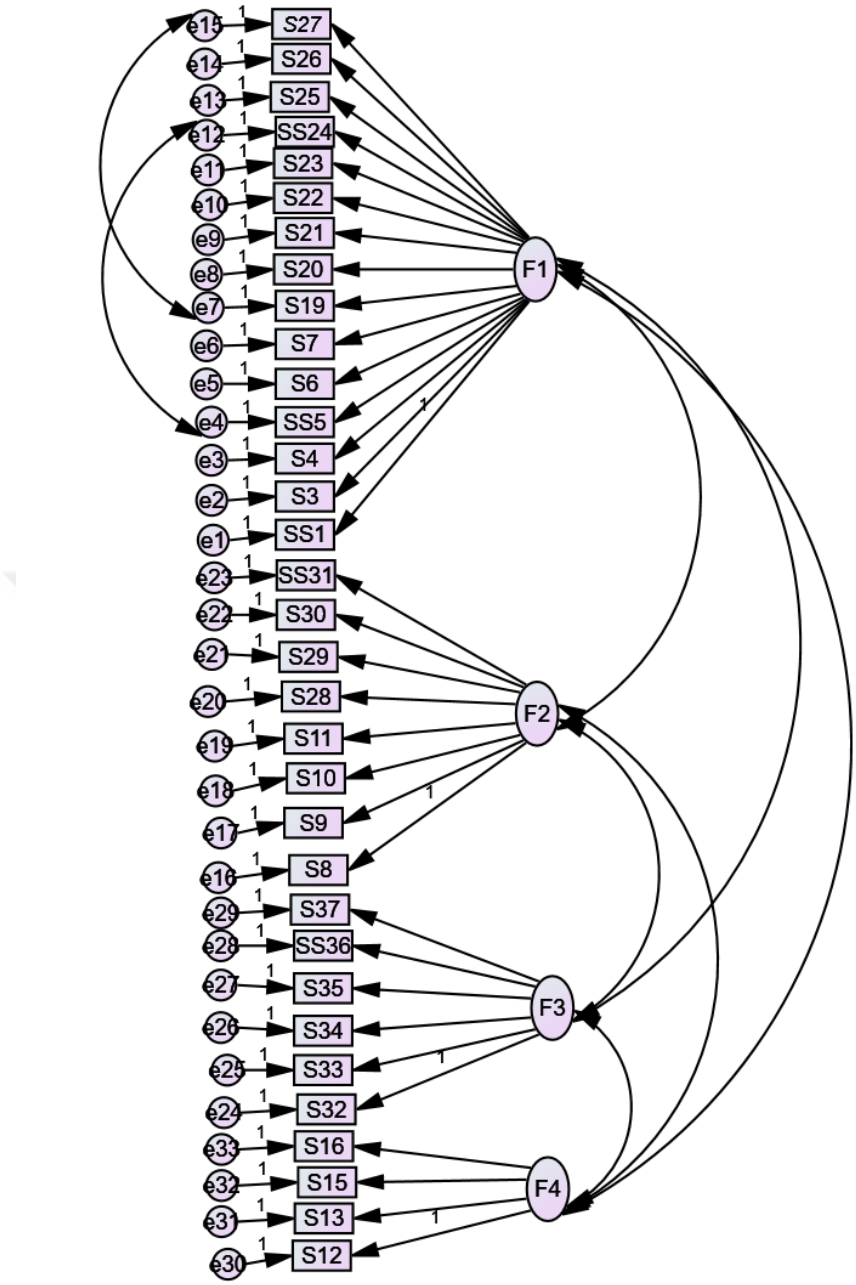
gruplarının bu faktörler ile yeterince temsil edilip edilmediğinin belirlenmesi için doğrulayıcı faktör analizinden faydalanılmaktadır (Aytaç ve Öngen, 2010: 16). Özetle, yapısal eşitlik modellerinde teoride var olan kavramsal model, veri yardımı ile test edilmeye çalışılmaktadır. Doğrulayıcı faktör analizi, genellikle ölçek geliştirme ve geçerlik analizinde kullanılmakta ve önceden belirlenmiş bir yapının doğruluğunu belirlemeyi amaçlamaktadır. Bu amaçla açımlayıcı faktör analizi sonunda elde edilen 4 faktörlü yapının geçerliliğini sınamak için ikinci örneklem grubuna (N_2=378) DFA uygulanmıştır. Literatürde açımlayıcı ve doğrulayıcı faktör analizinin farklı örneklem gruplarına uygulanması önerilmektedir. (Kabakçı vd., 2012; Wang vd., 2014; Çakıroğlu, Gökoğlu ve Çebi, 2015).

Açımlayıcı faktör analizi ile önceden belirlenen modellerin veriyi ne kadar iyi açıkladığı doğrulayıcı faktör analizinde uyum istatistikleri ile belirlenir. Modellerin uyumunu test eden birden fazla uyum istatistiği (fit statistic) vardır. Bu uyum istatistikleri, ileri sürülen modellerin parametreleri ile örnek verilerden elde edilen istatistiklerin uygunluğunu test etmektedir. Eğer model verilere uymuyorsa reddedilmektedir. İleri sürülen model reddedilemiyorsa, model gözlenen verilerin altında yatan nedensel yapıyı açıklama yeteneğine sahiptir (Özdamar, 2010: 251-252). Ki kare testi ile modelin genel uyumuna bakılır. Model uyumunun belirlenmesinde, başlangıç uyum indeksi olarak ki-kare uyum iyiliği indeksine (chi-square goodness of fit) bakılmaktadır. Ki-kare testi, veriyle model arasındaki uyumun testidir. Ki karenin anlamlı olmaması ve CMIN/DF = χ 2 /sd $\leq$ 5 olması modelin uyumluluğunu göstermektedir. Ki kare uyum iyiliği indeksi ile birlikte, Artırmalı Uyum İndeksi (Incremental Fit lndex, IFI), Karşılaştırmalı Uyum İndeksi (Comparative Fit Index, CFI), Yaklaşık Hataların Ortalama Karekökü (Root Mean Square Error of Approximation, RMSEA), İyilik Uyum İndeksi (Goodness Of Fit Index, GFI), Ortalama Hataların (Kalıntıların) Karekökü (Root Mean Square Residual, RMR) de sık kullanılmaktadır.

Aşağıdaki tabloda, uyum değerleri ve uyum aralıkları özetlenmiştir (Schermelleh Engel ve diğ., 2003).

Tablo 11. Uyum Değerleri ve Uyum Aralıkları

Model Uyum Kriteri	**İyi Uyum**	**Kabul Edilebilir Uyum**
x^2 Uyum Testi	0,05<p=<1	0,01<p=<0,05
CMIN/SD	x^2/sd≤3	x^2/sd≤5
IFI	0,95≤IFI	0,90≤IFI
CFI	0,97≤CFI	0,95≤CFI
RMSEA	RMSEA≤0,05	RMSEA≤0,08
GFI	0,90≤GFI	0,85≤GFI
RMR	0<RMR≤0,05	0<RMR≤0,08



Şekil 10. DFA Modeli

Doğrulayıcı faktör analizi modeli Şekil 10 ile verilmiştir. Bu modele ait uyum indeks değerleri Tablo 12 ile verilmiştir. Tablo 12 incelendiğinde bu modele ait $\boldsymbol{\chi^2/df}$ değerinin 1,937 olduğu görülmektedir $\boldsymbol{\chi^2} = 943{,}216\ ve\ df = 487$) bu değer 3'den küçük olduğu için modelin uyumu iyi olarak yorumlanabilir. Benzer şekilde IFI ve RMSEA değerleri sırasıyla 0,951 (≥0,95) ve 0,050 (≥0,050) olarak hesaplanmıştır. Hesaplanan her iki uyum indeks

değeri için modelin uyumu iyi olarak kabul edilmektedir. Diğer uyum değerleri olan GFI, CFI ve RMR değerleride sırasıyla 0,863(≥0,85), 0,950 (≥0,95) ve 0,055 (0<RMR<0,08) olarak tespit edilmiştir. Bu üç uyum değerine gore, elde edilen modelin kabul edilebilir uyum değerlerine sahip olduğunu ortaya koymaktadır.

Tablo 12. DFA Modeline Ait Uyum İyiliği Değeri

Uyum Kriterleri	χ^2/df	**GFI**	**IFI**	**CFI**	**RMSEA**	**RMR**
Değerleri	1,937	0,863	0,951	0,950	0,050	0,055
Uyum İyiliği Durumu	İyi	Kabul edilebilir	iyi	Kabul Edilebilir	İyi	Kabul Edilebilir

Tablo 13. Faktörler Arası Korelasyon Değerleri

	F1	F2	F3	F4
F1	1			
F2	0,588*	1		
F3	0,562*	0,618*	1	
F4	0,235*	0,301*	0,292*	1

Tüm faktörler arası elde edilen modele göre hesaplanan korelasyon değerleri Tablo 13 ile verilmiştir. Bu değerler incelendiğinde faktörler arası hesaplanan korelasyon değerlerinin ($p<0,05$) istatistiksel olarak anlamlı olduğu ve faktörler arası korelasyonların 0,235 ile 0,618 arasında değiştiği görülmektedir. En yüksek korelasyon değeri F2 ve F3 faktörleri arasında olup r=0,618'dir. En düşük korelasyon ise F1 ile F4 arasında olup r=0,235'dir.

3.5. Kobilerin Bilgi Güvenliği Ölçeği'nin Güvenirlilik Çalışması

KBGFÖ'nin güvenirliği iç tutarlılık Cronbach Alpha yöntemi ile hesaplanmıştır. Likert tipi ölçek geliştirme sürecinin temel varsayımlarından biri, ölçülmek istenen tutumla ölçekte yer alan her bir maddenin monotonik bir ilişkiye sahip olmasıdır. Başka bir ifadeyle herbir maddenin, ölçeğin ölçmek istediği tutumla aynı yönde olması gerekmektedir (Tavşancıl, 2002: 152). Bunun için iç tutarlılık analizi kapsamında Likert tipi ölçeklerde güvenirlik düzeyini belirlemek için Cronbach tarafından geliştirilen Alpha katsayısı kullanılması uygundur. Cronbach Alpha katsayısı (1,00-0,80: Yüksek; 0,79-0,60: İyi; 0,59-0,40: Düşük; 0,39-0,00: Güvenilir değil) ne derece yüksek ise ölçekte yer alan maddeler birbirleriyle o derece tutarlıdır ve ölçekte yer alan her bir madde ölçeğin geneliyle aynı amaca hizmet etmektedir şeklinde yorumlanmaktadır (Tezbaşaran, 1996).

Kobilerin bilgi güvenirliği farkındalığını ölçmek amacıyla bu çalışmada hazırlanan ölçeğin genel güvenirliği ile bu ölçek içerisinde yer alan dört faktöre ait Croncbach Alpha güvenirlilik değerleri Tablo ile verilmiştir. KBGFÖ ölçeğinin genel güvenirliği 0,954, Birinci faktörün 0,947, ikinci faktörün 0,927, üçüncü faktörün 0,923 ve dördüncü faktörün 0,924 olduğu tespit edilmiştir. Bu değerler dikkate alındığında ölçeğin oldukça güvenilir olduğu sonucuna varılmıştır. Ölçek içerisinde yer alan tüm maddelerin madde toplam korelasyon değerleri 0,50'nin üzerindedir. Madde-toplam korelasyonunun yorumlanmasında .30 ve daha yüksek olan maddelerin, bireyleri ölçülen özellik bakımından iyi derecede ayırt ettiği (Büyüköztürk, 2004) göz önüne alındığında, madde-toplam korelasyonlarının yeterli düzeyde olduğu görülmektedir.

Tablo 14. BGFA Ölçeğinde Yer Alan Maddelerinin ve Alt Boyutlarının Güvenirlilik Değerleri

Faktör	Madde No	Madde Toplam Korelasyonu		Cronbach's Alpha Güvenirlilik Katsayısı (α)			
		Faktör	Ölçeğin (Genel)	Faktörden Madde Silinirse	Ölçekten Madde Silinirse	Faktörlerin	Ölçeğin
F1	S3	,728	,624	,943	,953	,947	,954
	S20	,778	,719	,942	,952		
	S6	,787	,783	,942	,953		
	S7	,742	,689	,943	,953		
	S5	,668	,560	,944	,953		
	S24	,699	,604	,944	,953		
	S23	,752	,718	,942	,953		
	S4	,760	,712	,942	,953		
	S25	,715	,655	,943	,953		
	SS1	,666	,557	,944	,953		
	S19	,657	,558	,945	,953		
	S21	,719	,699	,943	,953		
	S27	,708	,703	,943	,953		
	S26	,694	,687	,944	,953		
	S22	,682	,699	,944	,953		

F2	S29	,774	,501	,916	,953	0,927	
	S10	,793	,643	,915	,953		
	S8	,718	,528	,921	,953		
	S9	,750	,659	,918	,953		
	S31	,701	,547	,922	,953		
	S11	,759	,639	,917	,953		
	S30	,733	,594	,919	,953		
	S28	,792	,702	,915	,953		

Faktör	**Madde No**	**Madde Toplam Korelasyonu**		**Cronbach's Alpha Güvenirlilik Katsayısı (α)**			
		Faktör	**Ölçeğin (Genel)**	**Faktörden Madde Silinirse**	**Ölçekten Madde Silinirse**	**Faktörlerin**	**Ölçeğin**
F3	S34	,729	,593	,916	,953	,923	,954
	S32	,761	,637	,912	,953		
	S33	,797	,666	,907	,953		
	S36	,767	,609	,911	,953		
	S37	,807	,636	,905	,953		
	S35	,813	,706	,905	,953		

F4	S16	,835	,525	,898	,954	,924	
	S13	,829	,684	,900	,954		
	S12	,825	,556	,902	,953		
	S15	,809	,749	,907	,953		

DÖRDÜNCÜ BÖLÜM

BULGULAR VE YORUMLAR

Araştırmanın bu bölümünde, araştırmada ele alınan problem ve alt problemlerin çözümü için toplanan verilerin istatistiksel analizlerinin sonuçları, sonuçlara ilişkin elde edilen bulgular ve bu bulgulara ait yorumlar verilmektedir. Araştırmada öncelikle kişisel bilgiler bölümünden elde edilen betimleyici istatistik sonuçlar, daha sonra da alt problemler doğrultusunda elde edilen istatistiksel veriler sistematik bir şekilde değerlendirilmiştir.

Tablo 15. Araştırmaya Katılanların Cinsiyetlere Göre Dağılımı

	Frekans	**Yüzde**	**Geçerli Yüzde**	**Toplam Yüzde**
Erkek	431	57,0	57,0	100,0
Kadın	325	43,0	43,0	100,0
Toplam	756	100,0	100,0	

Tablo 15'de görüldüğü gibi araştırmaya katılanların cinsiyetleri incelendiğinde %57'sinin erkek % 43'nün ise kadın olduğu tespit edilmiştir.

Tablo 16. Araştırmaya Katılanların Gelir Durumuna Göre Dağılımı

	Frekans	**Yüzde**	**Geçerli Yüzde**	**Toplam Yüzde**
2000 altı	311	41,1	41,1	41,1
2001-4000	246	32,5	32,5	73,7
4001-5000	108	14,3	14,3	88,0
5001-7000	61	8,1	8,1	96,0
7001 ve üzeri	30	4,0	4,0	100,0

Araştırmaya katılanların gelir düzeyleri incelendiğinde, %41,1'i 2000 TL ve altı bir gelire sahip olduğunu; %32,5'i 2001-4000 TL arasında; %14,3'ü 4001-5000 TL arasında; %8,1'i 5001-7000 TL arasında; %4'ü ise 7001 TL ve üzeri bir gelire sahip oldukları belirlenmiştir.

Tablo 17. Araştırmaya Katılanların Yaş Durumuna Göre Dağılımı

	Frekans	**Yüzde**	**Geçerli Yüzde**	**Toplam Yüzde**
20-25	262	34,7	34,7	34,7
26-30	201	26,6	26,6	61,2
31-35	145	19,2	19,2	80,4
36-40	72	9,5	9,5	89,9
41-45	54	7,1	7,1	97,1
46-51	18	2,4	2,4	99,5
52-56	2	,3	,3	99,7
57-65	2	,3	,3	100,0
Toplam	756	100,0	100,0	

Katılımcıların yaş aralığı incelendiğinde, 262'sı 20-25 yaş aralığında; 201'i 26-30 yaş aralığında; 145'i 31-35 yaş aralığında; 72'si 36-40 yaş aralığında; 54'ü 41-45 yaş aralığında; 18', 46-51 yaş aralığında; 4'ü ise 52 ve üzeri olduğu görülmektedir.

Tablo 18. Araştırmaya Katılanların Eğitim Durumuna Göre Dağılımı

	Frekans	**Yüzde**	**Geçerli Yüzde**	**Toplam Yüzde**
İlkögretim	33	4,4	4,4	4,4
Lise	129	17,1	17,1	21,4
Önlisans	185	24,5	24,5	45,9
Lisans	346	45,8	45,8	91,7
Lisansüstü	63	8,3	8,3	100,0
Toplam	756	100,0	100,0	

Tablo 18'de yer alan veriler incelendiğinde, ilköğretim düzeyinde mezun olanların 33 kişi; Lise mezunları 129 kişi; Önlisans mezunları 185 kişi; Lisans mezunları 346 kişi; lisansüstü mezunlarının 63 kişi olduğu belirlenmiştir

Tablo 19. Araştırmaya Katılanların Pozisyonlarına Göre Dağılımı

	Frekans	**Yüzde**	**Geçerli Yüzde**	**Toplam Yüzde**
Üst Düzey Yönetici	83	11,0	11,0	11,0
Orta Düzey Yönetici	134	17,7	17,7	28,7
Alt Düzey Yönetici	167	22,1	22,1	50,8
Teknik Çalışan	128	16,9	16,9	67,7
İdari Çalışan	244	32,3	32,3	100,0

	Frekans	Yüzde	Geçerli Yüzde	Toplam Yüzde
Üst Düzey Yönetici	83	11,0	11,0	11,0
Orta Düzey Yönetici	134	17,7	17,7	28,7
Alt Düzey Yönetici	167	22,1	22,1	50,8
Teknik Çalışan	128	16,9	16,9	67,7
İdari Çalışan	244	32,3	32,3	100,0
Toplam	756	100,0	100,0	

Katılımcıların çalıştığı kurumdaki pozisyonları incelendiğinde, üst düzey yönetici olarak 83 kişi ile %11, orta düzey yönetici grubunda 134 kişi ile %17,7, alt düzey yönetici grubunda 167 kişi ile %22.1, teknik çalışan pozisyonunda 128 kişi ile %16,9, idari çalışan kısmında 244 kişi ile %32,3 olduğu görülmektedir (Tablo 19).

Tablo 20. Araştırmaya Katılan Firmaların Çalışan Sayısına Göre Dağılımı

	Frekans	Yüzde	Geçerli Yüzde	Toplam Yüzde
1-10	142	18,8	18,8	18,8
11-49	207	27,4	27,4	46,2
50 ve üzeri	407	53,8	53,8	100,0
Toplam	756	100,0	100,0	

Kurumların çalışan kişi sayısı incelendiğinde, 1-10 çalışan sayısı olan 142 firma olduğu, 11-49 çalışan sayısı olan 207 firma, 50 ve üzerinde çalışanı olan 407 firma olduğu görülmektedir (Tablo 20).

Tablo 21. Araştırmaya Katılan Firmaların Faaliyet Yılına Göre Dağılımı

	Frekans	**Yüzde**	**Geçerli Yüzde**	**Toplam Yüzde**
0-5 yıl	125	16,5	16,5	16,5
6-10 yıl	196	25,9	25,9	42,5
11-15 yıl	136	18,0	18,0	60,4
16-20 yıl	120	15,9	15,9	76,3
21 ve üzeri yıl	179	23,7	23,7	100,0
Toplam	756	100,0	100,0	

Kurumların faaliyet yılları incelendiğide ise, kuruluşu 0-5 yıl içerisinde olan 125 firma (%16,5) olduğu, 6-10 yıl arasında 196 firma (%25,9) olduğu, 11-15 yıl arasında 136 firma (%18) olduğu, 120 firmanın (%15,9) 16-20 yıl içerisinde kurulduğu ve 21 yıl ve üzerinde ise 179 firmanın (%23,7) olduğu görülmektedir (Tablo 21).

BEŞİNCİ BÖLÜM

SONUÇ VE ÖNERİLER

5.1. Sonuç

Globallaleşen dünya ile birlikte, iletişim teknolojisinde yaşanan gelişmeler, firmalar için sınırları ortadan kaldırmıştır. Yaşanan bu dönüşüm, Sadece firmalar için değil, insanlığın her alanında değişime neden olmuştur.

İnternet ve bilişim teknolojileri, otomasyon, yapay zeka, internet ve yeni iş modelleri insan hayatının her alanı etkilemektedir. Teknolojiyle birlikte insanlar, oturdukları yerden istedikleri alışverişi yapmakta ve istediği bilgiye ulaşabilmektedir. İş dünyası hem üretim metotlarında ve ürün geliştirmede, hem de hizmet sunum süreçlerinde yeni dinamikler geliştirmektedir. Sağladığı avantaj ve getirdiği tehditlerle yaşadığımız yüzyıl, şirketler açısından büyük kolaylıklarla birlikte büyük sorunları da beraberinde getirmektedir.

Teknolojide yaşanan değişim, şüphesiz insanlık hayatına kolaylıklar getirmektedir. Bununla birlikte bu yenilikler, yeni tehditleri de berbarinde getirmekte ve sonuçta "Bilgi Güvenliği" kavramı dünyada yeni bir gündem olarak ortaya çıkmaktadır. Dünya, dijitalleşmeyle birlikte, pazarlama, satış, üretim, vergi gibi kavramları yeniden tanımlarken risk ve tehditleri de yeniden tanımlar hale gelmiştir. Daha önceden, hangi nedenlerle ve kaynağı tahmin edilebilecek risk ve tehditler konuşulurken, günümüzde tehditlerin nereden geleceği tahmin edilememektedir. Günümüzde sadece şirketler değil, kamu kurumları ve ülke güvenliği de tehdit altındadır.

Daha önceki bölümlerde bahsi geçen ve 2001 yılında ortaya çıkan Codered solucanı, 2003 yılında ortaya çıkan Blaster solucanı, 2013 Target firmasına yapılan saldırı ve

Türkiye'de 2015 yılında yapılan siber saldırı sonucunda oluşan elektirik kesintisi, üreticileri ve kamu kurumlarını çalışamaz hale getirmiştir.

Teknolojide yaşanan gelişim ile birlikte siber saldırı teknikleri aynı gelişim hızıyla kendini ilerletmektedir. Bununla birlikte, operasyon süreçlerinin zarar görmesi, maddi kayıplar, rekabet gücünde yaşanacak sorunlar ciddi itibar ve güven kaybına ve sonuçta firmalar için telafisi zor kayıplara neden olabilmektedir. Firmalar dijital gelişimin sağladığı fırsatlardan hız kesmeden yararlanması ama aynı zamanda gelebilecek olan tehditlere hazırlıklı olması gerekmektedir.

Dünya hızla dönüştüğü zaman herşey daha hızlı bir şekilde değişmektedir. Teknolojideki gelişime uyum göstermek, fırsatlardan yararlanabilmek, gelebilecek siber saldırılara karşı bilgi ve öngörüye ve gerekli adımları atabilecek esnekliğe sahip olmak firmalar için önemlidir.

Bütün bunlar sonucunda, bu çalışmanın amacı, Kobi'lerin bilgi güvenliği farkındalıklarını ölçebilmek için güvenilir ve geçerli bir ölçek geliştirmektir. Ölçeğin boyutlarının belirlenmesini belki ölçek geliştirmedeki en zor kısımdır. Bu amaçla literature araştırmasının yanında, faktör analizi yapılmıştır.

Sonuçlar, 37 maddenin ''Kobilerin Bilgi Güvenliği Farkındalığı Ölçeğini' ölçtüğünü göstermektedir. Sonuçlar, ölçeğin 8 boyutlu olduğunu göstermiştir. Sonuçlara göre alt ölçekler;

i. Süreklilik
ii. İzlenebilirlik ya da Kayıt Tutma
iii. Kimlik Sınaması
iv. Bilginin Erişebilirliği
v. Bilgi Bütünlüğü
vi. Gizlilik

vii. İnkar Edememe

viii. Mahremiyet

Ölçüt geçerliliğini ispatlamak için Hemzaman/Eşzaman geçerliliği yöntemi kullanılmıştır. 2014 yılında Akademisyenler üzerinde Bilgi güvenliği farkındalığı ölçeği (ABGFÖ) ile Bilgi güvenliği farkındalığı ölçeği aynı anda uygulanmış ve elde edilen sonuçlar arasında korelasyona bakılmıştır. Koreleason değeri r = 0,407 olup istatistiksel olarak anlamlıdır (p=0,003<0,05). Elde edilen bu korelasyon değerine göre geliştirilen ölçek ile daha önceki ölçek arasında pozitif yönde ve orta düzeyde bir ilişki olduğu tespit edilmiştir.

Yapı geçerliliğini ispatlamak için Açımlayıcı Faktör analizi ve Doğrulayıcı faktör analizi yapılmıştır. Faktör analizlerinin farklı örneklem gruplarından elde edilen veriler üzerinden yapılması gerektiği ifade edildiğinden, geçerli sayılan 756 ölçek formu rastgele ikiye bölünerek AFA ve DFA uygulanmıştır. (n1=378; n2:378) ilk grup üzerinde AFA, diğer grup zerinde DFA yapılmıştır.

Açımlayıcı faktör analizi sonuçları, örneklem büyüklüğü yeterliliği için KMO test edilmiş ve çıkan sonucun 0,942 olduğu tespit edilmiş ve örneklem büyükllüğünün yeterli olduğunu göstermiştir. Madde analiz sürecinde ‘’0,40’’ altında çıkan 4 maddenin (S2, S14, S17 VE S18), ölçekten çıkarılması kararına varılmıştır. Sonuçlara göre temel bileşenler yöntemi ve dik döndürme sonunda faktör özdeğerleri ve faktörlerin toplam varyansı %67,33’nü açıkladığı göstermiştir. Çıkan bu sonuç ölçeğin faktör yapısının güçlülüğüne işaret etmektedir. Faktör sayısını belirleme için çizgi grafiği incelenmiş olup, ölçeğin içerdiği anlamlı faktör sayısının dört olduğunu göstermiştir. Faktörlerin içindeki maddelere bakıldığında en fazla maddeye sahip olan faktör, faktör adları olarak kullanılmıştır. Bunun sonucunda, Faktör 1 Gizlilik, Faktör 2 Bütünlük, Faktör 3 Mahremiyet, Faktör 4 Erişebilirlik olarak adlandırılmıştır. Ölçeğin dört farktörde çıkma nedeni, Literatürde daha önce belirtildiği üzere bilgi güvenliğinin temelini CIA Bütünlük, Gizlilik ve Erişebilirlik

oluşturuyodu. Çıkan faktörlere baktığımızda Mahremiyet harcicinde diğer faktörler CIA modelini oluşturmaktadır.

Doğrulayıcı faktör analizi için, Ki kare uyum iyiliği indeksi ile birlikte, Artırmalı Uyum İndeksi (Incremental Fit lndex, IFI), Karşılaştırmalı Uyum İndeksi (Comparative Fit Index, CFI), Yaklaşık Hataların Ortalama Karekökü (Root Mean Square Error of Approximation, RMSEA), İyilik Uyum İndeksi (Goodness Of Fit Index, GFI), Ortalama Hataların (Kalıntıların) Karekökü (Root Mean Square Residual, RMR) bakılmıştır. Modele ait $\boldsymbol{\chi^2/df}$ değerinin 1,937 olduğu görülmektedir $\boldsymbol{\chi^2} = 943{,}216\ ve\ df = 487$) bu değer 3'den küçük olduğu için modelin uyumu iyi olarak yorumlanabilir. Benzer şekilde IFI ve RMSEA değerleri sırasıyla 0,951 (≥0,95) ve 0,050 (≥0,050) olarak hesaplanmıştır. Hesaplanan her iki uyum indeks değeri için modelin uyumu iyi olarak kabul edilmektedir. Diğer uyum değerleri olan GFI, CFI ve RMR değerleride sırasıyla 0,863($\geq$ 0,85), 0,950 ($\geq$ 0,95) ve 0,055 (0<RMR<0,08) olarak tespit edilmiştir. Bu üç uyum değerine gore, elde edilen modelin kabul edilebilir uyum değerlerine sahip olduğunu ortaya koymaktadır.

KBGFÖ'nin güvenirliği için iç tutarlılık Cronboach Alpha yöntemi ile hesaplanmıştır. . KBGFÖ ölçeğinin genel güvenirliği 0,954, Birinci faktörün 0,947, ikinci faktörün 0,927, üçüncü faktörün 0,923 ve dördüncü faktörün 0,924 olduğu tespit edilmiştir. Bu değerler dikkate alındığında ölçeğin oldukça güvenilir olduğu sonucuna varılmıştır.

5.2. Öneriler

Günümüzde, Bilgi güvenliği firmalar için çok önemli olması nedeni ile, bu ölçek firmaların bilgi güvenliği farkındalıklarını ölçülmesi için çok önemli katkıları olabilir. Firmalar bilgi güvenliği farkıdalıklarıyla ilgili güçlü ve zayıf olduğu noktaları görebilir ve gereken önlemleri alabilirler.

Gaziantep sınırları içerisinde kobilerin bilgi güvenliği farkındalıklarını ölçmeye yönelik geliştirilen ölçek kullanılarak, gelecek araştırmalar için çeşitli öneriler belirtilebilir. Bu konuda yapılan araştırmaların kobilerin bilgi güvenliği alanında literatürdeki boşluğun doldurulmasına katkıda bulunacağı düşünülmektedir..

Yapılan araştırmalar sonucunda geliştirilen 'kobilerin bilgi güvenliği farkındalığı ölçeği' kullanılarak farklı coğrafyalarda farklılıklar/benzerlikler ortaya konularak kuramsal tartışmalara katkı sağlamak amacıyla yeni araştırmalar yapılmalıdır.

Kobilerin bilgi güvenliği farkındalıklarıyla ilgili zayıf olduğu noktaların tespit edilmesi sonucunda bu zayıf noktaların giderilebilmesi için yeni araştırmalar, farklı örneklem grupları üzerinde yapılmalı, böylece sorunların çözümü için öneriler sunulmalıdır.

Araştırma, Gaziantep sınırları içerisinde kobiler üzerinde gerçekleşmiştir. Daha sonraki araştırmaların daha büyük örneklemlerde gerçekleştirilerek, sonuçların karşılaştırılması ile alan yazına katkıda bulunulması önerilmektedir.

KAYNAKÇA

Acılar, A. (2009). İşletmelerde bilgi güvenliği ve örgüt kültürü. *Organizasyonel Yönetim Bilimleri Dergisi.* I(1) 25-33.

Act, S. O. (2002). *An act to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes.* U.S Government Publisihing Office Law.107-204. Washington D.C.

AdaletBakanlığı. (2012). ttp://www.ankara.adalet.gov.tr/duyurular/dosyalar/2015/10/EK2.pdf (12.01.2017).

Adıgüzel, G. C. (2009). *Güvenlik endişesinn internet bankacılığı kullanımına etkisi ve vakıfbank müşterilerine yönelik bir araştırma.* Yüksek lisans tezi, Gazi Üniversitesi, Ankara. 90-91

AICPA. ve CICA. (2009). Generally accepted privacy principles. Chartered professional accountants Canada. *The Institute of Internal Auditors*. 7-9.

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

Akram, M. ve Habiba, H. (2015). Evaluation of users' awareness and their reaction on information security. *4th International Conference on Advanced Computer Science Applications and Technologies* (ACSAT).

Aksu, M. (1993). Uluslararası pazarlamanın önemi ve dışa açılma düşüncesinde olan işletmelerin dikkate alması gereken faktörler. *Pazarlama Dünyası Dergisi* (42), 19-25.

Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computer and Security*. 26(4), 276-289.

Aleamoni, L. M. (1976). The relation of sample size to the number of variables in using factor analysis techniques. *Sage journals.* 36(4).

Almagwashi, H. ve Gray, A. (2012). *Preserving privacy in E-government: A System Approach.* Proceedings of IFIP EGOV2012, Kristiansand, Norway

Altundal, Ö. F.(2014).Sibergüvenlikraporu14. http://www.siberguvenlik.org.tr/2015/01/2014-Siber-Guvenlik-Raporu- Yayinlandi.html (02.08.2017).

Anonim. (2003). *Pro-G Proje bilişim güvenliği ve araştırma San. ve Tic. Ltd. Şti*. Bilisim güvenliği kitapçığı. 7

Anderson, R. (2001). Security engineering: A guide to building dependable distributed systems. *Wiley Publishing* .

Apak, S. ve Atay, E. (2014). Küresel yenilik ve KOBİ'lerde yönetim pratiği ve Balkanlar. *Prcocedia-Social and Behavioral Sciences*. 150: 1260-1266.

Atalay, A. (2014). Siber güvenlik ve siber suçlar. http://www.slideshare.net/ahatalay/sber-gvenlk-ve-sber- sularahaaralk2014-43135183. (14.06.2016).

Aytaç, M., ve Öngen, B. (2010). Doğrulayıcı faktör analizi ile yeni çevresel paradigma ölçeğinin yapı geçerliliğinin incelenmesi. *İstatikçiler Dergisi.* 5,14-22.

Cox, B., Tygar, J. D. ve Sirbu, M. (1995). Net Bill security and transaction protocol. *Proceedings of the First USENIX Workshop on Electronic Commerce*. New York: 11

Barata, K., ve Cain, P. (2001). Information, Not Technology, Is Essential to Accountability: Electronic Records and Public-Sector Financial Management. *The Information Society*. 247-258.

Barışık, S. Temel, H. (2007). İnternet bankacılığı kullanımında güvenlik unsurlarının bilinirliği (Anket uygulamasına dayalı SPSS çözümlemesi): Karaelmas Üniversitesi, Zonguldak. 153

Baumhof, A. (2012)Credit Unions and the Evolving Cybercrime Landscape. from Credit Unions:http://www.cutimes.com/2012/02/08/credit-unions-and-the-evolving-cybercrime-landscap.(22.07.2016)

Başdandikçi N. (2017). *Sağlık kurumlarının bilgi güvenliği risk değerlendirmesi ve kullanıcıların bilgi güvenliği farkındalık düzeylerinin ölçülmesi*, Adana.

Bellare, M., Garay, J., ve Hauser, R. (1995). *iKP– A family of secure electronic payment protocols. Proceedings of the First USENIX Workshop on Electronic Commerce.* New York.

Bensghir, T.K. (2008). *Kurumsal bilgi güvenliği yönetim süreci*. www.erzincan. edu.tr/user les/ le/stratejidb/guvenlik.ppt. (10.06.2017)

Bhattacharya, A. ve Kumar, S. (2015). Advances in Computing, Communications and Informatics. *ICACCI. California* 125-131

Bilim, Sanayi ve Teknoloji Bakanlığı (2016). http://anahtar.sanayi.gov.tr/tr/news/kobiler-ve-girisimcilerin-turk-ekonomisindeki-yeri-ve-onemi/261 (12.10.2017)

Bisson, D. (2015). The OPM breach: Timeline of a hack, *Tripwire* 1-8.

Bishop, D. (2004) Immature cortical responses to auditory stimuli in specific language impairment: evidence from ERPs to rapid tone sequences Wesley Professional Publications California, USA: 14(7), 4.

Boateng, Y. ve Osei, E. (2013). *Cyber-Security Challenges with SMEs in Developing Economies: Issues of Confidentiality, Integrity and Availability (CIA).* Doktora tezi, Aalborg University, Aalborg: 185-187

Borenstein, ve Freed, N. (1993). *Multipurpose internet mail extensions (MIME). RFC:1521*

Brown, A., Johnston, S. ve Kelly, K. (2002). *Sing Service-Oriented Architecture and Component-Based Develop- ment to Build Web Service Applications.* Rational Software Corporation. United States, Foster City:6

Buchanan, S. ve Gibb, f. (2007). The information audit: Role and scope. *Elsevier Oxford United Kingdom.* 27(3), 159-172.

Buchanan, S., ve Gibb F. (2009). The information audit: Methodology selection. *International Journal of Information Management, Elsevier, Volume:28 Issue:1 Oxford United Kingdom.* 3-11.

Büyüköztürk, Ş. (2002). *Faktör analizi: Temel kavramlar ve ölçek geliştirmede kulanımı. Kuram ve Uygulmada Eğitimi Yönetimi. Dergipark Sayı:32:470-483*

Canberk, G. ve Sagıroglu, Ş. (2006). *Bilgi ve Bilgisayar Güvenliği Casus Yanlımlar ve Korunma Yöntemleri*. Ankara. Grafiker Yayınları 1.baskı Ankara 165-174.

Cavusoglu, H. (2004). *Bilgi işlem yönetiminin ekonomisi*. New York: Springer US.

CCITT. (1988). Message handling system and service overview Cambridge:2 Massachussets Institue of Technology: Rec. F.400.

Charney, S. (2009). Rethinking the Cyber Threat. Redmond: *Microsoft Corporation*. 12 http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=747(12.11.2017)

Chen, C., Show, R., ve Yang, S. (2006). Mitigating ınformation security risks by ınc- reasing user security awareness: A case study of an ınformation security awareness system. *Information Technology, Learning and Performance Journal 24(1)* ,1-14.

Cherdantseva, Y. ve Hilton, J. (2013). A Reference Model of Information Assurance and Security ARES 2013 secont workshop 2-6. *Regensburg:Germany University of Regensburg IEEE*. 57-50.

Cherdantseva, Y., Rana, O. Ivins, W. ve Hilton, J. (2016). A Multifaceted Evaluation of the Reference model of information assurance and security. *ScienceDirect,Computer&Security*. 63, 45-66:

CNSS. (2010). *Committee on national security systems*. National Information Assurance (IA) Glossary . Instruction No. 4009.

Combe, C. (2006). I*ntroduction to e-business: Management and strategy.* Oxford, United Kingdom.

Commision, E. U. (2009). *European union commision*. Bruksel: European union commision .

Comrey, A. L. ve Lee, H. B. (1992). *A first course in Factor Analysis.* Psychlogy Press.

Crocker, D. (1982). *Standard for the format of ARPA Internet text messages*. RFC, 822.

Çetin, H., Gundak, İ., ve Çetin, H. H. (2015). E-işletme güvenliği ve siber saldırılar üzerine bir araştırma. *Çankırı Karatekin Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*. 223-240.

Çetinkaya, M. (2008). *Bİlgi güvenliği yönetim sisem alyapısının değeredirilms iin bir test aracı geliştirilmesi*. Yüksek Lisans Tezi, İstanbul Kültür Üniversitesi, İstanbul.

Çokluk, Ö., Şekercioğlu, G., ve Büyüköztürk, Ş. (2010). *Sosyal bilimler için çok değişkenli istatistik. SPSS ve LISREL Uygulamaları.* Ankara: PEGEM Akademi Yayınları.

Parker. D. (1998). *Fighting Computer Crime*:*A New Framework for Protecting Information* New York : John Wiley and Sons.

D., P. (2010). Our excessively simplistic ınformation security model and how to fix ıt. *ISSAJournal*.http://www.issa.org/images/upload/files/ParkerSimplistic%20Information%20Security%20Model.pdf.(11.10.2017)

Damanpour, F. (2001). E-business e-commerce evolution: Perspective and strategy. *In Managerial Finance, 27 .Virginia James Madison University* 16-33.

DPT. (1999). *Sekizinci 5 yıllık kakınma planı(2001-2005).* Ankara:Başbakanlık Matbaası

Duda, G. (2016, Ocak 15). Küçük şirketler büyük siber tehdit altında, Sanayici Dergisi: http://www.sanayicidergisi.com/soylesi/kucuk-sirketler-buyuk-siber-tehdit-altinda.htm(16.09.2016)

Durumeric, Z., Kasten , J., Adrian , D., Halderman , J. and Bailey, M. (2014). The matter of Heartbleed. . *IMC'14 Proceedings of the 2014 Conference on Internet Measurement Conference.*

Duy Dang, P., Siddhi , P. ve Vince, B. (2016). Why employees share information security advice? Exploring the contributing factors and structural patterns of security advice sharing in the workplace. Autralia: *Science Direct*. 204-205.

Edinburg Grup. (2010). Growing the global economy through SMEs. Retrieved from http://www.edinburghgroup.org/media/2776/edinburgh_group_research__growing_the_global_economy_through_smes.pdf (22.10.2017).

E-Marketer. (2014). Global B2C Ecommerce Sales to Hit $1,5 Trillion This Year Driven by Growth in Emerging Markets,. http://www.emarketer.com/Article/Global-B2C-Ecommerce-Sales-Hit-15-Trillion-his-Year-Driven-by-Growth-Emerging-Markets/1010575. (25.09.2017).

Eminağaoğlu, M. ve Gökşen, Y. (2009). Bilgi güvenliği nedir, ne değildir, Türkiye' de bilgi güvenliği sorunları v e çözüm önerileri. *Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi.*4, İzmir:1-15.

Erkan, A. (2006). *An automated tool for information security management system*, Master. The Middle East Technical University, Ankara.

Enigma, S. (2016). Enigma software. http://www.enigmasoftware.com/top-20-countries-the-most-cybercrime/ (22.07.2016).

European Parliament ve the Council,(1995) Directive 95/46/EC of 24.10.1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, Brussels, 23 November 1995.

European Commission(2012). Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM(2012) 11/final, Brussels, 25 January 2012.

Eroğlu, N. ve Yücel İ. S.(2012). *Türkiye'deki kurumsal banka müşterilerinin internet bankacalığı kullanım eğilimlerini belirleyen başlıca faktörler üzerinde ampik bir çalışma.* Yüksek Lisans Tezi, Marmara Üniversitesi. İstanbul.

Farahmand, F., Shamkant, B. N., Gunter, P. S., ve Philip, H. E. (2006). A management perspective on risk of security threats to ınformation systems. *Springer Science.* 6(2-3), 203-225.

Fariborz Farahmand, Sharp, G., ve Enslow, P. (2005). A management perspective on risk of security threats to ınformation systems. *Springer Science*. 6(2-3), 203-225.

Financial Reporting Council (FRC). (2005). Internal Control: Revised Guidance for Directors on the Combined Code . London::3-38

Gelfand,, M. J. ve Realo, A. (1999). Individualism-collectivism and accountability in intergroup negotiations. *Journal of Applied Psychology*,84(5)Washington Dc::721-736

Gorsuch, R. L. (1983). *Factor analysis* (2nd ed.). Hillsdale, NJ: Erlbaum. https://link.springer.com/chapter/10.1007/978-1-4613-0893-5_6 (12.10.2017)

Government, Canada. (2013). *Staticstics of small business* . Public Works and Government Service Canada.Ottawa:5

Govenment UK (2015). *Small businesses: what you need to know about cyber security*. London: Crown copyright.

Guilford, J. P. (1954). *Psychometric methods*. New York: Mcgraw-Hill

Gülmüş, M. (2010). *Kurumsal bilgi güvenliği yönetim sistemleri ve güvenliği*. Yüksek lisans tezi. İstanbul: Yıldız Teknik Üniversitesi.

Hacigümüş H., Iyer, B., ve Mehrotra, S. (2007). *Encrypted database ıntegrıty ın database servıce provıder model.* California: IBM.

Hakli, T. (2012). *Bilgi Güvenliği Standartları ve Kamu Kurumları Bilgi Güvenliği için Bir Model Önerisi.*Yüksek Lisans tezi Süleyman Demirel Üniversitesi Isparta.:63

Harris, S. (2002). *Cissp certification exam guide*. CA: Osborne/McGraw-Hill, BerkeleY.

HMSO, (1971), *Report of the Committee of Inquiry on Small Firms* (Bolton Report), Cmnd 4811, HMSO, London.

Hpe Security Reseacrh (2016). *Cyber risk report* 2016. California: 57

Hindi, S. (1996). *Management responsibility for auditablity first edition*. Elsevier Science 12(1) Oxford United Kingdom:22

Hovay, A., ve D'Arcy, J. (2004). *The impact of virus attack announcements on the market value of firms. Fox school of business and management*. United States: Information Systems Security.:45

Ponemon. (2014). Anual Study: U.S. cost of a data breach. Retrieved from https://www.fbiic.gov/public/2011/mar/2010_Annual_Study_Data_Breach.pdf: (22.06.2016).

ISACA. (2009). *An introduction to the business model for ınformation security.* www.isaca.org/KnowledgeCenter/Research/ResearchDeliverables/Pages/An-Introduction-to-the-Business-Model-for-Information-Security.aspx(22.11.2017)

Isidore, C. (2015). http://money.cnn.com/2015/08/18/news/companies/target-visa-hack-deal/index.html,(26.02.2016).

ISO/IEC. (2009). Information technology Security techniques Information security management systems. ISO/IEC 27000 Scientific Research 2013 4 Hannover: 92-100

J., M. (1991). Information Systems Security: A Compre- hensive Model. *14th National Computer Security Conference.*

1. J.Bolton (1971). ″Report of the Committee of Inquiry on Small Firms," HMSO, London

Johnson, D. G. ve Mulvey, J. (1995). *Accountability and computer decision systems*,. Communications of the ACM.: 58

Johnson, D. G., ve Nissenbaum, H. (1995). *Computing and accountability. computers, ethics and social values*.Upper Saddle River Prentice Hall Skovira R:J: 526-538

Johnson, E. (2006). Towards an integrated conceptual model of security and dependability. *The Firts International Conference on IEEE.*

Johnson, M. (2013). *Cyber Crime*. Security and Digital Intelligence. London:Routledge.

Kalaycı, Ş. (2010). *SPSS uygulamalı çok değişkenli istatistiksel teknikleri.* Ankara: 1.baskı Asil Yayın Dağıtım.:64

Kapanoğlu, G. (2016). *Öğretmenlerin bilgi güvenliği farkındalığının incelenmesi.Yüksek lisans Tezi* Ankara Üniversite:84

Karabacak, B. (2003). *Bilgi güvenliği risk analizi (bigra) yöntemi*. Yüksek Lisans Tezi, Gebze Yüksek Teknoloji Üniversitesi, Kocaeli:84

Karasar, N. (1995). *Bilimsel araştırma yöntemi.* 7.basım Sim Matbaası. Ankara:62

Karsten, B. (2011). Authentıcatıon and securıty aspects in an international multi-user network. 5.

Kellaway, L. (2013) Bbc web site: http://www.bbc.com(11.02.2016)

Keser, H. ve Güldüren, C. (2015). Bilgi güvenliği farkındalık ölçeği (BGFÖ) geliştirme çalışması. *Kastamonu Eğitim Dergisi 6(2):223-240*

Ketizmen, M., ve Ülküderner, Ç. (2012). *E-Devlet Uygulamalarında Kişisel Verilen Korun(ma)ması.* XVII. Türkiye'de İnternet Konferansı. Anadolu Üniversitesi.

Kjorvik, H. (2010). *Implementing and improving awareness in information security.* (Master's thesis, University of Agder, Faculty of Engineering and Science, Grimstad).

Knorr, K. ve Rohrig, S. (2015). *Security requirements of e-business processes.* Zürih: University Of Zurich.

KOSGEB. (2003). *Kobi ekonomisi(Tarihi Gelişme)*. Ankara: 2Yayınları.

Kosgeb. (2008). *2008 yılı performans programı.* Ankara: Sanayi ve Ticaret Bakanlığı.

KOSGEB. (2012). *2011-2013 KOBİ stratejisi ve eylem planı*. Ankara: KOSGEB-Küçük ve Orta Ölçekli İşletmeleri geliştirme ve Destekleme İdaresi Başkanlığı.

Kovacich, G. (1998). Electronic-ınternet business and security. *Is Computers and Security*,17(2), 129-135.

Kritzinger, E., ve Smith, E. (2008). Information security management:An information security retrieval and awareness model for industry. *Computer and Security 27(5-6):*. 225

Kruger, H., ve Kearney, W. (2006). A prototype for assessing information security aware ness. *Computer and Security ISS, 1-11:16.*

KÜÇÜK, O. (2005). *Girşimcilik ve küçük işletme yönetimi.* (1.baskı) Ankara: Seçkin Yayıncılık.

Leclair J. ve Keeley G. (2015). *Cybersecurity in our digital lives.* New York: Hudson Whitman/ Excelsior College Press.

Lagou P. ve Chondrokoukoukis G. (2009). Survey on Nonrepudiation:Digital Signature Versus Biometrics Athens: Taylor & Francis Group 18: 257-266f

Maconachy, W., Schou, C., Ragsdale, D., ve Welch, D. (2011). A model for ınformation assurance: an ıntegrated approach . *2001 IEEE Workshop on Information Assurance and Security, . 2001: U.S. Military Academy* .

Maconanchy, W., Schou, C., Ragdale, D., ve Welch, D. (2001). A model for ınformation assurance: *An ıntegrated approach*. *2001 IEEEE Workshop on Information Assurance and Security. NY: U.S Military Academy.*.

Mark, J. (2013). *Cyber crime, security and digital ıntelligence*. Farnham Surrey.

Mart, i. (2012). *Bilişim kültüründe bilgi güvenliği farkındalığı.*Yüksek Lisans tezi Kahramanmaraş Sütçü İmam Üniversitesi, Kahramanmaraş.:92

Mcafee Labs & Mcafee Fundstone Professional Service. (2010, Mart 1). Değerli varlıklarını koru: "Aura Operasyonun' dan çıkartılan dersler. htttp://www.wired.com/images_blogs/threatlevel/2010/03/operationaurora_wp_0310_fnl.pdf, (25.05.2016).

McCumber, J. (1991). Information systems security: A compre- hensive model. *Baltimore 14th National Com- puter Security Conference.*

MEB. (2013). http://bigb.meb.gov.tr/meb ivs dosvalar/2013 01/03030227 a. nketsonucdegerlendirme.pdf (22.06.2016)

MÜSİAD. (2012). *Küresel rekabet için ar-ge ve inovasyon stratejik dönüşüm önerisi:*76.

Nabil, A. ve Yesha, Y. (1996). *Electronic commerce: An overview vol 1028. Springer, Berlin*,Heidelberg:5-12

NATO. (2006). http://www.nato.int/docu/review/2013/Cyber/timeline/TR/index.htm. (22.06.2017).

Neumann, P. (1995). *Computer-related risks*. ACM Press 4th edition. New York, USA:7

Nissenbaum, H. (2004). *Privacy as contextual ıntegrity*. Washington Law Review 79(1), 101-158

O'Brien, J. ve Marakas, G. (2008). *Management ınformation systems*. (8.nd. Ed). Boston: Mc.Graw-Hill Irwin.

OECD. (1980). *Guidelines on the protection of privacy and trans- border flows of personal data. OECD Vol 21 no:4 :405-420.*

OECD.(1997).etrievedhttp://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/cote=OCDE/GD(97)185&docLanguage=En (28.06.2017).

OECD. (2014). Small Businesses Job Creation and Growth: Facts. Retrieved from https://www.oecd.org/cfe/smes/2090740.pdf (28.06.2017).

Öner, N. (1997). *Türkiye'de kullanılan psikolojik testler, bir başvuru kaynağı*. Üçüncü baskı İstanbul: Boğaziçi Üniversitesi Yayınları, No 584

Öncü H. (1994) Eğitimde Ölçme ve Değerlendirme. Ankara: Matser Basım .

Özgüven, İ. E. (2000). *Psikolojik testler*. Ankara: PDREM Yayınları 4.Baskı: 83-109

Öztürkçi, H. (2016). *Görevimiz tehlike! siber güvenlikte yeni yaklaşımlar*. İstanbul: Microsoft.:16

Öğüt, P. (2006). *Küreselleşen dünyada bilgi güvenliğine yönelik politikalar: Sayısal İmza teknolojisi ve Türkiye*. Yüksek Lisans Tezi, Ankara Üniversitesi, Ankara.

Parker , D. (1998). *Fighting computer crime: A new framework for protecting information* New York: 57

Pearson, S. (2012). Privacy Management in Global Organisations. https://link.springer.com/conference/cms 217-237(12.10.2017)

Perez, N. L. (2000). Survey on nonrepudiation. *Digital Signature Versus Biometrics* (18)3, 257-266.

Peltier, T. R. (2001). *Information Security Risk Analysis*. Auerbach ISBN 0-8943-0880-1

Pierre, L. (2008). *The Wall Street Networks.*

Piggin, R. (2016). Cyber Security trends: What should keep CEOs awake at night. *ScienceDirect, International Journal of Critical Infrastructure protection 13, 36-38.*

Planque, B. (1988). La PME innovatrice : quel est le rôle du milieu local? *Revue*

Internationale PME, 1(2), 177-191.

Polit, H. ve Portney, W. (1993)*Research in health care:concepts designs and methods 2th Edition:112*

Privacy Protection Study Commission. (1977). United Statues privacy protection study commission fair ınformation practices. Personal Privacy in an Information Society. http://epic.org/privacy/ppsc1977report (12.11.2016)

Puhakainen, P. (2006). A design theory for Information Security Awareness, Oulu University Press ISSN 1796-22Ox, Oulu: 83

Report of the Secretary's Advisory Committee on Au. (1973). Computers ve the Rights of Citizens, .

Rezgui, Y., ve Marks, A. (2008). Information security awareness in higher education: An exploratory study. Comptuer And Security. https://www.epic.org/privacy/hew1973report/foreword.htm(12.11.2017)

Robert, B., ve Chun, W. C. (2017). Revisiting the information audit: A systematic literature review and synthesis. Elsevier Volume:37 Issue.1 1380-1390

Rogowsky, R. A., Koopman, R. B., ve Cummings, K. L. (2010). Small and Medium- Sized Enterprises: Overview of Participation in U.S. Exports. Washington dc: United States International Trade Commission.

Root, F. R.(1994). Entry Strategies for International Markets, Lexington Books, Lexington, MA

Rosen, H. (2001). Dünya Bankasının Küçük işletmelerin aktiviteleri ile ilgili görüşü. , http://www.ds.worldbank.org/external/default/WDSContentServer/WDSP/IB/2002/01/18/000094946_02010904093269/Rendered/PDF/multi0page.pdf (April 14, 2016).

Saltzer, J., ve Schroeder, M. (1975). The protection of information in computer systems. Procedings of the IEEE Volume:63 Issue:9:1278-1308

Sarbanes-Oxley. (2002). Act of 2002. Public Law 107-204:Washington Dc

Sayari, N. (2009). Bilgi Güvenliği Ve Yönetimi. Ankara: Türkiye Bilişim Derneği Ankara Şubesi Eğitim Etkinliği.

Schermelleh-Engel, K., ve Helfried, M. (2003). Evaluating the Fit of Structural Equation Models: *Tests of Significance and Descriptive Goodness-of-Fit Measures.Methods of Psychological Research*. 8(2), 23-74.

Sevim, A., ve Gül, M. (2012). Elektronik İşletmelerde (E-İşletmelerde) Satın Alma İşlemleri ve İç Kontrol İlişkisi. *Afyon Kocatepe Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*. 14(2), 91-118.

Sencer, M. ve Sencer, Y. (1978). *Toplumsal araştırmalarda yöntembi lim*. Ankara: 1.basım Doğan Basımevi.

Shackelford, S. (2016). Business and cyber peace: We need you! Indiana University, Bloomington, *ScienceDirect Volume:59 Issue:*5:539-548

Sharma, Kunal, Singh, A., ve Prakash, V. (2009). *Kobiler ve e-ticarette siber güvenlik tehditleri: 39*

Sharma, R. (2015). Five ways board members can improve cybersecurity. *Journal of Internet Law* . Aspen Publishers Inc 20-5. 11-12.

Siponen, M. (2001). Five Dimensions of ınformation security awareness. *Computer and Society New York.Volume:31 Issue2:24-29*

Skovira, J. R. (2003). The Social Contract Revised: Obligation and Responsibility in the Information Society. In: Azari, R. (ed.) Current Security Management & Ethical Issues of Information Technology.USA Chapter X IRM press.: 165

Smith, R., ve Shao, J. (2007). *Privacy and e-commerce: a consumer-centric perspective*. Electronic Commerce Research .Springer Science+Business Media Electron Commerce Res 7:89-116

Stahl, C. S. (2006). *Accountability and reflective responsibility in information system*. https://pdfs.semanticscholar.org/cf99/8c5840faf1a9f9e39c3a6372ee214a4ddc86.pdf(11.10.2017)

Stuides, C. F. (2014). Net losses: Estimating the global cost of cybercrime. Retrieved from http://www.mcafee.com/us/resources/reports/rp-economics-impact-cybercrime2.pdf .(22.06.2016).

Su, X. (2006). *An overview of economic approaches to ınformation security management*. Technical Report. TR CTIT 06-30 University of Twente

Suhail, Q., ve Quadri, S. (2016). Information Availability: An Insight into the Most Important Attribute of Information Security. Information Security.187:192 (22.06.2016).

Symantec,C.(2016).İnternetTehditraporuhttps://www.symantec.com/content/dam/symantec/docs/reports/istr212016en.pdf?aid=elq_&om_sem_kw=elq_16388824&om_ext_cid=biz_email_elq_&elqTrackId=283a3acdb3ff42f4a70ab5a9f236eb71&elqaid=2902&elqat=2. (22.06.2016).

Sorrentino, F., (2015) Cyber Attacks: 5 Ways Small Businesses Can Protect Themselves https://www.forbes.com/sites/franksorrentino/2015/10/26/cyber-attacks-5-ways-small-businesses-can-protect-themselves/#2a17abe53193. (5.02.2016).

Şahinaslan, E., Kandemir, R. ve Şahinaslan, Ö. (2009). Bilgi güvenliği farkındalık eğitimi örneği. *XI. Akademik Bilişim Konferansı Bildirileri* (ss. 189-194). Şanlıurfa: Akademik Bilişim.

Şahinaslan, E., Kantürk, A., Şahinaslan, Ö. ve Borandağ, E. (2009). *Kurumların bilgi güvenliği farkındalığı, önemi ve oluşturma yöntemleri.* XV. Akademik Bilişim Konferansı. Şanlıurfa: Harran üniversitesi.

Şağbanşua, L., (2006), "Strateji, Rekabet ve Rekabet Gücü İlişkileri", Akademik Bakış E-Dergi Sayı 9, s.2.

Tabacnick, ve Fidell. (2001). *Using multivariate statistics.* Pearson Education 6th edition New York:94

Tadmor, C. ve Tetlock, P. (2009). *Accountability.* In the cambridge dictionary of psychology. : 8

Tavşancıl, E. (2002). *Tutumların ölçülmesi ve SPSS ile veri analizi.* Ankara: Nobel Yayınevi.

Tezbaşaran, A. (1996). *Likert tipi ölçek gelştirme kılavuzu.* Ankara: 2.baskı Psikoloji Derneği Yayınları.

Tekin, H. (1977). *Eğitimde ölçme ve değerlendirme*. Ankara: Mars Matbaası 1.baskı:44

The White House: Consumer Data Privacy in a Network. (2012). *A framework for protecting privacy and promoting ınnovation in the global digital economy*. http://www.**whitehouse**.gov/sites /default/files/**privacy**-final.pdf (22.11.2017)

Trend, M. (2016). Güvenlik Raporu. Retrieved Ağustos 22, 2016, from http://blog.trendmicro.com.tr/siber-saldirilarda-turkiye-ilk-sirada/. (22.08.2016).

TrendMicro. (2015). Magnified Losses. Trendlabs 2014 Annual Security Roundop.:5 http://www.trendmicro.de/media/misc/magnified-losses-amplified-need-for-cyber-attack-preparedness-report-uk.pdf (12.07.2017)

Tsai, W., Wei, X., Chen, Y., Paul, R., Chung, J.-Y., ve Zhang, D. (2007). *Data provenance in SOA: security, reliability, and integrity.* Springer Link Volume:1 Issue:4London:223-247

Türkiye Cumhuriyeti Kalkınma Bakanlığı. (2016). Kalkınma Bakanlığı. http://www.kalkinma.gov.tr. (20.04. 2016).

Türkiye İstatistik Kurumu. (2015). Türkiye İstatistik Kurumu. http://www.tuik.gov.tr/ (12.02. 2016).

U.S. Privacy Protection Study Commission. (1977). *Personal privacy in an ınformation society. https://www.epic.org/privacy/ppsc1977report/ (13.06.2017)*

Ünver, M., Canybay, C. ve Mirzaoğlu, A. (2009). *Siber güvenliğinin sağlanması.* Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler Bilgi Teknolojileri ve Koordinasyon Dairesi Başkanlığı Ankara, Mayıs 2019

Vacca, J. R. (2009). *Computer and ınformation security handbook*. Second Edition Steve Eliot Waltham :92

Brumfield, J.(2016) "Verizon's 2016 data breach investigations report finds cybercriminals are exploiting human nature," http://www. verizon. com/about/news/verizons- 2016-data-breach-investigations-report-finds- cybercriminals-are-exploiting-human-0, 2016 (11.10.2017)

Ware, W. ve Pfleeger, S. (2006). *Security in computing Fifth Edition Prentice Hall San Francisco:312-320*

Warren, S., ve Brandeis, L. (1980). The right to privacy. (4.nd. Ed). US: Harvard Law Review.

Weitzner, D., Abelson, H., Berners-Lee, T., Feigenbaum, J., Hendler, J. ve Sussman, G. (2008). *Information accountability*. Communications of the ACM. 83

Westin, A. (1967). *Privacy and freedom*. Atheneum, New york.

Whitman, M. Ve Mattord, H. (2012). *Principles of ınformation security* (4.nd. Ed). Cengage Learning.:23

Whitman, M. ve Mattord, H. (2014). *Principles of ınformation security.* Fourth Edition Course Techonology, Cengage Learning:32

Wilson M. Hash J. (2003). *Computer security, national ınstitute of standards and techonology Nist Special Edition 800-50, Washington*: 9.

Yakel, E. (2001). The social construction of accountability: Radiologists and their record keeping practices. *The Information Society Volume:17,2001 Issue:4*.:233- 243.

Yan, Y., Qian, Y. H. ve Tipper, D. (2012). A survey on cyber security for smart grid communications. *IEEE COMMUNICATIONS SURVEYS and TUTORIALS.* 14(4), 998-1007.

Yıldız, M. (2014). *Siber suçlar ve kurum güvenliği.* Ankara: Ulaştırma Denizcilik ve Haberleşme Bakanlığı Bilgi İşlem Daire Başkanlığı. Denizcilik uzmanlık tezi 58-59

Yıldırım, H. M. (2014). Bilgi güvenliği ve kriptoloji . *Uluslararası Adli Bilişim Sempozyum. Ankara.*

Zeydan, Ö. (2006). Kişisel Bilgisayarlar ve İnternet Güvenliği. *XI. "Türkiyede internet.*

Zhou, J. ve Gollmann, D. (1997). Elsevier. *Journal of Network and Computer Applications.* 20(3), 267-281.

Zwass, V. (1996). Electronic commerce: Structures and issues. *International Journal of Electronic Commerce, Volume:1 Issue:1 United Kingdom* (3-23).

EKLER

EK 1.Anket Soruları

Değerli Katılımcı,

Bu anket çalışması, Hasan Kalyoncu Üniversitesi Sosyal Bilimler Enstitüsü İşletme Ana Bilim Dalında Prof. Dr. Gülçimen YURTSEVER danışmanlığında, Cüneyt ÇATUK tarafından hazırlanmakta olan **"Gaziantep'te Faaliyet Gösteren KOBİ'lerin Siber Riskler karşısında Bilgi güvenliği Farkındalığı "** adlı doktora tezine veri temin edilmek amacıyla yapılmaktadır. Bu tezin bilime katkısı aşağıda sunulan anketin tamamlanması sayesinde olacaktır. Bu anket ile toplanacak veriler sadece bilimsel amaç için kullanılacak olup çalışmanın başarıya ulaşabilmesi sizlerin düşüncelerinizi doğru olarak aktarabilmesine bağlıdır. Katılımınızdan dolayı şimdiden teşekkür ederiz. Lütfen her bir soru için verilen seçeneklerin sadece birinin işaretleyiniz.

Prof. Dr. Gülçimen YURTSEVER
Hasan Kalyoncu Üniversitesi İİSBF
Uluslararası Ticaret ve Lojistik Bölüm Başkanı

Cüneyt ÇATUK
Hasan Kalyoncu Üniversitesi
SBE Doktora Öğrencisi

1. **Cinsiyetiniz**	◯ **Erkek** ◯ **Kadın**
2. Aylık ortalama geliriniz ne kadar (TL) ?	◯ **2000 ve altı** ◯ **2001 -4000** ◯ **4001-5000** ◯ **5001-7000** ◯ **7001 ve üzeri**
3. **Kaç yaşındasınız?**	◯ **20- 25 Yaş Arası** ◯ **26-30 Yaş Arası** ◯ **31-35 Yaş Arası** ◯ **36-40 Yaş Arası** ◯ **41-45 Yaş Arası** ◯ **46- 51 Ya Arası** ◯ **52-56 Yaş Arası** ◯ **57- 65 Yaş Arası** ◯ **66 ve üzeri**
4. Eğitim durumunuz nedir?	◯ İlköğretim ◯ Lise ◯Ön lisans ◯ Lisans ◯ Lisansüstü
5. Firmanızdaki pozisyonunuz nedir?	◯Üst düzey yönetici (Genel Müd., Şirket Müd., Fabrika Müdürü, Genel Müdür Yardımcısı vb.) ◯Orta düzey yönetici (Bölüm Md., Departman Md., Kısım Md. vb.) ◯Alt Düzey yönetici(Şef, Md. Yrd., Vardiya Amiri vb.) ◯Teknik çalışan ◯İdari çalışan

6. Firmanızda kaç kişi çalışıyor?	◯ 0-10 Arası ◯ 11-49 Arası ◯ 50-249 Arası
7. Firmanız kaç yıldır faaliyette bulunmaktadır?	◯ **0-5** ◯**6-10** ◯ **11-15** ◯ **16-20** ◯ **21 ve üzeri**
8. Firmada ne zamandan beri çalışıyorsunuz?	◯ **0-5** ◯ **6-10** ◯ **11-15** ◯ **16-20** ◯ **21 ve üzeri**
9. Bilgisiyarınızda virüs programı var mı ?	◯ Evet ◯ Hayır
10. Virüs programınızı (en son ne zaman) güncellediniz ?	◯ **1 aydan kısa bir süre önce** ◯ **6 aydan önce** ◯ **1 yıldan önce** ◯ **2 yıldan önce** ◯ **3 ve daha fazla önce**

11.Firmanızda, kimlik doğrulması yaparken hangi teknikleri kullanıyorsunuz? Size en uygun seçeneği işaretleyiniz

- ☐ Herhangi bir teknik yok
- ☐ Basit faktörler(örnek kullanıcı adı + şifre)
- ☐ Donanım (akıllı kartlar**)**
- ☐ İkili yazılı faktörü(Dijital sertifikalar + sembol**)**
- ☐ Üçüncü faktör(göz taraması, parmak izi)

12. **Şifrelerinizi nasıl belirliyorsunuz? Size en uygun seçeneği işaretleyiniz.**

- İlk belirlenen ve bana verilen şifreyi kullanıyorum
- Unutmamak için akılda kalan kolay bir şifre belirliyorum
- Şifremi en az altı karakterden oluşturuyorum
- İçinde büyük, küçük harf, rakam ve simge gibi farklı karakterler bulunan şifre belirliyorum
- Unutmamak için tüm şifrelerimi aynı kullanıyorum.
- Kısa şifreler belirliyorum

13.Şifrelerinizi ne sıklıkla değiştiriyorsunuz? Size en uygun seçeneği işaretleyiniz.

- Hiç değiştirmiyorum
- Şifremin birinin eline geçtiğini düşünür isem değiştiriyorum
- Şifremi birisine vermek zorunda kalırsam değiştiriyorum
- Şifremi çok sık değiştiriyorum
- Şifremi altı aydan daha kısa sürede değiştiriyorum.
- En geç yılda bir değiştiriyorum

Lütfen, her bir ifadeye ilişkin katılım düzeyinizi belirtiniz. ***1-Kesinlikle Katılmıyorum*** ***2-Katılmıyorum*** ***3-Kararsızım*** ***4-Katılıyorum*** ***5.Kesinlikle Katılıyorum***	**Kesinlikle Katılmıyorum**	**Katılmıyorum**	**Kararsızım**	**Katılıyorum**	**Kesinlikle Katılıyorum**
1. Firmamız, yetkimizin olmadığı dosyalara girişlerimizi engeller.(Raporlar, Sistem dosyası, Bilgi deposu, Ortak dosya vs.)	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**
2. Firmamızda, teknolojik cihazlarda (makina, bilgisayar ve benzeri) izinsiz erişimi engellemek adına gerekli önlemler bulunur.	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**
3. Firmamızda, önemli bilgilerin gizliliğinin korunabilmesi için ‘’Güvenli belge deposu’na benzer önlemler bulunur.(Bilgi Deposu vs.)	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**
4. Firmamızda, önemli bilgilerin gizliliğinin korunabilmesi için ‘’Genel güvenlik politikaları’’ uygulanır.	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**
5. Firmamızda, önemli bilgilerin gizliliğini korunabilmesi için ‘’Bilgi saklama alanı’’ kullanılır.(Sistem Dosyası, Bilgi dosyası, vs.)	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**
6. Firmamız, önemli bilgilerin gizliliğinin korunabilmesi için ‘’son kullanıcıların eğitimine ‘’ önem verilir.	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**
7. Firmamızda, önemli bilgilerin gizliliğinin korunabilmesi için ‘’Bilgi sınıflandırması’’ kullanılır.(İhracat Departmanı, İthalat Departmanı, İç piyasa)	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**
8. Firmamız, internetten yüklenen bütün dosyaların virüs programıyla taranmasına önem gösterir.	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**
9. Firmamız, müşterilerimizle olan iletişim sırasında herhangi bir verinin değiştirilmesi olasılığına karşı önlem alınır.	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**

10. Ciddi bir siber saldırı ile bilgilerimizin zarar görmesi durumunda firmamızın önemli derecede etkileneceğini düşünmekteyim.	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**
11. Firmamızda, verilerin izinsiz değiştirilmesi konusunda önlemler alınır.	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**
12. Kullandığımız bilişim sistemlerinin herhangi bir unsurunun (yazılım veya donanım vb.) kendisinden beklenildiği şekilde çalışmaması işlerimizi önemli ölçüde yavaşlatır	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**
13. Firmamız, mail aracılığıyla gelebilecek olan virüslerin sistemimize girmemesi için önlemler alır.	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**
14. Firmamız, bilgisayarımıza casus yazılım yüklenmesini engellemek için önlem alır.	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**
15. Firmamız, dosya erişimlerine ulaşma hızımız yavaşladığında önlem alır.	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**
16. Firmamızın, mail aracılığıyla zararlı dosyaların sistemimize girmemesi için önlemleri göz ardı eder.	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**
17. Firmamızda evrakların imha işlemi verinin izlenebilirliğini azaltmak için kullanılır.	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**
18. Firmamızda, önemli evrakların değiştirilme ihtimaline karşı önlem alır.	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**
19. Firmamızda, bilgi sistemlerine ‘’üçüncü taraf’’ (dışarıdan) erişim, üst düzey bir yöneticinin onayını gerektirir.	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**
20. Firmamız verilerin kopyalanmasını engeller.	**1)**	**2)**	**3)**	**4)**	**5)**
21. Kimlik hırsızlığına karşı alınması gereken güvenlik tedbirlerini biliyorum.	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**
22. Firmamız, sistemdeki arızanın kaynağını tarihsel kayıtlardan çıkartabilir.	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**

23. Firmamız, dosya ya da önemli bir evrak değiştirildiği zaman, değişiklik yapan kullanıcıyı görebilir.	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**
24. Firmamız, sistemde değişikliklerden dolayı doğabilecek sorunları engellemek için önlemler alır.	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**
25. Firmamız, siber güvenlik açısından olası riskler olabileceğini düşünür ve bunlara karşı önlemler alır.	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**
26. Firmamızda, güvenlik politikalarımızı (süreçlerimizi) ihlal eden çalışanlar için resmi bir disiplin süreci vardır.	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**
27. Firmadaki bilgisayarıma Mp3, video benzeri dosyalar indirebilirim.	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**
28. Firmamız, önemli bilgiler paylaştığımızda karşıdan yazılı onay almamızı ister.(Rapor, Cari mutabakat vs.)	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**
29. Yazılı onayların, ileride doğabilecek hukuksal problemleri engelleyeceğinin farkındayım.	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**
30. Firmamızda, Dijital imzaya önem gösterilir.	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**
31. Firmamız, önemli bir evrak silindiği zaman, işlemi yapan kullanıcıyı kayıtlardan bulamaz.	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**
32. Firmamız, müşterilerimizin rızası olmadan onların bilgilerini başkalarıyla **paylaşmaz**.	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**
33. Firmamızda, müşterilerimizin rızası olmadan onların bilgilerini başka amaçlarla kullanmaz.	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**
34. Firmamız, müşterilerimizin bilgilerini başka kurumlarla paylaşmadan önce ilgili kişiye bilgi verir.	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**
35. Firmamız, müşterilerimizin kişisel bilgilerini olası tehditlere karşı korur.	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**
36. Kişisel bilgi mahremiyetin ne olduğunu biliyorum.	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**

37. Müşterimle olan ilişkilerimde kişisel bilgi mahremiyete göre hareket ederim.	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**