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

GAZİANTEP'TE FAALİYET GÖSTEREN ORTA VE BÜYÜK ÖLÇEKLİ İŞLETMELERİN SİBER GÜVENLİK YÖNETİM YAKLAŞIMLARININ ANALİZİ

DOKTORA TEZİ

HAZIRLAYAN
Ahmet BOZGEYİK

GAZİANTEP – 2018

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

GAZİANTEP'TE FAALİYET GÖSTEREN ORTA VE BÜYÜK ÖLÇEKLİ İŞLETMELERİN SİBER GÜVENLİK YÖNETİM YAKLAŞIMLARININ ANALİZİ

DOKTORA TEZİ

HAZIRLAYAN
Ahmet BOZGEYİK

TEZ DANIŞMANI
Doç. Dr. Mazlum ÇELİK

GAZİANTEP – 2018

KABUL VE ONAY

Ahmet BOZGEYİK tarafından hazırlanan **"Gaziantep'te Faaliyet Gösteren Orta ve Büyük Ölçekli İşletmelerin Siber Güvenlik Yönetim Yaklaşımlarının Analizi"** başlıklı bu çalışma **26/04/2018** tarihinde yapılan savunma sınavı sonucu **başarılı** bulunarak jürimiz tarafından **Doktora Tezi** olarak kabul edilmiştir.

Prof. Dr. İbrahim Sani MERT
(Başkan)

Doç. Dr. Mazlum ÇELİK
(Üye)

Dr. Öğr. Üye. Yakup DURMAZ
(Üye)

Dr. Öğr. Üye. Mehmet AYTEKİN
(Üye)

Dr. Öğr. Üye. İbrahim ÇÜTÇÜ
(Üye)

Onay
Yukarıdaki imzaların, adı geçen öğretim üyelerine ait olduğunu onaylarım. 26.04.2018

Doç. Dr. Mazlum ÇELİK
Enstitü Müdürü

TEZ ETİK VE BİLDİRİM SAYFASI

Doktora Tezi olarak sunduğum **"Gaziantep'te Faaliyet Gösteren Orta ve Büyük Ölçekli İşletmelerin Siber Güvenlik Yönetim Yaklaşımlarının Analizi"** 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. 26.04.2018

Ahmet BOZGEYİK

ÖNSÖZ

"If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology." (Schneier B. , 2011)

"Teknolojinin güvenlik sorunlarınızı çözebileceğini düşünüyorsanız, sorunları ve teknolojiyi bilmiyorsunuzdur"

Günümüzde herkesin bir siber saldırıya maruz kalma potansiyeli bulunmaktadır. Eğer bir saldırıya maruz kalmadıysanız, kendinizi şanslı görebilirsiniz veya bir siber saldırıya maruz kalmış ve bunun farkında olamamışsınızdır. Farkında olmamak işin daha vahim boyutudur. Siber tehditlere maruz kalmamak için alınan önlemler ve herhangi bir saldırı durumunda tahribatların bertaraf edilmesi veya en az zararla atlatılması için alınacak tedbirler büyük önem arz etmektedir. Günümüzde siber güvenliğin temelinde dikkat edilmesi gereken üç temel özellik bulunmaktadır. Bunlar; siber tehditlere karşı farkındalık, faaliyetlerin yürütüleceği güvenli bir ortamın oluşturulması ve saldırılara karşı dirençli olunmasıdır. Bir kurumun yüzde yüz güvenli olması mümkün olmasa da, bu üç temel özelliğe odaklanmak suretiyle siber tehditlerin etkilerini azaltarak, potansiyel iş zararını en aza indirmek mümkün olabilir. Bu kapsamda bu çalışmanın "siber güvenlik farkındalığı" oluşturmak adına işletmelerimize ve bu alanda çalışacak akademisyenlere katkı sağlamasını ümit etmekteyim.

Bu çalışmanın tüm aşamalarında bilgi ve deneyimlerini benden esirgemeyen danışmanım ve değerli hocam Doç. Dr. Mazlum Çelik'e ilgi desteklerinden dolayı çok teşekkür ederim. Bu çalışmanın analiz aşamasında desteklerini esirgemeyen Dr. Mehmet Aytekin ve Dr. Bülent Yıldız'a çok teşekkür ederim. Ayrıca bu yoğun çalışma temposunda sabırla beni destekleyen aileme sonsuz teşekkür ederim.

Gaziantep, 2018

Ahmet BOZGEYİK

ÖZET

Bilgi ve İletişim Teknolojilerinin (BİT), hayatımızın her alanına girdiği bir zamanda yaşamaktayız. BİT hemen hemen herkes tarafından sosyalleşmede, bilgiye erişimde, ticarette üretimde, devlet kurumlarında ve gündelik iş hayatında yaygın olarak kullanılmaktadır. Teknoloji iyi yönetildiği zaman işletmelere büyük fırsatlar sunmaktadır. Fakat kötü yönetildiği zaman bir tehdit unsuruna dönüşmektedir. Teknoloji aynı zamanda kötülere şeytanca fikirlerini uygulama fırsatı verdiği için her türlü bilgi hırsızlığına, casusluğa ve çeşitli siber suçlara da yol açmaktadır. Bu kapsamda teknoloji yönetimi, özelde de siber güvenlik yönetimi işletmeler için hayati bir konudur. Bu çalışmada; genel olarak Gaziantep'teki orta ve büyük ölçekli firmaların genel olarak siber güvenliğe yaklaşımları sevilerini tespiti ve firmaların demografik özelliklerine göre firmaların siber güvenlik yaklaşımlarında farlılıklar olup olmadığının belirlememesi amaçlanmıştır. Bu kapsamda çalışmada anket tekniği kullanılarak 128 firmadan elde edilen verilerin analizi sonucunda, araştırma kapsamındaki firmaların siber güvenlik yaklaşımlarının genel olarak düşük düzeyde olduğu tespit edilmiştir. Araştırma kapsamındaki firmaların siber güvenliğe kurumsal yaklaşım, yazılım geliştirme ve destek aşamalarında bilgi sistemleri erişim kontrolü güvenlik tedbirleri, siber güvenlik ihlalleri ve iş sürekliliği yönetimi ile genel siber güvenlik yaklaşımlarının düşük düzeyde olduğu; fiziksel ve çevresel güvenlik tedbirleri ile bilişim sistemleri ve iletişim ağlarının işletim ve bakım kontrolleri düzeyinin orta düzeyde olduğu tespit edilmiştir. Ayrıca bu çalışmada firmaların özelliklerine göre siber güvenlik yaklaşımlarının farklılıklar gösterdiği tespit edilmiştir. Örneğin; çalışan sayısı ve sermaye yapısı daha büyük olan firmalar, bilişim sistemlerine bağımlılığı daha yüksek olmanın yanında söz konusu firmaların siber güvenliğe kurumsal yaklaşım düzeyleri daha yüksektir.

Anahtar Kelimeler: Siber güvenlik, siber güvenliğe kurumsal yaklaşım.

ABSTRACT

Nowadays Information and Communication Technologies (ICT) widely use in each and every sector. Almost everyone has been using it for educational, business, social connections and every day work purposes. ICT provides benefits for good people as opportunities available for people with evil intentions as well. They steal personal, financial information, use it for espionage, and harm individuals and enterprises. ICT also serve as medium to commit cyber-crime.

Enterprises' most valuable data is stored on virtual environments and if not protected by proper security measures they all open to be abused. This research will focus on medium and large enterprises approach to protect their cyber assets. The paper will also examine cyber security awareness levels of their technology users as well as will look into demographic differences among them. The research will use survey technique conducted on 128 medium and large size enterprises located in Gaziantep Turkey. This study found out that the overall level of cyber security awareness and protection measures in institutional approach to cyber security, software development, access control during support stages, cyber security breach management, business continuity was low, physical security measures, communication and IT networks security and maintenance controls was moderate. Moreover the study found out that firms show differences according to their demographic characteristics. For example; firms with a larger number of employees and capital are more dependent on information systems, while firms also have higher levels of institutional approach to cyber security.

Keywords: Cyber security, institutional approach to cyber security.

İÇİNDEKİLER

Sayfa No.

DÖRDÜNCÜ BÖLÜM

BEŞİNCİ BÖLÜM

TABLOLAR LİSTESİ

Sayfa No.

ŞEKİLLER LİSTESİ

Sayfa No.

KISALTMALAR

AB : Avrupa Birliği

ABD : Amerika Birleşik Devletleri

MAC : Fiziksel Adres, Donanım Adresi

IP : İnternet Protokolü Adresi

ITU : Uluslararası Telekomünikasyon Birliği

BIT : Bilgi ve İletişim Teknolojileri

BT : Bilişim Teknolojileri

LAN : Yerel Ağ

WAN : Geniş Ağ

SPK : Sermaye Piyasası Kurulu

KAP : Kamuyu Aydınlatma Platformu

ISO : Uluslararası Standartlar Teşkilâtı

NIST : ABD Ulusal Teknoloji Standartları Enstitüsü

UDBH : Ulaştırma Denizcilik ve Haberleşme Bakanlığı

USOM : Ulusal Siber Olaylara Müdahale Merkezi

SOME : Siber Olaylara Müdahale Ekibi

WWW : Dünya Çapında Ağ Servisi

DNS : Alan Adı Sistemi

BİRİNCİ BÖLÜM

GİRİŞ

Bu bölümde, araştırmaya ilişkin olarak araştırmanın konusu, problemi, araştırmanın amacı, önemi, sınırlılıklar ve tanımlar yer almaktadır.

1.1. Problem Durumu

Bu yüzyılda bilgi; kişiler, işletmeler, toplumlar ve devletler açısından tek başına bir hak, varlık ve değer haline gelmiştir. Nitelik itibariyle soyut bir varlık olan bilgi, işletmeler için, sair maddi hakların aksine, daha yaygın bir değeri ifade edebilmekte ve bu sebeple daha yaygın ve etkin bir korumaya ihtiyaç duymaktadır.

İşletmelerin bilgi teknolojileri varlığı; bilgi sistemleri, bu sistemler üzerinde yer alan veya bu sistemler üzerinden erişilebilir olan her türlü bilgi ve veriyi ilgilendiren oldukça kapsamlı koruma konularını içermektedir. Bilgi sistemleri, işletmeler için sınırsız fırsatlar içerdiği gibi, sınırsız tehdit ve riskleri de beraberinde getirmektedir. Bu tehdit ve riskler, işletmenin geleneksel varlıklarına yönelen geleneksel tehditlere (çalınma, bozulma, eskime vb.) kıyasla çok daha mücadele edilemez bir nitelik taşımaktadır.

Bilgi güvenliği, işletmelerin stratejik bilgi ve bilgi teknolojileri varlığını ilgilendiren ve güvenlik araçlarını ihtiva eden bir kavramdır. Bilgi güvenliği kavramı yerine günümüzde "siber güvenlik" kavramının da kullanıldığı görülmektedir. Siber güvenlik; işletmelerin bilgi varlığına yönelen her türlü tehdit ve riske karşı alınan tedbirleri ifade eden geniş bir kavramdır. Kavram, birçok araştırmacı tarafından, bilgi güvenliği kavramı ile aynı anlamda kullanılmış ve kullanılma sebebi olarak da oluşacak sonuçların bilgi güvenliğini etkilemesi gösterilmiştir (Solms ve Niekerk, 2013: 98). Halbuki iki kavram birbirine benzese de kapsam itibarıyla birbirinden farklılaşmaktadır. "Bilgi güvenliği", doğrudan bilgi teknolojileri sistemleri üzerindeki bilginin korunmasına odaklanmış iken, "siber güvenlik" kavramında bilgi güvenliğinin ana standardı olan "gizlilik", "bütünlük" ve "erişebilirlik" kavramları**;** bilgiye erişimi sağlayan birbirine bağlı ağlarda *(interconnected networks)*, bilgi ve iletişim araç, sistem ve teknolojilerini de kapsayacak şekilde daha geniş bir şekilde ele alınmaktadır (Whitman ve Mattord, 2009).

BT sistemleri; kurulumu, kullanımı ve yönetimi için çok az bir düzenleyici veya yol gösterici kuralı bulunan bir alan olarak görülmektedir. Yapılan çalışmalarda, bu konunun doğru olarak anlaşılmadığı, gereken önemin verilmediği ve farkındalık düzeyinin yeterli seviyede olmadığı vurgulanmıştır (Vural ve Sağıroğlu, 2008: 507; Barrett, 2003: 57; Kudat, 2007). Bu durum, işletmelerin siber güvenlik kavramı ile tanışmasını geciktirmekte, bu sebeple yönetim araçlarının geliştirmesi ve BT sistemlerini güvenli ve verimli bir şekilde kullanmayı olumsuz etkilemektedir. Kurumlardaki üst yönetimin siber güvenliği önemsemeye başlamış olduğu durumlarda ise genelde bir başka hata yapılarak acele ve günü kurtarıcı çözümlere başvurulduğu ve sadece teknoloji temelli çözümlere odaklanıldığı görülebilmektedir (Richardson, 2008).

Günümüzde siber güvenlik konusu dünya çapında en üst düzeyde ilgi görmüş ve ellinin üzerinde devlet, resmi olarak bu konuda strateji belgeleri yayımlamıştır (Klimburg, 2012: 23). Beyaz Saray 2011'de yayımladığı siber güvenlik strateji belgesinde, mücadele için diğer ülkelerle iş birliğine vurgu yapmıştır. Ülkelerin her geçen gün siber güvenlik kapasitelerini geliştirdikleri günümüzde; toplumun her ferdi gibi kurum/kuruluşlar, ticari işletmeler, sivil toplum kuruluşları hatta devletler siber tehditlerin getirebileceği risklere karşı önlemler almak ve bunları doğru bir şekilde yönetmek zorundadırlar. Aksi takdirde bu tehditlerin oluşturacağı riskler maddi ve manevi birçok kayba neden olmaktadır.

Tsukayama tarafından 2011 yılında yapılan bir çalışmada, Nisan 2011'de Sony PlayStation ve çevrimiçi eğlence hizmetlerine düzenlenen siber saldırılarda; firmanın 102.000.000 müşteri bilgisinin *(isim, adres, kullanıcı adı, şifre ve kredi kartı numaraları)* çalındığı ve bu saldırının yarattığı imaj ve itibar kaybı dışında firmaya doğrudan bir-iki milyon dolar arasında bir maliyet yansıması olduğu bildirilmiştir. Hazırlanan kurumsal raporlarda bu hususa ilişkin öngörüler yer almaktadır. Örneğin, 2014 yılında yapılan McKinsey çalışmasında; 2020 itibarı ile siber saldırılar nedeniyle ortaya çıkabilecek ekonomik kaybın 20.000.000.000 ABD Dolarını bulabileceğini belirtmektedir (Chinn vd., 2014). Siber saldırılarla karşı karşıya kalan firmaları, Sony örneğinde olduğu gibi, genişletmek mümkündür. JPMorgan, Chase, Verizon, Best Buy, Target, Marriott, Hilton, IMF, Sega, Citibank gibi dünya çapında faaliyet gösteren önemli firmalar bu kapsamda sayılabilir. (Aspan, 2011; Goldman, 2011; Wolf ve Maclean, 2011) İngiliz Ticaret ve İnovasyon Bakanlığı'nın PwC'a yaptırdığı "2014 Bilgi Güvenliği İhlalleri" raporunda 2014 yılında yapılan siber saldırı sayısının düşmesine karşın, bir önceki yıl ile karşılaştırıldığında, bu saldırıların verdiği ekonomik zararın neredeyse iki katına çıktığı tespitine yer verilmiştir. Araştırmalarda belirtilen ekonomik kayıpların, sadece gün yüzüne çıkan kısmı olduğu dikkate alındığında siber tehditlere karşı önlem alınmasının önemi

daha da belirginleşecektir.

Günümüzde kurumlar faaliyetlerinin planlanan şekilde sürekliliğini sağlamak, kendilerine ait her türlü bilginin kötü amaçla ele geçirilmesini önlemek için her türlü tedbiri almak zorundadır. Bu tedbirler sadece fiziki güvenliğe veya teknolojik yatırıma dönük çalışmalar değildir. Kurumlar dünyanın en gelişmiş koruma sistemlerine sahip olsa bile güvenlik sistemleri uygun bir biçimde yönetilmediği veya kullanılmadığı zaman her türlü ihlalin yaşanması ve yapılan yatırımların boşa gitmesi söz konusu olabilecektir.

Günümüz rekabetçi ortamında işletmeler; fiziksel işletme güvenlikleri ve personel güvenlikleri (işçi sağlığı vs.) için tedbirler aldıkları gibi daha stratejik bir alan olan siber güvenlik konusunda da tedbir ve mücadele yöntemleri geliştirmeli, kurumsal farkındalıklarını ileri düzeye taşımalıdırlar. Bu çalışmada günümüzün en önemli konularından biri olan siber güvenliğinin işletmeler açısından incelenmesi ve analizi yapılması amaçlanmıştır. Bu kapsamda çalışmanın temel problemi; Gaziantep'te faaliyet gösteren orta ve büyük ölçekli işletmelerin siber güvenlik yönetiminde mevcut durumunun tespiti ve analizidir. Ayrıca çalışmanın diğer bir problemi; işletmelerin özelliklerine göre siber güvenlik yönetimine ilişkin kurumsal yaklaşım düzeylerinin analiz edilmesidir.

1.1.1. Problem Cümlesi

Bu çalışmanın temel problemi cümlesini; "Gaziantep'te faaliyet gösteren orta ve büyük ölçekli işletmelerin siber güvenlik yönetiminde kurumsal yaklaşım düzeyleri nedir?" ve "İşletmelerin siber güvenlik yönetimine kurumsal yaklaşım düzeyleri işletmenin özelliklerine göre farklılaşmakta mıdır?" soruları oluşturmaktadır.

1.1.2. Alt Problemler

Bu çalışmada genel olarak; Gaziantep'te faaliyet gösteren orta ve büyük ölçekli işletmelerin siber güvenlik yönetiminde mevcut durumunun ne olduğu sorusuna cevap aranmaktadır. Bu kapsamda çalışmanın amacına uygun olarak araştırmada aşağıdaki belirtilen alt problemlere cevap aranmaktadır:

1. Gaziantep'te faaliyet gösteren işletmelerin siber güvenlik yönetimine ilişkin mevcut durumları nasıldır?
2. Gaziantep'te faaliyet gösteren işletmelerin özelliklerine göre siber güvenlik yönetimi açısından fark var mıdır?

a. İşletmelerin özelliklerine göre siber güvenlik yönetiminde, kurumsal yaklaşım düzeyleri açısından fark var mıdır?

b. İşletmelerin özelliklerine göre siber güvenlik yönetiminde, fiziksel ve çevresel güvenlik tedbirleri açısından fark var mıdır?

c. İşletmelerin özelliklerine göre siber güvenlik yönetiminde, bilişim sistemleri ve iletişim ağlarının işletim ve bakım kontrolleri açısından fark var mıdır?

d. İşletmelerin özelliklerine göre siber güvenlik yönetiminde, yazılım geliştirme ve destek aşamalarında, bilgi sistemleri erişim kontrolü ve güvenlik tedbirleri açısından fark var mıdır?

e. İşletmelerin özelliklerine göre siber güvenlik ihlalleri ve iş sürekliliği yönetimleri açısından fark var mıdır?

3. Gaziantep'te faaliyet gösteren işletmelerin teknolojik ve internete bağımlılık düzeylerinin, siber güvenlik yönetimine etkisi var mıdır?

4. Gaziantep'te faaliyet gösteren işletmelerin siber güvenlik tehditleri ile karşı karşıya kalma durumları siber güvenlik yönetimi ne etki etmekte midir?

a. Gaziantep'te faaliyet gösteren işletmelerin siber güvenlik tehditleri ile karşı karşıya kalma durumlarına göre siber güvenlik yönetim düzeyleri farklı mıdır?

b. Gaziantep'te faaliyet gösteren işletmelerin siber güvenlik tehditlerine ile karşı karşıya kalma durumları işletme özelliklerine göre farklı mıdır?

c. Gaziantep'te faaliyet gösteren işletmelerin siber güvenlik tehditlerinin türleri işletme özelliklerine göre farklı mıdır?

1.2. Araştırmanın Amacı

Yapılan çalışmalar, siber güvenlik konusunun yöneticiler tarafından doğru olarak anlaşılmadığı, gereken önemin verilmediği ve farkındalık düzeyinin yeterli seviyede olmadığı vurgulamaktadır. Bu durum, işletmelerin kurumsal siber güvenlik yönetimi kavramı ile tanışmasını geciktirmekte, yönetim araçlarının geliştirilmesi ve teknolojinin güvenli ve verimli bir şekilde kullanılmasını olumsuz etkilemektedir. Günümüz şartlarında işletmelerin güncel ve gelişen teknolojileri kullanmadan müşteri ve iş ortakları ile iş yapmaları imkânsız görülmektedir. Bu yüzden siber güvenliğin iyi ve yönetimi elzemdir, İşletmeler bir yandan değişen çevre ve şartlara uyum sağlamaya çalışarak pazar payları ve verimliliklerini artırmaya çalışırken, diğer yandan bu değişimin getirebileceği sorunların belirlemek, dikkate almak ve bu sorunlara zamanında çözümler üretmek zorundadır.

Siber güvenlik yönetimi konusu özellikle son yıllarda birçok araştırmacının ilgisini çekmiş ve araştırmalara konu olmaya başlamıştır. Yapılan çalışmaların büyük bir kısmı mühendislik bilimlerinde ve güvenliğin teknik boyutunu incelediği gözlemlenmiş olup, konunun insan odaklı yönetim kısmına yeterli önem verilmemiştir. Bazı çalışmalarda siber güvenliğin organizasyonlar üzerine etkileri, farklı boyutlarda incelemiş ve başlı başına yönetilmesi gereken bir konu olduğu vurgulanmıştır. Türkiye'de siber güvenlik yönetimine ilişkin maalesef kapsamlı bir çalışmaya rastlanılmamıştır.

Bu çalışmanın temel amacı; Gaziantep'te faaliyet gösteren orta ve büyük ölçekli işletmelerin siber güvenlik yönetimine ilişkin kurumsal yaklaşım düzeylerinin belirlenmesi ve işletmelerin demografik özelliklerine göre farklılıkların analiz edilmesidir. Ayrıca literatüre katkı sağlamak bu çalışmanın diğer bir amacıdır.

1.3. Araştırmanın Önemi

Gelişen teknolojiler sunduğu eşsiz fırsatların yanında öngörülemeyen, karmaşık, telafisi mümkün olmayan zararlara neden olan siber tehditleri de beraberinde getirmektedir. Bu tehdit ve riskler, işletmenin varlıklarına yönelen geleneksel tehditlere (çalınma, bozulma, eskime vb.) kıyasla çok daha mücadele edilemez bir nitelik taşımaktadır. Ayrıca yapılan araştırmalar, siber tehditlerin her geçen gün daha da arttığını ve siber tehditlere bağlı olarak kuruluşların karşı karşıya kaldıkları kayıpların da arttığını göstermektedir. Dolayısıyla kurumlar bu tehdit ve risklere karşı gereken tedbirleri almak zorundadırlar.

Bu çalışmada genel olarak Gaziantep'te faaliyet gösteren işletmelerin siber güvenlik yönetimine ilişkin mevcut durumları analiz edilmektedir. Dolayısıyla bu çalışma kurumların siber güvenlik yönetimine ilişkin sorunlarını tespit etme ve bu sorunlara uygulamaya yönelik çözümler geliştirebilmek açısından büyük önem arz etmektedir. Ayrıca bu çalışma ilgili literatüre katkı sağlaması açısından da önemlidir.

1.4. Araştırmanın Hipotezleri

Bu çalışmada genel olarak; Gaziantep'te faaliyet gösteren orta ve büyük ölçekli işletmelerin siber güvenlik yönetiminde mevcut durumunun analizine yöneliktir. Dolayısıyla çalışmada test edilecek hipotezlerde bu kapsamdadır. Çalışmanın hipotezleri aşağıda sırasıyla verilmiştir.

H1: Gaziantep imalat sanayiinde faaliyet gösteren firmaların siber güvenlik yaklaşım

seviyesi düşüktür.

H2: Siber güvenlik yaklaşımları firmaların çalışan sayısına göre anlamlı farklılık göstermektedir.

H2a: Siber güvenliğe kurumsal yaklaşım firmaların çalışan sayısına göre anlamlı farklılık göstermektedir.

H2b: Fiziksel ve çevresel güvenlik tedbirleri firmaların çalışan sayısına göre anlamlı farklılık göstermektedir.

H2c: Bilişim sistemleri ve iletişim ağlarının işletim ve bakım kontrolleri firmaların çalışan sayısına göre anlamlı farklılık göstermektedir.

H2d: Yazılım geliştirme ve destek aşamalarında bilgi sistemleri erişim kontrolü güvenlik tedbirleri firmaların çalışan sayısına göre anlamlı farklılık göstermektedir.

H2e: Siber güvenlik ihlalleri ve iş sürekliliği yönetimi firmaların çalışan sayısına göre anlamlı farklılık göstermektedir.

H3: Siber güvenlik yaklaşımları firmaların yıllık cirosuna göre anlamlı farklılık göstermektedir.

H3a: Siber güvenliğe kurumsal yaklaşım firmaların yıllık cirosuna göre anlamlı farklılık göstermektedir.

H3b: Fiziksel ve çevresel güvenlik tedbirleri firmaların yıllık cirosuna göre anlamlı farklılık göstermektedir.

H3c: Bilişim sistemleri ve iletişim ağlarının işletim ve bakım kontrolleri firmaların yıllık cirosuna göre anlamlı farklılık göstermektedir.

H3d: Yazılım geliştirme ve destek aşamalarında bilgi sistemleri erişim kontrolü güvenlik tedbirleri firmaların yıllık cirosuna göre anlamlı farklılık göstermektedir

H3e: Siber güvenlik ihlalleri ve iş sürekliliği yönetimi firmaların yıllık cirosuna göre anlamlı farklılık göstermektedir.

H4: Siber güvenlik yaklaşımları firmaların ticari faaliyetlerde internete bağımlılık oranına göre anlamlı farklılık göstermektedir.

H4a: Siber güvenliğe kurumsal yaklaşım firmaların ticari faaliyetlerde internete bağımlılık oranına göre anlamlı farklılık göstermektedir.

H4b: Fiziksel ve çevresel güvenlik tedbirleri firmaların ticari faaliyetlerde internete bağımlılık oranına göre anlamlı farklılık göstermektedir.

H4c: Bilişim sistemleri ve iletişim ağlarının işletim ve bakım kontrolleri firmaların ticari faaliyetlerde internete bağımlılık oranına göre anlamlı farklılık göstermektedir.

H4d: Yazılım geliştirme ve destek aşamalarında bilgi sistemleri erişim kontrolü güvenlik tedbirleri firmaların ticari faaliyetlerde internete bağımlılık oranına göre anlamlı farklılık göstermektedir.

H4e: Siber güvenlik ihlalleri ve iş sürekliliği yönetimi firmaların ticari faaliyetlerde internete bağımlılık oranına göre anlamlı farklılık göstermektedir.

H5: Siber güvenlik yaklaşımları firmaların bilişim sistemlerinin 24 saat hizmet vermemesinin bir günlük satış/üretim oranlarını etkileme düzeyine göre anlamlı farklılık göstermektedir.

H5a: Siber güvenliğe kurumsal yaklaşım firmaların bilişim sistemlerinin 24 saat hizmet vermemesinin bir günlük satış / üretim oranlarını etkileme düzeyine göre anlamlı farklılık göstermektedir.

H5b: Fiziksel ve çevresel güvenlik tedbirleri firmaların bilişim sistemlerinin 24 saat hizmet vermemesinin bir günlük satış / üretim oranlarını etkileme düzeyine göre anlamlı farklılık göstermektedir.

H5c: Bilişim sistemleri ve iletişim ağlarının işletim ve bakım kontrolleri firmaların bilişim sistemlerinin 24 saat hizmet vermemesinin bir günlük satış / üretim oranlarını etkileme düzeyine göre anlamlı farklılık göstermektedir.

H5d: Yazılım geliştirme ve destek aşamalarında bilgi sistemleri erişim kontrolü güvenlik tedbirleri firmaların bilişim sistemlerinin 24 saat hizmet vermemesinin bir günlük satış / üretim oranlarını etkileme düzeyine göre anlamlı farklılık göstermektedir.

H5e: Siber güvenlik ihlalleri ve iş sürekliliği firmaların bilişim sistemlerinin 24 saat hizmet vermemesinin bir günlük satış / üretim oranlarını etkileme düzeyine göre anlamlı farklılık göstermektedir.

H6: Siber güvenlik yaklaşımları siber saldırıların firma imajı üzerindeki olası etkilerine göre anlamlı farklılık göstermektedir.

H6a: Siber güvenliğe kurumsal yaklaşım siber saldırıların firma imajı üzerindeki olası

etkilerine göre anlamlı farklılık göstermektedir.

H6b: Fiziksel ve çevresel güvenlik tedbirleri siber saldırıların firma imajı üzerindeki olası etkilerine göre anlamlı farklılık göstermektedir.

H6c: Bilişim sistemleri ve iletişim ağlarının işletim ve bakım kontrolleri firmaların siber saldırıların firma imajı üzerindeki olası etkilerine göre anlamlı farklılık göstermektedir.

H6d: Yazılım geliştirme ve destek aşamalarında bilgi sistemleri erişim kontrolü güvenlik tedbirleri siber saldırıların firma imajı üzerindeki olası etkilerine göre anlamlı farklılık göstermektedir.

H6e: Siber güvenlik ihlalleri ve iş sürekliliği siber saldırıların firma imajı üzerindeki olası etkilerine göre anlamlı farklılık göstermektedir.

H7: Siber güvenlik yaklaşımları firmaların elindeki kritik bilgilerin oranına göre anlamlı farklılık göstermektedir.

H7a: Siber güvenliğe kurumsal yaklaşım firmaların elindeki kritik bilgilerin oranına göre anlamlı farklılık göstermektedir.

H7b: Fiziksel ve çevresel güvenlik tedbirleri firmaların elindeki kritik bilgilerin oranına göre anlamlı farklılık göstermektedir.

H7c: Bilişim sistemleri ve iletişim ağlarının işletim ve bakım kontrolleri firmaların elindeki kritik bilgilerin oranına göre anlamlı farklılık göstermektedir.

H7d: Yazılım geliştirme ve destek aşamalarında bilgi sistemleri erişim kontrolü güvenlik tedbirleri firmaların elindeki kritik bilgilerin oranına göre anlamlı farklılık göstermektedir.

H7e: Siber güvenlik ihlalleri ve iş sürekliliği firmaların elindeki kritik bilgilerin oranına göre anlamlı farklılık göstermektedir.

H8: Siber saldırıya uğrayan firmaların siber güvenlik yaklaşım seviyesi daha yüksektir.

H8a: Siber saldırıya maruz olma durumuna göre firmaların siber güvenliğe kurumsal yaklaşım düzeyleri anlamlı farklılık göstermektedir.

H8b: Siber saldırıya maruz olma durumuna göre firmaların fiziksel ve çevresel güvenlik tedbirleri anlamlı farklılık göstermektedir.

H8c: Siber saldırıya maruz olma durumuna göre firmaların bilişim sistemleri ve iletişim ağlarının işletim ve bakım kontrolleri anlamlı farklılık göstermektedir.

H8d: Siber saldırıya maruz olma durumuna göre firmaların yazılım geliştirme ve destek aşamalarında bilgi sistemleri erişim kontrolü güvenlik tedbirleri anlamlı farklılık göstermektedir.

H8e: Siber saldırıya maruz olma durumuna göre firmaların siber güvenlik ihlalleri ve iş sürekliliği anlamlı farklılık göstermektedir.

H9: Siber güvenlik yaklaşımları firmaların personel değişim oranına göre anlamlı farklılık göstermektedir.

H9a: Siber güvenliğe kurumsal yaklaşım firmaların personel değişim oranına göre anlamlı farklılık göstermektedir.

H9b: Fiziksel ve çevresel güvenlik tedbirleri firmaların personel değişim oranına göre anlamlı farklılık göstermektedir.

H9c: Bilişim sistemleri ve iletişim ağlarının işletim ve bakım kontrolleri firmaların personel değişim oranına göre anlamlı farklılık göstermektedir.

H9d: Yazılım geliştirme ve destek aşamalarında bilgi sistemleri erişim kontrolü güvenlik tedbirleri firmaların personel değişim oranına göre anlamlı farklılık göstermektedir.

H9e: Siber güvenlik ihlalleri ve iş sürekliliği firmaların personel değişim oranına göre anlamlı farklılık göstermektedir.

1.5. Araştırmanın Varsayımları

Bu çalışma Gaziantep'te faaliyet gösteren orta ve büyük ölçekteki işletmeler üzerinde yapılmakta olup araştırma kapsamında elde edilen verilerin doğruluğunun ön kabulü çalışmanın temel bir varsayımıdır.

Bu çalışmanın diğer bir varsayımı çalışmada elde edilen verilerin Gaziantep'teki orta ve büyük ölçekli imalat işletmelerin genel durumunu yansıttığıdır. Dolayısıyla yapılan sonuç ve öneriler, örneklemin ana kütleyi temsil ettiği varsayımına dayanmaktadır.

1.6. Araştırmanın Sınırlılıkları

Bu araştırmanın kapsamı, konusu ile sınırlıdır. Bu çalışmada, siber güvenlikle ilişkili olmayan diğer güvenlik sorunları araştırma kapsamı dışındadır.

Bu çalışma araştırma süresi ile sınırlı olacağından çalışmada elde edilecek bulgular çalışma süresi ile sınırlıdır. Bundan sonra yapılacak çalışmalar ile önceki çalışmalar arasında farklılıklar olabilecektir. Bu durum çalışmanın bir diğer sınırlılığıdır.

Ayrıca yapılan analiz ve öneriler araştırma konusu kapsamında elde edilen veriler ile sınırlıdır. Bu çalışma Gaziantep'teki orta ve büyük ölçekli imalat işletmelerini kapsamaktadır. Dolayısıyla çalışma bu işletmeler sınırlıdır. Çalışmanın hizmet sektöründe veya farklı ana kütleler üzerinde yapılması durumunda farklı sonuçlar elde edilebilir.

1.7. Tanımlar

Bu çalışmada araştırma konusuyla ilgili temel kavramlar aşağıda kısaca açıklanmıştır.

Bilgi ve İletişim Teknolojileri (BİT): BİT, bir organizasyon için gerekli bilgi ve iletişim hizmetlerini sunan, altı bileşenden oluşan (insan, veri, iş süreçleri, yazılım, donanım, bilişim ağları) sosyo-teknik bir sistemdir. (Cherdantseva ve Hilton, 2013: 548)

Bilgi Güvenliği: Bilgi güvenliği; bilgiye sürekli olarak –izinler çerçevesinde– erişilebilirliğin sağlandığı bir ortamda, "bilginin göndericisinden alıcısına kadar gizlilik içerisinde, bozulmadan, değişikliğe uğramadan ve başkaları tarafından ele geçirilmeden bütünlüğünün sağlanması ve güvenli bir şekilde iletilmesi sürecidir." (Canbek ve Sağıroğlu, 2006: 165). Bilgi güvenliği denildiğinde; bilginin gizliliğinin sağlanması ve izinsiz kişilerin erişiminin engellenmesi, bütünlüğünün korunarak olası tehditlerin bu bütünlüğe zarar vermesinin önüne geçilmesi ve bilgiye erişimin garanti altına alınarak, yetkiler dâhilinde, erişilebilir olması anlaşılmalıdır.

Siber Güvenlik: Bilgi güvenliği ve siber güvenlik kavramları birçok çalışmada birbirinin yerine kullanılsa da siber güvenlik bilgi güvenliğine kıyasla klasik bilgi kaynaklarının korunmasının ötesinde birçok varlığın (bilgi, donanım, yazılım, bina, baraj, kurum, şirket, devlet hatta insan) güvenliğini sağlamayı ifade etmektedir (Solms ve Niekerk, 2013: 99).

Siber Tehdit: Tehdit; bir kurumun veya sistemin zarar görmesi ile sonuçlanabilecek istenmeyen bir olayın potansiyel nedenidir (T.C Ulaştırma Bakanlığı, 2016). Siber Tehdit**;** siber uzayda varlık bulan herhangi bir fiziksel veya sanal varlığın gizlilik, bütünlük veya erişebilirliğini olumsuz yönde etkileyecek eylemler bütünüdür. Siber tehdit, bazen bilgisayarlarda bulunan bir verinin istenmeyen ellere geçmesi, bazı hallerde ise bir şirketin müşterilerine sunduğu hizmetin geçici veya tamamen engellenmesi, çalınması, bozulması, ifşa edilmesi veya yok edilmesi şeklinde gerçekleşebilir.

Siber Güvenlik Standartları: Bilgi sistemleri yönetimi alanındaki standart ve kılavuzlar, bilgi/siber güvenlik standartları ve bilişim sistemleri yönetişim standartları olmak üzere iki kategoride incelenebilir (Arora, 2016). Bilgi/Siber Güvenlik standartlarına; ISO 27000 serisi standartlar, NIST 800 serisi standartlar, SOX, ISF, SOGP ve Risk IT örnek verilebilir. Bilişim Sistemleri Yönetişim standartlarına; COBIT, COSO ve ITIL örnek verilebilir.

İKİNCİ BÖLÜM

KAVRAMSAL ÇERÇEVE

2.1. Bilgi ve İletişim Teknolojileri (BİT)

Bilgi ve İletişim Teknolojileri (BİT); bilgiye telekomünikasyon aracılığı ile erişimi sağlayan teknolojidir. Bu teknoloji, her türlü, veri erişimi, iletimi ve depolanmasını sağlayan donanım, yazılım ve hizmetleri bir çatı olarak bünyesinde barındırmaktadır.

BİT'in stratejik bir varlık olan bilginin oluşturulması, depolanması, başka noktalara iletilmesi, üzerinde işlemler yapılarak anlamlı hale getirilmesi, yönetilmesi, değiştirilmesi ve yok edilmesi işlemlerinde rolü olan sayısal tabanlı herhangi bir cihaz, bu cihazların üzerinde çalışan yazılım, yöntem ve hizmetlerin bütünü olarak tanımlanması mümkündür.

Başka bir deyişle BİT, bir organizasyon için gerekli bilgi ve iletişim hizmetlerini sunan, altı bileşenden oluşan (insan, veri, iş süreçleri, yazılım, donanım, bilişim ağları) sosyo-teknik bir sistemdir. (Cherdantseva ve Hilton, 2013: 548)

BİT'in sağladığı fırsat ve kolaylıklardan faydalanmak için işletmeler faaliyetlerinde BİT'i kullanmakta ve daha iyi rekabet edebilmek, daha ucuza üretebilmek ve pazar paylarını artırmak gibi birçok nedenlerden dolayıda BİT'lerine yatırım yapmaktadırlar. BİT, sunduğu fırsatlar kadar tehditleri de beraberinde getirmiş, birçok işletme kötü niyetlilerin hedefi haline gelmiş, ticari sırları ifşa edilmiş, imaj kaybına uğramış, çeşitli kayıp ve zararlara maruz kalmıştır. Bu yüzden BİT'in iyi yönetilmesi işletmeler için çok önemlidir.

2.1.1. Siber Güvenlik Bağlamında BİT'in Tarihçesi

Sanayi devrimi birçok alanda olduğu gibi BİT'in gelişmesinin temelini oluşturan birçok icat ve buluşa neden olmuştur. Bu icatların BİT'ni etkilemesi açısından en önemlisi elektriğin kullanılmaya başlanmasıdır. Çünkü sayısal sinyallerin taşınması, ses ve görüntünün taşındığı teknolojilerin gelişmesi bu sayede mümkün olmuştur. Böylece insanların iş yapma yöntem ve iş süreçleri için kullandığı araçları farklı noktalara taşımıştır. (Güngör, 2015)

Elektrik ve elektromekanik kullanılarak iletişim kurma çalışmalarında 1837'den 1903'e kadar birçok gelişme olmuştur. Bu süreçte iletişim alanında icatlar birbirini takip etmiş, iletişimde kullanılan teknolojiler ve sunum şekilleri hızla değişmiştir. Birçok bilim insanı BİT'in

tarihçesini farklı olaylara bağlasa da genel kanı, telgrafın 1837'de icadına dayandırmaktadır. (Cridland, 2008)

İletişim açısından köşe taşı sayılabilecek bir diğer gelişme ise telgraf için okyanus aşırı kabloların çekilmesidir. Bu gelişme iletişimi hızlandırarak çok uzak mesafelerin yakınlaşmasını sağlamıştır. (Cridland, 2008)

BİT için dönüm noktası kabul edilen bir başka husus ise, "Enigma Şifreleme Sistemi"nin Polonyalı kriptoloji uzmanları ve matematikçiler Marian Rejewski, Henryk Zygalski ve Jerzy Różycki tarafından ikinci dünya savaşının ilk yıllarında kırılmasıdır. Bu gelişme, birçok yazar tarafından Almanların ikinci dünya savaşını kaybetme nedeni olarak kabul edilmektedir (Güngör, 2015).

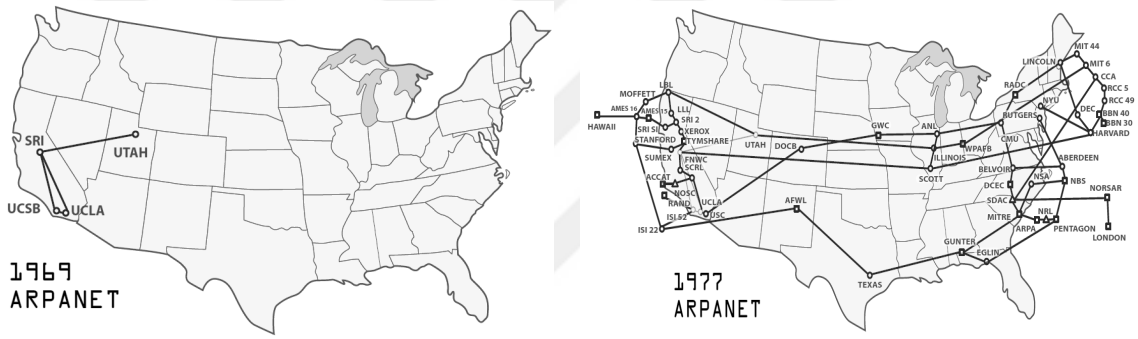
Sovyetler Birliği'nin 4 Ekim 1957'de "Sputnik 1" adlı uyduyu aya fırlatması ile bir dönüm noktası daha yaşanmıştır. ABD tarafından, nükleer saldırı durumunda bile askeri iletişimin sürdürülmesini amaçlayan ARPANET projesi geliştirilmeye başlanmış ve günümüz internetinin altyapısını oluşturacak çalışma 1968 yılının ortalarında internetin başlangıç aşaması olarak çalışmaya başlamıştır.

1967 yaz aylarında Amerikan Savunma Bakanlığı'nda bulunan bazı bilgisayarlarda güvenlik problemleri ile karşılaşılmış ve Ekim 1967'de "Amerikan Savunma İleri Araştırma Projeleri Ajansı (Defense Advanced Research Projects Agency)" tarafından bilgisayar sistemlerinin güvenlik problemlerini araştıracak bir çalışma grubu kurulmuştur. Bu grup tarafından hazırlanan raporda; bilgisayar sistemleri aracılığı ile bilgi paylaşımının çok kullanıcılı ortamlarda sorunlar doğurduğuna ve donanım, yazılım geliştiricilerin güvenlik için farklı bir katman oluşturmaları gerektiğine dikkat çekilmiştir (Ware, 1979). "RAND Report R-609-1" olarak adlandırılan bu rapor siber güvenlik alanında kaleme alınmış ilk rapor olarak tarihe geçmiştir. Tarihe geçmiş bu ilk bilgi güvenliği raporundan günümüze bu alanda sayılamayacak kadar gelişmeler olmuş, raporlar, analizler çeşitlenerek artmıştır. Günümüzde devletler, kurumlar, kuruluşlar, ilgili dernekler ve ticari firmalar tarafından hazırlanmış birçok rapor bulunduğu bilinmektedir.

1970'lerde BİT'in bu denli hayatımıza entegre olabileceğini düşünülmezken; Popular Science dergisinin mayıs 1970 sayısında NASA başkan yardımcısı Dr. Wernher Von Braun'un kaleme aldığı makalede; ünlü İngiliz yazarı ve eş zamanlı iletişim sağlayan uyduların mucidi sayılan Sir Artur C. Clark'tan naklen; eş zamanlı iletişim sağlayan uydular sayesinde birkaç tuşa basarak, birden fazla kişi ile konferans yapabilmeyi, görüntülü görüşmeyi hatta istediğiniz derse

uzaktan katılım sağlamayı gelecekte olabilecek şeyler arasında sayılmıştır. O zaman dile getirilen bu varsayımların günümüzde fazlasıyla gerçekleştiği görülmektedir (Popular Sience, 1970: 66). Günümüzde bu imkânlar dolaylı bir şekilde de olsa Clark'ın bahsettiği uydular sayesinde sağlanmakta, ancak temel iletişim platformu olarak internet kullanılmaktadır.

İnternetin temeli olarak kabul edilen ARPANET ilk kurulduğunda üç noktayı birbirine bağlamak için kullanılmış ve 1969'dan 1977'ye kadar hızla büyüyerek ABD'nin birçok noktasını kapsar hale gelmiştir. 1973'e gelindiğinde, Norveç'te Kraliyet Radar Üssü ve İngiltere'de Londra Üniversitesi'nin ağa dâhil olması ile birlikte ağ küresel bir nitelik kazanmıştır. 1974'de ARPANET'in ticari şekli olan Telnet oluşturulmuş, fakat 90'lı yıllara kadar devletlerin tekelinde kalmıştır (Cropf, 2008: 372).



Şekil 1. 1969 ve 1977 Yıllarında ARPANET
Kaynak: National Science Foundation, 1995.

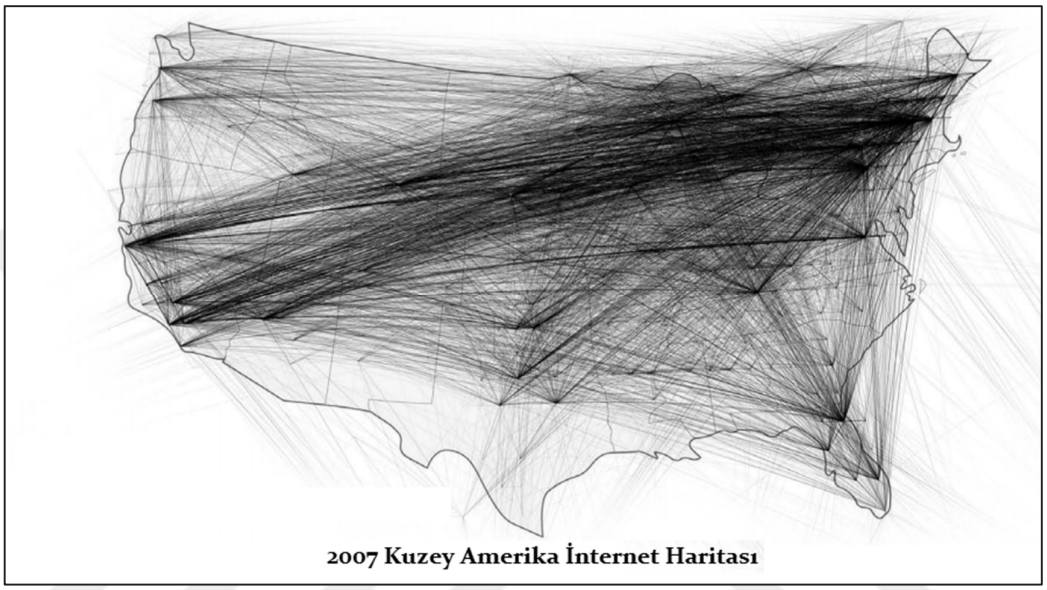
1982 yılında ilk defa "internet" kelimesi kullanılmış, yine 80'li yıllarda pahalı olmayan kişisel bilgisayarlar piyasaya çıkmaya başlamış, alan adı sistemi (DNS) 1983 yılında kullanılmaya başlanmıştır.

1988-1990 yıllarında birçok kesim tarafından kullanılmakta olan internet hakkında insanların güvenlik endişeleri baş göstermeye başlamış, 1989'da Robert Morris tarafından yazılan "solucan" (worm) 6000 civarında internet terminalinin bağlantısını geçici olarak durdurmuş ve siber güvenlik tarihindeki yerini almıştır (Cropf, 2008: 373).

1990'lara kadar daha çok devlet tekelinde askeri amaçlar için kullanılan ve geliştirilen internet, bu tarihle birlikte sivillerin kullanım ve katkılarına açılmıştır. Yine 90'lı yıllarda Avrupa Nükleer Araştırma Merkezinde (CERN) çalışma yapan bir grup bilim insanı tarafından geliştirilen ve küresel genişlikteki ağ anlamına gelen "World Wide Web" (WWW) ile internet

kullanımı her birey, kurum, işletme, hatta devlet için kaçınılmaz bir bağımlılık olmaya başlamıştır.

2007 yılında Amerikan Bilim Derneği'nin yayınladığı "Amerika'daki İnternet Haritası" aradan geçen 30 yılda ne kadar büyük değişiklerin olduğunu gözler önüne sermektedir.

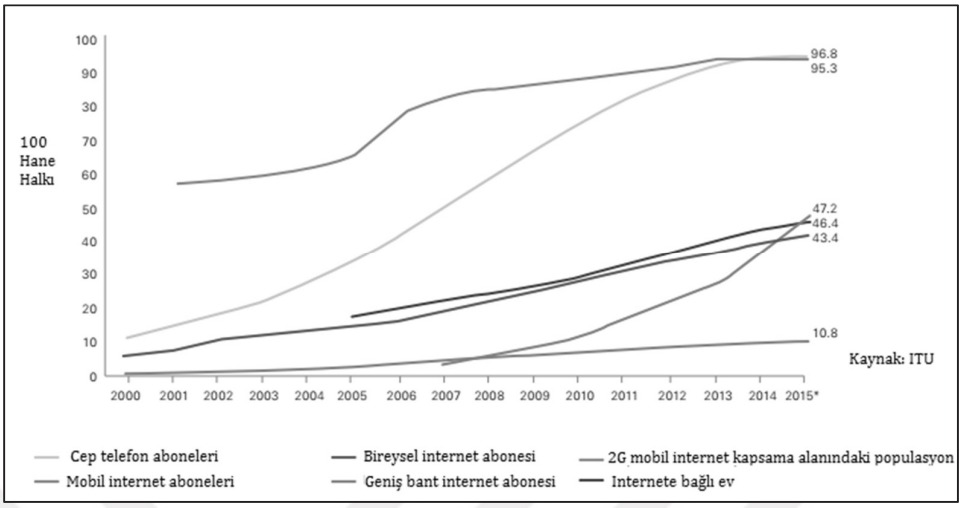


Şekil 2. 2007 Kuzey Amerika İnternet Haritası

Kaynak: National Science Foundation, 2007.

Birleşmiş Milletler, Uluslararası Telekomünikasyon Birliği 2015 verilerine göre (ITU, 2015: 2);

- 2015 itibari ile dünyada 3.200.000.000 kişi internet kullanmakta, bu sayının 2 milyarı gelişmekte olan ülkelerden.
- 2000 yılında internete bağlı olan mobil cihazların sayısı 738.000.000 iken bu sayı 2015'de 7.000.000.000 cihaza ulaşmıştır.
- 2000-2015 yılları arası dünya geneli internete bağlantı oranı %6,5 den %43 e yükselmiştir.

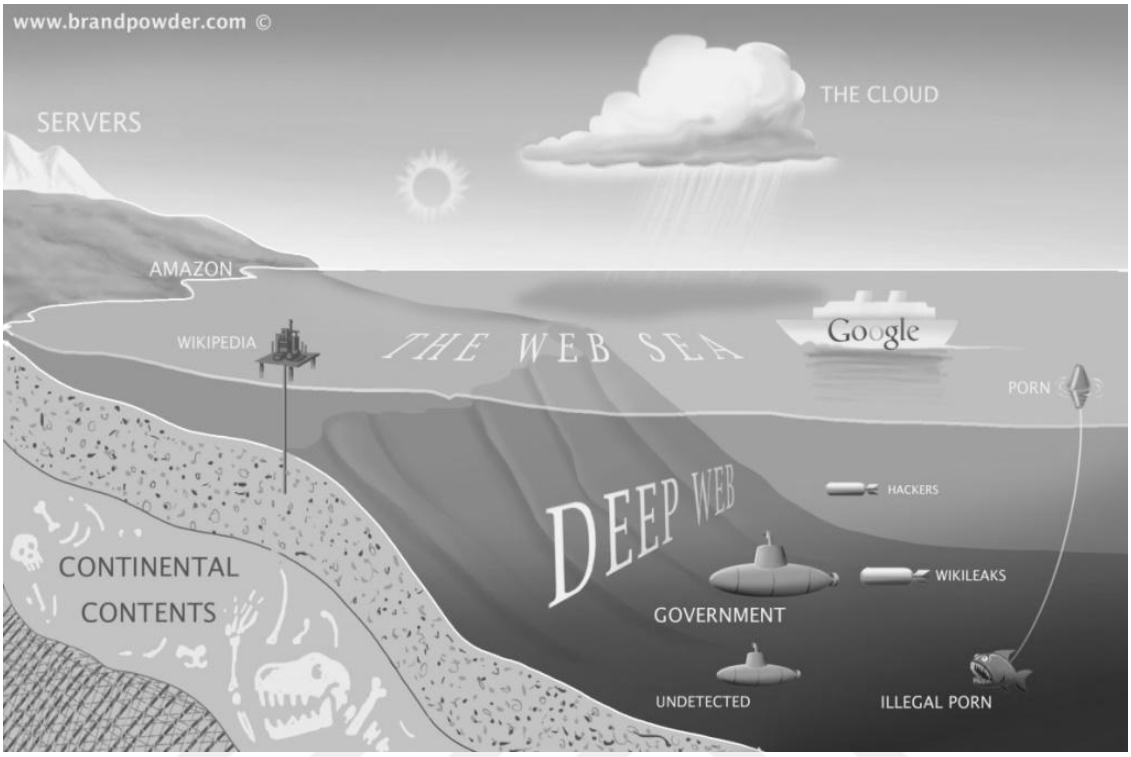


Şekil 3. 2015 - İnternet'e Bağlı Nüfus Oranları

Kaynak: ITU, 2015: 2.

İnternet; insanların kullanımına açıldıktan yirmi-yirmi beş yıllık bir zaman içerisinde tüm dünyayı kuşatarak, sunduğu fırsatlar ve kolaylıklar sayesinde, bireyler ve işletmeler tarafından benimsenmiş ve yoğun bir biçimde kullanılmaktadır.

Herkes tarafından bilinen ve günlük ve iş hayatında kullanılan internete ek olarak; suçluların ve bilgisayar korsanlarının kullandığı "Derin İnternet" veya "Karanlık İnternet" adı ile bilinen internetin geniş kitleler tarafından duyulması "Korkunç Korsan Roberts" olarak da bilinen Ross William Ulbricht'in ekim 2013'de tutuklanması ile olmuştur (Konrad, 2013).



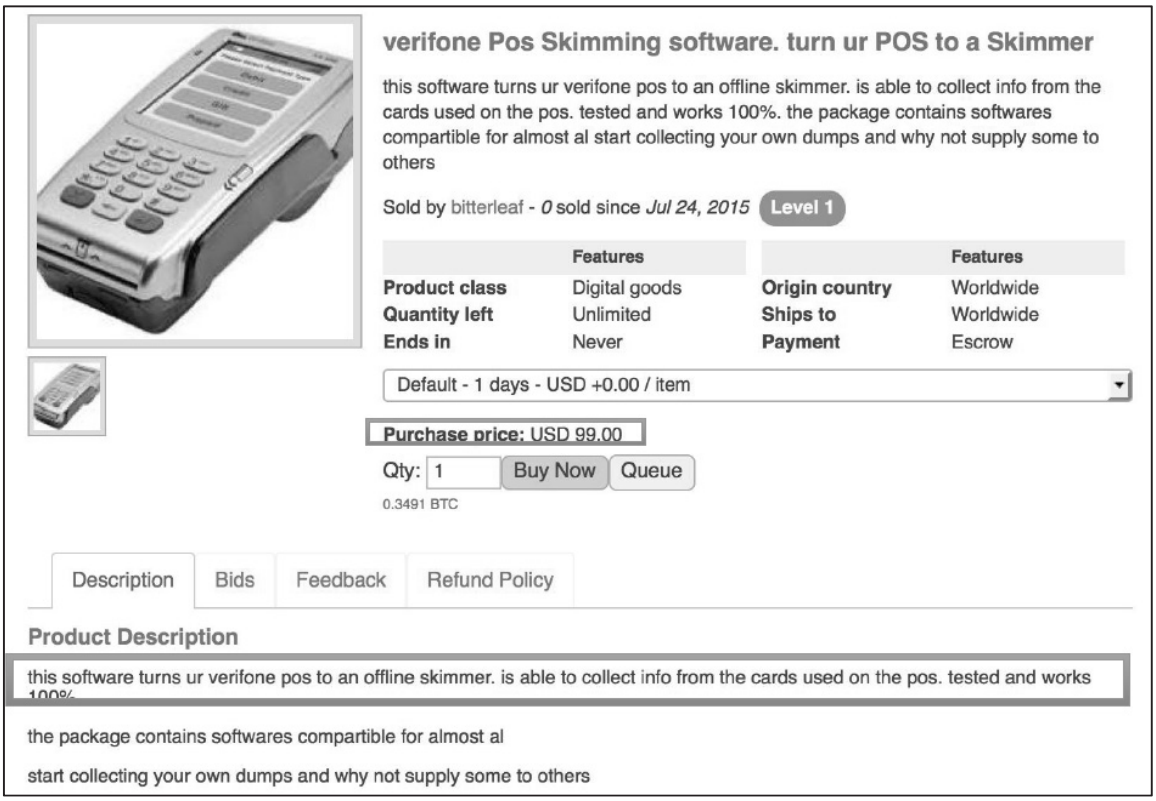
Şekil 4. Karanlık/Derin İnternet
Kaynak: Brandpowder, 2016.

Derin internet, bilinen internetten çok önemli birkaç noktada ayrışmaktadır. Bunlardan en önemlileri (Borland, 2013);

- Derin internette iki tarafta birbirini bilemez, web sitesi sahibi ziyaretçi kimliğini bilmez, ziyaretçi web sitesi sahibini bilmez, hâlbuki bilinen internette ziyaretçi ve web sitesi sahibi birbirini tanıyabilir (Dingledine vd., 2004: 21).
- Derin web sitelerine bilinen uygulamalarla *(Chrome, Internet Explorer vs.)* erişilemez, kendi uygulaması ve yönlendiricileri vardır.
- Arama motorları tarafından bulunamaz, bilinen internette ise aranan siteleri arama motorları aracılığı ile bulmanız mümkündür.
- Derin internette yasadışı olan her çeşit faaliyete rastlamak mümkündür; silah ticareti, uyuşturucu, hacker kiralama, zombi bilgisayar kiralama, vs.

Derin veya karanlık internet diye tabir edilen bu ağda birçok zararlı içerikle karşılaşmak mümkündür. Örneğin Şekil 5'te görüldüğü üzere kötü niyetli kişiler, sadece doksan dokuz dolara pos cihazındaki yazılımı değiştirerek kredi kartlarının kopyalanmasını sağlayan yazılıma erişebilmektedirler. Bir başka örnek Şekil 6'da görüldüğü üzere kötü niyetli kişiler, otuz beş

dolara Cryptolocker olarak adlandırılan çok tehlikeli bir fidye yazılımını (ransomware) satın alıp istedikleri bilgisayarlara bulaştırıp fidye isteyebilmektedirler.



Şekil 5. Karanlık İnternet Kredi Kartı Kopyalama Pos Uygulaması

Şekil 6. Karanlık İnternet Fidye Yazılım Satışı

2.1.2. BİT'in İşletmelere Faydaları

Bilgisayar/sayısal tabanlı sistemler ve iletişim teknolojilerinin birleşiminden meydana gelen bilişim ve iletişim teknolojileri, günümüz işletmelerinin bulundukları sektörlerde iş yapma şekilleri ve ürün / hizmet sunum alanında devrim niteliğinde değişimlere neden olmuş, bu değişim ve gelişim BİT'i işletmelerde yeri doldurulamaz bir konuma taşımıştır.

Rekabetin küreselleştiği günümüzde işletmelerin faaliyet gösterdikleri sektörlerde varlıklarını koruyabilmeleri ve yeni pazarlara girebilmeleri büyük ölçüde BİT'i işleri için kullanmada gösterdikleri marifet, dolayısıyla bilgiyi üretme, kullanma ve bundan yararlanmada ne ölçüde başarılı olduklarına bağlıdır (Rıfat ve Zerenler, 2008: 382)

Bilgi sistemleri aklımıza gelebilecek her sektörde yoğun bir şekilde kullanılmaktadır. Bu teknoloji-yoğun iş süreçleri ve üretim modelleri kuşkusuz işletmeler açısından da geçerlidir. Ürün ve hizmet üretimi yapan işletmelerin yolları bir şekilde bilgi teknolojileri ile kesişmekte,

bunlara ihtiyaç duymakta, baştan planlamış olmasalar da kendilerini bilgi teknolojileri kullanan ve bu teknolojilerden fayda sağlayanlar arasında bulmaktadırlar.

Bilgi sistemlerinin işletmelere sağladığı faydalar konusunda birçok bilimsel çalışma yapılmıştır. Örneğin; Öğüt tarafından 2003'te yapılan bir çalışmada bilgi sistemlerinin sağladığı faydalar şu şekilde sıralanmıştır;

• İşletme ile ilgili tüm bilgiler daha düzenli ve kolay erişilebilir bir biçimde yöneticilere sunulabilmektedir.

• Merkezi bilgi bankası, hızlı hesaplama yeteneği ve hızlı hazır programlar sayesinde örgüt yöneticilerinin bilgi talepleri daha çabuk karşılanabilmektedir.

• Yönetsel öngörülerin ve yönetsel planların dayandığı kararların tutarlılığı ve doğruluk derecesinde artış olmaktadır (Öğüt, 2003: 18-93).

Gökçen; yaptığı çalışmasında bilgi sistemlerinin işletmelere sağladığı faydaları 16 madde de özetlemiştir (Gökçen H., 2007). Bunlar;

1. Daha iyi hizmet
2. Daha iyi güvenlik
3. Rekabet avantajı
4. Daha az hata
5. Büyük ölçüde doğruluk
6. Yüksek kalitede çıktılar (ürünler)
7. Sağlıklı haberleşme
8. Etkinliğin artması
9. Verimliliğin artması
10. Daha etkin yönetim
11. Daha fazla fırsatlar
12. İşgücü ihtiyacının azaltılması
13. Maliyetlerin azaltılması
14. Daha etkin finansal karar verme
15. Aşırı faaliyetlerin etkin kontrolü
16. Daha etkin yönetimsel karar verme

Yöneticilerin en önemli görevlerinden birisi doğru karar almalarıdır. Bu kararların doğru ve güvenilir verilere dayanması şüphesiz gerekir. Bu açıdan bilişim sistemlerinin, karar almayı,

koordinasyonu ve kontrolü desteklemeye ek olarak, problem analizi, karmaşık konulara yaklaşım ve yeni ürünler ortaya koymada yönetici ve çalışanlara yardımcı olduğu görülmektedir (Tekin vd., 2000: 83).

2.2. Bilgi Güvenliği

Bilgi; mal ve hizmet üretimindeki, personel, malzeme, makine, tesis ve para gibi işletmelerin temel girdilerine ilaveten, stratejik öneme sahip, belki de en pahalı girdi ve şüphesiz korunması gereken bir değerdir (Gökçen, 2002).

Bilgi güvenliği, asırlardır var olan bir kavramdır. Bilgi, her daim korunması gereken bir varlık olarak karşımıza çıkmıştır. Gaius Julius Caesar'ın komutanlarına gönderdiği mesajları şifrelemek için milattan önce 50'li yıllarda icat ettiği "Caesar Cipher" yöntemi, bilginin, güvenliği sağlandığında stratejik bir varlık olduğunu gösteren tarihteki bilinen ilk örnektir (Srikantaswamy ve Phaneendra, 2012: 40).

Bilgi, günümüz işletmeleri şüphesiz ki en önemli varlıklarından biridir. Bu bilgi kimi zaman ürün kalitesi, kimi zaman hizmet kalitesi ile ilgilidir. Bir şirketin hayatını idame ettirmesi ve gelecekte var olması, sahip olduğu bilgiye ve bu bilgiyi doğru şekilde kullanmasına ve korumasına bağlıdır. Bruce Schneier 2008'de yayınladığı kitabında şu ifadeye yer vermiştir; "Eğer güvenliği, ürün ve hizmetinizle bütünleşik bir şekilde son kullanıcıya sunarsanız, insanları memnun eder ve kazanırsınız, aksi takdirde insanların sizin ürün veya hizmetinizin güvenliği hakkında endişe duymaları sizin sürekli zaman, enerji, para harcamak zorunda bırakacağından ve güvenliği başarılı bir şekilde pazarlayamazsınız." (Schneier, 2008).

Bilgi güvenliği; bilgiye sürekli olarak –izinler çerçevesinde– erişilebilirliğin sağlandığı bir ortamda, "bilginin göndericisinden alıcısına kadar gizlilik içerisinde, bozulmadan, değişikliğe uğramadan ve başkaları tarafından ele geçirilmeden bütünlüğünün sağlanması ve güvenli bir şekilde iletilmesi sürecidir." (Canbek ve Sağıroğlu, 2006: 165). Bilgi güvenliği denildiğinde; bilginin gizliliğinin sağlanması ve izinsiz kişilerin erişiminin engellenmesi, bütünlüğünün korunarak olası tehditlerin bu bütünlüğe zarar vermesinin önüne geçilmesi ve bilgiye erişimin garanti altına alınarak, yetkiler dâhilinde, erişilebilir olması anlaşılmalıdır.

Bilgi güvenliğinin; gizlilik, bütünlük ve erişebilirlik olarak üç ana unsuru bulunur. Bu unsurları ilk inceleyen yayının "Bilgisayar Sistemlerinde Bilginin Korunması", (The protection of information in computer systems) başlıklı çalışma olduğu kabul edilmektedir (Saltzer ve Schroeder, 1975: 1279). Ancak günümüzde kullanıldığı şekli ile "CIA Üçgeni" (CIA-triad)

kavramı ilk olarak "Johnson Uzay Merkezi" tarafından 1989'da "Pembe Kitap" olarak ta bilinen JSC-NASA "Bilgi Güvenliği Planları"nda yer almıştır (Parker, 2010: 14). Günümüze kadar birçok akademik çalışma, ulusal ve uluslararası standart, devlet kurum ve kuruluşları, özel şirketler, bilgi güvenliği çalışmalarında CIA Üçgeni'ni temel almışlardır (Cherdantseva ve Hilton, 2013: 546).

Şekil 7. CIA Üçgeni
Kaynak: Perez, 2016.

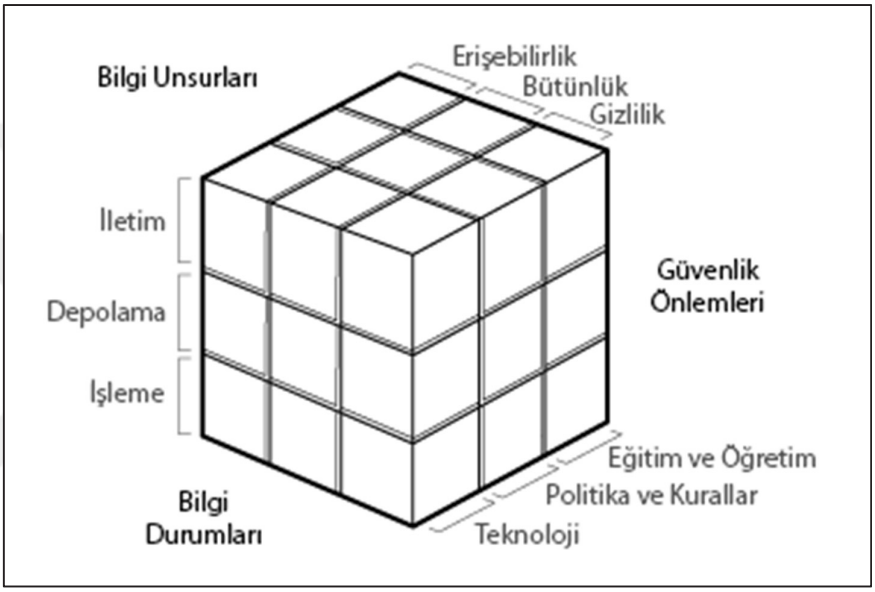
Uluslararası Bilgi Güvenliği Standardında da (ISO 27001'de) bilginin; gizlilik, bütünlük ve erişebilirlik unsurlarını temel almıştır (TS ISO/IEC 27001:2013, 2016). Gizlilik; bilginin yetkisiz kişiler, varlıklar ya da işlemlerde kullanılabilirliğinin engellenmesi ya da açıklanmaması özelliğidir (TS ISO/IEC 27001:2013, 2016). Gizlilik başka bir deyişle; izni olanların izin dâhilinde, belirtilen yol ve şekillerde bilgiye erişmesi, izni ve yetkisi olmayanların sadece bilgiyi değil bilginin varlığından dahi haberinin olmaması durumudur.

Bütünlük; varlıkların doğruluğunu ve tamlığını koruma özelliğidir. Anlamlı ve tutarlı olması, doğru ve kesin olması, kendi içinde çelişik olmaması, son halini almış bilgi üzerinde değişiklik yapılmamış olması durumudur (TS ISO/IEC 27001:2013, 2016). Erişebilirlik; yetkili bir varlık (kişi veya bilgiyi işleyen, veriden kullanılabilir bilgi üreten başka bir cihaz veya işlem) tarafından talep edildiğinde erişilebilir ve kullanılabilir olma özelliğidir. Bilgi yetkili kişilerin yetkileri kapsamında istedikleri zaman erişmelerini, amacı dâhilinde kullanılması durumudur (TS ISO/IEC 27001:2013, 2016).

BİT'de ilk kapsamlı bilgi güvenliği modeli 1991'de, McCumber tarafından geliştirilmiştir. Bu model "McCumber Küpü" olarak bilgi güvenliği literatürüne geçmiştir (McCumber, 1991; Cherdantseva ve Hilton, 2013: 550). McCumber Küpü aynı zamanda;

Amerikan Bilgi Güvenliği Uzmanlığı Ulusal Eğitim Standardı (National Training Standard for Information Systems Security Professionals), NCSS 4011'in bir parçasıdır (Whitman ve Mattord, 2012: 15).

McCumber Küpü üç ana bloktan oluşmaktadır. Bunlar; Bilginin Unsurları (gizlilik, bütünlük, erişebilirlik), Bilginin Durumları (iletim, depolama, işleme) ve Güvenlik Önlemleridir (eğitim ve öğretim, politika ve kurallar, teknoloji) (Loeb, 2002).



Şekil 8. McCumber (Küpü) Bilgi Güvenliği Modeli
Kaynak: Loeb, 2002.

Bilği güvenliğinde elektronik ticaretin yaygınlaşması ile beraber ihtiyaçlara cevap verme adına "doğruluk ve inkâr edilemezlik" ilkeleri ortaya çıkmıştır. Bu ilkeler literatürde e-ticaret yapan kişi ve kurumların yaptıkları işlemlerin, doğruluğunu sağlayıcı ve gerçekleştirdikleri işlemleri inkâr etmelerini önleyici tedbirler olarak yer almıştır (Güngör, 2015: 9).

Bilgi ister klasik yöntemlerle (yazılı) kayıt altına alınsın ve faydalanılsın, isterse sayısal tabanlı bilgi teknolojileri kullanılarak anlamlı hale getirilsin, her zaman korunması gereken stratejik bir varlık olmuş ve olmaya da devam etmektedir.

Verizon tarafından yapılan araştırma da "bilgi güvenliği unsurlarının en yoğun şekilde hangi tür saldırılara maruz kaldığı" sorusuna cevap aranmıştır. Araştırma sonucu, en çok saldırının "kötü amaçlı yazılımlar" aracılığı yapıldığını ve bilginin "bütünlük" unsurunu hedef alındığı ortaya koymuştur (Verizon, 2016).

Şekil 9. Bilgi güvenliği unsurlarını hedef alan siber saldırılar

Kaynak: Verizon, 2016: 74.

Ross Anderson, "Bilgi Güvenliği Neden Zor" (Why Information Security is Hard) isimli makalesinde; siber güvenlikte motivasyon, yükümlülükler ve sorumlulukların, hangi eylemlerin, kimin tarafından yapılacağını belirlediğini ve müşterek/ortaklaşa çalışmanın sonucu olarak siber savunmanın pozitif veya negatif etkilenebildiği vurgusu yapmıştır (Anderson, 2001).

Bilgi güvenliği organizasyonlar için dört önemli işlev gerçekleştirmektedir (Whitman ve Mattord, 2012: 41);

1. Organizasyonun hayatını devam ettirebilmesi için gerekli fonksiyonların korunması.
2. Kuruluşun bilgi sistemleri üzerinde çalışan uygulamaların güvenli bir şekilde çalışmaya devam etmesi.
3. Organizasyonun işleri için topladığı ve kullandığı verinin korunması.
4. Organizasyonun teknolojik varlıklarının korunması.

Bilgi güvenliği konusuna genellikle teknik bir problem olarak yaklaşılmaktadır. Oysa konu daha çok yönetimsel nitelik taşımaktadır. Bu nedenle ancak organizasyonların genel

yönetimi ile bilişim yönetimi birimlerinin ortak çalışması halinde bilgi güvenliği doğru bir şekilde yönetilebilir. Bilgi güvenliği konusunda eserleri bulunan Charles Cresson Wood; "Teknolojik problemlere daha çok teknoloji ile çözüm aramak doğru bir yaklaşım değildir, bilgi güvenliği sorunları teknik sorunlardan ziyade yönetim sorunu olarak değerlendirilmesi gerektiğine" vurgu yapmıştır (Wood, 2005).

Yapılan araştırmalar, bilgi güvenliği yöneticileri ile kullanıcılar arasında bakış açısı bakımından uçurum olduğunu göstermekte, alan yöneticilerinin kullanıcıları "tehdit" olarak vasıflandırdıklarını, kullanıcıların ise kendilerini bilgi güvenliği tehditleri ile mücadele de "yöneticiler tarafından yeteri kadar başvurulmayan" bir kaynak olarak gördüğünü göstermektedir. Yapılan çalışmalarda elde edilen bulgular; yöneticilerin gerçekçi olmayan varsayımlarla hareket ettiklerini göstermektedir (Albrechtsena ve Hovdena, 2009: 479).

Bilgi güvenliğinin yönetim boyutu hakkında yapılan çalışmalar, "kapsamlı ve kolektif" bir mücadele için dikkate alınması gereken en önemli konulardan birinin de "örgütsel yapılar" olduğu ve etkili bir mücadele için organizasyon yapılarının klasik yönetim şekillerinden uzaklaşarak kendilerini yenilemeleri gerektiğine vurgu yapılmaktadır (Persadha vd., 2016: 148). Hatta her gün daha karmaşıklaşan bilgi güvenliğine, yerinde ve zamanında müdahale etmek adına organizasyonlar, en tepe yöneticiye bağlı olarak çalışan, "bilgi güvenliği genel müdürü" (CISO, Chief Information Security Officer) istihdam etmektedirler.

2.3. Siber Güvenlik

Siber, bilgisayar ve ağlarını içeren kavram ya da varlıkları tanımlamak için kullanılır. Siber alan (cyber space) kelimesi de birbiriyle bağlantılı system, yazılım, donanım ve insanların iletişim ve/veya etkileşimde bulundukları soyut veya somut alanı tarif etmek için kullanılmaktadır. (Czosseck, C., Ottis, R., ve Ziolkowski, K., 2012: 8)

"Bilgi güvenliği" ve "siber güvenlik" kavramları birçok çalışmada birbirinin yerine kullanılsa da siber güvenlik bilgi güvenliğine kıyasla klasik bilgi kaynaklarının korunmasının ötesinde birçok varlığın (bilgi, donanım, yazılım, bina, baraj, kurum, şirket, devlet hatta insan) güvenliğini sağlamayı ifade etmektedir (Solms ve Niekerk, 2013: 99).

Siber güvenlik kavramı, ilk olarak bilgisayar sistemlerindeki ağ ve güvenlik açıklarına atfen bilgisayar bilim insanları tarafından kullanılmış, bu tehdit boyutunun hızla yükselmesi ve yıkıcı etkilerinin ortaya çıkması ile daha sonra diğer bilim dallarının da konusunu oluşturmuştur (Nissenbaum, 2005: 70). Siber güvenlik kavramı, soğuk savaş sonrası teknolojik yenilikler ve

jeopolitik değişimlerin sonucunda kullanılmaya başlanan bir kavram olarak karşımıza çıkmaktadır (Hansen ve Nissenbaum, 2009: 1155).

T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı siber güvenliği; "Siber uzayı oluşturan bilişim sistemlerinin saldırılardan korunmasını, bu ortamda işlenen bilgi/verinin gizlilik, bütünlük ve erişilebilirliğinin güvence altına alınmasını, saldırıların ve siber güvenlik olaylarının tespit edilmesini, bu tespitlere karşı tepki mekanizmalarının devreye alınmasını ve sonrasında ise sistemlerin yaşanan siber güvenlik olayı öncesi durumlarına geri döndürülmesi" olarak tanımlanmıştır (T.C Ulaştırma Bakanlığı, 2016).

Uluslararası Telekomünikasyon Birliği (ITU) siber güvenliği; "kurum, kuruluş ve kullanıcıların bilgi varlıklarını korumak amacıyla kullanılan yöntemler, politikalar, kavramlar, kılavuzlar, risk yönetimi yaklaşımları, faaliyetler, eğitimler, en iyi uygulama deneyimleri ve kullanılan teknolojiler bütünü" olarak tanımlamaktadır (BM Uluslararası Telekomünikasyon Birliği, 2008).

2.3.1. Siber Güvenlik Kavramları

Siber güvenlik kavramının daha iyi anlaşılması için siber varlık, siber olay, siber uzay, siber zorbalık, siber savaş, siber casusluk, siber silah, siber terörizm, siber saldırı ve siber tehdit kavramları aşağıda sırası ile açıklanmıştır.

2.3.1.1. Siber Varlık (Cyber Entity)

Hızla gelişen teknoloji, işletmelerin bitmek bilmeyen "bir adım önde olma" çabası ve pazar paylarını artırma çabaları her gün yeni bir cihazı insanlığın kullanıma sunmaktadır.

Bu cihazlar sayesinde işletmeler işlerini daha iyi yapabildiği gibi bireysel kullanıcılar da hayatlarını kolaylaştıran işlevlerden faydalanabilmektedir. Yeni teknolojileri bünyelerinde barındıran bu cihazlar, bazen akıllı telefon üzerinde çalışan bir uygulama aracılığı ile çalıştırılabilen bir çamaşır makinası ile karşımıza çıkmakta bazen de depo içerisine girmeye gerek kalmadan aranan ürünü istiflendiği yerde bulup getiren robotik depolama sistemleri ile karşımıza çıkmaktadır. Söz konusu bu cihazlar ister işletmelere, isterse bireye yönelik üretilmiş olsun bir şekilde bir yerlerle, bir şeylerle bağlantı kurmakta bu bağlantı sayesinde bu işlevleri yerine getirebilmektedir.

Klasik bilişim unsurlarının (bilgisayar, sunucu, ağ cihazları, vb.) yansıra, internet bağlantılı televizyondan, araçlardaki arızayı servise otomatik bildiren bileşenlere kadar, tüm bu

cihazları ve yazılım, donanım bileşenlerini "*siber varlık"* tanımı içine dâhil edebilmek mümkündür.

Siber varlıklar; fiziksel siber varlıklar ve mantıksal siber varlıklar olmak üzere iki kategoride sınıflandırmaktadır;

1. Fiziksel Siber Varlıklar: Fiziksel siber varlık denildiğinde BİT'nin fiziksel bir kütlesi olan, fiziksel güvenlik önlemleri ile korunması gereken, çevre faktörlerinden etkilenme olasılığı olan, fiziksel olarak taşınabilen, fiziksel etkilere (nem, yangın, elektrik kesintisi, hırsızlık) maruz kalabilen varlıklar anlaşılmalıdır.

2. Mantıksal Siber Varlıklar: Hür türlü yazılım ve uygulamanın yanı sıra bu varlıkların meydana gelmesinde rol oynayan bilgisayar kodları ve süreçleri mantıksal siber varlık olarak nitelendirilebileceği gibi fiziksel siber varlıklar aracılığı ile işlenen veri, bilgi ve yapılandırma ayarları da mantıksal siber varlıklar olarak sınıflandırılabilir.

2.3.1.2. Siber Olay

Siber olay; fiziksel veya mantıksal siber varlıkların çeşitli şekillerde paydaş olduğu olaydır. Bilişim ve endüstriyel kontrol sistemlerinin veya bu sistemler tarafından işlenen bilgi veya herhangi bir verinin gizlilik, bütünlük veya erişilebilirliğinin ihlal edilmesini veya buna teşebbüs edilmesini ifade eder (T.C Ulaştırma Bakanlığı, 2016: 8).

Ulaştırma Denizcilik ve Haberleşme Bakanlığı'nın bu tanımına ek olarak; bilgi ve iletişim teknolojilerinden yararlananların, bu teknolojiler sayesinde elde ettikleri menfaat ve faydanın olumsuz etkilendiği, doğal afet, elektrik kesintisi, fiber optik hatlarda oluşan arızalar veya benzer herhangi bir vaka *"siber olay"* olarak nitelendirilebilir.

Amerikan Milli Standartlar ve Teknoloji Enstitüsü siber olayı; "Örgütsel fonksiyonlar üzerinde etkiye sahip siber güvenlik değişikliği" olarak tanımlamıştır (NIST, 2016).

2.3.1.3. Siber Uzay

"Siber uzay" veya "siber alan" tanımı birçok kaynak tarafından benzer fakat farklı şekilde yapılmaktadır. Siber uzay; T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı tarafından hazırlanan "2016-2019 Ulusal Siber Güvenlik Strateji" çalışmasında; "Tüm dünyaya ve uzaya yayılmış durumda bulunan bilişim sistemlerinden ve bunları birbirine bağlayan ağlardan oluşan veya bağımsız bilgi sistemlerinden oluşan sayısal ortam" şeklinde tanımlanmaktadır (T.C Ulaştırma Bakanlığı, 2016)

Amerikan Savunma Bakanlığı siber uzayı; "internet iletişim ağlarını, gömülü işlemci ve kontrol birimlerini içeren, bilgi teknolojileri altyapılarından meydana gelen, bir birine bağlı ağların oluşturduğu bilgi ortamındaki bir küresel alan" şeklinde tanımlamıştır (Amerikan Savunma Bakanlığı, 2013).

Amerikan Kongre araştırmacılarından Hildreth; "insanların bilgisayarlar ve telekomünikasyon sistemleri aracılığıyla herhangi bir coğrafi sınırlamaya maruz kalmadan tamamen birbirine bağlı olma durumudur" şeklinde bir tanımlama yapmıştır (Hildreth, 2001).

Gürkaynak ve İren siber uzayı; "Herhangi bir coğrafi sınırlamaya maruz kalmaksızın, internete bağlı bilgisayar ağlarının oluşturduğu elektronik ortama siber ortam / siber uzay denmektedir" olarak ifade etmişlerdir (Gürkaynak ve İren, 2011: 265).

AB Komisyonunun tarafından yapılan siber uzay tanımının, "Dünya çapında kişisel bilgisayarların elektronik verilerinin dolaştığı elektronik ortam" şeklinde olduğu görülmektedir. NATO tarafından ise, "bilgisayarlar ve bilgisayar ağları kullanılarak veri saklamak, bu verileri işlemlere tabi tutmak ve iletmek için bilgisayarların ve elektromanyetik spektrumun kullanımı ile karakterize edilen fiziksel ve fiziksel olmayan çevre" şeklinde bir tanımlama yapıldığı görülmektedir (CCDCOE, 2009).

Bu tanımlardan yola çıkarak; herhangi bir teknoloji kullanarak, herhangi bir cihaz, sistem ve/veya siber varlıkla iletişim kuran, bilgi alışverişi yapan, doğrudan veya dolaylı olarak insan veya cihazlarla etkileşimde bulunan varlıkların bulundukları alana "siber uzay" demek mümkündür. Kavram, genel nitelikte olup, bireysel veya sınırları belirli alanlar için kullanılmamaktadır. Bu açıdan, herkes tarafından paylaşılan bir alanı ifade etmesi itibariyle gerçek uzay ile de benzeştiği söylenebilir.

2.3.1.4. Siber Zorbalık (Cyber Bullying)

Siber zorbalık; "bilgi ve iletişim teknolojilerini kullanarak başkalarına zarar vermek amaçlı, e-posta, kısa mesaj, sosyal medya üzerinden birilerine düşmanca yapılan eylemler bütünü" olarak tanımlanmaktadır (Li Q. , 2007: 437).

(Patchin ve Hinduja,2006: 152) yaptıkları çalışmada siber zorbalığı; "zarar verme amaçlı, tekrarlanan elektronik metinler" olarak ifade etmişlerdir.

Siber zorbalık, özellikle sosyal medyanın yaygın olarak kullanılması ile daha da yaygınlaşmıştır. Kişiler, şirketler veya devlet kurumları her gün e-posta veya sosyal medya aracılığı ile yapılan siber zorbalıklara maruz kalmaktadırlar.

2.3.1.5. Siber Savaş

Savaş, devletlerin var oluşu kadar eski bir terimdir. Ülkelerin kendi çıkarlarını korumak veya artırmak, gücü elinde tutanların ise güçlerini korumak adına başvurdukları bir yöntemdir (Keskin, 1998: 15). Savaş; uluslararası hukuk kurallarına uygun şekilde devletler arasında yürütülen silahlı çatışma veya çekişmedir (Meray, 1962: 469).

Sibernetik savaş olarak ta tanımlanan (Post, 1979: 44-104) siber savaştan tam olarak ne kast edildiğini tanımlamak zor olmakla birlikte siber savaş; belirlenen hedeflere bilgisayar ve bilişim teknolojileri kullanılarak yapılan saldırılar ve ulusal güvenliği etkileyecek şekilde yapılan BT tabanlı saldırılardır (Alford, 2000). Her ne kadar devletler kendi siber ordularını kurmuş ve bu ordular için yatırımlara devam ediyor olsalar da, bazı araştırmacılar siber savaşın hiçbir zaman olmayacağına, ama doğası gereği siber ortamların askeri casusluk ve sabotaj gibi operasyonlara uygun olduğuna vurgu yapmışlardır (Rid, 2012: 5–32).

2.3.1.6. Siber Casusluk

1889 Lahey Antlaşması'nın 29. maddesinde casusun tanımı şu şekilde yapılmaktadır; "gizlice veya sahte kimlikle, muharip bir devletin harekât sahasında bilgi elde eden veya etmeye çalışan kimsedir" (Türk Ansiklopedisi, 1958: 490).

Siber casusluk ise internet, internet ağları, bilgisayarlar veya yazılımlar kullanılarak, gizli, hassas veya kişiye/kuruma özel bilgilerin, siyasi, askeri, ekonomik avantaj sağlamak için düşmanca yasa dışı yöntemler kullanılarak sırların elde edilmesidir (Nickolov, 2008).

Ocak 2016'da Amerikan İstihbarat direktörü James R. Clapper; "Çin; Amerika, Amerikan şirketleri ve Amerika'nın müttefiklerine karşı başarılı bir şekilde siber casusluk faaliyetlerine devam etmektedir" (Gady, 2016) açıklaması ile Çin'in siber casusluk faaliyetleri yürüttüğünü ve Amerika'nın bu faaliyetlerden haberdar olduğunu vurgulamıştır.

Siber casusluk, ticari amaçlar doğrultusunda, genelde devlet desteği ile rakip veya daha önde olan işletme veya devletlerden ticari sırların çalınması olarak karşımıza çıkmaktadır.

2.3.1.7. Siber Silah

Silah genel olarak, saldırı veya savunma amaçlı "öldürme, yaralama, yok etmek, zarar vermek üzere tasarlanmış alet, cihaz, makine veya araç" olarak tanımlanmaktadır (Intoccia ve Moore, 2006: 480).

NATO siber silahı, “saldırı yeteneğine sahip zararlı yazılım” şeklinde tanımladığı görülmektedir (Czosseck vd., 2012). Sayısal tabanlı bir BİT sisteminin yazılım veya donanımın, her ne kadar yukarıda yapılan kinetik silah tanımlamasına uymadığı söylenebilir. Ancak etkileri göz önünde bulundurulduğunda, insanların ölümüne, yararlanmasına veya zararlı bir etki oluşturabilecek şekilde, hayatlarını doğrudan veya dolaylı etkilemek üzere, bilişim sistemleri kullanılarak, bazı kesimler tarafından “siber silah” olarak adlandırılan kötü amaçlı yazılım ve uygulamaların geliştirildiği, gelişmiş ve gelişmekte olan ülkelerin bu hususta yatırımlar yaptığı ulusal ve uluslararası medyada yer almaya devam etmektedir.

2.3.1.8. Siber Terörizm

Soğuk savaşın gereği olarak ortaya çıkan psikolojik savaş türü ve bu savaşın vazgeçilmez unsuru düşük yoğunluktaki çatışmalar (Low Indensity Conflict), terör kavramını da beraberinde getirmiştir (Mirdas, 2016).

3713 sayılı Terörle Mücadele Kanunu’nun 1. Maddesinde terör; “Cebir ve şiddet kullanarak; baskı, korkutma, yıldırma, sindirme veya tehdit yöntemlerinden biriyle, Anayasada belirtilen Cumhuriyetin niteliklerini, siyasî, hukukî, sosyal, laik, ekonomik düzeni değiştirmek, Devletin ülkesi ve milletiyle bölünmez bütünlüğünü bozmak, Türk Devletinin ve Cumhuriyetin varlığını tehlikeye düşürmek, Devlet otoritesini zaafa uğratmak veya yıkmak veya ele geçirmek, temel hak ve hürriyetleri yok etmek, Devletin iç ve dış güvenliğini, kamu düzenini veya genel sağlığı bozmak amacıyla bir örgüte mensup kişi veya kişiler tarafından girişilecek her türlü suç teşkil eden eylemlerdir.” şeklinde tanımlanmaktadır.

Schmid (1993) e göre terörizm; "gizli ya da yarı gizli birey, grup ya da devlet aktörleri tarafından, kişisel, kriminal veya siyasal sebeplerle, korku ve endişe kaynağı olan tekrarlanmış şiddet eylemleridir. Suikastlar hariç olmak üzere, bu eylemlerin doğrudan hedefleri, asıl mağdurlar değildir. Şiddetin insan mağdurları, ilk aşamada, mesaj jeneratörü olarak, genelde hedef nüfus kitle içerisinden fırsatın elverişliliğine bağlı olarak rastgele ya da önceden belirlenmiş temsili veya sembolik hedefler olarak seçilirler. Teröristler, doğrudan mağdur ve hedef kitle arasında tehdit ve şiddet üzerine kurulu bir iletişim süreci oluşturmak isterler. Teröristlerle mağdurlar ve esas hedef kitle arasındaki tehdit ve şiddet üzerine kurulu iletişim süreci, söz konusu esas kitleyi, yani toplumun genelini etkilemeyi amaçlamaktadır. Yıldırma, zorlama veya propaganda amaçlarından hangisine ulaşılması isteniyorsa; buna uygun olarak hedef kitle terörün, taleplerin veya ilginin odağı haline getirilir" (Schmid, 1993: 11).

Coady; "terör eylemi çoğunlukla organize bir grup tarafından işlenen, savaş dışı kişiler üzerinde kasıtlı öldürme veya diğer ciddi zararlar ya da tehdit içeren politik eylem, terörizm terörist eylemlere giren taktik veya politika" olarak tanımlamaktadır (Coady, 1996: 265).

Gelişen BİT'nin sağladığı fırsatlar ve kullanan sayısındaki astronomik artış kötü niyetlilerinde ilgilisini çekmiş ve terörizm siber uzaya taşınmıştır. Siber terörizm, "siber uzayda, siber varlıklar kullanılarak gerçekleştirilen terör eylemleri" şeklinde tanımlanabilir. Güngör, siber terörizmi; "konvansiyonel terör örgütlerinin son yıllarda faaliyetlerini internet üzerine kaydırmaları neticesinde görülmeye başlanan siber saldırı türü" olarak ifade etmiştir (Güngör, 2015).

2.3.1.9. Siber Saldırı ve Siber Saldırı Aşamaları

Siber saldırı; "ulusal siber uzayda bulunan bilişim sistemlerinin gizlilik, bütünlük veya erişilebilirliğini ortadan kaldırmak amacıyla, siber uzayın her hangi bir yerindeki kişi ve/veya bilişim sistemleri tarafından kasıtlı olarak yapılan işlemler" olarak tanımlanmaktadır (T.C Ulaştırma Bakanlığı, 2016).

Dönemin mucitlerinden Sir John Ambrose Fleming'in, rekabet içerisinde olduğu Guglielmo Marconi'nin icat ettiği radyo sinyalleri vasıtasıyla iletişim kuran cihazın çalışma şeklinin kırılarak, Marconi'nin halka açık sunumu esnasında iletişime bir takım kaba mesajların girilmesi, tarihte gerçekleşen ilk **"**siber saldırı/hacking**"** olarak kabul edilmektedir (New Scientist Magazine, 2016).

Bir siber saldırı mantıksal bir olaydır, ancak bu bilişim sistemleri gibi fiziksel ortam üzerinden, doğrudan veya dolaylı insan faktörünün katkısı ile kendini gösterir (Herrmann, 2007: 27). Başka bir deyişle; siber saldırı, siber tehdidi gerçekleştirmek ve hedef alınan siber varlığın gizlilik, bütünlük ve erişebilirliğini, saldırıyı gerçekleştirin menfaatine manipüle eden veya kurbanın, gerçekleşen siber olaydan maddi/manevi zarar görmesi ile sonuçlanan eylemler bütünüdür.

Uluslararası Elektronik Ticaret Konseyi Danışmanları (International Council of Electronic Commerce Consultants) "Sertifikalı Etik Bilgisayar Korsanlığı" veya "Beyaz Şapkalı Hacker" olarak Türkçe' ye çevrilen "CEH – Certified Ethical Hacker" dokümanlarına göre, bir siber saldırıyı beş ana başlıkta/aşamada kategorize etmek mümkündür (EC Council-CEH, 2016). Bu aşamalar aşağıda açıklanmıştır.

2.3.1.9.1. Birinci Aşama: Keşif / Tanıma (Reconnaissance)

Bu aşamada bilgisayar korsanı hedef (siber kurban) hakkında bilgi edinmeye çalışır. Bilgi genelde herkesin kullanımına açık kaynaklardan elde edilmeye çalışılır. Saldırı aşamalarından belki de en uzun süreli olan budur. Korsan, hedef aldığı firma/kurum/kişi hakkında iş süreçleri, firmanın nasıl çalıştığı, çalışanlar, kullanılan cihaz ve sistemler, güvenlik önlemleri vs. hakkında aşağıdaki yöntem ve araçları kullanarak bilgi toplar (EC Council-CEH, 2016):

- İnternet arama motorları (Internet searches)
- Sosyal mühendislik (Social engineering)
- Çöpçülük (Dumpster diving)
- Alan adı yönetim ve aramaları (DNS Management/searches)
- Basit ağ taraması (Non-intrusive network scanning)

CEH'e göre bu aşama önlem alınması en zor olan aşamadır. Firmalar/kurumlar hakkında bilgiler çeşitli kaynaklardan paylaşılabilir, bu kaynaklardan bazıları bilgiyi elinde bulunduranların üzerinde detaylı düşünülmemiş, çevrim içi hizmetler aracılığı ile olabileceği gibi bazı bilgilerin çalışanlar tarafından sosyal medya üzerinden paylaşıldığı da dikkate alınmalıdır (EC Council-CEH, 2016). Saldırgan; saldırıda bulunmadan önce hedefinde olanlar hakkında çeşitli yöntemleri kullanarak bilgi toplar ve keşifte edindiği bilgi üzerinden saldırı yöntemine karar verir. (Efe, 2006)

Keşif/Tanıma çalışmaları; ağ araçları, arama motorları ve teknik doküman desteği kullanılarak yapılabilir. Bu amaçla kullanılan araçlarla; hedef cihaz ve/veya ağ hakkında yazılımsal ve donanımsal olarak planlanan saldırı için önemli ipuçlarına ulaşmak hedeflenmektedir. Bu ipuçları, karşıdaki bir cihazın kullandığı işletim sistemi olabileceği gibi, bunun bir bilgisayar olması halinde üzerinde çalışan uygulamalar, açık servisler ve açık portlar gibi bilgiler de olabilecektir. Bunların dışında saldırgan, hedefindeki ağ yapısı hakkında çeşitli bilgiler de elde edilebilmektedir (Efe, 2006).

2.3.1.9.2. İkinci Aşama: Tarama (Scanning)

Saldırgan, kurban (işletme/kurum) hakkında yeterli bilgiyi elde edip, kurum/işletmenin nasıl çalıştığı hakkında bilgi sahibi olduktan sonra; elindeki bilgiyi kullanarak firmanın internete açık ve kurum içinde bulunan cihazlarında aşağıdaki listelenen açıklara erişmeye çalışır (EC Council-CEH, 2016).

- Açık portlar,

- Açık servisler,
- Bilinen siber güvenlik açıkları bulunan uygulama ve yazılımlar ve işletim sistemleri,
- Verilerin bir yerden başka bir yere aktarılırken korunamaması,
- Kurbana ait ağ cihazlarının bir simülasyonu ile olası açıklıkları test etmek.

2.3.1.9.3. Üçüncü Aşama: Erişim Sağlama (Gaining Access)

Bu kavram ile "BT sistemlerine yetkisiz erişim" kastedilmektedir. Erişim sağlama, günümüz siber saldırılarının ana nedenidir. Saldırgan hedef kurbanın BT sistemlerinden ya direkt olarak fayda sağlamayı amaçlar veya kurbanın BT sistemlerini kaynak olarak kullanıp başka bir hedefe saldırı gerçekleştirir. Bu iki yöntem içinde korsan, kurbanın BT sistemlerine tamamen veya kısmen erişim sağlamış olması gereklidir (EC Council-CEH, 2016).

2.3.1.9.4. Dördüncü Aşama: Erişimi Sürdürme (Maintaining Access)

Saldırgan, erişim sağladığı BT sistemlerinde, bu erişimi kalıcı veya en azından uzun süreli bir şekilde devam ettirmek ister; buna "erişimi sürdürme" denilmektedir. Bu bağlamda saldırgan, erişiminin devamı adına "açık kapılar" oluşturur, sisteme erişmek için alternatif yöntemler kurgular ve erişimini fark edilmeden sürdürmeyi amaçlar (EC Council-CEH, 2016).

2.4.1.9.5. Beşinci Aşama: İzleri Saklama (Covering Tracks)

Siber korsanlar (Hacker), amaçlarına ulaşıp, kurbanın BT sistemlerini ele geçirdikten sonra, sisteme erişmek için izledikleri yöntem veya yolu gizlemek ve bunların sistem yöneticileri tarafından tespitini imkânsız hale getirmek veya zorlaştırmak için çeşitli izleri saklama yöntemleri kullanırlar.

Yukarıda belirtilen beş ana kategoriye ek olarak, saldırgan bazı durumlarda özellikle erişim sağlayamadığı sistemlerin çalışmasına zarar vermek adına "Engelleme Saldırıları" düzenler. Bu saldırılarda amaç, hedef sisteme zarar verip manipüle etmek veya bilgi çalmak yerine, sistemin kullanıcılarının sistemden sağladıkları faydaya engel olmakla beraber, imaj kaybına uğratarak hedef kurbana çeşitli zararlar vermektir.

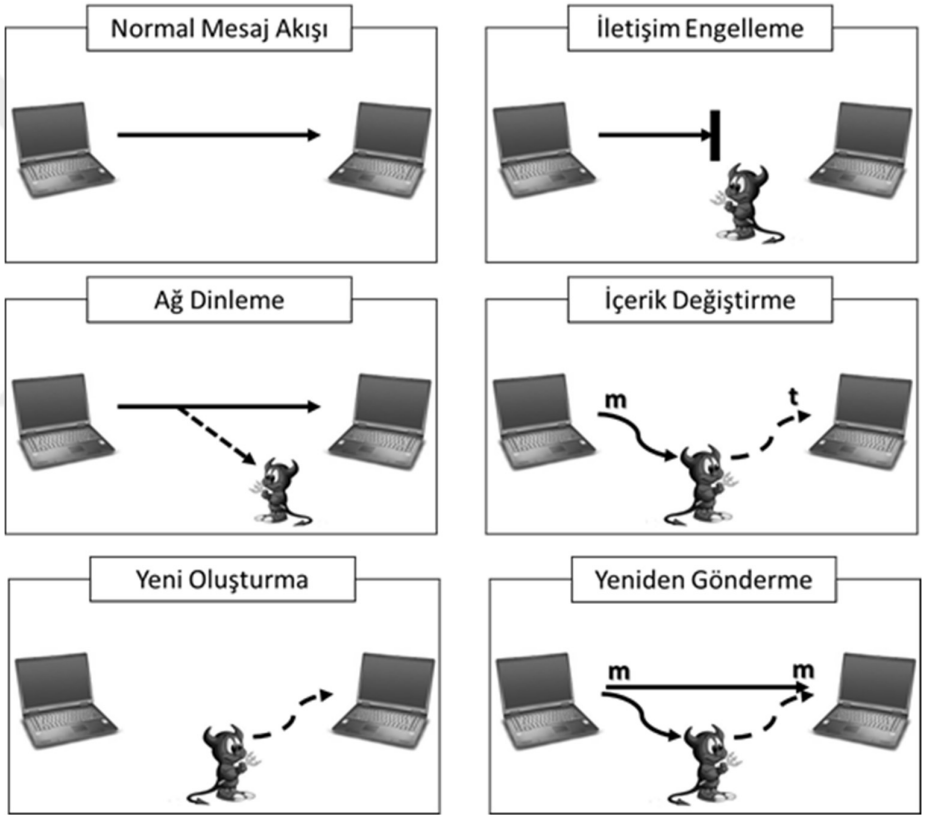
2.4.1.9.6. Engelleme Saldırıları

Saldırgan, bazı durumlarda, sisteme karşı engelleme ve servis dışı etme amaçlı saldırıda bulunur. Bu saldırılarda amaç, kurbanın bilgilerini çalmak veya sisteme erişmek değil, kurbanın BT sistemleri üzerinden verdiği hizmeti engellemek ve hizmet alan kişi veya kurumların hizmet alamaz hale gelmesini sağlamaktır. Aralık 2015'te, bazı devlet kurum, kuruluş ve bankaların web

üzerinden sağladıkları hizmetlere erişim engellenmiştir. Kamuoyunu günlerce meşgul eden bu "siber saldırılar" engelleme saldırıları türüne bir örnektir.

Engelleme saldırıları genel olarak (Hanaylı, 2014);

- İletişim engelleme,
- Ağ dinleme,
- İçerik değiştirme,
- Yeni oluşturma ve
- Yeniden gönderme saldırı yöntemlerini kullanmaktadır.



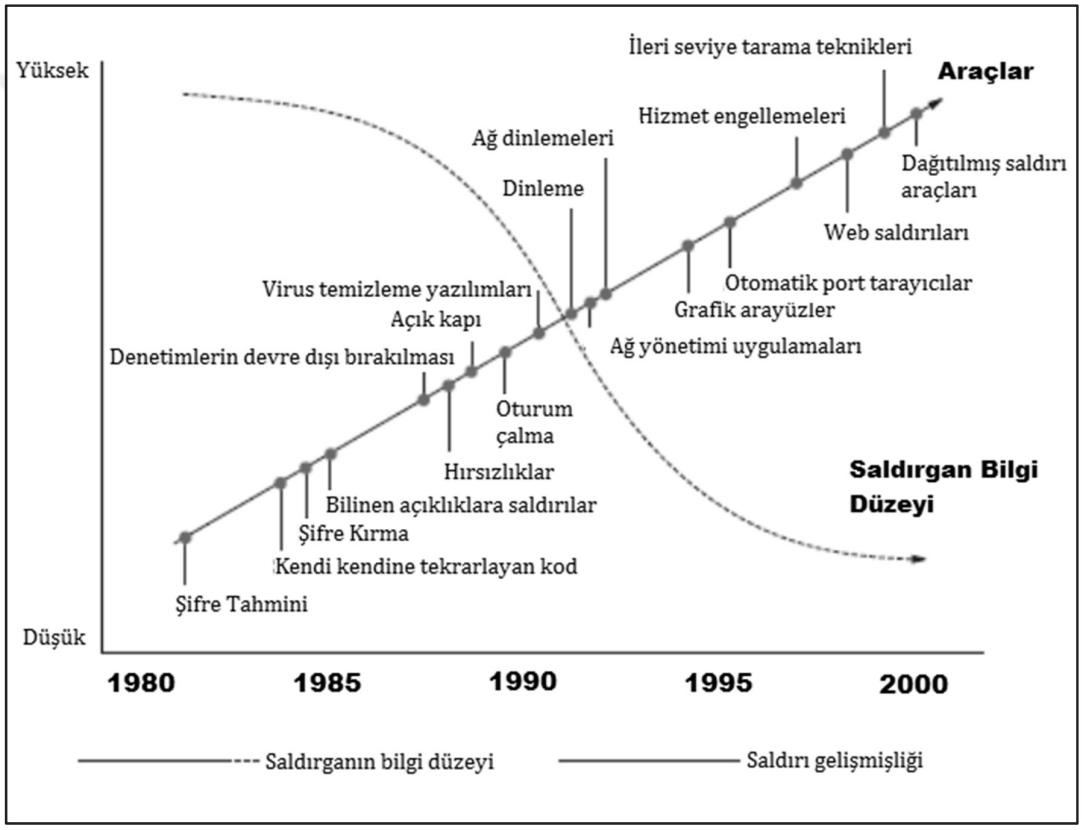
Şekil 10. Siber Saldırı Yöntemleri
Kaynak: Hanaylı, 2014.

2.3.1.10. Siber Tehdit

Tehdit; bir kurumun veya sistemin zarar görmesi ile sonuçlanabilecek istenmeyen bir olayın potansiyel nedenidir (T.C Ulaştırma Bakanlığı, 2016). Siber Tehdit**;** siber uzayda varlık bulan herhangi bir fiziksel veya sanal varlığın gizlilik, bütünlük veya erişebilirliğini olumsuz yönde etkileyecek eylemler bütünüdür. Siber tehdit, bazen bilgisayarlarda bulunan bir verinin istenmeyen ellere geçmesi, bazı hallerde ise bir şirketin müşterilerine sunduğu hizmetin geçici

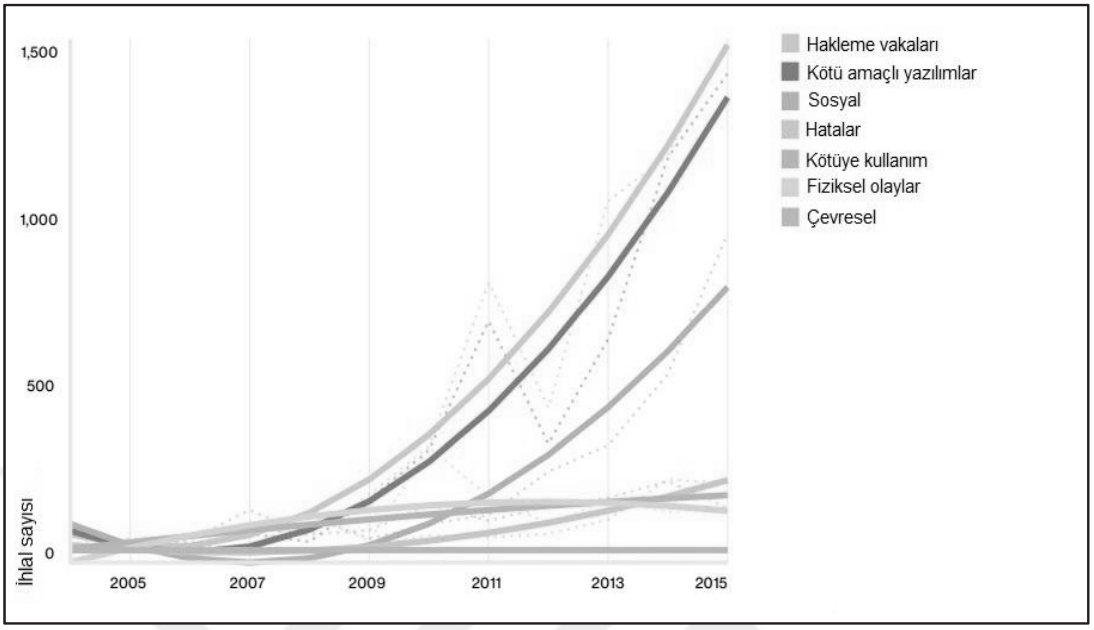
veya tamamen engellenmesi, çalınması, bozulması, ifşa edilmesi veya yok edilmesi şeklinde gerçekleşebilir.

Siber tehditler, 1980'li yıllarda, sadece bilgi sistemlerine fiziksel erişimi olan kötü niyetli, ileri düzeyde uzman kişiler tarafından gerçekleştirilmesine karşın (Winther, Gran, ve Dahll, 2005: 371) 1990'lı yıllarda bu eğilim, BİT'lerinde görülen gelişmeler aracılığı ile Şekil 11'de görüldüğü gibi, daha az bilgi gerektiren ve çok daha gelişmiş saldırılar olarak karşımıza çıkmaktadırlar.



Şekil 11. Saldırı Gelişmişliğine Karşın Saldırgan Bilgi Düzeyi

Kaynak: McHugh vd., 2000.

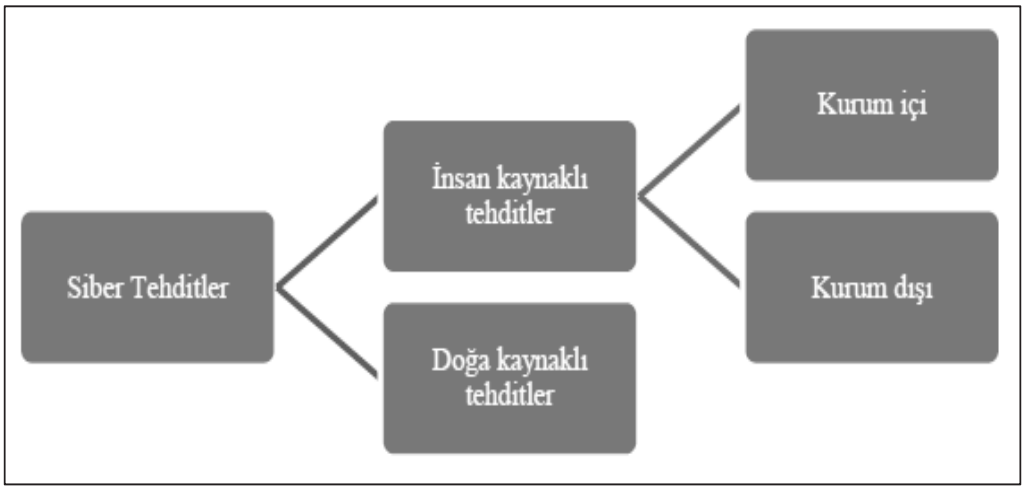


Şekil 12. Yıllara göre ihlal türleri (2016)

Kaynak: Verizon, 2016: 8.

2.3.2. Siber Tehdit Yöntem ve Çeşitleri

Teknolojinin toplumun hemen hemen her kesimi tarafından kullanıldığı günümüzde siber tehditlere de her gün yenileri eklenmekte, kötü niyetliler tarafından yeni yöntem ve araçlar kullanılmaktadır. Siber tehditler genel olarak "insan kaynaklı siber tehditler" ve "doğa kaynaklı siber tehditler" olarak iki ana kategoride incelemek mümkündür (Yaşar ve Çakır, 2015: 489).



Şekil 13. Siber Tehditlerin Sınıflandırılması

Kaynak: Yaşar ve Çakır, 2015: 490.

İnsan kaynaklı siber tehditler; insanların doğrudan veya dolaylı olarak katılımının olduğu tehditlerdir. Bilinçli tehdit oluşturacak eylemler; zararlı kod, virüs, casusluk faaliyetleri vb. kapsamaktadır. Bilinçsiz tehdit oluşturacak eylemler ise hatalı sistem yapılandırmaları, dikkatsizlik, yazılım hataları vb. olarak ifade edilebilir.

Doğa kaynaklı siber tehditler; doğal afet, beşeri bir sebebe dayanmayan, doğal etkilerden kaynaklanan tehditlerdir. Örneğin elektrik kesintileri veya iklimlendirmeden kaynaklanan sistem aksaklıkları bu tür tehditlerdir.

İnsan kaynaklı siber tehditler; kurum içi (iç tehdit) ve kurum dışı (dış tehdit) olmak üzere iki alt kategoriye ayrılır (Yaşar ve Çakır, 2015). İç tehdit; eğitimsiz bilinçsiz kullanıcıların farkında olmadan bir parçası oldukları tehdit türüdür. Bu tehdit türünde kullanıcı davranışları, BİT sistemlerinin kendinden beklenen fonksiyonlarda aksamalara veya açıklıklar oluşmasına hatta kötü niyetlilerin bu açıklıkları kullanarak sisteme dışarıdan sızmasına neden olmaktadır. Dış tehdit; BİT sistemleri veya bu sistemler üzerinde barınan siber varlıklarına karşı, genellikle internet üzerinden, yetkisiz, izinsiz ve kötü niyetliler tarafından gerçekleştirilen art niyetli eylemler bütünüdür.

Avrupa Birliği Ağ ve Bilgi Güvenliği Kurumu'nun yaptığı "ENISA 2015 Siber Tehdit Panoraması" raporunda; siber varlıkların en fazla maruz kaldıkları siber tehditleri incelemiş, 2014 siber tehdit raporu ile karşılaştırmalar yapmıştır. Bu çalışma kapsamında 2014 ve 2015 yıllarında kamuya açık bir şekilde rapor edilen ve kamuya açık olmayan kaynaklardan, (MISP, "Malware Information Sharing Platform and Threat Sharing", CYjAX, "CYjAX Information Management", CERT-EU, "Computer Emergency Response Team-Europe") siber güvenlik bağlamında bilgilerden faydalanılmıştır (Marinos, Belmonte, ve Rekleitis, 2016: 8). Aşağıdaki tabloda görüldüğü üzere; ilk beş saldırı türü, kötücül yazılım, web tabanlı siber saldırı, web uygulama saldırıları, botnetler (zombi bilgisayar ağları), servis engelleme saldırıları olup bunlar 2014 ve 2015 yılında ilk 5 sırada yer almaktadır. 2014 ve 2015 verilerine göre en az tehdit içeren unsurlar siber casusluk ve fidye yazılımları olduğu görülmektedir (Marinos vd., 2016: 51).

Tablo 1. Siber Tehdit Yöntemleri 2014-2015 Karşılaştırması

Tehdit Sıralaması 2014	Eğilim 2014	Tehdit Sıralaması 2015	Eğilim 2015	Değişim
1. Zararlı kod: Kurtçuk/Trojans	↑	1. Kötücül yazılım	↑	→
2. Web-tabanlı saldırı	↑	2. Web-tabanlı siber saldırı	↑	→
3. Web uygulama/enjeksiyon saldırıları	↑	3. Web uygulama saldırıları	↑	→
4. Botnetler	↓	4. Botnetler	↓	→
5. Servis engelleme	↑	5. Servis engelleme	↑	→
6. Spam/istenmeyen eposta	↓	6. Fiziksel zarar/hırsızlık/kayıp	➲	↑
7. Oltalama	↑	7. İç tehdit (bilinçli/bilinçsiz)	↑	↑
8. Exploit kits/İstismar Kiti	↓	8. Oltalama	➲	↓
9. Veri ihlalleri	↑	9. Spam/ istenmeyen eposta	↓	↓
10. Fiziksel zarar /hırsızlık /kayıp	↑	10. Exploit kits/İstismar Kiti	↑	↓
11. İç tehdit (bilinçli/bilinçsiz)	➲	11. Veri ihlalleri	➲	↓
12. Bilgi sızıntısı	↑	12. Kimlik hırsızlığı	➲	↑
13. Kimlik hırsızlığı/dolandırıcılık	↑	13. Bilgi sızıntısı	↑	↓
14. Siber casusluk	↑	14. Fidye yazılımları	↑	↑
15. Fidye yazılımları	↓	15. Siber casusluk	↑	↓
Eğilim: ↓ Düşüş eğilimi, ➲ Durağan, ↑ Artma eğilimi: ↑Artıyor, → Aynı, ↓ Düşüyor				

Kaynak: Marinos vd., 2016: 51.

Her ne kadar siber varlıkları hedef alan siber tehdit yöntem ve metodu çeşitlilik gösterse de bu çalışmada güncel ve kabul edilebilirliği yüksek olan Avrupa Birliği Ağ ve Bilgi Güvenliği Kurumu'nun yaptığı "ENISA 2015 Siber Tehdit Panoraması" raporunda yer alan ilk on beş siber tehdit unsuruna yer verilecek ve açıklanacaktır.

2.3.2.1. Kötü Amaçlı Yazılımlar (Malware)

Kötü amaçlı yazılımlar, altı kategoride incelenebilir (Ünver vd., 2011). Bunlar;

- Bilgisayar virüsleri,
- Solucan (Worm) ve Truva atı (Trojan),
- Klavye izleme (Key logger) yazılımları,
- İstem dışı olarak gönderilen ticari reklam ve tanıtım (Adware) yazılımları,
- Bilgi toplayan casus / köstebek (Spyware) yazılımlarıdır.

Avrupa Birliği Ağ ve Bilgi Güvenliği Kurumunun yaptığı "ENISA 2015 Siber Tehdit

Panoraması" isimli raporunda ifade edilen ilk on beş tehditten birincisi kötü amaçlı yazılımlardır.

2.3.2.1.1. Bilgisayar Virüsleri

Bilgisayar yazılım dilleri kullanılarak hazırlanan virüsler, aslında birer bilgisayar uygulaması/programıdır. Bu programcıklar, kendilerini bilgisayarda yüklü bulunan programlara yamarlar, bilinen faydalı programların aksine bulaştıkları bilgisayarın çalışmasını etkileyecek eylemler içerisine girerler. Bilgisayar virüsleri kendilerini gizlemeyi ve daha fazla kaynağa yaymayı amaç edinmişlerdir (Krutz ve Vines, 2007: 131-135).

2.3.2.1.2. Solucan ve Truva Atı

Bir çeşit virüs olan solucanlar, tıpkı virüsler gibi kendi kendilerine çoğalırlar. Solucanları virüslerden ayrılan en önemli özellik kendi başlarına hareket edebilmeleridir. Solucanların kendilerini herhangi bir programla ilişkilendirmeye ihtiyacı yoktur. Solucanlar, daha çok BİT varlıklarını hedef alarak atıl hale getirmek üzere bellek, bant genişliği ve sistem kaynaklarına bulaşarak bu sistemlerin ulaşılabilirliğini engeller ve bu varlıkların kontrolünü ele geçirmeyi amaç edinirler (Ünver vd., 2011: 11).

Truva atı; genelde e-posta, internet üzerinden oynanan oyunlar, mesajlaşma programları ya da internet üzerinden yüklenen ücretsiz ve lisanssız yazılımlar yoluyla yayılmaktadırlar. Solucanlardan farklı olarak sisteme bulaştığında hangi programla bulaşmışsa o programın açılmasını bekler (açılmadığı sürece aktifleşmez). Direkt olarak bilgisayarın işletim sistemine zarar verebilir. Bilgisayar üzerinde (monitör izleme, programlar açabilme v.b…) işlemler gerçekleştirerek tüm kontrolü ele alabilir. Truva atı bir virüs değildir. Gerçek bir uygulama gibi gözüken zararlı bir program türüdür. Truva atı kendini çoğaltmaz ama virüs kadar yıkıcı olabilir. Truva atı bilgisayarınıza güvenlik açığı oluşturur ki bu da zararlı programların, kişilerin sisteminize girmesi için bir yol açar. Truva atı faydalı gibi göründüğü halde, bilgisayarlara girdiği zaman gizli olarak zararlı eylemlerde bulunan bilgisayar programcıklarıdır (Gordon ve Chess, 1999).

2.3.2.1.3. Klavye İzleme (Key Logger) Yazılımları

Bu tür yazılımlar; sayısal tabanlı sistemlere tıpkı virüs gibi bulaşarak, kendilerini gizlerler ve kullanıcının klavye aracılığı ile girdiği verilerin birebir kopyasını alırlar. Alınan bu kopyalar genellikle internet üzerinden başka bir merkeze gönderilir. Kullanıcı adı, kredi kartı bilgisi ve şifre gibi kullanıcılar için değerli olan bilgiler, klavye izleme yazılımları aracılığı ile kötü niyetli kişiler tarafından ele geçirilen verilere örnek verilebilir (Krutz ve Vines, 2007: 149-151).

2.3.2.1.4. İstem Dışı Ticari Reklam ve Tanıtım (Adware) Yazılımları

Adware, genellikle arzu edilen özelliklere sahip bir yazılımın ücretsiz veya düşük maliyetli kullanımı karşılığında, sizin bilgi ve onayınız dâhilinde reklam sunan yazılımlardır. Bir tür casus yazılım olan *adware* pratikte casus yazılımların en iyi huylu olanları olarak kabul edilebilir ancak söz konusu *adware* izniniz ve bilginiz olmadan bilgisayarınız ve bilgisayarınız üzerinde yüklü bulunan uygulamaların ayarlarını değiştirebilir, bilgisayarınızda bulunan kişisel verilerinizi toplayıp reklam verenlerle paylaşabilir. Bu durumunda *adware,* casus yazılım kategorisi içerisinde değerlendirilir (NC State University, 2016).

2.3.2.1.5. Bilgi Toplayan Casus/Köstebek (Spyware) Yazılımları

Casus/köstebek yazılımlar hakkında herkes tarafından kabul edilen bir tanımlama bulunmamasına rağmen, pratikte casus yazılımların eylemlerinden yola çıkarak, "Bilginiz ve onayınız olmadan bilgisayarınızın ayarlarını değiştiren, veri toplayan, topladığı verileri başkalarına ileten ve kullanan yazılımlardır" şeklinde tanımlanabilir (NC State University, 2016).

Bazı kaynaklarda snoopware (burun sokan yazılım) olarak da adlandırılan casus yazılımlar, virüs ve solucanlardan farklı olarak hedef sisteme bir kez bulaştıktan sonra kendi kopyasını oluştur ve daha fazla yayılmaya ihtiyaç duymazlar. Casus yazılımın amacı kurban olarak seçilen sistem üzerinde gizli kalarak istenen bilgileri toplamaktır. Casus/köstebek yazılımları, kişisel gizliliğe karşı gerçekleştirilen en tehlikeli kötü amaçlı yazılımlardandır (Canbek ve Sağıroğlu, 2007: 170).

Avrupa Birliği Ağ ve Bilgi Güvenliği Kurumu'na göre kötü amaçlı yazılımlar, siber tehditler arasında ilk sırada yer almaktadır. "ENISA 2015 Siber Tehdit Panoraması" raporu 2015 yılı araştırmasında incelenen kötü amaçlı yazılımların yirmi yıl öncenin Word, Excel Makroları gibi tehdit tekniklerini kullandığını komplike, karmaşık yöntemler yerine daha çok verimliliğe odaklandıklarının altını çizmiş, mobil platformlarda her geçen gün daha çok yaygınlaşan kötü amaçlı yazılımların bir önceki yıla göre %50 artış gösterdiğine vurgu yapılmıştır. Bu raporda kötü amaçlı yazılımlardan en çok etkilenen beş ülkenin; Bangladeş (%60), Vietnam (%60), Pakistan (%58), Moğolistan (%58), Gürcistan (%58) olduğu ve kötü amaçlı yazılımları barındıran, alan ve sağlayıcılığı yapan ülkelerin ise Rusya (%50), ABD (%12), Hollanda (%8), Almanya (%5) ve Fransa (%3) olduğu belirtilmiştir (Marinos vd., 2016: 20).

2.3.2.2. Web-Tabanlı ve Web Uygulamalı Siber Saldırılar

Günümüzde web teknoloji ve uygulamaları tarafından işlenen, derlenen, transfer edilen bilgiler; toplum, kurum ve kuruluşlar, hatta devletler için kritik ve stratejik bir varlık haline dönüşmüştür (Crist, 2007: 4-5). Bu yüzden web tabanlı sistemler, stratejik varlık olan bilgiyi; güvenli bir şekilde işlemeli, bilginin unsurlarına yönelik olabilecek herhangi bir tehdide karşı da verimliliği ve kullanılabilirliğini muhafaza ederek gerekli önlemler almalıdır.

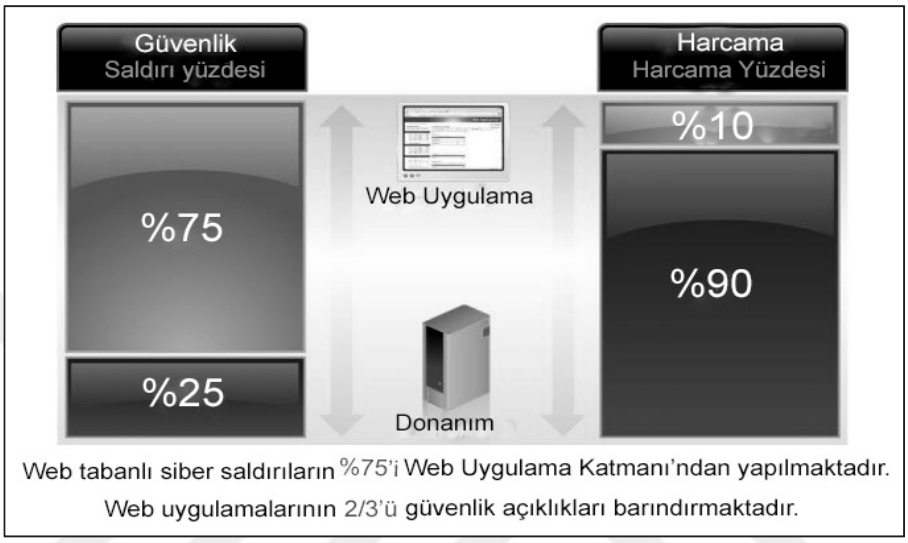
Web tabanlı siber saldırılar; uygulama katmanında gerçekleşir ve uygulamanın kendisine ve uygulamanın fonksiyonlarına odaklanır. Bu saldırılarda web bir platform olarak kullanılarak ve saldırının daha çok kurbana yayılması sağlanır (Crist, 2007: 5). Bu saldırılarda saldırgan genel olarak kötü amaçlı yazılımları web sunucusuna yüklemek için yazılım açıklıklarından faydalanmaya çalışır. Ve bu amacını gerçekleştirmek için hem web sunucularını hem de web istemcilerini, yani kullanıcıları hedef alır. Web-tabanlı siber saldırılara örnek olarak; zararlı internet adresleri (URL), saldırıya uğramış ve içeriği kötü amaçlı yazılımlarla enfekte olmuş web sunucularından yapılan saldırılar, web açık kapılarından ve tarayıcı güvenlik açıklarından yapılan saldırılar verilebilir (Marinos vd., 2016: 22).

"ENISA 2015 Siber Tehdit Panoraması" raporunda, web tabanlı siber saldırılara ABD'nin %40 oranında ev sahipliği yaptığı ve ABD'den sonra %8 ile Fransa, %6 ile Rusya ve %4 ile Almanya'nın geldiği belirtilmiştir. Ayrıca raporda bu saldırı türüne en çok maruz kalan ülkelerin; %30 ile ABD, %20 ile Japonya ve %4 ile Tayvan'ın olduğu ve bu durumun ülkelerin gelir seviyesi ve web altyapı bileşenlerinin kötüye karşı koruma durumu ile alakalı olabileceği ileri sürülmüştür (Marinos vd., 2016: 23).

Genelde meşru web siteleri kullanılarak söz konusu sitelerin kullanıcılarını hedef alan ve kurbanın bilgisayarına zararlı kod parçacıkları yüklemek, kullanıcı verilerinin istismarı şeklinde görülen bu saldırı türüne "Web Uygulama Saldırısı" denilmektedir. Web uygulama saldırılarında saldırgan, siber tehdit oluşturmayan web siteleri üzerinden (sosyal medya uygulamaları gibi) sunulan hizmetler aracılığı ile kurban bilgisayar sistemlerine erişmeyi amaç edinmiştir. Dolayısıyla saldırıya temel teşkil eden web uygulamasının zararsız olması hesabıyla bu tip saldırılar, web tabanlı saldırılardan ayrışmaktadır.

Web uygulama saldırılarının dünya genelinde %80'i ABD'de, %7'si Brezilya'da % 4'ü Çin'de, geri kalan %'9'u ise dünyanın diğer ülkelerinde görülmektedir. (Marinos vd., 2016: 25). Web uygulamalarına yapılan saldırılar, donanım tabanlı saldırılardan daha fazladır. Fakat kurumların web uygulamalarına yaptıkları harcamalar, donanım yatırımlarına yapılan

harcamalardan daha azdır. Örneğin Wei yapmış olduğu bir çalışmasında; kurumlara yönelik donanım tabanlı saldırıların %25 olmasına rağmen bu alana yapılan yatırım harcamalarının %90 olduğunu ve web uygulamalarına yapılan saldırılarının %75 olmasına rağmen yatırım oranının %10 olduğunu tespit etmiştir (Wei, 2016).

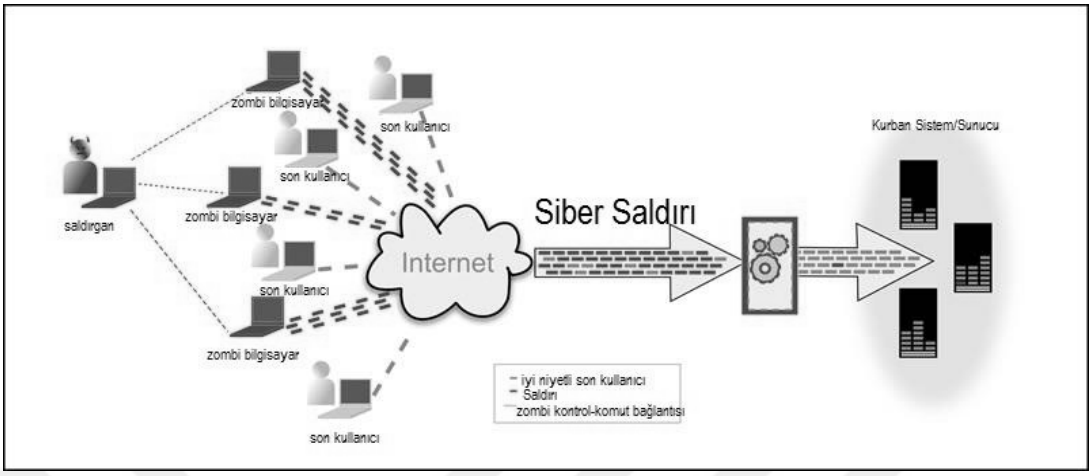


Şekil 14. Web Uygulama Saldırıları ve Donanım Harcamaları
Kaynak: Wei, 2016.

2.3.2.3. Botnet / Zombi Bilgisayar

Robotun kısaltması olarak kullanılan **"**bot**"** kelimesi ile ağın İngilizcesinin birleşiminden oluşan **"**botnet**",** siber güvenlik literatürüne *robotlaşmış, köleleştirilmiş, kontrolü başkasında olan bilgisayar ağı* olarak kullanılmaktadır. Kullanıcısının haberi olmadan zararlı yazılım yüklenen, kontrolü tamamen veya kısmen bilgisayar korsanlarının eline geçen ve kötü niyetli, yetkisiz kişi veya sistemler tarafından verilen siber saldırı görevlerini yerine getirmeye başlayan bilgisayarlara **"**zombi bilgisayar**"** adı verilmektedir. Zombi bilgisayarlar, siber saldırıların merkezinde bulunmasına karşın işlenen siber suça alet olduğunun farkında dahi olmayan cihaz ve sistemlerdir. Botnet veya zombi bilgisayar ağı siber saldırı altyapı bileşenlerinin en önemlilerinden biridir. Botnet ağı; komuta ve kontrol sunucuları ve yüzbinlerce enfekte olmuş, uzaktan yönetilebilen bilgisayarlardan oluşur (Marinos vd., 2016: 26).

Güncel ve yasal bir işletim sistemi ve güvenlik yazılımı sahibi olmayan, internette kaynağı belirsiz sitelerde gezinen ve bu sitelerdeki bağlantılara gelişi güzel tıklayan, bu bağlantılar vasıtasıyla indirmeler yapan, bilgisayarları belirli süreden sonra yavaşladığından şikâyet eden bireylerin bilgisayarlarının zombi bilgisayara dönüşmüş olma olasılığı yüksektir.



Şekil 15. Zombi bilgisayarlar ve siber saldırı

Kaynak: Avnet, 2016.

Kötü niyetli bilgisayar korsanları, illegal web siteleri üzerinden siber saldırılarda kullanılmak üzere zombi bilgisayar kiralayabilmekte, hatta saldırı fiilini tamamen taşeron olarak yerine getirebilmektedirler. Siber Suç Hizmet Kiralama *(Cybercrime-As-A-Service)* olarak adlandırılan bu suç hizmetinin 2015 yılı rakamlarıyla bir saatlik ücretinin 20 $ ile 40 $ arasındadır. Zombi bilgisayarlar kullanılarak gerçekleştirilen siber saldırılarda, Amerika Birleşik Devletleri, Ukrayna, Rusya, Hollanda, Almanya, Türkiye, Fransa, Birleşik Krallık, Vietnam ve Romanya'nın saldırı kaynağı olarak kullanılan ilk on ülkedir (Marinos vd., 2016: 27).

2.3.2.4. Hizmet Dışı Bırakma (Denial of Service – DOS)

Hizmet Dışı Bırakma Saldırısı; BT sistemlerinin yasal kullanıcılarına sunduğu bilişim hizmetlerinin kötü niyetliler tarafından erişilemez hale getirilmesidir. Hizmet dışı bırakma, en çok tercih edilen siber saldırı türlerinden birisidir (Vacca, 2006: 12). Bilgi hırsızlığı veya hedef alınan BT sistemlerine sızmadan çok, BT sistemleri tarafından sunulan hizmetin geçici veya tamamen hizmet veremez hale getirilmesini amaçlamaktadır. Teknik bilgi gereksiniminin az oluşu ve etkisinin fazlalığından dolayı "Dağınık Hizmet Dışı Bırakma Saldırısı" *(Distributed Denial of Service Attack - DDOS)* olarak da bilinmektedir. Bu saldırılarının genel özellikleri;

- Genellikle Botnet / Zombi Bilgisayar Ağı kullanılarak yapılır.
- Binlerce hatta milyonlarca bilinçsiz botnet bilgisayar kaynak olarak kullanılır.
- Hedef olarak genellikle itibar kaybına uğratarak finansal zarar vermek amaçlanır.
- Saldırının arkasındaki kişi veya kişileri bulmak neredeyse imkânsızdır.

Verisign 2016 İkinci Çeyrek Hizmet Dışı Bırakma Saldırı Eğilimleri Raporu (Verisign, 2016) (The Verisign Distributed Denial of Service (DDoS) Trends Report 2016 Q2) 2015 ve 2016 yılı için rapor edilen DOS saldırılarını temel alarak, saldırılarda;

- Önceki yıllara göre daha büyük çapta ve daha sık aralıklarla yapıldığına,
- Ortalama saldırı boyutunun % 214 daha büyük boyutta gerçekleştiğine,
- Saldırıların % 64'ünün birden fazla saldırı yöntemi ve tekniği kullandığına,
- % 45'inin bilişim teknolojileri ve bulut bilişim teknolojilerini,
- % 23'ünün finansal sistemleri,
- % 14'ünün de kamu kurum ve kuruluşlarını hedef aldığına vurgu yapıldığı görülmektedir.

2.3.2.5. Fiziksel Zarar / Hırsızlık / Kayıp

İlk bakışta oldukça önemsiz bir tehdit gibi algılansa da BT sistemlerinin gizlilik, bütünlük ve erişilebilirliğe zarar veren fiziksel tehditler, teknik bir saldırı olmamasına karşın önemli bir tehlikedir. Fiziksel tehditler özellikle kamu sektöründe bilgi güvenliği ihlallerinde, ilk ihlal şekli olarak karşılaşılmaktadır. Kamu kurumlarında fiziksel zarar veya cihaz kaybı %50 seviyelerindedir.

ENISA 2015 Siber Tehdit Panoraması raporunda; 2014 yılında fiziksel tehditler 10'uncu sırada iken 2015 yılında bu tehditler altıncı sıraya yükselmiştir (Marinos vd., 2016: 30).

Şekil 16. Fiziksel Tehditler

Kaynak: Radikal Gazetesi, 2016.

2.3.2.6. İç Tehdit

İç tehdit; BT sistemlerinde çalışanlar, iş ortakları veya hizmet taşeronlarından kaynaklanabilecek kasıtlı veya kasıtsız siber tehditler olarak tanımlanabilir. Bilişim sistemleri hakkında teknik olarak yeterli olmayan, daha çok iş için kullandığı uygulamaların sağladığı yetkilerden faydalanan çalışan veya iş ortaklarının, siber saldırı yöntem ve metotları kullanmadan oluşturduğu kasıtlı iç tehditler çoğunlukla uygulama katmanında gerçekleşmektedir (Salem,vd., 2008: 70-77).

ENISA 2015 Siber Tehdit Panoraması raporuna göre iç tehditler; siber tehdit sıralamasında 2014 yılında 11'inci sırada iken 2015 yılında 7'inci sıraya yükselmiştir. İç tehdit kaynakları; mevcut veya eski çalışanlar, iş ortakları, danışmanlar, tedarikçiler, müşteriler olarak sıralanabilir. İç tehdit oluşmasındaki nedenler (Marinos vd., 2016: 32);

- Hassas veriler ile ilgili çalışanların dikkatinin azalması,
- Güvenlik kural ve politikalarını uygulamak için yeterli eğitimin sağlanmaması,
- İş yükünden dolayı bilgi güvenliğin önemsenmemesi,
- Çalışanların bilgi güvenliğini ciddiye almaması,
- Bilgi güvenliği kural ve politikalarının ek iş yükü getirmesi.

2.3.2.7. Oltalama (Phishing)

Kullanıcıya tanıdık, bilinen, güvenilir, meşru, olağan gibi görünerek kullanıcının eylemde bulunmasını sağlamaya yönelik geliştirilen ve kullanıcı eylemi ile harekete geçerek, kullanıcının bilişim cihaz ve sistemlerine zararlı yazılımlar ve kod parçacıkları yükleyerek bilgi çalma işlemlerinin bütününe oltalama denilmektedir.

Oltalamanın temel amacı kurbanın bilgilerini çalmak veya kurban sisteme zararlı yazılımlar yüklemektir. Oltalamada, sahte güveni tesis etmek adına kurbana tanıdık olaylar, güvenilir kuruluşlar, markalar, hizmetler, kendi tanıdığı kişilerinden geldiği izlenimi oluşturan e-postalar, web sayfaları ve reklamlar şeklinde algı yanılması yapılarak, kullanıcının bu e-posta ve web adreslerindeki bağlantılara tıklaması sağlanır. Kullanıcı eylemi ile beraber zararlı yazılımlar kurban sisteme yüklenir veya kurbanın dijital verileri çalınır (Marinos vd., 2016: 33).

2.3.2.8. İstenmeyen e-posta (Spam)

BT kullanıcıları tarafından istenmediği halde, istem dışı gönderilen e-posta mesajlarına "istenmeyen e-posta" veya *"spam"* denilmektedir. En eski siber tehditlerden biri olan istenmeyen e-postalar, günümüzde siber suçlular tarafından kullanılan en önemli tehdit yöntemlerinden biridir.

İstenmeyen e-posta, 1990'lı yıllarda reklam maksadıyla aynı anda binlerce hatta milyonlarca kişiye, maliyeti çok düşük reklam ulaştırmak adına kullanılırken, günümüzde reklam faaliyetleri yanı sıra kötü niyetli bilgisayar korsanları tarafından, kurbanlarının bilgi sistemlerine zararlı yazılımları yüklemek ve bilgi hırsızlığı yapmak için kullanılmaktadır.

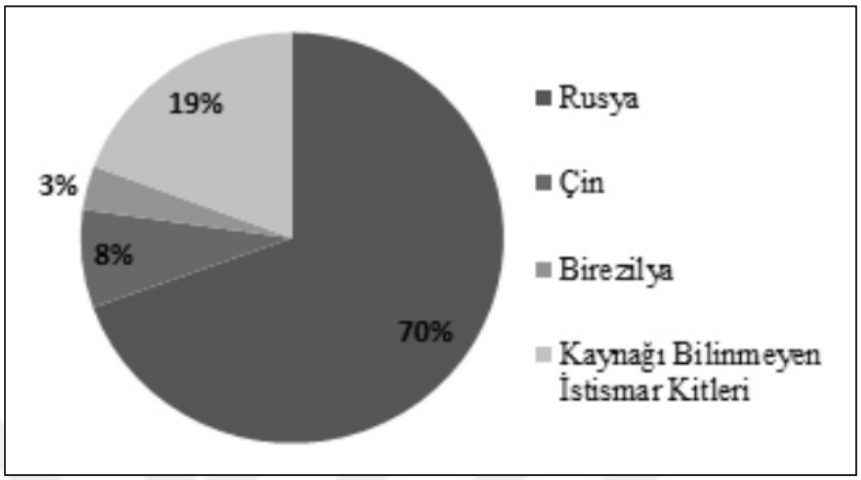
ENISA 2015 Siber Tehdit Panoraması'nda, istenmeyen e-posta oranlarında bir önceki yıla göre düşüş olduğunu belirtilmiştir. İstenmeyen e-posta iletilerinin, tıpkı diğer siber tehditlerde olduğu gibi ticareti yapılmakta ve hizmet olarak kötü niyetliler tarafından satılmaktadır. Örneğin; 1000 adet çalıntı e-posta adresi 0,5-10 dolar arasında satıldığı, istenmeyen bir e-postanın, adresleri doğrulanmış bir milyon kullanıcıya iletiminin 70-100$'a yapıldığı bilinmektedir (Marinos vd., 2016: 36).

2.3.2.9. İstismar Kiti (Exploit Kits)

İstismar Kitleri; siber güvenlik bağlamında oldukça tehlikeli, sık kullanılan ve hedef sistemlere yönelik saldırıları otomatize etmek için oluşturulmuş, içerisinde hedef sistem üzerinde bulunan siber güvenlik açıklarından yararlanmaya yönelik geliştirilmiş kötü amaçlı kodları ve diğer saldırı bileşenlerini barındıran, mantıksal bir siber saldırı aracıdır (Küçüksille vd., 2014).

İstismar kitleri için çoğunlukla yazılım uzmanlarının yazılım geliştirme esnasında yaptıkları hatalardan faydalanılır. Bu hatalar "sıfırıncı gün açıkları" (zero day vulnerability) olarak ifade edilmektedir. Bu açıklıklar yazılım üreticileri tarafından bilinmediği ve yazılım üreticisinin bu açıkları kapatmak için zamanı olmadığından dolayı "sıfırıncı gün açıkları" denilmektedir. Sıfırıncı gün açıklarını ihtiva eden istismar kitleri, bazı internet sitelerinden ücretsiz olarak kolayca temin edilebildiği gibi daha gelişmiş ve güncel istismar kitlerinin alım satımı da yapılmaktadır. İstismar kitleri kullanılarak çok gelişmiş BT sistemlerine bilgisiz bir saldırgan tarafından siber saldırı düzenlenebilmekte ve hedef sistem zarar görebilmektedir. Dolayısıyla BT sistemlerinin "sıfırıncı gün açıkları"na karşı güncellemelerinin yapılması ve gerekli olmayan yazılım ve uygulamaların, veri barındıran kritik olan sistemlere yüklenmemesi gerekmektedir. İk istismar kiti 2005 yılında üretilmiş ve bazı ülkelerde istismar kiti üretimi bir

sektör haline gelmiştir. İstismar kitinin üretiminde; birinci sırada % 70 oran ile Rusya, % 8 ile Çin ve % 3 ile Brezilya yer almaktadır (Küçüksille vd., 2014).



Şekil 17. İstismar Kiti Kaynak Ülkeler

Kaynak: Küçüksille vd., 2014.

Çok tehlikeli bir siber saldırı aracı olan istismar kitleri ile yapılan siber saldırılarda, , 2015 yılında bir önceki yıla oranla % 67 artış gözlenmiştir. Ayrıca 2015 yılında rapor edilen saldırıların % 80'i üç ülkeye yapılmıştır. Japonya (%50), Amerika Birleşik Devletleri (%22) ve Avusturalya (%6) en çok istismar kiti saldırısına maruz kalan ülkelerdir (Marinos vd., 2016: 37).

2.3.2.10. Veri İhlalleri (Data Breaches)

Kişi, kurum ve kuruluşların iş ve işlemleri için kritik öneme sahip siber varlıklarının gizlilik, bütünlük ve erişebilirliğinin siber saldırılar sonucunda yetkisiz kişiler tarafından ele geçirilmesi "veri ihlali" olarak ifade edilmektedir. Diğer bir deyişle; korumalı, hassas veya gizli bilgilerin, yetkisiz ve izinsiz kişiler tarafından kopyalanması, bir yerlere iletilmesi, görülmesi, incelenmesi veya çalınması bir veri ihlalidir (ABD Sağlık Hizmetleri, 2016).

Dünyada birçok ülke, kurum ve şirket, düzenli periyotlarda veri ihlalleri raporları yayımlamaktadırlar. Veri ihlallerinin ilgili taraflara bildirilmesi için ABD'de kırk yedi eyalet ve Columbia Bölgesi ve ABD'ye bağlı özerk toprak statüsünde bulunan Guam, Porto Riko ve Virgin Adaları "Güvenlik İhlalleri Bilgilendirme Kanunu" çıkarmış, kamu ve özel sektör ile eğitim şirketleri, kurum ve kuruluşlarının meydana gelen siber güvenlik vakalarını duyurması zorunlu hale getirilmiştir (NCSL, 2016).

Türkiye'de siber istismarların nasıl ve nereye bildirilmesi gerektiğine dair 6698 Sayılı Kişisel Verilerin Korunması Kanunu 12. maddesinin 5. fıkrasında "İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgilisine ve Kişisel Verileri Koruma Kuruluna bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir" şeklinde ifade edilmektedir. Diğer bir kanun ise; 5809 Elektronik Haberleşme Kanunu'nun 60. maddesine eklenen 10. fıkradır. (Ek: 15/8/20165-KHK-671/25 md.) "Bilgi Teknolojileri ve İletişim Kurumu, kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerin siber saldırılara karşı korunması ve bu saldırılara karşı caydırıcılık sağlamak için her türlü tedbiri alır veya aldırır" şeklinde düzenlenmiştir. Ayrıca, "Sermaye Piyasası Kanunu"nda borsaya kayıtlı şirketlerin payların değerini etkileyecek seviyede bir olayı borsaya bildirme zorunluluğu yer almaktadır. SPK m.15 (1)'e göre "Sermaye piyasası araçlarının değerini, fiyatını veya yatırımcıların yatırım kararlarını etkileyebilecek nitelikteki bilgi, olay ve gelişmeler, ihraççılarca veya ilgili taraflarca kamuya açıklanır". Bu hükümde "güvenlik vakaları" açıkça belirtilmemektedir. Aslında hüküm soyut ve genel olup kapsadığı hiçbir duruma örnek vermemektedir. KAP'a siber güvenlik özelinde herhangi bir bildirim zorunluluğuna rastlanmadığından, ülkemizde gerek sermaye piyasası ile bağlantılı, gerekse bundan başka kaynağı teyit edilebilir herhangi bir veri ihlali istatistiğine ulaşılması mümkün olamamaktadır. Mevcut durumda bu konudaki tek veri kaynağı bazı siber güvenlik olaylarına ilişkin olarak yerel ve ulusal basında çıkan haberlerdir.

Veri ihlallerinin, telafisi çok zor olan kayıplara neden olduğu bir gerçektir. Bu kayıpları itibar kayıpları ve finansal kayıplar olarak ikiye ayırmak mümkündür. Veri ihlalinden kaynaklanan itibar kaybı ve itibar kaybını gidermek adına atılan adımlar, teknolojik adımlar, davalar, halkla ilişkiler bağlamında yapılan harcamalar, satış ve hizmetlerdeki azalmalar ve kar oranlarının azalması, itibar kaybı yanında finansal kayıpları da beraberinde getirmektedir (Hemphill ve Longstreet, 2016: 30-38).

Avrupa Birliği üyesi ülkelerinde veri ihlallerinin 2015 yılı için tahmini finansal bedeli büyük ölçekli işletmeler için firma başına 2.000.000-4.300.000 €, küçük ölçekli işletmeler içinse 100.000-430.000 € olduğu rapor edilmiştir (Marinos vd., 2016, s. 40). Diğer bir çalışmada, Amerikan perakende devi Target'ın 70.000.000 müşterisine ait kişisel bilgilerin, bilgisayar korsanları tarafından çalınmasının gerçek finansal ve itibar kaybının ölçülememesine rağmen, itibar kaybını telafisi adına yapılan çalışmaların firmaya maliyetinin 450.000.000-500.000.000 $ olduğuna vurgu yapılmıştır (Hemphill ve Longstreet, 2016: 30-38).

2.3.2.11. Kimlik Hırsızlığı

Kişisel verileri hedef alan siber saldırıların sonucunda gerçekleşen kimlik hırsızlığı, her tür kişisel bilginin çalınması olayını ifade eder. Örneğin; BT kullanıcılarının bu sistemleri kullanmak için kullandıkları kullanıcı bilgileri ve şifreler, kullanıcı veya BT sistemlerinden faydalananların kişisel bilgileri, isim, adres, telefon, kredi kartı, vb bilgiler kimlik hırsızlıkları olabilir. "Amerikan Milli Standartlar ve Teknoloji Enstitüsü" (NIST) kişisel kimlik bilgilerini, (personally identifiable information - PII) kişinin tam adı, ev adresi, e-posta adresi, (varsa bir dernek/kulüp üyeliği, vb.) ulusal kimlik numarası, pasaport numarası, IP adresi (bazı durumlarda), araç tescil plaka numarası, sürücü belgesi seri numarası, yüz, parmak izi ya da el yazısı, kredi kartı numaraları, dijital kimlik, doğum tarihi, doğum yeri, cinsiyeti, telefon numarası, bilgisayar kullanıcı adı olarak tanımlamaktadır (NIST, 2010). Kimlik hırsızlığında, çalınan bilgi bir kişiye ait olduğundan, kötüye kullanım durumunda diğer siber güvenlik vakalarının aksine, bu kişi doğrudan olumsuz etkilenmektedir.

Türkiye'de "Kişisel Verilerin Korunması Kanunu" 7 Nisan 2016 tarihinde resmi gazetede yayınlanarak yürürlüğe girmiş ve kanunun genel gerekçesi kişisel veriyi; "bireylerin kimliklerini belirli hale getirmeye elverişli her türlü bilgi" olarak tanımlamakta ve "kişinin kimlik, iletişim, sağlık ve mali bilgileri ile özel hayatına, dini inancına ve siyasi görüşüne ilişkin bilgilerin kişisel veri olarak nitelendirileceği" ifade edilmektedir.

İstatiksel verilere bakıldığında; 2014 yılına oranla 2015 yılında kimlik hırsızlığı bakımından tehdit seviyesinin "durağan" olduğu ve en çok kimlik hırsızlığının sağlık sektöründe (% 33) gerçekleştiği anlaşılmaktadır. Sağlık sektörünü % 15 ile perakende ve % 13 ile kamu kurum ve kuruluşlarından çalınan kişisel veriler takip etmiştir (Marinos, cd., 2016: 41).

2.3.2.12. Bilgi Sızıntısı

"Bilgi sızıntısı" BT sistemlerinden kötüye kullanım, hileli işlemler veya teknik aksaklıklar sebebiyle, farkında olunamayacak kadar az miktarlarda sızdırılan veridir. Söz konusu sızıntı sadece nicel olarak değil, aynı zamanda niteliğinden dolayı veri ihlalinden farklı olmasından dolayı ayrı bir siber tehdit olarak ifade edilmektedir.

Teknik bileşenlerin yetersizliğinden veya BT uygulamalarının işlevlerinin bozulmasına bağlı olarak meydana gelen bilgi sızıntısı, bir sistemin bilgisayar korsanları tarafından ele geçirmesinde bir adım olarak kullanılmaktadır. Bilgi sızıntısını, "kurban BT sistem ve hizmetleri üzerine, sistemin bilgisayar korsanları tarafından ele geçirmesi amacıyla yerleştirilen ve çok

yavaş ve zamana yayılarak çalışan zararlı yazılımlar" şeklinde tanımlamak mümkündür (Marinos vd., 2016: 43).

BT sistemleri ve bu sistemler tarafından barındırılan, işlenen, iletilen bilgi ve bu bilgilere ait meta verilerin (veri hakkında veri / bilgi) kasıtlı veya yanlışlıkla olması gereken kişi veya sistem haricinde bir yerlere zamana yayılarak ulaşması işlemi, "Bilgi sızıntısı" olarak ifade edilmektedir.

2.3.2.13. Fidye Yazılımları (Ransomware)

Fidye Yazılımları ile bilginin erişilebilirliğini engelleyerek, bilgi sahibinden bu erişimi tekrar sağlaması için ödeme talebinde bulunulmaktadır. Bu tür yazılımların tek amacının, kurbanı zor durumda bırakarak ödeme yapmasını sağlamak olduğu söylenebilir. Fidye yazılımları; BT kullanıcısının cihaz veya bilgisayarındaki bilgileri şifreleyerek kullanılamaz hale getirirler. Söz konusu şifreleme için karmaşık kriptoloji teknikleri kullanılmakta olup, kurbanın bilgilerini geri elde etmesi veya zararlı yazılım kaynağının bulunması günümüz teknolojisi ile neredeyse imkânsızdır. Kripto edilmiş bilginin geri dönüşü, sadece kriptografik şifrenin kullanımı ile mümkün olduğundan, bu şifre saldırganlar tarafından yüksek paralar karşılığında kurbana iletilmekte, saldırgan ve kurban arasında iletişim de genelde "Karanlık/Derin İnternet" üzerinden sağlanmaktadır. Ödemeler ise Bitcoin (dijital para) olarak yapıldığından, saldırganların tespiti yapılamamaktadır (Öcüt, 2016).

Şekil 18. Fidye Virüsü Ekran Görüntüsü

Kaynak: Öcüt, 2016.

Siber güvenlik araştırması yapan kurum ve kuruluşlar araştırmalarında 2015 yılına "Fidye Yazılım Yılı" adını vermişler, bu tehdidin bir önceki yıla göre % 100 artış gösterdiğini ve hali hazırda artmakta olduğunun altını çizmişlerdir. Fidye yazılım aracılığı ile yapılan istismarlarda Avrupa ve Amerika Birleşik Devletleri % 50 ile başı çekmektedirler. Diğer yandan, fidye yazılımların; % 50 oranı ile son kullanıcıları, % 25 oranı ile büyük işletmeleri, % 14 ile küçük ve orta ölçekli işletmeleri hedef aldığı görülmektedir (Marinos vd., 2016: 45).

2.3.2.14. Siber Casusluk

Siber casusluk, "bilgi toplamak maksadıyla BT sistemlerinin izinsiz ihlali" olarak tanımlanmaktadır (Brown ve Poellet, 2012: 133). ABD Savunma Bakanlığı Teknik Bilgi Merkezi; BT sistemlerinde bulunan güvenlik açıklarından faydalanarak siber uzayda korumalı halde bulunan bilginin yasa dışı ve gizli bir biçimde toplanması faaliyetlerini" siber casusluk olarak tanımlamaktadır (DTIC, 2012: 4).

Siber casusluk; devletler veya rakip firmalar tarafından birbirleri arasında, belli bir amaç doğrultusunda veya gelişigüzel olarak bilgi/istihbarat toplamak amacıyla, BT sistemleri kullanılarak siber varlıkların kendileri hakkında veya üzerinde depolanan bilgiye gizli bir şekilde erişim sağlama faaliyetlerinin bütünü şeklinde tanımlanabilir. Literatürde, her türlü yetkisiz erişimin siber casusluk kapsamında değerlendirip değerlendirilmeyeceği konusunda araştırmacılar farklı fikirlere sahiptir (Brown ve Poellet, 2012).

Siber casusluğun karakteristikleri aşağıdaki şekildedir;

- Kesinlikle gizlidir.
- Hiçbir zaman varlığı yapanlar tarafından kabul edilmez.
- Devletlerin doğrudan veya dolaylı katılımı vardır.
- BT sistemleri aracılığı ile yapılan istihbarat faaliyetlerinden oluşur.
- Çok uzun zaman, çok kalifiye insan gücü ve para gerektiren faaliyetlerdir.
- Fidye yazılımlarının aksine, gerçek ve tüzel kişilere doğrudan ve hemen etkisi olan faaliyetler değildir.
- Siber casusluk faaliyetleri sonucunda toplanan bilginin siber saldırılarda veya başka amaçlarla kullanılması mümkündür.
- Amaç genellikle askeri, siyasi veya ekonomik olmaktadır.

2.3.2.15. Gelişmiş Siber Tehdit (APT-Advanced Persistent Threat)

"Gelişmiş Siber Tehdit" veya "Gelişmiş Israrcı Tehdit" olarak Türkçe'ye çevrilen "Advanced Persistent Threat" siber saldırı türlerinin içinde, bilinen en karmaşık saldırı şeklidir. Bu saldırı türü diğer tehdit yöntemlerine kıyasla çok farklı olup, alanında uzman kişilerin uzun ve karmaşık çalışmaları sonucunda meydana çıktığı söylenebilir. İran'ın nükleer santraline zarar vermek amaçlı geliştirilen Stuxnet, "Gelişmiş Siber Tehdide" örnek gösterilebilir.

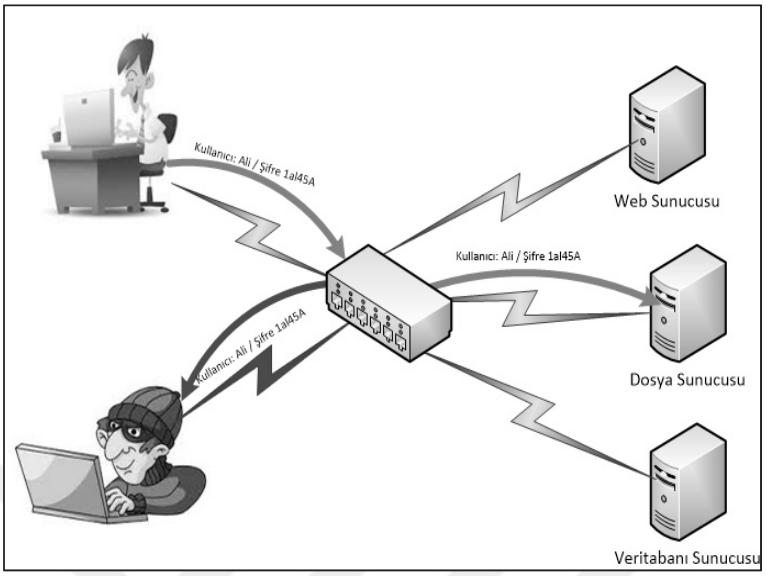
Bilinen örneklerine bakılarak gelişmiş siber tehdit konusunda şu çıkarımlar yapılabilir:

- Bir veya birkaç hedef için özel üretilmiş zararlı yazılım kodcuklarıdır.
- Üretim aşaması zorlu ve uzmanlık gerektirir.
- Farklı alanlardan (bilişim, elektronik, askeri, istihbarat, makine, vb.) uzmanların katılımı ile hazırlanır.
- Devletler tarafından finanse edilen bu saldırıda, başka devlet ve kurumları hedef alınır.
- Hedef sisteme kalıcı olarak yerleşir ve bilgi çalma, sistemi çalışamaz hale getirme gibi hedeflere yöneliktir (Kara, 2013).
- Tespiti ve müdahalesi neredeyse imkânsızdır (Lachow, 2013).

2.3.2.16. Ağ Dinleme (Network Sniffing)

Ağ Dinleme veya "ağ koklama", aslında ağ yöneticilerine ağ sorunlarını araştırmalarında, performans problemlerini çözmelerinde yardımcı olarak geliştirilmiş bir araçtır. Saldırganlar ağ dinleme araçlarını kullanarak, ağ hakkında bilgilere ulaşır ve ağ üzerinden geçen şifre, kullanıcı bilgilerini elde ederler (BM Uluslararası Telekomünikasyon Birliği , 2008).

Ağ dinleme araçlarının hem iyi hem de kötü amaçlara hizmet ettiğinden bahsedilebilir. İyi niyetli bir ağ uzmanı, hâlihazırda devam eden ağ sorunlarını, söz konusu ağı dinleyerek tespit etmeye çalışabileceği gibi, devam eden bir siber saldırının özelliklerini öğrenmek ve bertaraf etmek için de ağ dinlemesi yapabilir. Diğer taraftan, kötü niyetli bir bilgisayar korsanı tarafından ağ dinlemesi, hedef alınan siber varlığa erişmek, kontrol altına almak, zarar vermek, bilgi çalmak veya diğer siber saldırı yöntemlerinden hangisinin seçileceğine karar vermek için başvurulan bir yöntem olabilmektedir.



Şekil 19. Ağ Dinleme

Kaynak: SSL Shop, 2016.

2.3.2.17. ARP Zehirlenmesi (ARP Poisoning)

ARP Zehirlenmesi; ağ cihazlarında cihazların yerel ağda birbirleri ile iletişimin daha hızlı ve güvenli olarak sağlanması adına kayıt altına alınan MAC ve IP adres bilgilerinin bulunduğu tabloların saldırganlar tarafından manipüle edilerek iletişime zarar verilmesi veya kötü amaçları için kullanılmasıdır.

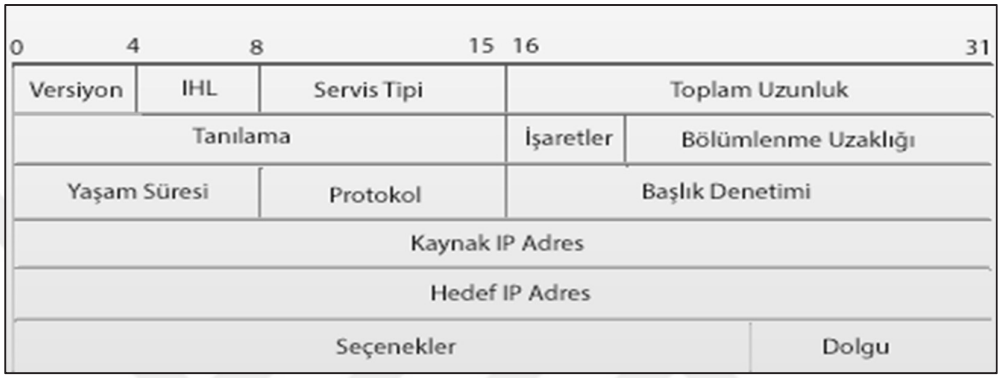
ARP tablolarında IP-MAC eşleşme bilgileri muhafaza edilir ve yerel ağdaki herhangi bir cihaz diğer bir cihazla iletişime geçmek isterse, önce bu tablolardan karşı cihazın MAC adresini sorgular. Hedef cihazın IP ve MAC adresleri ARP tablosunda mevcut ise iletişim başlar, mevcut değil ise kaynak cihaz ARP isteği göndererek ARP tablosunda bu kaydın oluşmasını talep eder ve iletişim bu kaydın oluşmasına bağlı olarak başlar.

Saldırganlar ARP zehirlenmesi ile kendine ait, saldırı için kullanacağı bilişim ekipmanlarının adreslerini bu tabloya yazarak, güvenilen başka bir cihaz gibi davranır ve trafiğin kendi üzerinden geçmesini sağlayabilir. Bu yöntem, erişim kısıtlamalarını aşmak için de kullanılabilmektedir.

2.3.2.18. IP Aldatması (IP Spoofing)

IP Aldatması, gönderen ve alıcının güven ilişkisinden yararlanan karmaşık bir saldırı türüdür. Kurban güven ilişkisi kurduğu alıcı ile veri alışverişi yaptığını sanır, ancak saldırgan kurbanın kimliğini kullanarak saldırısına maskeleme yapmaktadır. İnternette bilgiler, paketler

şeklinde transfer edilmektedir. Her bir pakete ait bir "başlık" bulunmakta, bu başlıklar IP protokolünün unsurlarını beraberinde taşımaktadır. Bu unsurlardan biri de "Kaynak IP" adresidir. Kötü niyetli kişiler, bu kaynak adresini değiştirerek kimliklerini gizlemekte ve saldırılarını bu değiştirme işleminden sonra başlatmaktadır. Bu işleme "IP aldatması" denilmektedir (BM Uluslararası Telekomünikasyon Birliği , 2008).



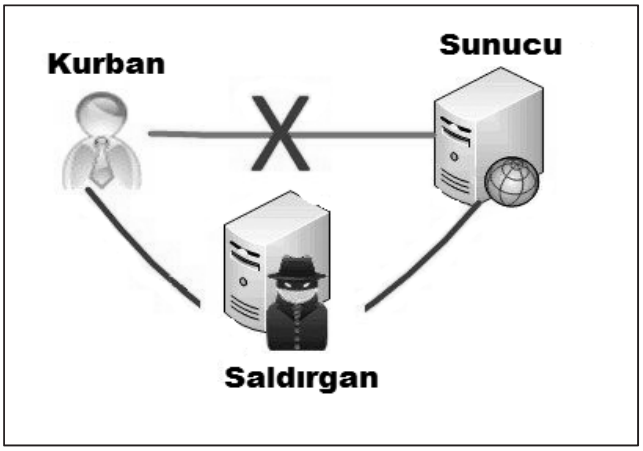
Şekil 20. IP Paket Başlığı

Kaynak: McMaster Universitesi, 2016.

2.3.2.19. Ortadaki Adam Saldırısı (Man in the Middle Attack),

İletişim kuran her siber varlık, iletişim kurmak adına veri gönderme ve alma için çeşitli ağlarla bağlantı kurmaktadır. Bu ağlar aracılığı ile kurulan iletişimin saldırgan tarafından manipüle edilerek kendi cihaz ve bilgisayarları üzerinden geçmesini sağladığı yöntem "Ortadaki Adam Saldırısı" olarak bilinmektedir.

Ortadaki adam saldırısında saldırgan, kurbanının BT trafiğini olağan yoldan gitmesini engeller ve trafiğin kendi üzerinden geçmesini sağlayarak dinler. Bu yöntem, genellikle kurbana ait dijital verilerin çalınması için kullanılmakta olup sunucu tarafı veya kurban iletişimin devam ettiğinden dolayı, genellikle, saldırıdan haberdar olmazlar.



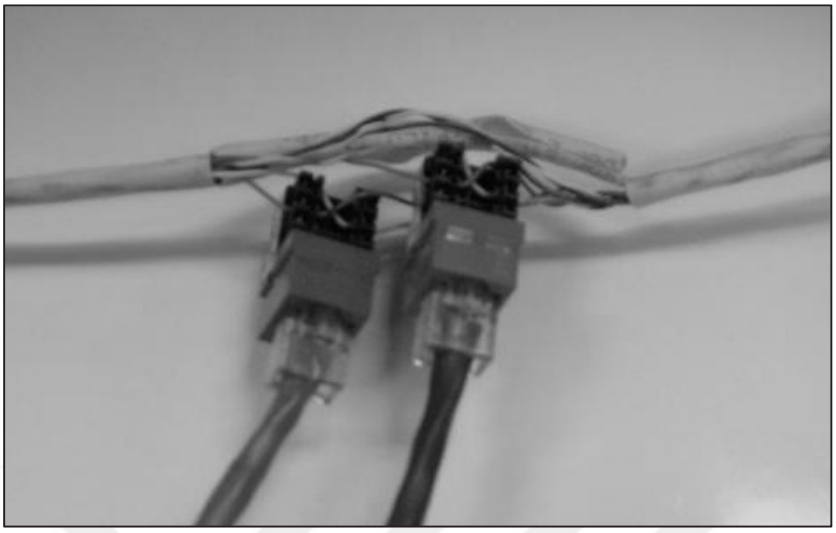
Şekil 21. Ortadaki Adam Saldırısı
Kaynak: Scott, 2016.

2.3.2.20. Kabloya Saplama Yapma (Wire Tapping)

"Kabloya Saplama Yapma" yöntemi, bir fiziksel siber saldırı yöntemidir. Bu saldırı için saldırganın ağ kablolarına erişimi olmalıdır. Saldırgan bu yöntemle, siber varlıkların iletişimi için ikame edilmiş olan ağ kablolarına müdahale ederek, ağ üzerinden geçen BT trafiğini dinler ve şifrelenmemiş veya basit yöntemlerle şifrelenmiş ağ trafiğini ele geçirir.

Pasif saplama olarak da ifade edilen Kabloya Saplama Yöntemi sadece metal kabloların kullanıldığı ağlarda yapılabilmektedir. Fiziksel saplama yapılabilmesi için ağ teknolojisinin 10/100 Mbps olması gerekir. Gigabit ağlarda bu yöntemin çalışmadığı ve saldırganlar tarafından ağ kablolarından kahverengi ve/veya mavi olanların kesilmesi durumunda, ağın hızı otomatik olarak 10/100 Mbps'e düşeceği için kablo tamamen kesilerek iletişimin engellenmesi bir yöntem olarak kullanılmaktadır (Karunaratne, 2016).

Teknolojinin her geçen gün daha da ilerlediği günümüzde, kabloya saplama yönteminin bir istismar yöntemi olarak kullanılıp kullanılmadığı, çeşitli ağ test cihazları (Time Domain Reflectometer) ile tespit edilebilmektedir. Bu tür cihazlar aslında metal kabloların kullanıldığı ağlardaki arızaları bulmak için geliştirilmiş olmasına rağmen saplama yapılan yeri tam olarak verebilmektedir (Karunaratne, 2016).



Şekil 22. Kabloya Saplama Yapma

Kaynak: Karunaratne, 2016.

2.3.2.21. Sosyal Mühendislik

Siber saldırı amaçlı "Sosyal Mühendislik" "saldırganların kurban hakkında erişebildikleri sosyal ve kültürel verileri toplayarak, siber saldırılarda kullanmak üzere, kurbana ait bilgisayar sistemleri ve ağlarına erişim sağlamak için, çeşitli sosyal hilelere başvurması" olarak tanımlanmaktadır (Erbschloe, 2005). "Sosyal Mühendislik", siber saldırganlar tarafından, siber saldırı öncesinde, saldırı esnası ve sonrasında veya planlanan saldırıyı aktif etmek için yapılan eylemler bütünü olarak ifade edilmektedir. Örneğin, saldırganın, kurbanın kullandığı bilgisayarın özelliklerinin ne olduğunu, sosyal medyada paylaştığı bir fotoğraftan yola çıkarak, üzerinde çalışan işletim sisteminin örneğin Windows olduğunu bulması, bir sosyal mühendislik çalışması olup, saldırısını Windows tabanlı işletim sistemleri üzerine yoğunlaştırmasıdır.

Bilgisayar korsanları ve kötücül yazılımları geliştirmekle uğraşanlar için, uzun süreler kurban sistemlerine izinsiz erişebilmek için yapılan çalışmalara kıyasla kurbana ait şifreyi çeşitli hilelerle edinmek daha kolay olduğundan, bu amaçla yapılan sosyal mühendislik çalışmaları siber saldırganların en güçlü silahıdır (Mitnick ve Simon, 2003).

2.3.3. Siber Güvenlik Vakaları

Günümüzde her an siber saldırıların meydana geldiği bilinen bir gerçektir. Bu saldırıların bazıları kamuoyu tarafından hiç bilinmemesine karşın bazı saldırılar basın organlarında geniş yer bulmaktadır. Aşağıda karşılaşılan bazı saldırılar açıklanmıştır.

Estonya Vakası: İkinci Dünya Savaşında Nazilere karşı verilen mücadeleyi temsilen Rusya tarafından Estonya'ya dikilen bir heykelin, Estonya tarafından kaldırılmasından sonra ülkeyi hedef alan birtakım siber saldırılar gerçekleşmiş ve Estonya'nın bankaları, e-devlet sistemi, internet hizmetleri çok büyük zararlar görmüş, ülkenin internet altyapısı tamamıyla çökme tehlikesi ile karşı karşıya kalmıştır (Bakır, 2011).

Gürcistan Saldırısı: Gürcistan'ın Rusya ile tüm ilişkilerini kesmesi ve çok ağır kayıplar vererek kısmi kontrolü altında bulunan Güney Osetya'yı tamamen kaybetmesi ile sonuçlanan "2008 Güney Osetya Savaşı" ile eş zamanlı olarak Gürcistan'ın siber sistemleri hedef alınmıştır. Gerçekleştirilen siber saldırılarda Gürcistan'a ait web siteleri ve bu siteler tarafından sağlanan hizmetler erişilemez hale gelmiştir (Gürkaynak ve İren, 2011: 271).

Kırgızistan Saldırıları: Kırgızistan'ın başkenti Bişkek'te bulunan ve ABD'ye ait olan Manas Üssü'nün kapatılması hakkında karar alan ve karar sonrası ABD ile askeri üssün tekrar kullanıma açılması hakkında müzakereler yapan Kırgızistan, müzakereler akabinde siber saldırılara hedef olmuş ve ülkede hizmet veren dört internet sağlayıcısının verdikleri internet hizmetleri % 80 oranında verilemez hale gelmiştir. Saldırıların üs kurulmasına ilişkin müzakerelerin hemen ardından gelmesi, şüphelerin Rusya üzerine yoğunlaşmasına sebep olmuştur (Bakır, 2016).

Stuxnet Vakası: Bir tür endüstriyel virüs olarak ifade edilen Stuxnet, türünün bilinen ilk örneğidir. Stuxnet, hedefini belirli bir coğrafi konumda arayıp imha etmeye programlanmış çok gelişmiş bir siber saldırı aracıdır. İlk kez Haziran 2010'da fark edilen Stuxnet, İran'da bir nükleer santralde üretimde kullanılan cihazları hedef almış ve söz konusu nükleer santrali çalışamaz hale getirdiği çeşitli medya organlarında yer almıştır (Gürkaynak ve İren, 2011: 273).

Türkiye'ye Yapılan Saldırılar: Mayıs 2010 tarihinde çeşitli din ve millete mensup kişiler, İsrail'in Gazze'ye uyguladığı ambargoyu delmek için "Mavi Marmara" adlı Türk bayraklı gemi ile insani yardım ulaştırmak adına çıktıkları yolda, uluslararası sularda İsrail'in saldırısına uğramışlardır. Gemide bulunan gönüllülerin iletişim sağlamak ve gelişmeleri dünya medyasına canlı ulaştırmak için kullandıkları uydu frekansları ve uydu telefonlarının iletişimi saldırı öncesinde kesilmiştir.

Türk Hava Kuvvetlerinin Rusya'ya ait bir savaş uçağını Türk Hava Sahasını ihlali nedeniyle düşürmesi olayını takiben, Türkiye, 14 Aralık 2015'te başlayıp haftalarca süren siber saldırılarla karşı karşıya kalmıştır. Saldırılar süresince birçok çevrim içi hizmete erişilememiş, bankalar, noterler ve çeşitli web hizmetlerinde aksaklıklar meydana gelmiştir.

2.4. Siber Güvenliğin İşletmeler İçin Önemi

Birçok firma ve kuruluş, siber güvenlik olayları ve bu olaylardan kaynaklanan kayıplarını, birçok nedenden dolayı açıklamamaktadır. Bu nedenlerin başında, olumsuz reklam ve itibar kaybı gelmektedir (Richardson, 2011; Hoffer ve Straub, 1989: 35-43; Panko, 2009). Whitman; siber güvenlik bağlantılı gerçek kaybın bulmasının imkânsız olduğu ve çeşitli çalışmalarda yer alan maliyetlerin gerçek maliyetin çok küçük bir bölümü olduğunu belirtmektedir (Whitman, 2003: 91-95). Siber güvenlik konusunda literatür incelendiğinde, yapılan çalışmaların ağırlıklı olarak borsaya açık ve siber saldırılar hakkında borsaya bilgi verilmesi gereken ülkelerde bulunan işletmelerde yapıldığı ve şirketlerin ekonomik kayıplarını incelediği gözlemlenmektedir (Campbell vd., 2003: 433; Cavusoglu vd., 2004: 69-104).

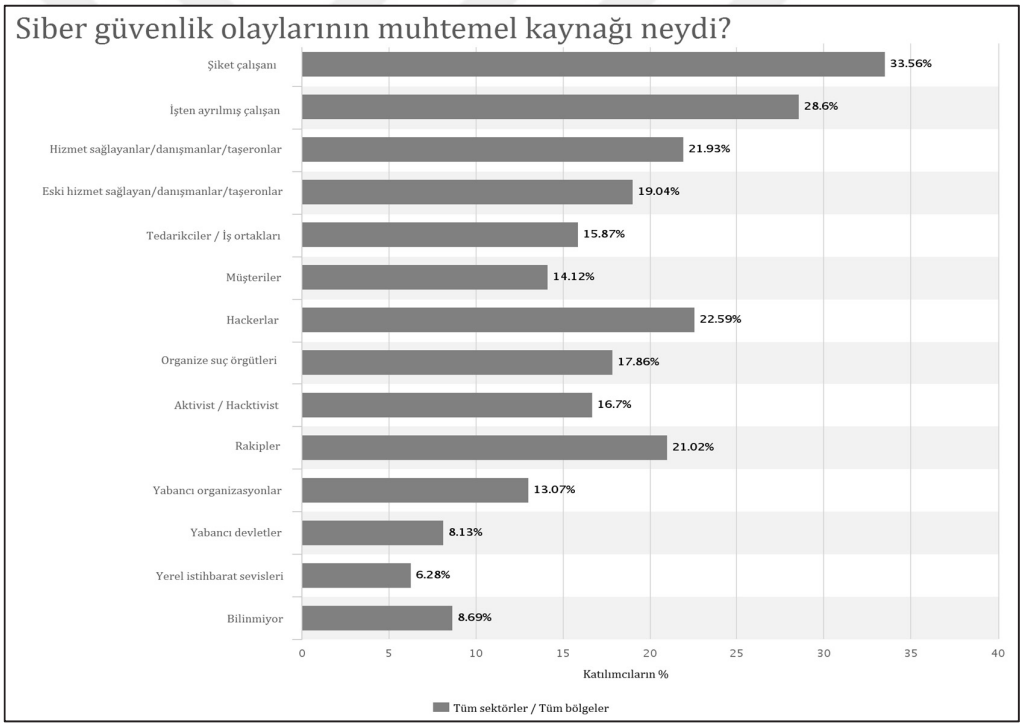
Yayla ve Hu; siber saldırıların birçok firmayı siber güvenlik alanında yatırım yapmaya zorladığı ve bilişim bütçelerinin ön sıralarında yer almaya başladığının altını çizmiştir (Yayla ve Hu, 2011: 61). İşletmelerin siber güvenlik alanındaki yatırımları, doğru yönde atılmış birer adımdır. Fakat bu yatırımların toplam BT bütçelerindeki payı maalesef çok azdır. 2014 yılında şirketler toplam BT bütçesinin % 4-6'sını siber güvenliğe ayırmışken, 2016 bütçelerinde bu oranın % 7-9'a çıktığı görülmektedir (Filkins, 2016:6).

Fiziksel varlıklarının/değerlerinin güvenliğini bir şekilde sağlayan işletmelerin, aynı şekilde siber varlıklarının da güvenliğini sağlaması, işletmeler acısından hayati öneme sahiptir. Bazı ülkelerde, örneğin ABD'de, siber değerlerin önemi her seviyede yöneticiler tarafından gündeme getirilmekte ve bu alanın fiziksel güvenlikle eş değer hatta daha önemli olduğu vurgulanmaktadır. "Amerikan Siber Ordu Komutanlığı" (USCYBERCOM) komutanı General Keith Alexander, "Siber sistemler aracılığı ile yapılan fikri mülkiyet hırsızlığını tarihte görülen en büyük zenginlik transferi" olarak ifade etmiştir. Alexander; fikri mülkiyet hırsızlığının Amerikan firmalarına yıllık ortalama maliyetinin 250.000.000.000 dolar olduğunu, siber suçlarla bağlantılı ekonomik kaybın 114.000.000.000 dolar ve bilişim sistemlerinin hizmet veremediği süre de eklendiğinde toplam kaybın 338.000.000.000 doları bulduğuna vurgu yapmış ve Amerika'da hâlihazırda kullanılan siber sistemlerin güvenli olmadığını belirmiştir (Rogin, 2012).

2014 yılında Amerikan halkının % 47'sinin siber saldırılara maruz kaldığı, 2013 yılında ise Amerikan şirketlerinin % 43'ünün veri ihlaline bir ve birden fazla hedef olduğu rapor edilmiştir. Yakın geçmişte "Target", "Home Depot" ve "JP Morgan Chase" gibi büyük Amerikan şirketlerinin müşteri verilerinin korunması bağlamında yaşadıkları sıkıntılar basın organlarında yer almıştır (Ponemo Institute Research, 2015). 2015 yılı için üç yüz elli şirket ve on bir ülkeyi

kapsayan IBM ve Ponemo Enstitüsünün beraber hazırladıkları "Veri İhlali Maliyet Çalışmasında" (Cost of Data Breach Study)*;* ortalama veri ihlali maliyetinin şirketlere son iki yıl için % 23 artışla 3.790.000 dolara ulaştığı belirtilmiştir (Ponemo Institute Research, 2015).

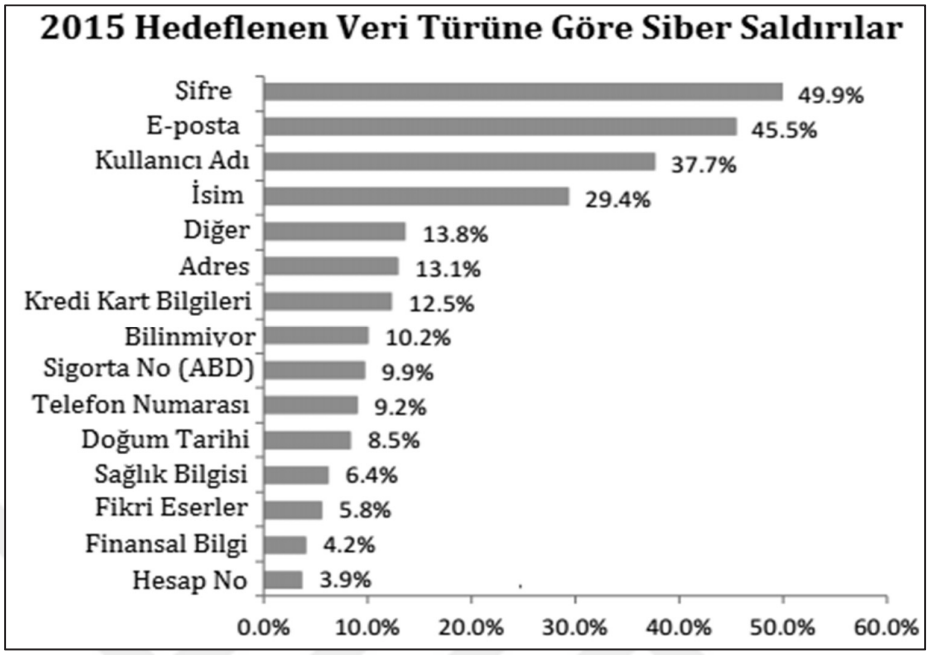
PwC tarafından yüz yirmi yedi ülkede, on binin üzerinde üst düzey yönetici, CEO ve genel müdür üzerinde yapılan "2016 Bilgi Güvenliği Araştırması"na göre; bir önceki yıla göre siber güvenlik vakalarında % 38 artış gözlemlenmiştir. Raporda, bu saldırılar karşısında şirketlerin yeterli kalifiye elemana sahip olmadıkları ve sofistike saldırılara karşı "tespit ve önleme" mekanizmalarının yetersiz olduğuna vurgu yapılmıştır. Raporda ayrıca, üst düzey yöneticilerin, yoğun BT kullanımına ve bu platformlarda barındırılan verilerin her zamankinden daha fazla risk oluşturduğuna yer verilmiştir (PwC, 2016).



Şekil 23. PwC Siber Güvenlik Olaylarının Muhtemel Kaynağı

Kaynak: PwC, 2016.

Risk Based Security 2015 raporunda, veri ihlal türlerinde % 49,9 ile şifre ihlalleri ve % 45,5 oranında e-posta alakalı ihlaller gelmektedir (Risk Based Security, 2015).



Şekil 24. 2015 Hedeflenen Veri Türüne Göre Siber Saldırılar

Kaynak: Risk Based Security, 2015.

Siber güvenlik konusunda karşılaşılan en büyük sıkıntı, özgürlükler ile güvenliğin dengelenmesidir (Weimann, 2006). Bu bağlamda organizasyonlar, BT kullanıcılarına ihtiyaçları düzeyinde erişim yetkileri tanımlamalı ve tanımlanan yetkiler periyodik aralıklarla gözden geçirilerek güncellenmelidir.

2.5. Siber Güvenlik Standartları

Teknolojiyi kullanım oranının artması, siber varlık kullanım ve sahiplenme oranlarını da artırmaktadır. Siber varlıkların doğrudan veya dolaylı olarak maruz kalabileceği herhangi bir siber tehdit, BT güvenliğinin ihlaline ve çeşitli zararlara maruz kalmasına neden olabilir. Dijital tehdit ve riskler günümüzde kişi ve kuruluşlar için her geçen gün daha fazla tehlike oluşturmaktadır. Kişiler gündelik hayatlarında çevrim içi birçok hizmetten faydalanmakta, gündelik işlerini bu olmazsa olmaz sistemler aracılığı ile yapmaktadırlar. Kişilerin kendi siber varlıklarının güvenliği önem arz etmekle birlikte, etkileşimde bulundukları ve bilgi girişi yaparak hizmetlerinden faydalandıkları kurum ve kuruluşlara ait sistemlerin siber güvenliği çok daha önemlidir. Bazı yazarlar kurumsal siber varlıkların güvenliği sağlanmadan kişisel siber varlıkların güvenliğinin sağlanamayacağına dikkat çekmektedir (Vural ve Sağıroğlu, 2008: 521).

Akıl almaz bir hızda gelişen tehdit ve risklerle mücadelede, kişisel kabiliyetler kifayetsiz kalmakta; geliştirilen yetersiz mücadele yöntemleri beraberinde başka tehditleri

barındırabilmektedir. Günümüzün siber tehditleri ile mücadele ve riskleri en aza indirebilme konusunda uluslararası kabul görmüş bilgi güvenliği/siber güvenlik standartlarının uygulanması elzemdir. Her sektörde olduğu gibi, bilgi güvenliği/siber güvenlik alanında da uluslararası kabul görmüş standartlar ile bu standartları düzenleyen ve güncelleyen organizasyonlar bulunmaktadır. Bu standartlar siber tehditlerle mücadele ve siber varlıkların korunması çalışmalarında temel köşe taşları arasındadır. Bilgi sistemleri yönetimi alanındaki standart ve kılavuzlar, bilgi/siber güvenlik standartları ve bilişim sistemleri yönetişim standartları olmak üzere iki kategoride incelenebilir (Arora, 2016). Bu standartlara;

- Bilgi/Siber Güvenlik standartları:
  - ISO 27000 serisi standartlar, (daha önceden ISO/IEC 17799 olarak bilinenler)
  - NIST 800 serisi standartlar,
  - SOX,
  - ISF,
  - SOGP,
  - Risk IT,
- Bilişim Sistemleri Yönetişim standartları:
  - COBIT,
  - COSO,
  - ITIL, standartları için örnek verilebilir.

Bu çalışmada; bilgi güvenliği ve BT sistemlerinin yönetişimi standartlarından, en sık karşılaşılan ISO 27000 serisi standartlardan ISO 27001 ve ISO 27002 ile COBIT ayrıntılı olarak incelenecektir.

Siber güvenlik bağlamında "Uluslararası Standartlar Teşkilâtı" (ISO) tarafından geliştirilen ISO 27000 serisi standartlar; organizasyonlarda bilgi güvenliğinin sağlanması amacıyla uygulanacak metot ve pratikleri, ayrıntılı adımlar şeklinde ele alan ve risk yaklaşımını da kapsayan güvenli veri alışverişi ve iletişimi hedefler.

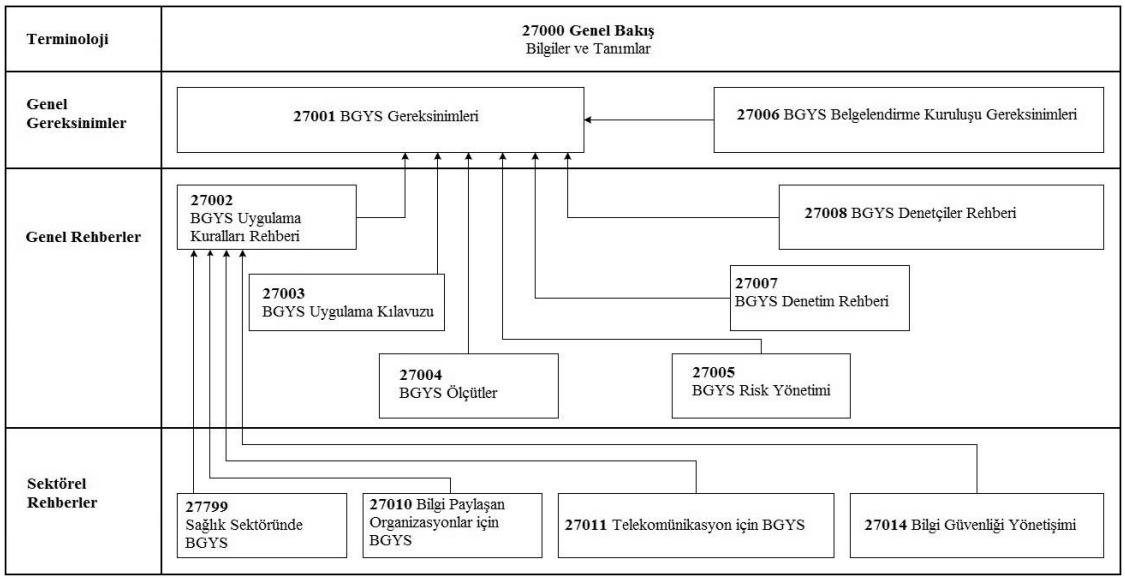
COBIT ise her ne kadar bünyesinde bilgi güvenliği konusunda kılavuzlar barındırsa da, daha çok BT sistemleri yönetişiminim doğru şekilde yapılması ve iyileştirilmesi hedefine odaklandığı, buna karşı teknik ayırtılara girmediği söylenebilir. COBIT, kaynaklar, altyapılar, süreçler, sorumluluklar ve kontrol olarak bölümlediği yönetişim çerçevesini, en iyi şekilde yönetmeyi amaç edinmiştir. Bu iki standardizasyon benzer özellikleri olmasına rağmen, COBIT güvenlik boyutunu çok detaya inmeden incelemekte, ISO 27001'in ise güvenlik boyutunu daha

detaylı incelemektedir (Arora, 2016). Bu iki standardizasyon grubunu inceleyen diğer bir çalışmada Solms, COBIT'in bilgi güvenliği bağlamında nelerin yapılması gerektiği konusunda iyi bir kılavuz olmasının yanında, bu gerekliliklerin nasıl yapılacağı konusunda detay barındırmadığından, kısır kaldığının üzerinde durmuştur (Solms, 2005: 99-102).

Bilişim teknolojileri ile alakalı standartların, diğer standartlarda olduğu gibi, çeşitli versiyonlarının olduğu göz önünde bulundurulmalıdır. Örneğin; COBIT 4 güvenlik boyutunu çok fazla ele almamasına karşın COBIT 5, gelişen eğilim ve teknolojilerin etkisiyle çok daha fazla güvenlik politikası barındırmaktadır.

2.5.1. Uluslararası Standartlar Teşkilâtı ISO 27000 Standartlar Serisi

Bilgi, işletmelerin faaliyetlerini sürdürebilmesi, rekabet edebilmesi ve hatta gelecekte var olabilmesi adına stratejik öneme sahip bir varlıktır. ISO 27000, kuruluşlar için stratejik öneme sahip bilgi varlıklarının yönetilmesi ve korunması için "Uluslararası Standartlar Teşkilatı" tarafından geliştirilen bir standartlar serisidir. ISO 27000 serisi standartlar, Bilgi Güvenliği Yönetim Sistemi (Information Security Management System) gereksinimlerini tanımlayan, söz konusu gereksinimleri sağlamak için hangi güvenlik denetimlerinin yeterli ve orantılı bir şekilde yerine getirilmesi gerektiğini belirleyen, bünyesinde çeşitli kılavuz ve yönergeleri barındıran, sektörel denetimlerle zenginleştirilmiş bir denetim çerçevesi (framework) sunmaktadır (Huang, Farn, ve Lin, 2011: 625).



Şekil 25. ISO BGYS Standartlar Serisi

Kaynak: Huang, Farn, ve Lin, 2011: 625.

2.5.1.1. ISO 27001

İlk olarak "İngiliz Standartları Enstitüsü" (BSI) tarafından 1999'da BS7799-2 olarak yayınlanmıştır. "Uluslararası Standartlar Teşkilatı" tarafından ISO 27000 ailesi bünyesine adapte edilerek katılmış ve ISO 27001 olarak adlandırılmıştır. Bilgi sistemleri yönetimine odaklanmış olan ISO 27001 bünyesinde ISO 9000 Kalite Standartları benzeri standartları da barındırmaktadır. Bilginin güvenli ve emniyetli bir şekilde kullanılması, muhafazası ve iletilmesi için çeşitli uygulama ve pratikleri bünyesinde barındıran ISO 27001 "Bilgi Güvenliği Standardizasyonu"na odaklanmış ve en son 2013 tarihinde güncellenmiştir. ISO 27001 standardı yöneticilere bilgi güvenliği açıklarını ve boşlukları belirleyerek bu zaafları en iyi şekilde azaltma, riskleri minimize imkânı sağlar. ISO 27001'in diğer standart ve kılavuzların aksine, bilgi güvenliği alanına odaklandığından, kapsamının daha dar olduğu söylenebilir.

ISO 27001 dünya çapında tanınan ve kabul gören bir standarttır. Uluslararası ticarette aranır olan ve belgelendirme imkânı sağlayan bu standart, faydalananın bilgi güvenliğinin sağlamasına yardımcı olduğu gibi çeşitli fırsatlara da kapı açtığı bilinmektedir.

Türkiye'de 2015 yılında ISO 27001 sertifikası sahibi olan kuruluş sayısı iki yüz altmış sekizdir, Japonya'da bu sertifikaya aynı yıl içerisinde 8.240 kuruluş sahip olmuştur. Bugün ülkemizde toplam 1.178 kuruluş ISO 27001 sertifikası sahibi olduğu "Uluslararası Standartlar Teşkilatı" raporlarında yer almakta olup Avrupa ülkelerinde bu sayı 51.760'dır (ISO, 2015).

Tablo 2. ISO 27001 2015 Belgelendirme İlk 10 Sıralaması

1	Japonya	8240
2	Birleşik Krallık (İngiltere)	2790
3	Hindistan	2490
4	Çin	2469
5	Amerika Birleşik Devletleri	1247
6	Romanya	1078
7	İtalya	1013
8	Almanya	994
9	Tayvan	939
10	İspanya	676

Kaynak: ISO, 2015.

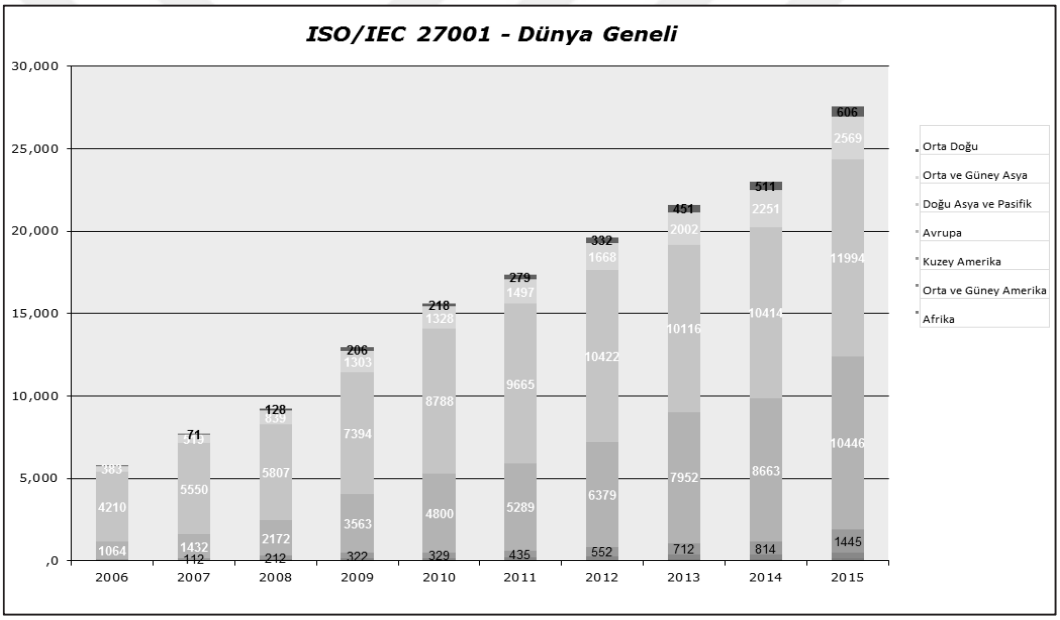
Bilgi teknolojilerinin, her geçen gün daha fazla kuruluş tarafından kullanıldığı bir gerçektir. Teknoloji kullanımındaki artışa paralel olarak kuruluşlar, BT tabanlı sistemlerinin güvenliğinin sağlandığından emin olmak adına ISO 27001 ve türevleri "siber güvenlik"

sertifikasyon ve yönetişim modellerini uygulamaktadırlar. Bilgi güvenliğinin sağlanması ve kontrolü bağlamında, en itibarlı sertifikasyon sistemi olarak kabul gören ISO 27001'in tüm dünyada ve Türkiye'de 2006-2015 yılları arasındaki istatistiklere bakıldığında artış gösterdiği gözlemlenmektedir.

Tablo 3. Türkiye'de Yıllara Göre ISO 27001 Sertifikasyonu

Yıl	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015
Türkiye	10	27	33	86	117	100	132	181	224	268

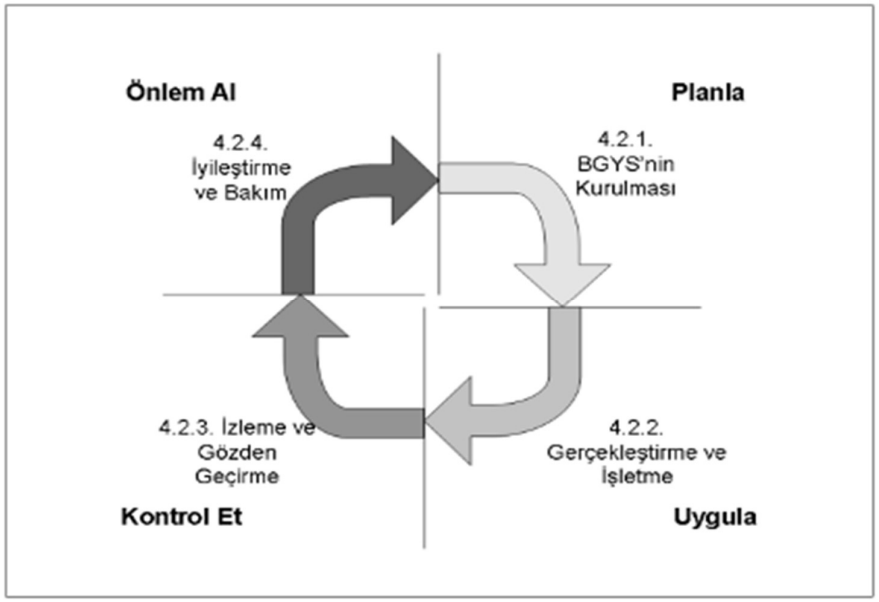
Kaynak: ISO, 2015.



Şekil 26. ISO 27001 Sertifikasyonu Dünya Geneli

Kaynak: ISO, 2015.

ISO 27001, siber güvenlik risklerini en aza indirmek için yüz on dört kontrol yöntemini, detaya girmeden sıralamaktadır. Aynı aileden olan ISO 27002:2013 ise bu kontrol yöntemlerinin nasıl uygulanacağını detaylı bir şekilde açıklamaktadır. ISO 27001 planlama, uygulama, kontrol ve önlem alma aşamalarından oluşan bir "bilgi güvenliği yönetim sistemi" olup yöneticilerin sorumluluklarına vurgu yapar. Bu görev ve sorumluluklar ISO 27001'de yer almasına karşın ISO 27002'de yer almaz, dolayısıyla bir kuruluş için ISO 27001 standardında belgelendirme, sertifikasyon mümkün olmasına karşın, 27002 sertifikasyonu mümkün değildir (Ottekin, 2016).



Şekil 27. ISO 27001 Standardında Bilgi Güvenliği Döngüsü

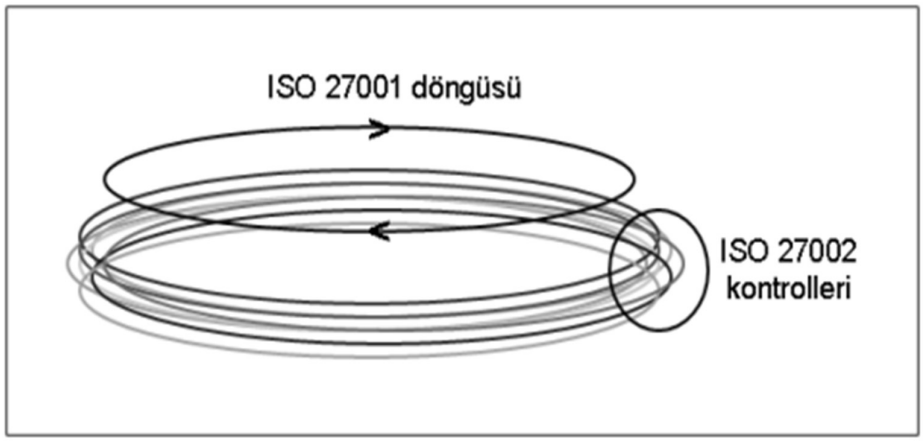
Kaynak: Ottekin, 2016.

ISO 27001 ve ISO 27002 birbirini tamamlayan standartlardır. ISO 27002 olmadan sadece ISO 27001'in Ek A'sında birer cümlede belirtilen kontrol yöntemleri ile uygulanması mümkün olmadığı gibi, ISO 27002'de yer verilen sayfalarca detaylarında yalnız başına tepe yönetimin katılımı olmaksızın uygulaması mümkün değildir.

2.5.1.2. ISO 27002

ISO 27002 seçim, uygulama ve risk faktörlerini dikkate alarak, yönetim kontrolleri bağlamında kurumsal bilgi güvenliği standartları ve bilgi güvenliği yönetimi kılavuzlarından meydana gelir. ISO 27002 aşağıda belirtilen amaçları hedef edinmiş kuruluşlar için tasarlanmıştır (ISO/IEC 27002, 2016):

- ISO/IEC 27001 dayalı bir "Bilgi Güvenliği Yönetim Sistemi" uygulama sürecinde kontrollerini seçmek;
- Yaygın olarak kabul edilen bilgi güvenliği kontrolleri uygulamak;
- Kendi bilgi güvenliği yönetim politikalarını oluşturmak isteyenler.



Şekil 28. ISO 27001 Döngüsü ve ISO 27002 Kontrolleri

Kaynak: Ottekin, 2016.

ISO 27001 standardında tarif edilen yönetim döngüsü, ISO 27002 standardından seçilen önlemler için hayata geçirilerek, bilgi güvenliği süreci gerçekleştirilmeye ve yaşatılmaya çalışılmakta, ISO 27002'de yer alan her önlem için ISO 27001 yönetim döngüsüne atıf yapılmaktadır. Dolayısıyla, ISO 27002 önlemleri, ISO 27001 ise bu önlemlerin nasıl hayata geçirileceği ve yaşatılacağını açıklamaktadır (Ottekin, 2016).

2.5.2. Bilgi ve İlgili Teknolojiler İçin Kontrol Hedefleri (COBIT)

COBIT (Bilgi ve İlgili Teknolojiler İçin Kontrol Hedefleri/Control Objectives for Information and Related Technology), ISACA (Bilgi Sistemleri Denetim ve Kontrol Birliği / Information Systems Audit and Control Association) tarafından ilk olarak 1996'da yayınlanmıştır.

COBIT; kuruluşların BT kaynaklarını, altyapılarını, süreçlerini, sorumlulukları, kontrolleri ve BT alanında en iyi uygulamaları bünyesinde barındıran bir denetim çerçevesidir. COBIT; Bilişim Teknoloji ve Sistemlerini örgüt bünyesinde doğru yerleşimine odaklanmış (Ridley vd., 2004: 8), teknik detaylardan daha çok kurumsal hedeflerle uyumlu BT süreçlerini yönetmeyi amaçlayan bir denetim çerçevesidir.

COBIT aşağıda sıralanan nedenlerden dolayı dünya çapında birçok kurum/kuruluş tarafından denetim çerçevesi olarak kabul görmektedir.

- Hızla değişen teknolojiden bağımsız olması,
- Diğer standart ve çerçevelerle (ITIL, COSO, ISO 17799, SOX) uyumlu olması,
- Denetim odaklı süreç tesisine yönelik entegre bir yaklaşım içermesi,

- Ölçme ve derecelendirme yöntemlerinin bulunması,
- Avrupa Birliği Bilişim Sistemleri Yönetişim mevzuatlarına uyumlu olması.

COBIT; BBDK (Bankacılık Düzenleme ve Denetleme Kurumu) tarafından BT denetim çerçevesi olarak kabul edilmiş ve tüm bankalara BT süreç ve yönetişim çerçevelerinde kullanılmak üzere zorunlu kılınmıştır. Ayrıca, Sayıştay ve Başbakanlık Yüksek Denetleme Kurulu tarafından da kullanılmaktadır (ISACA, 2016).

Arora'ya göre COBIT; diğer BT standartları ve kılavuzları ile beraber uygulanacak bir çözüme alternatif olarak, kendi içinde bütünleşmiş bir çözüm arayan BT yöneticileri için ideal bir denetim çerçevesidir. Ancak COBIT'in kontrol fonksiyonlarını gerçekleştirmek adına en büyük eksikliği "nelerin yapılacağına" cevap vermesine karşın "nasıl yapılacağına" dair bir kılavuzunun bulunmamasıdır (Arora, 2016). COBIT'in BT yönetişiminde etkili bir risk yönetimine sahiptir ve BT ile ilgili maliyetlerin finansal boyutlarını da kapsar ancak ISO 27002 sadece bilgi güvenliğine odaklanmıştır (Gehrmann, 2012: 68).

Tablo 4. COBIT – ISO 27001 Karşılaştırması

	COBIT	**ISO 27001**
Odak Konusu	Bütün olarak iş odaklılık ve BT yönetişimi	Risk faktörlerini göz önünde bulunduran güvenlik kontrollerinin uygulanmasını hedefleyen bir yönetim yaklaşımı
Yaklaşım	BT süreçlerinin planlanması	Bilgi güvenliği yönetim sistemi
Kapsam	Güvenlik planlamasını da kapsayan bütüncül BT yönetişimi	Bilgi güvenliği için tek başına denetim çerçevesi
Yapı	4 ana başlıkta 34 BT süreci: Planlama ve Organizasyon, Teknoloji Edinme ve Uygulama, Hizmet Sağlama ve Destek, İzleme ve Değerlendirme.	11 Bölüm ve alt hedeflerle desteklenmiş 36 hedef
Organizasyon Modeli	Tüm paydaşlar	Yönetim ve BT birimi
Sertifikasyon	Kuruluşlar için mümkün değil	Mümkün

Kaynak: Arora, 2016.

2.6. Siber Tehditlerle Mücadele Yöntemleri

Yapılan araştırmalar, siber tehditlerin ve siber tehditlere bağlı olarak kuruluşların karşı karşıya kaldıkları kayıpların her geçen gün daha da arttığını göstermektedir (Marinos vd., 2016; Verizon, 2016; Şentürk vd., 2012). Karşı karşıya olunan bu tehditler, yeterince incelenmeden yapılacak teknolojik yatırımların yetersiz kaldığı, istenen sonuçların elde edilemediği ve başarısızlıkla sonuçlandığı birçok araştırmada vurgulanmıştır (Dhillon ve Backhouse, 2001;

Baskerville, 1993; Straub ve Welke, 1998; Sisaneci vd., 2013). Siber güvenliğin sağlanması "ancak teknolojik ve yönetimsel mücadele unsurlarının harmanlanarak birbirini tamamlar şekilde uygulanması ile mümkündür" (Berghel, 2005; Sundt, 2006). Siber tehditlerle mücadele; ancak organizasyonel ve kurumsal nitelikler, yasal gereksinimler, en iyi sektörel uygulamalar ve güvenlik teknolojileri temel alınarak yapılabilir (Von Solms, 2000). Siber tehditlerle mücadelede anahtar unsur; teknolojik bileşenlerden ziyade organizasyonun kendisidir (Segev vd., 1998).

Her geçen gün daha da artan siber istismarlar ve oluşturduğu riskleri ortadan kaldırmak veya en azından kabul edilebilir düzeye indirgemek adına, siber tehdit artış oranına benzer şekilde bu tehditlerle mücadele için yöntem, araç ve denetim standartları geliştirilmektedir. Bazı mücadele yöntem ve araçlarının, uluslararası kabul görmüş kurum ve kuruluşlar tarafından, paydaşların kullanımına sunulan mücadele yöntem ve araçlarından bazıları aşağıda listelenmiştir.

Tablo 5. Siber Güvenlik Yöntem, Denetim Çerçevesi ve Kontrol Listeleri

Yöntem / Denetim Çerçevesi / Kontrol Listesi	**Hazırlayan Kurum / Kuruluş / Organizasyon**
Kurumlar İçin Siber Güvenlik Önlemlerini Ölçme Testi Dokümanı	UDBH (UDHB, 2016)
Kamu Kurumlarının Uyması Gereken Asgari Bilgi Güvenliği Kriterleri	UDBH (UDHB, 2016)
Güvenli Yazılım Geliştirme Temel Kuralları Dokümanı	UDHB (UDHB, 2016)
Kurumlar Tarafından Alınması Gereken Siber Önlemler	UDHB Haberleşme Genel Müdürlüğü (EK-1)
ISO 27001, 27002 ve diğer 27000 serisi çerçeveler	ISO (ISO/IEC 27002, 2016)
NIST Siber Güvenlik Denetim Çerçevesi	NIST (NIST, 2016)
DHS Sürekli İzleme ve Önleme Programı	ABD İçişleri Bakanlığı (DHS, 2016)
NSA-IAD Yönetilebilir Ağ Planı	ABD Bilgi Güvencesi (IAD, 2016)
Avusturalya "İlk Dört" Siber Önlem Yönergesi	ASD (ASD, 2016)
Birleşik Krallık (İngiltere) Siber Güvenlik için 10 Adım	Birleşik Krallık (UK-NCSC, 2016)
Birleşik Krallık (İngiltere) Siber Güvenlik Olmazsa Olmazları	Birleşik Krallık (UK Cyber Essentials, 2014)
Birleşik Krallık (İngiltere) ICO Bilgi Koruma Kılavuzu	Birleşik Krallık (UK ICO, 2016)
PCI DSS	Güvenlik Standartları Komisyonu (PCI SSC, 2016)
FFIEC Sınav El Kitabı	Federal Finans Enstitüleri Sınav Komisyonu (FFIEC, 2016)
COBIT 5	ISACA (COBIT, 2016)
NERC CIP	ABD Elektrik Güvenirliliği Kurumu (NERC, 2016)
Bulut Bilişim Güvenliği Birliği	CSA (CSA, 2016)
ITIL	AXELOS (ITIL, 2016)
Japonya Bilişim Güvenliği Portalı, çeşitli kılavuz ve testler	JP IPA (IPA, 2016)

Siber güvenlik kapsamında iyileştirmeler yapmak adına, paydaşların faydalanabilecekleri çok fazla kaynak bulunmaktadır. Kaynak bolluğu yöneticilere işlerini daha iyi yapmaları için birçok faydalı bilgiler sağladığı gibi, kafalarını karıştırabilecek derecede karmaşık ve çok boyut da içermektedir. Bu bağlamda; kaynakların gereksiz yere heba edilmemesi adına hangi siber tehdidin kurum/kuruluş için daha riskli olduğu çalışmasının yapılması elzemdir. Bir organizasyonun risk yönetimini aşağıda belirtilen dört adımda gerçekleştirilebilir (Baze, 2016: 5);

1. Risk tanımlarının yapılarak, kuruluşu hangi ölçekte etkileyebileceğinin belirlenmesi,
2. Risklerin ortadan kaldırılması, azaltılması veya farklı alanlara kaydırılması için öncelikli planların oluşturulması,
3. Oluşturulan planların uygulanması,
4. Paydaşların sürekli bilgilendirilerek, planların geliştirilmesi ve oluşabilecek açıklıkların kapatılarak güncellemelerin yapılması.

Şekil 29. Risk Yönetiminin Basit Bileşenleri

Kaynak: ISACA, 2015.

Yapılan araştırmalarda bir siber saldırının tespit edilebilmesinin ortalama yedi ay sürebildiğini ve BT sistemleri iyi yapılandırılmadığından bu saldırıların ancak % 3'ünün tespit edilebildiğini belirtilmektedir (Valenzuela, 2016). Bu yüzden siber güvenlik yönetiminin etkin ve verimli olması çok önemlidir. Siber tehditlerle mücadele; teknolojik yöntem ve araçlarla ile teknoloji dışı yöntem ve araçlarla mücadele olmak üzere iki ana kategoride incelenebilir.

2.6.1. Teknolojik Yöntem ve Araçlarla Mücadele

Klasik BT bileşenleri donanım, yazılım ve ağ olmak üzere üç katmandan oluşmaktadır. Bu üç katmana son yıllarda bulut bilişim katmanı da eklenmiştir. Tüm BT bileşenlerin

güvenliğini sağlamak tüm paydaşların üzerinde çalıştıkları kritik öneme sahip bir konudur. Söz konusu bileşenlerde meydana gelebilecek herhangi bir istismar, bilginin gizlilik, bütünlük ve erişebilirliğini zedeleyebilecek, çeşitli maddi manevi zararlarla karşı karşıya kalmasına neden olabilecektir. BT bileşenlerinin ayrıntılı şekilde planlanarak, oluşabilecek muhtemel istismarları oluşmadan engellemek için siber güvenlik bileşenlerin gereksinimlerinin ayrı ayrı ele alınması gerekmektedir (Yeh ve Chang, 2007; Ismail ve Zainab, 2011).

Sağlıklı bir BT altyapısı için, öncelikle, siber varlıkların *(Donanım, Yazılım, Ağ ürünleri),* fiziksel güvenliği sağlanmış bir ortamda konumlandırılması gerekmektedir. Fiziksel tehditlerin ortadan kaldırılması veya en aza indirilmesi, BT varlıkları üzerinde barındırılan veya bunlar üzerinden işlenen bilginin korunması için zaruridir. Bu bağlamda fiziksel önlemler;

- Erişim denetimi yapılan, fiziksel olarak korunaklı bir sistem odasının oluşturulması,
- Bu odayı nem, su, yangın, ısı açısından 7/24 gözleme imkanı sunan bir sistemin kurulması,
- Barındırılan donanımların enerji tüketiminin doğru hesaplanması ve enerji devamlılığını sağlayacak bileşenlerin doğru ve eksiksiz yapılandırılması (jeneratör, kesintisiz güç kaynağı vb.) gerekmektedir.

2.6.1.1. Donanım Güvenliği

Yiyecek ve içecekleri saklama şartları, bunları kullanma ömrünü etkilediği gibi, dijital varlıkların muhafazalarında donanım büyük rol oynar. Siber varlıklar için saklama, iletme ve işleme aracı olan donanımların, belli standart ve kalitede ve siber istismarlara karşı korunaklı olması, barındırılan siber varlığın barınma ömrünü ve koşullarını olumlu veya olumsuz etkileyecektir.

Donanım aracılığı ile meydana gelecek herhangi bir istismarın tespiti ve önlenmesi; zor, maliyetli ve zaman alır. Donanım, BT sistemlerinin manipüle yeteneğine sahip en ayrıcalıklı bileşenidir. Siber istismara karşı çeşitli araç ve yöntemlerin (virüs yazılımı, güvenlik yazılımları vb.) mevcut olduğu yazılım katmanı ile karşılaştırıldığında, daha az siber savunma araç ve yöntemi bulunur (Li vd., 2008).

Saldırganlar siber saldırılarda kullanmak üzere çeşitli donanım bileşenlerini klonlamakta ve saldırılarını bu manipüle edilmiş bileşenlerden faydalanarak gerçekleştirmektedir (Karri vd., 2010: 42). Klonlama genel olarak, bir donanımın bire bir kopyalanması olup saldırganlar tarafından RFID ödeme sistemleri başta olmak üzere (HGS, OGS, manyetik kartlar vb.) biletleme

ve güvenli belgelerin (pasaport vb.) birebir aynısını oluşturmak için kullanılmaktadır (Kong ve Li, 2013: 34).

Donanım düzeyinde yapılan siber saldırıları önlemede bir takım yöntem, teknik ve cihazlar geliştirilmiştir (Jang-Jaccard ve Nepal, 2014: 977). Dış müdahalelere dirençli donanım aygıtları olarak adlandırılan bu tür cihazlar, (HSM - Hardware Security Module - Donanımsal Güvenlik Modülü) Türkiye'de e-fatura uygulamalarında kullanıldığı gibi bazı büyük şirket ve bankalar tarafından da tercih edilmektedir. Bu tür cihazlar, kritik uygulamalarda sağladıkları kolaylıklar ve ileri seviye güvenlikten dolayı tercih edilmektedirler.

Günümüzde donanımlar, fonksiyonlarını üzerlerinde gömülü bulunan bir işletim sistemi veya firmware denilen kod parçacıklarını çalıştıran yongalar sayesinde yerine getirirler. Bu kod parçacıkları o cihazı yönetmek için üreticisi tarafından tasarlanmış ve geliştirilmiş yazılımlardır. Söz konusu bu yazılımlar, bünyelerinde yazılım hataları barındırabildiği gibi bazı durumlarda da üreticisi tarafından donanımın daha verimli çalışması, daha güvenli olması bağlamında yazılım güncellemeleri gerektirirler. Bu güncellemelerin yapılmaması veya geç yapılması ihlale neden olabilecek ve bu cihazları istismara karşı savunmasız kılacaktır. BT sistemlerinde kullanılan birçok donanım, kullanıcılara, kendilerinden beklenenden daha fazla fonksiyon sunabilmektedir. Fabrikasyon yapılandırmasında aktif olarak satışa sunulan bu özellikler, BT yöneticileri tarafından devreden çıkarılarak, oluşabilecek muhtemel bir istismarın önüne geçilebilir. Çünkü yapılandırması doğru ve ihtiyaçlar düzeyinde olmayan donanım konfigürasyonları, muhtemel tehditlere açık kapılar açabilmektedir.

2.6.1.2. Yazılım Güvenliği

Yazılım bileşenleri siber istismarla en çok karşı karşıya kalan BT unsurudur. Yazılım geliştirenlerin dikkatsizliği veya kasıtlı olarak yazılım bünyesine yerleştirilen ve yazılım açıklıkları olarak tabir edilen hatalar (software bug), siber saldırı amaçlı erişimi sağlama ve hedef sistem üzerindeki bilgiyi istismar için kullanılmaktadır. Yazılım açıkları; yazılımlarda meydana gelebilecek hata, kusur, arıza veya kasti durumları tanımlamak için kullanılan ortak bir tabirdir (Shahriar ve Zulkernine, 2012). Bu açıklıklar siber saldırılarda kullanılmaktadır. Günümüzde gerçekleşen siber saldırıların ekseriyeti yazılım açıklıkları üzerinden yapılmaktadır (Liu ve Cheng, 2009: 15).

Yazılım açıkları ile mücadelede, kurulu işletim sistemi ve sair yazılımlar için üreticileri tarafından çıkarılan güncellemelerinin zamanında yapılması önemlidir. Bu güncellemeler, üretici

tarafından ürün piyasaya sürüldükten sonra fark edilen açıklık ve zafiyetleri kapatmak ve sistemi daha güvenli hale getirmek için yayınlanmaktadır. Donanımda olduğu gibi bazı yazılımlar da üreticiden standart yapılandırmalar ile gelmektedir. Yazılımların kullanılmayan özellik ve fonksiyonların iptali veya sistemden kaldırılması, sistemin bu özellik veya fonksiyonlardan dolayı istismardan korunması bakımından önem taşımaktadır.

2.6.1.3. Ağ Güvenliği

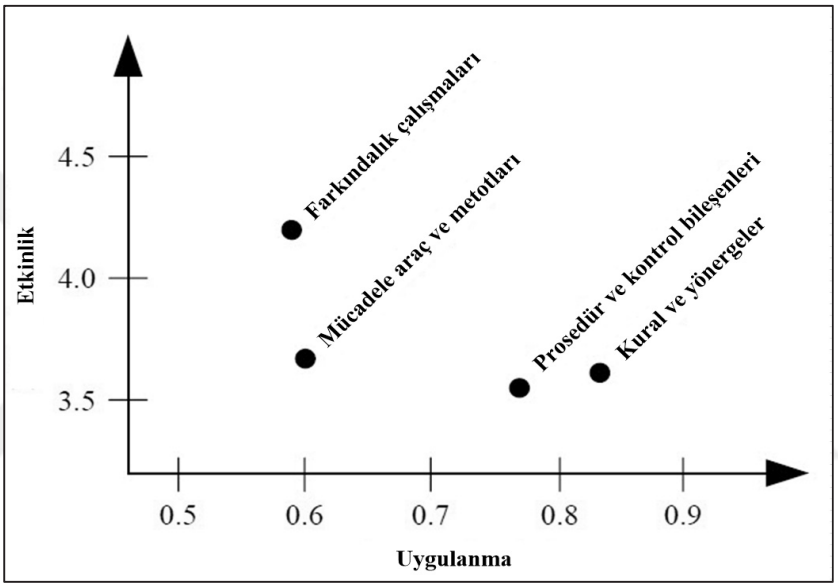
Ağ güvenliği, bilişim uzmanlarının en çok üzerinde durduğu konulardan biridir. Ağ sistemlerinde kullanılan, cihaz ve sistemlerin birbiri ile iletişimini sağlayan protokoller (IP, TCP, DNS gibi) ilk dizayn edildiklerinde, günümüzdeki kullanımından çok farklı ve küçük ölçekte kullanılmaktaydı. Ağ protokolleri bakımından başlangıçtaki odak noktası verinin transfer edilip edilmediği (işlevsellik) iken, günümüzde ağ güvenliği (güvenlik) ön plana çıkmıştır. Olası bir güvenlik açığı ve istismara neden olmamaları için bu protokollerin ağ yöneticileri tarafından doğru yapılandırılması gerekmektedir.

Her geçen gün daha da büyüyen ve kompleks hale gelen ağlar ile bu ağlar üzerinde çalışan protokollerin zaafları göz önünde bulundurulduğunda; ağ altyapıları ve güvenliği hakkında oldukça sınırlı bilgi ve deneyim sahibi olan bilgisayar kullanıcılarının ağlar vasıtasıyla veya ağlara karşı gerçekleşebilecek olası bir saldırıyı tespit etmeleri neredeyse imkânsızdır (Stallings, 2006). Bu tespitin kısmen de olsa BT sistem yöneticileri bakımından da geçerli olduğu kabul edilebilir.

2.6.2. Teknoloji Dışı Yöntem ve Araçlarla Mücadele

Bilişim ve Bilgi Sistemlerinin güvenliğini sağlamada teknolojik koruma yöntemlerinin yanı sıra teknoloji dışı yöntem ve araçlar da kullanılmalıdır. Bu sistemlerin tasarım ve analiz aşamalarında, yalnızca teknoloji değil, aynı zamanda insan faktörü de dikkate alınmalı, örgüt yönetiminin konuyu tam ve eksiksiz anlaması sağlanmalıdır. Bilgi ve iletişim teknolojilerinin en önemli unsuru insandır. İnsan, bu sistemlerin tasarlayıcısı ve yöneticisi olduğu gibi aynı zamanda kullanıcısı durumundadır. İnsan faktörünü dikkate almadan bilgi güvenliği sorununu etkili bir şekilde çözmek mümkün olmayacak, teknolojik mücadele yetersiz kalacaktır (Zhang vd., 2015). Ayrıca, tabi olunan ulusal ve uluslararası kanun ve yasalar, sözleşmeler ve benzer birçok bileşen detaylı olarak incelenmeli ve ileride oluşması muhtemel sorunlar meydana gelmeden bertaraf edilmelidir.

Hagen ve arkadaşları, siber güvenliğin teknolojik olmayan boyutunu dört ana başlık altında (kural ve yönergeler, prosedür ve kontrol bileşenleri, mücadele araç ve metotları ile farkındalık çalışmaları) incelemişler ve farkındalık çalışmalarının az uygulanma oranına sahip olmasına rağmen siber güvenlikte en etkili yöntemin olduğunu belirtmişlerdir. Hagen ve arkadaşları ayrıca teknolojik olmayan siber güvenlik önlemlerinin teknolojik önlemler olmadan bir mana ifade etmeyeceğini ve yönetimsel önlemlerin teknolojik önlemler üzerine inşa edilebileceği sonucuna varmışlardır (Hagen vd., 2008).

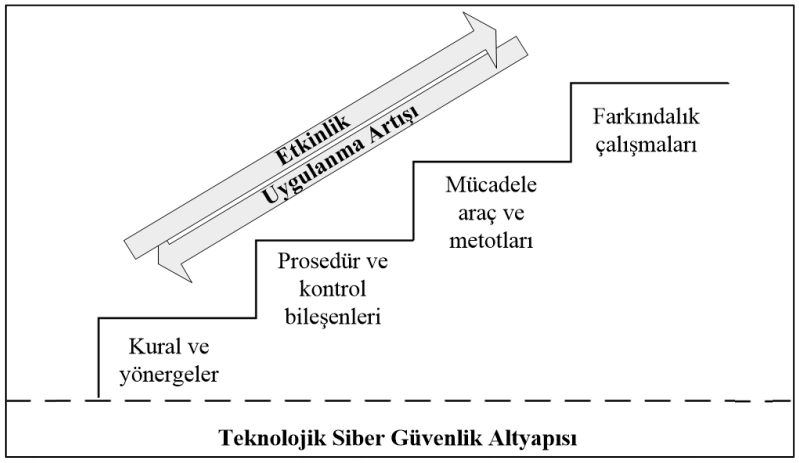


Şekil 30. Yönetimsel Metotların Uygulanma ve Etkinlik Endeksi

Kaynak: Hagen vd., 2008: 391.

Siber güvenliğin sağlanması bağlamında birçok kurum ve kuruluşun "Siber güvenlik yönetimi ve denetimi" için hazırladığı rehber, standart ve kılavuzlar mevcuttur. Bu rehber, standart ve kılavuzlardan en popüler olanları arasında ISO 27000 ve COBIT sayılabilir. (Hagen vd., 2008; Ismail ve Zainab, 2011). Siber güvenliğe ilişkin yönetimsel önlemlerin ele alındığı ve Kurumsal Siber Güvenlik Merdiveni adı verilen söz konusu önlemler şunlardır (Hagen vd., 2008: 391):

1. Kurumsal siber güvenlik kural ve yönergeleri
2. Prosedür ve kontrol bileşenleri
3. Teknolojik olmayan mücadele araç ve metotları
4. Farkındalık çalışmaları



Şekil 31. Kurumsal Siber Güvenlik Merdiveni

Kaynak: Hagen, vd. 2008: 391.

2.6.2.1. Kurumsal Siber Güvenlik Kural ve Yönergeleri

Siber tehditlerle mücadele etmek üzere kurumların en üst düzey yönetiminin onayı ve desteği ile hazırlanmış kural ve yönergeleri içeren stratejik belgelere, siber güvenlik veya bilgi güvenliği politikaları adı verilmektedir (Ismail ve Zainab, 2011: 50). Siber güvenlik politikaları; bilgi güvenliğini sağlama amacına yönelik ve üzerinde anlaşmaya varılmış, üst yönetimin destek ve taahhütlerini içeren belgelerdir (Thomson ve Solms, 2005: 75).

ISO 27001 (Bilgi teknolojisi-Güvenlik teknikleri-Bilgi güvenliği yönetim sistemleri-Gereksinimler) standardında, kurumsal bir bilgi güvenliği politikasını oluşturmanın üst yönetimin sorumluluğunda olduğuna vurgu yapılarak, kurumsal bilgi güvenliği politikasının aşağıda belirtilen hususları karşılaması gerektiğinin önemine dikkat çekilmiştir (TS ISO/IEC 27001:2013, 2016):

a) Kuruluşun amacına uygunluk,
b) Bilgi güvenliği amaçlarını içermek veya bilgi güvenliği amaçlarını belirlemek için bir çerçeve sağlamak,
c) Bilgi güvenliği ile ilgili uygulanabilir şartların karşılanmasına dair bir taahhüt içermek,
d) Bilgi güvenliği yönetim sisteminin sürekli iyileştirilmesi için bir taahhüt içermek.

Bilgi güvenliği politikasının ayrıca;

a. Yazılı biçimde mevcut olması,
b. Kuruluş içinde duyurulması ve
c. İlgili taraflarca erişilebilir olması da gerekmektedir.

Ismail ve Zainab, kurumsal siber güvenlik kural ve yönergelerine örnek olarak aşağıda listelenen politikalara yer vermiş ve bu politikaların Hagen ve arkadaşları tarafından ifade edilen "Kurumsal Siber Güvenlik Merdiveni"nin (Şekil 34) ilk basamağını oluşturduğuna dikkat çekmiştir (Ismail ve Zainab, 2011: 48):

- Kullanıcı sözleşmesi
- Demirbaş kullanım/koruma kuralları
- Yedekleme politikası
- Veri sınıflandırma ve saklama sözleşmesi
- İş gereksinimleri sözleşmesi
- Erişim denetimi ve izinler politikası
- Gizlilik politikası
- Kayıt ve yetkilendirme politikası
- Raporlama, bildirim ve geri bildirim politikaları
- Güvenli imha kuralları
- Kablosuz ağlar kullanım *sözleşmesi.*

2.6.2.2. Prosedür ve Kontrol Bileşenleri

İşletme üst yönetiminin katılımıyla oluşturulan siber güvenlik politika ve kurallarının nasıl uygulanacağa dair bilgiler içeren prosedür ve kontrol bileşenleri; kurum bünyesinde siber güvenlik politika, kural ve yönergelerinin adım adım nasıl uygulanması ve icra edilmesi gerektiğini gösteren bir rehber olarak ifade edilmektedir. Prosedür ve kontrol bileşenleri siber varlık ve kaynakların nasıl ve hangi iş süreçler ile korunacağını göstermesi açısından önemlidir (Ismail ve Zainab, 2011).

Hagen ve arkadaşları prosedür ve kontrol bileşenlerinin doğrudan kurumsal siber güvenlik politikalarından türetildiğinin altını çizerek, çalışanların bireysel ve organizasyonel davranışlarını yönlendiren belgeler olduğuna dikkat çekmişlerdir (Hagen vd., 2008). Prosedür ve kontrol bileşenleri aşağıda listelenen bileşenleri içermektedir (Ismail ve Zainab, 2011):

- Denetim ve disiplin prosedürleri,
- Fikri mülkiyet / telif hakları ile alakalı kural ve prosedürler,
- Gizlilik sözleşmeleri,
- Hassas veri ve bilgileri bulundurma / taşıma yönergeleri,
- Hali hazırda mevcut olan siber güvenlik politikalarının güncellenme yönergesi,
- Hizmet / Dış kaynak kullanım ile alakalı prosedürler.

2.6.2.3. Mücadele Araç ve Metotları

Herhangi bir siber güvenlik ihlali gerçekleşmemesi için veya ihlal gerçekleştikten sonra yapılması gereken eylemlerin yer aldığı belgeler olarak ifade edilen yönetimsel araç ve metotlar "Kurumsal Siber Güvenlik Merdiveni"nin üçüncü basamağını oluşturur ve aşağıdaki listelenen bileşenlerden oluşur (Hagen vd., 2008: 384).

- Siber varlıkların sınıflandırılması,
- Risk analizleri,
- İç ve dış denetiler,
- Önemli performans göstergeleri,
- Raporlama sistem ve süreçleri,
- Acil eylem planları.

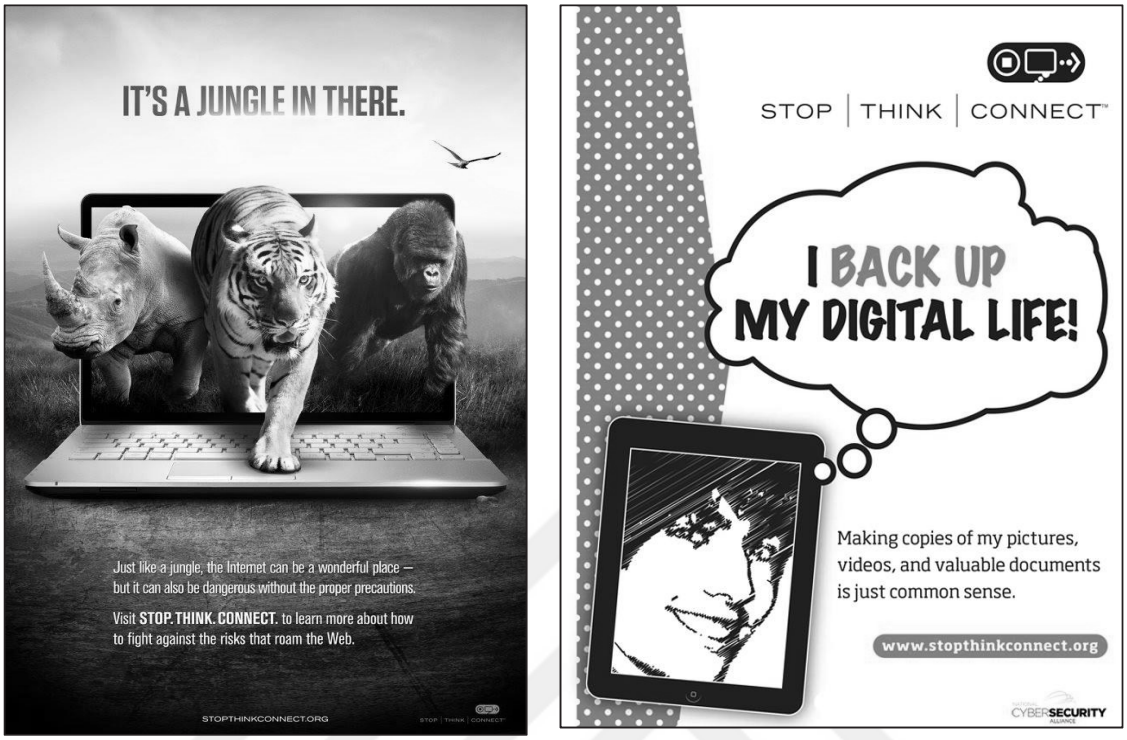
2.6.2.4. Farkındalık Çalışmaları

Hagen ve arkadaşlarının yaptıkları araştırmaya göre, "Kurumsal Siber Güvenlik Merdiveni"nin dördüncü basamağını oluşturan "farkındalık çalışmaları", zahmetli ve masraflı, ancak en etkili siber güvenlik mücadele yöntemidir (Hagen, vd. 2008).

Günümüzde birçok siber tehdit (virüs, trojan vs.) taşınabilir bellek, internette zararlı sitelerde gezinme, sosyal medya kanalları vb. yollarla bulaşmakta ve yayılmaktadır. Aynı zamanda, ne yazık ki internet kullanıcılarının neredeyse %70'i olan bitenin farkında dahi olamamakta, ilgili güvenlik risklerinin ve yüklenmiş oldukları sorumlulukların ne gibi sorunlara yol açabileceği konusunda neredeyse hiç bilgileri bulunmamaktadır (Eminağaoğlu, 2008).

Çalışanları siber güvenlik konusunda bilgilendirmek, mevcut olan bilgi birikimlerini arttırmak, zenginleştirmek ve daha nitelikli hale getirmek için düzenlenen farkındalık çalışmalarında amaç; kullanıcıların siber güvenliğin önemini kavramaları ve proaktif mücadele çalışmalarına katkıda bulunmalarıdır. Hagen ve arkadaşlarına göre farkındalık çalışmaları beş öğeden oluşmaktadır:

1. Eğitim / öğretim,
2. Farkındalığı teşvik edici çalışmalar, promosyonlar,
3. Hazırlık çalışmalarına kullanıcıların katkı sağlaması,
4. Üst yönetim katılımı,
5. Siber güvenlik olay veya vakalarından öğrenme süreçlerine tüm kurumun katılımının sağlanması.



Şekil 32. Farkındalık Posterleri

Kaynak: Stop-Think-Connect, 2016.

2.7. Siber Güvenlik İçin 10 Adım - İngiltere Örneği

Siber alanda, siber güvenliklerini sağlamak isteyen organizasyonlar için dizayn edilen "Siber Güvenlik için 10 Adım Rehberi" ilk olarak 2012'de yayınlanmıştır. Bu rehber günümüzde Londra Borsa'sında işlem gören en büyük 100 ve takip eden en büyük 250 kuruluşunun işlem gördüğü "FTSE 350 endeksi" işletmelerinin çoğunluğu tarafından uygulanmaktadır (UK-NCSC, 2016).

Şekil 33. Siber Güvenlik İçin 10 Adım

Kaynak: UK-NCSC, 2016.

Mart 2016 tarihinde Birleşik Krallık Hükümeti, Ipsos Araştırma Şirketi ve Portsmouth Üniversitesinin katılımı ile hazırlanan "2016 Güvenlik İhlalleri Raporu"nda, Birleşik Krallık genelinde işletmelerin çoğunun çeşitli teknik kontroller uyguladığı ancak "Siber Güvenlik için 10 Adım Rehberi"nde belirtilen tüm adımları yerine getiren çok az işletme olduğuna vurgu yapılmıştır. Bu araştırma kapsamında incelenen 1008 işletmenin rehberi uygulama oranları Tablo 6'da verilmiştir. Ayrıca Şekil 34'de de işletme büyüklüklerine göre bu rehberi uygulama yüzdeleri verilmiştir.

Tablo 6. Siber Güvenlik için 10 Adım Rehberi Uygulama Oranları

Siber Güvenlik için 10 Adım		
1	Siber Güvenlik Risk Sistemi	%34
2	Güvenli Yapılandırma	%88
3	Ağ Güvenliği	%86
4	Kullanıcı Yetki Yönetimi	%77
5	Kullanıcı Eğitimi ve Farkındalık	%28
6	Olay Yönetimi	%10
7	Kötü Niyetli Yazılımlardan Korunma	%83
8	İzleme	%51
9	Taşınabilir Depolama Aygıtları Kontrolü	%21
10	Evden veya Mobil Çalışma	%20

Kaynak: Ipsos Mori, 2016.

2.7.1. Adım 1: Siber Güvenlik Risk Yönetim Sisteminin Belirlenmesi

Siber güvenliğin etkili bir şekilde yönetilmesi, istismar ve ihlallerin ortadan kaldırılması veya en aza indirilmesi amacına yönelik olarak "Siber Güvenlik için 10 Adım" rehberinin merkezinde, kurumsal siber güvenlik risk yönetim sistemi bulunur (Şekil:33).

Siber tehditlerle etkin mücadele için organizasyonların ilk önceliğinin tepe yöneticilerin katılımı ile bir kurumsal siber güvenlik risk yönetim sistemi oluşturulması gerekir. Bu sistem, onu çevreleyen ve risk sistemi ile etkileşimde bulunan adımlardan oluşur.

2.7.2. Adım 2: Güvenli Yapılandırma

Sahip olunan siber sistemlerin güvenirliliğini önemli ölçüde artıracak olan güvenli yapılandırma adımı; BT sistem ve hizmetleri üzerinde çalışan gereksiz işlevlerin sistemlerden kaldırılması veya devre dışı bırakılması ile yerine getirilebilir. Bu kapsamda, BT sistem ve bileşenlerinin kullanıcı ihtiyaçlarına göre dizayn edilmesi, sistem ve cihazlar üzerinde isteğe bağlı bir şekilde yüklü gelen bazı hizmetlerin devre dışı bırakılması, kaldırılması veya silinmesi sağlanmaktadır.

Güvenli yapılandırma adımı; BT sistem ve hizmetlerinin bilinen siber güvenlik açıklarına karşı yamalarının zamanında ve uygun bir biçimde yapılmasını da kapsamaktadır.

2.7.3. Adım 3: Ağ Güvenliği

Yerel ağlardan internete ve diğer paylaşımlı ağlara yapılan bağlantılar, BT sistemlerini siber saldırılar ile karşı karşıya bırakabilmektedir. Bu saldırılar; bazı basit politika ve yazılı kurallar oluşturarak ve düzgün planlanmış bir ağ mimarisi uygulayarak bertaraf edilebilir.

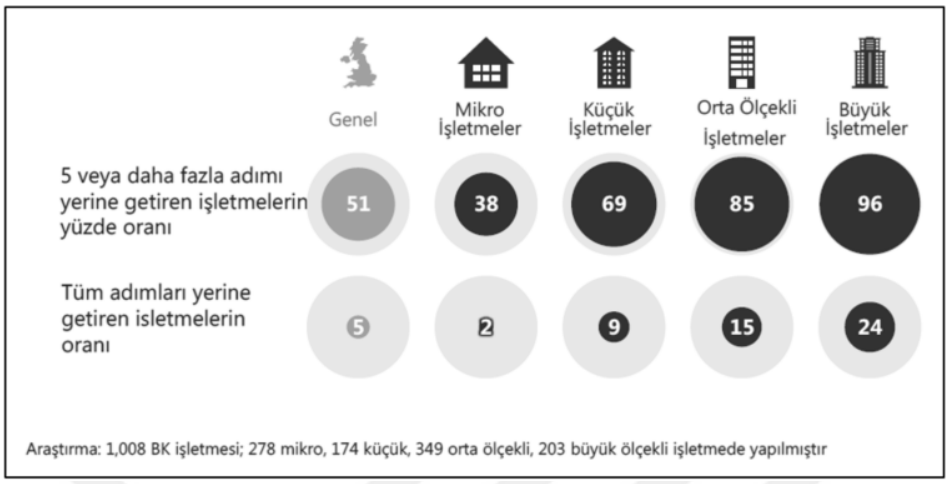
Özellikle, işletme ağlarının birçok fiziksel lokasyonu bünyesinde barındırdığı ve çalışanların iş sistemlerine uzaktan bağlandığı durumlarda, yerel ağların fiziksel sınırlarının belirlenmesi yerine, değerli verilerin depolandığı ve işlendiği yerlere odaklanarak, saldırganların nereye, neden saldıracaklarını saptamaya çalışarak stratejiler geliştirilmelidir. Bazı yerel ağ koruma önlemleri aşağıda sıralanmıştır;

- Ağların mantıksal bölümlere ayrılması (VLAN),
- Ağ geçitlerinin yapılandırılması ve sınırlandırılması,
- Güvenlik duvarlarının kullanılması,
- İçerik filtreleme ile zararlı sitelere kullanıcıların erişiminin engellenmesi,
- Doğrudan çalıştırılabilir içeriklerin engellenmesi,
- Kullanıcıların doğrudan internet ile iletişim kurmasının engellenmesi (çeşitli politika ve kuralların uygulandığı ağ geçitleri ve güvenlik duvarlarından geçerek internete erişim).

2.7.4. Adım 4: Kullanıcı Yetki Yönetimi

Birçok siber istismarın kasıtlı veya bilmeden verilen kullanıcı yetkilerinden kaynaklandığı bilinmektedir. Kullanıcılara bilişim sistemleri üzerinde ihtiyaçlarından daha fazla yetkiler verilmesi kötüye kullanımın önünü açabilmekte, bu yetkiler bazı kullanıcılar tarafından kullanılması "bilinçsiz" hasar ve arızalara neden olabilmektedir.

Tüm kullanıcılara rollerinin gerektirdiği, işlerini yapabilecekleri kadar yetkiler verilmesi ve bu yetkilerin periyodik olarak gözden geçirilmesi, yetkiler aracılığı ile yapılan istismarın önüne geçecektir.



Şekil 34. SG için 10 Adımın Uygulanma Oranları
Kaynak: UK-NCSC, 2016.

2.7.5. Adım 5: Kullanıcı Eğitimi ve Farkındalık

BT kullanıcıları kuruluşların siber güvenliklerinin sağlanmasında kritik önemde bir role sahiptirler. Bu nedenle siber güvenlik kurallarının ve kullanıcıların kullanımına sunulan siber varlıkların, kullanıcıların bu sistemler vasıtasıyla işlerini yapmalarına ve kuruluşun siber güvenliğinin sağlanmasına yardımcı olmaları önemlidir. Dolayısıyla siber güvenlik eğitim ve farkındalık çalışmaları, güvenlik bilincine sahip kullanıcı yetiştirmeye ve kurumsal siber güvenlik kültürünün oluşmasına yardımcı olacaktır.

2.7.6. Adım 6: Olay Yönetimi

Tüm organizasyonlar çeşitli ölçeklerde güvenlik olayları ile zaman zaman karşılaşırlar. Etkili olay yönetimi politikaları ve süreçlerinin oluşturulmasına yönelik yatırım, dayanıklılığı artırmaya, iş sürekliliğini desteklemeye, müşteri ve paydaş güvenini geliştirmeye ve olası etkileri azaltmaya yardımcı olacaktır. Bu anlamda kurumsal seviyede ve olay bazlı tecrübe biriktirme ve paylaşımı ile bu olaylardan pratik sonuçlar çıkararak uygulamayı geliştirmenin önemli bir yeri vardır.

2.7.7. Adım 7: Kötü Niyetli Yazılımlardan Korunma

"Kötü amaçlı yazılım" veya "zararlı yazılım" kavramları, sistemlerde kötü amaçlı ve istenmeyen etkilere neden olabilecek herhangi bir kodu veya içeriği kapsayan yazılım veya yazılım parçalarını ifade etmektedir. Siber sistemler aracılığı ile herhangi bir veri alışverişi, kötü amaçlı yazılımların sistemlere bulaşmasına ve bu sistemlerin sunduğu hizmetlerin ciddi şekilde

etkilenmesine neden olabilmektedir. İşletmelerin genel "siber savunma stratejisi" yaklaşımının bir parçası olarak uygun anti-virüs ve kötücül yazılım politikaları geliştirilip uygulayarak bu riski azalmaları mümkündür.

2.7.8. Adım 8: İzleme

Bilgi sistemleri açısından "izleme" önemli bir kavramdır. İzleme bir yandan siber güvenlik, diğer yandan sistemin ve örneğin siber güvenlik ile doğrudan bağlantılı olan yetkilerin doğru yapılandırılması bakımından önemli bir adımdır. Siber sistemlerin izlenmesi, gerçekleşmiş ve gerçekleşmekte olan siber saldırıların yanı sıra başarısız olmuş saldırı girişimleri hakkında fikir sahibi olunması işin gereklidir. İzleme faaliyetleri ayrıca, saldırılara karşı gerekli ve yerinde tepkinin zamanında verilebilmesi, BT sistemlerinin varoluş nedenlerine uygun kullanılıp kullanılmadığı sorusuna cevap verme yeteneğine sahiptir. İzleme, bazı durumlarda yasal zorunlukların yerine getirilmesi ve hukuksal mekanizmalara yardımcı olmak açısından da önemlidir.

2.7.9. Adım 9: Taşınabilir Depolama Aygıtlarının Kontrolleri

Taşınabilir depolama aygıtları, zararlı yazılımların taşınmasında ve yanlışlıkla veya kasıtlı olarak hassas bilgilerin sızdırılması eylemlerinde önemli bir role sahiptir.

Bir işletmedeki siber güvenlik politika ve yazılı kurallarının taşınabilir depolama aygıtlarının kullanımını düzenleyen güvenlik kontrolleri içermesi, işletme siber varlıklarının korunması bakımından büyük öneme sahiptir.

2.7.10. Adım 10: Evden veya Mobil Çalışma

"Mobil çalışma", "evden çalışma" ve "uzaktan sistem erişimi" işletmeler için büyük öneme sahiptir. Ancak bunların beraberinde getirdiği kolaylık ve pratiklik, aynı zamanda yönetilmesi gereken siber güvenlik riskleri de içermektedir. Bu bağlamda işletme politika ve siber güvenlik kurallarının, söz konusu hizmet ve kolaylıklarını sunan teknoloji ve hizmetleri kapsar şekilde hazırlanması önem arz etmektedir.

Ayrıca, yukarıda bahsi geçen teknolojilerden faydalanan kullanıcıların gerekli eğitimlerden periyodik olarak geçirilmesi bu kanal üzerinden oluşabilecek siber istismarların önüne geçecektir.

2.8. Siber Güvenlik Önlemleri Kıyaslama Sistemi – Japonya Örneği

Teknolojinin yoğun olarak kullanıldığı günümüzde, ister kamu, isterse özel sektör olsun, her ölçekte kuruluş siber güvenlik önlemleri almak zorundadır.

Organizasyonlar, siber güvenlik önlemlerini "kendilerinin bir siber güvenlik olayı tarafından mağdur edilmesini önlemek için" veya "bir siber güvenlik olayıyla karşılaştıklarında, hasarın boyutunu en aza indirgemek için" almak durumundadırlar (Kanno, 2005).

İlk versiyonu Japonya Ekonomi Ticaret ve Endüstri Bakanlığı'na bağlı "Bilgi Teknolojileri Özendirme Kurumu" (IPA) (Information-technology Promotion Agency of Japan) 2005'de yayınlanan "Siber Güvenlik Önlemleri Kıyaslama Sistemi" (ISM Benchmark) web tabanlı, ücretsiz bir hizmet olup, ilgililerin uyguladığı siber güvenlik önlemlerini, diğer katılımcı kuruluşlarla kıyaslama imkânı sunmaktadır. Dolayısıyla, kuruluşlar tarafından, "siber güvenlik önlemleri geliştirme safhalarında ve bilgi teknolojileri ilintili işlemlerde güvenlik seviyelerini iyileştirmelerine katkı sağlamak için" kullanılan ve devamlı güncellenen bir e-hizmettir (Vorakulpipat, vd. 2010: 1-4).

Tablo 7. ISO/IEC 27001:2005 vs. ISM-Benchmark

ISO/IEC 27001:2005- EK A		**ISM-Benchmark**	
Madde Başlıkları	Kontrol	Bölüm Başlıkları- Soru Sayıları /Yardımcı İpuçları	
1. Bilgi Güvenliği Politikaları	2	1.Siber Güvenliğe Kurumsal Yaklaşım	**7**/50
2. Bilgi Güvenliği Organizasyonu	11		
3. Varlık Yönetimi	5		
4. İnsan Kaynakları Güvenliği	9		
5. Uyum	10		
6. Fiziksel ve Çevresel Güvenlik	13	2.Fiziksel ve Çevresel Güvenlik Tedbirleri	**4**/22
7. Haberleşme ve İşletim Güvenliği	32	3.Bilişim Sistemleri ve İletişim Ağlarının İşletim ve Bakımı	**6**/33
8. Erişim Kontrolü	25	4.Yazılım Geliştirme ve Destek Aşamalarında Siber Güvenlik Tedbirleri	**5**/25
9. Sistem Temini, Geliştirme Ve Bakımı	16		
10. Bilgi Güvenliği İhlal Olayları Yönetimi	5	5.Siber Güvenlik İhlalleri Ve İş Sürekliliği Yönetimi	**3**/16
11. İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları	5		
Toplam	133	Toplam	**25**/146

Kaynak: Kanno, 2005: 4.

"ISM Benchmark", ISO 27001:2005 uluslararası bilgi güvenliği standardının yüz otuz üç kontrol bileşeni temel alınarak hazırlanmış, ISO 27001:2013'e göre güncellenmiş, soru sayısı yirmi yediye ve kontrol bileşenlerinin sayısı yüz altmış ikiye çıkmıştır. Kıyaslama sistemi iki kısım ve kırk yedi sorudan oluşmaktadır.

- Siber güvenlik önlemleri hakkında yirmi yedi soru
- Kuruluş hakkında yirmi soru

Testin ilk kısmında kullanıcılar siber güvenlik uygulamaları hakkında sorulara (beşli Likert tipi) cevaplar vermektedir ve bu bölüm beş alanını kapsayacak şekilde kategorize edilmiştir. Bu kategoriler:

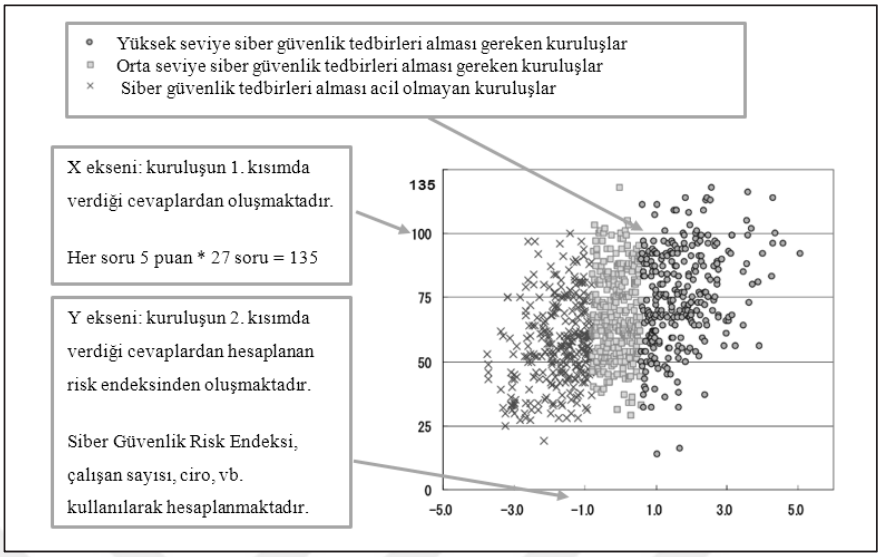
1. Siber Güvenliğe Kurumsal Yaklaşım (8 soru),
2. Fiziksel ve Çevresel Güvenlik Tedbirleri (4 soru),
3. Bilişim Sistemleri ve İletişim Ağlarının İşletim ve Bakımı (7 soru),
4. Yazılım Geliştirme ve Destek Aşamalarında Siber Güvenlik Tedbirleri (5 soru),
5. Siber Güvenlik İhlalleri ve İş Sürekliliği Yönetimi (3 soru)

2.8.1. ISM Benchmark Analiz Sonuçları

Kullanıcılarına, kuruluşlarının siber güvenlik önlemleri bağlamında nerede olduklarını kıyaslama imkânı sağlayan ISM Benchmark, aşağıda yer alan analiz sonuçlarını üretir (Kanno, 2005: 5).

2.8.1.1. Serpilme Diyagramı

Kuruluş tarafından sağlanan veriler kullanılarak, kuruluşunuzun ve tüm katılımcıların siber güvenlik konumlarını serpilme diyagramı üzerinde gösterir. Serpilme diyagramı sayesinde, kuruluşlar organizasyon boyutuna dayalı dağılımlarda konumlarını ve kuruluşun diğer katılımcılarla karşılaştırmasını görsel olarak ifade etmektedir (bk. Şekil 36).



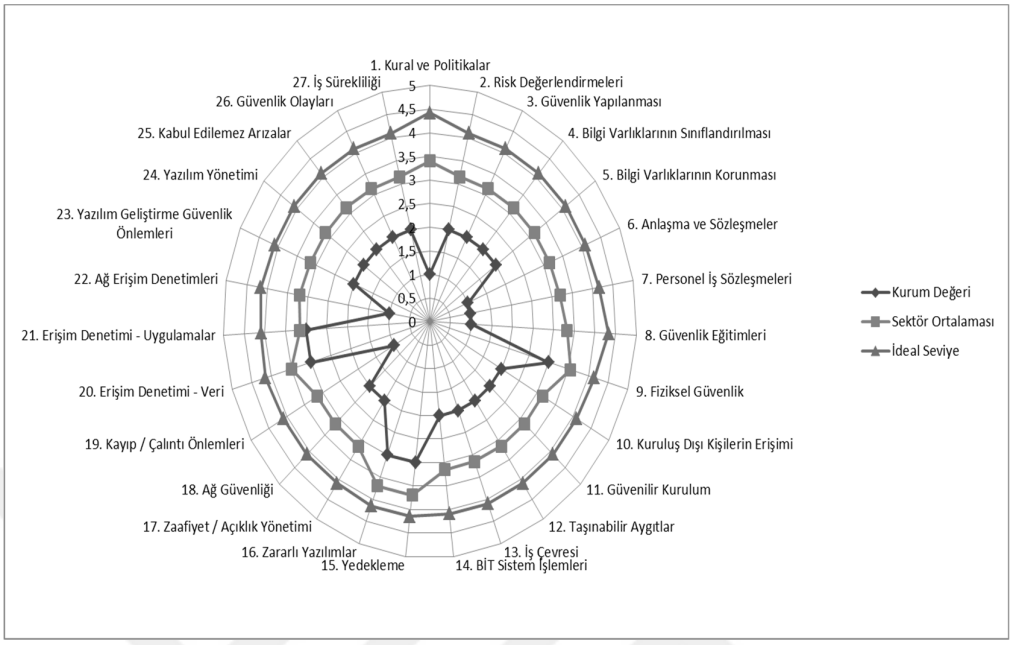
Şekil 35. ISM Benchmark – Serpilme Diyagramı
Kaynak: METI, 2005: 32.

2.8.1.2. Radar Grafikleri

Katılımcı tarafından sağlanan veriler yardımıyla radar grafikleri oluşturulmaktadır. Radar grafiği yirmi yedi siber güvenlik önleminin uygulama durumu hakkında bilgi vermektedir. Grafikler, sadece yirmi yedi siber güvenlik önlemi için kullanıcı kuruluşun verilerinin yanı sıra, ortalama ve ideal değerler de yer almaktadır. Bunlardan bazıları:

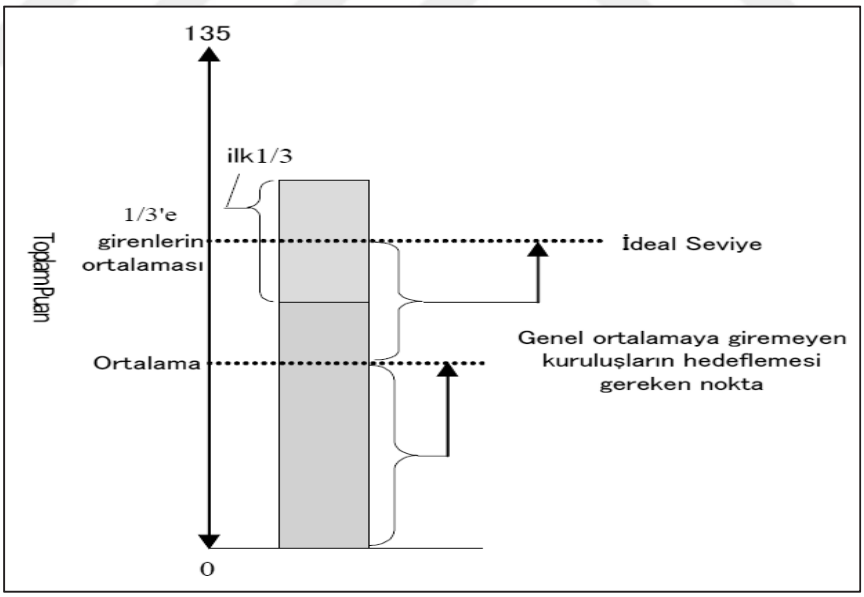
- **Siber Güvenlik Risk Grubu Bazlı Kıyaslama,** kuruluşlar, siber güvenlik risk endeksi verilerini aynı risk grubuna giren kuruluşlarla kıyaslayabilme imkânı sağlar.
- **Kuruluş Büyüklüğüne Dayalı Kıyaslama,** katılımcılar, kuruluşun boyutuna göre sınıflandırılan aynı gruptaki başkalarının verileriyle karşılaştırma imkânı sağlar.
- **Sektör Bazlı Kıyaslama,** kuruluş verilerini faaliyet gösterdikleri sektöre bağlı olarak sınıflandırılan aynı gruptaki başkalarıyla kıyaslama imkanı sunar.
- **İdeal değerler,** kıyaslama yapılan grubun en iyi 1/3 katılımcısının ortalama değerini gösterir.

Grafikler sayesinde katılımcılar, ilgili grupların (risk seviyesi, sektörel) ortalama seviyelerine ulaşmayı hedef alabilir, ortalama değerlere ulaşan kuruluşlar ise ideal seviyeye ulaşmaya çalışabilir ve güvenlik seviyelerini adım adım iyileştirebilirler (Kanno, 2005: 6).



Şekil 36. ISM Benchmark – Radar Grafiği

Kaynak: METI, 2005: 33.



Şekil 37. ISM Benchmark – İdeal Seviye

Kaynak: METI, 2005: 32.

2.8.2. ISM Benchmark Kullanılarak Yapılan Araştırmalar

"Tayland Milli Elektronik ve Bilgisayar Teknolojileri Merkezi" tarafından yapılan "ISM Benchmark Kullanarak Tayland'da Bilgi Güvenliği Uygulamaları Araştırması", Taylandlı kuruluşların bilgi güvenliğini göz ardı ettiğini ve bilgi güvenliği konusunda yeterli donanıma

sahip kalifiye personel ve bilgi birikiminden yoksun olduklarını göstermiştir. Araştırmaya katılan kuruluşlardan bazıları olumlu sonuçlara sahip olsalar da, bazı konularda (erişim kontrolü, dış kaynak kullanım sözleşmeleri, bilgi işleme vb.) farkındalık oluşturulması gerektiği vurgulanmıştır (Vorakulpipat vd., 2010: 2).

Yukarıda belirtilen araştırmanın tüm katılımcıları, aşağıda listelenen nedenlerden dolayı, ISM Benchmark'ı kuruluşlarının BT güvenlik düzeylerini değerlendirmek için çok yararlı ve etkili bulduklarını ifade etmişlerdir:

- Bilgi güvenliğinin neden olabileceği sorunlar hakkında bilgi sahibi olmak,
- Bilgi güvenliği tedbirleri hakkında fikir edinmek,
- Kuruluş bilgi güvenliği seviyelerini diğer kuruluşlarla karşılaştırma imkânı bulabilmek.

Katılımcıların bir kısmı ISM Benchmark'ı kuruluşlarının BT güvenlik seviyelerini kontrol etmek için uygulayacaklarını belirtmiş ancak, katılımcılardan bazıları ISM Benchmark'ı aşağıdaki nedenlerden dolayı kuruluşlarında uygulamayı düşünmediklerini ifade etmişlerdir(Vorakulpipat vd., 2010: 3):

- Siber güvenliği kuruluşları için bir problem olarak görmediklerinden,
- Siber güvenlik kaynaklı sorunların meydana gelme olasılığını düşük gördüklerinden,
- Çalışanlarının siber güvenlik konusunda yeterli bilgi birikimine sahip olmadıklarından,
- ISM Benchmark sisteminin zaman alan ve basit bir araç olmadığından dolayı.

Merkezi Jakarta, Endonezya'da bulunan "Asya Ekonomik Araştırmalar Enstitüsü – (ERIA)" tarafından, altı ülkede yerleşik kırk sekiz kuruluşta yapılan "İş Sektöründe Bilgi Güvenliğinin Güçlendirilmesi" çalışmasında, IPA tarafından geliştirilen ISM Benchmark uygulamasının etkinliği araştırılmıştır. Çalışma kapsamında katılımcı kuruluşların yöneticilerine ISM Benchmark hakkında çeşitli sorular yöneltilmiştir (ERIA, 2009: 92).

Tablo 8. ERIA Araştırmasına Katılan Kuruluşlar

Toplam		Ölçek		Faaliyet Alanı
		Büyük	KOBİ	
Malezya	13	% 54	% 46	Karma
Singapur	4	% 0	% 100	Karma
Tayland	3	% 67	% 33	İnternet sağlayıcılar, Sağlık, Gıda ve Tarım
Vietnam	14	% 43	% 57	Bilgi hizmetleri, Üretim, Telekom, Finans/Sigorta, Yayın, Gazete, Kamu hizmetleri
Çin	6	% 50	% 50	Bilgi hizmetleri, Yazılım, Kredi Kartı Üretimi, Bilgi Güvenliği Ürün Geliştirme, İnternet Oyunları, İnsan Kaynakları Puantaj İşleri.
Güney Kore	10	%70	%30	Orta ve büyük ölçekli bazı Bilişim firmaları ve diğer kuruluşlar.

Kaynak: ERIA, 2009: 92.

Araştırma kapsamında "kuruluşların bilgi güvenliği seviyelerinin belirlenmesi bağlamında ISM Benchmark'ın etkili bir araç" olup olmadığı sorulmuştur. Katılımcılar % 60 - % 100 oranında ISM Benchmark'ın etkili bir araç olduğunu belirmişlerdir.

Tablo 9. ISM Benchmark Etkili Bir Araç mıdır?

	Evet	Hayır	Katılımcıların Yorumları
Malezya	% 83	% 17	- Yüksek düzeyde değerlendirme için etkilidir.
Singapur	% 67	% 33	Oldukça kapsamlı; Üst seviye önlemlerin uygulandığı kuruluşlarda kullanılabilir, sorulara cevap verebilmek için bir Bilgi Güvenliği Yönetim Sistemi (BGYS) olması gereklidir. Bir BGYS varsa anket sonuçlarında değişiklik gözlemlemek zor. BGYS eksikliği ISM Benchmark kullanarak giderilemez, alternatifi değil.
Tayland	% 100	% 0	BT güvenlik düzeyini değerlendirmede çok yararlı, etkili
Vietnam	% 100	% 0	Bilgi güvenliği hakkında birçok konuda bilgi veren bir araç Pratik ve kullanımı kolay
Çin	% 100	% 0	Yorum yapılmamış
Güney Kore	% 60	% 40	Genel önlemleri içeren, detaylı önlemler hakkında bilgi bulundurmayan kendi kendine teşhis için güzel bir araç. Detay analizler için daha fazla soru gerekli. Hedefler açık ve net değil.

Kaynak: ERIA, 2009: 94.

Araştırma, "katılımcıların ISM Benchmark'ı kuruluşlarında kullanmak isteyip istemedikleri" sorulmuş, katılımcıların çoğunluğu "ISM Benchmark'ı kullanacaklarını" ifade etmişlerdir (ERIA, 2009: 95)

Tablo 10. ISM Benchmark'ı Kullanma İsteği

	Evet	Hayır	Neden (Katılımcı Yorumu)
Malezya	% 86	% 14	Evet: Etkili bir araç Hayır: Başka bir araç kullanıyoruz
Singapur	% 67	% 33	Evet: Tekrarlanan soruların çıkarılması, kullanılan dilin daha sadeleştirilmesi, yapılandırma biçiminde iyileştirmeler gerektiriyor Kuruluş bilgi güvenliği seviyesini kontrol için iyi bir araç Hayır: Anket verilerinin kötüye kullanımı konusunda endişe, daha yüksek yönetim onayını ve desteğini gerektirir.
Tayland	-	-	Bazı katılımcılar bilgi güvenliği seviyelerini değerlendirmek için kullanmayı düşünmekte
Vietnam	% 93	% 7	Evet: Ücretsiz ve kullanımı kolay. Bilgi güvenliği seviyesini değerlendirmek için etkili araç. Bu kıyaslama yoluyla bilgi güvenliğinde gelişmeler görebiliriz.
Çin	% 83	% 17	Hayır: ISM ölçütü çok genel, firmamıza uygun daha özel bir sisteme ihtiyaç duyuyoruz.
Güney Kore	% 30	% 70	Evet: Aynı alanlar arasındaki seviye karşılaştırması mümkündür. Hayır: Esnek değil, hedef önlemler belirtilmemiş. Çok genel.

Kaynak: ERIA, 2009: 95.

"Asya Ekonomik Araştırmalar Enstitüsü – (ERIA)" tarafından "bilgi güvenliği uygulamalarının Asya Ekonomisini nasıl etkileyeceği" üzerine yapılan "İş Sektöründe Bilgi Güvenliğinin Güçlendirilmesi" çalışmasına katılan kuruluşların çoğunluğunun ISM Benchmark'ı kurumsal bilgi güvenliğinin değerlendirilmesinde etkili bir araç olarak kabul ettikleri ifade edilmiş, tüm siber olayları da ISM Benchmark çerçevesinde kapsamanın zor olduğuna vurgu yapmıştır (ERIA, 2009: 100).

2.9. Siber Güvenlikle ile İlgili Yapılan Çalışmalar

Türkiye ve dünyada siber güvenlik ile ilgili yapılan çalışmalara ilişkin araştırma, Hasan Kalyoncu Üniversitesi ve Gaziantep Üniversitesi'nin abone olduğu çevrimiçi veri tabanları yardımı ile yapılmıştır. Yapılan araştırmalar sonucunda Türkiye'de siber güvenlik ile ilgili yapılmış çok fazla bir çalışma bulunmadığı görülmüştür.

Türkiye'de 2017 yılına kadar siber güvenlik ile ilgili yapılan çalışmalara taramalar; Siber Güvenlik, Siber Güvenliğe Kurumsal Yaklaşım, Siber Saldırı, Siber Savaş, Siber Suç, Siber Hukuk ve Bilgi Güvenliği anahtar kelimeleri ile yapılmıştır. Yapılan tarama sonucunda, 2017 yılına kadar Türkiye'de 69 yüksek lisans ve 12 tane doktora tezi olmak üzere toplam 81 tez çalışması yapıldığı tespit edilmiştir. Bu tezlerde ağırlıklı olarak; bilgi güvenliği, bilgi güvenliği farkındalığı, bilgi güvenliği standartlarının oluşturulması, bilişim suçları, bilişim suçları ile müdahale, siber güvenlik suçları, siber terör, Türkiye'nin siber güvenlik politikaları, siber tehditlere karşı savunma gibi konuların çalışıldığı görülmüştür. Fakat söz konusu bu

çalışmalarda, işletmelerin siber güvenliğe kurumsal yaklaşımı veya işletmelerin siber güvenliğe ilişkin farkındalığı konularına yönelik bir çalışmaya rastlanmamıştır. Türkiye'de 2017 yılına kadar siber güvenlik ile alakalı yapılan tezlerin büyük çoğunluğu (55 tanesi) bilgi güvenliğine ilişkindir. Bilgi güvenliği kapsamında yapılan bu tezlerde; bilgi güvenliği, bilgi güvenliği farkındalığı, bilgi güvenliği standartlarının oluşturulması, bilgi güvenliği risk seviyelerinin belirlenmesi, kamu kurumlarında, sağlık kurumlarında bilgi güvenliği uygulamaları, bilgi varlıklarının ve kişisel verilerin hukuksal düzenlemeler ile korunması, bilgi güvenliği ihlallerinin tespiti, bilgi güvenliği yönetim sistemleri ile şirket performansı ilişkisi. vb. konular çalışıldığı görülmektedir. Yukarıda ifade edildiği üzere hem siber güvenlik hem de bilgi güvenliği adı altında yapılan bu çalışmalarda, işletmelerin siber güvenliğe yaklaşım düzeylerinin belirlenmesi veya işletmelerin siber güvenlik yönetim yaklaşımlarının analiz edilmesine ilişkin bir çalışmaya rastlanmamıştır.

Türkiye'de 2017 yılına kadar kitap adında "siber güvenlik" kavramını içeren basılı kitap sayısı 23'tür. Türkçe yazılan bu kitapların tamamı ülke güvenliği eksenli olup, hukuki ve sosyal içeriktedir. Diğer taraftan kitap adında "bilgi güvenliği" kavramı geçen basılı kitap sayısı 21 adettir. Bu kitapların neredeyse tamamı bilgi güvenliğine ilişkin teknik konuları ele almaktadır.

Türkiye'deki 2017 yılına kadar siber güvenlik ile yazılan makale ve bildirilerin büyük çoğunluğu sosyal ve hukuksal çalışma niteliği taşımaktadır. Az sayıdaki bazı çalışmaların ise bilgi güvenliği standartlarının oluşturulması ve örgütte bilgi güvenliği farkındalığının oluşturulmasına yönelik olduğu görülmektedir. Türkiye'de 2017 yılına kadar siber güvenlik ile alakalı yapılan çalışmalardan bazıları aşağıda verilmiştir.

Vural ve Sağıroğlu bir çalışmalarında; kurumsal bilgi güvenliği standartları konusunu genel olarak ele almış ve bu çalışmalarında mevcut bilgi güvenliği standartları ile yeni oluşturulmakta olan bilgi güvenliği standartlarını gözden geçirmişlerdir (Vural ve Sağıroğlu 2008:507-522). Vural ve Sağıroğlu başka bir çalışmalarında, kurumsal bilgi güvenliğinin sağlanmasında önemli bir role sahip olan güvenlik testleri, standartlar ve kılavuzları geliştiren kurumlar kapsamlı olarak ele alınmış ve kurumsal bilgi güvenliğine ilişkin testlere yönelik önerilerde bulunulmuştur. Bu çalışmada; güvenlik farkındalığının arttırılması, yeni çözüm önerilerinin geliştirilmesi ve uygulanmasının kolaylaştırılması önerilmiş ve sunulan önerilerin hayata geçirilmesiyle, yüksek seviyede kurumsal bilgi güvenliğinin sağlanmasına katkı sağlanacağı iddia edilmiştir (2011:89-103).

Baykara ve arkadaşları (2013) tarafından yapılan bir çalışmada; günümüzde yaygın olarak kullanılan bilgi güvenliği araçlarını incelenmiş ve bu araçları; işlevler, kullanım alanları gibi birçok

özellikleri dikkate alınarak 22 farklı kategoriye ayrılmıştır. Ayrıca bu çalışmada, bilgi sistemleri güvenliğinin sağlanmasına yönelik çeşitli çözüm önerilerinde bulunulmuş ve bilgi sistemleri güvenliği konusunda ihtiyaç duyulan temel güvenlik stratejileri belirlenmeye çalışılmıştır (Baykara, vd. 2013, 231-239).

Şahinaslan ve arkadaşları (2009), "Kurumlarda Bilgi Güvenliği Farkındalığı, Önemi ve Oluşturma Yöntemleri" isimli çalışmalarında; kurumlarda bilgi güvenliğine yönelik risklerin önlenmesinde, bilgi güvenliği farkındalığının önemi ve farkındalık oluşturma yöntemleri ele almış ve çözüm önerilerinde bulunmuşlardır (Şahinaslan, vd. 2009, 597-602).

Acılar (2009); bir çalışmasında örgüt kültürü ile bilgi güvenliği arasındaki ilişkiyi incelemiş ve bilgi güvenliğinin sağlanmasında örgüt kültürünün önemli olduğunu belirtmiştir. Bu çalışmada; bilgi güvenliğinin etkin bir şekilde sağlanmasında, alınacak teknik önlemlerin yanında işletmenin sahip olduğu bilgi güvenliği kültürünün de önemli olduğu ve bilgi güvenliği kültürüne sahip olmayan işletmelerin güvenlik için yapmış olduğu yatırımlardan (yazılım, donanım ve fiziki tedbirler) istenen sonuçların alınamayacağını belirtmiştir (Acılar, 2009, 25-33).

Alagöz ve Allahverdi (2011) yapmış olduğu çalışmalarında; bilgi güvenliği kavramını genel olarak ele almışlar, bilgi güvenliği ile ilgili Dünyada ve Türkiye'deki mevcut sorunları incelemişlerdir. Ayrıca çalışmalarında, işletmelerin muhasebe uygulamalarında bilgi güvenliği alanında atılacak adımları değerlendirmişlerdir (Alagöz ve Allahverdi, 2011, 47-64).

Yeşilyurt (2015); Türkiye'de çevrimiçi ödeme sistemleri ve bu sistemin siber güvenliğini destekleyen yazılım tedarik zincirlerinin barındırdıkları riskleri bir çalışmasında incelemiştir. Bu çalışmasında potansiyel riskler, siber güvenlik normları kapsamında tanımlanmış ve siber güvenlik önlemleri yönetimsel açıdan tartışılmıştır. Çalışmada finans kurumlarının siber güvenlik için yabancı kaynaklı yazılım ve donanım çözümlerinin kullanıldığı belirtilmiş ve sadece yabancı kaynaklı çözümlerle yetinilmemesi gerektiğine dikkat çekmiştir. Çalışmada ayrıca elektronik tabanlı ödeme sistemlerinin önemi ve bu sistemlerin ilgili kamu kurum ve kuruluşlarının bilgisi dahilinde çalışması gerektiğine vurgu yapılmıştır (Yeşilyurt, 2015, 97-120).

Mil (2015) bir çalışmasında, Sosyal Güvenlik Kurumu'nun siber güvenlik bağlamında yönetimi, uygulama ve politikaları incelenmiş ve değerlendirmiştir. Bu çalışmada Sosyal Güvenlik Kurumun siber güvenlik alanında yazılı kural ve politikalarının olmasına rağmen bu kural ve politikaların tamamının uygulanmadığı tespit edilmiştir. Çalışmada, siber güvenlik yönetimi

bağlamında rol ve sorumlulukların tam olarak paydaşlarla paylaşılması ve öğretilmesi gerektiğini vurgulanmıştır (Mil, 2015, 398-416).

Yavanoğlu ve arkadaşları (2012) yapmış oldukları bir çalışmada; sık kullanılan sosyal paylaşım ağlarını incelenmişler ve bu sosyal paylaşım ağlarında karşılaşılan güvenlik ihlalleri örneklendirilmiş, meydana gelebilecek güvenlik açıkları ve tehlikeleri sınıflandırılmış, alınması gereken güvenlik önlemleri belirtilmiştir (Yavanoğlu, vd, 2012: 15-27).

Yılmaz ve arkadaşları (2015) yapmış olduğu bir çalışmada; teknolojinin gelişmesiyle birlikte küreselleşmeye bağlı güvenlik kaygılarının ortaya çıkışı, Türkiye'de uygulanan bilgi toplumu stratejisi, Türkiye ve Dünyada bilgi toplumuna geçiş süreci, bilgi teknolojileriyle oluşturulan kritik altyapı sistemleri, bu sistemlere karşı siber tehditler ve bu sistemlerin risk analizleri ele alınmıştır. Çalışmada; siber güvenlik farkındalık ve bilinçlendirme eğitimlerinin tüm personel düzeyinde tam ve yeterli şekilde yapılmadığı sonucuna ulaşılmıştır. Bu çalışmada; kurum ve kuruluşların bilişim sistemlerinde rol bazlı yetkilendirme yaparak bu yetkileri belirli periyotlarda ve belirli süreçler çerçevesinde denetlemesi ve güncellemesi gerektiğinin altını çizmişlerdir. Ayrıca çalışmada; siber güvenlik alanında çalışan teknik ve teknik olmayan personelin yedeklenmesi gerekliliğine de işaret etmişlerdir (Yılmaz vd, 2015: 133-146).

Türkiye'de siber güvenlik ile ilgili yukarıda belirtilen çalışmaların büyük çoğunluğunda sosyal ve hukuksal az sayıdaki bazı çalışmalarda ise bilgi güvenliği standartlarının oluşturulması ve örgütte bilgi güvenliği farkındalığının oluşturulmasına yöneliktir. Fakat yapılan çalışmalarda, işletmelerin siber güvenliğe kurumsal yaklaşımı veya işletmelerin siber güvenliğe ilişkin farkındalığı konularına yönelik bir çalışma yapılmamıştır. Diğer taraftan siber güvenlik konusunda yurt dışında yapılan çalışmalar Türkiye'ye kıyasla çok daha fazladır. Yurt dışında yapılan çalışmaların çoğunluğu, Türkiye'de olduğu gibi hukuki ve teknik konuları ele almaktadır. Fakat yurt dışında yapılan birçok çalışmada; siber güvenliğin ekonomik, psikolojik ve sosyo-kültürel boyutlarını ele alan çalışmalar bulunmakta ve bu çalışmaların sayısının son zamanlarda giderek arttığı görülmektedir.

Okoye (2017), siber güvenlikle alakalı (bilgi güvenliği, veri güvenliği, siber güvenlik, vb.) anahtar kelimeleri kullanarak veri tabanlarında yaptığı araştırmada toplam 112 yayına ulaşmıştır. Tablo 11 yurt dışında 2013 – 2017 yılları arasında yapılan yayınları göstermektedir. (Okoye, 2017:16).

Tablo 11. Yurt Dışında Siber Güvenlik İle Alakalı Yayınlar

	Yayın Yılı		
Yayın Türü	2013-2017 arası	2013 öncesi	Toplam
Kitap	0	2	2
Tez	0	0	0
Hakemli Makale	97	1	98
Web Sitesi	1	0	1
Kamu raporları	2	0	2
Diğer kaynaklar	9	0	9
Toplam	109	3	112

Dimopoulos ve arkadaşları (2004) yapmış olduğu çalışmalarında; KOBİ'lerin siber güvenlik ile alakalı farkındalıkları konusunda endişelerinin olduğunu belirtmişlerdir. Söz konusu endişenin, a) İşletmelerin siber güvenlik çalışmalarını koordine edecek yeterli kaynaklarının olmaması (personel, bütçe zaman ve bilgi), b) İşletmelerde siber güvenlik kültürünün yerleşmediğinin, siber güvenliğe ilişkin yazılı kural ve prosedürlerinin bulunmaması ve işletmelerin bu kural ve yönergeleri oluşturma gibi bir niyetinde olmamasından kaynaklandığını ifade etmişlerdir (Dimopoulos, vd., 2004).

Desai (2013) yapmış olduğu çalışmasında, yöneticilerin siber güvenlik konusunda gerekli yatırım yapmak ve işletmelerini korumak için gerekli tedbirleri almak için yeterli bilgi düzeyinde olmadıklarına vurgu yapıştır. Desai (2013) ayrıca çalışmasında, işletmelerin çok hızlı gelişen siber tehditlerle mücadelede yetersiz kaldığı gibi bu alanda yapılması gereken eğitimlere de yeteri önem vermediğinin altını çizmiştir (Desai, 2013). Valli ve arkadaşları ise, yapmış olduğu çalışmalarında; KOBİ'lerde çalışan yöneticilerinin %75'i, kendi işletmelerinin siber güvenlik tehditleri ile karşı karşıya olmadığını düşündüklerini belirtmişlerdir (Valli vd., 2014).

Tomlin yapmış olduğu çalışmada; işletmelerin kendi siber güvenlik seviyelerini kontrol edebilecekleri araçların, siber güvenlik farkındalık düzeylerini artırdığını ve tehditlerden korunmaya yardımcı olacağını belirtmiştir (Tomlin, 2015:28). Kivikoski ve Kaup-pinen, Finlandiya'da faaliyet gösteren KOBİ'ler üzerinde yapmış olduğu çalışmalarında ise; araştırma kapsamında KOBİ'lerin sadece %3'nün siber güvenlik ihlali yaşadıklarının bilincinde olduklarını ve bu işletmelerin %13'ün çalışanlarının farkındalık düzeyini artırmak için eğitimler düzenlediğini tespit edilmiştir. Bu çalışmada ayrıca siber güvenliğe kurumsal yaklaşımım telekom ve sağlık gibi farklı sektörlerde farklılıklar göstereceğine dikkat çekmişlerdir (Kivikoski ve Kaup-pinen, 2016: 48.).

Aho ve Nevala (2016) yapmış olduğu araştırmalarında; KOBİ'lerin yüzde 66'sının siber güvenlik alanında atanmış bir personel bulundurmadıklarını, bu alanda çalışanlara eğitimler verilmediği ve ilgili doküman ve yazılı kuralların bulunmadığının belirtmişlerdir, Ayrıca çalışmada; çalışanların %31'inin iş için kişisel bilgisayar ve ekipman kullandığını ve bunun işletmeler için bir risk oluşturduğunu belirmişlerdir (Aho ve Nevela, 2016:20).

Hassinen (2017) yapmış olduğu çalışmada; araştırma sorularının güvenlikle alakalı olmasından dolayı katılımcıların cevap vermekte tereddüt ettiğine vurgu yapmış ve bazı katılımcıların bazı sorulara cevap vermek istemediklerini ve bu durumun nedeni olarak siber güvenlik bilincinin daha oturmadığından kaynakladığını ve zamanla değişeceğine inandığını belirtmiştir (Hassinen, 2017:18)

Sonuç olarak Hem Dünyada hem de Türkiye'de siber güvenlik yönetimine ilişkin araştırmaların kısıtlı olduğu, ancak son yıllarda bu konuların akademisyenlerinde gündemlerine daha fazla geldiği görülmektedir. Yapılan araştırmalar işletmelerin siber güvenlik yönetimine yeterli kaynak ve teknik personel ayırma konusunda isteksiz olduklarını, Finlandiya gibi eğitim seviyesi yüksek bir ülke de bile KOBİ'lerin sadece % 3'ünün ihlallerin farkında oldukları, % 13'ünün siber güvenlik konusunda personele eğitim verdiklerini göstermektedir. KOBİ'lerin genel olarak siber tehditlere karşı hazırlık seviyelerinin ne durumda olduğuna yönelik araştırmaların olmamasının işletmelerin bu konuyu namahremleri kabul etmelerinden ve bilgi vermekten imtina etmelerinden kaynaklandığı düşünülmektedir. Bu araştırma ve incelemelerin yapılmaması ve siber güvenlik yönetimi konusunda bir kurum kültürünün oluşturulmaması her geçen gün daha fazla teknoloji kullanan işletmelerin siber saldırılar karşısında aciz kalmalarına ve tehdit kaynaklarının taleplerine boyun eğmelerine sebep olacağından işletme bazında incelemelerin belli standartlara göre yapılmasında fayda bulunmaktadır.

ÜÇÜNCÜ BÖLÜM

YÖNTEM

3.1. Araştırmanın Yöntemi

Bu araştırma kapsamında nicel araştırma yöntemlerinden tarama modeli kullanılmıştır. Nicel araştırma; deneme, gözlem ve deneylere dayanılarak yapılan görgül (ampirik) araştırma yaklaşımına ya da gözlem ve ölçmelerin tekrarlanabildiği niceliksel veya sayısal araştırma yaklaşımı olarak ifade edilmektedir (Özdamar vd., 1999: 6). Tarama modeli ise; geçmişte ya da halen var olan bir durum var olduğu şekliyle betimlemeyi amaçlayan araştırma yaklaşımıdır (Karasar, 2008: 77).

Siber güvenlik yönetimi konusunun uygulanma düzeyi hakkında yaygın literatür bulunamadığından, araştırmanın keşifsel olması uygun görülmüştür. Keşifsel araştırma problemin açıklığa kavuşturmak ve tanımlamak için yapılan bir başlangıç çalışmasıdır (Zikmund, 2002: 368).

Bu çalışma, temel felsefesi açısından uygulamalı, amaç açısından keşifsel, yöntemi açısından nicel, süresi açısından kesitsel, analiz birimi açısından örgüt seviyesinde bir araştırmadır.

3.2. Araştırmanın Evren ve Örneklemi

Bu çalışma, 2016 yılının ikinci yarısı ve 2017 yılının ilk çeyreğinde Gaziantep'te faaliyet gösteren orta ve büyük ölçekli kuruluşlarda yapılmıştır. Araştırma kapsamında alınacak kuruluşların belirlenmesinde orta ölçekli işletmeler için en az 50-249 çalışanı olması veya yıllık 10.000.000 TL üzeri ciroya sahip olmaları, büyük ölçekli kuruluşlar içinse 250 ve üzeri çalışanı veya yıllık 40.000.000 TL üzeri ciroya sahip olmaları kriter olarak belirlenmiştir. (KOSGEB, 2017) Çeşitli sektörlerde faaliyet gösteren küçük ve mikro büyüklükteki kuruluşlar araştırma kapsamı dışında tutulmuştur.

2016 yılı GTO (Gaziantep Ticaret Odası) ve GSO (Gaziantep Sanayi Odası) verilerine göre Gaziantep'te 99 büyük ölçekli ticari işletme ve 203 orta ölçekli ticari işletme faaliyet göstermektedir. Dolayısıyla, araştırmanın ana kütlesini Gaziantep ilinde imalat sanayiinde faaliyet gösteren orta ve büyük ölçekli 302 kuruluş oluşturmaktadır.

Bu çalışmada öncelikle örneklem seçiminde çalışan sayısına göre orta ve büyük işletmeler olmak üzere iki tabaka oluşturulmuş, sonra bu tabakalar içinden kolayda örneklem yöntemi ile veriler toplanmıştır. Veri toplanan işlemelere firma isminin ifşaa edilmeyeceği ve verilerin başka bir amaçla kullanılmayacağına yönelik taahhütte bulunulmuştur. Bunun sebebi işletmeler için sır niteliği taşıyan siber güvenlik hazırlık seviyesi konusundaki bilgilerin daha kolay toplanabilmesidir. Kolayda örnekleme, ana kütle içerisinden seçilecek örnek kesimin araştırmacının yargılarınca belirlendiği tesadüfî olmayan örnekleme yöntemidir. Kolayda örneklemede veriler, ana kütleden en kolay, hızlı ve ekonomik şekilde toplanır (Malhotra, 2004: 321, Aaker vd., 2007: 394).

Bu çalışmada elde edilen verilerin tamamı yüz yüze görüşme yolu ile toplanmıştır. Bu kapsamda analize değer görülen toplam 128 veri elde edilmiştir. Yani araştırmanın örneklemi 128 işletmeden oluşmaktadır. Örneklemin ana kütleyi yansıtma oranı % 42'dir (128/302=0,423).

3.3. Veri Toplama Araçları

Bu çalışmada veri toplama aracı olarak anket tekniği kullanılmıştır. Uygulanan anket formu Ek1 de sunulmuştur. Anket formu 6 bölümden oluşmaktadır. Birinci bölümde Siber Güvenliğine Kurumsal Yaklaşım ile ilgili, ikinci bölümde Fiziksel ve Çevresel Güvenlik Tedbirleri ile ilgili, üçüncü bölümde Bilişim Sistemleri ve İletişim Ağlarının İşletim Ve Bakım Kontrolleri ile ilgili, dördüncü bölümde Yazılım Geliştirme ve Destek Aşamalarında Bilgi Sistemleri Erişim Kontrolü Güvenlik Tedbirleri ile ilgili, beşinci bölümde Siber Güvenlik İhlalleri ve İş Sürekliliği Yönetimi ile ilgili sorular bulunmaktadır. Altıncı bölümde ise işletmelerin çalışan sayısı, sermayesi, cirosu, ofis sayısı vb. bazı işletme özelliklerine yönelik sorular bulunmaktadır.

3.3.1. Araştırma Kullanılan Ölçekler

Bu çalışma kapsamında işletmelerin siber güvenlik yönetimi düzeylerini belirlemek amacıyla ölçekler, Japonya Ticaret ve İnovasyon Bakanlığı'na bağlı Japonya Bilgi Teknolojileri Özendirme Ajansı'nın (IPA) Bilgi Güvenliği Yönetimi Kıyaslama Sistemi'nden (ISM-Benchmark) uyarlanarak hazırlanmıştır (IPA, 2016). Bu kapsamda araştırmada kullanılan değişkenlere ilişkin ölçek; alanında uzmanlar tarafından İngilizceden Türkçeye çevrilmiş, Türkçeleştirilen soruların geçerliliği ve güvenirliliği, alanında uzman akademisyenler tarafından kontrol edilerek gerekli görülen düzenleme ve geliştirmeler yapılmıştır.

Araştırmada kullanılan ölçekler, 5'li Likert tipindedir. Bu kapsamda katılımcılardan değişkenlere ait her bir soru için 1=Hiç katılmıyorum/hiç uygulanmıyor, 2=Kısmen katılıyorum/kısmen uygulanıyor, 3=Çoğunlukla katılıyorum/çoğunlukla uygulanıyor, 4=Katılıyorum/uygulanıyor ve 5=Tamamen katılıyorum/tamamen uygulanıyor seçeneklerinden birisini tercih etmeleri istenmiştir.

3.4. Pilot Çalışma

Bir araştırmada kullanılacak ölçek geliştirilirken ölçek soruların her biri ayrı ayrı ve tümü bir bütün olarak değerlendirmeye alınmalıdır. Bu değerlendirme sürecine pilot test veya ön test denir. Pilot testinin amacı, ölçekteki her sorunun nasıl ifade edilmesi gerektiği, soruları cevaplayanların nasıl anlayacağını değerlendirmek ve verilebilecek alternatif cevapların yeterli olup olmadığını kontrol etmektir. Yeni geliştirilen bir ölçeğin sorularının çok iyi pilot test yapılması gerekse de daha önceden kullanılmış ve test edilmiş ölçeklerdeki soruların da ön test yapılması gerekir. Çünkü bir örneklemdeki sorular başka bir örneklem için uygun olmayabilir. Bir pilot çalışma veya test yapılırken aşağıdaki hususlara dikkat edilmelidir (De Vaus, 2002:151):

1.Kime pilot çalışma yapılmalıdır? Temel çalışma hangi grup üzerinden yapılacaksa pilot çalışma da benzer grup üzerinden alınan örneklem ile yapılmalıdır.

2.Pilot çalışma kaç defa yapılmalıdır? Pilot çalışmada elde edilen veri istatistiksel analize uygun olmalıdır.

Pilot çalışmada ölçeğin geçerlik ve güvenirliği ne kadar kanıtlanmış olsa da uyarlanan ölçekteki bazı maddelerin uyarlandığı kültürdeki geçerlik ve güvenirliği sorgulanmalıdır. Dolayısıyla ölçekteki bir maddenin uyarlama yapılan kültüre uygun olmaması durumunda madde ya değiştirilir ya da tamamen anketten çıkarılır. Eğer uygun olmayan maddeler araştırmacılar tarafından belirlenememişse, bu maddeler veri analizinde ortaya çıkacaktır. (Akbaş ve Korkmaz, 2017:16).

Bu çalışmada temel çalışma yapılmadan önce Gaziantep organize sanayi bölgesindeki imalat işletmeleri üzerinde bir pilot çalışma yapılmıştır. Bu kapsamda araştırmada kullanılacak anket formu; 2016 yılı Kasım ve Aralık aylarında Gaziantep'teki toplam 53 işletmede yüz yüze görüşme yolu elde edilen verilerle pilot çalışma yapılmıştır. Pilot çalışma sırasında anketin cevaplandırılma süresinin 5-10 dakika aralığında olduğu ve ankete cevap veren kişilerin soruları doğru anladığı ve cevapları samimi bir şekilde verdiği görülmüştür. Bu durum anket formunun veya soruların iyi hazırlandığına yönelik bir kanaat oluşturmuştur. Pilot çalışmada elde edilen 53

verinin tamamı ön test için değerlendirmeye alınmıştır. Pilot çalışmada elde edilen verilerin analizlerine ilişkin bulgular aşağıda sırası ile verilmiştir.

Tablo 12. Pilot Uygulama Demografik Bilgiler

Çalışan Sayısı	**Frekans**	**Yüzde**	**Kümülatif Yüzde**
0-49	7	13,2	13,2
51-250	22	41,5	54,7
250 ve üstü	24	45,3	100
Toplam	53	100	
Yıllık Ciro	**Frekans**	**Yüzde**	**Kümülatif Yüzde**
8.000.001-40.000.000	5	9,4	9,4
40.000.001 ve üzeri	48	90,6	100
Toplam	53	100	
Firma Sermayesi	**Frekans**	**Yüzde**	**Kümülatif Yüzde**
1 milyondan az	2	3,8	3,8
1-10 milyon	7	13,2	17
10-50 milyon	13	24,5	41,5
50-100 milyon	17	32,1	73,6
100 milyon üzeri	14	26,4	100
Toplam	53	100	
Bilişim Sistemlerine Bağımlılık Oranı	**Frekans**	**Yüzde**	**Kümülatif Yüzde**
%25 az	-	-	-
%25-50	1	1,9	1,9
%50-75	18	34	35,8
%75 üstü	34	64,2	100
Toplam	53	100	
Siber Güvenlik Olayı İle Karşılaşma	**Frekans**	**Yüzde**	**Kümülatif Yüzde**
Evet	38	71,7	71,7
Hayır	15	28,3	100
Toplam	53	100	

Tablo 12'de görüleceği üzere pilot çalışmaya katılan işletmelerin büyük çoğunluğu orta ve büyük işletmeden oluşmaktadır. Pilot çalışmaya katılan işletmelerden yalnızca 7'si küçük işletmedir. Yıllık ciroları açısından çalışmaya katılan işletmelerin %90,6'sı büyük işletme kapsamındadır. Yine pilot araştırmaya katılan firmaların %83'nün sermayesi 10 milyondan üzerindedir. Pilot çalışmanın elde verilerinin genelde orta ve büyük imalat işletmelerinden oluşması, yapılacak ana çalışmanın örneklem özellikleri ile örtüşmektedir. Dolayısıyla çalışmada

elde edilen verilerin pilot çalışma için uygun olduğunu göstermektedir. Pilot araştırmaya katılan işletmelerin iş faaliyetlerinin dayandığı bilişim sistemlerine bağımlılık oranları çok yüksek olduğu görülmektedir. Pilot çalışmaya katılan işletmelerin %98,1'nin bilişim sistemlerine yüzde 50'nin üzerindedir. Yine bu işletmelerin büyük çoğunluğu (%71,7'si) bir siber güvenlik olayı ile karşılaşmışlardır.

3.4.1. Pilot Uygulama Keşfedici Faktör Analizi

Bu çalışmada kullanılacak ölçeğin yapısal geçerliliğini test etmek için temel bileşenler analizi kullanılarak keşfedici faktör analizi uygulanmıştır. Analiz sonucunda büyüklüğünün faktör analizi için yeterli olduğu belirlenmiştir. KMO ve Barlett değerleri Tablo 13'de verilmiştir

Tablo 13. Pilot Uygulama Ölçeği KMO ve Barlett Değerleri

KMO ve Bartlett Testi		
Kaiser-Meyer-Olkin Örnekleme Yeterliliğinin Ölçümü		,754
Bartlett'in Küresellik Testi	Yaklaşık Ki-Kare	304,684
	df	28
	Sig.	,000

Tablo 13'de görüldüğü üzere Örnekleme Yeterliliğinin Ölçümü Testi KMO değerinin 0,754 olduğu ve dolayısıyla örneklem büyüklüğünün faktör analizi için yeterlidir. Ayrıca, Bartlett küresellik testinin anlamlı olması [$\chi 2$ (28) =304,684 ρ<0.000] maddeler arasındaki korelasyon ilişkilerinin faktör analizi için uygun olduğunu göstermektedir. Analiz sonucunda 5 faktörden oluşan ve toplam varyansın %74.386'sını açıklayan bir yapıya ulaşılmıştır. Ölçeğin döndürülmüş bileşenler matrisi Tablo 14'de verilmiştir

Tablo 14. Pilot Uygulama Ölçeği Döndürülmüş Bileşenler Matrisi

Değişkenler	**Faktör 1**	**Faktör 2**	**Faktör 3**	**Faktör 4**	**Faktör 5**
Soru 1	,807				
Soru 2	,916				
Soru 3	,758				
Soru 4	,836				
Soru 5	,734				
Soru 6	,818				
Soru 7	,685				
Soru 8	,759				
Soru 9		,760			
Soru 10		,758			
Soru 11		,747			

Soru 12		,760			
Soru 13			,811		
Soru 14			,725		
Soru 15			,852		
Soru 16			,851		
Soru 17			,869		
Soru 18			,755		
Soru 19			,739		
Soru 20				,769	
Soru 21				,823	
Soru 22				,833	
Soru 23				,802	
Soru 24				,766	
Soru 25					,822
Soru 26					,848
Soru 27					,915

Tablo 14'de görüldüğü üzere araştırmada kullanılan 5 değişkene yönelik ölçek, öngörüldüğü üzere 5 faktörlü yapısı doğrulamıştır. Bu kapsamda analizinde; 8 maddeden oluşan "Siber Güvenliğine Kurumsal Yaklaşım" ölçeği Faktör 1 altında, 4 maddeden oluşan "Fiziksel ve Çevresel Güvenlik Tedbirleri" ölçeği Faktör 2 altında, 7 maddeden oluşan "Bilişim Sistemleri ve İletişim Ağlarının İşletim ve Bakım Kontrolleri" ölçeği Faktör 3 altında, 5 maddeden oluşan "Bilişim Sistemleri ve İletişim Ağlarının İşletim ve Bakım Kontrolleri" ölçeği Faktör 4 altında ve 3 maddeden oluşan "Siber Güvenlik İhlalleri ve İş Sürekliliği Yönetimi" ölçeği Faktör altında toplanmıştır. Tabloda görüldüğü üzere en düşük fakör yükü 0,685 olup tüm faktörlerin yükleri yüksektir. Dolayısıyla araştırmada kullanılan ölçeklerin, her değişken iyi ölçtüğünü göstermektedir.

3.4.2. Pilot Uygulama Güvenilirlik Analizi

Güvenilirlik kavramı, ölçeklerde yer alan ifadelerin birbirleri ile olan tutarlılığını ve ölçeğin ilgilenilen sorunu ne derece yansıttığını ifade eder. Pilot çalışmada da araştırmada kullanılan ölçeklerin güvenilirlik analizleri yapılmış ve elde edilen analizi sonuçları Tablo 15'de verilmiştir.

Tablo 15. Pilot Uygulama Güvenilirlik Analizi

Ölçekler	Cronbach Alpha	Madde Sayısı
1.Siber Güvenliğine Kurumsal Yaklaşım	0,913	8
2.Fiziksel ve Çevresel Güvenlik Tedbirleri	0,749	4
3.Bilişim Sistemleri ve İletişim Ağlarının İşletim ve Bakım Kontrolleri	0,906	7
4.Yazılım Geliştirme ve Destek Aşamalarında Bilgi Sistemleri Erişim Kontrolü Güvenlik Tedbirleri	0,857	5
5.Siber Güvenlik İhlalleri ve İş Sürekliliği Yönetimi	0,817	3

Tablo 15'de görüldüğü üzere araştırmada kullanılan ölçeklerin tümünün alpha katsayıları yüksek çıkmıştır. Alpha katsayısı 0,60'nın üzerinde olursa ölçek, oldukça güvenilir, 0,80'nin üzerinde olursa ölçek, yüksek derecede güvenilirdir (Kalaycı, 2008: 405). Dolaysıyla pilot çalışmada kullanılan ölçeklerin güvenilirliklerinin oldukça iyi ve yüksek olduğu görülmektedir.

3.5. Faktör Analizleri

Araştırmada kullanılan ölçeklerin yapı geçerliliğini belirlemek amacıyla keşfedici faktör analizi ve ardından ölçeklerin öngörülen yapıya uyup uymadığını belirlemek maksadıyla doğrulayıcı faktör analizleri yapılmıştır. Daha sonra ölçekleri oluşturan ifadelerin kendi aralarında tutarlılık gösterip göstermediğini belirlemek maksadıyla ölçeklere ve alt boyutlarına ilişkin güvenilirlik analizleri uygulanmıştır.

3.5.1. Keşfedici Faktör Analizleri

Araştırmada yer alan ölçekleri oluşturan değişkenlerin faktör yapısını belirlemek ve bu değişkenlerin hangi faktörler altında toplandığını belirlemek amacıyla Keşfedici Faktör Analizi (KFA) yapılmıştır. Altunışık vd. (2010: 262)'ne göre faktör analizi, aralarında ilişki bulunan çok sayıda değişkenden oluşan veri setine ait temel faktörlerin ortaya çıkarılmasını ve araştırmacı tarafından ilişkinin yapısına dair veri setinde yer alan kavramlar arasındaki ilişkilerin daha kolay anlaşılır olmasını sağlar. Faktör analizinde; aralarında yüksek korelasyon bulunan veri setinin bir araya getirilmesi yoluyla faktör adı verilen genel değişkenlerin (faktörlerin) oluşturulması söz konusudur (Kalaycı, 2008: 321). Keşfedici faktör analizi, daha çok ölçek geliştirme ve test etme çalışmalarının ilk aşamalarında kullanılır. KFA'da yapının geçerliliğine dair kanıtlar; gözlenen değişkenlerin hangi faktörler altında toplandığı, değişkenlerin faktör yük kat sayıları, faktörlerin açıkladıkları varyans oranları gibi ölçütlere göre yorumlanır (Gürbüz ve Şahin, 2016: 310).

Veri setine faktör analizi uygulanabilirliğinin test edilmesi amacıyla KMO (Kaiser-Meyer-Olkin) "Örnekleme Yeterliliğinin Ölçümü Testi" ve Bartlett'in (Bartlett's Test of Sphericity) "Küresellik Testi"nden yararlanılmaktadır. KMO değerinin 0,60 ve üstünde olması, örneklemin faktör analizi için yeterli olacağına işaret etmekteyken, Hutcheson ve Sofroniou (1999) bu değerin 0,5 ile 0,7 arasının normal; 0,7 ile 0,8 arasının iyi; 0,8 ile 0,9 arasının çok iyi; 0,9 ve üzerinin ise mükemmel olduğunu belirtmektedir (Dağlı, 2015: 205). Bartlett'in küresellik testi ise korelasyon matrisindeki ilişkilerin faktör analizi yapacak ölçüde yeterli olup olmadığını test etmektedir. Bu test sonucunun anlamlı olması ($\rho<0,05$) değişkenler arası ilişkilerin oluşturduğu matrisin faktör analizi için anlamlı olduğunu ve faktör analizi yapılabileceğini göstermektedir (Gürbüz ve Şahin, 2016: 311). KMO değerlerine ilişkin bilgiler Tablo 16'da sunulmuştur.

Tablo 16. KMO Değerleri

KMO Değeri	Yorum
0,90	Mükemmel
0,80	Çok İyi
0,70	İyi
0,60	Orta
0,50	Zayıf
0,50'nin altı	Kabul Edilemez

Kaynak: Sharma, 1996:116'den aktaran Kalaycı, 2014:322.

3.5.1.1. Siber Güvenliğine Kurumsal Yaklaşım Ölçeği KFA

Araştırmada yer alan ölçekleri oluşturan değişkenlerin faktör yapısını belirlemek ve bu değişkenlerin hangi faktörler altında toplandığını belirlemek amacıyla Keşfedici Faktör Analizi (KFA) yapılmıştır. KFA sonucunda elde edilen KMO ve Barlett testi değerleri Tablo 17'de verilmiştir.

Tablo 17. Siber Güvenliğine Kurumsal Yaklaşım KMO ve Barlette Değerleri

KMO ve Bartlett Testi		
Kaiser-Meyer-Olkin Örnekleme Yeterliliğinin Ölçümü		,885
Bartlett'in Küresellik Testi	Yaklaşık Ki-Kare	697,267
	df	28
	Sig.	,000

Yapılan keşfedici faktör analizi neticesinde tek faktörlü bir yapıya ulaşılmıştır. 8 maddeden oluşan ölçeğin tek faktör altında toplandığı ve toplam varyansın %64,127'sini açıkladığı tespit edilmiştir. KMO sonucunda örneklem yeterlilik değerinin 0,885 olduğu ve örneklem büyüklüğünün faktör analizi için yeterli olduğu belirlenmiştir. Ayrıca, Bartlett küresellik testinin anlamlı olması [$\chi 2$ (28) =697,267, $\rho<0.001$] maddeler arasındaki korelasyon ilişkilerinin faktör analizi için uygun olduğunu göstermektedir. Maddelerin faktör yükleri Tablo 18'de verilmiştir.

Tablo 18. Siber Güvenliğine Kurumsal Yaklaşım Döndürülmüş Bileşenler Matrisi

Maddeler	Faktör Yükü
Kurumumuzun bilgi güvenliğine ilişkin yazılı kural ve politikaları vardır.	,758
Kurumumuz bilgi güvenliğine ilişkin yazılı kural ve politikaları oluştururken hayati öneme sahip alanlarda oluşabilecek, tehlike ve güvenlik açıklarını dikkate almıştır.	,918
Kurumumuz bilgi güvenliğine ilişkin kural ve politikaları, ülkemizdeki ilgili kanun ve yönetmeliklere uygundur.	,838
Kurumumuz kritik bilişim teknolojilerini önem derecesine göre sınıflandırıp, bu sistemleri oluşturulan sınıflandırmaya göre yönetir.	,704
Kurumumuz bilgi yaşam döngüsünün tüm aşamalarında gerekli güvenlik önlemlerini almaktadır. (Bilgi yaşam döngüsü: bilginin oluşturulması, kullanılması, depolanması, iletilmesi, işlenmesi ve imha edilmesi)	,796
Kurumumuz bilgi teknolojilerine yönelik hizmet alımlarında, gerekli güvenlik önlemlerini sözleşme maddelerine dahil eder.	,891
Kurumumuz tüm çalışanlara bilgi güvenliğine ilişkin yükümlülükleri açıkça bildirilmektedir.	,699
Kurumumuz tüm çalışanlara düzenli olarak bilgi güvenliği eğitimleri vermektedir.	,773

KFA sonucu siber güvenliğine kurumsal yaklaşım ölçeğine ait tüm maddelerin faktör yükleri 0,699 ile 0,918 arasında değerler aldığı bulgusu elde edilmiştir.

3.5.1.2. Fiziksel ve Çevresel Güvenlik Tedbirleri Ölçeği KFA

Ölçeğin yapısal geçerliliğini test etmek için temel bileşenler analizi kullanılarak KFA uygulanmıştır (Gürbüz ve Şahin, 2016: 322). KMO sonucunda örneklem yeterlilik değerinin 0,769 olduğu ve örneklem büyüklüğünün faktör analizi için yeterli olduğu belirlenmiştir. Ayrıca, Bartlett küresellik testinin anlamlı olması [$\chi 2$ (6) =258,225, $\rho<0.001$] maddeler arasındaki korelasyon ilişkilerinin faktör analizi için uygun olduğunu göstermektedir. KMO ve Barlett değerleri Tablo 19'da verilmiştir.

Tablo 19. Fiziksel ve Çevresel Güvenlik Tedbirleri KMO ve Barlett Değerleri

KMO ve Bartlett Testi		
Kaiser-Meyer-Olkin Örnekleme Yeterliliğinin Ölçümü		,769
Bartlett'in Küresellik Testi	Yaklaşık Ki-Kare	258,225
	df	6
	Sig.	,000

Yapılan keşfedici faktör analizi neticesinde tek faktörlü bir yapıya ulaşılmıştır. 4 maddeden oluşan ölçeğin tek faktör altında toplandığı ve toplam varyansın %70,52'sini açıkladığı tespit edilmiştir. Maddelerin faktör yükleri Tablo 20'de verilmiştir.

Tablo 20. Fiziksel ve Çevresel Güvenlik Tedbirleri Döndürülmüş Bileşenler Matrisi

Maddeler	Faktör Yükü
Kurumumuza ait tesislerin güvenliğini iyileştirmek için gerekli güvenlik önlemleri uygulanmaktadır.	,838
Kurumumuza ait tesislere giriş-çıkışı düzenleyen yazılı kurallar vardır.	,926
Kurumumuz, bilgi teknolojilerine yönelik her türlü tehlikeye (doğal felaketler veya insan kaynaklı zararlar) karşı koruyu önlemler alınmıştır.	,841
Kurumumuzda, taşınabilir bilgisayar veya harici depolama aygıtlarının kullanımına ilişkin güvenlik önlemleri alınmıştır	,746

KFA sonucu ölçeğin faktör yüklerinin 0,746 ile 0,926 arasında değerler aldığı bulgusu elde edilmiştir.

3.5.1.3. Bilişim Sistemleri ve İletişim Ağlarının İşletim ve Bakım Kontrolleri Ölçeği KFA

Ölçeğin yapısal geçerliliğini test etmek için temel bileşenler analizi kullanılarak KFA uygulanmıştır. KMO sonucunda örneklem yeterlilik değerinin 0,787 olduğu ve örneklem büyüklüğünün faktör analizi için yeterli olduğu belirlenmiştir. Ayrıca, Bartlett küresellik testinin anlamlı olması [$\chi 2$ (21) =274,881, $\rho<0.001$] maddeler arasındaki korelasyon ilişkilerinin faktör analizi için uygun olduğunu göstermektedir. KMO ve Barlett değerleri Tablo 21'de verilmiştir.

Tablo 21. Bilişim Sistemleri ve İletişim Ağlarının İşletim ve Bakım Kontrolleri KMO ve Barlett Değerleri

KMO ve Bartlett Testi		
Kaiser-Meyer-Olkin Örnekleme Yeterliliğinin Ölçümü		,787
Bartlett'in Küresellik Testi	Yaklaşık Ki-Kare	274,881
	df	21
	Sig.	,000

Yapılan keşfedici faktör analizi neticesinde tek faktörlü bir yapıya ulaşılmıştır. 7 maddeden oluşan ölçeğin tek faktör altında toplandığı ve toplam varyansın % 47.645'ini açıkladığı tespit edilmiştir. Maddelerin faktör yükleri Tablo 22'de verilmiştir.

Tablo 22. Bilişim Sistemleri ve İletişim Ağlarının İşletim ve Bakım Kontrolleri Döndürülmüş Bileşenler Matrisi

Maddeler	Faktör Yükü
Kurumumuz, bilgi teknolojileri verilerini (sistem konfigürasyon ve yedekleri) uygun bir şekilde korur.	,702
Kurumumuzda bilgi teknolojileri kurulum ve kullanım süreçleri bilgi güvenliği hususları dikkate alınarak icra edilir.	,570
Kurumumuz, verilerini uygun bir şekilde yedekler.	,740
Kurumumuz, kötü amaçlı yazılımlara (virüs, trojan, vb.) karşı önlemler alır.	,654
Kurumumuz, bilişim sistemlerinin güvenlik açıklarını azaltmak için önlemler alır.	,762
Kurumumuz, bilişim sistemlerine bağlantıları güvenli bir şekilde tesis eder. (VPN, sertifika vb.)	,720
Kurumumuz, tüm cihaz ve aygıtların çalınma riskine karşı önlemler alır.	,664

KFA sonucu ölçeğin faktör yüklerinin 0,570 ile 0,740 arasında değerler aldığı bulgusu elde edilmiştir.

3.5.1.4. Yazılım Geliştirme ve Destek Aşamalarında Bilgi Sistemleri Erişim Kontrolü Güvenlik Tedbirleri Ölçeği KFA

KMO sonucunda örneklem yeterlilik değerinin 0,787 olduğu ve örneklem büyüklüğünün faktör analizi için yeterli olduğu belirlenmiştir. Ayrıca, Bartlett küresellik testinin anlamlı olması [$\chi 2$ (10) =234,346, $\rho<0.001$] maddeler arasındaki korelasyon ilişkilerinin faktör analizi için uygun olduğunu göstermektedir. KMO ve Barlett değerleri Tablo 23'de verilmiştir.

Tablo 23. Yazılım Geliştirme ve Destek Aşamalarında Bilgi Sistemleri Erişim Kontrolü Güvenlik Tedbirleri KMO ve Barlett Değerleri

KMO ve Bartlett Testi		
Kaiser-Meyer-Olkin Örnekleme Yeterliliğinin Ölçümü		,787
Bartlett'in Küresellik Testi	Yaklaşık Ki-Kare	234,346
	df	10
	Sig.	,000

Yapılan keşfedici faktör analizi neticesinde tek faktörlü bir yapıya ulaşılmıştır. 5 maddeden oluşan ölçeğin tek faktör altında toplandığı ve toplam varyansın % 59,374'ünü açıkladığı tespit edilmiştir. Maddelerin faktör yükleri Tablo 24'de verilmiştir.

Tablo 24. Yazılım Geliştirme ve Destek Aşamalarında Bilgi Sistemleri Erişim Kontrolü Güvenlik Tedbirleri Döndürülmüş Bileşenler Matrisi

Maddeler	Faktör Yükü
Kurumumuz, bilişim sistemlerine bağlantı için gerekli kimlik denetimlerini yapar.	,791
Kurumumuzda bilişim teknolojilerine kimlerin hangi şartlarda erişebileceği düzenlemiştir.	,819
Kurumumuz, yerel ağlar üzerinde yetki denetimi uygular.	,800
Kurumumuz, yazılım geliştirme projelerinin güvenlik gereksinimlerini projelere dâhil eder.	,711
Kurumumuz, yazılım ürünlerinin seçimi, satın alınması ve / veya bakım işlerinde güvenlik kontrolleri gerçekleştirir.	,724

KFA sonucu ölçeğin faktör yüklerinin 0,711 ile 0,819 arasında değerler aldığı bulgusu elde edilmiştir.

3.5.1.5. Siber Güvenlik İhlalleri ve İş Sürekliliği Yönetimi Ölçeği KFA

KMO sonucunda örneklem yeterlilik değerinin 0,657 olduğu ve örneklem büyüklüğünün faktör analizi için yeterli olduğu belirlenmiştir. Ayrıca, Bartlett küresellik testinin anlamlı olması [$\chi 2\ (3) = 138{,}939$, $\rho < 0.001$] maddeler arasındaki korelasyon ilişkilerinin faktör analizi için uygun olduğunu göstermektedir. KMO ve Barlett değerleri Tablo 25'de verilmiştir.

Tablo 25. Siber Güvenlik İhlalleri ve İş Sürekliliği KMO ve Barlett Değerleri

KMO ve Bartlett Testi		
Kaiser-Meyer-Olkin Örnekleme Yeterliliğinin Ölçümü		,657
Bartlett'in Küresellik Testi	Yaklaşık Ki-Kare	138,939
	df	3
	Sig.	,000

Yapılan keşfedici faktör analizi neticesinde tek faktörlü bir yapıya ulaşılmıştır. 3 maddeden oluşan ölçeğin tek faktör altında toplandığı ve toplam varyansın % 71,595'ini açıkladığı tespit edilmiştir. Maddelerin faktör yükleri Tablo 26'da verilmiştir.

Tablo 26. Siber Güvenlik İhlalleri ve İş Sürekliliği Döndürülmüş Bileşenler Matrisi

Maddeler	Faktör Yükü
Kurumumuz, bilişim arızalarının kurum faaliyetlerini aksatmaması için önlemler alır.	,749
Kurumumuzda, olası bilişim kaynaklı problemler için acil eylemleri belirten yazılı prosedürler bulunur.	,888
Kurumumuzun, tüm bileşenleri kapsar nitelikte arızalara karşı mücadeleyi ele alan bir İSY (İş Sürekliliği Yönetimi) bulunmaktadır.	,893

KFA sonucu ölçeğin faktör yüklerinin 0,749 ile 0,893 arasında değerler aldığı bulgusu elde edilmiştir.

3.5.2. Doğrulayıcı Faktör Analizleri

Çalışmada; keşfedici faktör analizi (KFA) sonucunda elde edilen faktör yapılarını doğrulamak amacıyla "Doğrulayıcı Faktör Analizleri (DFA)" yapılmıştır. Doğrulayıcı faktör analizi (DFA); daha önce geliştirilmiş veya sağlam bir kuramsal temele dayalı olan ölçek ve yapıların veri ile doğrulanması amacıyla kullanılır (Gürbüz ve Şahin, 2016: 310). DFA ile doğrulanmaya çalışılan modelin uyum yeterliliğini test amacıyla çeşitli uyum indeksleri kullanılmaktadır. Bu uyum indeksleri arasında en çok $\chi 2$ (Relative Chi Square Index), RMSEA (Root Mean Square Error of Approximation), GFI (Goodness of Fit Index), AGFI (Adjustment Goodness of Fit Index), CFI (Comparative Fit Index), NFI (Normed Fit Index), TLI (Tucker-Lewis Index) veya NNFI (Non-Normed Fit Index) indeksleri kullanılmaktadır (Olpak ve Çakmak, 2009, 150). DFA İyi Uyum ve kabul edilebilir uyum değerleri Tablo 27'de verilmiştir.

Tablo 27. DFA Uyum İyiliği Değerleri

Uyum İndeksleri	İyi Uyum	Kabul Edilebilir Uyum
CMIN/DF	≤3	≤5
RMSEA	≤0,05	≤0,08
GFI	≥0,90	≥0,85
AGFI	≥0,90	≥0,85
NFI	≥0,95	≥0,90
CFI	≥0,97	≥0,90
TLI	≥0,95	≥0,90

Kaynak: Meydan ve Şeşen, 2015:37; Gürbüz ve Şahin, 2016:337.

χ2 (Relative Chi Square Index); ki-kare uyum testi değeri, araştırmacının kuramsal olarak önermiş olduğu model ile örneklemden elde edilen verinin uyumlu olup olmadığını test etmektedir. χ2/df değerinin 3 ve altında olması modelin iyi bir uyum gösterdiğini, 3-5 arasında bir değer alması ise modelin kabul edilebilir olduğunu göstermektedir (Gürbüz ve Şahin, 2016: 337).

RMSEA (Root Mean Square Error of Approximation); yaklaşık hataların ortalama karekökü şeklinde tanımlanan ve modelin örneklem ile uyumlu olup olmadığını test eden bu değer, 0 ile 1 arasında değerler alır. Sıfıra yakın değerler vermesi istenir. 0,08'e kadar olan değerlerin kabul edilebilir uyuma sahip olduğunu gösterir (Meydan ve Şeşen, 2015: 34).

GFI (Goodness of Fit Index); iyilik uyum indeksi olarak ifade edilen bu değer model uyumunu örneklem büyüklüğünden bağımsız olarak test eder. 0 ile 1 değerleri arasında değişmektedir. 0,90 ve üzeri değerler oldukça iyi uyumu gösterirken 0,85 ve üzeri değerler, ise kabul edilebilir değer olarak görülmektedir (Meydan ve Şeşen, 2015: 34).

AGFI (Adjustment Goodness of Fit Index); düzeltilmiş iyilik uyum indeki olarak tanımlanan bu değer, örneklem genişliği dikkate alınarak düzeltilmiş GFI değeridir. 0,90 ve üzeri değerler iyi uyumu, 0,85 ve üzeri değerler ise kabul edilebilir uyumu göstermektedir (Gürbüz ve Şahin, 2016: 337).

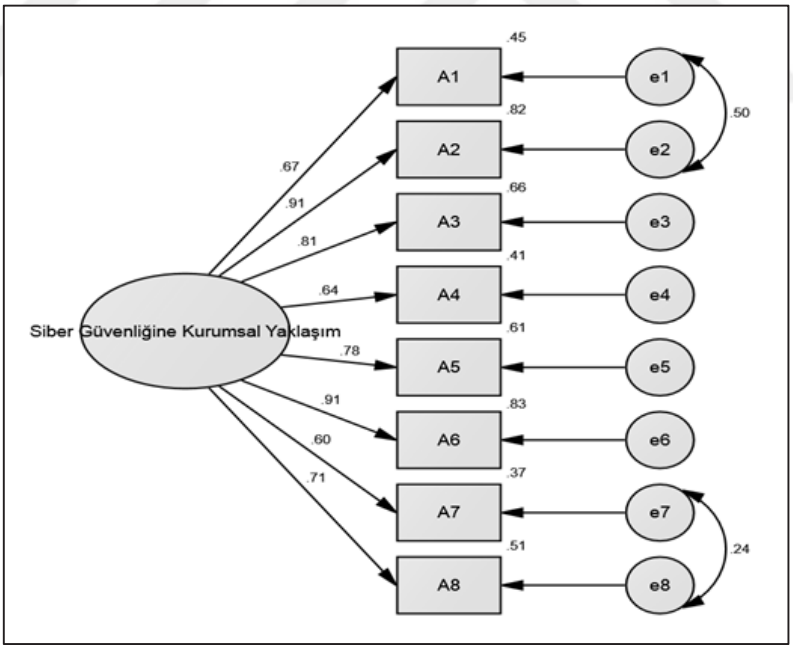
NFI (Normed Fit Index); normlaştırılmış uyum indeksi olarak tanımlanan bu değer, test edilen modelin ki-kare değerinin, bağımsız modelin ki-kare değerine bölünmesi ile bulunur. İndeksin alacağı 0,90 ve üzeri değerler kabul edilebilir uyumu göstermektedir (Meydan ve Şeşen, 2015: 33).

CFI (Comparative Fit Index); karşılaştırmalı uyum indeksi olarak bilinen CFI, serbestlik derecesi ($\chi 2$) ve örneklem büyüklüğünü dikkate alarak test edilen modelin, temel modele göre karşılaştırmasını yapar. Bu değerin 1'e yakın olması uyumun iyiliğine işaret eder. GFI'nın 0,90 ve üzerinde olması modelin kabul edilebileceğine işaret etmektedir (Gürbüz ve Şahin, 2016: 338).

TLI (Tucker-Lewis Index) veya NNFI (Non-Normed Fit Index); normlaştırılmamış uyum indeksi, NFI'nin serbestlik derecesi dikkate alınarak hesaplanmış halidir. Bu değerin 0,90 ve üzeri olması kabul edilebilir uyumu göstermektedir (Meydan ve Şeşen, 2015: 33).

3.5.2.1. Siber Güvenliğine Kurumsal Yaklaşım Ölçeği DFA

Ölçekte yer alan ifadelerin oluşturduğu faktör yapısı KFA ile belirlendikten sonra ölçeğin yapısal doğruluğunu test etmek amacıyla DFA yapılmıştır. DFA analizi sonuçları Şekil 38'de, analiz sonucunda elde edilen uyum iyiliği değerleri diğer ölçeklerle birlikte toplu olarak Tablo 27'de verilmiştir.



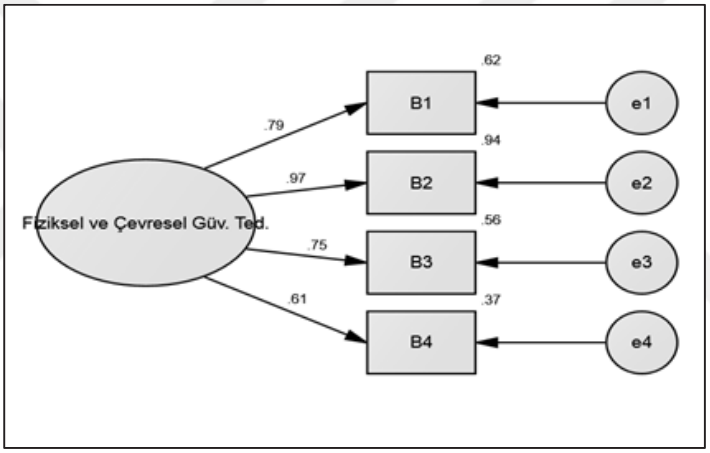
Şekil 38. Siber Güvenliğine Kurumsal Yaklaşım DFA

DFA sonucu ölçeğin faktör yükleri 0,61 ile 0,91 arasında elde edilmiştir. Uyum iyiliği değerlerinin sağlamak amacı ile "Kurumumuzun bilgi güvenliğine ilişkin yazılı kural ve politikaları vardır" maddesi ile" Kurumumuz bilgi güvenliğine ilişkin yazılı kural ve politikaları oluştururken hayati öneme sahip alanlarda oluşabilecek, tehlike ve güvenlik açıklarını dikkate almıştır" maddesi ve "Kurumumuz tüm çalışanlara bilgi güvenliğine ilişkin yükümlülükleri

açıkça bildirilmektedir" maddesi ile "Kurumumuz tüm çalışanlara düzenli olarak bilgi güvenliği eğitimleri vermektedir" maddesi hata terimleri arasında modifikasyon yapılmıştır. Modifikasyon yapma gerekliliğinin nedeninin bu maddelerin katılımcılar tarafından birbirine yakın olarak algılanmasından kaynaklandığı düşünülmektedir.

3.5.2.2. Fiziksel ve Çevresel Güvenlik Tedbirleri Ölçeği DFA

Ölçekte yer alan ifadelerin oluşturduğu faktör yapısı KFA ile belirlendikten sonra ölçeğin yapısal doğruluğunu test etmek amacıyla DFA yapılmıştır. DFA analizi sonuçları Şekil 39'da, analiz sonucunda elde edilen uyum iyiliği değerleri diğer ölçeklerle birlikte toplu olarak Tablo 27'de verilmiştir.

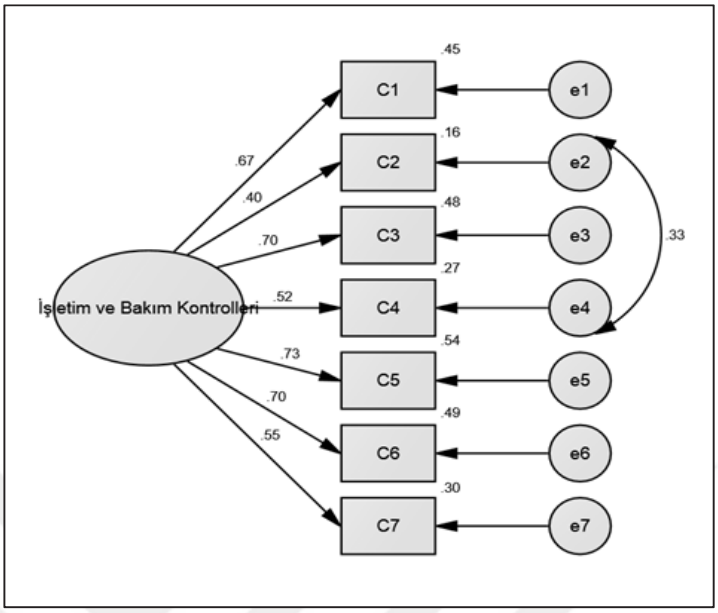


Şekil 39. Fiziksel ve Çevresel Güvenlik Tedbirleri DFA

DFA sonucu ölçeğin faktör yükleri 0,61 ile 0,97 arasında elde edilmiştir.

3.5.2.3. Bilişim Sistemleri ve İletişim Ağlarının İşletim ve Bakım Kontrolleri Ölçeği DFA

Ölçekte yer alan ifadelerin oluşturduğu faktör yapısı KFA ile belirlendikten sonra ölçeğin yapısal doğruluğunu test etmek amacıyla DFA yapılmıştır. DFA analizi sonuçları Şekil 40'da, analiz sonucunda elde edilen uyum iyiliği değerleri diğer ölçeklerle birlikte toplu olarak Tablo 27'de verilmiştir.

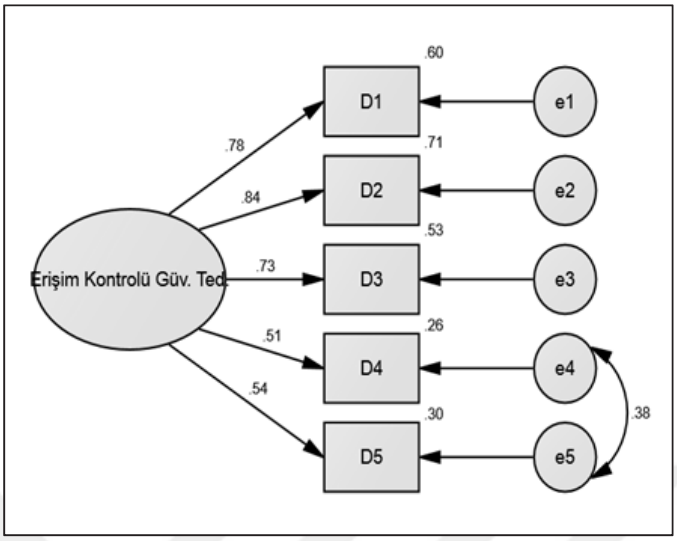


Şekil 40. Bilişim Sistemleri ve İletişim Ağlarının İşletim ve Bakım Kontrolleri DFA

DFA sonucu ölçeğin faktör yükleri 0,40 ile 0,73 arasında elde edilmiştir. Uyum iyiliği değerlerini elde edebilmek amacı ile "Kurumumuzda bilgi teknolojileri kurulum ve kullanım süreçleri bilgi güvenliği hususları dikkate alınarak icra edilir" maddesi ile "Kurumumuz, kötü amaçlı yazılımlara (virüs, trojan, vb.) karşı önlemler alır" maddesi hata terimleri arasında modifikasyon yapılmıştır.

3.5.2.4. Yazılım Geliştirme ve Destek Aşamalarında Bilgi Sistemleri Erişim Kontrolü Güvenlik Tedbirleri Ölçeği DFA

Ölçekte yer alan ifadelerin oluşturduğu faktör yapısı KFA ile belirlendikten sonra ölçeğin yapısal doğruluğunu test etmek amacıyla DFA yapılmıştır. DFA analizi sonuçları Şekil 41'de, analiz sonucunda elde edilen uyum iyiliği değerleri diğer ölçeklerle birlikte toplu olarak Tablo 27'de verilmiştir.

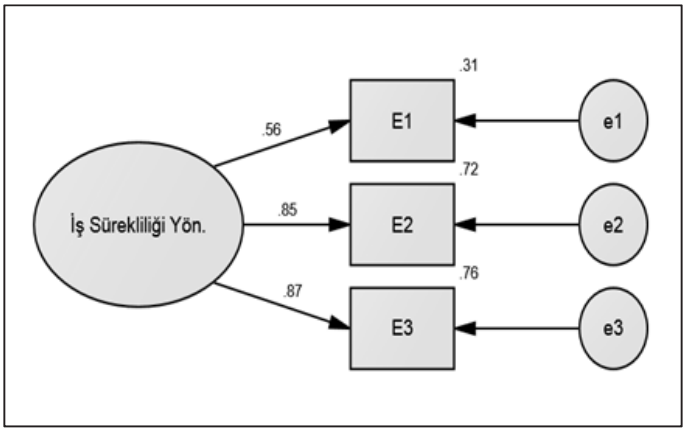


Şekil 41. Yazılım Geliştirme ve Destek Aşamalarında Bilgi Sistemleri Erişim Kontrolü Güvenlik Tedbirleri DFA

DFA sonucu ölçeğin faktör yükleri 0,51 ile 0,84 arasında elde edilmiştir. Uyum iyiliği değerlerini elde edebilmek amacı ile "Kurumumuz, yazılım geliştirme projelerinin güvenlik gereksinimlerini projelere dâhil eder" maddesi ile "Kurumumuz, yazılım ürünlerinin seçimi, satın alınması ve/veya bakım işlerinde güvenlik kontrolleri gerçekleştirir" maddesi hata terimleri arasında modifikasyon yapılmıştır.

3.5.2.5. Siber Güvenlik İhlalleri ve İş Sürekliliği Yönetimi Ölçeği DFA

Ölçekte yer alan ifadelerin oluşturduğu faktör yapısı KFA ile belirlendikten sonra ölçeğin yapısal doğruluğunu test etmek amacıyla DFA yapılmıştır. DFA analizi sonuçları Şekil 42'de, analiz sonucunda elde edilen uyum iyiliği değerleri diğer ölçeklerle birlikte toplu olarak Tablo 27'de verilmiştir.



Şekil 42. Siber Güvenlik İhlalleri ve İş Sürekliliği Yönetimi DFA

DFA sonucu ölçeğin faktör yükleri 0,56 ile 0,87 arasında elde edilmiştir.

Tablo 28. Ölçekler Uyum İyiliği Değerleri

Değişkenler	X2	df	CMIN/df	GFI	AGFI	CFI	TLI	RMSEA
Siber güvenliğine kurumsal yaklaşım	32,445	18	0,802	0,939	0,877	0,979	0,967	0,079
Fiziksel ve çevresel güvenlik tedbirleri	2,378	2	1,189	0,991	0,953	0,999	0,996	0,039
Bilişim sistemleri ve iletişim ağlarının işletim ve bakım kontrolleri	18,14	11	1,649	0,963	0,906	0,973	0,948	0,071
Yazılım Geliştirme ve Destek Aşamalarında Bilgi Sistemleri Erişim Kontrolü Güvenlik Tedbirleri	7,102	4	1,775	0,979	0,92	0,986	0,966	0,078
Siber Güvenlik İhlalleri ve İş Sürekliliği Yönetimi	0,00	0,00	0,00	1,00	1,00	1,00	1,00	0,00

Tablo 28'de görüldüğü üzere araştırmada kullanılan ölçeklerin uyum iyiliği değerlerini sağladığı ve iyi uyum gösterdiği bulgusu elde edilmiştir. Tabloda görüldüğü üzere; CMIN/df değeri tüm değişkenlerde ≤3, GFI değeri tüm değişkenlerde ≥0,90, AGFI değeri tüm değişkenlerde ≥0,90, CFI değeri tüm değişkenlerde ≥0,90, TLI değeri tüm değişkenlerde ≥0,95 ve RMSEA değeri tüm değişkenlerde ≤0,08 çıkmış olup bu değerler araştırma kapsamındaki değişkenlerin iyi veya kabul edilebilir uyum gösterdiğini gösterir.

3.6. Güvenilirlik Analizi

Güvenilirlik kavramı, ölçekte yer alan ifadelerin birbirleri ile olan tutarlılığını ve ölçeğin ilgilenilen sorunu ne derece yansıttığını ifade eder. Bununla birlikte, elde edilen ölçümler üzerindeki yorumlar ve daha sonra ortaya çıkabilecek analizler için bir temel teşkil eder (Kalaycı, 2008: 403). Güvenilirlik ölçümümde en yaygın olarak kullanılan yöntem Cronbach's Alpha olarak bilinen alfa katsayısı (α) dır (Altunışık vd., 2010: 124).

Alpha katsayısına göre ölçeğin güvenilirliği aşağıdaki şekilde yorumlanabilir (Kalaycı, 2008: 405);

- $0.00 \leq \alpha < 0.40$ ise ölçek güvenilir değildir,
- $0.40 \leq \alpha < 0.60$ ise ölçeğin güvenilirliği düşük,
- $0.60 \leq \alpha < 0.80$ ise ölçek oldukça güvenilir,
- $0.80 \leq \alpha < 1.00$ ise ölçek yüksek derece güvenilir bir ölçektir

Yapılan güvenilirlik analizi sonucu elde edilen Cronbach Alpha katsayısı değerleri Tablo 29'da verilmiştir.

Tablo 29. Güvenilirlik Analizi

Ölçek	Cronbach Alpha	Madde Sayısı
Siber Güvenliğine Kurumsal Yaklaşım	0,919	8
Fiziksel ve Çevresel Güvenlik Tedbirleri	0,724	4
Bilişim Sistemleri ve İletişim Ağlarının İşletim Ve Bakım Kontrolleri	0,814	7
Yazılım Geliştirme ve Destek Aşamalarında Bilgi Sistemleri Erişim Kontrolü Güvenlik Tedbirleri	0,829	5
Siber Güvenlik İhlalleri ve İş Sürekliliği Yönetimi	0,801	3
Genel Siber Güvenlik	0,926	27

Güvenilirlik analizi sonucu ölçeklerin güvenilirliklerinin iyi olduğu bulgusuna ulaşılmıştır.

3.7. Normal Dağılım Testi

Verilerin normal dağılıma sahip olup olmadıklarını test etmek amacı ile ölçeklerin basıklık ve çarpıklık değerlerine bakılmıştır. Elde edilen analiz sonuçları Tablo 30'da verilmiştir.

Tablo 30. Normal Dağılım Testi

Ölçekler	Çarpıklık	Basıklık
Siber Güvenliğine Kurumsal Yaklaşım	0,757	-0,232
Fiziksel ve Çevresel Güvenlik Tedbirleri	-0,520	0,161
Bilişim Sistemleri ve İletişim Ağlarının İşletim Ve Bakım Kontrolleri	0,286	-0,740
Yazılım Geliştirme ve Destek Aşamalarında Bilgi Sistemleri Erişim Kontrolü Güvenlik Tedbirleri	0,218	-0,986
Siber Güvenlik İhlalleri ve İş Sürekliliği Yönetimi	-0,258	-1,083
Genel Siber Güvenlik	0,310	-0,568

Basıklık ve çarpıklık değerleri -2 ile +2 arasında bir değer alıyor ise veriler normal dağılıma sahiptir (Bayram, 2013:109). Tablo 25'de sunulduğu üzere değişkenlerin basıklık ve çarpıklık değerleri -2 ile +2 arasında değerler aldığı görülmektedir. Dolayısıyla araştırma kapsamında kullanılan veriler normal dağılıma sahiptir.

DÖRDÜNCÜ BÖLÜM

BULGULAR VE YORUM

Bu bölümde araştırma kapsamında elde edilen verilerin analizleri sonucunda elde edilen bulgular ve yorumları verilmiştir. Bu kapsamda önce demografik sorulara verilen cevaplara ilişkin bulgular verilmiş sonra araştırma hipotezlerini test etmek amacı ile yapılan T ve F testi analizlerine ilişkin bulgular verilmiştir.

4.1. Demografik Sorulara İlişkin Bulgular

Aşağıda araştırma kapsamında elde edilen verilere ilişkin demografik verilerin frekans dökümleri sırasıyla verilmiştir.

Tablo 31. Firmaların Çalışan Sayısı

Çalışan Sayısı	Frekans	Yüzde	Kümülatif Yüzde
50-249 kişi	91	71,1	71,1
250 ve kişi üstü	37	28,9	100
Toplam	128	100	

Araştırmaya katılan firmaların çalışan sayılarına ilişkin bilgiler Tablo 31'de verilmiştir. Araştırma katılan firmalarının 91'i 50-249 arası çalışana sahip olup, 37'si 250 ve üzeri çalışana sahiptir. Dolayısıyla araştırmaya katılan firmaların çalışan sayısına göre çoğunluğunu orta ölçekli işletmeler oluşturmaktadır.

Tablo 32. Firmaların Yıllık Cirosu

Yıllık Ciro	Frekans	Yüzde	Kümülatif Yüzde
8.000.001-40.000.000	24	18,8	18,8
40.000.001 üzeri	104	81,3	100
Toplam	128	100	

Tablo 32'de görüldüğü üzere araştırma araştırmaya katılan firmalarının 24'ünün yıllık cirosu 8.000.001 – 40.000.000 arası, 104'ünün ise yıllık cirosu 40.000.001 ve üzeridir. Dolayısıyla araştırmaya katılan firmaların büyük çoğunluğunu (ciroya göre) büyük ölçekli işletmeler oluşturmaktadır.

Tablo 33. Firmaların Sermayesi

Firma Sermayesi	Frekans	Yüzde	Kümülatif Yüzde
1 milyondan az	7	5,5	5,5
1-10 milyon	16	12,5	18,0
10-50 milyon	34	26,6	44,5
50-100 milyon	45	35,2	79,7
100 milyon üzeri	26	20,3	100,0
Toplam	128	100,0	

Tablo 33'de verildiği gibi araştırmaya katılan firmaların 7'si 1 milyon TL'den az sermayeye sahip olup, 16'sı 1-10 milyon TL arası, 34'ü 10-50 milyon TL arası, 45'i 50-100 milyon TL arası sermayeye sahiptir ve 26 firmanın ise sermayesi 100 milyon TL'nin üzerindedir.

Tablo 34. Bilişim Sistemleri Bağımlılık Oranı

Bilişim Sistemleri Bağımlılık Oranı	Frekans	Yüzde	Kümülatif Yüzde
%25 az	11	8,6	8,6
%25-50	8	6,3	14,8
%50-75	47	36,7	51,6
%75 üstü	62	48,4	100,0
Toplam	128	100,0	

Tablo 34'de araştırmaya katılan firmaların iş faaliyetlerinin dayandığı bilişim sistemleri (diğer şirketler tarafından sağlanan sistemler de dahil olmak üzere, e-mail, web sitesi, kiralık sunucu vb.) bağımlılık oranları verilmiştir. Tabloda görüldüğü üzere 11 firmanın ana hizmet faaliyetlerinin dayandığı bilişim sistemlerine bağlılık oranı % 25'den az, 8 firma için % 25-50 arası, 47 firma için % 50-75 arası ve 62 firma için ise % 75'in üstüdür. Dolayısıyla firmaların bilişim sistemlerine bağlılık oranı konusundaki değerlendirmelerinin yüksek olduğu söylenebilir.

Tablo 35. İnternete Bağımlılık Oranı

İnternete Bağımlılık	Frekans	Yüzde	Kümülatif Yüzde
%25 az	35	27,3	27,3
%25-50	22	17,2	44,5
%50-75	27	21,1	65,6
%75 üstü	44	34,4	100,0
Toplam	128	100,0	

Katılımcılara sorulan "Ticari/Üretim faaliyetlerinizde ne derece internete bağımlısınız?" sorusuna verilen cevaplara ilişkin bilgiler Tablo 35'de verilmiştir. Tabloda görüleceği gibi firmaların 35'i ticari/üretim faaliyetlerin % 25'den az, 22'si % 25-50 arası, 27'si % 50-75 arası internete bağımlı iken 44 firma da % 75'in üzerinde internete bağımlıdır. Bu durum araştırma kapsamında firmaların faaliyetlerinde internete bağımlılık düzeyinin yüksek olduğunu göstermektedir.

Tablo 36. Bilişim Sistemindeki Aksamanın Tolere Süresi

	Frekans	Yüzde	Kümülatif Yüzde
En fazla bir saat	51	39,8	39,8
En fazla yarım gün	32	25,0	64,8
En fazla bir gün	13	10,2	75,0
Birkaç gün	29	22,7	97,7
Daha fazla kesinti sıkıntı oluşturmaz	3	2,3	100,0
Toplam	128	100,0	

Katılımcı firmalara sorulan "Satışlarınızı etkilemeyen bilişim sistem ve hizmetlerinin aksamasını ne kadar süre tolere edebilirsiniz? sorusuna verilen cevaplara ilişkin bilgiler Tablo 36'da verilmiştir. Tabloda görüleceği gibi firmaların satışlarını etkilemeyen bilişim sistemleri aksamasını tolere etme süreleri 51 firma için en fazla bir saat, 32 firma için en fazla yarım saat, 13 firma için en fazla bir gün, 29 firma için birkaç gün iken 3 firma için ise sıkıntı oluşturmayacak düzeydedir. Elde edilen bulgular firmaların bu aksaklığı tahammül sürelerinin düşük olduğunu göstermektedir. Yani araştırma kapsamındaki firmaların büyük çoğunluğu bir günün altında bu aksaklıkları tolere edebilmektedirler. Bu sürenin uzaması durumunda firmaların satışlarında olumsuzluklar yaşanabilecektir.

Tablo 37. Bilişim Sistemlerinin 24 Saat Hizmet Verememesinin Satış/Üretim Oranına Etkisi

	Frekans	Yüzde	Kümülatif Yüzde
%25 az	27	21,1	21,1
%25-50	18	14,1	35,2
%50-75	29	22,7	57,8
%75 üstü	54	42,2	100,0
Toplam	128	100,0	

Katılımcı firmalara sorulan "Bilişim sistemlerinizin 24 saat hizmet verememesi bir günlük satış/üretim oranlarınızı ne derece etkiler?" sorusuna verdikleri cevaplara ilişkin bilgiler Tablo 37'de verilmiştir. Tabloda görüldüğü gibi bilişim sistemlerinin 24 saat hizmet vermemesi

durumunda 27 firmanın satış/üretim oranın %25'den az, 18 firmanın % 25-50 arası, 29 firmanın % 50-75 arası etkilenmekte, 54 firmanın ise satış/üretim oranı % 75'in üzerinde etkilenmektedir. Bu durum araştırma kapsamında firmaların bilişim sistemlerinin bir gün hizmet verememesi durumunda firmaların çoğunluğunda günlük satış ve üretimlerine olumsuz etkisinin büyük olduğunu göstermektedir.

Tablo 38. Siber Saldırıların Firma İmajı Üzerindeki Olası Etkileri

	Frekans	Yüzde	Kümülatif Yüzde
Neredeyse olmaz	20	15,6	15,6
Az	30	23,4	39,1
Çok	24	18,8	57,8
Firma geleceğini etkileyecek kadar fazla	54	42,2	100,0
Toplam	128	100,0	

Katılımcılara sorulan "Firmanızı hedef alan ve kişisel bilgilerin (müşteri bilgileri vb.) sızdırılması ile sonuçlanan bir siber saldırının firma imajı üzerine olası etkileri ne oranda olur?" sorusuna verdikleri cevaplara ilişkin bilgiler Tablo 38'de verilmiştir. Tabloda görüleceği üzere 20 firma için siber saldırıların firma imajı üzerindeki etkisi neredeyse hiç olmamakta, 30 firma için az olmakta, 24 firma için çok olmakta ve 54 firma için ise firma geleceğini etkileyecek kadar fazla olmaktadır. Yani araştırma kapsamında firmaların çoğunluğu, bir siber saldırı olduğunda firma imajlarının olumsuz etkileneceğini öngörmektedirler.

Tablo 39. Barındırdıkları Kritik Bilgi Oranları

	Frekans	Yüzde	Kümülatif Yüzde
Neredeyse yok	21	16,4	16,4
Az	26	20,3	36,7
Bilgilerin yarısı diyebiliriz	45	35,2	71,9
Çoğunluğu kritik öneme sahip	36	28,1	100,0
Toplam	128	100,0	

Firmalara sorulan "Kritik bilgilerde sızıntı (ulusal sırlar, ticari sırlar, gizlilik bilgileri gibi) meydana gelirse faaliyetler üzerinde ciddi etkilere neden olabilir. Bu kritik bilgilerin, firmanızın elinde tuttuğu, yönettiği ve kullandığı tüm bilgilere oranı ne kadardır?" sorusuna verilen cevaplara ilişkin bilgiler Tablo 39'da verilmiştir. Tabloda görüleceği gibi 21 firmanın elinde tuttuğu kritik bilgi neredeyse yok, 26 firmanın az, 45 firmanın elinde tuttuğu bilgilerin yarısı kritik bilgilerden oluşmakta, 36 firmanın ise elinde tuttuğu bilgilerin çoğunluğu kritik bilgilerden oluşmaktadır. Bu durumda araştırma kapsamındaki firmaların çok azının (%16,4) kritik bilgisi

olmadığını fakat geri kalan büyük çoğunluğun az veya çok kritik bilgilerinin olduğu görülmektedir. Bu yüzden firmalar kritik bilgilerinin sızdırılmaması için gerekli önlemleri almak zorundadırlar.

Tablo 40. Bilişim Sistemlerindeki Korunması Gerekli Bilgi Adedi

	Frekans	Yüzde	Kümülatif Yüzde
1000 veya daha az	7	5,5	5,5
1001-5000	21	16,4	21,9
5001-10000	30	23,4	45,3
10001-100000	56	43,8	89,1
100000'den fazla	14	10,9	100,0
Toplam	128	100,0	

Firmalara sorulan "Firmanızın bilişim sistemlerinde ortalama ne kadar kişi veya firmaya ait korunması gerekli bilgi bulunmaktadır? (bilgi miktarından ziyade adedi, müşteri bilgisi tedarikçi bilgisi gibi)" sorusuna verilen cevaplara ilişkin bilgiler Tablo 40'da verilmiştir. Tabloda görüleceği gibi 7 firmanın 1000'den az korunması gerekli bilgi bulunmakta iken 21 firmanın 1001-5000 arası, 30 firmanın 5001-10000 arası, 56 firmanın 10001-100000 arası korunması gerekli bilgisi bulunmakta, 24 firmanın ise 100000'den fazla korunması gerekli bilgisi bulunmaktadır. Bu durum araştırma kapsamındaki firmaların ilişkili olduğu ve korunması gereken bilgi sayısının çok büyük olduğunu göstermektedir.

Tablo 41. Personel Değişim Oranı

	Frekans	Yüzde	Kümülatif Yüzde
%10 ve altı	78	60,9	60,9
%11-30	34	26,6	87,5
%31-50	16	12,5	100,0
Toplam	128	100,0	

Firmaların personel değişim oranlarına ait bilgiler Tablo 41'de verilmiştir. Tabloda görüldüğü üzere 78 firmanın personel değişim aranı %10'un altında, 34 firmanın %11-30 arasında, 16 firmanın ise %31-50 arasındadır. Bu durum araştırma kapsamındaki firmaların personel değişim oranlarının düşük olduğu görülmektedir.

Tablo 42. Siber Güvenlik Olayı İle Karşılaşma

	Frekans	Yüzde	Kümülatif Yüzde
Evet	92	71,9	71,9
Hayır	36	28,1	100,0
Toplam	128	100,0	

Firmaların herhangi bir siber güvenlik olayı ile karşı karşıya kalıp kalmadıklarına ilişkin bilgiler Tablo 42'de verilmiştir. Tabloda görüldüğü üzere 92 firma daha önce siber güvenlik olayı ile karşılaşmış, 36 firma ise karşılaşmamıştır. Bu durum firmaların büyük çoğunluğunun daha önce bir siber saldırıya maruz kaldığını ve firmaların siber güvenliğe daha fazla önem vermeleri gerektiğini göstermektedir.

4.2. Tanımlayıcı İstatistik Bilgileri

Araştırma değişkenlerinin ortalama ve standart sapma değerlerine ilişkin bilgiler Tablo 43'de verilmiştir.

Tablo 43. Tanımlayıcı İstatistik Bilgileri

Değişken	Ortalama		Std. Sapma	Varyans
	Statistic	Std. Hata	Statistic	Statistic
Siber güvenliğine kurumsal yaklaşım	2,2441	,08212	,92906	,863
Fiziksel ve çevresel güvenlik tedbirleri	3,1582	,07091	,80223	,644
Bilişim sistemleri ve iletişim ağlarının işletim ve bakım kontrolleri	2,9219	,07270	,82248	,676
Yazılım geliştirme ve destek aşamalarında bilgi sistemleri erişim kontrolü güvenlik tedbirleri	2,5828	,08751	,99004	,980
Siber güvenlik ihlalleri ve iş sürekliliği yönetimi	2,8516	,09308	1,05310	1,109
Genel ortalama	2,7517	,06033	,68259	,466

Araştırma kapsamındaki firmaların siber güvenliğe ilişkin yaklaşımları 5'li likert tipi ölçekle (1=Kesinlikle katılmıyorum… 5=Kesinlikle katılıyorum) ölçülmüştür. Tablo 43'de görüldüğü üzere firmaların siber güvenliğe ilişkin yaklaşımları soruya verilen cevaplara göre; ortalama değerlere bakılarak değerlendirilmiştir. Tabloda görüldüğü üzere araştırma kapsamındaki firmaların siber güvenliğe kurumsal yaklaşım, yazılım geliştirme ve destek aşamalarında bilgi sistemleri erişim kontrolü güvenlik tedbirleri, siber güvenlik ihlalleri ve iş sürekliliği yönetimi ile genel siber güvenlik yaklaşımlarının düşük düzeyde olduğu; fiziksel ve çevresel güvenlik tedbirleri ile bilişim sistemleri ve iletişim ağlarının işletim ve bakım kontrolleri düzeyinin orta düzeyde olduğu tespit edilmiştir. Bu durum araştırma kapsamındaki firmaların siber güvenliğe yaklaşım düzeylerinin genel olarak düşük olduğunu veya yeterince önem

vermediğini göstermektedir. Dolayısıyla araştırmanın temel hipotezlerinden birisi olan "Gaziantep İmalat Sanayiinde faaliyet gösteren firmaların siber güvenlik yaklaşım seviyesi düşüktür." H1 hipotezi desteklenmiştir.

4.3. T Testi

Bu çalışmada araştırmaya firmaların özelliklerine göre (ikili gruplar için) siber güvenlik yaklaşımları arasındaki ilişkileri incelemek için T testi analizleri yapılmıştır. Aşağıda T testi ile yapılan analizler sırasıyla verilmiştir.

Tablo 44. Çalışan Sayısına Göre T Testi

Değişkenler		N	Ortalama	Std. Sap.	T	Sig.
Siber güvenliğine kurumsal yaklaşım	50-249	91	2,0082	,78236	-4,896	,000
	250 ve üzeri	37	2,8243	1,01399		
Fiziksel ve çevresel güvenlik tedbirleri	50-249	91	3,1209	,68044	-,824	,411
	250 ve üzeri	37	3,2500	1,04914		
Bilişim sistemleri ve iletişim ağlarının işletim ve bakım kontrolleri	50-249	91	2,7928	,73471	-2,863	,005
	250 ve üzeri	37	3,2394	,94404		
Yazılım geliştirme ve destek aşamalarında bilgi sistemleri erişim kontrolü güvenlik tedbirleri	50-249	91	2,3538	,90090	-4,388	,000
	250 ve üzeri	37	3,1459	,98505		
Siber güvenlik ihlalleri ve iş sürekliliği yönetimi	50-249	91	2,8864	1,03067	,586	,559
	250 ve üzeri	37	2,7658	1,11628		
Genel ortalama	50-249	91	2,6324	,60085	-3,212	,002
	250 ve üzeri	37	3,0451	,78530		

Araştırma kapsamında test edilen, "H2. Siber güvenlik yaklaşımları firmaların çalışan sayısına göre anlamlı farklılık göstermektedir." temel hipotezi ve bu hipoteze ilişkin alt hipotezler Tablo 44'de görüldüğü üzere T testi ile analiz edilmiştir. Tabloda görüldüğü üzere "H2a: Siber güvenliğe kurumsal yaklaşım firmaların çalışan sayısına göre anlamlı farklılık göstermektedir.", "H2c: Bilişim sistemleri ve iletişim ağlarının işletim ve bakım kontrolleri firmaların çalışan sayısına göre anlamlı farklılık göstermektedir." ve "H2d: Yazılım geliştirme ve destek aşamalarında bilgi sistemleri erişim kontrolü güvenlik tedbirleri firmaların çalışan sayısına göre anlamlı farklılık göstermektedir." hipotezleri, T testindeki sig.(2-tailed) değerleri %1 seviyesinde anlamlı olduğu için desteklenmiştir. Yani %1 güven seviyesinde Siber güvenliğe kurumsal yaklaşım, Bilişim sistemleri ve iletişim ağlarının işletim ve bakım kontrolleri ve Yazılım geliştirme ve destek aşamalarında bilgi sistemleri erişim kontrolü güvenlik tedbirleri, firmaların çalışan sayılarına göre farklılık göstermektedir. Araştırma kapsamındaki büyük

işletmelerin (çalışan sayısı 250 ve üzeri) siber güvenliğe yaklaşım düzeyleri, orta büyüklükteki işletmelere göre daha fazladır.

Tabloda görüldüğü üzere araştırma kapsamında test edilen, "H2b: Fiziksel ve çevresel güvenlik tedbirleri firmaların çalışan sayısına göre anlamlı farklılık göstermektedir." ve "H2e: Siber güvenlik ihlalleri ve iş sürekliliği yönetimi firmaların çalışan sayısına göre anlamlı farklılık göstermektedir." hipotezleri istatiksel olarak anlamlı çıkmadığı için desteklenmemiştir. Yani fiziksel ve çevresel güvenlik tedbirleri ile siber güvenlik ihlalleri ve iş sürekliliği yönetimi firmaların çalışan sayılarına göre farklılık göstermemektedir. Diğer bir ifade ile çalışan sayısı 50-249 olan firmalar ile çalışan sayısı 250 ve üzeri firmaların; fiziksel ve çevresel güvenlik tedbirleri ile siber güvenlik ihlalleri ve iş sürekliliği yönetimi yaklaşım düzeyleri aynı düzeydedir.

Araştırma kapsamında test edilen, "H2. Siber güvenlik yaklaşımları firmaların çalışan sayısına göre anlamlı farklılık göstermektedir." temel hipotezi desteklenmiştir. Zira bu hipotezin desteklenmesi için alt hipotezlerinden en az birinin desteklenmesi yeterlidir. Araştırmada H2a, H3c ve H3d alt hipotezleri desteklendiği için H2 hipotezi de desteklenmiştir. Ayrıca firmaların siber güvenlik yaklaşımlarının genel ortalamaları alınarak yapılan T testinde de firmaların çalışan sayısına göre anlamlı farklılık göstermektedir.

Tablo 45. Yıllık Ciroya Göre T Testi

Değişkenler		N	Ortalama	Std. Sap.	T	Sig.
Siber Güvenliğine Kurumsal Yaklaşım	8.000.001-40.000.000	24	1,6146	,49442	-3,881	,000
	40.000.001 üzeri	104	2,3894	,94659		
Fiziksel ve Çevresel Güvenlik Tedbirleri	8.000.001-40.000.000	24	2,9688	,43808	-1,287	,201
	40.000.001 üzeri	104	3,2019	,86046		
Bilişim Sistemleri ve İletişim Ağlarının İşletim ve Bakım Kontrolleri	8.000.001-40.000.000	24	2,4405	,53105	-3,303	,001
	40.000.001 üzeri	104	3,0330	,83945		
Yazılım Geliştirme ve Destek Aşamalarında Bilgi Sistemleri Erişim Kontrolü Güvenlik Tedbirleri	8.000.001-40.000.000	24	1,9250	,77530	-3,797	,000
	40.000.001 üzeri	104	2,7346	,97481		
Siber Güvenlik İhlalleri ve İş Sürekliliği Yönetimi	8.000.001-40.000.000	24	3,1250	,93670	1,417	,159
	40.000.001 üzeri	104	2,7885	1,07241		
Genel ortalama	8.000.001-40.000.000	24	2,4148	,43359	-2,751	007
	40.000.001 üzeri	104	2,8295	,70707		

Araştırma kapsamında test edilen, "H3. Siber güvenlik yaklaşımları firmaların yıllık cirosuna göre anlamlı farklılık göstermektedir." temel hipotezi ve bu hipoteze ilişkin alt hipotezler T testi ile analiz edilmiştir. Tablo 45'de görüldüğü üzere Siber güvenliğine kurumsal yaklaşım, Bilişim sistemleri ve iletişim ağlarının işletim ve bakım kontrolleri, Yazılım geliştirme

ve destek aşamalarında bilgi sistemleri erişim kontrolü güvenlik tedbirleri ve Genel siber güvenlik yaklaşımı firmaların cirolarına göre anlamlı farklılık göstermektedir. Farklılığın yönünü test edebilmek amacı ile değişkenlerin cirolarına göre ortalama değerlerine bakılmıştır. Siber güvenliğine kurumsal yaklaşım 40 milyon üzeri ciroya sahip olan firmalar lehine, Bilişim sistemleri ve iletişim ağlarının işletim ve bakım kontrolleri 40 milyon üzeri ciroya sahip olan firmalar lehine, Yazılım geliştirme ve destek aşamalarında bilgi sistemleri erişim kontrolü güvenlik tedbirleri 40 milyon üzeri ciroya sahip olan firmalar lehine ve genel siber güvenlik yaklaşımı da 40 milyon üzeri ciroya sahip olan firmalar lehine anlamlı farklılık göstermektedir. Yani, 40 milyon üzeri ciroya sahip olan firmaların siber güvenlik yaklaşımları 8-40 milyon arası ciroya sahip olan firmalara göre daha yüksektir. Diğer taraftan Fiziksel ve çevresel güvenlik tedbirleri ile Siber güvenlik ihlalleri ve iş sürekliliği yönetimi firmaların cirosuna göre anlamlı farklılık göstermemektedir.

Araştırma kapsamında test edilen, "H3a: Siber güvenliğe kurumsal yaklaşım firmaların yıllık cirosuna göre anlamlı farklılık göstermektedir.", "H3c: Bilişim sistemleri ve iletişim ağlarının işletim ve bakım kontrolleri firmaların yıllık cirosuna göre anlamlı farklılık göstermektedir.", H3d: Yazılım geliştirme ve destek aşamalarında bilgi sistemleri erişim kontrolü güvenlik tedbirleri firmaların yıllık cirosuna göre anlamlı farklılık göstermektedir." ve "H3: Siber güvenlik yaklaşımları firmaların yıllık cirosuna göre anlamlı farklılık göstermektedir." temel hipotezi desteklenmiştir. Diğer taraftan "H3b: Fiziksel ve çevresel güvenlik tedbirleri firmaların yıllık cirosuna göre anlamlı farklılık göstermektedir." ve "H3e: Siber güvenlik ihlalleri ve iş sürekliliği yönetimi firmaların yıllık cirosuna göre anlamlı farklılık göstermektedir." hipotezleri desteklenmemiştir.

Tablo 46. Siber Saldırı Olma durumuna göre T Testi

Değişkenler		N	Ortalama	Std. Sap.	T	Sig.
Siber Güvenliğine Kurumsal Yaklaşım	Evet	92	2,1168	,86836	-2,530	,013
	Hayır	36	2,5694	1,00997		
Fiziksel ve Çevresel Güvenlik Tedbirleri	Evet	92	3,1005	,78627	-1,304	,195
	Hayır	36	3,3056	,83476		
Bilişim Sistemleri ve İletişim Ağlarının İşletim ve Bakım Kontrolleri	Evet	92	2,8773	,77456	-,979	,329
	Hayır	36	3,0357	,93608		
Yazılım Geliştirme ve Destek Aşamalarında Bilgi Sistemleri Erişim Kontrolü Güvenlik Tedbirleri	Evet	92	2,5109	,93497	-1,318	,190
	Hayır	36	2,7667	1,11150		
Siber Güvenlik İhlalleri ve İş Sürekliliği Yönetimi	Evet	92	2,8732	1,08136	,370	,712
	Hayır	36	2,7963	,98972		
Genel ortalama	Evet	92	2,6958	,65324	-1,490	,139
	Hayır	36	2,8947	,74290		

Araştırma kapsamında test edilen, H8a: Siber saldırıya maruz olma durumuna göre firmaların siber güvenliğe kurumsal yaklaşım düzeyleri anlamlı farklılık göstermektedir.” alt hipotezi %5 anlamlılık seviyesinde desteklenmiştir. Yani araştırma kapsamındaki işletmelerin siber saldırıya maruz olma durumuna göre siber güvenliğe kurumsal yaklaşım düzeyleri anlamlı farklılık göstermektedir, Bu farklılık bir saldırıya maruz kalmamış işletmeler lehinedir. Bir siber saldırıya maruz kalmamış işletmelerin siber güvenliğe kurumsal yaklaşım düzeyleri daha yüksektir. Diğer taraftan araştırma kapsamında test edilen “H8: Siber saldırıya maruz olma durumuna göre firmaların siber güvenliğe yaklaşım düzeyleri anlamlı farklılık göstermektedir.” temel hipotezi ve bu hipoteze ilişkin “H8b: Siber saldırıya maruz olma durumuna göre firmaların fiziksel ve çevresel güvenlik tedbirleri anlamlı farklılık göstermektedir.”, “H8c: Siber saldırıya maruz olma durumuna göre firmaların bilişim sistemleri ve iletişim ağlarının işletim ve bakım kontrolleri anlamlı farklılık göstermektedir.”, “H8d: Siber saldırıya maruz olma durumuna göre firmaların yazılım geliştirme ve destek aşamalarında bilgi sistemleri erişim kontrolü güvenlik tedbirleri anlamlı farklılık göstermektedir.” ve “H8e:Siber saldırıya maruz olma durumuna göre firmaların siber güvenlik ihlalleri ve iş sürekliliği anlamlı farklılık göstermektedir.” alt hipotezleri Tablo 46’da görüldüğü üzere istatiksel olarak anlamlı çıkmadığı için desteklenmemiştir. Yani siber saldırıya maruz olma durumuna göre firmaların siber güvenliğe genel yaklaşım düzeyleri ile bu alt boyutlara ilişkin yaklaşımlar aynı düzeydedir. Bu durumda araştırma kapsamında test edilen H8, H8b, H8c, H8d ve H8e hipotezleri desteklenmemiştir.

4.4. Anova (F) Testi

Anova analizi bağımsız değişkenlerin kendi aralarında nasıl etkileşime girdiklerini ve bu etkileşimlerin bağımlı değişken üzerindeki etkilerini analiz etmek için kullanılır. Bağımsız örneklem tek yönlü F testi analizinde, ikiden fazla grubun ortalamaları karşılaştırılır. Anova, gruplar arasındaki farklılıkları bir bütün olarak değerlendirir. İkili gruplar arasındaki farkın anlamlı olup olmadığı için Tukey testi yapılmalıdır (Yazıcıoğlu ve Erdoğan, 2004:190). Bu çalışmada araştırmaya firmaların demografik özelliklerine göre (ikiden fazla gruplar için) siber güvenlik yaklaşımları arasındaki ilişkileri incelemek için anova testleri yapılmış ve aşağıda sırası ile verilmiştir.

Tablo 47. İnternete Bağımlılık Oranına Göre Anova Testi

Değişken		Kareler Toplamı	df	Kareler Ortalaması	F	Sig.	Farklılık
Siber Güvenliğine Kurumsal Yaklaşım	Gruplar arası	30,208	3	10,069	15,723	,000	1-3 1-4
	Gruplar içi	79,412	124	,640			
	Toplam	109,621	127				
Fiziksel ve Çevresel Güvenlik Tedbirleri	Gruplar arası	6,824	3	2,275	3,766	,013	1-3
	Gruplar içi	74,910	124	,604			
	Toplam	81,734	127				
Bilişim Sistemleri ve İletişim Ağlarının İşletim Ve Bakım Kontrolleri	Gruplar arası	12,559	3	4,186	7,077	,000	1-3 1-4
	Gruplar içi	73,353	124	,592			
	Toplam	85,913	127				
Yazılım Geliştirme ve Destek Aşamalarında Bilgi Sistemleri Erişim Kontrolü Güvenlik Tedbirleri	Gruplar arası	30,391	3	10,130	13,350	,000	1-3 1-4
	Gruplar içi	94,091	124	,759			
	Toplam	124,482	127				
Siber Güvenlik İhlalleri ve İş Sürekliliği Yönetimi	Gruplar arası	4,724	3	1,575	1,434	,236	-
	Gruplar içi	136,122	124	1,098			
	Toplam	140,846	127				
Genel ortalama	Gruplar arası	14,448	3	4,816	13,353	,000	1-3 1-4 2-4
	Gruplar içi	44,724	124	,361			
	Toplam	59,172	127				

Araştırma kapsamında firmaların siber güvenlik yaklaşımlarının ticari faaliyetlerdeki internete bağımlılık oranına göre anlamlı farklılık gösterip göstermediğini analiz etmek için anova testi yapılmış ve analiz sonuçları Tablo 47'de verilmiştir. Tabloda görüldüğü üzere siber güvenlik ihlalleri ve iş sürekliliği yönetimi haricinde bütün değişkenler firmaların ticari faaliyetlerinde internete bağımlılık oranına göre anlamlı farklılık göstermektedir. Bu durumda araştırma kapsamında test edilen; "H4: Siber güvenlik yaklaşım düzeyleri firmaların ticari

faaliyetlerde internete bağımlılık oranına göre anlamlı farklılık göstermektedir.” temel hipotezi ve bu hipoteze ait “H4a: Siber güvenliğe kurumsal yaklaşım firmaların ticari faaliyetlerde internete bağımlılık oranına göre anlamlı farklılık göstermektedir.”, “H4b: Fiziksel ve çevresel güvenlik tedbirleri firmaların ticari faaliyetlerde internete bağımlılık oranına göre anlamlı farklılık göstermektedir.”, “H4c: Bilişim sistemleri ve iletişim ağlarının işletim ve bakım kontrolleri firmaların ticari faaliyetlerde internete bağımlılık oranına göre anlamlı farklılık göstermektedir.”, “H4d: Yazılım geliştirme ve destek aşamalarında bilgi sistemleri erişim kontrolü güvenlik tedbirleri firmaların ticari faaliyetlerde internete bağımlılık oranına göre anlamlı farklılık göstermektedir.” alt hipotezleri desteklenmiştir. Diğer taraftan H4e: Siber güvenlik ihlalleri ve iş sürekliliği yönetimi firmaların ticari faaliyetlerde internete bağımlılık oranına göre anlamlı farklılık göstermektedir.” hipotezi desteklenmemiştir.

Araştırmada hangi gruplar arasında farklılık olduğu, Tukey testi kullanılarak analiz edilmiştir. Tukey analizi sonuçlarına göre siber güvenliğine kurumsal yaklaşım ticari faaliyetlerinde internete bağımlılık oranı % 25’den az olan firmalar ile % 50-75 arası ve % 75 üstü bağımlılığı olan firmalar arasında % 75 üstü bağımlılığı olan firmalar lehine anlamlı farklılık göstermektedir. Fiziksel ve çevresel güvenlik tedbirleri % 25’den az bağımlılığı olan firmalar ile % 75 üstü bağımlılığı olan firmalar arasında % 75 üstü internete bağımlılığı olan firmalar lehine anlamlı farklılık göstermektedir. Bilişim sistemleri ve iletişim ağlarının işletim ve bakım kontrolleri ticari faaliyetlerinde internete bağımlılık oranı % 25’den az olan firmalar ile % 50-75 arası ve % 75 üstü bağımlılığı olan firmalar arasında % 75 üstü bağımlılığı olan firmalar lehine anlamlı farklılık göstermektedir. Yazılım geliştirme ve destek aşamalarında bilgi sistemleri erişim kontrolü güvenlik tedbirleri ticari faaliyetlerinde internete bağımlılık oranı % 25’den az olan firmalar ile % 50-75 arası ve % 75 üstü bağımlılığı olan firmalar arasında % 75 üstü bağımlılığı olan firmalar lehine anlamlı farklılık göstermektedir. Genel siber güvenlik yaklaşımı ticari faaliyetlerinde internete bağımlılık oranı % 25’den az olan firmalar ile % 50-75 arası ve % 75 üstü bağımlılığı olan firmalar arasında % 75 üstü bağımlılığı olan firmalar lehine anlamlı farklılık göstermektedir. Yani ticari faaliyetlerinde % 75 üzeri internete bağımlı olan firmaların siber güvenlik yaklaşım düzeyleri daha yüksektir.

Tablo 48. Bilişim Sistemlerinin 24 Saat Hizmet Vermemesinin Bir Günlük Satış / Üretim Oranlarını Etkileme Düzeyine Göre Anova Testi

Değişken		Kareler Toplamı	df	Kareler Ortalaması	F	Sig.	Farklılık
Siber Güvenliğine Kurumsal Yaklaşım	Gruplar arası	22,260	3	7,420	10,532	,000	1-3 1-4 2-3 2-4
	Gruplar içi	87,360	124	,705			
	Toplam	109,621	127				
Fiziksel ve Çevresel Güvenlik Tedbirleri	Gruplar arası	7,684	3	2,561	4,289	,006	2-3 2-4
	Gruplar içi	74,050	124	,597			
	Toplam	81,734	127				
Bilişim Sistemleri ve İletişim Ağlarının İşletim Ve Bakım Kontrolleri	Gruplar arası	8,380	3	2,793	4,468	,005	2-3 2-4
	Gruplar içi	77,532	124	,625			
	Toplam	85,913	127				
Yazılım Geliştirme ve Destek Aşamalarında Bilgi Sistemleri Erişim Kontrolü Güvenlik Tedbirleri	Gruplar arası	21,427	3	7,142	8,594	,000	1-3 1-4 2-3 2-4
	Gruplar içi	103,055	124	,831			
	Toplam	124,482	127				
Siber Güvenlik İhlalleri ve İş Sürekliliği Yönetimi	Gruplar arası	3,489	3	1,163	1,050	,373	-
	Gruplar içi	137,358	124	1,108			
	Toplam	140,846	127				
Genel Siber Güvenlik Yaklaşımı	Gruplar arası	10,718	3	3,573	9,142	,000	1-3 1-4 2-3 2-4
	Gruplar içi	48,455	124	,391			
	Toplam	59,172	127				

Tablo 48'de görüldüğü üzere araştırma kapsamında test edilen "H5: Siber güvenlik yaklaşımları firmaların bilişim sistemlerinin 24 saat hizmet vermemesinin bir günlük satış/üretim oranlarını etkileme düzeyine göre anlamlı farklılık göstermektedir." temel hipotezi ve bu hipoteze ilişkin alt hipotezler Anova testi ile analiz edilmiştir. Tabloda görüldüğü üzere; siber güvenlik ihlalleri ve iş sürekliliği yönetimi dışındaki tüm değişkenler bilişim sistemlerinin 24 saat hizmet vermemesinin bir günlük satış/üretim oranlarını etkileme düzeyine göre anlamlı farklılık göstermektedir. Bu durumda araştırma kapsamında test edilen; H5 temel hipotezi ve diğer alt hipotezlerden "H5a: Siber güvenliğe kurumsal yaklaşım firmaların bilişim sistemlerinin 24 saat hizmet vermemesinin bir günlük satış/üretim oranlarını etkileme düzeyine göre anlamlı farklılık göstermektedir.", "H5b: Fiziksel ve çevresel güvenlik tedbirleri firmaların bilişim sistemlerinin 24 saat hizmet vermemesinin bir günlük satış/üretim oranlarını etkileme düzeyine göre anlamlı farklılık göstermektedir.", "H5c: Bilişim sistemleri ve iletişim ağlarının işletim ve bakım kontrolleri firmaların bilişim sistemlerinin 24 saat hizmet vermemesinin bir günlük satış/üretim oranlarını etkileme düzeyine göre anlamlı farklılık göstermektedir." ve "H5d: Yazılım geliştirme ve destek aşamalarında bilgi sistemleri erişim kontrolü güvenlik tedbirleri

firmaların bilişim sistemlerinin 24 saat hizmet vermemesinin bir günlük satış/üretim oranlarını etkileme düzeyine göre anlamlı farklılık göstermektedir."alt hipotezleri desteklenmiştir. Diğer taraftan "H5e: Siber güvenlik ihlalleri ve iş sürekliliği firmaların bilişim sistemlerinin 24 saat hizmet vermemesinin bir günlük satış/üretim oranlarını etkileme düzeyine göre anlamlı farklılık göstermektedir." hipotezi desteklenmemiştir.

Farklılığın yönünü görebilmek için Tukey testine bakılmıştır. Tukey testi sonuçlarına göre siber güvenliğine kurumsal yaklaşım bilişim sistemlerinin 24 saat hizmet vermemesi durumunda satış ve/veya üretimi % 25 oranından az etkileyen firmalar ile % 50-75 arası ve % 75 üzeri etkileyen firmalar arasında % 75 üzeri etkileyen firmalar lehine anlamlı farklılık göstermektedir. Fiziksel ve çevresel güvenlik tedbirleri bilişim sistemlerinin 24 saat hizmet vermemesi durumunda satış ve/veya üretimi % 25-50 oranı arasında etkileyen firmalar ile % 75 üstü etkileyen firmalar arasında % 75 üstü etkileyen firmalar lehine anlamlı farklılık bulunmaktadır. Bilişim sistemleri ve iletişim ağlarının işletim ve bakım kontrolleri bilişim sistemlerinin 24 saat hizmet vermemesi durumunda satış ve/veya üretimi % 25-50 oranında etkilenen firmalar ile % 50-75 arası ve % 75 üstü etkilenen firmalar arasında % 50-75 arası etkilenen firmalar lehine anlamlı farklılık göstermektedir. Yazılım geliştirme ve destek aşamalarında bilgi sistemleri erişim kontrolü güvenlik tedbirleri bilişim sistemlerinin 24 saat hizmet vermemesi durumunda satış ve/veya üretimi % 25'den az etkilenen firmalar ile % 50-75 arası etkilenen ve % 75 üstü etkilenen firmalar arasında % 75 üstü etkilenen firmalar lehine anlamlı farklılık göstermektedir. Genel siber güvenlik yaklaşımı bilişim sistemlerinin 24 saat hizmet vermemesi durumunda satış ve/veya üretimi % 25'den az etkilenen firmalar ile % 50-75 arası etkilenen ve % 75 üstü etkilenen firmalar arasında % 75 üstü etkilenen firmalar lehine anlamlı farklılık göstermektedir.

Tablo 49. Siber Saldırının Firma İmajı Üzerine Olası Etkileri Göre Anova Testi

Değişkenler		Kareler Toplamı	df	Kareler Ortalaması	F	Sig.	Farklılık
Siber Güvenliğine Kurumsal Yaklaşım	Gruplar arası	20,611	3	6,870	9,571	,000	1-4 2-3 2-4
	Gruplar içi	89,009	124	,718			
	Toplam	109,621	127				
Fiziksel ve Çevresel Güvenlik Tedbirleri	Gruplar arası	3,175	3	1,058	1,670	,177	-
	Gruplar içi	78,559	124	,634			
	Toplam	81,734	127				
Bilişim Sistemleri ve İletişim Ağlarının İşletim Ve Bakım Kontrolleri	Gruplar arası	7,206	3	2,402	3,784	,012	1-4
	Gruplar içi	78,707	124	,635			
	Toplam	85,913	127				
Yazılım Geliştirme ve Destek Aşamalarında Bilgi Sistemleri Erişim Kontrolü Güvenlik Tedbirleri	Gruplar arası	16,593	3	5,531	6,357	,000	1-4 2-4
	Gruplar içi	107,889	124	,870			
	Toplam	124,482	127				
Siber Güvenlik İhlalleri ve İş Sürekliliği Yönetimi	Gruplar arası	7,591	3	2,530	2,355	,075	-
	Gruplar içi	133,256	124	1,075			
	Toplam	140,846	127				
Genel Siber Güvenlik Yaklaşımı	Gruplar arası	9,196	3	3,065	7,606	,000	1-4 2-4
	Gruplar içi	49,976	124	,403			
	Toplam	59,172	127				

Tablo 49'da görüldüğü üzere araştırma kapsamında test edilen "H6: Siber güvenlik yaklaşımları siber saldırıların firma imajı üzerindeki olası etkilerine göre anlamlı farklılık göstermektedir." temel hipotezi ve bu hipoteze ilişkin alt hipotezler Anova testi ile analiz edilmiştir. Anova testi sonuçlarına göre siber güvenliğine kurumsal yaklaşım, bilişim sistemleri ve iletişim ağlarının işletim ve bakım kontrolleri, yazılım geliştirme ve destek aşamalarında bilgi sistemleri erişim kontrolü güvenlik tedbirleri ve genel siber güvenlik yaklaşımı siber saldırının firma imajı üzerine olası etkilerine göre anlamlı farklılık göstermektedir. Fiziksel ve çevresel güvenlik tedbirleri ile siber güvenlik ihlalleri ve iş sürekliliği yönetimi siber saldırının firma imajı üzerine olası etkilerine göre anlamlı farklılık göstermemektedir. Bu durumda araştırma kapsamında test edilen; H6 temel hipotezi ve diğer alt hipotezlerden "H6a: siber güvenliğe kurumsal yaklaşım siber saldırıların firma imajı üzerindeki olası etkilerine göre anlamlı farklılık göstermektedir.", "H6c: bilişim sistemleri ve iletişim ağlarının işletim ve bakım kontrolleri firmaların siber saldırıların firma imajı üzerindeki olası etkilerine göre anlamlı farklılık göstermektedir." ve "H6d: yazılım geliştirme ve destek aşamalarında bilgi sistemleri erişim kontrolü güvenlik tedbirleri siber saldırıların firma imajı üzerindeki olası etkilerine göre anlamlı

farklılık göstermektedir.” Hipotezleri desteklenmiştir. Diğer taraftan alt hipotezlerden “H6b: fiziksel ve çevresel güvenlik tedbirleri siber saldırıların firma imajı üzerindeki olası etkilerine göre anlamlı farklılık göstermektedir.” ve “H6e: siber güvenlik ihlalleri ve iş sürekliliği siber saldırıların firma imajı üzerindeki olası etkilerine göre anlamlı farklılık göstermektedir.” hipotezleri desteklenmemiştir.

Araştırmada gruplar arası farklılığın yönünü görebilmek için Tukey testine bakılmıştır. Tukey testi sonuçlarına göre siber güvenliğine kurumsal yaklaşım siber saldırının firma imajı üzerine olası etkisi firmaların geleceğini etkileyecek kadar fazla olan firmalar ile az olanlar ve neredeyse hiç olmayan firmalar arasında firmanın geleceğini etkileyecek kadar fazla olan firmalar lehine anlamlı farklılık göstermektedir. Ayrıca siber güvenliğine kurumsal yaklaşım siber saldırının firma imajı üzerine olası etkisi az olanlar ile çok olanlar arasında çok olanlar lehine bir farklılık vardır. Bilişim sistemleri ve iletişim ağlarının işletim ve bakım kontrolleri siber saldırının firma imajı üzerine olası etkisi firmaların geleceğini etkileyecek kadar fazla olan firmalar ile neredeyse hiç olmayan firmalar arasında firmanın geleceğini etkileyecek kadar fazla olan firmalar lehine anlamlı farklılık göstermektedir. Yazılım geliştirme ve destek aşamalarında bilgi sistemleri erişim kontrolü güvenlik tedbirleri siber saldırının firma imajı üzerine olası etkisi firmaların geleceğini etkileyecek kadar fazla olan firmalar ile az olan ve neredeyse hiç olmayan firmalar arasında firmanın geleceğini etkileyecek kadar fazla olan firmalar lehine anlamlı farklılık göstermektedir. Genel siber güvenlik yaklaşımı siber saldırının firma imajı üzerine olası etkisi firmaların geleceğini etkileyecek kadar fazla olan firmalar ile az olan ve neredeyse hiç olmayan firmalar arasında firmanın geleceğini etkileyecek kadar fazla olan firmalar lehine anlamlı farklılık göstermektedir. Araştırma kapsamında elde edilen verilere göre siber saldırının firma imajı üzerine olası etkileri dikkate alındığında; firmanın geleceğini etkileyecek kadar fazla olması durumundaki firmalar diğerlerine göre (nerdeyse olmaz, az olur ve çok olur) siber güvenliğine yaklaşım düzeyleri daha yüksektir. Yani bu firmalar siber güvenliğe daha fazla önem vermektedirler.

Tablo 50. Kritik Bilgilerin Tüm Bilgilere Oranına Göre Anova Testi

Değişken		Kareler Toplamı	df	Kareler Ortalaması	F	Sig.	Farklılık
Siber Güvenliğine Kurumsal Yaklaşım	Gruplar arası	31,879	3	10,626	16,949	,000	1-3 1-4 2-3 2-4
	Gruplar içi	77,741	124	,627			
	Toplam	109,621	127				
Fiziksel ve Çevresel Güvenlik Tedbirleri	Gruplar arası	13,764	3	4,588	8,370	,000	1-3 1-4 2-3 2-4
	Gruplar içi	67,970	124	,548			
	Toplam	81,734	127				
Bilişim Sistemleri ve İletişim Ağlarının İşletim Ve Bakım Kontrolleri	Gruplar arası	11,409	3	3,803	6,330	,000	1-4 2-4
	Gruplar içi	74,503	124	,601			
	Toplam	85,913	127				
Yazılım Geliştirme ve Destek Aşamalarında Bilgi Sistemleri Erişim Kontrolü Güvenlik Tedbirleri	Gruplar arası	17,234	3	5,745	6,642	,000	1-3 1-4 2-4
	Gruplar içi	107,248	124	,865			
	Toplam	124,482	127				
Siber Güvenlik İhlalleri ve İş Sürekliliği Yönetimi	Gruplar arası	14,480	3	4,827	4,736	,004	1-3 2-3
	Gruplar içi	126,366	124	1,019			
	Toplam	140,846	127				
Genel Siber Güvenlik Yaklaşımı	Gruplar arası	15,901	3	5,300	15,189	,000	1-3 1-4 2-3 2-4
	Gruplar içi	43,271	124	,349			
	Toplam	59,172	127				

Tablo 50'de araştırma kapsamında test edilen "H7: Siber güvenlik yaklaşımları firmaların elindeki kritik bilgilerin oranına göre anlamlı farklılık göstermektedir." temel hipotezi ve bu hipoteze ilişkin alt hipotezler Anova testi ile analiz edilmiştir. Tablo 50'de görüldüğü üzere siber güvenliğine kurumsal yaklaşım; fiziksel ve çevresel güvenlik tedbirleri, bilişim sistemleri ve iletişim ağlarının işletim ve bakım kontrolleri, yazılım geliştirme ve destek aşamalarında bilgi sistemleri erişim kontrolü güvenlik tedbirleri, siber güvenlik ihlalleri ve iş sürekliliği yönetimi ve genel siber güvenlik yaklaşımı firmaların kritik bilgilerinin oranına göre anlamlı farklılık göstermektedir. Bu durumda araştırma kapsamında test edilen H7, H7a, H7b, H7c, H7d ve H7e hipotezlerinin tamamı desteklenmiştir. Yani araştırma kapsamında elde edilen verilere göre firmaların elindeki kritik bilgilerin oranına göre firmaların siber güvenlik yaklaşımları farklılık göstermektedir. Farklılığın yönünü görebilmek için Tukey testi yapılmıştır.

Tukey testi sonuçlarına göre siber güvenliğine kurumsal yaklaşım firmaların elindeki bilgilerin çoğunluğu kritik öneme sahip olanlar ile neredeyse hiç kritik öneme sahip bilgisi bulunmayanlar ve az bilgi bulunanlar arasında bilgilerinin çoğunluğu kritik öneme sahip olan firmalar lehine anlamlı farklılık bulunmaktadır. Ayrıca siber güvenliğine kurumsal yaklaşım

firmaların elindeki bilgilerin yarısı kritik öneme sahip olanlar ile neredeyse hiç kritik öneme sahip bilgisi bulunmayanlar ve az bilgi bulunanlar arasında bilgilerinin yarısı kritik öneme sahip olan firmalar lehine anlamlı farklılık bulunmaktadır. Fiziksel ve çevresel güvenlik tedbirleri firmaların elindeki bilgilerin çoğunluğu kritik öneme sahip olanlar ile neredeyse hiç kritik öneme sahip bilgisi bulunmayanlar ve az bilgi bulunanlar arasında bilgilerinin çoğunluğu kritik öneme sahip olan firmalar lehine anlamlı farklılık göstermektedir. Ayrıca fiziksel ve çevresel güvenlik tedbirleri firmaların elindeki bilgilerin yarısı kritik öneme sahip olanlar ile neredeyse hiç kritik öneme sahip bilgisi bulunmayanlar ve az bilgi bulunanlar arasında bilgilerinin yarısı kritik öneme sahip olan firmalar lehine anlamlı farklılık göstermektedir. Bilişim sistemleri ve iletişim ağlarının işletim ve bakım kontrolleri firmaların elindeki bilgilerin çoğunluğu kritik öneme sahip olanlar ile neredeyse hiç kritik öneme sahip bilgisi bulunmayanlar arasında bilgilerinin çoğunluğu kritik öneme sahip olan firmalar lehine anlamlı farklılık göstermektedir. Yazılım geliştirme ve destek aşamalarında bilgi sistemleri erişim kontrolü güvenlik tedbirleri firmaların elindeki bilgilerin çoğunluğu kritik öneme sahip olanlar ile neredeyse hiç kritik öneme sahip bilgisi bulunmayanlar ve az bilgi bulunanlar arasında bilgilerinin çoğunluğu kritik öneme sahip olan firmalar lehine anlamlı farklılık bulunmaktadır. Ayrıca yazılım geliştirme ve destek aşamalarında bilgi sistemleri erişim kontrolü güvenlik tedbirleri firmaların elindeki bilgilerin yarısı kritik öneme sahip olanlar ile neredeyse hiç kritik öneme sahip bilgisi bulunmayanlar arasında bilgilerinin yarısı kritik öneme sahip olan firmalar lehine anlamlı farklılık bulunmaktadır. Siber güvenlik ihlalleri ve iş sürekliliği yönetimi firmaların elindeki bilgilerin neredeyse yarısı kritik öneme sahip olanlar ile neredeyse hiç kritik öneme sahip bilgisi bulunmayanlar arasında bilgilerinin yarısı kritik öneme sahip olan firmalar lehine anlamlı farklılık göstermektedir. Siber güvenlik ihlalleri ve iş sürekliliği yönetimi firmaların elindeki bilgilerin neredeyse yarısı kritik öneme sahip olanlar ile neredeyse hiç kritik öneme sahip bilgisi bulunmayanlar arasında bilgilerinin yarısı kritik öneme sahip olan firmalar lehine anlamlı farklılık göstermektedir. Genel siber güvenlik yaklaşımı firmaların elindeki bilgilerin çoğunluğu kritik öneme sahip olanlar ile neredeyse hiç kritik öneme sahip bilgisi bulunmayanlar ve az bilgi bulunanlar arasında bilgilerinin çoğunluğu kritik öneme sahip olan firmalar lehine anlamlı farklılık göstermektedir. Ayrıca siber güvenlik yaklaşımı firmaların elindeki bilgilerin yarısı kritik öneme sahip olanlar ile neredeyse hiç kritik öneme sahip bilgisi bulunmayanlar ve az bilgi bulunanlar arasında bilgilerinin yarısı kritik öneme sahip olan firmalar lehine anlamlı farklılık göstermektedir. Özet olarak siber güvenlik yaklaşım düzeyleri tüm değişkenlerde firmaların elindeki bilgilerin çoğunluğu ve yarısı kritik öneme sahip olanların firmaların elindeki bilgilerin neredeyse hiç kritik öneme sahip bilgisi bulunmayanlar ve

az bilgi bulunanlar arasında farklılık bulunmaktadır. Bu farklılık bilgilerin kritik önemi yüksek olan firmaların lehinedir. Yani araştırma kapsamındaki firmaların bilgilerinin kritik önemi arttıkça siber güvenlik yaklaşım düzeyleri de artmaktadır.

Tablo 51. Personel Değişim Oranına Göre Anova Testi

Değişken		Kareler Toplamı	df	Kareler Ortalaması	F	Sig.	Farklılık
Siber Güvenliğine Kurumsal Yaklaşım	Gruplar arası	6,154	2	3,077	3,718	,027	1-3
	Gruplar içi	103,466	125	,828			
	Toplam	109,621	127				
Fiziksel ve Çevresel Güvenlik Tedbirleri	Gruplar arası	3,198	2	1,599	2,545	,083	-
	Gruplar içi	78,536	125	,628			
	Toplam	81,734	127				
Bilişim Sistemleri ve İletişim Ağlarının İşletim Ve Bakım Kontrolleri	Gruplar arası	2,078	2	1,039	1,549	,216	-
	Gruplar içi	83,835	125	,671			
	Toplam	85,913	127				
Yazılım Geliştirme ve Destek Aşamalarında Bilgi Sistemleri Erişim Kontrolü Güvenlik Tedbirleri	Gruplar arası	,554	2	,277	,279	,757	-
	Gruplar içi	123,928	125	,991			
	Toplam	124,482	127				
Siber Güvenlik İhlalleri ve İş Sürekliliği Yönetimi	Gruplar arası	,526	2	,263	,234	,792	-
	Gruplar içi	140,321	125	1,123			
	Toplam	140,846	127				
Genel ortalama	Gruplar arası	1,781	2	,891	1,940	,148	-
	Gruplar içi	57,391	125	,459			
	Toplam	59,172	127				

Araştırma kapsamında firmaların siber güvenlik yaklaşımlarının personel değişim oranına göre anlamlı farklılık gösterip göstermediğini analiz etmek için anova testi yapılmış ve analiz sonuçları Tablo 51'de verilmiştir. Tabloda görüldüğü üzere siber güvenliğe kurumsal yaklaşım haricinde bütün değişkenler firmaların personel değişim oranına göre oranına göre anlamlı farklılık göstermemektedir. Bu durumda araştırma kapsamında test edilen "H9: Siber güvenlik yaklaşımları firmaların personel değişim oranına göre anlamlı farklılık göstermektedir." temel hipotez ile "H9a: Siber güvenliğe kurumsal yaklaşım firmaların personel değişim oranına göre anlamlı farklılık göstermektedir." alt hipotezi desteklenmiştir. Diğer alt hipotezler; "H9b: Fiziksel ve çevresel güvenlik tedbirleri firmaların personel değişim oranına göre anlamlı farklılık göstermektedir.", "H9c: Bilişim sistemleri ve iletişim ağlarının işletim ve bakım kontrolleri firmaların personel değişim oranına göre anlamlı farklılık göstermektedir.",

"H9d: Yazılım geliştirme ve destek aşamalarında bilgi sistemleri erişim kontrolü güvenlik tedbirleri firmaların personel değişim oranına göre anlamlı farklılık göstermektedir." ve "H9e: Siber güvenlik ihlalleri ve iş sürekliliği firmaların personel değişim oranına göre anlamlı farklılık göstermektedir." Araştırma kapsamında desteklenmemiştir.

Araştırmada hangi gruplar arasında farklılık olduğu, Tukey testi kullanılarak analiz edilmiştir. Tukey analizi sonuçlarına göre siber güvenliğine kurumsal yaklaşım personel değişim oranına göre % 10 ve altı ile % 31-50 arası personel değişim olan firmalar arasında % 31-50 olan firmalar lehine anlamlı farklılık göstermektedir. Yani personel değişim oranına % 31-50 olan firmaların siber güvenlik yaklaşım düzeyleri daha yüksektir.

4.5. Hipotez Sonuçları

Araştırma kapsamında test edilen hipotezlere ilişkin analizler ve sonuçları daha önce ayrıntılı olarak verilmişti. Aşağıda bu hipotezlere ilişkin sonuçları toplu olarak tablo 52'de verilmiştir.

Tablo 52. Hipotez Sonuçları

Hipotezler	**Sonuçlar**
H1: Gaziantep İmalat Sanayiinde faaliyet gösteren firmaların siber güvenlik yaklaşım seviyesi düşüktür.	Desteklendi
H2: Siber güvenlik yaklaşımları firmaların çalışan sayısına göre anlamlı farklılık göstermektedir.	Desteklendi
H2a: Siber güvenliğe kurumsal yaklaşım firmaların çalışan sayısına göre anlamlı farklılık göstermektedir.	Desteklendi
H2b: Fiziksel ve çevresel güvenlik tedbirleri firmaların çalışan sayısına göre anlamlı farklılık göstermektedir.	Reddedildi
H2c: Bilişim Sistemleri ve İletişim Ağlarının İşletim Ve Bakım Kontrolleri firmaların çalışan sayısına göre anlamlı farklılık göstermektedir.	Desteklendi
H2d: Yazılım Geliştirme ve Destek Aşamalarında Bilgi Sistemleri Erişim Kontrolü Güvenlik Tedbirleri firmaların çalışan sayısına göre anlamlı farklılık göstermektedir.	Desteklendi
H2e: Siber Güvenlik İhlalleri ve İş Sürekliliği Yönetimi firmaların çalışan sayısına göre anlamlı farklılık göstermektedir.	Desteklendi
H3: Siber güvenlik yaklaşımları firmaların yıllık cirosuna göre anlamlı farklılık göstermektedir.	Desteklendi
H3a: Siber güvenliğe kurumsal yaklaşım firmaların yıllık cirosuna göre anlamlı farklılık göstermektedir.	Desteklendi
H3b: Fiziksel ve çevresel güvenlik tedbirleri firmaların yıllık cirosuna göre anlamlı farklılık göstermektedir.	Reddedildi
H3c: Bilişim Sistemleri ve İletişim Ağlarının İşletim Ve Bakım Kontrolleri firmaların yıllık cirosuna göre anlamlı farklılık göstermektedir.	Desteklendi
H3d: Yazılım Geliştirme ve Destek Aşamalarında Bilgi Sistemleri Erişim Kontrolü Güvenlik Tedbirleri firmaların yıllık cirosuna göre anlamlı farklılık göstermektedir	Desteklendi
H3e: Siber Güvenlik İhlalleri ve İş Sürekliliği Yönetimi firmaların yıllık cirosuna göre anlamlı farklılık göstermektedir.	Reddedildi
H4: Siber güvenlik yaklaşımları firmaların ticari faaliyetlerde internete bağımlılık oranına göre anlamlı farklılık göstermektedir.	Desteklendi
H4a: Siber güvenliğe kurumsal yaklaşım firmaların ticari faaliyetlerde internete bağımlılık oranına göre anlamlı farklılık göstermektedir.	Desteklendi

H4b: Fiziksel ve çevresel güvenlik tedbirleri firmaların ticari faaliyetlerde internete bağımlılık oranına göre anlamlı farklılık göstermektedir.	Desteklendi
H4c: Bilişim Sistemleri ve İletişim Ağlarının İşletim Ve Bakım Kontrolleri firmaların ticari faaliyetlerde internete bağımlılık oranına göre anlamlı farklılık göstermektedir.	Desteklendi
H4d: Yazılım Geliştirme ve Destek Aşamalarında Bilgi Sistemleri Erişim Kontrolü Güvenlik Tedbirleri firmaların ticari faaliyetlerde internete bağımlılık oranına göre anlamlı farklılık göstermektedir.	Desteklendi
H4e: Siber Güvenlik İhlalleri ve İş Sürekliliği Yönetimi firmaların ticari faaliyetlerde internete bağımlılık oranına göre anlamlı farklılık göstermektedir.	Reddedildi
H5: Siber güvenlik yaklaşımları firmaların bilişim sistemlerinin 24 saat hizmet vermemesinin bir günlük satış / üretim oranlarını etkileme düzeyine göre anlamlı farklılık göstermektedir.	Desteklendi
H5a: Siber güvenliğe kurumsal yaklaşım firmaların bilişim sistemlerinin 24 saat hizmet vermemesinin bir günlük satış / üretim oranlarını etkileme düzeyine göre anlamlı farklılık göstermektedir.	Desteklendi
H5b: Fiziksel ve çevresel güvenlik tedbirleri firmaların bilişim sistemlerinin 24 saat hizmet vermemesinin bir günlük satış / üretim oranlarını etkileme düzeyine göre anlamlı farklılık göstermektedir.	Desteklendi
H5c: Bilişim Sistemleri ve İletişim Ağlarının İşletim Ve Bakım Kontrolleri firmaların bilişim sistemlerinin 24 saat hizmet vermemesinin bir günlük satış / üretim oranlarını etkileme düzeyine göre anlamlı farklılık göstermektedir.	Desteklendi
H5d: Yazılım Geliştirme ve Destek Aşamalarında Bilgi Sistemleri Erişim Kontrolü Güvenlik Tedbirleri firmaların bilişim sistemlerinin 24 saat hizmet vermemesinin bir günlük satış / üretim oranlarını etkileme düzeyine göre anlamlı farklılık göstermektedir.	Desteklendi
H5e: Siber Güvenlik İhlalleri ve İş Sürekliliği firmaların bilişim sistemlerinin 24 saat hizmet vermemesinin bir günlük satış / üretim oranlarını etkileme düzeyine göre anlamlı farklılık göstermektedir.	Reddedildi
H6: Siber güvenlik yaklaşımları siber saldırıların firma imajı üzerindeki olası etkilerine göre anlamlı farklılık göstermektedir.	Desteklendi
H6a: Siber güvenliğe kurumsal yaklaşım siber saldırıların firma imajı üzerindeki olası etkilerine göre anlamlı farklılık göstermektedir.	Desteklendi
H6b: Fiziksel ve çevresel güvenlik tedbirleri siber saldırıların firma imajı üzerindeki olası etkilerine göre anlamlı farklılık göstermektedir.	Reddedildi
H6c: Bilişim Sistemleri ve İletişim Ağlarının İşletim Ve Bakım Kontrolleri firmaların siber saldırıların firma imajı üzerindeki olası etkilerine göre anlamlı farklılık göstermektedir.	Desteklendi
H6d: Yazılım Geliştirme ve Destek Aşamalarında Bilgi Sistemleri Erişim Kontrolü Güvenlik Tedbirleri siber saldırıların firma imajı üzerindeki olası etkilerine göre anlamlı farklılık göstermektedir.	Desteklendi
H6e: Siber Güvenlik İhlalleri ve İş Sürekliliği siber saldırıların firma imajı üzerindeki olası etkilerine göre anlamlı farklılık göstermektedir.	Reddedildi
H7: Siber güvenlik yaklaşımları firmaların elindeki kritik bilgilerin oranına göre anlamlı farklılık göstermektedir.	Desteklendi
H7a: Siber güvenliğe kurumsal yaklaşım firmaların elindeki kritik bilgilerin oranına göre anlamlı farklılık göstermektedir.	Desteklendi
H7b: Fiziksel ve çevresel güvenlik tedbirleri firmaların elindeki kritik bilgilerin oranına göre anlamlı farklılık göstermektedir.	Desteklendi
H7c: Bilişim Sistemleri ve İletişim Ağlarının İşletim Ve Bakım Kontrolleri firmaların elindeki kritik bilgilerin oranına göre anlamlı farklılık göstermektedir.	Desteklendi
H7d: Yazılım Geliştirme ve Destek Aşamalarında Bilgi Sistemleri Erişim Kontrolü Güvenlik Tedbirleri firmaların elindeki kritik bilgilerin oranına göre anlamlı farklılık göstermektedir.	Desteklendi
H7e: Siber Güvenlik İhlalleri ve İş Sürekliliği firmaların elindeki kritik bilgilerin oranına göre anlamlı farklılık göstermektedir.	Desteklendi
H8: Siber saldırıya uğrayan firmaların siber güvenlik yaklaşım seviyesi daha yüksektir.	Reddedildi
H8a: Siber saldırıya maruz olma durumuna göre firmaların siber güvenliğe kurumsal yaklaşım düzeyleri anlamlı farklılık göstermektedir.	Reddedildi
H8b: Siber saldırıya maruz olma durumuna göre firmaların fiziksel ve çevresel güvenlik tedbirleri anlamlı farklılık göstermektedir.	Reddedildi
H8c: Siber saldırıya maruz olma durumuna göre firmaların bilişim sistemleri ve iletişim ağlarının işletim ve bakım kontrolleri anlamlı farklılık göstermektedir.	Reddedildi

H8d: Siber saldırıya maruz olma durumuna göre firmaların yazılım geliştirme ve destek aşamalarında bilgi sistemleri erişim kontrolü güvenlik tedbirleri anlamlı farklılık göstermektedir.	Reddedildi
H8e: Siber saldırıya maruz olma durumuna göre firmaların siber güvenlik ihlalleri ve iş sürekliliği anlamlı farklılık göstermektedir.	Reddedildi
H9: Siber güvenlik yaklaşımları firmaların personel değişim oranına göre anlamlı farklılık göstermektedir.	Desteklendi
H9a: Siber güvenliğe kurumsal yaklaşım firmaların personel değişim oranına göre anlamlı farklılık göstermektedir.	Desteklendi
H9b: Fiziksel ve çevresel güvenlik tedbirleri firmaların personel değişim oranına göre anlamlı farklılık göstermektedir.	Reddedildi
H9c: Bilişim sistemleri ve iletişim ağlarının işletim ve bakım kontrolleri firmaların personel değişim oranına göre anlamlı farklılık göstermektedir.	Reddedildi
H9d: Yazılım geliştirme ve destek aşamalarında bilgi sistemleri erişim kontrolü güvenlik tedbirleri firmaların personel değişim oranına göre anlamlı farklılık göstermektedir.	Reddedildi
H9e: Siber güvenlik ihlalleri ve iş sürekliliği firmaların personel değişim oranına göre anlamlı farklılık göstermektedir.	Reddedildi

BEŞİNCİ BÖLÜM

SONUÇ VE ÖNERİLER

5.1. Sonuçlar

Bu çalışma, 2016 yılının ikinci yarısı ve 2017 yılının ilk çeyreğinde Gaziantep'te faaliyet gösteren orta ve büyük ölçekli imalat firmalarında yapılmıştır. Bu kapsamda çalışmada yüz yüze anket tekniği kullanılarak elde edilen 128 veri analiz edilerek aşağıdaki sonuçlara ulaşılmıştır.

Çalışan sayılarına göre, araştırmaya katılan firmaların çoğunluğu orta ölçekli işletmelerden oluşmaktadır. Yıllık ciroları dikkate alındığında ise; çoğunluğun büyük ölçekli işletmelerden oluştuğu görülmektedir. Bu durumun yapılan teknoloji yatırımları ile personel sayısı azalan işletmelerin cirolarının her geçen gün artmasından ve işletme ölçekleri belirlenirken bazen çalışan sayısı bazen de cirolarına bakılmasından kaynaklanmaktadır.

Araştırmaya katılan firmaların faaliyetlerinin dayandığı bilişim sistemlerine (diğer şirketler tarafından sağlanan sistemler de dahil olmak üzere, e-posta, web sitesi, kiralık sunucu vb.) bağımlılık oranların yüksek olduğu tespit edilmiştir. Bu durum; bilişim sistemlerinde yaşanabilecek herhangi bir aksaklık veya olumsuzluğun araştırma kapsamındaki firmaların faaliyetlerinde aksama ve olumsuzluklara neden olacağı anlamına gelmektedir. Bu sonuç araştırma kapsamındaki firmaların siber güvenliğe daha çok önem vermesi gereğini ortaya koymaktadır.

Bu araştırmada, firmaların üretim ve ticari faaliyetlerinde internete bağımlılık düzeyinin yüksek olduğu tespit edilmiştir. Aynı şekilde, araştırma kapsamındaki firmaların çoğunluğu, bilişim sistemlerinin bir gün hizmet verememesi durumunda, günlük satış ve üretim faaliyetleri üzerindeki olumsuz etkisinin çok fazla olacağını tespit edilmiştir. Diğer taraftan bilişim sistem ve hizmetlerindeki aksamaları tolere etme süresinin bir günün üzerinde olan işletme sayısının araştırma kapsamındaki işletmelerin yüzde elliye yakını olduğu tespit edilmiştir. Dolayısıyla bilişim hizmetlerinde yaşanabilecek herhangi bir olumsuzluğun, firmaların faaliyetlerine de olumsuzluk olarak yansıyacağını, bu yüzden firmaların, faaliyetlerinde olumsuzluklara maruz kalmamak için siber güvenliğe daha çok önem vermek zorunda olduklarını göstermektedir.

Araştırma kapsamındaki firmalar, kendilerini hedef alan ve kişisel bilgilerin (müşteri bilgileri vb.) sızdırılması ile sonuçlanan bir siber saldırının firma imajı üzerinde olumsuz etkilere yol açacağını düşünmektedirler. Hatta araştırmaya katılan firmaların yarısı firma geleceğini

etkileyecek kadar olumsuz bir etkisinin olacağını belirtmişlerdir. Yani araştırma kapsamında firmaların çoğunluğu, bir siber saldırı olduğunda firma imajlarının olumsuz etkileneceğini öngörmektedirler. Bu durum da firmaların bir siber saldırı oluşmaması ve firma imajlarının olumsuz etkilenmemesi için siber güvenliğe daha çok önem vermeleri gereğini ortaya çıkarmaktadır.

Firmaların kritik bilgilerinde sızıntı (ulusal sırlar, ticari sırlar, gizlilik bilgileri gibi) meydana gelirse faaliyetler üzerinde ciddi etkilere neden olabilir. Araştırma kapsamındaki firmaların çok azının kritik bilgisinin olmadığı, fakat geri kalan büyük çoğunluğunun az veya çok kritik bilgilerinin olduğunu düşündükleri tespit edilmiştir. Dolayısıyla firmalar kritik bilgilerinde bir sızıntının olmaması için gerekli önlemleri almak zorundadırlar. Aksi takdirde kritik bilgilerinde bir sızıntı olursa firmaların faaliyetlerinde de ciddi olumsuzluklar meydana gelebilir.

Araştırma kapsamındaki firmaların müşteri veya tedarikçilerine ait bilişim sistemlerinde korunması gerekli çok miktarda bilgi bulundurduğu tespit edilmiştir. Örneğin bu firmaların yarısından fazlasının sayı olarak on bin adedin üzerinde korunması gerekli bilgisi bulunmaktadır. Bu durum araştırma kapsamındaki firmaların ilişkili olduğu ve korunması gereken bilgi miktarının çok büyük olduğunu göstermektedir. Dolayısıyla firmaların bu bilgilerin korunması için siber güvenliğe daha çok önem vermeleri gerekmektedir. Aksi takdirde bu bilgilerin korunamaması durumunda; firmalar sıkıntı yaşayabilecek, güvenilirlik ve imajları olumsuz etkilenecektir. Ayrıca söz konusu bu bilgiler kendileri ile ilgili müşteri, tedarikçi ve firmanın diğer ilgi çevresinin de ayrıca zarar görmesi kaçınılmaz olacaktır.

Araştırma kapsamında firmaların çoğunun personel değişim oranlarının %10'un altında olduğu görülmüştür. Bu durum araştırma kapsamındaki firmaların personel değişim oranlarının düşük olduğunu göstermektedir. Firmaların personel değişim oranının düşük olması siber güvenlik açısından olumlu bir durumdur. Zira firmadan ayrılan personel, sahip olduğu bilgilerle güvenlik ihlallerine neden olabilmektedir. Bu nedenle firmaların personel değişim oranlarının düşük olması, özellikle kritik noktadaki personellerini firmada tutmak için gerekli tedbirleri almasının önemini göstermektedir.

Araştırma kapsamındaki firmaların büyük çoğunluğunun daha önce çeşitli siber güvenlik olayları ile karşılaştığı görülmüştür. Bu durum firmaların siber güvenliğe daha fazla önem vermeleri gerektiğini göstermektedir.

Araştırma kapsamındaki firmaların siber güvenliğe ilişkin yaklaşımlarına ilişkin soruya verilen cevaplara göre; ortalama değerlere bakılarak değerlendirilmiştir. Araştırma kapsamındaki firmaların siber güvenliğe kurumsal yaklaşım, yazılım geliştirme ve destek aşamalarında bilgi sistemleri erişim kontrolü güvenlik tedbirleri, siber güvenlik ihlalleri ve iş sürekliliği yönetimi ile genel siber güvenlik yaklaşımlarının düşük düzeyde olduğu; fiziksel ve çevresel güvenlik tedbirleri ile bilişim sistemleri ve iletişim ağlarının işletim ve bakım kontrolleri düzeyinin orta düzeyde olduğu tespit edilmiştir. Bu durum araştırma kapsamındaki firmaların siber güvenliğe yaklaşım düzeylerinin genel olarak düşük olduğunu veya yeterince önem vermediğini göstermektedir. Dolayısıyla bu çalışmada Gaziantep imalat sanayiinde faaliyet gösteren firmaların siber güvenlik yaklaşım seviyelerinin düşük olduğu sonucuna varılmıştır. Bu durum ne yazık ki normal bir sonuçtur. Zira literatürde de işletmelerin siber güvenliğe yeterince önem vermediğine yönelik kanıtlar bulunmaktadır. Örneğin; Mil (2015) Türkiye'deki Sosyal Güvenlik Kurumun siber güvenlik alanında yazılı kural ve politikalarının olmasına rağmen bu kural ve politikaların yeterince uygulanmadığı tespit edilmiştir. Firmaların siber güvenliğe yeterince önem vermemeleri; konunun öneminin farkına yeterince varmamış olmalarından veya siber güvenliğinin öneminin farkında olsalar bile güvenlik gereklerini yeterli ölçüde yerine getirmemiş veya getirememiş olmalarından kaynaklanmaktadır. Araştırma kapsamında böyle bir sonucun çıkmış olması firmalar açısından istenmeyen bir durumdur. Çünkü siber güvenliğe yeterince önem vermeyen firmalar her an telafisi mümkün olmayan veya çok büyük maliyetlere ve sıkıntılara neden olabilecek siber saldırılara maruz kalabilirler.

Araştırmada firmaların siber güvenliğe kurumsal yaklaşım, bilişim sistemleri ve iletişim ağlarının işletim ve bakım kontrolleri ve yazılım geliştirme, destek aşamalarında bilgi sistemleri erişim kontrolü güvenlik tedbirleri ile genel siber güvenlik yaklaşımlarının firmaların çalışan sayılarına göre farklılık gösterdiği tespit edilmiştir. Araştırma kapsamında yer alan ve çalışan sayısı 250 ve üzeri olan büyük işletmelerin siber güvenliğe yaklaşım düzeyleri, orta büyüklükteki firmalara göre daha yüksektir. Literatürle bu sonuca ilişkin kanıtlar mevcuttur. Örneğin Dimopoulos, vd. (2004); çalışmalarında KOBİ'lerin siber güvenlik çalışmalarını koordine edecek yeterli kaynaklarının olmaması (personel, bütçe zaman ve bilgi) nedeni ile siber güvenlik farkındalıklarının daha düşük olduğunu tespit etmişlerdir. Bu çalışmada büyük firmaların, siber güvenliğe kurumsal yaklaşım düzeylerinin yüksek olmasının nedeni; diğer firmalara göre daha fazla yatırım yapma potansiyeline (yatırım yapabilecek güç ve bilgiye) sahip olmalarından, istihdam ettikleri personellerin daha nitelikli olmasından veya siber güvenliğin önemini daha önce ve daha çabuk fark etmelerinden kaynaklanıyor olabilir. Fiziksel ve çevresel güvenlik

tedbirleri ile siber güvenlik ihlalleri ve iş sürekliliği yönetimi firmaların çalışan sayılarına göre farklılık göstermemektedir. Bu, araştırmaya katılan tüm işletmelerin fiziksel ve çevresel güvenliklerini sağlamak için gerekli tedbirleri almaya çalıştıklarından kaynaklandığı düşünmektedir. Ayrıca, anket için yapılan görüşmeler sırasında alınan bilgilere göre firma yöneticilerinin işletmelerinin fiziksel güvenlik çalışmaları için (kamera, güvenlik personeli vb.) yatırımdan kaçınmadıkları ancak siber güvenlik hakkında yeterli bilgi ve farkındalığa sahip olmadıklarından ve doğrudan bir sonucu gözleri ile görmedikleri için bu sonuç çıkmış olabilir.

Araştırma kapsamında siber güvenliğe kurumsal yaklaşım, bilişim sistemleri ve iletişim ağlarının işletim ve bakım kontrolleri, yazılım geliştirme ve destek aşamalarında bilgi sistemleri erişim kontrolü güvenlik tedbirleri ve genel siber güvenlik yaklaşımı firmaların cirolarına göre anlamlı farklılık gösterdiği tespit edilmiştir. Araştırmada 40 milyon üzeri ciroya sahip olan firmaların siber güvenlik yaklaşım hassasiyetleri, 8-40 milyon arası ciroya sahip olan firmalara göre daha yüksek çıkmıştır. Yani cirosu yüksek olan firmaların siber güvenlik yaklaşımlarının daha yüksek olduğu görülmüştür. Diğer taraftan fiziksel ve çevresel güvenlik tedbirleri ile siber güvenlik ihlalleri ve iş sürekliliği yönetiminin, firmaların cirosuna göre anlamlı bir farklılık göstermediği tespit edilmiştir. Bunun nedeni, yukarıda ifade edildiği üzere, işletme büyüklüğünden kaynaklanıyor olabilir. Araştırmada fiziksel ve çevresel güvenlik tedbirleri ile siber güvenlik ihlalleri ve iş sürekliliği yönetimi bakımından firmaların cirosuna göre anlamlı bir farklılık çıkmamasının nedeni, bu değişkenlere ilişkin alınması gereken güvenlik tedbirlerinin asgari seviyede alınma zorunluğundan kaynaklanıyor olabilir.

Araştırma kapsamında siber saldırıya maruz olma durumuna göre firmaların siber güvenliğe yaklaşım düzeyleri, siber güvenliğe kurumsal yaklaşım düzeyleri dışında farklılık göstermemektedir. Bir saldırıya maruz kalmamış işletmelerin siber güvenliğe yaklaşım düzeyleri daha yüksektir. Diğer taraftan siber saldırıya maruz olma durumuna göre firmaların siber güvenliğe yaklaşım düzeyleri genel olarak aynı düzeyde olduğu tespit edilmiştir. Yani bir siber saldırı ile karşılaşan firmalar ile karşılaşmayan firmaların siber güvenliğe bakış açıları aynı düzeydedir. Bu durumun oldukça ilginç olduğu değerlendirilmektedir. Zira bir saldırıya maruz kalan firmaların siber güvenliğe daha fazla önem vermeleri beklenirken, araştırmada karşılaşılan bu sonuç; araştırma kapsamındaki firmaların siber güvenlik yaklaşımlarının genel olarak düşük olmasından kaynaklanıyor olabilir. Ayrıca araştırma kapsamındaki firmaların karşılaştığı siber saldırıların etkisinin düşük olmasından veya firmaların siber güvenlik anlayışlarından kaynaklanıyor olabilir.

Araştırma kapsamında firmaların siber güvenliğe kurumsal yaklaşımları, fiziksel ve çevresel güvenlik tedbirleri, bilişim sistemleri ve iletişim ağlarının işletim ve bakım kontrolleri, yazılım geliştirme ve destek aşamalarında bilgi sistemleri erişim kontrolü güvenlik tedbirleri firmaların ticari faaliyetlerde internete bağımlılık oranına göre anlamlı farklılıklar gösterdiği tespit edilmiştir. Diğer taraftan siber güvenlik ihlalleri ve iş sürekliliği yönetimi firmaların ticari faaliyetlerde internete bağımlılık oranına göre anlamlı farklılık göstermektedir. Araştırmada kapsamındaki verilere göre ticari faaliyetlerinde internete bağımlılık oranı artıkça, firmaların siber güvenliğine yaklaşım düzeyleri de artmaktadır. Yani araştırma kapsamında ticari faaliyetlerinde % 75 üzeri internete bağımlı olan firmaların siber güvenlik yaklaşım düzeyleri daha yüksektir. Bu sonucun çıkması gayet doğaldır. Çünkü bilişim sistemlerine bağımlılık düzeyi arttıkça, bu sistemlere yapılan siber güvenlik yatırımları da artmaktadır. Ayrıca bağımlılığı yüksek olan firmalarda oluşabilecek herhangi bir olumsuzluğun maliyeti daha yüksek olabileceğinden bu sonuç kaynaklanıyor olabilir.

Araştırma kapsamında firmaların siber güvenliğe kurumsal yaklaşım, fiziksel ve çevresel güvenlik tedbirleri, bilişim sistemleri ve iletişim ağlarının işletim ve bakım kontrolleri ve yazılım geliştirme ve destek aşamalarında bilgi sistemleri erişim kontrolü güvenlik tedbirleri firmaların bilişim sistemlerinin 24 saat hizmet vermemesinin bir günlük satış/üretim oranlarını etkileme düzeyine göre anlamlı farklılıklar gösterdiği tespit edilmiştir. Araştırma kapsamında; bilişim sistemlerinin 24 saat hizmet vermemesi durumunda satış ve/veya üretimi % 75 ve üzeri etkilenen firmaların siber güvenliğine kurumsal yaklaşımları %25'ten az ve % 25-50 arası etkilenen firmalardan daha yüksektir. Yani bilişim sistemlerinin 24 saat hizmet vermemesi durumunda satış ve/veya üretimi daha çok etkilenen firmalar daha az etkilenen firmalara göre siber güvenlik yaklaşımları daha yüksektir. Bu sonuç doğal bir durumdur. Zira bilişim sistemlerinde yaşanan aksama firmaların faaliyetlerini olumsuz etkileniyor ise firmalar siber güvenliğe daha çok önem vermelidir. Diğer taraftan siber güvenlik ihlalleri ve iş sürekliliği firmaların bilişim sistemlerinin 24 saat hizmet vermemesinin bir günlük satış/üretim oranlarını etkileme düzeyine göre anlamlı bir farklılık göstermediği sonucuna ulaşılmıştır. Bu durum, teknoloji yoğun çalışmayan işletmelerin bilişim sistemlerinde oluşabilecek arızaları tolere edebilmeleri ve faaliyetlerinin aksamamasından kaynaklandığı düşünülmektedir.

Araştırma kapsamında siber güvenliğine kurumsal yaklaşım, bilişim sistemleri ve iletişim ağlarının işletim ve bakım kontrolleri, yazılım geliştirme ve destek aşamalarında bilgi sistemleri erişim kontrolü güvenlik tedbirleri ve genel siber güvenlik yaklaşımı, siber saldırının firma imajı üzerine olası etkilerine göre anlamlı farklılıklar gösterdiği tespit edilmiştir. Siber saldırının firma

imajı üzerine olası etkisi; firmaların geleceğini etkileyecek kadar fazla olan firmaların siber güvenlik yaklaşımı düzeylerinin diğerlerine göre daha fazla olduğu görülmüştür. Diğer bir ifade ile siber saldırının firma imajı üzerine olası etkileri dikkate alındığında; firmanın geleceğini etkileyecek kadar fazla olması durumundaki firmalar diğerlerine göre (nerdeyse olmaz, az olur ve çok olur) siber güvenliğine yaklaşım düzeyleri daha yüksektir. Yani bu firmalar siber güvenliğe daha fazla önem vermektedirler. Diğer taraftan fiziksel ve çevresel güvenlik tedbirleri ile siber güvenlik ihlalleri ve iş sürekliliği yönetimi siber saldırının firma imajı üzerine olası etkilerine göre anlamlı bir farklılık göstermediği tespit edilmiştir. Bu durum fiziksel ve çevresel güvenlik tedbirlerinin işletmenin siber varlıklarını da -firma imajı gibi- kapsar şekilde ele alınmadığından kaynaklandığı varsayılmaktadır. Öte yandan siber güvenlik ihlalleri ve iş sürekliliğinin firma imajı üzerinde olası etkilerinde anlamlı bir farkın çıkmamasını katılımcıların iş sürekliliği ve firma imajı arasında bir bağlantı kuramamaları, imaj kaybının sadece uygun fiyat ve kaliteli ürün bağlamında ele aldıklarından kaynaklandığı düşünülmektedir.

Araştırma kapsamında siber güvenliğine kurumsal yaklaşım; fiziksel ve çevresel güvenlik tedbirleri, bilişim sistemleri ve iletişim ağlarının işletim ve bakım kontrolleri, yazılım geliştirme ve destek aşamalarında bilgi sistemleri erişim kontrolü güvenlik tedbirleri, siber güvenlik ihlalleri ve iş sürekliliği yönetimi ve genel siber güvenlik yaklaşımı firmaların kritik bilgilerinin oranına göre anlamlı farklılık gösterdiği tespit edilmiştir. Yani araştırma kapsamında elde edilen verilere göre firmaların elindeki kritik bilgilerin oranına göre firmaların siber güvenlik yaklaşımları farklılık göstermektedir. Bu farklılıkların firmaların elindeki bilgilerin çoğunluğu ve yarısı kritik öneme sahip olanların firmaların elindeki bilgilerin neredeyse hiç kritik öneme sahip bilgisi bulunmayanlar ve az bilgi bulunanlar arasında olduğu görülmüştür. Kritik bilgilerinin oranı yüksek olan firmaların siber güvenlik yaklaşım düzeyleri daha yüksektir. Yani araştırma kapsamındaki firmaların bilgilerinin kritik önemi arttıkça siber güvenlik yaklaşım düzeyleri de artmaktadır.

Araştırma kapsamında firmaların siber güvenliğe kurumsal yaklaşımlarının personel değişim oranına göre oranına göre anlamlı farklılık gösterdiği tespit edilmiştir. Araştırma kapsamında siber güvenliğine kurumsal yaklaşım, personel değişim oranına göre % 10 ve altı ile % 31-50 arası personel değişimi olan firmalar arasında % 31-50 olan firmalar lehine anlamlı farklılık göstermektedir. Yani personel değişim oranına % 31-50 olan firmaların siber güvenlik yaklaşım düzeyleri daha yüksektir. Diğer siber güvenlik değişkenlerinin personel değişim oranına göre bir farklılık göstermediği tespit edilmiştir.

Sonuç olarak araştırma kapsamında firmaların fiziksel güvenliğe daha çok önem verdikleri ve yatırım yaptıkları gözlemlenmiştir. Bilgi işlem yöneticilerine fiziksel güvenliğe verilen önemin neden siber güvenliğe verilen önemden fazla olduğu sorulduğunda, yöneticilerin veya patronların tesis ve işletmeleri kontrol altında tutabilme ve "görebilme" arzularından kaynaklandığı cevabı ile karşılaşılmıştır. Diğer yandan, siber güvenliğe önem vermeye çalışan ve bu alanda yatırım yapıp riskleri kontrol edilebilir düzeyde tutmaya çalışan firmaların ise genelde siber güvenlik açıklarından dolayı özellikle mali kayıplarla karşı karşıya kalan firmalar oldukları gözlemlenmiştir. Araştırma kapsamında görüşülen bilgi işlem yöneticilerinin vurguladıkları bir diğer husus ise çeşitli nedenlerden dolayı veri kayıplarının bir bütün olarak siber güvenlik yönetimi kapsamında ele alınmadığı, firma tepe yönetimlerinin verinin korunması alanına yapılan yatırımları gereksiz bir masraf olarak gördükleri gerçeğidir. Oysaki günümüzün en değerli varlığı bilgidir ve korumak için gerekli önlemlerin alınması firmanın yaşamını devam ettirmesi bağlamında elzem ve önemlidir.

5.1.1. Araştırmacılara Öneriler

Bu çalışmada siber güvenliğe kurumsal yaklaşım; Gaziantep'teki imalat işletmeleri üzerinde incelenmiştir. Bundan sonraki çalışmalarda araştırmacılar evreni Türkiye'yi kapsayacak şekilde genelleştirilebilir ve daha büyük gruplar üzerinde yapabilir.

Yeni araştırmacılar Türkiye'deki işletmelerin siber güvenliğe kurumsal bakış açılarını ve siber güvenlik seviyelerini, farklı ülkelerle veya kültürlerle kıyaslanabilir. Böyleye kültürel farkındalık ortaya çıkarılabilir.

Bu çalışma sektörel farklılıklar dikkate alınmadan imalat işletmeleri üzerinde yapılmıştır. Gelecek araştırmacılar sektörel farklılıkları dikkate alarak işletmelerin siber güvenlik yaklaşımlarını araştırılabilirler. Farklı sektörlerde siber güvenlik yaklaşımlarının nasıl farklılaştığı tespit edilerek farklılık nedenlerini analiz edilebilir.

Gelecek çalışmalarda araştırmacılar çalışmalarına yeni değişkenler ekleyebilirler. Örneğin çevresel dinamizm, eğitim, demografik ve sosyo-kültürel özellikler yeni çalışmalarda incelenebilir. Ayrıca gelecekte araştırmacılar; siber saldırıların işletmelerdeki örgüt kültürü ve iklimine etkisi, siber güvenlik yaklaşımların işletmelerin finansal performanslarına etkisi, vb. konularda yeni çalışmalar yapabilir. Yine gelecekte araştırmacılar; siber güvenliğe kurumsal yaklaşım farkındalığının oluşturulması için alınabilecek tedbirlere yönelik çalışmalar yapabilirler.

Siber güvenlik günümüzde birçok alanın konusu haline gelmiştir. Bu bağlamda araştırmacıların siber güvenlik konusunda; teknik, ekonomik, sosyal, psikolojik ve yönetim alanında yeni araştırmalar yaparak, ülkemiz ve milletimizin her alanda olduğu gibi bu alanda da gelişmesine ve bilinçlenmesine katkı yapacak yeni çalışmalar yapılabilir.

5.1.2. İşletmelere Öneriler

Bu çalışmada elde edilen bulgular doğrultusunda işletmelere birtakım önerilerde bulunulmuştur. Çalışmada işletmelerin faaliyetlerinde bilişim ve internet sistemlerine bağımlılık oranlarının yüksek olduğu tespit edilmiştir. Bilişim ve internet sistemlerinde yaşanabilecek herhangi bir olumsuzluk, işletmelerin faaliyetlerinde aksama ve olumsuzluklara neden olur. Bu yüzden tüm işletmeler, özellikle bilişim ve internet sistemlerine bağımlılık oranların yüksek işletmelerin faaliyetlerinde olumsuzluklara maruz kalmamak için siber güvenliğe daha çok önem vermesi ve yatırım yapması gerekmektedir.

Araştırma kapsamında işletmelerin çoğunluğu, bir siber saldırı olduğunda ve kritik bilgilerinde sızıntı (ulusal sırlar, ticari sırlar, gizlilik bilgileri gibi) meydana gelirse faaliyetler üzerinde ciddi etkiler olacağını ve işletme imajlarının olumsuz etkileneceğini öngörmektedirler. Bu durum da işletmeler faaliyetlerinde sıkıntı yaşamamak ve firma imajlarının olumsuz etkilenmemesi için siber güvenliğe daha çok önem vermeleri gereğini ortaya çıkarmaktadır. Aksi takdirde firma imajlarında ve faaliyetlerinde de ciddi olumsuzluklar meydana gelebilir.

İşletmelerde personel devir hızının düşük olması siber güvenlik açısından olumlu bir durumdur. Zira işletmeden ayrılan bir personel, sahip olduğu bilgilerle güvenlik ihlallerine neden olabilmektedir. Bu nedenle firmaların personel devir hızının düşük olması, özellikle kritik noktadaki personellerin işletmede devamlılığın sağlanması için gerekli tedbirleri almasının siber güvenlik açısından önemlidir.

Bu çalışmada Gaziantep imalat sanayiinde faaliyet gösteren işletmelerin siber güvenlik yaklaşım seviyelerinin düşük olduğu tespit edilmiştir. Bunun nedeni; siber güvenliğinin öneminin farkına yeterince varılmamış olması veya farkında olsalar bile güvenlik gereklerini yeterli ölçüde yerine getirmemiş/getirememiş olmalarından kaynaklanmaktadır. Siber güvenliğe yeterince önem vermeyen firmalar her an telafisi mümkün olmayan veya çok büyük maliyetlere ve sıkıntılara neden olabilecek siber saldırılara maruz kalabilirler. Dolayısıyla işletme sahipleri/yöneticileri siber güvenliğe yönelik farkındalık çalışmalarında bulunmalıdırlar. Bu

kapsamda siber güvenliğin önemine yönelik eğitimler verilmeli, özellikle kritik noktadaki kişilerin ve sistemlerin eksiklikleri giderilmeli ve gerekli yatırımlar yapılmalıdır.

Bilginin korunması bağlamında en iyi mücadele yönetimi paydaşlara ihtiyaçları kadar ve devamlı olarak güncellenen eğitimler verilmesidir. Araştırma kapsamında görüşülen firmaların en büyük açıklarından birisi bu alanda kullanıcılara yeterli eğitimin verilmediği ve bilinçsiz kullanıcılardan kaynaklı siber güvenlik açıklarıdır. Firmalar her düzeyden çalışanlarına bu bağlamda düzenli eğitimler organize etmeli ve devamlı olarak bu eğitimleri gelişen ve değişen tehditlere karşı yenilemelidir.

KAYNAKÇA

Aaker, D. A. (2007). *Strategic market management.* Hoboken, NJ: John Wiley & Sons.

ABD Sağlık Hizmetleri. *Information memorandum.* U.S. Department Of Health And Human Services. http://www.acf.hhs.gov/sites/default/files/cb/im1504.pdf (Erişim Tarihi: 5 Ekim 2016)

Acılar, A., *İşletmelerde Bilgi Güvenliği ve Örgüt Kültürü,* , Organizasyon ve Yönetim Bilimleri Dergisi, Cilt 1, Sayı 1, 2009 sh.25-33.

Aho, J., and Nevala, J., 2016. *Keskisuomalaisten yritysten kyberturvallisuus. Jyväskylä.* Principal Regional Council of Central Finland and Jyväskylän koulutuskuntayhtymä. http://edu360.fi/wp-content/uploads/2016/08/Yrityspuolen_kybertutkimus-FINAL-20160829.pdf (Erişim Tarihi: 15 Ekim 2016)

Alagöz, A. ve Allahverdi, M., *Kurumsal Bilgi Güvenliği ve Muhasebe Bilgi Sistemi,* Muhasebe ve Vergi Uygulamaları Dergisi, 2011-3 sh.47-64.

Albrechtsena, E., and Hovdena, J. (2009). *The information security digital divide between information security managers and users.* Computers & Security Volume 28, Issue 6, September 2009, , 28(6), 476–490.

Alford, L. D. (2000). *Cyber warfare: protecting military systems.* The Journal of the Defense Acquisition University Review Quarterly, 7(2).

Alter, S., and Sherer, S. (2004). *A general, but readily adapable model of information system risk.* Communicaitons of the AIS , 14(1),1-28.

Altunışık, R., Coşkun, R., Bayraktaroğlu, S. ve Yıldırım, E. (2010) *Sosyal bilimlerde araştırma yöntemleri,* SPSS Uygulamalı, 6. Baskı, Ankara, Pegem Akademi.

Amerikan Savunma Bakanlığı. (2013). *Cyberspace operations.* DOD. http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf (Erişim Tarihi: 12 Kasım 2016)

Anderson, R. (2001). *Why information security is hard—an economic perspective.* 17th Annual Computer Security Applications Conference. New Orleans: University of Cambridge Computer Laboratory.

Arora, V. (2016). *Comparing different information security standards: COBIT v s. ISO 27001.* Carnegie Mellon University, Qatar., 7-9. https://qatar.cmu.edu/media/assets/CPUCIS2010-1.pdf (Erişim Tarihi: 12 Ekim 2016)

ASD. (2016). *Strategies to Mitigate Targeted Cyber Intrusions*. Australian Signals Directorate: http://www.asd.gov.au/publications/protect/Top_4_Mitigations.pdf (Erişim Tarihi: 25 Ekim 2016)

Aspan, M. (2011). *Citi says 360,000 accounts hacked in May cyber-attack.* Reuters http://www.reuters.com/article/2011/06/16/us-citigroup-hacking-idUSTRE75F17620110616 (Erişim Tarihi: 18 Kasım 2016)

Avnet. (2016). *Cyber attack how it works*. http://www.ts.avnet.com/uk/images/DDoS-Howitworks-4.jpg (Erişim Tarihi: 3 Aralık 2016)

Bakır, E. (2016). *5. Boyutta savaş: siber savaşlar - II*. Tubitak Bilgem: https://www.bilgiguvenligi.gov.tr/siber-savunma/5.-boyutta-savas-siber-savaslar-ii.html (Erişim Tarihi: 3 Eylül 2016)

Bakır, E. (2011). *İnternet güvenliğinin tarihçesi.* TUBİTAK Bilgem Dergisi, 3(5), 16.

Barrett, N. (2003). *Penetration testing and social engineering: Hacking the weakest link.* Information Security Technical Report, 8(4), 56-58

Baskerville, R. (1993). *Information systems security design methods: implications for information systems development.* ACM Computing Surveys, 25, 375–414.

Baykara, M., Daş, R. ve Karadoğan, İ., *Bilgi Güvenliği Sistemlerinde Kullanılan Araçların İncelenmesi,* 1 st International Symposium on Digital Forensics and Security (ISDFS'13), 20-21 May 2013, sh.231-239 Elazığ, Turkey.

Baykara, M., Daş, R., Karadoğan, İ., *Bilgi Güvenliği Sistemlerinde Kullanılan Araçların İncelenmesi,* 1 st International Symposium on Digital Forensics and Security (ISDFS'13), 20-21 May 2013, sh.231-239 Elazığ, Turkey.

Bayram, N. (2013), *Yapısal eşitlik modellemesine giriş,* Ezgi Kitabevi Yayınları, Ankara.

Baze, A. (2016). *Realistic risk management using the CIS 20 security security controls.* SANS Institute InfoSec Reading Room.

Berghel, H. (2005). *The two sides of RoI: return on investment vs. risk of incarceration.* Communications of the ACM, 48(4), 15-20.

BM Uluslararası Telekomünikasyon Birliği . (2008). *X.1205 : Overview of cybersecurity.* ITU. https://www.itu.int/rec/T-REC-X.1205-200804-I (Erişim Tarihi: 20 Ekim 2016)

Borland, J. (2013). *For tor, publicity a mixed blessing. Wired:* http://www.wired.com/2013/12/tor-publicity-mixed-blessing/ (Erişim Tarihi: 10 Ekim 2016)

Brandpowder. (2016). *How deep is your web.* Brandpowder http://www.brandpowder.com/how-deep-is-your-web/ (Erişim Tarihi: 28 Ekim 2016)

Brown, G., and Poellet, K. (2012). *The customary international law of cyberspace.* Strategic studies, 127-145. http://www.au.af.mil/au/ssq/2012/fall/brown-poellet.pdf (Erişim Tarihi: 3 Kasım 2016)

Campbell, K., Gordon, L., Loeb, M., and Zhou, L. (2003). *The economic cost of publicly announced information security breaches: empirical evidence from the stock market.* Computer Security, 11, 431–448.

Canbek, G., ve Sağıroğlu, Ş. (2006). *Bilgi, bilgi güvenliği ve süreçleri üzerine bir inceleme.* Gazi Üniversitesi Politeknik Dergisi, 9(3), 165-174.

Carr, N. (2003). *It doesn't matter.* Harvard Business Review 81 (5), 41-49.

Cavusoglu, H., Mishra, B., and Raghunathan, S. (2004). *The effect of Internet security breach announcements on market value: capital market reactions for breached firms and internet security developers.* Int. J. Electron. Commerce, 9, 69–104.

CCDCOE. (2009). *Tallinn manual on the international law applicable to cyber warfare.* Talinn: NATO Cooperative Cyber Defence Centre of Excellence.

Cherdantseva, Y., and Hilton, J. (2013). *A reference model of information assurance & security. Availability, reliability and security (ARES),* 2013 Eighth International Conference (pp. 546 - 555). Regensburg: IEEE.

Chinn, D., Kaplan, J., and Weinberg, A. (2014). *Risk and responsibility in a hyper-connected world: implications for enterprises insights and publications.* McKinsey & Company.

Coady, C. (1996). *Terörün ahlakı, cogito (şiddet).* İstanbul: Yapı Kredi Yayınları, Kış-Bahar.

COBIT. (24 Ekim 2016). *COBIT 5*. COBIT 5: http://www.isaca.org/cobit/pages/default.aspx (Erişim Tarihi: 12 Aralık 2016)

Cridland, C. (2008). *The history of the internet: the interwoven domain of enabling technologies and cultural interaction, terrorism (ed.), responses to cyber terrorism NATO Science for Piece and Security.* Ankara: IOS Press (Cilt 34).

Crist, J. (2007). *Web based attacks.* SANS Institute InfoSec Reading Room. GIAC Gold Certification.

Cropf, R. (2008). *American public administration: public service for the 21st century.* Pearson Education.

CSA. (27 Ekim 2016). *Cloud controls matrix v3.0.1 (10-6-16 update)*. CSA - Cloud Security Alliance : https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3-0-1/

Czosseck, C., Ottis, R., and Ziolkowski, K. (2012). *4th International Conference on Cyber Conflict.* 4th International Conference on Cyber Conflict . NATO CCD COE Publications.

Dağlı, A. (2015). *Örgütsel muhalefet ölçeğinin Türkçe"ye uyarlanması: geçerlilik ve güvenirlik çalışması.* Elektronik Sosyal Bilimler Dergisi, 14 (53). 198-218.

Denning, P. (1991). *Computers under attack: intruders, warms, and viruses.* USA: Addison-Wesley Publishing Company.

Desai, D. (2013). *Beyond location: Data security in the 21st century.* Communications of the ACM, 56(1), 34-36. doi:10.1145/2398356.2398368

Dhillon, G., and Backhouse, J. (2001). *Current directions in IS security research: towards socio-organizational perspectives.* Information Systems Journal, 11, 127–153.

DHS. (2016). C*ontinuous diagnostics and mitigation (CDM)*. ABD İçişleri Bakanlığı: https://www.dhs.gov/cdm (Erişim Tarihi: 18 Ekim 2016)

Dimopoulos, V., Furnell, S., Jennex, M.E., and Kritharas, I., *Approaches to IT security in small and medium enterprises.* In Proceedings of the 2nd Australian Information Security Management Conference, Securing the Future, Perth, Australia, 26 November 2004; pp. 73–82.

Dingledine, R., Mathewson, N., and Syverson, P. (2004). *Tor: the second-generation onion router.* SSYM'04 Proceedings of the 13th conference on USENIX Security Symposium, 13, pp. 21-21.

DTIC. (2012). *Objective 3.3 Lexicon & Abbreviations MNE7 Multinational Experiment 7 "Access to the Global Commons".* Defense Technical Information Center. http://www.dtic.mil/dtic/tr/fulltext/u2/a590834.pdf (Erişim Tarihi: 3 Ocak 2017)

EC Council-CEH. (2016). *Certified Ethical Hacker - InfoSec Cyber Security Certification*. International Council of E-Commerce Consultants: https://www.eccouncil.org/ (Erişim Tarihi: 24 Agustos 2016)

Efe, A. (2006). *Yeni nesil internet Protokolü'ne (IPv6) geçişle birlikte internet saldırılarının geleceğine yönelik beklentiler.* Akademik Bilişim 2006, (s. 134 Numaralı Bildiri). Denizli: Akademik Bilişim. http://ab.org.tr/ab06/bildiri/134.doc (Erişim Tarihi: 25 Ekim 2016)

Eminağaoğlu, M. (2008). *Dikkat Casus Var!* Bilgi Güvenliği Yazı Dizisi. İstanbul:Tekborsa Dergisi, p. Sayı:15.

Erbschloe, M. (2005). Trojans, worms, and spyware: a computer security professional's guide to malicious code. . Burlington,MA: Elsevier Butterworth-Heinemann.

ERIA. (2009). *Strengthening Information Security in the Business Sector (FY2009).* Jakarta: The Economic Research Institute for ASEAN and East Asia (ERIA). 2016, from

http://www.eria.org/publications/research_project_reports/strengthening-information-security-in-the-business-sector-1.html (Erişim Tarihi: 15 Ocak 2017)

FFIEC. (2016). *FFIEC Information Technology Examination Handbook.* FFIEC. http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_InformationSecurity.pdf (Erişim Tarihi: 25 Ekim 2016)

Filkins, B. (2016). *A Sans Survey. IT Security Spending Trends.* SANS Institute. www.sans.org/reading-room/whitepapers/leadership/security-spending-trends-36697. (Erişim Tarihi: 15 Agustos 2016)

Fischer, A. E. (2009). C*reating a National Framework for Cybersecurity: an Analysis of Issues and Options.* New York: Nova Sience Publisher Inc.

Gady, F.-S. (2016). *Top US Spy Chief: China Still Successful in Cyber Espionage Against US*. The Diplomat: http://thediplomat.com/2016/02/top-us-spy-chief-china-still-successful-in-cyber-espionage-against-us (Erişim Tarihi: 22 Agustos 2016)

Gehrmann, M. (2012). *Combining ITIL, COBIT and ISO/IEC 27002 for structuring comprehensive information technology for management in organizations.* Navus - Revista de Gestão e Tecnologia, 2(2), 66-77.

Goel, S., and Chen, V. (2008). *Can business process reengineering lead to security vulnerability: analyzing the reengineered process.* International Journal of Production Economics 115 (1), 104-112.

Goldman, G. (2011). *Mass e-mail breach: Just how bad is it?* CNN Money http://money.cnn.com/2011/04/06/technology/epsilon_breach/index.htm (Erişim Tarihi: 3 Aralık 2016)

Gordon, S., and Chess, D. (1999). *Attitude Adjustment: Trojans and Malware on the Internet.* Proceedings of the EICAR Conference. Aalborg, Denmark.

Gökçen, H. (2002). *Yönetim Bilgi Sistemleri.* Ankara: Epi Yayıncılık.

Gökçen, H. (2007). *Yönetim Bilgi Sistemleri.* Ankara: Palme Yayıncılık.

Güngör, M. (2015). *Ulusal Bilgi Güvenliği: Strateji Ve Kurumsal Yapılanma,* Uzmanlık Tezi. Ankara: TC. Kalkınma Bakanlığı, Bilgi Toplumu Dairesi Başkanlığı.

Gürbüz, S. ve Şahin, F. (2016). *Sosyal Bilimlerde Araştırma Yöntemleri: Felsefe-Yöntem-Analiz,* 3. Baskı, Ankara: Seçkin Yayıncılık.

Gürkaynak, M., ve İren, A. A. (2011). *Reel Dünyada Sanal Açmaz: Siber Alanda Uluslararası İlişkiler.* Süleyman Demirel Üniversitesi İktisadi Ve İdari Bilimler Fakültesi Dergisi, 16, 263-279.

Hagen, J. M., Albrechtsen, E., and Hovden, J. (2008). Implementation and effectiveness of organizational information security measures. *Information Management & Computer Security, 16*(4), 377-397.

Hanaylı, M. (2014). *Linux Tabanlı Ftp Sunucularda Veri Transferinde Algoritmalar Yardımıyla Güvenli Erişim Yönetimi Uygulaması.* Dumlupınar Üniversitesi, Fen Bilimleri Enstitüsü Matematik Anabilim Dalında Yüksek Lisans Tezi.

Hansen, L., and Nissenbaum, H. (2009). *Digital Disaster, Cyber Security, and the Copenhagen School.* International Studies Quarterly, 53, 1155-1175.

Hassinen, T., (2017) *Enhancing Cyber Security for SME organizations through self-assess-ments How self-assessment raises awareness* Master's Thesis April 2017 School of Technology Master´s Degree Programme in Information Technology Cyber Security

Hemphill, A. T., and Longstreet, P. (2016). *Financial data breaches in the U.S. retail economy: Restoring confidence in information technology security standards.* Technology in Society, 44, 30-38.

Herrmann, D. S. (2007). *Complete Guide To Security and Privacy Metrics Measuring Regulatory Compliance,Operational Resilience, and ROI.* New York: Auerbach Publications.

Hildreth, S. (2001). *Cyberwarfare Congressional Research Service Report for Congress.* DC: Congressional Research Service & The Library.

Hoffer, J. A., and Straub, D. W. (1989). *The 9 to 5 underground: Are you policing computer crimes.* Sloan Management Review, 30(4), 35–43.

Huang, C., Farn, K., and Lin, F., (2011). *A Study on Information Security Management with Personal Data Protection*. 2011 IEEE 17th International Conference on Parallel and Distributed Systems (pp. 624-630). IEEE Computer Society.

Hutcheson, G. and Sofroniou, N. (1999) *The Multivariate Social Scientist: Introductory Statistics Using Generalized Linear Models.* Sage Publication, Thousand Oaks, CA.

IAD. (2016). *Manageable Network Plan Guide (version 4.0)*. Information Assurance: https://www.iad.gov/iad/customcf/openAttachment.cfm?FilePath=/iad/library/ia-guidance/security-configuration/networks/assets/public/upload/manageable-network-plan-guide.pdf&WpKes=aF6woL7fQp3dJiQy4zLnU2u8sNVpdxKAnjUjkp (Erişim Tarihi: 25 Ekim 2016)

Intoccia, G., and Moore, W. J. (2006). *Communications Technology, Warfare, and the Law: Is the Network a Weapon System.* Houston Journal of International Law, 28, 467-489.

IPA. (2016). *Information Technology Promotion Agency*. IPA: http://www.ipa.go.jp/security/english/benchmark_system.html (Erişim Tarihi: 20 Ekim 2016)

Ipsos Mori. (2016). *Cyber Security Breaches Survey 2016 Main Report.* London: Ipsos MORI's Social Research Institute. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/521465/Cyber_Security_Breaches_Survey_2016_main_report_FINAL.pdf (Erişim Tarihi: 5 Ekim 2016)

ISACA. (2015). *CISM Review Manual,* 14th Edition. ISACA.

ISACA. (2016). *COBIT Global Regulatory and Legislative Recognition*. ISACA: http://www.isaca.org/COBIT/Pages/Recognition.aspx (Erişim Tarihi: 23 Ekim 2016)

Ismail, R., and Zainab, A. (2011). *Information systems security in special and public libraries: an assessment of status.* Malaysian Journal of Library & Information Science, 16(2), 45-62.

ISO. (2015). *ISO Survey 2015.* ISO.ORG. http://www.iso.org/iso/home/standards/certification/iso-survey.htm?certificate=ISO%209001&countrycode=AF (Erişim Tarihi: 20 Ekim 2016)

ISO/IEC 27002. (2016). *ISO/IEC 27002 Information technology -- Security techniques -- Code of practice for information security controls*. ISO.ORG: http://www.iso.org/iso/catalogue_detail?csnumber=54533 (Erişim Tarihi: 25 Ekim 2016)

ITIL. (2016). *What is ITIL? Best Practice?* Axelos: https://www.axelos.com/best-practice-solutions/itil/what-is-itil (Erişim Tarihi: 27 Ekim 2016)

ITU. (2015). *ITU Facts and Figures.* ITU Telecommunication Development Bureau. http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf (Erişim Tarihi: 25 Ekim 2016)

Jang-Jaccard, J., and Nepal, S. (2014). *A survey of emerging threats in cyber security.* Journal of Computer and System Sciences, 80, 973–993.

Kalaycı, Ş. (2008). *SPSS uygulamalı çok değişkenli istatistik teknikler.* 3.Baskı, Ankara: Asil Yayın Dağıtım.

Kanno, Y. (2005). *Information Security Measures Benchmark (ISM-Benchmark).* Tokyo: Information-technology Promotion Agency (IPA) Japan. https://www.ipa.go.jp/files/000011796.pdf (Erişim Tarihi: 15 Haziran 2016)

Kara, M. (2013). *Siber Saldirilar - Siber Savaşlar Ve Etkileri.* İstanbul: Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi, Sosyal Bilimler Enstitüsü, Bilişim ve Teknoloji Hukuku Yüksek Lisans Programı.

Karasar, N. (2008). *Bilimsel Araştırma Yöntemi.* Ankara: Nobel yayın Dağıtım.

Karri, R., Rosenfeld, K., Rajendran, J., and Tehranipoor, M. (2010). *Trustworthy Hardware: Identifying and Classifying Hardware Trojans.* IEEE Computer, 43, 39-46.

Karunaratne, J. (2016). *The Passive Splice Network Tap*. Janitha: http://www.janitha.com/articles/passive-splice-network-tap/ (Erişim Tarihi: 5 Ekim 2016)

Kauppinen, T., and Kivikoski, J. (2016) *Tutkimus suomalasten PK-yritysten digitaalisuudesta ja tietoturvasta.* Helsinki. Principal Elisa Oyj and Yrittäjäsanomat. http://hub.elisa.fi/download/9327/ (Erişim Tarihi: 10 Ekim 2016)

Keskin, F. (1998). *Uluslararası Hukukta Kuvvet Kullanma: Savaş, Karışma ve Birleşmiş Milletler.* Ankara: Öteki Matbaası.

Klimburg, A. (2012). *National Cyber Security Framework Manual.* NATO CCD COE Publications.

KOSGEB, (2016). *KOBİ Tanımı Değişti,* KOSGEB, http://www.kobi.org.tr/index.php?option=com_content&view=article&id=239:kob-tanm-deiti&itemid=348 (Erişim Tarihi: 17 Mayıs 2016)

Kong, F., and Li, M. (2013). *Hardware Attacks. In A. Miri,* Advanced Security and Privacy for RFID Technologies (pp. 33-44). Hershey,PA: IGI Global.

Konrad, A. (2013). *Feds Say They've Arrested 'Dread Pirate Roberts,'Shut Down His Black Market' The Silk Road.* Forbes 2013,7.

Krutz, R. L., and Vines, R. D. (2007). *The CEH Prep Guide: The Comprehensive Guide to Certified Ethical Hacking.* Indianapolis, IN: Wiley Publising Inc.

Kudat, B. (2007). *Kötü adamların hızına yetişen daha güvenli.* BThaber, 6004:15.

Küçüksille, E. U., Yalçınkaya, M. A., ve Uçar, O. (2014). *Siber Saldırılarda İstismar Kitlerinin Kullanımı Üzerine Bir Analiz ve Savunma Önerileri.* 7. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı. İstanbul: ISC Turkey.

Lachow, I. (2013). *Active Cyber Defense A Framework for Policymakers.* Center for a New American Security.

Li, Q. (2007). *Bullying in the new playground: Research into cyberbullying and cyber victimisation.* Australasian Journal of Educational Technology, 23(4), 435-454.

Li, Q., Gao, H., Xu, B., and Jiao, Z. (2008). *Hardware Threat: the Challenge of Information Security.* International Symposium on Computer Science and Computational Technology. IEEE Computer Society.

Liu, S., and Cheng, B. (2009). *Cyberattacks: Why, What, Who, and How.* IT Professional Magazine, 11(3), 14-21.

Loeb, L. (2002). *Information Assurance Powwow Part 1.* IEEE Systems, Man, and Cybernetics Information Assurance Workshop. IEEE.http://www.ibm.com/developerworks/security/library/s-confnotes2/ (Erişim Tarihi:5 Aralık 2016)

Malhotra, N. K. (2004) *Marketing research: an applied orientation, 4th edition,* Prentice-Hall International, London.

Marinos, L., Belmonte, A., and Rekleitis, E. (2016). *ENISA Threat Landscape 2015.* European Union Agency For Network And Information Security.

Maskun, A., Manuputty, A., Noor, S., and Sumardi, J. (2013). *Cyber Security: Rule of Use Internet Safely.* Socail and Behavioral Sciences 103, 255-261.

McCumber, J. (1991). *Information systems security: A comprehensive model.* Proceedings 14th National Computer Security Conference. Baltimore: National Institude of Standarts and Technology.

McHugh, J., Christie, A., and Allen, J. (2000). *Defending Yourself: The Role of Intrusion Detection Systems.* IEEE Software, 17(5), 42-51.

McMaster Universitesi. (2016). *IP (Internet Protocol) Spoofing*. McMaster University-Computer and Software Engineering:http://wiki.cas.mcmaster.ca/index.php/IP_Spoofing (Erişim Tarihi: 25 Agustos 2016)

Meray, S. L. (1962). *Devletler Hukukuna Giriş.* Ankara Üniversitesi Siyasal Bilgiler Fakültesi Yayınları.

Meydan, C. H. ve Şeşen, H. (2015) *Yapısal Eşitlik Modellemesi AMOS Uygulamaları*, Seçkin Yayınevi, Ankara.

Mil, H. İ.,(2015) *Sosyal Güvenlik Kurumundaki Siber Güvenlik Yönetimi Uygulamalarının İncelenmesi ve Değerlendirilmesi,* Dicle Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, Nisan 2015 YIL-7 S.13 sh.398-416.

Mirdas, A. (2016). *Terör Nedir Ne Dğildir*. Akademik Perspektif: http://akademikperspektif.com/2013/11/28/teror-nedir-ne-degildir/ (Erişim Tarihi: 26 Agustos 2016)

Mitnick, K. D., and Simon, W. L. (2003). *The art of deception: controlling the human element of security.* Indianapolis,Indiana: Wiley & Sons.

NC State University. (2016). *IT Security*. NC State University, Office of Information Technology: https://oit.ncsu.edu/it-security/safe-computing/spyware/ (Erişim Tarihi: 2 Eylül 2016)

NCSL. (2016). *Security Breach Notification Laws*. National Conferance of State Legistratures: http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (Erişim Tarihi: 5 Ekim 2016)

NERC. (2016). *Critical Infrastructure Protection Standards*. The North American Electric Reliability Corporation: http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx (Erişim Tarihi: 27 Ekim 2016)

New Scientist Magazine. (2016). *New Scientist Magazine, Issue 2844 "Dot-dash-diss: The gentleman hacker's 1903 lulz"*. New Scientist Magazine. Issue 2844: http://www.newscientist.com/article/mg21228440.700-dotdashdiss-thegentleman-hackers-1903-lulz.html (Erişim Tarihi: 10 Temmuz 2016)

NIST. (2010). *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII).* Computer Security Division. Gaithersburg, MD: National Institute of Standards and Technology (NIST). http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf (Erişim Tarihi: 11 Ekim 2016)

NIST. (2016). *Cybersecurity Framework.* National Institute of Standards and Technology. https://www.nist.gov/programs-projects/cybersecurity-framework (Erişim Tarihi: 25 Agustos 2016)

Nickolov, E. (2008). *Modern trends in the cyber attacks against the critical information infrastructure.* Regional Cybersecurity Forum, 7-9.

Nissenbaum, H. (2005). Where Computer Security Meets National Security. *Ethics and Information Technology, 2*, 61-73.

Okoye, S.,(2017) *Strategies to Minimize the Effects of Information Security Threats on Business Performance,* College of Management and Technology, Walden University, Doctoral Study 2017

Ottekin, F. (2016). *Bilgi Güvenliğinde ISO 27000 Standartlarının Yeri ve Öncelikli ISO 27002 Kontrolleri*. Bilgi Güvenliği: https://www.bilgiguvenligi.gov.tr/bt-guv.-standartlari/bilgi-guvenliginde-iso-27000-standartlarinin-yeri-ve-oncelikli-iso-27002-kontrolleri.html (Erişim Tarihi: 21 Ekim 2016)

Öcüt, A. (2016). *Mail ile Gelen TTNET Faturalarına Dikkat Ediniz*. Adem Öcüt Kişisel Blog: http://ademocut.com/mail-ile-gelen-ttnet-faturalarina-dikkat-ediniz/ (Erişim Tarihi: 10 Aralık 2016)

Öğüt, A. (2003). *Bilgi Çağında Yönetim* (2. Baskı). Ankara: Nobel Yayın Dağıtım.

Özdamar, K., Odabaşı, Y., Hoşcan, Y., Kırcaali-İftar, G., Özmen, A., ve Uzuner, Y. (1999). *Sosyal Bilimlerde Araştırma Yöntemleri, (Edt.Ali Atıf Bir).* Eskişehir: Anadolu Üniversitesi Açıköğretim Fak.Yay.

Panko, R. (2009). *Business computer and network security.* Englewood Cliffs, NJ: Prentice-Hall.

Parker, D. (2010). *Our Excessively Simplistic Information Security Model and How to Fix It.* ISSA Journal, 12-21.

Patchin, J., and Hinduja, S. (2006). *Bullies move beyond the schoolyard: A preliminary look at cyberbullying.* Youth Violence and Juvenile Justice, 4, 148-169.

PCI SSC. (2016). *Requirements and Security Assessment Procedures*. PCI Security Standards Council: https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss (Erişim Tarihi: 29 Ekim 2016)

Persadha, P., Waskita, A., and Yazid, S. (2016). *Comparative Study of Cyber Security Policies among Malaysia, Australia, Indonesia: A Responsibility Perspective.* Proceedings - 4th

International Conference on Cyber Security, Cyber Warfare, and Digital Forensics, CyberSec 2015 (pp. 146-150). Jakarta: IEEE.

Ponemo Institute Research. (2015). *2015 Cost of data breach study: Global Analysis.* Ponemo Institute L.L.C.

Popular Sience. (1970). Popular Sience Popular Sience http://www.popsci.com/archive-viewer?id=8QAAAAAAMBAJ&pg=66 (Erişim Tarihi: 3 Ekim 2016)

Post, J. V. (1979). *Cybernetic War, The Omni Book of Computers & Robots.* Zebra Books.

PwC. (2016). *The Global State of Information Security Survey 2016.* PwC. Agustos 12, 2016, http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/data-explorer.html

Radikal Gazetesi. (2016). *Radikal Ekonomi*. Radikal Gazetesi Web Sitesi: http://www.radikal.com.tr/haber.php?haberno=240161 (Erişim Tarihi: 28 Eylül 2016)

Rıfat, İ. R., ve Zerenler, M. (2008). T*urizm İşletmelerinde Yönetim Bilişim Sistemleri Kullanımının Yönetsel Kararlar Üzerindeki Etkisi.* S.Ü Sosyal Ve Ekonomik Araştırmalar Dergisi(1(15)), 375-391.

Richardson, R. (2008). *2008 CSI/FBI Computer Crime & Security Survey.* CSI.

Richardson, R. (2011). *2011 CSI Computer Crime and Security Survey.* Computer Security Institute.

Richardson, R. (2011). *CSI Computer Crime and Security Survey.* Computer Security Institute.

Rid, T. (2012). *Cyber War Will Not Take Place.* Journal of Strategic Studies, 35(1).

Ridley, G., Young, J., and Carroll, P. (2004). *COBIT and its utilization: a framework from the literature.* System Sciences,Proceedings of the 37th Annual Hawaii International Conference (p. 8). IEEE.

Risk Based Security. (2015). *2015 Reported Data Breaches Surpasses All Previous Years.* Risk Based Security. https://www.riskbasedsecurity.com/2016/02/2015-reported-data-breaches-surpasses-all-previous-years/ (Erişim Tarihi: 13 Kasım 2016)

Rogin, J. (2012). *NSA Chief: Cybercrime constitutes the "greatest transfer of wealth in history"*. Foreign Policy: http://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/ (Erişim Tarihi: 9 Kasım 2016)

Salem, M. B., Shlomo, H. S., and Stolfo, S. J. (2008). *A Survey of Insider Attack Detection Research.* Insider Attack and Cyber Security, 39, 69-90.

Saltzer, J., and Schroeder, M. (1975). T*he protection of information in computer systems.* Proceedings of the IEEE. 63(9), pp. 1278-1308. IEEE.

Schmid, A. P. (1993). *The Response Problem As a Definition Problem, Western Responses to Terrorism.* England: Frank Cass & Co. Ltd.

Schneier, B. (2008). *Schneier on Security.* USA: John Wiley & Sons Inc.

Scott. (2016). *Why HTTPS and SSL are not as secure as you think*. Scott.Net: https://www.sott.net/article/275524-Why-HTTPS-and-SSL-are-not-as-secure-as-you-think (Erişim Tarihi: 13 Ekim 2016)

Segev, A., Porra, J., and Roldan, M. (1998). *Internet security and the case of Bank of America.* Communications of the ACM, 41, 81–87.

Shahriar, H., and Zulkernine, M. (2012). *Mitigating program security vulnerabilities: Approaches and challenges,* ACM Computer Survey., 44(3).

Sisaneci, İ., Akin, O., Karaman, M., and Saglam, M. (2013). *A Novel Concept For Cybersecurity: Institutional Cybersecurity.* 6th International Conference on Information Security and Cryptology, 89.

Solms, B. (2005). *Information Security governance: COBIT or ISO 17799 or both?* Computers and Security, 24, 99-104.

Solms, V., and Niekerk, V. (2013). *From Information security to Cyber Security.* Computers & Security 38, 97-102.

Srikantaswamy, S., and Phaneendra, H. (2012). *Improved Caesar Cipher with Random Number Generation Technique and Multistage Encryption.* International Journal on Cryptography and Information Security (IJCIS), 2(4), 39-49.

SSL Shop. (2016). *Eavesdropping Attack: A Dark Shadow on the Network.* SSL Shop: https://www.cheapsslshop.com/blog/eavesdropping-attack-a-dark-shadow-on-the-network (Erişim Tarihi: 25 Ağustos 2016)

Stallings, W. (2006). *Cryptography and network security: principles and practices.* Pearson Education.

Stop-Think-Connect. (2016). *Back Up Poster*. Stop-Think-Connect: https://www.stopthinkconnect.org/resources/preview/back-up-poster (Erişim Tarihi: 19 Ekim 2016)

Straub, D., and Welke, R. (1998). *Coping with systems risks: security planning models for management decision making.* MIS Quarterly, 22, 441–469.

Sundt, C. (2006). *Information security and the law.* Information Security Technical Report, 11(1), 2-9.

Şahinaslan, E., Kantürk, A., Şahinaslan, Ö., ve Borandağ, E., *Kurumlarda Bilgi Güvenliği Farkındalığı, Önemi ve Oluşturma Yöntemleri,* Akademik Bilişim'09 - XI. Akademik Bilişim Konferansı Bildirileri 11-13 Şubat 2009 sh.597-602 Harran Üniversitesi, Şanlıurfa

Şentürk, H., Çil, C. Z., and Sağıroğlu, Ş. (2012). *Cyber Security Analysis of Turkey.* International Journal of Information Security Science, 1(4), 112-125.

T.C Ulaştırma Bakanlığı. (2016). *2016-2019 Ulusal Siber Güvenlik Stratejisi.* Ankara: T.C Ulaştırma Denizcilik ve Haberleşme Bakanlığı.

Tarcan, M., Gul, Y., Gul, F., and Tarcan, G. (2010). *The Exchange Ratio In The Dimensions Of Integrity, Confidentiality And Availablity Of Information Security In The Teaching And General Hospitals: Case Study Of Ministry Of Health Hospitals Of Turkey.* Northeast Decision Siences Institute Proceedings, (p. 610).

Tekin, M., Güles, H., ve T., B. (2000). *Dünyadaki Teknoloji Yönetimi Bilişim Teknolojileri.* Konya: Damla Ofset.

Thomson, K. L., and Solms, R. V. (2005). *Information security obedience:a definition.* Computers & Security, 24, 69-75.

Tipton, H., and Krause, M. (2007). *Information Security Management Handbook.* Auerbach Publicaions.

Tomlin M., (2015) *Advancing Small Business Cyber Maturity: An application of the NIST Cybersecurity Framework.* Master's thesis, Royal Holloway, University of London, 2015.

TS ISO/IEC 27001:2013. (2016). *Bilgi Güvenliği Yönetim Sistemi Standardı.*

Tsukayama, H. (2011) *Cyber attack was large-scale, Sony says.* Washington Post https://www.washingtonpost.com/blogs/faster-forward/post/cyber-attack-waslarge-scale-sony-says/2011/05/04/AF78yDpF_blog.html (Erişim Tarihi: 25 Ocak 2017)

Türk Ansiklopedisi. (1958). *Türk Ansiklopedisi, Cilt 9.* Ankara: Maarif Basımevi.

Türk Dil Kurumu. (2017). *Güncel Türkçe Sözlük* http://www.tdk.gov.tr/index.php?option=com_gts&view=gts (Erişim Tarihi: 17 Mayıs 2016)

UDHB (2016). *Siber Güvenlik*. Ulaştırma Denizcilik ve Haberleşme Bakanlığı: http://www.udhb.gov.tr/h-12-siberguvenlik.html (Erişim Tarihi: 27 Ekim 2016)

UK Cyber Essentials. (2014). *Cyber Essentials Scheme.* GOV.UK. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/317481/Cyber_Essentials_Requirements.pdf (Erişim Tarihi: 18 Ekim 2016)

UK ICO. (2016). *Data protection self assessment toolkit*. ICO: https://ico.org.uk/for-organisations/improve-your-practices/data-protection-self-assessment-toolkit/ (Erişim Tarihi: 15 Eylül 2016)

UK-NCSC. (2016). *10 Steps: Summary*. UK National Cyber Security Centre: https://www.ncsc.gov.uk/guidance/10-steps-executive-summary (Erişim Tarihi: 5 Eylül 2016)

Ünver, M., Canbay, C., ve Mirzaoğlu, A. (2011). *Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler.* Ankara: Bilgi Teknolojileri ve İletişim Kurumu.

Vacca, R. J. (2006). *Guide to Wireless Network Security.* Pomeroy, OH: Springer Science & Business Media LLC.

Valenzuela, I. (2016). *Game Changer: Identifying and Defending Against Data Exfiltration Attempts.* SANS Cyber Defense Summit. Nashville, TN: SANS. https://files.sans.org/summit/Cyber_Defense_Summit_2015/PDFs/Identifying-and-Defending-Against-Data-Exfiltration-Attempts-Ismael-Valenzuela-Foundstone.pdf (Erişim Tarihi: 3 Eylül 2016)

Valli, C., Martinus, I., ve Johnstone, M. (2014). *Small to medium enterprise cyber security awareness: An initial survey of Western Australian business.* In Proceedings of the International Conference on Security and Management (SAM) (p. 1). The Steering Committee of the World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp). http://worldcomp-proceedings.com/proc/p2014/SAM9779.pdf (Erişim Tarihi: 10 Ağustos 2016)

Vardal, N. (2009). *Yükseköğretimde Bilgi Güvenliği: Bilgi Güvenlik Yönetim Sistemi İçin Bir Model Önerisi Ve Uygulaması.* (Yayımlanmış doktora tezi). Ankara: Gazi Üniversitesi/Eğitim Bilimleri Enstitüsü.

Verizon. (2016). *Verizon's 2016 Data Breach Investigations Report.* Verizon. http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf (Erişim Tarihi: 2 Aralık 2016)

Von Solms, B. (2000). *Information security – the third wave?* Computers & Security, 19(7), 615-620.

Vorakulpipat, C., Siwamogsatham, S., and Pibulyarojana, K. (2010). *Exploring Information Security Practices in Thailand Using ISM-Benchmark*. Technology Management for Global Economic Growth (PICMET), 2010 Proceedings of PICMET '10 (pp. 1-4). Phuket: IEEE.

Vural, Y. ve Sağıroğlu, Ş. (2011). *Kurumsal Bilgi Güvenliğinde Güvenlik Testleri ve Öneriler,* Gazi Üniv. Müh. Mim. Fak. Der. Cilt 26, No 1, 89-103, 2011

Vural, Y., ve Sağıroğlu, Ş. (2008). *Kurumsal Bilgi Güvenliği ve Standartları üzrine bir inceleme.* Gazi Üniversitesi Müh, Mimarlık Fakültesi Dergisi Cilt 23, No 2, 507-522.

Ware, H. (1979). *Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security - RAND Report R-609-1.* Santa Monica: The Rand Corporation. http://www.rand.org/pubs/reports/R609-1/index2.html (Erişim Tarihi: 15 Ekim 2016)

Wei, O. K. (2016). *Reality: Security and Spending Are Unbalanced*. IBM Software Group: http://www-07.ibm.com/sg/smarterbusiness/meettheexperts/includes/downloads/Securing_Your_Web_0910_eve.pdf (Erişim Tarihi: 29 Ekim 2016)

Weimann, G. (2006). *Terror On The Internet: The New Arena The New Challenges,* . Washington D.C.: United States Institue Of Peace.

Whitman, M. (2003). *Enemy at the gate: threats to information security.* Communications of the ACM, 46(8), 91-95.

Whitman, M., and Mattord, H. (2012). *Principles of Information Security, 4th ed.* Cengage Learning.

Winther, R., Gran, B. A., and Dahll, G. (2005). *Computer Safety, Reliability, and Security.* 24th International Conference SAFECOMP 2005, (p. 371). Fredrikstad, Norway.

Wolf, J., and Maclean, W. (2011). IMF cyber attack aimed to steal insider information: Expert. Reuters http://www.reuters.com/article/2011/06/12/us-imfcyberattack-idUSTRE75A20720110612 (Erişim Tarihi: 19 Kasım 2016)

Wood, C. C. (2005). *Information Security Policies Made Easy.* Houston,TX: Information Shield.

Yaşar, H., ve Çakır, H. (2015). *Kurumsal Siber Güvenliğe Yönelik Tehditler ve Önlemleri.* Düzce Üniversitesi Bilim ve Teknoloji Dergisi, 3, 488-507.

Yavanoğlu, U., Sağıroğlu, Ş., ve Çolak, İ., *Sosyal Ağlarda Bilgi Güvenliği Tehditleri ve Alınması Gereken Önlemler,* Politeknik Dergisi, Cilt:15 Sayı: 1 s. 15-27, 2012.

Yayla, A., and Hu, Q. (2011). *The impact of information security events on the stock value of firms: The effect of contingency factors.* Journal of Information Technology, 26, 60-77.

Yazıcıoğlu, Y. ve Erdoğan, S. (2004). *SPSS Uygulamalı Bilimsel Araştırma Yöntemleri.* Ankara: Detay Yayıncılık.

Yeh, Q.J., and Chang, A. J. (2007). *Threats and Countermeasures for Information System Security: A Cross-Industry Study.* Information & Management, 44(5), 480-491.

Yeşilyurt, H.(2015) *Finansal Hizmet Sektöründe Siber Güvenlik Riskleri Ve Çözüm Yolları: Ödeme Sistemleri ve Tedarik Zinciri Bütünlüğü,* CBÜ Sosyal Bilimler Dergisi, Cilt:13, Sayı:2, Haziran 2015 sh.97-120.

Yılmaz, E., Ulus, H.İ., ve Gönen, S., *Bilgi Toplumuna Geçiş ve Siber Güvenlik,* Bilişim Teknolojileri Dergisi, Cilt: 8, Sayı: 3, Eylül 2015 s. 133-146.

Zhang, H., Han, W., Lai, X., Lin, D., Ma, J., and Li, J. (2015). *Survey on cyberspace security.* Science China, Information Sciences, 58, 110101:1–110101:43.

Zikmund, W. G. (2002). *Business Research Methods.* Nashville, TN: South-Western College Pub.

EKLER

EK-1 UDHB Kurumlar Tarafından Alınması Gereken Siber Önlemler

8904159 / 19.08.2016

HİZMETE ÖZEL

T.C.

ULAŞTIRMA DENİZCİLİK VE HABERLEŞME BAKANLIĞI

Haberleşme Genel Müdürlüğü

11 Ağustos 2016

Sayı : 65512645-265.99/57837

Konu : Kurumlar Tarafından Alınması Gereken Siber Güvenlik Tedbirleri

MİLLİ EĞİTİM BAKANLIĞINA

Bilindiği üzere 2012/3842 sayılı Bakanlar Kurulu Kararı ve 5809 sayılı Elektronik Haberleşme Kanunu ile "Ulusal Siber Güvenliğin sağlanması için politika, strateji ve eylem planlarını hazırlamak" görevi Bakanlığımıza verilmiş olup bu hususta çalışmalarımız devam etmektedir.

Bilgi ve iletişim teknolojilerinin hızla gelişmekte olduğu, bu gelişmeler doğrultusunda risklerin ve tehditlerin günden güne çeşitlenerek arttığı, artan risk ve tehditlerin Siber Güvenliğe, dolayısıyla da Ülke güvenliğine ciddi tehditler oluşturduğu gözlemlenmektedir.

Gelişen bahse konu teknolojiler, edinilen tecrübeler ve Ülkemizde yaşanan gelişmeler sonucu Kurumlarda Siber Güvenlik ile ilgili tedbirlerin almarak ivedilikle uygulanması amacıyla ve 10 Şubat 2016 tarihli Siber Güvenlik Kurulu Kararı gereğince, Kurumlar tarafından alınması gereken Siber Güvenlik tedbirleri paketi hazırlanmış olup Ek'te gönderilmektedir.

Bahse konu tedbirlerin Kurumunuz ile Kurumunuzun bağlı, ilgili ve ilişkili kuruluşlarında, gerek sistem gerekse personel düzeyinde farkındalığın artırılması amacıyla uygulanması hususunda bilgilerinizi ve gereğini arz ve rica ederim.

Dr. Özkan POYRAZ
Bakan a.
Müsteşar V.

EK:
1. Dağıtım Listesi (3 sayfa)
2. Kurumlar Tarafından Alınması Gereken Tedbirler (Hizmete Özel – 3 sayfa)

Hakkı Turayliç Caddesi No 5 06338 Emek / Çankaya / ANKARA
Telefon: (0 312) 203 1787
E-posta: [redacted]
Faks: (0 312) 203 1885
İnternet Adresi: www.udhb.gov.tr
Ayrıntılı bilgi alınacak kişi:
Ünver DİKİCİ
Ulaştırma ve Haberleşme Uzman Yardımcısı

T.C.
Ulaştırma Denizcilik ve
Haberleşme Bakanlığı

HİZMETE ÖZEL

EK

KURUMLAR TARAFINDAN ALINMASI GEREKEN TEDBİRLER

1. Bilişim sistemlerine erişimlerde; bilişim hizmeti satın alınan firma personelinin ve kurum çalışanlarının yetkilendirilmesi ve emeklilik, istifa, işten çıkarılma, açığa alınma gibi nedenler ile ücretsiz izin, askerlik, doğum izni gibi uzun süreli işe ara vermelerde gerek firma personelinin gerekse kurum çalışanlarının sisteme erişim yetkilerinin -**gecikme olmaksızın**- dondurulması veya kaldırılması süreçleri net bir şekilde belirlenip uygulamaya konularak bu doğrultuda yetkisiz erişimlerin önüne geçilmesi,
2. Bilişim sistemlerinin kurulması veya işletilmesi nedeniyle bilişim sistemlerine ve bu sistemlerde bulunan verilere ilişkin bilgilere sahip olan bilişim hizmeti alınan firmalarla gizlilik sözleşmesi imzalanması, imzalanan gizlilik sözleşmelerinin içerik olarak yeterli güvenceyi sağlayacak doğrultuda yapılması,
3. Kurumsal ŞOME Kurulum ve Yönetim Rehberi'nde de belirtildiği üzere, bilgi sistemlerinin kurulması ve işletilmesi amacıyla hizmet satın alınan özel ticari işletmelerde çalışan firma personeline ilişkin güvenlik araştırmaları yapılması, kurum ve firma personeli ile bilgi sistemleri ve buradaki verilere ilişkin edindikleri bilgilerin gizliliğini koruyacaklarını ve korumamaları durumundaki yükümlülüklerini belirten bir gizlilik sözleşmesinin de imzalanması,
4. Güçlü parola oluşturulması, parolaların belli periyotlarla değiştirilmesi, parolaların gizliliğine ilişkin personelin yükümlülükleri gibi hususları içeren yazılı parola politikasının kurumda oluşturulması; kurumda bahse konu yazılı politikanın uygulamaya geçirilmesi ve oluşturulan parola politikasının personele duyurulması,
5. İki haneli veya 1111, 0000, 1234 gibi kolayca tahmin edilebilir parolalar ile ilk kez verilen parolaların değiştirilmeden kullanılması, parolanın e-posta ile iletilmesi, diğer personelle sıklıkla paylaşılması gibi bilgi güvenliği açısından önemli risk oluşturabilecek uygulamaların önlenmesi,
6. Kurumlarda farklı sistem veya uygulamalar için birbirinden bağımsız yetkilendirme mekanizmaları oluşturulmasından doğacak sorunların aşılabilmesi için merkezi kimlik yönetim/yetkilendirme sistemlerinin devreye sokulması; bu amaçla alınan yazılımların alındığı tüm sistemlere entegre edilebilecek yapıda olması (lisans kısıtlaması, teknik özelliklerinin kısıtlılığı vb. engeller teşkil etmeyen nitelikte olması),

EK

7. Bilgi sistemlerinde kullanılan yazılımlarda ortaya çıkan hata ve açıklıkların giderilmesi amacıyla düzenli olarak yayımlanan yama programları için yama yönetimi süreçlerini açık şekilde tanımlayan **yazılı yama yönetimi politikası** oluşturularak sürecin politikaya uygun şekilde işletilmesi; yama yönetim süreçlerinin tüm sistemleri kapsaması, kişilere bağlı ve bağımlı olmaksızın yürütülmesi,
8. Kullanım dışı kalan veya mülkiyeti devredilen, üzerine kişisel veri kaydedilmiş elektronik kayıt ortamlarının güvenli imhası ile ilgili yazılı politikanın oluşturulması, personelin politika konusunda farkındalığının da oluşturularak politikanın uygulanması,
9. Ulusal Siber Olaylara Müdahale Merkezi (USOM) tarafından gönderilen, yayınlanan ve duyurulan "Siber Güvenlik bildirimlerinin" kurumsal kullanıcılara ve sistem yöneticilerine iletilmesi ve gereğinin yapılmasının sağlanması,
10. USOM tarafından güncel biçimde sunulan "Zararlı Bağlantıların" kurumsal güvenlik cihazlarına kural olarak eklenmesi,
11. Güncel gelişmelerden hareketle önemi ortaya çıktığı üzere ve-iletişim eksikliğinden doğan problemlerin tekrar yaşanmaması adına, güncel değilse SOME personeli iletişim bilgilerinin güncellenerek USOM'a bildirilmesi,
12. Kurumsal SOME Kurulum ve Yönetim rehber dokümanının "Kurumsal SOME'lerin Görev ve Sorumlulukları" başlıklı 4. kısmında bulunan (siber olay öncesi, siber olay esnası, siber olay sonrası) metin ve akış diyagramlarının gözden geçirilmesi,
13. Kurum bünyesinde mevcut kullanıcıların zombi olup olmadığının tespitinin yapılması, tespit edilememesi halinde hafta sonraları ve akşamları "kurum internet" ağının "zorunlu kullanıcılar" haricinde kullanımının önüne geçilerek bu kuralın dikkatli biçimde uygulanmasının sağlanması,
14. Olası bir siber saldırı neticesinde kurum sistemlerinin hızlı biçimde ayağa kaldırılması amacıyla gerekli **acil durum planlarının** hazırlanması,
15. Kritik altyapılar başta olmak üzere kurum ve kuruluşlar bünyesindeki sistemlerin güvenlik testlerinin (sızma testi, APT analizleri vb.) düzenli olarak yaptırılması ve analizler sonucunda tespit edilen açıklıkların **-gecikme olmaksızın-** kapatılması,
16. Kamu Kurumlarının Uyması Gereken Asgari Bilgi Güvenliği Kriterleri dokümanındaki "Kamu Kurumlarının Sağlaması Gereken Kriterler" başlığı altında da belirtildiği üzere manyetik kart vb. kimlik doğrulama yöntemleri ile sistem odalarının güvenliği sağlanarak yetkisiz kişilerin girişlerinin önlenmesi,

EK

17. Kurumsal olarak kullanılan mobil cihazların (telefon, tablet vb.) uzaktan yönetimi için MDM (Mobil Device Management – Mobil Cihaz Yönetimi) uygulamalarının kullanılması, merkezi olarak profil ve güvenlik politikalarının tanımlanmasına imkan verecek sistemlerin devreye alınması,
18. Kritik görev icra eden kamu kurum ve kuruluş personelinin çalışma ortamlarında veya görevi sırasında yanında bulundurduğu akıllı cihazın görevin gizliliğini tehlikeye düşüreceği bilinciyle hareket etmesi ve kritik konuların görüşüleceği toplantılara cep telefonu vb. akıllı cihazların alınmamasına yönelik kurumsal düzenlemelerin yapılması (Kurum girişlerindeki ziyaretçi kayıt noktalarında kilitli dolaplarda muhafaza edilmesi vb),
19. Kurum mahremiyetini içeren görüşme ve yazışmaların anlık mesajlaşma uygulamaları (Whatsapp, Viber vb.) üzerinden yapılmaması,
20. Akıllı cihazlar üzerinde kurulacak uygulamalar için verilecek izinlerin incelenerek onaylanması,
21. Uygulama kurulumlarının resmi uygulama sağlayıcılarından yapılması,
22. 2016 yılı Mart ayında Kurum ve Kuruluşlarla paylaşılan 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı kapsamında belirlenen eylemlerle ilgili çalışmaların Kurumlarca zamanında, titizlikle ve eksiksiz olarak yerine getirilmesi.

Not: Siber Güvenlikle ilgili Bakanlığımız tarafından yayınlanan dokümanlara www.udhb.gov.tr/h-12-siber-guvenlik.html web adresinden ulaşabilirsiniz.

EK-2 Anket Soruları

SİBER GÜVENLİK YÖNETİMİ FARKINDALIK ARAŞTIRMASI

"Bu çalışma **şahsınız veya firmanız tüzel kişiliği** hakkında sorular içermez. Anket; firmaların genel siber güvenlik algısını ölçmek için tasarlanmıştır"

Kıymetli vaktinizi ayırarak anketi yanıtladığınız ve değerli katkılarınız için çok teşekkür ederim.

Bölüm 1 - Siber Güvenliğine Kurumsal Yaklaşım

1- Hiç katılmıyorum, hiç uygulanmıyor
2- Kısmen katılıyorum, kısmen uygulanıyor
3- Çoğunlukla katılıyorum, çoğunluğu uygulanıyor
4- Katılıyorum, uygulanıyor
5- Tamamen katılıyorum, tamamen uygulanıyor

	1	2	3	4	5
1 - Kurumumuzun bilgi güvenliğine ilişkin yazılı kural ve politikaları vardır.	O	O	O	O	O
2 - Kurumumuz bilgi güvenliğine ilişkin yazılı kural ve politikaları oluştururken hayati öneme sahip alanlarda oluşabilecek, tehlike ve güvenlik açıklarını dikkate almıştır.	O	O	O	O	O
3 - Kurumumuz bilgi güvenliğine ilişkin kural ve politikaları, ülkemizdeki ilgili kanun ve yönetmeliklere uygundur.	O	O	O	O	O
4 - Kurumumuz kritik bilişim teknolojilerini önem derecesine göre sınıflandırıp, bu sistemleri oluşturulan sınıflandırmaya göre yönetir.	O	O	O	O	O
5 - Kurumumuz bilgi yaşam döngüsünün tüm aşamalarında gerekli güvenlik önlemlerini almaktadır. (Bilgi yaşam döngüsü: bilginin oluşturulması, kullanılması, depolanması, iletilmesi, işlenmesi ve imha edilmesi)	O	O	O	O	O
6 - Kurumumuz bilgi teknolojilerine yönelik hizmet alımlarında, gerekli güvenlik önlemlerini sözleşme maddelerine dahil eder.	O	O	O	O	O
7 - Kurumumuz tüm çalışanlara bilgi güvenliğine ilişkin yükümlülükleri açıkça bildirilmektedir.	O	O	O	O	O
8 - Kurumumuz tüm çalışanlara düzenli olarak bilgi güvenliği eğitimleri vermektedir.	O	O	O	O	O

Bölüm – 2 Fiziksel ve Çevresel Güvenlik Tedbirleri

1- Hiç katılmıyorum, hiç uygulanmıyor
2- Kısmen katılıyorum, kısmen uygulanıyor
3- Çoğunlukla katılıyorum, çoğunluğu uygulanıyor
4- Katılıyorum, uygulanıyor
5- Tamamen katılıyorum, tamamen uygulanıyor

	1	2	3	4	5
9 - Kurumumuza ait tesislerin güvenliğini iyileştirmek için gerekli güvenlik önlemleri uygulanmaktadır.	O	O	O	O	O
10 - Kurumumuza ait tesislere giriş-çıkışa düzenleyen yazılı kurallar vardır.	O	O	O	O	O
11 - Kurumumuz, bilgi teknolojilerine yönelik her türlü tehlikeye (doğal felaketler veya insan kaynaklı zararlar) karşı koruyu önlemler alınmıştır.	O	O	O	O	O
12 - Kurumumuzda, taşınabilir bilgisayar veya harici depolama aygıtlarının kullanımına ilişkin güvenlik önlemleri alınmıştır	O	O	O	O	O

Bölüm – 3 Bilişim Sistemleri ve İletişim Ağlarının İşletim Ve Bakım Kontrolleri

1- Hiç katılmıyorum, hiç uygulanmıyor
2- Kısmen katılıyorum, kısmen uygulanıyor
3- Çoğunlukla katılıyorum, çoğunluğu uygulanıyor
4- Katılıyorum, uygulanıyor
5- Tamamen katılıyorum, tamamen uygulanıyor

	1	2	3	4	5
13 - Kurumumuz, bilgi teknolojileri verilerini (sistem konfigürasyon ve yedekleri) uygun bir şekilde korur.	O	O	O	O	O
14 - Kurumumuzda bilgi teknolojileri kurulum ve kullanım süreçleri bilgi güvenliği hususları dikkate alınarak icra edilir.	O	O	O	O	O
15 - Kurumumuz, verilerini uygun bir şekilde yedekler.	O	O	O	O	O
16 - Kurumumuz, kötü amaçlı yazılımlara (virüs, trojan, vb.) karşı önlemler alır.	O	O	O	O	O
17 - Kurumumuz, bilişim sistemlerinin güvenlik açıklarını azaltmak için önlemler alır.	O	O	O	O	O
18 - Kurumumuz, bilişim sistemlerine bağlantıları güvenli bir şekilde tesis eder. (VPN, sertifika vb.)	O	O	O	O	O
19 - Kurumumuz, tüm cihaz ve aygıtların çalınma riskine karşı önlemler alır.	O	O	O	O	O

Bölüm – 4 Yazılım Geliştirme ve Destek Aşamalarında Bilgi Sistemleri Erişim Kontrolü Güvenlik Tedbirleri

1- Hiç katılmıyorum, hiç uygulanmıyor
2- Kısmen katılıyorum, kısmen uygulanıyor
3- Çoğunlukla katılıyorum, çoğunluğu uygulanıyor
4- Katılıyorum, uygulanıyor
5- Tamamen katılıyorum, tamamen uygulanıyor

	1	2	3	4	5
20 - Kurumumuz, bilişim sistemlerine bağlantı için gerekli kimlik denetimlerini yapar.	O	O	O	O	O
21 - Kurumumuzda bilişim teknolojilerine kimlerin hangi şartlarda erişebileceği düzenlemiştir.	O	O	O	O	O
22 - Kurumumuz, yerel ağlar üzerinde yetki denetimi uygular.	O	O	O	O	O
23 - Kurumumuz, yazılım geliştirme projelerinin güvenlik gereksinimlerini projelere dâhil eder.	O	O	O	O	O
24 - Kurumumuz, yazılım ürünlerinin seçimi, satın alınması ve / veya bakım işlerinde güvenlik kontrolleri gerçekleştirir.	O	O	O	O	O

Bölüm – 5 Siber Güvenlik İhlalleri ve İş Sürekliliği Yönetimi

1- Hiç katılmıyorum, hiç uygulanmıyor
2- Kısmen katılıyorum, kısmen uygulanıyor
3- Çoğunlukla katılıyorum, çoğunluğu uygulanıyor
4- Katılıyorum, uygulanıyor
5- Tamamen katılıyorum, tamamen uygulanıyor

	1	2	3	4	5
25 - Kurumumuz, bilişim arızalarının kurum faaliyetlerini aksatmaması için önlemler alır.	O	O	O	O	O
26 - Kurumumuzda, olası bilişim kaynaklı problemler için acil eylemleri belirten yazılı prosedürler bulunur.	O	O	O	O	O
27 - Kurumumuzun, tüm bileşenleri kapsar nitelikte arızalara karşı mücadeleyi ele alan bir İSY (İş Sürekliliği Yönetimi) bulunmaktadır.	O	O	O	O	O

28 - Çalışan sayınız? (mevsimsel, yarı zamanlı ve geçici çalışanlar dâhil)

- O max 10
- O 11-100
- O 101-300
- O 301-1000
- O 1000 üstü

29 - Çalışanlarınız % (yüzde) kaçı tam zamanlı?

- O max %10
- O %11-%30
- O %31-%50
- O %51-%70
- O %70 üstü

30 - Firmanızın yıllık cirosu? (Kamu/STK iseniz bütçeniz)

- 10.1 USD veya daha az
- 10.2 USD / 100.000 USD arası
- 100.000 USD / 1.000.000 USD arası
- 1.000.001 USD / 10.000.000 USD arası
- 10.000.000 USD üzeri

31 - Firma sermayesi? Kamu/STK iseniz bütçeniz)

- 10.1 USD veya daha az
- 10.2 USD / 100.000 USD arası
- 100.000 USD / 1.000.000 USD arası
- 1.000.001 USD / 10.000.000 USD arası
- 10.000.000 USD üzeri

---

32 - Firmanızın ülke ekonomisine katkı, istihdam ve sektörel önemi dikkate alındığında toplumsal etkisi nedir? Lütfen aşağıdaki seçeneklerden en uygununu seçiniz.

- Nerdeyse yok
- Çok az
- Sektörde faaliyet gösteren diğer firmalardan daha fazla
- İşimiz gereği çok fazla

33 - Firmanızın müşterilerinin/hizmet verdiği kişi veya kurumların yaşamı, sağlığı, sahip oldukları değerler (taşınmazlar, araç, vb.) üzerindeki etkisi ne derece?

- Nerdeyse yok
- Az
- Çok
- Oldukça fazla

---

34 - Ana iş faaliyetlerinizin dayandığı bilişim sistemleri (diğer şirketler tarafından sağlanan sistemler de dahil olmak üzere, email, web sitesi, kiralık sunucu vb.) bağımlılığı oranı nedir? Lütfen en uygun olanı daire içine alın.

- %25 veya daha az
- %25 - %50 arası
- %50 - %75 arası
- %75 ve ya daha fazla

35 - Ticari/Üretim faaliyetlerinizde ne derece internete bağımlısınız? Lütfen en uygun olanı daire içine alın.

- %25 veya daha az
- %25 - %50 arası
- %50 - %75 arası
- %75 ve daha fazla

---

36 - Satışlarınızı etkilemeyen bilişim sistem ve hizmetlerinin aksamasını ne kadar süre tolere edebilirsiniz? (Kamu/STK iseniz kritik işlerinizin aksaması olarak düşününüz)

- ○ En fazla bir saat
- ○ En fazla yarım gün
- ○ En fazla bir gün
- ○ Birkaç gün
- ○ Daha fazla kesinti bizim için sıkıntı oluşturmaz

37 - Bilişim sistemlerinizin 24 saat hizmet verememesi 1 günlük satış/üretim oranlarınızı ne derece etkiler? (Kamu/STK lütfen %25 veya daha az seçeneğini işaretleyiniz)

- ○ %25 veya daha az
- ○ %25 - %50 arası
- ○ %50 - %75 arası
- ○ %75 ve daha fazla

---

38 - Firmanızı hedef alan ve kişisel bilgilerin (müşteri bilgileri vb.) sızdırılması ile sonuçlanan bir siber saldırının firma imajı üzerine olası etkileri ne oranda olur?

- ○ Nerdeyse olmaz
- ○ Az
- ○ Çok
- ○ Firma geleceğini etkileyecek kadar fazla olur

39 - Faaliyetleriniz ne derecede iş ortaklarınıza, hizmet sağlayıcılara, taşeronlara bağımlı? Lütfen en uygun olanı daire içine alın.

- ○ Arada bir
- ○ Kısmen
- ○ Aşırı derecede
- ○ Onlar olmadan iş yapmamız imkansız

---

40 - Kritik bilgilerin sızıntısı (ulusal sırlar, ticari sırlar, gizlilik bilgileri gibi) meydana gelirse, işiniz üzerinde ciddi etkilere neden olabilir. Bu kritik bilgilerin, şirketinizin elinde tuttuğu, yönettiği ve kullandığı tüm bilgiler arasındaki oranı ne kadardır?

- ○ Nerdeyse yok
- ○ Az
- ○ Bilgilerin yarısı diyebiliriz
- ○ Firmamızın sahip olduğu bilgilerin çoğunluğu kritik öneme sahiptir

41 - Firmanızın bilişim sistemlerinde ortalama ne kadar kişi veya firmaya ait korunması gerekli bilgi bulunmakta? (bilgi miktarından ziyade adedi, müşteri bilgisi, hasta bilgisi gibi)

- ○ 1.000 veya daha az
- ○ 1.001 – 5.000
- ○ 5.001 – 10.000
- ○ 10.001 – 100.000
- ○ 100.000 den fazla

---

42 - Firmanızın personel sirkülasyon oranı (değişim) nedir?

○ %10 / %10 altı ○ %11 - %30 arası ○ %31 - %50 arası ○ %51 - %70 arası ○ %70 üstü

---

43 - Firmanız herhangi bir siber güvenlik olayı ile karşı karşıya kaldı mı?

○ Evet ○ Hayır

47. soruya cevabınız "Evet" ise, lütfen firmanızın karşılaştığı bilişim olay/olaylarını seçiniz. (birden fazla seçebilirsiniz.)

- ☐ İş faaliyetlerini yürüttüğümüz ana bilgisayar / sistemlere (sunuculara) virüs bulaştı
- ☐ Firma geneli bilgisayarlara virüs bulaştı
- ☐ Ağ üzerinden saldırı ile karşılaştık (kablosuz ağ ve yerel ağlardan yapılan ihlaller)
- ☐ Firma web sitesine saldırı oldu
- ☐ Gizli bilgilerin sızdırılması, özel bilgiler, işletme bilgi birikimi (know-how) ve müşteri bilgileri, vb. (desen, hasta bilgisi, yurt dışı müşteri bilgileri vb.)
- ☐ Virüslü e-postalar ile yapılan saldırılar (Cryptolocker vb.)
- ☐ Tolere edilemez sistem arıza veya kesintileri (internet kesintisi dahil)