Üçüncü Sektör Sosyal Ekonomi Dergisi
Third Sector Social Economic Review
56(1) 2021, 163-188
doi: 10.15659/3.sektor-sosyal-ekonomi.21.02.1520

Araştırma Makalesi

Türkiye'de Siber Risk Sigortalarına İlişkin Bir Değerlendirme

An Evaluation of the Cyber Risk Insurance in Turkey

İpek CEBECİ
Dr. Öğr. Üyesi, Giresun Üniversitesi
İktisadi ve İdari Bilimler Fakültesi Ekonometri Bölümü
ipek.cebeci@giresun.edu.tr
https://orcid.org/0000-0002-2341-9379

Makale Gönderme Tarihi	Revizyon Tarihi	Kabul Tarihi
28.12.2020	24.01.2021	10.02.2021

Öz

Teknolojik gelişmelerle birlikte artık birçok suç çeşidi sanal ortama taşınmıştır. Suçluların kurbanlarına fiziksel bir teması olmadan, internet yoluyla bu suçlar işlenebilmektedir. Dünyada gerçekleşen siber saldırıların sayısının artması nedeniyle, sigorta şirketleri harekete geçmiştir. Bireyleri ve işletmeleri bu risklere karşı koruyabilmek adına "siber risk sigortaları" sigorta sektörünün bir ürünü olarak sunulmuştur.

Bu çalışmada; siber tehditler, siber saldırı türleri açıklandıktan sonra, siber saldırılara karşı hazırlanan siber risk sigortaları Türkiye özelinde incelenmeye çalışılmıştır. Türkiye'de sigorta sektöründe siber risklere karşı sunulan ürünlerin varlığına karşın, hem bireysel hem de kurumsal manada bu ürünlere yönelik farkındalık arttırılmalıdır. Özellikle işletmelerin maruz kaldıkları siber saldırılar neticesinde ortaya çıkan; veri ihlalleri, finansal zararlar, itibar kayıpları ciddi sorunlardır. Küçük işletmeler siber risklere gereken önemi vermelidirler. Zira saldırganlar sıklıkla küçük işletmeleri hedef almakta ve onlarla faaliyetlerde bulunan büyük işletmelerin verilerini de böylelikle sızdırabilmektedirler. Dolayısıyla siber tehditlere karşı işletmelerin korunması siber sigortalarla sağlanmalıdır.

Anahtar Kelimeler: *Siber risk, Sigorta, Siber risk sigortası*

Abstract

Along with the technological developments, various of crimes have been transferred to the virtual environment. They can be committed via the internet, without any physical contact of criminals with their victims. Insurance companies have taken action due to the increasing number of cyber attacks happening around the world. In order to protect individuals and businesses against these risks, "cyber insurance" has been presented as a product of the insurance industry.

In this study; cyber threats, cyber attack types were announced, then "cyber insurance" has researched for Turkey. The study reached the following conclusions: there are products offered against cyber risks in Turkey. However, awareness of these products should be increased. Especially as a result of cyber attacks that businesses are exposed to; data breaches, financial damages, loss of reputation are serious problems. Small businesses should pay due attention to cyber risks. This is because attackers often target small businesses and can leak data from large businesses that operate with them. Therefore, the protection of businesses against cyber threats should be provided with cyber insurance.

Keywords: *Cyber risk, Insurance, Cyber risk insurance*

Önerilen Atıf /Suggested Citation
Cebeci, İ.,2021 Türkiye'de Siber Risk Sigortalarına İlişkin Bir Değerlendirme, *Üçüncü Sektör Sosyal Ekonomi Dergisi*, 56(1), 163-188

1. GİRİŞ

Teknoloji ve teknolojik ürünler günümüzün olmazsa olmazıdır. Bu ürünlerin, insanlığın hayatını kolaylaştırmak ve fayda sağlamanın yanı sıra, bir takım kötüye kullanımlarla insanoğluna hem bireysel hem de kurumsal açıdan zarar vermesi de söz konusudur. Bu noktada siber saldırı riskleri önemli bir konu olarak gündeme gelmektedir.

Dünya üzerinde 6 milyar kadar akıllı cihaz bulut teknolojisi üzerinden birbirlerine bağlanmış durumdadır. 2020 yılı için ise bu rakamın 20 milyara ulaşması beklenmektedir. Günümüze kadarki sürede dolandırıcılık, hırsızlık vb. olaylar kurumları olumsuz yönde etkilerken, artık dijital dünyada gerçekleştirilen siber saldırılarla çalışma hayatı sekteye uğratılmakta, hatta kimi zaman durma noktasına dahi getirilebilmektedir. Dolayısıyla günümüzde siber riskler çok daha mühim bir konu haline gelmiştir. Zira siber saldırılar kurum ve kuruluşların verilerine zarar vermekte, fidye karşılığında bu işletmelerin sistemlerini ele geçirebilmektedir. Konunun ehemmiyetini anlayan ülkeler[1]; siber riskleri ve siber saldırıları, deniz, hava, kara ve uzaydan sonraki beşinci harekât sahası olarak belirlemişlerdir (Orend,2014; Bayraktar,2014,s.122; Güntay, 2017,s.82;). Nitekim Varşova Zirvesi'nde (2016) "siber-uzay" NATO tarafından operasyonel alan olarak resmen tanınmıştır. Toplumlar, dijitalleşme seviyelerine bağlı olarak, bilgi odaklı yaşamlarını sürdürdükleri ölçüde siber tehditlere daha açık hale gelirler. Bu açıdan, ülkelerin gelişmişlik düzeyleri de siber risklere açıklık hususunda etkilidir (Kasapoğlu, 2017; Tarhan,2020,s.92; Kotan,2020).

2020 yılı itibariyle başlayan ve tüm dünyayı olumsuz yönde etkileyen COVID-19 salgını sonrasında, dijitalleşme süreci daha da hızlanmıştır. Toplumlar, salgına karşı uygulanan karantina sürecinde daha çok internet kullanımına yönelmiş ve birçok işlem (çevrimiçi alışveriş, çevrimiçi finansal işlemler, çevrimiçi eğitim, çevrimiçi çalışma gibi) sanal alemde çevrimiçi gerçekleştirilmeye başlanmıştır. Bu durum ülkelerin siber ataklara maruz kalma riskini, hem bireysel hem de kurumsal açıdan arttırmıştır (Yılmaz,2020; Vidas ve Diğ., 2016)

Siber saldırılar zaman ilerledikçe daha da değişim göstererek artış göstermektedir. Bu hususta artan riskler sonucunda sigorta şirketleri harekete geçmiş, siber tehditlere karşı poliçeler hazırlayarak siber risklerin de sigortalanmasını kendi faaliyetleri kapsamına almışlardır. Siber risk sigortası, birtakım gizlilik seviyesini taşıyan ve korunması lazım gelen bilgilerin açığa çıkması ya da zarar görmesi neticesinde doğabilecek hasarlara karşı işletmeleri koruyan bir sigorta poliçesidir (Şekeroğlu ve Özüdoğru, 2019, s.55).

Bu çalışmada genel olarak, siber tehditler doğrultusunda olası siber saldırılara karşı hazırlanan siber risk sigortaları Türkiye özelinde incelenmek istenmiştir. Bu amaç doğrultusunda, öncelikle siber tehdidin ne olduğu, siber tehdit türleri ortaya konarak siber sigortaların gereksinimi vurgulanmak istenmiştir. Siber risk sigortasının önemi ve bu ürünün Türkiye'deki mevcut durumu, teminat kapsamı, gibi detayları açıklanmıştır. Ayrıca Türkiye'de siber risk sigortalarına yönelik farkındalığın arttırılması için öneriler sunulmuştur.

[1] Bu ülkelerin başında Amerika, Çin, Rusya, İngiltere gelir. Örneğin; Amerika'da "Birleşik Devletleri Siber Komutanlığı (USCYBERCOM), siber uzay hareketler komutasını merkezde toplar, mevcut siber kaynaklarını düzenler ve ABD askeri bilgisayar ağları müdafaasını eşzamanlı bir hale getirir (www.cybercom.mil). Çin ise 2011 yılında yaptığı bir açıklamayla, ilk kez bir süper elit siber savaşçı birliğine sahip olduğunu duyurmuştur. Siber savaşçılardan meydana gelen bu ekibin, Çin Halk Kuruluş Ordusu'nun internet ağlarını dış ataklardan korumak gayesini taşıdığı belirtilmiştir (www.sabah.com.tr/). Rusya'nın 2000 yılında yayımladığı "Rusya Enformasyon Güvenliği Doktrini" Rusya Federasyonu'nun siber güç olma hedefi doğrultusundaki ilk temel doküman olarak kabul edilir (Darıcılı ve Özdal,2017). İngiltere 2011 yılında, "The UK cyber security strategy protecting and promoting the UK in a digital world" isimli bir siber güvenlik belgesi hazırlamış olup, ülke siber güvenlik için 2009-2013 yılları için 650 milyon sterlin bütçe ayırmıştır (https://assets.publishing.service.gov.uk).

2. SİBER TEHDİTLER

Siber tehdit, siber uzayda[2] mevcut olan bilgini bozulması, açığa çıkarılması, ulaşılabilirliğinin engellenmesi veya kesintiye uğraması gibi arzu edilmeyen durumlara yol açma potansiyeline sahip unsular olarak ifade edilebilir. Bu tehditler, bilgi ve teknolojilerinden yararlanılarak oluşturulmuş, bütünüyle yeni suç kavramları meydana getiren siber saldırıların yanı sıra; bilgi ve iletişim teknolojilerinin getirdiği olanakların araç olarak kullanıldığı, klasik saldırıların siber ortama uyarlanmış hallerini de içermektedir (Çotak, 2019, s.40).

Siber tehditlerin neden olduğu tesirleri kısa vadeli ve uzun vadeli olmak üzere iki gruba ayırarak inceleyebiliriz. Kısa vadeli tehditler; hedef kişi, kurum/kuruluş ve devletlerin günlük aktivitelerini etkileyen tehditlerdir. Bu tarz kısa vadeli tehditlere örnek olarak; dolandırıcılık olayları, veri ihlalleri, ATM makinelerinden yasal olmayan şekilde para çekilmesi vb. günlük olarak gerçekleştirilen işlem ve faaliyetler verilebilir. Uzun vadeli tehditler ise; tesirleri uzunca bir süre devam eden, daha geniş bir insan topluluğunu etkileyebilen, devletin ve toplumun istikrarını değişikliğe uğratabilen faaliyetleri kapsar. Uzun vadeli tehditlere örnek olarak da; sınaî ve askeri ajanlık, toplumsal memnuniyetsizlik ve huzursuzluk oluşturma, ulusal güvenliğe zarar vermek vb. tehditler verilebilir (Choo, 2011).

Siber tehditlerin geliş yönüne ve kaynağına göre ayrılır (Tablo 1). Bu tehditlerden en tehlikeli olan; kurum içindeki küskün ve kötü niyetliler ile kötü niyetli olmayan fakat eğitimsiz ve bilinçsizlik nedeniyle istemeden de olsa zarar verenlerdir. Zira bu tehditlerin kaynakları bütünüyle kapalı kutu olup, ne zaman, ne şekilde ve ne seviyede bir zarar verebileceğine dair bir öngörüde bulunmak ve tedbir almak çok güçtür. Oysaki olası diğer tehditlere karşı muhtemel hareket biçimleri, potansiyel hedeflere yönelik bir tahmin ve tedbir geliştirme olanağı bulunmaktadır (Kılınççeker, 2018, s.59).

Tablo 1. Siber Tehdit Kaynakları

TEHDİT KAYNAĞI AÇISINDAN		**GELİŞ YÖNÜ AÇISINDAN**
İnsan Kaynaklı Tehditler 1-Kötü niyetli olmayan 2-Kötü niyetli olan	**Doğa Kaynaklı Tehditler**	1-Kurum içi 2-Kurum dışı

Kaynak: Bensghır, (2011)

Siber alanlar 1980'li ve 1990'lı yıllarda teknoloji ve bilhassa internetin yaygınlaşmasıyla hızlı bir şekilde gelişim göstermiştir. Bu gelişim beraberinde birçok sorunun ve gereksinimin giderilmesini sağlamış, fakat bir yandan da yeni sorunların doğmasına da neden olmuştur. Siber alanın sağladığı bir takım kolaylıklar bireyleri ve kurumları bu ortama bağlarken, bu ortamın korsanları olan "hacker"lar tarafından saldırılara maruz bırakmakta; birey, sektör, kurum ve hatta ülke çapında bu türden saldırıların artmasıyla birlikte siber ortamda da güvenliğin yeri ve önemi üzerinde tartışmalar yapılmaya başlanmıştır. Siber alanda bilgi alkışında güvenliğin sağlanması, eldeki verilerin kontrol altında güvenli bir şekilde depolanması, birey ve kurumların bilgilerinin gizliliği gibi konuların güvenliği açısından farklı ve yeni yollar aranmıştır. Ancak teknolojik gelişim, siber korsanların birçok strateji ile bireysel veya kurumsal sistemlere sızma yollarını arttırmıştır (Şekeroğlu ve Özüdoğru, 2019, s. 56).

[2]Siber Uzay (cyberspace); tüm dünyada, uzaya yayılmış olan bilişim sistemlerinden ve bunları birbirine bağlayan ağlardan meydana gelen veya bağımsız bilgi sistemlerinden oluşan sayısal ortama denir. Siber uzayın bileşenleri; kamu, özel sektör ve bireylerdir (usom.gov.tr).

Büyük işletmeler bilgi ve iletişim teknolojilerinden kaynaklanan risklere yönelik; bütçe ayırarak, gereksinim duyulan seviyede profesyoneli çalıştırarak bir takım tedbirler almaya çalışmaktadırlar. Ancak; bilgi güvenliğine yatırım yapmayan, maliyetlerden ötürü gereken miktarda bilgi teknolojileri çalışanının istihdamından kaçınan KOBİ'ler siber risklere karşı gerekli önlemleri alamadıkları için suiistimallere ve siber suçlulara kolay hedef olmaktadırlar (Baykız ve Tanrıöven, 2019, s.479).

3. SİBER SALDIRI TÜRLERİ

Siber saldırı türleri günümüzde oldukça çeşitlenmiş olup, bu saldırıların başında fidyecilik (ransomware), nesnelerin interneti (the internet of things), sosyal mühendislik ve oltalama (phishing), kırma, ortadaki adam şeklindeki saldırı türleri en bilinenleridir.

3.1. Fidyeleme (Ransomware)

Fidye yazılımları, bir cihazı kilitleyebilen veya sahibinden para koparmak amacıyla içeriklerini şifreleyen kötü amaçlı yazılımlardır (eset.com). Bu kötü niyetli yazılımlar; insanların özel bilgilerini ifşa etme, kritik verilerini kaybetme veya geri dönüşü olmayan donanım hasarlarıyla karşılaşma korkusundan faydalanır. Fidye yazılımı, kurbanın cihazına gizlice yüklenen ve kurbanın verilerini rehin tutan kripto virolojisinden kripto-viral gasp saldırısını gerçekleştiren kötü amaçlı bilgisayar yazılımlardır (Tabiaa ve Diğ., 2017, s.192; Kharraz ve Diğ., 2015). Fidyeleme saldırı yaptığı sistem üzerinde yapmış olduğu değişikliklerle kişilerin verilerini şifrelemekte ya da kullanıcıların sisteme erişimini kısıtlayarak bir ödeme talebinde bulunmaktadır (Şekeroğlu ve Özüdoğru, 2019, s.57).

Kurbanlar dosyalarına yeniden erişim sağlamak için genellikle bitcoin veya diğer sanal para birimleriyle ödeme yaparlar. Ayrıca premium SMS[3] mesajları ve ön-ödemeli kredi kartları da saldırganlar tarafından kullanılmaktadır. İleri seviyedeki fidye yazılımı saldırıları, disk veya dosya düzeyinde şifreleme kullanır ve bilgisayar korsanlarının talep ettiği fidyeyi ödemeden dosyaların kullanılmasını imkânsız hale getirir. Fidye yazılımını dağıtmanın kolay olması nedeniyle siber suçlular kazanç elde etmek için bu tür kötü amaçlı yazılım saldırılarını gün geçtikçe daha fazla tercih etmektedirler (Sanders, 2018).

İlk bilinen fidye yazılımı 1989 yılında,189$ fidye talep eden "PC Cyborg" yazılımıdır. 2005 yılında da Rusya'da 300$ fidye isteyen; XLS, DOC, JPG, PDF, ZIP dosyaları şifreleyen yazılımlar yaygınlaşmıştır. Gpcode, TROJ.RANSOM.A,, Archiveus, Cryzip, Krotten, MayArchive gibi adlarla ifade edilen bu zararlılar çift anahtarlı şifreleme algoritmasını kullanmaya başladılar. 2007 yılında ise SMS atılmasını veya paralı telefon sistemlerinin aranmasını isteyen farklı bir fidye yazılımı ortaya çıkmıştır. 2012'de bilgisayarı kilitleyip, açılması için şifre isteyen bir sürüm aktif olmuştur. Bilgisayarlarda *"Yasa dışı faaliyetlerinizden ötürü FBI bilgisayarınızı kilitlemiştir. Suç işlemektesiniz, bu kilidin açılması için şu hesaba para ödenmesi gerekmektedir*." şeklinde uyarılarla karşı karşıya kalınmıştır. Rusya'da daha fazla aktif olan dosya şifreleme yapan fidye yazılımları 2012'den sonra diğer ülkelere de sıçramış, 2014 yılından itibaren daha da gelişen yazılımlar giderek yaygınlaşmıştır. Yeni sürüm zararlı uygulamalar Windows dışında MacOS, Android, Web sunucular ve Linux sistemlere de bulaşmaya başlamıştır (bilisiminovasyon.org.tr).

CryptoLocker, Locky, WannaCry, Petya en çok bilinen fidye yazılımı saldırılarındandır (Sanders, 2018). Örneğin bunlardan WannaCry fidye yazılımı 2017 yılında ortaya çıkmıştır. Bu saldırı 150'den fazla ülkeye sıçrayarak, yüzbinlerce bilgisayarı etkilemiştir. Elde edilen verilere göre bu saldırıya karşı halen kullanıcılar yeterli derecede güvence altında değillerdir. Bilhassa güncel işletim sistemlerine sahip olmayan kullanıcılar bu saldırıya daha çok açıktırlar. Tahminlere göre

[3] Premium SMS: Örneğin kredi kartı bilgilerinizi ifşa etmeden, hizmetler için hızlı ve kolay bir şekilde ödeme yapmanızı sağlayan, cep telefonuyla pratik bir ödeme yöntemidir (https://www.tariftip.de).

1,7 milyon bilgisayar WannaCry saldırısına her an uğrayabileceği öngörülmektedir. (Kalelioğlu, 2019; Mohurle ve Patil, 2017). WannaCry fidye yazılımı nedeniyle çok sayıda firma işlemlerini yürütememiş ve parasal olarak önemli meblağlarda zararlara uğramışlardır. Siber risk modelleme firması Cyence, saldırıdan kaynaklanan potansiyel maliyeti 4 milyar dolar olarak tahmin ederken, diğer gruplar kayıpların çok daha fazla olacağını belirtilmiştir (Berr, 2017).

Mobil teknolojilerin gelişimine paralel olarak, telefon işletim sistemleri üzerinden gerçekleştirilen fidye saldırılarında da hızlı yükseliş gözlenmiştir. Siber güvenlik devi Symantec'in yıllık İnternet Güvenliği Tehdit Raporuna (ISTR) göre, mobil teknolojiler üzerinden yapılan fidye saldırılıları 2018 yılında, bir önceki yıla oranla % 54 artış göstererek 18 milyon adet olarak gerçekleşmiştir. (Dobran, 2019).

3.2. Nesnelerin İnterneti (Internet of Things: IoT);

Teknoloji ve iletişim ağlarındaki gelişmelerle birlikte; birbirine bağlanarak bilgi akışını sağlayan, belirli haberleşme kanallarıyla ağ oluşturan cihazlar sistemi olarak tanımlanan "Nesnelerin İnterneti" gün geçtikçe daha fazla yaşam alanımıza girmektedir (Doyduk ve Tiftik, 2017, s.128). Gerçekleştirilen araştırmalara göre; nesnelerin interneti 2020 yılında 50 milyar cihaza eriştiği tahmin edilmektedir. Dünyadaki kişi başına düşen nesnelerin internetini kullanan cihaz oranı 2003 yılında %0.08 iken, bu oranın 2020 yılında %6.48 olacağı öngörülmektedir. 2020 yılında yirmi cihazın üreteceği ağlar içerisindeki bilgi akışının, 2008 yılı internet trafiğinde bulunan bilgi akışından daha fazla olacağı da belirtilmektedir (www.karel.com.tr).

Nesnelerin internetinin hedefi; ses, görüntü alıcıları, duman detektörü vb. gündelik hayatta kullandığımız aletleri teknoloji ile çevrimiçi hale getirmektir. Diğer bir hedefi de, her bir aletin internetten erişimini sağlayan, aletleri içeren ağların uyumudur. Tedarik zincirinde ürünleri takibe yarayan bu "Radyo Frekanslı Tanımlama (RFID)" uzun zamandan beri kullanılmaktadır. Fakat ürün paketlerde raflarından alındıktan sonra, üreticinin takibi sonlandırılır. Her ürüne dair belirleyiciler tanımlanarak, bunların web üzerinden erişilebilir olmasını ve böylelikle ürünün tüm yaşam döngüsü süresince takip edilebilir olmasını sağlayan şey nesnelerin internetidir (Doyduk ve Tiftik, 2017, s.128).

Nesnelerin internetini kullanan ürünlerin başında; akıllı gözlükler, akıllı saatler, akıllı bileklikler, akıllı ev sistemleri, akıllı otomobiller, ev otomasyonu gelir. Fakat belirli bir ağ üzerinden çalışan bu cihazların siber saldırılar açısından güvenliği sınırlıdır. Genellikle basit şifrelemeyle birlikte iletişim kuran bu aygıtlar, siber saldırılar bakımından kolay bir hedeftir. Kablosuz iletişim sağlayan pek çok cihaz bu tehdide oldukça açıktır (Şekeroğlu ve Özüdoğru, 2019, s.58). Örneğin 2019 yılında açıklanan bir araştırmanın sonuçlarına göre, siber saldırganlar tarafından hack'lenebilecek 100.000 webcam'in kullanımda olduğu ortaya çıkmıştır. Bir diğer güvenlik riski içeren IoT cihazı ise akıllı saatlerdir. Çocuk akıllı saatlerin güvenlik riski konusu gündeme gelmiştir.

Iot cihazlarının siber saldırı neticesinde ne tür verileri ele geçirebileceği konusunu incelenecek olursa; internet aracılığıyla ulaşılabilen temel düzeyde bir akıllı evi örnek verilebilir: Akıllı bir kahve makinesi sizin uyanma bilginizi, akıllı bir müzik sistemini müzik zevkinizi, akıllı fırınınızın ise sevdiğiniz yemeklere dair bilgi verecektir. Bunlar gibi size ait veriler şayet kötü niyetli birilerinin eline geçerse, size ait küçük veri parçalarından kişisel bilgi bütünlüğünüze dair büyük veya kritik bir veriye ulaşılabilir. Bu tarz senaryolar rahatlıkla çoğaltılabilir. Birey için yaptığımız böyle bir inceleme, kurumsal bazlı da yapılabilir. Kurumsal yaşamda toplantı odalarında yer alan akıllı iletişim araçları, bir işletmenin gelecek planlarına dair kilit detayları toplayabilir. Bu kurumsal verilere yine kötü niyetli kişilerin erişmesi ciddi bir sorun oluşturabilir (www.bilgiguvende.com).

Muhtemel Iot güvenliği hususunda gerçekleştirilen akademik çalışmalarda; potansiyel tehditler ve saldırganlar incelenmiş, güvenlik ve mahremiyet açısından 3 grup saldırgan olduğu ifade edilmiştir (Atamli ve Martin,2014, aktaran: Zeybek ve Yılmaz, 2019, s. 77).

- **Kötü niyetli kullanıcı:** Üreticinin gizli bilgilerini ele geçirmek ve kısıtlanmış fonksiyonlara erişmek amacıyla saldırıyı gerçekleştiren kullanıcıdır. Sistem üzerinden bu sır olan bilgileri edinerek, bunları diğer firmalara satabilir veya elde ettiği bir güvenlik açığını aynı özellikteki diğer cihazlarda kullanabilir.
- **Kötü niyetli üretici:** Ürünlerini sattıkları kullanıcılar veya onların kullandığı diğer cihazlar hakkında veri toplamak amacıyla ürün geliştiren üretici firmalardır. Ürünlerin tasarımı sırasında cihazlara oluşturulan arka kapı veya zararlı yazılımlar aracılığıyla topladığı verileri casusluk amacıyla kullanabilirler. Bunun yanı sıra ortamda bulunan diğer internete bağlı nesnelerle iletişim kurup, zarar vererek bu ürünleri üreten işletmelerin güvenilirliğini sarsabilirler.
- **Dış saldırganlar:** Akıllı cihazlara erişimi ve yetkisi olmayan kötü niyetli kişilerdir. Değişik biçimlerde saldırılar yaparak; kullanıcıya dair bilgi toplamak, maddi zarar vermek türünden gayeleri olabilir. Tehdit kaynakları içerisinde en yüksel orana sahip gruptur.

Konu ile ilgili mevcut yazın incelendiğinde, gerçekleştirilen çalışmalarda; IoT ağlarındaki cihazlarının sahip olduğu kısıtlı bant genişliği, hafıza ve hesaplama yeteneğinin, bu cihazları tehditlere karşı savunmasız bıraktığı ifade edilmiştir. Bundan ötürü, bu cihazların geleneksel güvenlik tekniklerini kullanarak internetin ortaya koyduğu güvenlik problemleriyle başa çıkmalarının mümkün olmadığı ve IoT mimarisini meydana getiren katmanların farklı özellikteki saldırılara karşı savunmasız kaldığı belirtilmiştir (Karlof ve Wagner, 2003; Wood ve Stankovic, 2002; Görmüş ve Diğ., 2018; Korkmaz ve Diğ., 2012).

3.3. Sosyal Mühendislik (Social Engineering)

Kişileri maniple ederek, belirli eylemleri yaptırmayı hedefleyen veya bireye özel bilgileri açığa çıkarmaya çalışan edimdir. Terim olarak; bilgisayar sistemine sızmak, bilgi toplamak şeklinde bilinir. Bu teknikte genelde saldırgan ile kurban yüz yüze gelmemektedir. Bu teknik, insanların akıllarını karıştırarak onları maniple etmeye dayalıdır. Sosyal mühendislik çok eski toplumlarda bireyleri yönetmek için da kullanılmış, ancak 1960 sonrasında, internetin yaygınlaşmasıyla birlikte, yeniden gündeme gelmiştir. Sosyal mühendislik uygulamaları ile karşıdaki kişilere çok büyük zararlar verilebilir (Özgül, 2017).

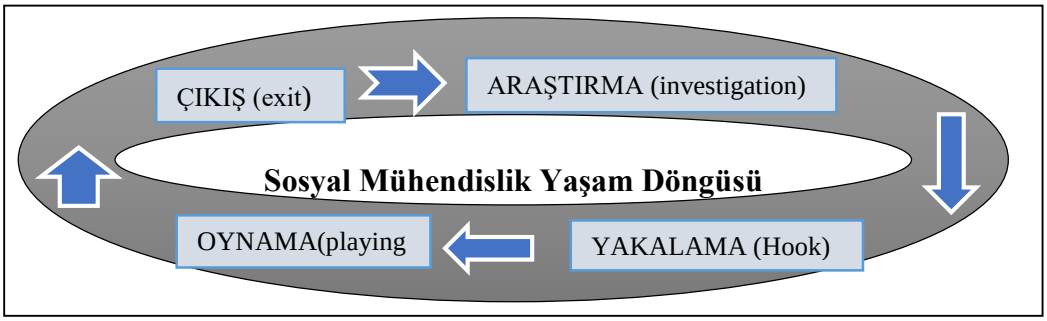
Sosyal mühendislik, bilgisayar korsanlarının temelde bildikleri kandırma veya bir yanıltma yöntemidir. Bu korsanlara göre sistemin en zayıf noktası insan faktörüdür. Sosyal mühendislik 4 aşamadan (Şekil 1) meydana gelir. Bunlar (imperva.com);

- Birinci aşama **"araştırma"** (investigation) aşamasıdır. Bu aşamada saldırı yapılacak kişi yani kurban tayin edilir. Tayine edilen kurban hakkında yeterli bilgi toplandıktan sonra, bu aşamanın son bölümünde kurbana yönelik geçerli olabilecek saldırı çeşitleri belirlenip ikinci aşamaya geçilir.

- **Yakalama** (hook), ikinci aşamadır. Bu aşamada kurban kişiyle ilgili, onun inanacağı bir hikâye oluşturulur. Kurban hikâyenin tesiri altındayken, sergileyeceği olası davranışlar öngörülerek kurbanın etkileşimleri kontrol altına alınmaya çalışılır.

- Üçüncü aşama **"oynama"** (playing) aşamasında ise kurbana yönelik inandırıcılığın arttırılabilmesi amacıyla oluşturulmuş olan hikâye genişletilir. Bu esnada kurbandan saldırı için gerekecek gizli bilgiler sağlanır ve saldırı başlatılır. Kurbanın sistemine erişimi ya da verileri şifrelenir.

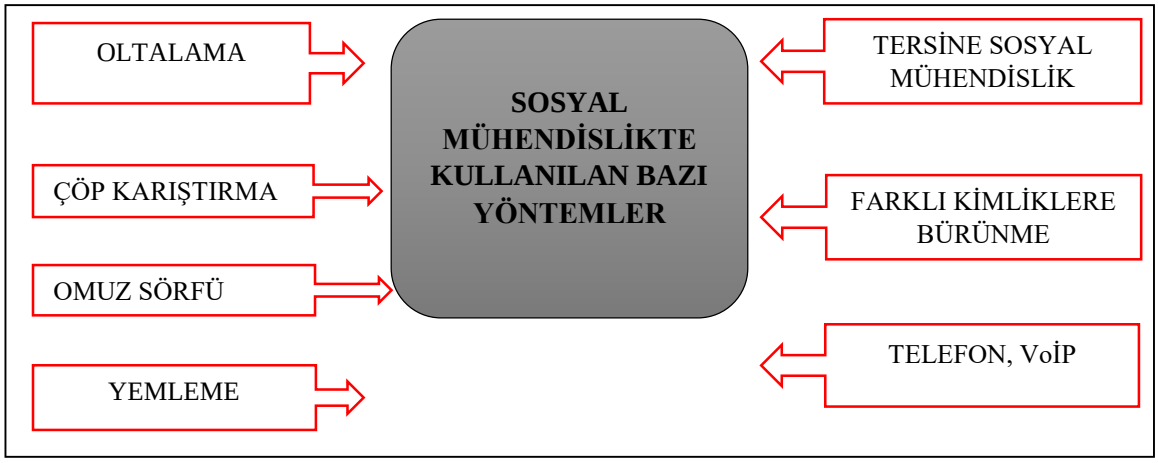
- Son aşama olan **"çıkış"** (exit) aşamasında; saldırıyı gerçekleştiren kişinin bıraktığı izler silinir. Kurbanın temasa geçmesi beklenir.



Şekil 1. Sosyal Mühendisliğin Aşamaları

Kaynak: https://www.imperva.com/learn/application-security/social-engineering-attack/

Sosyal Mühendislikte kullanılan yöntemlerden belli başlıları; oltalama,(phishing), çöp karıştırma (dumpster diving**)**, omuz sörfü, yemleme, tersine sosyal mühendislik, farklı kimliklere bürünme, telefonla arama gibi yöntemlerdir (Bakınız Şekil 2).



Şekil 2. Sosyal Mühendislikte Kullanılan Bazı Yöntemler

Kaynak: Irmak ve Reis, 2018, s.109

Sosyal mühendislik saldırılarını gerçekleştirmenin çok farklı yöntemleri olmakla birlikte, bunlardan bazı popüler olanları aşağıda açıklanacaktır:

3.3.1. Oltalama (Phishing)[4]

Bu yöntemde; saldırgan kurbanı aldatarak, kurbana ait gizli bilgileri (kurbanın şifre, kredi kartı bilgileri, banka hesap numarası vb. gibi) ele geçirir. Bu dolandırıcılık türünde saldırganların en çok kullandıkları yöntem sosyal mühendislik tekniklerdir. Bu manada kurbanlara "phish" (fish), balık denilmektedir. Nasıl ki balık avlama sırasında balıkların yakalanabilmesi için değişik oltalar kullanılıyor, oltalar balıkların yoğun olarak bulunduğu yerlere, tutulması istenen balığın türüne göre belirli şekillerde yerleştiriyor ve balıkların oltaya takılması bekleniyorsa, Phishing saldırılarında da sistem benzer bir şekilde işletilmektedir. Bu türden saldırılar günümüzde oldukça fazla çeşitlenmiştir. Farklı türlerinin olmasına rağmen, genel kabul görmüş sistem şu şekilde işler: İlk etapta popüler ve çok müşterisi bulunan bir banka veya finans kurumu seçilir. Bu durum balıkların fazla olduğu bir yerde avlanmayı seçen avcıya benzetilebilir. Ardından seçilen kurumun internet şubesi gözlem altına alınır ve mevcut sistem tespit edilir. Bu tespit örneğin kullanıcı kodu sistematiği, şifre düzeneği gibi bazı teknik ayrıntılar ile kurumun müşterilerin profili, demografik

[4] "Phishing" İngilizce bir kelime olan "fhishing" yani "balık avlamak" kelimesinden türetilmiştir.

ve ekonomik yapısı gözden geçirilerek en uygun tuzak (yem) hazırlanır. Bu aşamadan sonra hedef sitenin genel kopyası veya bir benzeri yapılır. Daha sonra saldırgan tarafından seçilen bir sistemlerden biri kullanılarak bir geçişi sunucuda sistem çalışır hale getirilir. Bu anda saldırgan kişi hazırlamış olduğu e-postaları elindeki hazır e-posta listelerine SPAM olarak gönderir. Bu postalarda banka/finans kuruluşunun sisteminde güncelleme yapılmakta olduğu ve sistemde eksik bilgilerin tamamlanması talebi iletilir ve altına saldırganın daha önceden hazırladığı sitenin adresi gizli bir şekilde konulur. Bu postaya kanan kurban ise kendi eliyle saldırana kişisel bilgilerini dolandırıcıya vermiş olur. Nihai olarak saldırgan kişi, kurbandan topladığı verileri maddi çıkar sağlamak amacıyla kullanır (Alataş ve Atan, 2007).

İlk olarak 1996 yılında ortaya çıkan oltalama yönteminin, 2003 yılına kadar çok fazla bir kullanımı olmasa da, bu tarihten sonra çok hızlı ve farklı şekilde karşımıza çıkmaya başlamıştır. Bu durumun en önemli nedeni; dinamik sitelerin yaygınlaşması ve bedelsiz alan veren sunucuların sayısının artmasıdır. Türkiye'de bu yöntemin kullanılması ise 2004 yılı itibariyle olmuştur. Başlangıçta inandırıcılığı düşük gelen bu yöntem, zaman içinde farklılaşmış ve çok sayıda insanı etkileyecek bir hale gelmiştir (Şenol ve Karacan,2012, s.2).

Saldırganların bu yöntemde hedefteki kişi ile elektronik posta, sohbet ya da sahte web sitesi üzerinden iletişim kurarak verileri elde eder. Bu elde ettiği verileri ya kendi kullanır ya da satar. Bu yöntem sanal alemde en çok kullanılan yöntemdir (Çatak, 2016; Hekim ve Başıbüyük, 2013; Irmak ve Reis, 2018).

2019 yılına ait oltalama (phishing) ve e-posta dolandırıcılığı istatistiklerine göre (retruster.com); veri ihlalinin ortalama finansal maliyeti 3,86 milyon dolar seviyesine ulaşmıştır. Phishing, veri ihlallerinin %90'ını oluşturmaktadır. Şirket e-posta dolandırıcılığı (kısa adı BEC dolandırıcılığı), 12 milyar doları aşmıştır.

3.3.2. Omuz Sörfü (Shoulder surfing); klavyeyle bilgi girişi gerçekleştiren kişinin şifresini veya diğer başka kullanıcı bilgilerini görüp, çalmak gayesiyle başka kişilerin gizli bir şekilde, doğrudan izleme yapmasıdır (Gündüz ve Daş, 2014; Krombholz ve Diğ., 2014, s.5, Irmak ve Reis, 2018).

3.3.3. Çöp Karıştırma (Dumpster diving); özel şahısların ya da şirketlerin çöplerinin elenerek, incelenmesi yoluyla, bir sisteme ait hassas bilgiler veya belirli bir kullanıcıya ait kişisel bilgiler (hesap bilgileri gibi) kötü niyetli kişilerce bulunmaya çalışılır **(**Krombholz ve Diğ., 2014, s.5)

3.3.4. Telefonla Arama, Telefonla Oltalama (Voİp); "vishing" olarak bilinen bu yöntem, saldırganın hedef kişiye ait kredi kart numarası, şifre, ayrıntılı ikamet adresi gibi önemli bilgileri ele geçirmek amacıyla, kurbanı telefonla arayarak; şantaj, korkutma gibi kandırma metotları kullanarak, kurbanın kişisel bilgileri ele geçirmek için bu türden bir sosyal mühendislik saldırısı türünü kullanabilir. Saldırgan dünyanın herhangi bir yerinden, kimliğini gizleyerek sesli arama (voice phishing) yapabilir (Airehrour ve Diğ., 2018, s.5; Tabiaa ve Diğ., 2017, s.193).

3.3.5. Kimliğe Bürünme (Impersonation), saldırganın bir başkasının kimliğine bürünmesi; o kişi gibi davranması, bir başkası adına hesap açmak veya profil oluşturmak şeklinde saldırısını yapılır. Bu yöntem, sanal alandaki en önemli tehlikelerden biridir. Saldırgan kişi kendini farklı bir kişinin rolüne girerek (şarkıcı, siyasetçi, ünlü bir sanatçı, vb. gibi) sosyal medya gibi sanal alanlarda arkadaşlık ilişkileri kurabilir. Kendisini yardıma ihtiyacı olan bir kişi gibi gösterip, hedef kitleyi kandırabilir. Bu yöntemle kişilik haklarına zarar verebileceği gibi, insanları kandırarak usulsüz kazanç elde edebilir (Yavanoğlu ve Diğ., 2012, s.23). Kimliğe bürünmek türünden bir sosyal mühendislik çeşidi uygulayan saldırgan, BİT kurumda çalışan bir işçi veya sistem üzerinde yetkililere sahip kullanıcı gibi davranabilir. Saldırgan kişi; bir kapıcı, işçi veya taşeron gibi davranarak ortama fiziksel bir erişim de sağlayabilir (Gündüz ve Daş, 2014).

3.3.6. Tersine Sosyal Mühendislik (Reverse Social Engineering); bu yöntemde genelde saldırgan ile kurban arasında güvenin kurulduğu bir durum söz konusudur. Saldırganlar, kurbanın yardıma ihtiyacı olduğu bir hadise meydana getirirler; örneğin kurbanın internetini kesmek, bilgisayarını bir şekilde bozmak gibi… Ardından kurbanın sorununu giderebilecekmiş gibi

kurbana yardımcı olmaya çalışırlar. Bu sırada kurbanın hususi bilgilerini elde ederler. Bu yöntemde genelde saldırganlar önemli bilgilere sahip kişileri hedef olarak tercih ederler (Krombholz ve Diğ., 2014, s.5)

3.3.7. Yemlemek/Truva Atı: (Baiting /Trojan Horse); kötü amaçlı yazılım yüklenmiş bir depolama aracının (USB, CD gibi), hedeflenen kişilerce bulunması ve merakına yenilerek bunu kendi bilgisayarına takıp, kullanılması sonucunda saldırganların kurbanın bilgisayarında arka kapı açarak, bilgisayara sızması şeklinde gerçekleşir (Airehrour ve Diğ., 2018, s.5)

3.4. Kırma (Cracking) yöntemi, genellikle bireylerin finansal bilgilerini ele geçirmek amacıyla kullanılır. Bu metot, bir program içerisine yerleştirilmiş ilave programlar sayesinde kişisel bilgisayarların güvenlik sitemini aşarak bir arka kapı oluşturur. Örneğin halka açık alanlarda kullanılan kablosuz ağlar, kırma şeklindeki saldırıların yayılmasın bir diğer yolu olarak karşımıza çıkar. Bu alanlarda güvenlik koruması düşük olduğundan, bu alanlardan ağa bağlanmak sanal korsanlara hedef olmak anlamına gelmektedir (avast.com, Şekeroğlu ve Özüdoğru, 2019, s.60).

3.5. Ortadaki Adam Saldırısı (Man-in-the-middle Attack) yönteminde saldırgan, kullanıcı ile web sayfasının yer aldığı sunucu arasında konumlanır ve iki taraftan gelen veriler saldırganın üzerinden geçer. Bu şekilde saldırgan, kullanıcı ile sunucu arasındaki iletişimi dinleyebilir. Genelde SSL protokolü ile şifrelenmiş iletişimin bu metot ile saldırgan tarafından çözülmesi mümkün değildir. Fakat saldırgan, kullanıcı ya da sunucu tarafından zararlı yazılım kullanarak iletişimin şifrelenmesinde kullanılan anahtarı ele geçirebilir ya da değiştirebilir. Böyle bir durumda her ne kadar veri şifrelenmiş olsa da, şifre saldırgan tarafından temin edilmiş olur. Ortadaki adam saldırısının kullanıcılar tarafından fark edilmesi oldukça zordur. Zira kullanıcı bağlandığı web sitesinin çalışma sürecinde normale aykırı bir durum algılamayacak, bir ihtimal bağlantı hızında yavaşlama yaşayabilecektir (Ünlü, 2018, s.90).

4. SİBER RİSK SİGORTASI

İçinde bulunduğumuz bilgi çağında, bilginin bir yerden bir yere ulaşma hızı oldukça yüksektir. Böyle bir ortamda; bilginin son derece hızlı yayılması gereksinimi, ciddi bir otomasyonu da beraberinde getirir. İnternetten baktığımızda aynı bulut teknolojisi üzerinden birbirine bağlı milyara yakın cihaz vardır ve bu sayı gün geçtikçe daha da artmaktadır. Telefondan, şahsi tablet ve bilgisayarlara, bankalardan borsa şirketlerine, kredi kurum ve kuruluşlarından, doğalgaza, elektrikten su dağıtan şirketlere kadar birçok kurum ve kuruluş aynı bulut sistemi üzerinden birbirine bağlanmış durumdadır. Böyle bir sanal ortamda siber risk sigortasının oldukça önemli bir ürün olduğu da anlaşılmaktadır (atabrokerlik.com). Siber sigorta, bilgisayar güvenliği ihlallerinin neden olduğu mali kayıpları karşılamanın uygun bir yolu olarak kabul edilir (Böhme,2005, s.1)

Büyük işletmelerin maruz kaldığı siber saldırılar ve neticesinde ortaya çıkan veri ihlalleri, finansal zararlar ve itibar kayıplarını minimuma indirmek için siber saldırı riskini büyük oranda azaltmak ya da ortadan kaldırmak için belirli güvenlik önlemleri almaktadırlar. Fakat küçük işletmeler bu konuya gereken önemi vermemektedirler. Bu nedenle de siber saldırganlar küçük işletmeleri daha çok hedef olarak tercih etmektedir. Nitekim küçük işletmelere yönelik bu türden siber saldırılara dair sayılar da bunu destekler niteliktedir. Siber korsanlar küçük işletmelere saldırılarını yaparken bir taraftan da küçük işletmelerle faaliyetlerde bulunan büyük işletmelerin verilerine; ortak ağ, sistem vb. araçlarını kullanarak sızmakta, onlara finansal zararlar vermekte ve hatta itibar kayıpları yaşatmaktadırlar. Bu durumları kısman engellemek için küçük ve orta büyüklükteki tüm işletmelerin de siber risk sigortası alması gerekmektedir (Şekeroğlu ve Özüdoğru, 2019, s.61).

İşletmelerin sahip oldukları bilgilerin değerini tam olarak bilmemeleri ve muhtemel bir kayıp (çalınma) durumuna yönelik risklerin sigorta ürünleriyle teminat altına alınmaması, siber risk sigortasının gelişimi sürecinde önemli bir role sahiptir (Çotak, 2019,s.17). Siber risk sigortası 1990'lı yılların sonunda ilk olarak Amerika Birleşik Devletleri'nde ortaya çıkmıştır. 2000'li yılların başı itibarı ile de Avrupa'da siber risk teminatları sağlanmaya başlanmıştır. Türkiye'de,

2010 yılında siber risk sigortalarının bir gereksinim olduğu düşüncesi hâsıl olmuştur. Bu doğrultuda başlangıçta teminat yurtdışı piyasalardan karşılanmış, ancak çok kısa bir süre sonra Türkiye'de bulunan sigorta şirketleri tarafından da yurtiçinde teminat verilmeye başlanmıştır. İlk etapta siber riskler konusu hafife alınmış, sadece veri kayıpları siber riskler olarak görülmüş; zamanla ortaya çıkan siber zararlar ise siber risklerin, veri kayıplarından çok daha kapsamlı olduğunu göstermiş ve verilen teminatların kapsamı arttırılmıştır. Şüphesiz gün geçtikçe, siber risk sigortalarına duyulan ihtiyaç artacaktır (Altuntaş vd.,2018). Teknolojik gelişim ve dijitalleşme siber risk sigortasına yönelik talebin ana kaynağını oluşturur. Siber sigorta ilk olarak telekomünikasyon ve medya şirketleri ve profesyonel hizmet şirketleri tarafından satın alınmıştır. Son yıllarda ise; çoğunlukla kişisel olarak tanımlanabilir bilgileri depolayan şirketler, büyük çaplı finansal işlemleri takip ve kaydını gerçekleştiren finansal kurumlar ve perakendeciler tarafından talep edildiği görülmektedir (Çotak,2019,s.74).

Orlando ve Diğ., (2017), siber sigortanın yavaş başlangıcı ve birçok soruna rağmen siber sigorta pazarının büyüdüğünü gördüklerini ve bu büyümenin, dünyada daha yaygın olarak uygulanan düzenleyici girişimcilere bağlı olduğunu ifade etmişlerdir. Ancak pazarın gelişmesinin tek nedeni bu değildir. Siber sigortanın kendisi, riskleri karşılamanın yanı sıra toplumsal refaha katkıda bulunmak için eşsiz bir fırsat sunar. Çalışmadaki karşılaştırma sonuçları, siber sigortanın acenteler için arzu edilen bir seçenek olmasına rağmen, bilim adamları ve uygulayıcılar tarafından henüz çözülememiş birçok açık sorunu olduğunu göstermiştir. Siber sigortanın toplum üzerindeki olumlu etkisinin yanı sıra piyasanın olgunlaşması için gerekli yeni standartlar ve uygulamalar için yeni yaklaşımlar ve tedaviler gereklidir. Farklı teknolojik sistemlerin siber sigortaya farklı zorluklar getirdiğini ve aynı zamanda farklı fırsatlar sunduğunu gördüklerini belirten araştırmacılar, bu nedenle siber sigortanın spesifik bağlamlarındaki ihtiyaçlarını ele almak için daha fazla araştırmaya ihtiyaç duyulduğunu belirtmişlerdir.

Siber risk sigortası veya siber güvenlik sigortası, bilişim sektöründe faaliyette bulunan firmalar ve bu sektörün ortaya çıkardığı yazılımları kullanan işletmeler, veri depolarken üzerlerine aldıkları riskleri bu poliçeler aracılığıyla ortadan kaldırabilirler. Siber risk sigortaları; işletmeler, müşterilerinin kredi kartı, hesap numara, adres ve benzeri kişisel bilgilerini bazı yazılımlarla depolamaktadırlar. Bu verilerin güvenliğinden sorumlu olan işletmeler, depolanan verilerin çeşitli yasa dışı yöntemlerle yetkisiz şahısların eline geçmesinden dolayı oluşacak zararları bu tür özel poliçeler ile karşılayabilmektedirler (egeiz.com.tr).

Siber risk sigortası, siber güvenlik veya siber korunma sigortaları olarak ifade edilen bu sigortada; siber şantajdan medya sorumluluğuna, işin durmasından siber suça kadar detaylı bir koruma sağlar (sigortateklif.net). Siber risk sigortaları; siber saldırılarla ortaya çıkan zararların, kayıpların onarılması ve bulunması, mahkeme ve bilişim masrafları, veri kayıplarıyla ilgili bilgilendirme maliyetleri, hatta itibar zedelenmesini önleyecek çalışmaları güvence altına alan bir sigorta türüdür. Ayrıca sigorta şirketleri işletmeye özel teminatları da poliçelere ekleyebilir. Her ne kadar siber sigortalar siber riski azaltıp, saldırılara karşı koruma sağlarsa da, bu saldırıların gerçekleşmeyeceğine dair bir güvence sunmaz (Şekeroğlu ve Özüdoğru, 2019, s.62).

Sektörde siber sigortalar kapsamında ağırlıkla verilen teminatlar şunlardır (sigortateklif.net, www.anadolusigorta.com.tr, www.allianz.com.tr, www.atabrokerlik.com, www.aksigorta.com.tr, phillipsigorta.com.tr, asronsigorta.com.tr);

- **Olay ve/veya Yetkisiz Girişi Müdahalesi:** Meydana gelmiş veya gerçekleştiğinden şüphe duyulan bir siber olay neticesinde; olayın nedenlerinin ve detaylarının araştırılması, yasa ve kanunlar karşısında yapılması gereken bilgilendirmeler, siber saldırı neticesi itibar korunmasına yönelik halkla ilişkiler masrafları, olayın ortadan kaldırılmasına yönelik ilave çalışmalar sonucu beliren ilave mesai giderleri poliçe kapsamındadır.
- **Eski Haline Getirme İşlemleri:** Siber olay neticesinde kaybedilen veri ve yazılımların, olayın gerçekleşmeden önceki en yakın hale getirme teminatıdır.

- **Siber Fidye:** Siber saldırının doğrudan neticesi olarak sigortalıdan yasa dışı yollarla alınan para teminatıdır**.**
- **Güvenlik ve Gizlilik İhlali:** Siber olay sonucunda, şahsi veri ve güvenlik bilgilerinin gizliliğinin ihlali nedeniyle 3. Kişilerden gelebilecek tazminat talepleri ve kişisel verilerin korunması kanununun ihlali nedeniyle sigortalıya yansıyabilecek para cezaları teminatıdır.
- **Ağ Güvenliği:** Siber olay neticesinde sigortalının bilgisayar ağlarındaki üçüncü şahısların bilgisayarlarında veri hırsızlığı, tahribat veya DoS saldırısı meydana gelmesi neticesinde 3. şahıslardan gelebilecek tazminat istekleri ve sigortalının savunma masrafları teminatıdır.
- **İş Durması:** Bu teminat isteğe bağlı bir teminattır. Sigortalının veya sigortalıya bir sözleşmeyle bağlı olan bir hizmet sağlayıcısının bilgisayar sistemlerinin, siber olay sonucunda kısmen veya tamamen devre dışı kalmasının bir neticesi olarak yaşanan iş durması nedeniyle karşı karşıya kalınan brüt kâr kaybı teminatıdır.
- **Siber Suç:** İsteğe bağlı bir teminattır. Sigortalının banka hesaplarından yasa dışı elektronik aktarım yapılması veya sigortalının bilgisayar sistemlerindeki verilerin yasa dışı olarak değiştirilmesinin bir neticesi olarak hırsızlık teminatı.
- **Ödeme Kartı-Veri Güvenliği Standartları (PCI-DSS):** İsteğe bağlı bir teminattır. PCI-DSS'e tabi olan sigortalılara yönelik, bir siber olay neticesinde PCI-DSS'in ihlal edilmesine bağlı olarak uygulanan para cezaları ve tekrardan sertifikasyon giderleri teminatı.
- **Medya Sorumluluk:** İsteğe bağlı teminat içerisinde yer almaktadır. Sigortalıya ait internet sitesi ya da sosyal medya hesaplarından bir siber olay neticesi; karalama, telif hakkı, unvan, slogan, ticari ad veya marka ihlali ya da gizlilik haklarının ihlali sonucunda sigortalıya yansıyabilecek tazminat istekleri ve savunma giderleri teminatı.

Siber Risk Sigortası prim tablosu örneği Tablo 2'de verilmiştir. Bu tabloda ana ürün teminatlarına ait prim bilgisi verilmiş, isteğe bağlı teminatlar dahil edilmemiştir.

Tablo 2. Siber Risk Prim Tablosu

	Teminat Limitleri (TL) >>	125.000	250.000	500.000	1.250.000	2.500.000
	Muafiyet Tutarı (TL) >>	2.500			7500	
	BRÜT PRİM (TL)					
YILLIK CİRO	0-2.5 mio TL	535	735	1.110	X	X
	2.5 mio TL- 5 mio TL	X	865	1.295	2.160	X
	5 mio TL- 15 mio TL	X	1.230	1.845	3.090	5.530
	15 mio TL- 35 mio TL	X	X	2.770	4.630	8.290
	35 mio TL- 50 mio TL	X	X	X	5.310	9.510
	50 mio TL ve üzeri	X	X	X	U.W	

Kaynak: https://sigortateklif.net/siber-risk-sigortasi.php

5. SİBER RİSK SİGORTASININ TÜRKİYE ÖZELİNDE İNCELENMESİ

5.1 Türkiye'de Sigortacılık Sektörünün Mevcut Durumu ve Sigortanın Önemi

Türkiye'de sigortacılık sektörü istenen seviyede gelişme gösterememiştir. Sektör, hak ettiği yerde değildir. Örneğin, dünyada sigortacılık penetrasyonu %6 oranında seyrederken, Türkiye'de bu oran dünya seviyesinin dörtte biri (%1,5) düzeyindedir (Gökşin,2018). Türkiye Sigorta Birliği Strateji Raporu'nda, Türkiye'de sigorta sektörünün geçtiğimiz beş yıllık periyoddaki (2015-2020) brüt primler dikkate alındığında %20'lik bileşik büyüme oranı ile büyüdüğü ve sigorta penetrasyonunun; hayat-dışı, hayat ve yıllık emeklilik katkı payları göz önüne alındığında %2'ler düzeyine ulaştığı belirtilmiştir. Kârlılık açısından da son yıllarda şirketlerin pozitif teknik kârlılık

sağlamada yaşadığı güçlüğü, ağırlıklı olarak yatırım gelirleri ile net kâr elde ederek aşmaya çalıştıkları görülmüştür. Sektörün mevcut durumu dört madde ile özetlenebilir (www.tsb.org.tr):

1-Talep dinamikleri güçlüdür: Türkiye demografik yapısı açısından ve ekonomik büyüme potansiyeli dikkate alındığında, sigorta sektörünün çeşitli alanlarında büyüme olanağı sunmaktadır. Nitekim Türkiye'nin nüfusu çoğu Avrupa ülkesinin nüfusundan daha gençtir. Ülkedeki nüfusun %70'inin 15-64 yaş aralığında olması, sigorta sektörünün büyük bir hedef kitlesi olduğunu ve orta vadede oluşacak talep artışına işarettir. Türkiye'deki nüfus artış oranı da (%1,5) Avrupa'daki çoğu ülkeden daha yüksektir.

2-Rekabet ve büyüyen piyasa koşulları: Türkiye'de sigortacılık sektörü geçmiş beş yılda %20 yıllık bileşik büyüme oranıyla büyümüştür. 2018 yılında bürüt primlerde 55 milyar TL'ye ulaşılmıştır. Pek çok sigorta branşında rekabetçi piyasa koşulları sağlanmış, sektöre ciddi miktarda yabancı yatırımcı çekilmiştir.

3-Teknik kârlılığa ilişkin zorluluklar: Teknik kârlılık negatif seyretmektedir. Hayat-dışı branşlarda teknik kârlılık sağlanamamaktadır. 2018 yılında hayat dışında kârlılık risksiz getiri oranı düzeyine gelmiştir. Hayat ve emeklilik branşlarında kârlılık benzer ülkelere göre yüksektir. Türk parasının göreceli değer kaybı, enflasyon gibi faktörler kârlılığı negatif yönde etkilemektedir.

4- Penetrasyon potansiyeli vardır: Türkiye'deki sigorta penetrasyonunu artırmak için fırsatlar vardır. Değişik branşlarda penetrasyonu tayin eden farklı faktörler ve penetrasyonu beklenen düzeyin üzerine çıkaran branşlara özel unsurlar ve uygulamalar göz önüne çıkmaktadır.

Türkiye'de sigortaya dair şuurun geç yerleşmeye başlaması, vatandaşların gelirinin düşük olması, serbest piyasaya geçilinceye kadarki dönemdeki sabit fiyat uygulamaları ve bu fiyatların yüksekliği nedeniyle poliçe satışlarının çok az sayıda gerçekleşmesi ve bu duruma bağlı olarak da prim üretiminin uzun yıllar yavaş bir seviyede seyri söz konusu olmuştur. Ülke kanunlarındaki değişimler sonucunda serbest piyasa ortamının gelişimine imkân sağlandıktan sonra rekabet ortamı oluşmuş ve fiyatlarda yaşanan düşüş ile birlikte poliçe satışları artmıştır. Hayat ve hayat dışı olmak üzere çok sayıda branşta poliçe satışa sunulmuştur. Fakat ülkemizde hayat sigortalarının payı, hayat dışı branşlara göre düşük seviyede kalmıştır (Çekici ve İnel, 2013:142, Özüdoğru,2017). Türkiye'de 2020 yılında şirketlerin toplam prim üretimleri 81 milyar TL olup (hayat dışı toplam 66,7 milyar TL, hayat toplamı 14,3 milyar TL), hayat dışı ürünlerin toplam pazar payı %82,5'tur (www.tsb.org.tr). Ülkemizde hayat dışı branşlarda ekonominin değişimi, yaşanan doğal afetler ve felaketler neticesinde; zorunlu deprem sigortası, zorunlu seyahat sigortası, devletin desteklediği tarım sigortası vb. sigortaların devreye alınması ile sigorta prim üretiminin hızlandırılması sağlanmıştır. Ayrıca kredi satışlarında ve kredili konut satışlarında sigorta yapılması, araç satışlarının kolaylaştırılması ile araç poliçe satışlarındaki yükseliş prim üretimini arttıran faktörler arasındadır (Çekici ve İnel, 2013:142). Türkiye için sigorta penetrasyonunu arttırma potansiyeli vardır. Sigorta penetrasyonunu etkileyen faktörleri üç ana başlık altında toplayabiliriz (www.tsb.org.tr):

1- Makroekonomik unsurlar: Gelir seviyesi, iş gücüne katılım, sigortayı karşılama gücü olan nüfusun toplam nüfus içerisindeki payı, ekonomik büyüme, nüfus artışı, kentsel nüfusun payı.

2- Devletin rolü: Risklerin gerçekleşmesi durumunda devletin üstleneceği sorumluluğun boyutu (örneğin, devletin afet finansmanındaki rolü gibi), özel sektörün rol almasını sağlamak için oluşturulan mekanizmalar (örneğin, zorunlu sigortalar, teşvikler vb.).

3- Kültürel ve coğrafi koşullar: Riskin gerçekleşme sıklığı (örneğin yüksek dolu veya fırtına riski) ve riskin büyüklüğü, risklere ilişkin farkındalık düzeyi ve ülkedeki dayanışma kültürü.

Bu kapsamda Türkiye'de, sigortaya sektörünün arzu edilen gelişim düzeyini sağlayabilmesi için; kültürel, sosyal, iktisadi ve yasal sorunların çözümüne dair çalışmalar yapılmalıdır. Gelişmiş ülkelerdeki yasal zeminin sağlamlığı, sermaye piyasalarının gelişmiş olması, eğitimli bireylerin

sayısının fazlalığı vb. nedenlerle sigorta bilincinin yerleşmesi, sektörün kolayca büyümesine, yayılmasına imkân sağlamıştır (Özüdoğru ve Çetin, 2017: s.60-21).

Günümüzde birçok ülkede sigortacılığın iktisadi kalkınma ve büyüme için çok önemli bir sektör olduğu anlaşılmış ve sektörün gelişmesine imkân sağlanarak iktisadi büyüme-kalkınma aşamalarında sigortacılıktan faydalanılmıştır. Örneğin, Türkiye'de 2020 yılında şirketler toplam 81 milyar TL prim üretmiştir. Sektörün aktif büyüklüğü ise 284 milyar TL iken, 32 milyar tazminat ödemesi ile mağduriyetleri giderdiği görülmektedir. Sektörde yaklaşık 80 bin kişi istihdam edilmektedir. Ayrıca sigortacılığın istihdamına dolaylı şekilde katkıda bulunduğu kişiler de dikkate alındığında bu sayının daha da arttığı görülmektedir. (Detaylı bilgi için bakınız Tablo 3)

Tablo 3. Sigortanın Ülkeye Sağladığı Katkılar

SİGORTANIN ROLÜ	TÜRKİYE İÇİN ÖNEMİ
Ekonomideki rolü	
* Toplumda sosyal transfer mekanizması meydana getirir. Güvenlik ve istikrar ortamı sağlar.	Zorunlu sigortalar ile sosyal transfer mekanizması oluşturur. Sosyal devlet olgusunu güçlendirir. Sağlanan güvenceler ile yeni girişimler ve inovasyon desteklenir.
***** Finansal istikrar sağlar.	Poliçeler kapsadıkları riske uygun fiyatlandırıldıkları ve yüksek yatırım riskleri üstlenmedikleri sürece sigorta şirketleri finansal istikrara katkıda bulunur.
***** İstihdam sağlar. Vergi gelirlerine katkıda bulunur.	Yaklaşık 80 bin kişi sektörde istihdam edilmektedir. Sigortacılığın istihdamına dolaylı olarak katkı yapan kişiler de dikkate alındığında bu sayı daha da büyümektedir.
Finansal sektördeki rolü	
* Ülke ekonomisine uzun vadeli kaynak sağlar, nakit akımlarını borç vadeleriyle uyumlu kılar.	Sektörün yükümlülükleri bankacılık sektöründen daha uzun vadeli olduğu için, uzun vadeli finansman gereksinimlerini karşılamak adına sigortacılık sektörü daha uygun
* Finans piyasaların gelişimine katkı sağlar.	Sigorta şirketleri finansal piyasalar arasındaki bağlantının kurulmasına katkı sunar. Borç alan kişilere ve tasarruf sahiplerine likidite olanağı sunar.
Düzenleyici rolü	
* Ülke ekonomisindeki diğer sektörlerin iyi uygulamaları benimsemelerine destek olur. Ekonomideki kayıt dışılığı azaltır.	Madencilik, tarım, trafik vb. alanlardaki risklere yönelik farkındalığın artmasını sağlar. Risklere dair sunulan teminatların koşullarını tayin eder. Zararların tazmini sistemde kayıtlı hesaplar aracılığıyla gerçekleşir.
Risk yönetimindeki rolü	
* İstenmeyen olaylara karşı kişilere ve işletmelere koruma sağlar.	Risk havuzları meydana getirerek ve bu riskleri reasürörlere ve finansal piyasalara yayarak, depremlerden ve sağlık sorunlarından kaynaklanan zararları karşılar.
* Devletin üstlendiği riskleri azaltmak için mekanizmalar oluşturur.	Devletin geçmişte üstlendiği risklere karşı güvence sağlamak için özel sektör devreye girebilir.

Kaynak: Türkiye Sigorta Birliği Strateji Raporu (2020-2024)

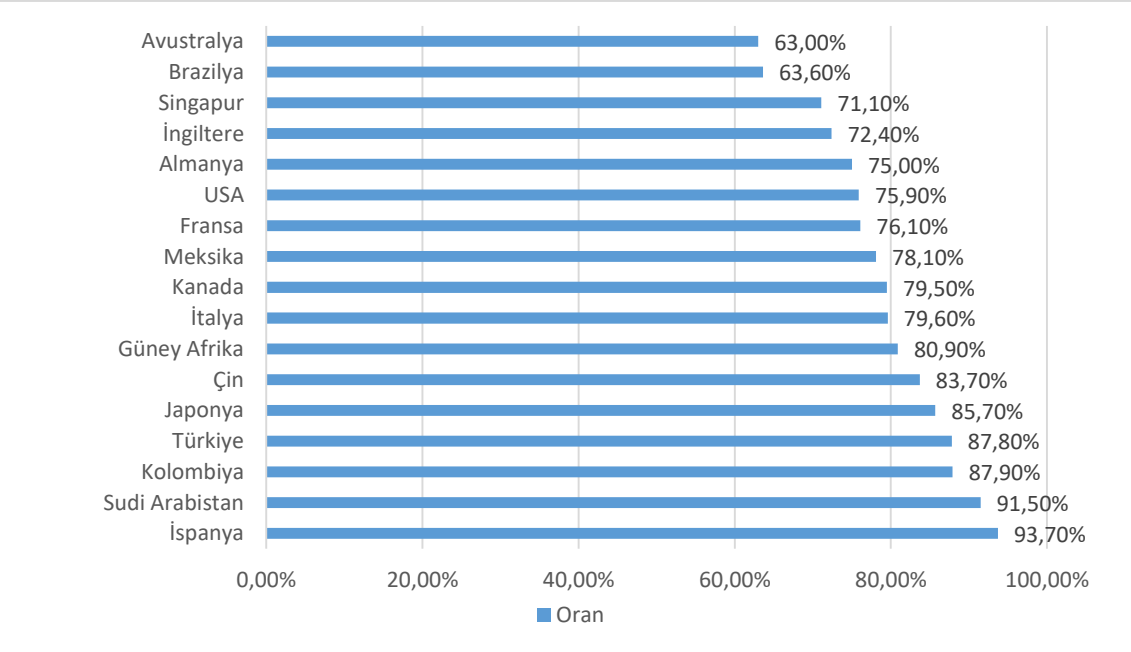
Türkiye'de ise sigortacılığın gelişmesini destekleme hususu genel olarak, sigorta şirketlerinin ticari faaliyetlerini arttırmak yönünde bir katkı olarak görülmüştür. Ülke ekonomisi için hayati bir öneme sahip olan sigortacılık sektörünün, ekonomi içindeki temel faaliyetlerini yerine getirebilmesi için ihtiyaç duyulan desteğe ve donanıma kavuşamamıştır. Türkiye'de sektörün istenen konuma ulaşamamış olmasının bir diğer nedeni de, sigortacılığın etkin bir biçimde

tanıtımının yapılamamasıdır. Bu sorun; sigorta pazarlamacılığının yetersizliği ve sigorta sektöründe istihdam edilenlerin eğitim noksanlığından kaynaklanmaktadır. Eğitime dair yaşanan sorunlar sigorta pazarlama sürecini negatif yönde etkilemektedir. Burada ilk olarak sektör çalışanlarının eğitimine öncelik ve önem verilmesi gerektiği konusu açığa çıkmaktadır. Zira sigorta ürünlerini satın alacak olan bireylerin ve/veya kurumların ürünlere dair yeterli bilgiyi çalışandan alabilmesi gerekir. Sigorta ürünlerini iyi bir biçimde tanıtacak olan bilgili, donanımlı sigorta sektörü personelidir (Özüdoğru ve Çetin, 2017: s.60-21).

İşletmelerin siber risk bilincine erişmesiyle ve siber riskleri paylaşmanın önemi artmasıyla birlikte siber risk pazarının artması beklenir. Ancak, kendi güvenlik eksiklikleri noktasında öz farkındalığı yetersiz olan işletmelerin isabetli sigorta poliçeleri satın almaları da zordur. Terminoloji eksikliği ve teminat sunma noktasındaki farklı yaklaşımlar poliçelerin karmaşıklığıyla birleşince hayal kırıklığı meydana getirmekte ve ürüne yönelik alıcı talebini azaltmaktadır. Siber riskleri modellemenin zorluğu, ürünün yeterli fiyatlandırmasını da güçleştirmektedir. İşletmelerin çoğu, bunun temel nedeninin bu konudaki uzman çalışan yetersizliğinde ve arz-talep uyumsuzluğunda görmektedir. Arz-talep uyumsuzluğu siber sigorta ürünlerinin yetersiz seviyede anlaşılmasından ve talep cephesindeki müşteriler ilgi düzeyinden kaynaklandığı söylenebilir (Çotak,2019).

5.2 Türkiye'de Siber Risk Sigortaları

Siber saldırılar nedeniyle, Türkiye için de yükselen riskler arasında siber riskler bulunmaktadır. 2019 yılı CyberEdge'in yıllık Siber Savunma Raporunda Türkiye'nin mevcut güvenlik durumuna ilişkin bilgilere yer verilmiştir. Grafik 1, ülkeler bazında son 12 ayda en az bir adet başarılı olarak gerçekleşmiş saldırı bilgisine dayanılarak hazırlanmış ve yüzde olarak sunulmuştur. Ayrıca Grafik 2'de, yıllara göre gerçekleşen saldırıların sıklığı verilmiştir.



Grafik 1. (2019 Yılı) Ülkeler Bazında Gerçekleşen Saldırı Oranları

Kaynak: 2019 Cyberthreat Defense Report, Çevrimiçi Erişim Tarihi: 31.01.2021, https://www.imperva.com/resources/reports/CyberEdge-2019-CDR-Report-v1.1.pdf

Grafik 2. Yıllar İtibarıyla Başarılı Olarak Gerçekleşen Saldırıların Sıklığı

Kaynak: 2019 Cyberthreat Defense Report, Çevrimiçi Erişim Tarihi: 31.01.2021, https://www.imperva.com/resources/reports/CyberEdge-2019-CDR-Report-v1.1.pdf

Telekomünikasyon Birliği Global Siber Güvenlik Endeksi Raporu'na göre dünyada en çok siber saldırıya uğrayan ülkeler arasında Türkiye ilk üçte yer almaktadır. Siber saldırıların düzenlendiği ülkeler arasında; Amerika, Çin, Yunanistan ve Rusya başta yer almaktadır (yenisafak.com). Siber saldırılar kapsamında hazırlıklarını devam ettiren Türkiye'de, 2014 yılında "Ulusal Siber Olaylara Müdahale Merkezi" (USOM, TR-CERT) kurulmuştur. 10.02.2020 tarihinde de fiziki olarak "Ulusal Siber Olaylara Müdahale Merkezi" hizmete girmiştir. Türkiye'ye yönelik yapılan siber saldırılar 2016 yılında 9000'i bulmazken, 2019 yılında bu rakam 136.000'i aşmıştır (https://eng.btk.gov.tr).

İçişleri Bakanlığı'nın 2020 yılı yaptığı araştırma raporuna göre; COVID-19 salgın döneminde halkın en çok maruz kaldığı siber suç türü "zararlı yazılım bulaşması" olmuş ve salgın döneminde, sosyal izolasyon sürecinde en az bir siber suç mağduru olanların oranı %7,1 olarak belirlenmiştir (trthaber.com).

Türkiye'de özel sektör şirketlerinin siber risklere olan bakış açılarını tespite yönelik yapılan "2020 Türkiye Siber Risk Algı Araştırması[5]" sonuçlarına göre, işletmelerin %78'i siber saldırı olmadan bu hususta harekete geçmediği belirlenmiştir. Siber risklere dair işletmelerin farkındalıklarının düşük olması, konunun üst yönetim tarafından yeterli düzeyde ele alınmamasına dayandırılabilir. Ayrıca yaşanan siber saldırıların, şu ana dek; işlerin durması, yavaşlaması ya da finansal kayıplara neden olabilecek durumların yaşanmasına sebep olmaması, siber güvenlik konusunun göz ardı edilmesinin nedeni olarak da görülmektedir (www.bloomberght.com). Türkiye'de risk yönetimi ve bilgi teknolojilerinde yetkili pozisyonda görev yapanların %9'u kurum için en ciddi riskin siber riskler olduğu kanısındadır. 2019'daki benzer katılımcı kitlesiyle yapılan Global Siber Risk Algı Araştırması'nda bu oran %22'ler seviyesinde ve raporda siber risklerin gün geçtikçe daha da önem kazandığı belirtilmiştir. Bu bulgular Türkiye'nin siber risk farkındalığı adına (Tablo.4) henüz küresel şirketlerin oranına ulaşamadığını göstermektedir (mars.com.tr).

[5] Bu araştırma; Marsh ve TUSİAD iş birliğinde gerçekleştirilmiştir. Türkiye'deki firmaların siber risklere bakış açılarına, siber yönetim yaklaşımlarına ve bu kapsamdaki yatırım tercihlerine, dijital tedarik zincirine ve kamu politikalarına dair iç görü elde etmek hedeflenmiştir.

Tablo 4. Siber Risk Farkındalığı Algısı

Soru: Şirketiniz için en önemli bulduğunuz 5 risk başlığını önem sırasına göre belirtiniz.		
	En Önemli Risk Faktörü	Önemli Bulunan Tüm Risk Faktörleri
Ekonomik belirsizlik	%19	%65
Endüstriyel iş kazası	%14	%34
Siyasi istikrarsızlık/savaş	%13	%51
Siber saldırılar ve tehditler	% 9	%61
Doğal felaketler	%8	%34
Kredi ve likidite riski	%8	%32
Marka/itibar zedelenmesi	%8	%48
Tedarik zincirinde aksaklıklar	%6	%38
Kilit personelin kaybı	%4	%30
Ürün kalite problemleri	%4	%31
Suç unsuru taşıyan fiziksel eylemler	%2	%9
Yönetmelik ve yasa değişmelerine adaptasyon	%2	%30
Terörizm	%1	%13
Sanayi casusluğu/ fikri mülkiyet hırsızlığı	%1	%11

Kaynak: https://www.marsh.com/tr/tr/insights/research-briefings/2020-turkey-cyber-risk-perception-survey.html

Araştırmaya katılan işletmelerden, siber güvenlik yönetimine yatırım yapanların %77'si hukuki düzenlemelerin teşvik edici etkisi olduğunu düşünmektedir. Finans, havacılık, bilgi teknolojileri, enerji ve üretim sektörlerindeki firmaların siber riskin yönetimi hususunda nispeten daha bilgili oldukları belirlenmiştir. Devletin yasa ile çerçevesini çizdiği, izlediği konular işletmeler tarafından daha çok dikkate alınmaktadır. Bu kapsamda KVKK, GDPR gibi kanunlar; ISO gibi standartlar; EPDK, BDDK gibi sektör denetleme kurumları; halka açılma süreçlerinden geçen kurumlar için SPK tarafından belirlenen zorunluluklar firmaların siber risk hususunda harekete geçmesini etkilediği de görülmektedir (mars.com.tr).

İşletmelerin %78'inin siber risk yönetimi konusundaki ilk refleksi, riski azaltıcı uygulamaları devreye sokmak yönünde gerçekleşmektedir. İşletmelerin en fazla cihazların güvenliğini arttırmaya, sisteme ya da ağlara şirket içinden ve dışından erişimi daha güvenli kılmaya yönelik yatırımlar yaptıkları görülmüştür. İşletmelerin %50'si siber riski ölçme, yönetme ve önleme süreçlerine yönelik; altyapı, organizasyon ve insan kaynakları gibi belirgin alanlara yatırım yapma konusunda çekimser davranmaktadır. Bir diğer önemli tespit de; işletmelerin siber güvenlik alanındaki olgunlukları siber risk sigortasına yatkınlıklarını pozitif yönde etkilediğidir. Siber risk sigortası konusunda firmaların çoğunun yeterli bilgisi olmadığı da belirlenmiştir (bloomberght.com; mars.com.tr).

Tablo 5. Siber Risk Sigortası Farkındalığı

Soru: Şirketiniz siber risk sigortası ile ilgili olarak mevcut durumu nedir?		
Şu anda bir sigorta poliçemiz var ve mevcut kapsamı yenilemeyi planlıyoruz.	%23	**%33** (SİBER RİSK SİGORTASI SAHİPLİĞİ)
Şu anda bir sigorta poliçemiz var ve kapsamını/limitini veya her ikisini birden genişletmeyi planlıyoruz.	%4	
Şu anda bir poliçemiz var fakat yenilemeyi planlamıyoruz	%6	
Siber risk sigortamız yak fakat önümüzdeki 12 ay içerisinde satın almayı planlıyoruz.	%19	
Siber risk sigortamız yok ve önümüzdeki 12 ay içerisinde satın almayı planlamıyoruz.	%23	
Bilmiyorum/Fikrim yok	%25	
Siber risk sigortası sahipleri içerisinde, mevcut sigorta sahiplik durumunu bilenlerin oranı %43		

Kaynak: https://www.marsh.com/tr/tr/insights/research-briefings/2020-turkey-cyber-risk-perception-survey.html

Altuntaş ve Diğ. (2018) tarafından gerçekleştirilen çalışmada; Türk sigortacılık sisteminin, siber risklere yönelik güvence sağlama hususundaki etkinliği sınanmak istenmiştir. Bu kapsamda 2016 yılında Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı'nın gerçekleştirdiği "Siber Sorunlar: Son Gelişmeler, Uygulamalar ve Sorunlar" adlı proje temel alınarak, projede kullanılan metot ve soru formu birebir paralel şekilde, araştırma ekibi tarafından Türkiye'de de uygulanmıştır. Bu çerçevede Türkiye'de siber riskler hususunda aktif şekilde çalışan şirket yöneticileriyle yarı yapılandırılmış görüşme tekniğinden yararlanılarak ve "Risk Management Forum 2015" da konuşmaların söylem analizi yapılarak siber risklerle mücadelenin etkinliği tespit edilmeye çalışılmıştır. Neticede Türkiye ve Avrupa Birliği (AB) sigorta şirketlerinin risk algıları ve risk değerlendirme bakış açıları arasında çok büyük farklılıklar olmadığı belirlenmiştir. Fakat Türkiye'deki siber risklerin neden olacağı sorunlara dair işletmelerin farkındalığının AB'den farklılık gösterdiği görülmüştür. Türkiye'de siber uygulamaların gelişimi her ne kadar gelişmiş ülkelerle paralel seyretse de bu siber uygulamalar sonucunda belirecek risklere dair farkındalık ve risk algısı henüz düşük düzeyde seyrettiği belirlenmiştir.

Türkiye'deki bireysel risk algısının görece düşük olmasından siber riskler de nasibini almıştır. Bu durumun, sigortacıların bu türden risklere dair teminat sunmalarında birtakım kısıtlar oluşturacağı düşünülmektedir. Riskin yönetimi veya mümkün zararlardan korunmak ve önlem almak, ilk etapta sigortalı bilincinin ve risk farkındalığının yüksek olmasına bağlıdır. Bu nedenle toplumsal olarak risk farkındalığı oluşturulmadığı sürece sigortacılar için siber sigortaların sürdürülebilir olması zorlaşmaktadır (Altuntaş ve Diğ., 2018, s.20).

Altuntaş ve Diğ. (2018) çalışmasındaki yapılan görüşme sonuçları göstermektedir ki; sigortacılar hem işletmeler içerisinde yeterli teknik beceriye sahip personel noksanlığından, hem de üst yönetim ve diğer çalışanların farkındalığının yetersizliğinden dolayı siber sigorta ürününü satmaktan çekinmektedirler. Hâlbuki AB ülkelerinin çoğunda bu sigorta ürününün satışı artmaktadır. Bu nedenle ülkemizde bu konudaki çabaların henüz karşılığını bulduğunu söylemek güçtür. Ayrıca çalışmanın Türkiye uygulamasından elde edilen neticeler bilhassa risk analizinin sigortacının soru formuyla başladığını ve işletme sahiplerine sorulan sorularla risklerin açığa çıkarıldığı bir durumu ortaya koymaktadır. Bu hususta belirlenecek açıkların sabit kıymetlerinde, sorumluluklarında bilhassa kâr kaybında meydana getireceği hasarların sigortacılar tarafından işletme sahiplerine raporlanarak risk farkındalığı oluşturulmaktadır. Bunun en zayıf yönü, farkındalık analizinin müşterinin izin verdiği nispette gerçekleşebiliyor olmasıdır. Fakat tam

tersine AB sigortacılık sistemi özellikle siber riske maruz kalacak işletmelerin hali hazırda bir risk yönetimi sistemine, politika ve prosedürlerine sahip olunmasını mecbur kılmaktadır. Daha net bir ifadeyle sigorta satılacak bir işletmenin öncelikle risk yönetimi ve politikasına sahip olması zorunludur.

Dünyada beliren siber risklerin ve saldırıların artmasına istinaden bireysel, kurumsal ve devlet bazında fiziki ve teknik tedbirler alınmaya başlanmıştır. Bu tedbirlerin yeterli olamayacağı ve akabinde oluşacak risklerin de tahmin edilemeyecek başka riskleri ortaya çıkarabileceği ortak bir kanaat olarak belirtilmektedir. Bu kapsamda gereksinime konu olan sigorta hizmeti, belirecek bir tehdidi önleme mekanizmasına sahip olmamakla birlikte, saldırı neticesinde oluşan riske teminat sağlama nedeniyle tercih edilen bir koruma yönetimidir. Siber risklere yönelik olarak geliştirilen siber sigorta hizmeti 1997 yılında kullanıcısına sunulmaya başlanmış ve dünyada yayılımı zaman almıştır. Halen gelişmeye devam eden bu hizmet, ülkelerde farklı teminat kapsamları ile sunulmaktadır. Teminat kapsamlarındaki farklılıklara rağmen genellikle koruma kapsamında alınan hizmetler; itibar kaybı, kimlik hırsızlığı, danışmanlık hizmeti, veri korunması ve maddi kayıpların karşılanması şeklindedir (Çotak,2019).

Tablo 6'da, Türkiye'de sigorta hizmeti veren kurumlardan bazılarının siber risklere yönelik, siber riskler kapsamında sundukları ürün ve teminat bilgileri kısaca özetlenmiştir. Genel olarak Türkiye'de; siber fidyeden (şantajdan) medya sorumluluğa, iş durmasından siber suça kadar detaylı teminatlar ve talebe bağlı teminatlar ile poliçelerini genişletme olanağı sunulduğu görülmektedir. Stratejik olarak kurum yapısını kuvvetlendiren, uluslararası platformlarda geçerli poliçelerle mali gücü destekleyen, umulmayan zamanlarda beliren davalarda işletme sorumluluklarını teminat altına alan, siber risklerin arttığı dönemlerde kurum ve kuruluşları yarı yolda bırakmayan farklı kombinasyondaki talepleri karşılayan ürünler sunulmaktadır.

Tablo 6. Türkiye'de Sigorta Hizmeti Veren Bazı Kurumların Siber Risk Ürünleri

KURUM	ÜRÜN ADI	TEMİNATLAR							
		Eski haline getirme	Siber fidye	Güvenlik ve gizlilik ihlali	Ağ Güvenliği	İş Durması	Siber suç	Ödeme kartı-Veri güvenliği	Medya Sorumluluk
Aksigorta	Siber Korunma Sigortası	x	x	x	x	x	x	x	x
Anadolu Sigorta	Ticari Siber Güvenlik Paket	x	x	x	x	x	x	x	x
Ata Sigorta	Siber Risk Sigortası	x	x	x	x	x	x	x	x
Allianz	Siber Sorumluluk Sigortası	x	x	x	x	x	x	x	x
Phillip Sigorta	Ticari Siber Güvenlik	x	x	x	x	x	x	x	x
Asron Sigorta	Siber Sigorta	x	x	x	x	x	x	x	x

Kaynak: www.anadolusigorta.com.tr, www.allianz.com.tr, www.atabrokerlik.com, www.aksigorta.com.tr, phillipsigorta.com.tr, asronsigorta.com.tr adreslerinden edinilen bilgilerle derlenmiştir.

İşletmelere yönelik siber risk sigortalarının yanı sıra bireyleri de siber risklere karşı korunmaya yönelik sigorta ürünleri bulunmaktadır. Örneğin RaySigorta'nin "Cyberella" isimli ürünü, 18-70 yaş grubundaki kişileri hem sanal hem de gerçek kimlik hırsızlığına yönelik güvence altına alır. Bu ürün, sigortalının hasarı olmadan da önleyici asistans hizmetleri ile korunmasını sağlar. "Cyberella" şu durumları koruma altına alır: * Kimlik hırsızlığı/ sahtekârlığı durumlarında yapılan harcamalar, * kimlik çalınması/ kaybolması sonrasında yapılan yenileme harcamaları, *ATM kapkaç/ gasp olayları, *kişisel şifrelerin çalınması (çevrimiçi bankacılık hizmetleri, finansal kurumlara ait internet hesapları, banka ve kredi kartları vb.), *hukuki süreçler (raysigorta.com.tr).

Bir diğer örnek olarak Anadolu Anonim Türk Sigorta Şirketinin "Bireysel Siber Güvenlik Sigortası" verilebilir. Bireysel Siber Güvenlik sigorta poliçesiyle sigortalının kimlik hırsızlığına uğraması, ödeme araçlarının hileli ya da kötüye kullanımı, yaşadıkları çevrimiçi alışveriş anlaşmazlıkları ve sanal alemde saygınlıklarına zarar durumunda destekle bu süreçlerde gerekli olması halinde hukuki danışmanlık verilmesi gibi hizmetler sunulmaktadır (www.anadolusigorta.com.tr).

6. SONUÇ VE DEĞERLENDİRME

Günümüzde bilgi ve iletişim teknolojilerindeki gelişmelerle birlikte yaşantımıza girmiş olan birçok teknolojik ürün, çevrimiçi sistemle birlikte sanal alemin risklerini de beraberinde getirmiştir. Yeni siber tehditler, siber suç çeşitleri gün geçtikçe artmıştır. Dünya üzerindeki yaşanan bu sanal suçlar ülkeleri ekonomik açıdan ciddi ölçüde sarsmaktadır.

Ülkemizde siber risklerle ilgili farkındalık gün geçtikçe artmasına rağmen, artan siber riskleri işletmelerin kendi öncelikleri arasına yeterli düzeyde almadıkları da görülmektedir. Marsh ve TÜSİAD'ın iş birliği ile gerçekleştirdikleri araştırmanın bulguları da bunu destekler niteliktedir. Türkiye'deki siber risklere karşı genel tutum "bekle-gör" şeklinde olup, özellikle firmaların %78'inin tehditle karşılaşmadan siber riski fark etme ve harekete geçme pratiğine sahip olmadıkları söylenebilir. Bu şu demektir: işletmeler için deneyimlenen saldırının etki gücü siber saldırı öngörüsünden daha yüksektir. Yaşanan siber saldırıların, günümüze kadar; işlerin aksaması; durması veya iktisadi zarara neden olabilecek bir vaka meydana getirmemiş olması, siber güvenlik konusunun daha az gündemde tutulmasının ana nedeni olarak görülebilir. Ayrıca firmaların büyük bir çoğunluğu ülkedeki hukuki düzenlemelerin teşvik edici etkisinin olduğu görüşündedir. Sektör olarak; havacılık, bilgi teknolojileri, finans, enerji ve üretim sektörlerindeki firmaların siber riskin yönetimi konusuna nispeten daha duyarlı oldukları ve bilgi sahibi oldukları söylenebilir. Devletin yasalar koyduğu, takip ettiği konular işletmelerce daha fazla dikkate alınmaktadır. Dolayısıyla kanunlar, standartlar ve sektör denetleyen ve düzenleyen kurumlar tarafından tayin edilen zorunluluklar işletmelerin siber risk hususunda harekete geçmesini etkilemektedir.

COVID-19 salgınının tesiri ile birlikte birçok alanda hızlanan dijital dönüşümün hem farkındalığı arttıracağı hem de kurumları siber risk yönetimine yönelik daha fazla önlem almaya teşvik edeceği öngörülmektedir. COVID-19 salgını nedeniyle ülkemizdeki birçok firmanın tam olarak gerekli önlemleri alamadan ivedi bir şekilde dijitalleşmesi, siber saldırı olasılıklarını da yükseltmiştir. Bu durum firmaların siber risk sigortasına eğilimlerini pozitif yönde etkilemektedir. Siber risk sigortası yaptırılmasının önündeki en önemli engeller; bu sigortalara yönelik bilgi yetersizliği ve sigortaya yönelik duyulan güvensizliktir. Ayrıca bu alanda çalışan uzman kişi sayısının arttırılması ile birlikte sigorta mevzuat ihtiyacı dikkat çekmektedir. Siber Sigortacılık alanında pazarın yaşadığı engellere dair şu öneriler paylaşılabilir (Çotak,2019,s.158-160):

- Siber atak, risk ve korunma hakkında etkin bilgi birikiminin oluşturulması ve sigorta primlerinin isabetli olarak hesaplanabilmesi,
- Asimetrik bilginin giderilmesiyle poliçe karşılaştırılmasının yapılabilmesi,
- Siber atak veri tabanının oluşturulması,

- Siber atakların işletme ve bireysel kapsamı dışında, ülke güvenliği faaliyeti olarak da görülmesi ve devletin reasürör olarak devrede olması,
- BT güvenlik uzmanlarıyla sigorta şirketlerinin eş zamanlı çalışma gerçekleştirmesi yoluyla siber atak ve siber riskin kapsamının net olarak belirlenmesi,
- İşletmelere hangi sektörden olurlarsa olsun, ayırım yapılmadan siber risklere dair bilgiler verilmesi,
- Saldırı kayıplarına dair aktüerya veri eksikliğinin giderilmesi,
- Güvence altına alınan riskler düşünüldüğünde poliçe maliyetlerinin bir yük olarak görülmemesi gerektiği anlayışının yaygınlaştırılması, dolayısıyla sigortanın genel olarak gerekli olduğu anlayışının yaygınlaştırılması,
- "Genel Veri Koruma Yönetmeliği" gibi yasaların devreye girmesiyle piyasaya düzenleyici bir etki sağlanması ve sigorta sektörünü desteklenmesi,
- Çalışanların düzenli olarak eğitimlere tabi tutulması ve bu sektörde uzman bireylerin istihdamının sağlanması,
- Gerçekleşen saldırıların noksansız olarak bilgisinin paylaşılmasıyla riskin karmaşık yapısının aşılması sağlanmalıdır.

Siber sigortacılık, olumlu ve olumsuz yönleri ile birlikte günümüzde gelişmeye açık bir sigorta alanıdır. Küresel alandaki ilerlemesine paralel olarak, Türkiye'de de bu alanın gelişimi için, siber sigortacılık pazarında arz-talep cephesine yönelik çalışmaların ivedilikle yapılması gerekmektedir.

KAYNAKÇA

Airehrour, D., Nair, N.V. ve Madanian, S. (2018). "Social Engineering Attacks and Countermeasures in the New Zealand Banking System: Advancing a User-Reflective Mitigation Model", Information 2018, Vol.9, No.110, ss.1-18.

Alataş, Ş. ve Atan, M. (2007). Phishing: İnternet Denizinin Popüler Avlanma Yöntemi, XII. Türkiye'de İnternet Konferansı, Bilkent Üniversitesi, Ankara, 8-10 Kasım 2007, 226-236.

ALLİANZ: https://www.allianz.com.tr/tr_TR/urunler/diger-urunler/sorumluluk-sigortalari/finansal-sigortalar.html , Erişim tarihi: 25.12.2020.

Altuntaş, E.; Kara, E.; Soylu, A.B. ve Kırkbeşoğlu, E. (2018). Siber Sigortalar: Son Gelişmeler, Uygulamalar ve Sorunlar. Bankacılık ve Sigortacılık Araştırmaları Dergisi, Sayı:12, 8-22.

AKSİGORTA, https://www.aksigorta.com.tr/urunler/kurumsal-urunler/diger-sigortalar/siber-koruma-sigortasi, Erişim tarihi: 25.12.2020.

ANADOLU SİGORTA, https://www.anadolusigorta.com.tr/ticari-siber-guvenlik-paket-policesi, Erişim tarihi: 25.12.2020.

ASRON: http://www.asronsigorta.com.tr/insurance-products/finansal-sigortalar-kredi-sigortalari/, Erişim tarihi: 25.12.2020.

ASSETS PUBLISHING SERVICE- UK (2011). " The UK Cyber Security Strategy: Protecting and promoting the UK in a digital World" , https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf

ATA SİGORTA VE RESÜRANS BROKERLİĞI A.Ş. "Siber Risk sigortası", https://www.atabrokerlik.com/siber-risk-sigortasi/ , Erişim tarihi: 23.12.2020.

AVAST: "What is cracking? It's hacking, but Evil". https://www.avast.com/c-cracking , Erişim tarihi: 23.12.2020.

Baykız, M. S. ve Tanrıöven, C. (2019). "Küçük ve Orta Büyüklükteki İşletmelerde Bilgi Güvenliği", Üçüncü Sektör Sosyal Ekonomi Dergisi, Cilt:54, Sayı:1, 478-501.

Bayraktar, G. (2014). Harbin Beşinci Boyutunun Yeni Gereksinimi: Siber İstihbarat. Güvenlik Stratejileri Dergisi, Cilt:10, Sayı:20, 119-147.

Bensghır, (2011). "Kurumsal Bilgi Güvenliği Yönetim Süreci". TODAİE eDevlet Merkezi Bilgi Yönetim Semineri 23 Kasım 2011, http://strateji.deu.edu.tr/wp-content/uploads/2014/09/Kurumsal-Bilgi-G%C3%BCvenli%C4%9Fi-Y%C3%B6netim-S%C3%BCreci.pdf, Erişim tarihi:14.12.2020.

Berr, J. (2017). "WannaCry" ransomware attack losses reach $4 billion. https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/, Erişim tarihi 20.12. 2020.

BİLGİ GÜVENDE: "Nesnelerin İnterneti (IoT) ve Siber Tehditler" https://bilgiguvende.com/nesnelerin-interneti-iot-ve-siber-tehditler/, Erişim tarihi: 21.12.2020.

BİLGİ TEKNOLOJİLERİ VE İLETİŞİMİ KURUMU; "Cumhurbaşkanı Erdoğan: Yerli 5G Teknolojisi Altyapısını Kurmadan 5G'ye Geçemeyiz". https://eng.btk.gov.tr/haberler/cumhurbaskani-erdogan-yerli-5g-teknolojisi-altyapisini-kurmadan-5g-ye-gecemeyiz , Çevrimiçi erişim tarihi:23.12.2020

BİLİŞİM İNOVASYON DERNEĞİ: "Fidye Yazılımları". http://www.bilisiminovasyon.org.tr/tr/main/blog/fidye-yazilimlari/3#:~:text=%C4%B0lk%20bilinen%20fidye%20yaz%C4%B1l%C4%B1m%C4%B1%201989,dosyalar%C4%B1%20%C5%9Fifreleyen%20yaz%C4%B1l%C4%B1mlar%20gittik%C3%A7e%20yayg%C4%B1nla%C5%9Ft%C4%B1 ,Erişim tarihi: 21.12.2020.

BLOOMBERGHT: "2020 Türkiye Siber Risk Algı Araştırması Sonuçları Açıklandı". 7 Temmuz 2020 tarihli haber, https://www.bloomberght.com/2020-turkiye-siber-risk-algi-arastirmasi-sonuclari-aciklandi-2259609, Çevrimiçi erişim tarihi: 23.12.2020.

Böhme, R. (2005). Cyber-Insurance Revisisted. Workshop on the Economics of Information Security (WEIS), Kennedy School of Government, Cambridge, MA, USA.

Choo K-K R. (2011). "The cyber threat landscape: Challenges and future research directions. Computers & Security, Sayı: 30, No:8, ss. 719–731.

Çatak, F. Ö. (2016). "Bilgi Toplama ve Sosyal Mühendislik", http://www.ozgurcatak.org/files/sosyal_muhendislik_1.pdf, Erişim tarihi: 27.12.2020

Çekici, M. E. ve İnel, M. N. (2013). Türk Sigorta Sektörünün Direkt Prim Üretimlerinin Tahmin Teknikleri ile İncelenmesi. Marmara Üniversitesi İ.İ.B. Dergisi, Cilt XXXIV, Sayı I, 135-152.

Çotak, A. (2019). *Sigortacılık Sektöründe Siber Güvenliği, Dünyada ve Türkiye'deki Gelişmelerin İncelenmesi*.(Yayınlanmamış yüksek lisans tezi). Marmara Üniversitesi Bankacılık ve Sigortacılık Enstitüsü Anabilim Dalı, İstanbul.

Darıcılı, A. B. ve Özdal, B. (2017). Rusya Federasyonu'nun Siber Güvenlik Kapasitesini Oluşturan Enstrümanların Analizi. Bilig, Sayı:83, 121-146.

Dobran, B. (2019) "27 Terrifying Ransomware Statistics & Facts You Need To Read'', https://phoenixnap.com/blog/ransomware-statistics-facts , Erişim tarihi: 20.12.2020.

Doyduk, H.B.B. ve Tiftik, C. (2017). Nesnelerin İnterneti: Kapsamı, Gelecek Yönelimi ve İş Fırsatları, Üçüncü Sektör Sosyal Ekonomi Dergisi, Cilt:52, Sayı:3,127-147.

EGEİZ: "Bilişim/Cyber Sigortaları" https://www.egeiz.com.tr/urunler/isletme-sigortalari/hayat-sigortalari , Erişim tarihi: 22.12.2020.

ESET TÜRKİYE: https://www.eset.com/tr/ransomware/ Erişim tarihi: 20.12.2020

Gökşin, O. D. (2018). "Ülkemizde Penetrasyon Dünya Seviyesinin Dörtte Biri, https://sigortacigazetesi.com.tr/ulkemizde-penetrasyon-dunya-seviyesinin-dortte-biri/, Erişim Tarihi: 30.01.2021.

Görmüş S., Aydın H. ve Ulutaş, G. (2018). "Nesnelerin İnterneti Teknolojisi İçin Güvenlik: Var Olan Mekanizmalar, Protokoller ve Yaşanılan Zorlukların Araştırılması", Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi, Cilt:33,Sayı:4,1247-1272.

Gündüz, M. Z., Daş. R. (2014). "Sosyal Mühendislik: Yaygın Ataklar ve Güvenlik Önlemleri", 9. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı 17-18 Ekim 2014, İTÜ, İstanbul.

Güntay, V. (2017). Uluslararası Sistem ve Güvenlik Açısından Değişen Savaş Kurgusu; Siber Savaş Örneği. Güvenlik Bilimleri Dergisi, Cilt:6, Say:2, 81-108.

Hekim, H. ve Başıbüyük, O. (2013). "Siber Suçlar Ve Türkiye'nin Siber Güvenlik Politikaları", Uluslararası Güvenlik ve Terörizm Dergisi, Cilt:4, Sayı:2, 135–158.

IMPREVA, "Social Engineering'' https://www.imperva.com/learn/application-security/social-engineering-attack/, Çevrimiçi erişim tarihi: 22.12.2020.

Irmak, H. ve Reis, Z. A. (2018). "Sosyal Mühendislik Saldırılarına Karşı Web Tabanlı Bir Farkındalık Eğitimi". 7th International Conference on "Innovations in Learning for the Future: Digital Transformation in Education Future-Learning 2018, September 11-14, İstanbul.

Kalelioğlu, E. (2019). "WannaCry Saldırısının Üstünden İki Yıl Geçse de Hâlâ Milyonlarca Bilgisayar Risk Altında'', https://www.webtekno.com/wannacry-saldirisinin-ustunden-iki-yil-gecse-de-h-l-milyonlarca-bilgisayar-risk-altinda-h68524.html Erişim tarihi: 20.12.2020.

KAREL: "Internet of Things (Nesnelerin İnterneti) Nedir? Cihazların Etkileşim Trendleri'', https://www.karel.com.tr/blog/internet-things-nesnelerin-interneti-nedir-cihazlarin-etkilesim-trendleri, Erişim tarihi:21.12.2020.

Karlof C. ve Wagner D. (2003). "Secure routing in wireless sensor networks: attacks and countermeasures". Ad Hoc Networks 1 (2003), 293–315.

Kasapoğlu, C. (2017). "Siber Güvenlik: Beşinci Boyutu Anlamak", EDAM Siber Politikalar Kağıtları Serisi 2017/1, https://edam.org.tr/wp-content/uploads/2017/10/besinciboyut.pdf, Erişim tarihi:27.01.2021.

Kharraz, W. Robertson, D. Balzarotti, L. Bilge and E. Kirda (2015). "Cutting the gordian knot: A look under the hood of ransomware attacks," In International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA 07,2015), ss. 3–24.

Kılınççeker, Görkem (2018). "*Değişen Paradigmalar Doğrultusunda Siber Tehditlerin Savunma Planlamalarındaki Dönüşüme Etkisi*", (Yayınlanmamış yüksek lisans tezi), Yıldız Teknik Üniversitesi, Sosyal Bilimler Enstitüsü İşletme Ana Bilim Dalı, Savunma Kaynakları Yönetimi, İstanbul.

Korkmaz, I., Dagdeviren, O., Tekbacak, F. ve Dalkilic, M. E. (2012). A Survey on Security in Wireless Sensor Networks: Networks: Attacks and Defense Mechanisms. http://akademik.ube.ege.edu.tr/netos/source/publications/igi12.pdf, Erişim tarihi: 22.12.2020

Kotan, Y. (2020). Sigortacılık Sektörünün Gelişimi ve Dijitalleşmesi Sürecinin SWOT Analizi: Erzurum İli Üzerine Bir Araştırma. Ekonomi Bilimleri Dergisi, Cilt (12), No (2), 179-192.

Krombholz, K., Hobel, H., Huber, M. ve Weippl, E. (2014). Advanced social engineering attacks. Journal of Information Security and Applications, file:///C:/Users/uzay/Downloads/jisa_revised.pdf , Çevrimiçi erişim tarihi: 19.12.2020.

MARSH: "2020 Türkiye Siber Risk Algı Araştırması" https://www.marsh.com/tr/tr/insights/research-briefings/2020-turkey-cyber-risk-perception-survey.html, Çevrimiçi erişim tarihi: 25.12.2020.

Mohurle, S. ve Patil, M. (2017). "A brief study of Wannacry Threat: Ransomware Attack 2017". International Journal of Advanced Research in Computer Science, Sayı:8, No.5, ss.1938-1940.

Orend, B. (2014). Fog in the Fifth Dimension: The Ethics of Cyber-War. In: Floridi L., Taddeo M. (eds) The Ethics of Information Warfare. Law, Governance and Technology Series, Vol 14. Springer.

Özgül, I. (2017). "Sosyal Mühendislik Nedir ve Nasıl Korunulur?" Çevrimiçi erişim: https://teknobolge.com/nedir/sosyal-muhendislik-nedir-ve-nasil-korunulur, Erişim tarihi: 15.12.2020.

Özüdoğru, H. (2017). "Türkiye Sigortacılık Sektörünün Değerlendirilmesi". Bankacılık ve Finansal Araştırmalar Dergisi (BAFAD), Cilt:4, Sayı:1, 38-47.

Özüdoğru, H. ve Çetin, Ç. (2017). "Türkiye'de Sigortacılıkta Güncel Sorunlar", Üçüncü Sektör Sosyal Ekonomi Dergisi, Cilt:52, Sayı:2, 57-70.

PHILLIP SİGORTA: https://phillipsigorta.com.tr/siber-risk-veri-koruma-sigortasi/ , Çevrimiçi erişim: 24.12.2020.

RAY SİGORTA, "Cyberella", https://www.raysigorta.com.tr/Product/Detail/11595/cyberella, Çevrimiçi erişim: 24.12.2020.

RETRUSTER, "2019 Phishing Statistics and Email Fraud Statistics", https://retruster.com/blog/2019-phishing-and-email-fraud-statistics.html , Erişim tarihi:22.12.2020

SABAH: "İşte Çin'in Gizli Ordusu" , https://www.sabah.com.tr/dunya/2011/05/27/cin-super-gizli-ordusunu-acikladi, Erişim Tarihi:27.01.2021.

Sanders, J. (2018). "Ransomware: A cheat sheet for professionals", https://www.techrepublic.com/article/ransomware-the-smart-persons-guide/, Erişim tarihi:25.12.2020

SİGORTA TEKLİF: "Siber Risk Sigortası", https://sigortateklif.net/siber-risk-sigortasi.php, Erişim tarihi: 23.12.2020.

Şekeroğlu, S. ve Özüdoğru, H. (2019). Dijital Dönemin Koruyucuları: Siber Risk Sigortaları. 4. International Research Congress on Social Sciences (USOBAK 11-13 September 2019), 55-64.

Şenol, A. ve Karacan, H. (2012). "Savan Avlama (Phishing): Kullanılan Teknikler ve Bunlardan Korunma Yöntemleri". *5. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı,* https://www.researchgate.net/profile/Ali_Senol/publication/269405477_Sazan_Avlama_Phishing_Kullanilan_Teknikler_ve_Bunlardan_Korunma_Yontemleri/links/5d908491299bf10cff1888e7/Sazan-Avlama-Phishing-Kullanilan-Teknikler-ve-Bunlardan-Korunma-Yoentemleri.pdf , Erişim Tarihi:10.12.2020.

Tabiaa, M., Madani, A. ve Kamoun, N.E. (2017). "E-Banking: Security risks, previsions and recommendations", IJCSNS International Journal of Computer Science and Network Security, Sayı.17, No.11, ss.189-196.

TARIFTIP: "Definition und Kosten", https://www.tariftip.de/rubrik2/12257/2/Definition-und-Kosten.html, Erişim Tarihi:30.01.2021.

Tarhan, K. (2020). Covid-19 ile Mücadele Sırasında Güney Asya'da Siber Güvenlik ve İnsan Hakları. Cyberpolitik Journal Vol.5, No. 9,88-112.

TRT HABER, "Salgın döneminde kullanıcılar en fazla zararlı yazılıma maruz kaldı". https://www.trthaber.com/haber/bilim-teknoloji/salgin-doneminde-kullanicilar-en-fazla-zararli-yazilima-maruz-kaldi-540204.html, Erişim tarihi: 23.12. 2020

TÜRKİYE SİGORTA BİRLİĞİ: "Türkiye Sigorta Birliği Strateji Raporu (2020-2024)", file:///C:/Users/uzay/Desktop/T%C3%9CRK%C4%B0YE%20S%C4%B0GORTA%20B%C4%B0RL%C4%B0%C4%9E%C4%B0%20strateji%20raporu.pdf, Erişim Tarihi: 30.01.2021.

U. S. CYBER COMMAND: https://www.cybercom.mil/ , Erişim tarihi: 27.01. 2021

USOM: "Siber Güvenliğe İlişkin Temel Bilgiler". https://www.usom.gov.tr/dosya/1418807122-USOM-SGFF-001-Siber%20Guvenlige%20Giris%20ve%20Temel%20Kavramlar.pdf Erişim tarihi: 23.12. 2020

Ünlü, U. (2018). "İnternet Bankacılığı Sisteminde Tüketicilerin Karşılaşacağı Olası Saldırılar ve Çözüm Önerileri", Bankacılar Dergisi, Sayı: 104, 82-96.

Vidas T., Owusu E., Wang S., Zeng C., Cranor L.F., Christin N. (2013) QRishing: The Susceptibility of Smartphone Users to QR Code Phishing Attacks. In: Adams A.A., Brenner M., Smith M. (eds) Financial Cryptography and Data Security. FC 2013. Lecture Notes in Computer Science, vol 7862. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-41320-9_4

Wood, A.D. ve Stankovic, J.A. (2002). "Denial of Service in Sensor Networks". http://web.cs.wpi.edu/~emmanuel/courses/cs525m/S04/slides/wk12_p1_Luba_sensor_DoS.pdf, Erişim tarihi: 22.12.2020

Yavanoğlu, U., Sağıroğlu, Ş. ve Çolak , İ. (2012). "Sosyal Ağlarda Bilgi Güvenliği Tehditleri ve Alınması Gereken Önlemler", Journal of Polytechnic Cilt:15, Sayı: 1, 15-27.

Yılmaz, O. (2020). "Covid-19 Salgını Sonrası Dönemin Dijital Kodları ve Siber Güvenlik". https://www.tasav.org/index.php/covid-19-salgini-sonrasi-donemin-dijital-kodlari-ve-siber-guvenlik.html, Erişim Tarihi:28.01.2021

YENİŞAFAK: "En çok Siber Saldırı Türkiye'ye", 28.11.2020 tarihli yazı, https://www.yenisafak.com/gundem/en-cok-siber-saldiri-turkiyeye-3587012, Erişim tarihi: 23.12.2020.

Zeybek, M. ve Yılmaz, E.N. (2019). "Nesnelerin İnterneti: Risk Temelli Yaklaşım". Denetişim, Sayı:10, 73-88.

Research Article

Türkiye'de Siber Risk Sigortalarına İlişkin Bir Değerlendirme

An Evaluation of the Cyber Risk Insurance in Turkey

İpek CEBECİ

Dr. Öğr. Üyesi, Giresun Üniversitesi

İktisadi ve İdari Bilimler Fakültesi Ekonometri Bölümü

ipek.cebeci@giresun.edu.tr

https://orcid.org/0000-0002-2341-9379

Extensive Summary

Technology and technological products are indispensable today. These products, in addition to making humanity's life easier and more beneficial, can harm people individually and institutionally with some abuse. At this point, cyber-attack risks come to the fore as an important issue. Around six billion smart devices are connected to each other via cloud technology. For 2020, this figure is expected to reach 20 billion. While incidents such as fraud and theft have had a negative impact on institutions until today, working life is interrupted by cyber-attacks in the digital world, and sometimes even brought to a standstill. Therefore, cyber risks have become a much more important issue today. Because cyber-attacks damage the data of institutions and organizations and also cyber-attacks can take over the systems of these enterprises in return for ransom. Countries that understand the importance of the subject; identified cyber risks and cyber attacks as the fifth area of operations after sea, air, land and space. Cyber attacks are increasing day by day. As a result of the increasing risks in this regard, insurance companies took action, prepared policies against cyber threats and included the insurance of cyber risks within their own activities.

Cyber risk insurance is an insurance policy that protects businesses against damages that may arise as a result of disclosure or damage of information that has a certain level of confidentiality and needs to be protected. Cyber risk insurance; it provides detailed protection from cyber blackmail to media liability, from business stop to cybercrime. Cyber risk insurances ensure that the damages and losses arising as a result of attacks from the virtual world are repaired and found. Court and IT expenses, information expenses related to data loss and even damage to reputation are insured. In addition, insurance companies can add business-specific guarantees to their policies. Although cyber insurances reduce cyber risk and protect against attacks, there is no assurance that these attacks will not occur.

In this study, cyber risk insurance and its scope are examined in more detail. Then examined the issue of cyber risk insurance for Turkey. The literature was used when examining cyber risk insurance.

The study reached the following conclusions: there are products offered against cyber risks in Turkey. Although the awareness of cyber risks in our country is increasing day by day, it is seen that the companies do not take the increasing cyber risks as one of their priorities. The findings of the research carried out in cooperation with Marsh and TÜSİAD also support this. The general attitude against cyber risks in Turkey "wait-and-see" mode. It can be said that

especially 78% of the companies do not have the practice of recognizing and taking action without facing a threat. This means that the attack experienced for businesses is more potent than cyber-attack predictions. The main reason why cyber security is less on the agenda is that the cyber-attacks experienced did not cause an event that could cause business disruption or economic damage. In addition, most of the companies think that the legal regulations in the country have a stimulating effect. As a sector; It can be said that companies in aviation, information technologies, finance, energy and production sectors are relatively more sensitive and knowledgeable about cyber risk management. The issues that the state puts laws and follows are taken into consideration more by businesses. Therefore, the obligations determined by laws, standards and industry supervision institutions affect businesses to act on cyber risk.

Marsh and TÜSİAD's research shows that, businesses mostly invest in increasing the security of their devices. They invest in making the system or networks more secure, inside and outside the company. 50% of businesses abstain from measuring, managing and preventing cyber risk. Businesses are reluctant to invest in specific areas such as infrastructure, organization and human resources to protect against cyber risks. Another important point is; The maturity of businesses in the field of cybersecurity positively affects their susceptibility to cyber risk insurance. It has also been determined that most of the companies do not have sufficient knowledge about cyber risk insurance (marsh.com.tr).

It is predicted that the digital transformation accelerating in many areas with the impact of the COVID-19 epidemic will both increase awareness and encourage organizations to take more measures for cyber risk management. Due to the COVID-19 epidemic, the rapid digitalization of many companies in our country without taking the necessary precautions has increased the possibilities of cyber-attacks. This situation positively affects the tendency of companies to cyber risk insurance. Obstacles to cyber risk insurance; lack of knowledge about cyber protection insurances and lack of trust in insurance. In this context, adequate information and training on cyber risks and cyber insurances should be given to institutions and individuals.