BÖLÜM 2/1

# SİBER GÜVENLİK SİGORTALARI: UYGULAMADAKİ YERİ VE GELİŞİMİ

--

GÖKSUN CANBERK ULUĞ

## ÖZET

Bilgi ve teknolojinin hızla gelişmesiyle sanal ortamda birçok tehdit ortaya çıkmıştır ve bu tehditler siber riskleri oluşturmaktadır. Dünyada gerçekleşen siber saldırıların artması nedeniyle meydana gelen zararların engellenmesi veya en aza indirgenmesi için siber güvenlik sigorta sektörü ortaya çıkmış ve siber güvenlik sigortaları yeni bir ürün olarak piyasaya sunulmuştur.

Bu çalışmada siber güvenlik kavramıyla birlikte siber risk kavramı ve önemi, siber güvenlik sigortalarının önemi, tarihsel gelişimi ve ülkemiz de dahil olmakla beraber uygulamadaki yeri incelenmiştir.

## ANAHTAR KELİMELER

SİBER GÜVENLİK, SİBER RİSK, SİBER GÜVENLİK SİGORTALARI.





## I. GİRİŞ

Kamu kurum ve kuruluşları, özel şirketler, bireyler dahil her kesim için internet ve teknoloji, hayatımızın vazgeçilmez bir parçası kabul edilmektedir. İnternet ve teknolojideki gelişmeler hayatımızı kolaylaştırmakla beraber birçok riski de yaşamımıza sokmuştur ve bu riskler maddi-manevi zararlara sebep olabilmektedir. Bir insanın ismi, soy ismi, kimlik numarası gibi en temel kişisel verilerinin birtakım kişilerin eline geçmesi ve kötü niyetle kullanılması, bir ülkenin ticari, mali, siyasi ve birçok farklı alandaki kamu kurum ve kuruluşlarının faaliyetlerinin durması gibi çok büyük ölçekli zararlar meydana getirebilmektedir.

Bu zararların engellenmesi için siber güvenlik faaliyetlerinin öneminin kavranması ve bu faaliyetlerle beraber tamamlayıcı koruma olarak siber güvenlik sigortalarının ele alınması gerekmektedir. Veri ihlallerinin ve siber saldırıların meydana gelmesiyle birlikte ortaya çıkan zararların güvence altına alınması konusunda piyasada gelişmeler yaşanmış ve siber güvenlik sigortaları konusunda atılımlar gerçekleşmiştir. Her ne kadar günümüzde siber riskler neticesinde meydana gelen zararlarda hızlı bir artış mevcut olsa da, siber güvenlik sigortalarındaki gelişim ülkelere göre farklılık göstermekle beraber ülkemizde ve Kıta Avrupası'nda ne yazık ki istenilen gelişimi gösterememektedir. Sektörün başını ise Amerika Birleşik Devletleri çekmektedir. İstenilen gelişimi yakalayamamanın birçok sebebi olmakla birlikte; yetkin eleman eksikliği, farkındalığın yeterli düzeyde olmaması, gerekli kanuni düzenlemelerin yapılmasında geç kalınması gibi sebepler temel olarak gösterilebilir.

## II. SİBER GÜVENLİK

### A. Siber Güvenlik Kavramı ve Amacı

Siber Uzay; Ulusal Siber Güvenlik Stratejisi ve Eylem Planı'nda (2020-2023), doğrudan ya da dolaylı olarak internete, elektronik haberleşme ve bilgisayar ağlarına bağlı olan tüm sistem ve hizmetler olarak tanımlanmıştır[1]. Ayrıca kurum, kuruluş ve kullanıcıların varlıkları, bilgi işlem donanımları, personeli, altyapıları, uygulamaları, hizmetleri, telekomünikasyon sistemleri ve siber ortamda iletilen ve/ veya saklanan bilgilerin tümü olarak ifade edilmektedir. Siber güvenlik ise siber uzayın ihtiva ettiği sistem ve hizmetlerin güvenliği noktasında karşımıza çıkmaktadır.

Siber güvenliğin amacı, siber risklerin engellenmesi ve bunların etkilerinin olabildiğince minimalize edilmesidir. Siber tehditler günümüzde daha da kompleks hale gelmiş olup, bunun sonucu olarak zarar verme potansiyelleri de giderek artmıştır. İşbu sebepten ötürü siber güvenliğin sağlanması hem uluslararası hem de ulusal çapta etkin ve yetkin mücadeleyi gerektirmektedir.

**DİPNOT**

1 Ulusal Siber Güvenlik Stratejisi ve 2020-2023 Eylem Planı, https://hgm.uab.gov.tr//uploads/pages/siber-guvenlik/ulusal-siber-guvenlik-stratejisi-ep-2020-2023.pdf, Son Erişim Tarihi: 21.08.2021

BÖLÜM 2/1

Siber uzayda güvenli bir kullanım alanı oluşturmak, bu ortamda kullanıcıların haklarını korumak, bilgilerinin çalınmasını önlemek, saldırılara karşı durmak gibi konularla gündeme gelen siber güvenlik; Bilgi Teknolojileri ve İletişim Kurumu'nun ("BTK") tanımı uyarınca, siber ortamda kurum, kuruluş ve kullanıcıların varlıklarını korumak amacıyla kullanılan araçlar, politikalar, güvenlik kavramları, güvenlik teminatları, kılavuzlar, risk yönetimi yaklaşımları, faaliyetler, eğitimler, en iyi uygulamalar ve teknolojiler bütünüdür.

Siber güvenlik faaliyetlerinin önemi günümüzde daha da artmaktadır. Zira günümüzde siber saldırılar sonucu meydana gelebilecek zararlar hayatı durma noktasına getirebilecek kadar büyük çaplı gerçekleşmektedir. 2007 yılında gerçekleşen Estonya siber saldırıları buna en büyük örnektir. 2007 yılında Estonya'da siber saldırı sonucu bankacılık, medya, siyaset kurumları hedef alınmış ve 2 hafta süren saldırılarda ülkede kamu kurum ve kuruluşlar ile bankacılık sektöründeki faaliyetler durma noktasına gelmiştir. İşbu saldırılar neticesinde dünyada siber güvenliğe verilen önem daha da artmış ve hem devletler hem de insanlar nezdinde farkındalık oluşmaya başlamıştır.

## III. SİBER GÜVENLİK SİGORTALARI

### A. Siber Risk Kavramı

Bilgi teknolojilerinin gelişmesiyle birlikte, her şeyin birbiriyle bağlantılı, bağlı ve bağımlı olduğu bir dünya ortaya çıkmıştır. Küçük esnaftan büyük şirketlere, büyük şirketlerden devletlere her kişi ve kurum, finansal işlemlerden askeri harekatlara kadar siber uzaya güvenmektedir. İşbu siber uzay üzerindeki faaliyetlerin devamı için siber risklerin engellenmesi gerekmektedir. Siber risk kavramının anlaşılması için ilk önce siber kelimesinin tanımı irdelenmelidir.

"Siber" kelimesi iki kurucu unsura sahiptir. Bu kurucu unsurlar siber riskleri diğer risk türlerinden ayırmaktadır. Kurucu unsurlardan biri elektronik iletişim ağları, diğeri ise sanal gerçekliktir. Elektronik iletişim ağları internet ile beraber kullanılan siber uzay ile yakından bağlantılıdır[2]. Siber risk, bilişim ve iletişim teknolojilerinin kullanımından kaynaklanan, verilerin veya hizmetlerin gizliliğini, geçerliliğini veya bütünlüğünü tehlikeye sokan herhangi bir risk olarak tanımlanmaktadır[3]. Buna ilaveten siber güvenlik olaylarından, verilerin kötüye kullanılmasından ve verilerin işlenmesinden doğan sorumluluk nedeniyle ortaya çıkabilecek fiziksel zararlar da siber riskin kapsamındadır[4]. Türkiye mevzuatında ise siber riskin açık bir tanımı bulunmamakla birlikte, siber suçlar; Türk Ceza Kanunu'nun[5] 243 ile 246 maddeleri arasında "Bilişim Alanında Suçlar" başlığı altında düzenlenmiştir.

**DİPNOT**

**2 Ahmet Karayazgan,** Hukuki Yönüyle Siber Riskin Sigorta ve Reasüransı (Siber Riskin Sigorta ve Reasüransı), Kasım 2020, s.6

**3 Martin Eling/Werner Schnell,** Ten Key Questions on Cyber Risk and Cyber Risk Insurance (Ten Key Questions), November 2016, s.35

**4** International Association of Insurance Supervisors, Issues Paper on Cyber Risk to the Insurance Sector, August 2016, s.5

**5 Türk Ceza Kanunu,** 12.10.2004 tarih, 25611 sayılı Resmi Gazete (RG)





Siber riskler doğal ya da insan kaynaklı olarak ortaya çıkabilmektedir. Ancak siber risk hadiselerinin çok büyük bir bölümü insan kaynaklıdır. Yapay siber riskler; insan hatasından, siber saldırılardan, siber terörizm ve siber savaş gibi faaliyetlerden dolayı meydana gelebilir. Fiziksel olarak verilerin çalınması, çalışanların verileri manipüle etmesi de yapay siber risklere dahildir. Afetler gibi doğal yoldan ortaya çıkan siber riskler ise çok nadir görülmektedir. Böyle bir ayrım mevcut olmasına karşın insan kaynaklı da olsa doğal yoldan da meydana gelse ortaya çıkan zararlar ortalama olarak birbirine yakındır[6].

Siber saldırılar neticesinde her yıl milyonlarca kişinin kimlikleri çalınmakta ve deşifre edilmektedir. 2014 yılında 1.2 milyar, 2015 yılında 564 milyon ve 2016 yılında 1.1 milyar kişinin kimlikleri deşifre edilmiştir. 10 milyondan fazla kişinin kimliğinin deşifre edildiği olay sayısı 2014 yılında 11, 2015 yılında 13 ve 2016 yılında 15 olarak ifade edilmektedir[7]. Dünyada; Home Depot'un 2200 mağazayı ihtiva eden bir hackleme sonrası 56 milyon müşterinin kredi ve banka kartlarının çalınması; Sony Pictures'dan çalışanlarının kişisel bilgileriyle birlikte yayınlanmamış filmlerin çalınması; JP Morgan Chase'in hesap sahiplerinin isim, adres, telefon numaraları ve e-postalarını ihtiva eden 76 milyon kaydın çalınması; McKenna Long & Aldridge'de müşteri yazılımına yerleştirilen bir programla müşterilerin kişisel verilerinin çalınması gibi saldırı örnekleri gösterilebilir. Türkiye'de ise en büyük çevrimiçi yemek sipariş sitesi olan Yemeksepeti; 27.03.2021 tarihinde Twitter üzerinden, kullanıcılarının; adı soyadı, doğum tarihi, telefon numaraları, e-posta adresleri, ev adresleri olmak üzere bilgilerinin çalındığını açıklamıştır[8].

Fiziksel olarak verilerin çalınması, çalışanların verileri manipüle etmesi de yapay siber risklere dahildir.

Temmuz 2021 itibariyle ise yakın tarihimizdeki en büyük veri ihlallerinden bazıları aşağıda belirtilmiştir:
· Ağustos 2013 tarihinde Yahoo'nun 3 milyar kullanıcı hesap bilgisinin hackerlar tarafından ele geçirilmesi.
· Kasım 2019 tarihinde Çin menşeli satış sitesi Alibaba'nın 1.1 milyar kullanıcı bilgisinin çalınması.
· Temmuz 2021 tarihinde Linkedin'in 700 milyon kullanıcıyı etkileyen veri ihlalinin gerçekleşmesi.
· Mart 2020 tarihinde Çin'in en büyük sosyal medya platformlarından biri olan Sina Weibo'nun 538 milyon kullanıcısının isim, soy isim, cinsiyet, telefon numarası, konum bilgileri gibi kişisel verilerinin çalınması.
· Nisan 2019 tarihinde dünyanın en büyük sosyal medya platformu olan Facebook'un 530 milyon kullanıcısının telefon numaraları, Facebook ID'leri, kullanıcı isimleri gibi verilerinin çalınması.

Siber riskler ayrıca ekonomik olarak önemli maddi zararlara da yol açabilmektedir. IBM ve Ponemon Enstitüsü'nün "Bir Veri İhlalinin Maliyeti" adlı 2020 yılı raporuna göre, Amerika Birleşik Devletleri'nde, 2019 Ağustos ile 2020 Nisan arası siber güvenlik ihlallerinin maliyeti 8.640.000 $ olarak ifade edilmektedir[9]. Bazı yazılım firmalarının yayınladıklarına göre ise siber risklerin yıllık maliyeti 1 trilyon $ tutarındadır; ancak bu bulguların ciddi bir şekilde sorgulanması gerektiği ifade edilmektedir[10]. Dünya Ekonomik Forumu 2015 Küresel Risk Raporu'na göre, küresel ölçekte ekonominin karşılaşacağı ilk on risk arasında; veri sahtekarlığı, siber güvenlik olayları ve bilgi işlem altyapısı çökmesi gibi teknolojik riskler yer almaktadır. Siber risk, dijitalleşme ile birlikte günümüzde en büyük ticari risklerden biri olarak kabul edilmektedir.

**DİPNOT**

**6 Christian Biener/Jan Wirfs/Martin Eling,** Insurability of Cyber Risk: An Empirical Analysis (An Empirical Analysis), June 2014, s.9

**7 Marsh & Mc Lennan Companies Global Risk Center,** Cyber Handbook 2018 – Perspectives on the next wave of cyber, 2018, s.5

**8** https://twitter.com/yemeksepeti/status/1375764826241314818, Son Erişim Tarihi 22.08.2021

**9 LeeAnne M. Pelzer,** The True Cost of Cybersecurity Incident: The Problem, June 2021, https://www.paloaltonetworks.com/blog/2021/06/the-cost-of-cybersecurity-incidents-the-problem/, Son Erişim Tarihi:23.08.2021

**10 Eling/Schnell,** Ten Key Questions, s.35

BÖLÜM 2/1

## B. Siber Güvenlik Sigortası Kavramı

Günümüzde teknolojinin hızlı gelişimi ile beraber akıllı telefonlardan bilgisayarlara, banka sistemlerinden enerji şirketlerine her kişi ve kurum, kişisel verilerden ticari verilere kadar her çeşit veriyi bulut sistemi üzerinde tutmaktadır. İşbu teknoloji çağının getirdiği verimlilik, yukarıda açıklanan siber riskleri de beraberinde getirmektedir. Kişi ve kurumlar maruz kaldığı siber saldırılar ve akabinde ortaya çıkan maddi ve manevi zararları ortadan kaldırmak ve/ veya en aza indirmek için siber güvenlik sigortalarına başvurmaktadır.

Siber güvenlik sigortası, bilgisayar tabanlı bir saldırı veya şirketin bilgi teknolojileri sisteminde oluşan bir arıza neticesi ortaya çıkan birinci ve üçüncü taraf zararlarını ele alan sigorta poliçeleri için kullanılan geniş bir tanımdır[11]. Siber risk sigortası olarak da adlandırılan siber güvenlik sigortası; bir kuruluşun bilgisayar veya bilgisayar bağlantılarıyla yani siber uzay ile ilgili bir güvenlik ihlali ya da benzer bir olay sonrası kurtarma ve iyileştirme ile ilgili maliyetleri dengeleyerek, riske maruz kalmasını azaltmaya yardımcı olmak için tasarlanmıştır[12].

Siber güvenlik sigortaları; koruma önlemlerinin yeterli olmadığı durumlarda, kurumların mevcut işlemlerinin aksamaması ve yaşanan kayıpların telafisinin yapılarak en kısa zamanda kurumların faaliyetlerine geri dönmesine yardım etmektedir.

## C. Siber Güvenlik Sigortalarının Kapsamı

Siber güvenlik sigortaları, birçok sigorta ürünü gibi iki zarar türünü kapsamaktadır. Bunlar birinci taraf zararları ile üçüncü taraf zararlarıdır. Birinci taraf zararları, sigortalının doğrudan maruz kaldığı zararlardır. Üçüncü taraf zararları ise sigortalının davranışı yüzünden, sigorta sözleşmesine taraf olmayan üçüncü kişilerin zarar taleplerini ifade etmektedir[13].

Güvenlik veya veri ihlalinin sebeplerinin araştırılması için yapılan masraflar, ticari hizmetlerin aksamasından kaynaklanan zararlar, aksayan ticari hizmetlerin restore edilmesi için yapılan masraflar, veri ihlali sebebiyle zarar gören üçüncü şahısların bu konu hakkında bilgilendirilmesi için yapılan masraflar birinci taraf zararlarına örnek verilebilir. Bu tarz siber güvenlik hadiselerinin olası risklerini yönetebilmek için sigorta şirketleri belirli bir alt sınır koymaktadırlar[14]. Üçüncü taraf zararlarında ise veri ihlalinden dolayı üçüncü kişilerin uğradığı zararları sigortalıdan talep etmesi örnek gösterilebilir.

Birinci taraf zararlarında en çok karşılaşılan örnekler, adli inceleme masrafları, ceza ödemeleri, kredi izleme, halkla ilişkilere yönelik harcamalar olarak gösterilebilir. Üçüncü kişi zararları kapsamında ise mal zararları, gizlilik ihlali, cismani ve/ veya manevi zarar talepleri en çok karşılaşılan örneklerdendir[15].

Her ne kadar siber güvenlik sigortası poliçelerinde standart teminatlar olmasa da meydana gelen ihlalin veya saldırının ve zararlarının; soruşturma masrafları, siber hadise sonucu ortaya çıkan ticari zararlar, ihlalden zarar gören üçüncü taraflara bildirim masrafları, gizli bilgilerin, kişisel verilerin, fikri ve sınai mülkiyet hakların ihlal edilmesinden kaynaklı karşı karşıya kalınan ceza ve hukuk davaları, fidye yazılımı gibi zararlı yazılımlar ile karşı karşıya kalınan şantaj ve fidye ödeme maliyetleri siber güvenlik sigortası poliçelerinde yaygın olarak teminat altına alınan zararlara örnek olarak verilebilir[16]. Siber ortamla doğrudan bağlantılı olmayan zararlar ise poliçelerde teminat dışı bırakılmıştır.

Uygulamada, sigorta şirketlerinin sigorta poliçelerini düzenlerken karşılaştığı risklerden birisi siber risklerin fiyatlandırılmasıdır. Siber riskleri fiyatlandırmada karşılaşılan problem, verilerin yetersizliğinde yatmaktadır. Sigorta şirketleri, siber risk modellemesi yaparken ne kadar isabetli ve sofistike davransalar da bu modellemeleri test edecek veri olmadığı sürece hiçbir işe yaramayacaktır. Sigorta şirketleri bu sebeple siber risk hadiseleri sonucu meydana gelecek ortalama kayıplarla ilgili belirsizliğe, sigorta kapsamını düşük tutarak ve primleri yükselterek tepki göstermektedir. Siber risklerin fiyatlandırmasında karşılaşılan diğer bir problem ise siber risklerin hızlı bir şekilde değişmesidir. Teknolojik ilerlemenin çok hızlı olması neticesinde yeni sistem ve araçların ortaya çıkması, siber risklerin değerlendirilmesinde zorluk yaratmakta ve sigorta şirketlerinin riskleri yanlış değerlendirmesine sebep olmaktadır[17].

### DİPNOT

**11 Sasha Romanosky/Lillian Ablon/Andreas Huehn/Therese Jones,** Content Analysis of Cyber Insurance Policies: How do Carries Price Cyber Risk? ( Analysis of Cyber Insurance) December 2018, s.2

**12 Kim Lindros/Ed Tittel,** What is cyber insurance and why you need it (What is Cyber Insurance), May 2016, https://www.csoonline.com/article/3065474/what-is-cyber-insurance-and-why-you-need-it.html, Son Erişim Tarihi: 25.08.2021

**13 Romanosky/Ablon/Huehn/Jones,** Analysis of Cyber Insurance Policies, December 2018, s.4

**14 Romanosky/Ablon/Huehn/Jones,** Analysis of Cyber Insurance Policies, December 2018, s.4 December 2018, s.5

**15 Karayazgan,** Siber Riskin Sigorta ve Reasüransı, Kasım 2020, s.9

**16 Lindros/Tittel,** What is Cyber Insurance, May 2016, https://www.csoonline.com/article/3065474/what-is-cyber-insurance-and-why-you-need-it.html, Son Erişim Tarihi: 25.08.2021

**17 Biener/Wirfs/Elin,** An Empirical Analysis, June 2014, s.12





Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı'nın gerçekleştirdiği siber risk araştırması sonuçları, sigorta şirketlerinin müşteri riskini değerlendirirken; gözetim mekanizması, çalışan farkındalığı, olay tepkisi, güvenlik ölçümleri, üst yönetim farkındalığı gibi ana kategorilere odaklanması gerektiğini belirtmiştir[18].

## D. Siber Güvenlik Sigortalarının Gelişimi ve Dünyadaki Yeri

İlk olarak Amerika Birleşik Devletleri'nde 1990'lı yıllarda ortaya çıkan siber sigortaların geçmişi bu tarihlere uzanmaktadır. 1994 ile 2000 yılları arasında Amerika Birleşik Devletleri, internetin hızlı gelişimine adapte olmuş ve bu döneme "dot-com balonu" adı verilmiştir. Bu ismin verilmesinin sebebi, 2000 yılına gelindiğinde gelişen bilgisayar ve internet teknoloji şirketlerinin borsada büyük değer kaybı yaşaması sonucu, bu şirketlere yatırım yapan sermaye şirketlerinin hızlı bir şekilde teknoloji sektöründen çekilmesidir. Dot-com balonunun sonucu olarak; veri ihlalleri, veri kayıpları, sistemlere izinsiz erişim gibi siber risklerin karşısında siber sigortalar popülerlik kazanmıştır[19].

Teknolojinin gelişimi ile beraber siber risklerin evrilmesi, siber güvenlik sigortalarında da büyük değişimler meydana getirmiştir. 1990'larda siber güvenlik sigorta poliçeleri, online medya ve veri işleme hataları gibi sınırlı siber riskleri teminat altına almaktaydı. Birinci taraf zararları olan para cezaları ve idari talepler poliçe dışı bırakılmıştı. 2000'lere gelindiğinde ise siber risklerin gelişmesinin ve farkındalığın artmasının sonucu olarak sigorta poliçeleri birinci taraf zararları ile beraber üçüncü taraf zararlarını da teminat altına almaya başlamıştır.

2003 yılına gelindiğinde Amerika Birleşik Devletleri California eyaletinde, "Security Breach and Information Act" adlı güvenlik ihlali konusunda kanun yürürlüğe girmiş, işbu kanun ile şifrelenmemiş kişisel verileri yetkisiz kişiler tarafından erişime uğrayan kişilerin bilgilendirilmesi yükümlülük altına alınmıştır[20]. Bu kanunun yürürlük tarihinden itibaren birçok eyalet, peş peşe veri güvenliği ile alakalı yasa yürürlüğe sokmuş ve siber güvenlik konusunda hukuki yükümlülükler getirmiştir. Bu yükümlülüklerin sonucunda siber güvenlik sigorta piyasası gelişim göstermeye başlamıştır.

Amerika Birleşik Devletleri'nde siber güvenlik sigortaları diğer ülkelere göre daha yaygın olarak kullanılıyor olsa da yalnızca şirketlerin üçte biri siber güvenlik sigortası sahibidir. Siber güvenlik sigortalarının kullanımı da sektörlere göre farklılık göstermektedir. İmalat şirketlerinin yalnızca %5'i sigorta sahibiyken, sağlık, teknoloji ve perakende sektöründe bu oran %50'lere yaklaşmaktadır. Ancak siber güvenlik sigortalarının her sektörde %27'lik bir oranla artış gösterdiği ifade edilmiştir[21].

### DİPNOT

**18 Eda Altuntaş/Emine Kara/Abdullah Buğra Soylu/Erdem Kırkbeşoğlu,** Siber Sigortalar: Son Gelişmeler, Uygulamalar ve Sorunlar (Siber Sigortalar), Aralık 2018, s.17

**19** A History of Cyber Liability Insurance, August 2021, https://colony-west.com/a-history-of-cyber-liability-insurance/, Son Erişim Tarihi: 26.08.2021

**20** A History of Cyber Liability Insurance, August 2021, https://colony-west.com/a-history-of-cyber-liability-insurance/, Son Erişim Tarihi: 26.08.2021

**21 Romanosky/Ablon/Huehn/Jones,** Analysis of Cyber Insurance Policies, December 2018, December 2018, s.2

# BÖLÜM 2/1

Global olarak ise siber güvenlik sigortası piyasası 2016 yılında brüt prim olarak yaklaşık 4 milyar $'a ulaşmıştır. Yapılan çalışmalara göre piyasanın, küresel ölçekte 2022 yılına kadar ortalama 14 milyar $ prim üreteceğini, 2025 yılına kadar ise primin 20 milyar $'a ulaşabileceği ifade edilmektedir.

2013 Yılında Kıta Avrupası'nda 8 adet siber güvenlik sigortası teminatı sağlayan pazar varken, bu sayı 2017 yılında 25'e yükselmiştir. Küresel çapta ise 50 civarı pazarın siber güvenlik sigortası teminatı sağladığı ifade edilmektedir[22]. Avrupa Birliği'nde 2018 yılında AB Genel Veri Koruma Yönetmeliği'nin[23] de yürürlüğe girmesiyle birlikte siber güvenlik sigortalarına olan talep artmaya başlamış ve siber güvenlik sigortaları popülerlik kazanmıştır.

Türkiye'de ise 2016 yılında yürürlüğe giren Kişisel Verilerin Korunması Kanunu ile birlikte siber güvenlik ve siber risk alanında büyük bir gelişme yaşanmıştır. İşbu yürürlüğe giren kanun ile birlikte şirketlerin veri politikaları regüle edilmiş ve siber güvenlik alanında farkındalığın kazanılmasında fayda sağlamıştır. Her ne kadar bu kanun ile birlikte Türkiye'de de siber risk farkındalığı konusunda gelişme yaşanmış olsa da Amerika Birleşik Devletleri dışındaki bölgelerde siber güvenlik sigortalarının daha yeni olduğu söylenebilir.

## E. Türkiye'de Siber Güvenlik Sigortaları

Türkiye'de siber saldırılar her geçen gün sayısını artırmakta ve saldırıların sebep olduğu maddi ve manevi zararlar siber riskler konusunda kişi ve kurumlarda farkındalık oluşturmaktadır. 2019 yılında 12 ayda en az bir adet başarılı şekilde gerçekleşen saldırı oranı Türkiye için %87,80 seviyesindedir[24]. Bu sebepte ülkemizde siber güvenlik sigortalarının öneminin vurgulanması gerekmektedir.

Telekomünikasyon Birliği Global Siber Güvenlik Endeksi Raporu'na göre Türkiye, dünyada en çok siber saldırıya uğrayan ülkeler arasında ilk üçtedir. 2016 yılında 9000 civarı olan siber saldırılar yaklaşık 15 kat artarak 2019 yılında 136.000'i aşmıştır[25]. Ancak Türkiye Siber Risk Algı Araştırması'na göre, söz konusu artışlara rağmen Türkiye'de kurumların %78'i siber riske karşı önlem almak için riskin gerçekleşmesinin gerektiğini ifade etmişlerdir[26].

Siber riskin mahiyeti her geçen gün anlaşılmakta ise de bir tamamlayıcı çözüm yöntemi olan siber güvenlik sigortaları konusunda fikir sahibi olmayan, yahut bu sigortaların siber riskler konusunda bir işlevinin olmadığını düşünen kurumlar da bulunmaktadır. Türkiye Siber Risk Algı Araştırması katılımcılarının %25'i, çalıştığı kurumun siber güvenlik sigortasına sahip olup olmadığını bilmemektedir. %43'ünün ise çalıştıkları kurumların siber güvenlik sigortasına sahip olduğunu ifade etmiştir. Ayrıca 500'den fazla çalışanı olan finans şirketlerinde siber güvenlik sigortasına sahip olanlar çoğunluğu oluşturmaktadır. Araştırmaya katılanların %33'ü siber güvenlik sigortası sahibi olup 1 yıl içinde siber güvenlik sigortası almayı düşünenlerin oranı %45'tir[27]. Siber güvenlik sigortalarına olan ilgi artıyor gözükse de Türkiye'de şirketlerin siber güvenlik sigortalarının kapsamına güvenmedikleri görülmektedir. Araştırmaya katılan kurumların sadece %49'u siber güvenlik sigortalarının kapsamına güvenmektedir. Bu oran dünya genelinde ise %89 düzeyindedir. Dünya ile Türkiye arasında %40'lık bir fark olması, her ne kadar siber riskler ve siber saldırılar hayatımızın her köşesinde karşımıza çıksa da hâlâ yeterli bilincin sağlanamadığına işaret etmektedir.

Gerek Avrupa'da gerek Türkiye'de; siber güvenlik sigortaları konusunda Amerika Birleşik Devletleri'nde gelinen farkındalık düzeyine gelinememesi, siber risklere ilişkin hususların çalışanlarca yeterince kavranamamış olması ve yetkin personelin istihdam edilemiyor olması siber riskle mücadele konusundaki problemler olarak değerlendirilmektedir.

## IV. SONUÇ

Bu çalışmada detaylıca incelendiği üzere, bilgi ve teknolojinin gelişimiyle birlikte siber riskler gün geçtikçe artış göstermektedir. Sistemlerin birbirine bağlı ve birbiriyle bağlantılı olduğu günümüz teknoloji çağında siber riskler neticesi meydana gelmesi muhtemel zararların güvence altına alınması, bu zararların engellenmesi veya en aza indirgenmesi hayati önem taşımaktadır. Siber güvenlik sistemleriyle birlikte siber güvenlik sigortalarının yaygınlaştırılması tamamlayıcı bir koruma sağlayacaktır ancak yukarıda da belirtildiği gibi dünyanın birçok ülkesinde bu bilinç ve gelişim istenilen düzeyde değildir. Türkiye'de yer alan işletmelerin ve sigorta şirketlerinin bu konu hakkındaki farkındalığı dünyanın geri kalanından farklılık göstermektedir. Özellikle sigorta bilincinin ve siber risk algısının öneminin kavranması, siber güvenlik sigortalarının gelişimiyle sıkı bir bağlantı içerisindedir. Yine siber riskin yönetimi ve zararların engellenmesi bu sayılan kavramların gelişkin olmasına bağlıdır. Amerika Birleşik Devletleri dışında Kıta Avrupası ve Türkiye'de siber risk bilinci düşüktür, bu yüzden de siber güvenlik sigortalarının uygulamadaki gelişimi siber riskler ile doğru orantılı olarak gitmemektedir.

Teknolojinin yadsınamaz ve önüne geçilemeyen gelişimi ile birlikte ulusal ve uluslararası kapsamda alınacak tedbirlerin farkındalığı yükselteceği açıktır. Türkiye'de de siber güvenlik alanında farkındalığın kurumsal ve bireysel düzeyde artırılması, siber güvenlik sigortalarının kullanımının gelişim göstermesinin ve dolayısıyla siber risklerden korunmanın önünü açacaktır.

### DİPNOT

**22 Eda Altuntaş/Emine Kara/ Abdullah Buğra Soylu/Erdem Kırkbeşoğlu,** Siber Sigortalar: Son Gelişmeler, Uygulamalar ve Sorunlar (Siber Sigortalar), Aralık 2018

**23** General Data Protection Regulation (GDPR), Mayıs 2018, https://gdpr-info.eu/

**24** 2019 Cyberthreat Defense Report, Son Erişim Tarihi: 27.08.2021 https://www.imperva.com/resources/reports/CyberEdge-2019-CDR-Report-v1.1.pdf

**25 Cebeci,** İ.,2021 Türkiye'de Siber Risk Sigortalarına İlişkin Bir Değerlendirme, Üçüncü Sektör Sosyal Ekonomi Dergisi, 56(1), s.177

**26 Marsh & Mclennan Companies,** 2020 Türkiye Siber Risk Algı Araştırması (Siber Risk Araştırması), 2020, s.2

**27 Marsh&Mclennan,** Siber Risk Araştırması, 2020, s.14

### KAYNAKÇA


Ulusal Siber Güvenlik Stratejisi ve 2020-2023 Eylem Planı, https://hgm.uab.gov.tr//uploads/pages/siber-guvenlik/ulusal-siber-guvenlik-stratejisi-ep-2020-2023.pdf, Son Erişim Tarihi: 21.08.2021

**AHMET KARAYAZGAN,** Hukuki Yönüyle Siber Riskin Sigorta ve Reasüransı (Siber Riskin Sigorta ve Reasüransı), Kasım 2020

**MARTİN ELİNG/ WERNER SCHNELL,** Ten Key Questions on Cyber Risk and Cyber Risk Insurance (Ten Key Questions), November 2016

International Association of Insurance Supervisors, Issues Paper on Cyber Risk to the Insurance Sector, August 2016

Türk Ceza Kanunu, 12.10.2004 tarih, 25611 sayılı Resmi Gazete (RG)

Yemeksepeti Resmi Twitter Hesabı, https://twitter.com/yemeksepeti/status/1375764826241314818, Son Erişim Tarihi: 24.08.2021

Marsh & Mc Lennan Companies Global Risk Center, Cyber Handbook 2018 – Perspectives on the next wave of cyber, 2018

**LEEANNE M. PELZER,** The True Cost of Cybersecurity Incident: The Problem, June 2021, https://www.paloaltonetworks.com/blog/2021/06/the-cost-of-cybersecurity-incidents-the-problem/, Son Erişim Tarihi:23.08.2021

**SASHA ROMANOSKY/ LİLLİAN ABLON/ ANDREAS HUEHN/ THERESE JONES,** Content Analysis of Cyber Insurance Policies: How do Carries Price Cyber Risk? ( Analysis of Cyber Insurance) December 2018

**KİM LİNDROS, ED TİTTEL,** What is cyber insurance and why you need it (What is Cyber Insurance), May 2016, https://www.csoonline.com/article/3065474/what-is-cyber-insurance-and-why-you-need-it.html, Son Erişim Tarihi: 25.08.2021

**EDA ALTUNTAŞ, EMİNE KARA, ABDULLAH BUĞRA SOYLU, ERDEM KIRKBEŞOĞLU,** Siber Sigortalar: Son Gelişmeler, Uygulamalar ve Sorunlar (Siber Sigortalar), Aralık 2018

A History of Cyber Liability Insurance, August 2021, https://colony-west.com/a-history-of-cyber-liability-insurance/, Son Erişim Tarihi: 26.08.2021

2019 Cyberthreat Defense Report, Son Erişim Tarihi: 27.08.2021 https://www.imperva.com/resources/reports/CyberEdge-2019-CDR-Report-v1.1.pdf

**İPEK CEBECİ,** 2021 Türkiye'de Siber Risk Sigortalarına İlişkin Bir Değerlendirme, Üçüncü Sektör Sosyal Ekonomi Dergisi, 56(1)

**MARSH & MCLENNAN COMPANİES,** 2020 Türkiye Siber Risk Algı Araştırması, 2020

**CHRİSTİAN BİENER/ JAN WİRFS/ MARTİN ELİNG,** Insurability of Cyber Risk: An Empirical Analysis (An Empirical Analysis), June 2014