Üçüncü Sektör Sosyal Ekonomi Dergisi
Third Sector Social Economic Review
58(1) 2023, 708-726
doi: 10.15659/3.sektor-sosyal-ekonomi.23.03.2065

Araştırma Makalesi

Türk Sigorta Sektöründe Siber Sigortalara İlişkin Değerlendirme: Sektörel Bir Araştırma[1]

Assessment of Cyber Insurance in the Türk Insurance Sector: A Sectoral Research

Nuriye VAROL GÖNEN	Emine ÖNER KAYA
Arş. Gör., Ankara Hacı Bayram Veli Üniversitesi	Doç. Dr., Ankara Hacı Bayram Veli Üniversitesi
Bankacılık ve Sigortacılık Yüksekokulu	Bankacılık ve Sigortacılık Yüksekokulu
nuriye.varol@hbv.edu.tr	emine.oner@hbv.edu.tr
https://orcid.org/0000-0001-9159-5983	https://orcid.org/0000-0002-4247-0866

Makale Geliş Tarihi	Makale Kabul Tarihi
09.01.2023	09.03.2023

Öz

Bilgi teknolojisi (BT)'nin ekonomik büyümeyi destekleyen kritik bir bileşen olarak görüldüğü günümüzde, BT ürünleri ve hizmetleri bireyler ve işletmeler için ekonomik ve sosyal hayatın ayrılmaz bir parçası haline gelmiştir. Küreselleşme ve dijitalleşmeyle daha fazla gündeme gelen bilgi teknolojilerinin olumlu sonuçları olmasının yanı sıra siber suçların eğilimi ve şiddetinin artması gibi olumsuz sonuçları da bulunmaktadır. Günümüzde tüm işletmelere, özellikle de küçük ve orta ölçekli işletmelere yönelik siber saldırılar daha sık ve karmaşık hale gelmiştir. Siber saldırıların giderek artan sıklığı ve şiddeti göz önüne alındığında, siber sigorta piyasasının gelişmeye devam etmesi beklenmektedir. Bu doğrultuda çalışmanın amacı, Türkiye'de siber sigortaya ilişkin piyasa uygulamalarının araştırılması ve Türkiye siber sigorta piyasasının incelenmesidir. Nitel araştırma yönteminin kullanıldığı çalışmada, veri toplama aracı olarak yarı-yapılandırılmış görüşme formlarından yararlanılmıştır. Araştırmaya katılan hayat dışı sigorta şirketlerinin siber sigortalar konusunda uzman yöneticileriyle yapılan görüşmeler neticesinde, Türkiye'de siber sigorta piyasasının mevcut durumu, sigortalama süreci ve fiyatlandırma, sektör tercihi, sigortalıda aranan şartlar, sigorta kapsamı ve siber olay şüphesi olduğunda müdahale süreci başlıkları altında incelenmiştir. Ayrıca Covid-19 salgınının siber sigorta piyasası üzerindeki etkileri ile Türkiye'de siber sigorta piyasasının önündeki fırsatlar ve/veya engeller ortaya koyulmaya çalışılmıştır.

Anahtar Sözcükler: *Siber Risk, Siber Sigorta, Siber Sigorta Piyasası, Nitel Araştırma, Yarı-Yapılandırılmış Görüşme*

Jel Kodları: *G22*

Abstract

Information technology (IT) has been seen as a critical component supporting economic growth in recent years. IT products and services have become an integral part of economic and social life for individuals and businesses. Information technologies coming to the fore more with globalization and digitalization have positive consequences

[1] Türk Kooperatifçilik Kurumu tarafından 19-21 Ekim 2022 tarihleri arasında Girne/KKTC'de düzenlenen 24. Milletlerarası Türk Kooperatifçilik Kongresi'nde sunulan çalışmanın özeti "Bildiri Özetleri Kitabı"nda ayrıca basılmıştır.

Önerilen Atıf /Suggested Citation
Varol Gönen, N. & Öner Kaya, E., 2023 Türk Sigorta Sektöründe Siber Sigortalara İlişkin Değerlendirme: Sektörel Bir Araştırma, *Üçüncü Sektör Sosyal Ekonomi Dergisi,* 58(1), 708-726

as well as negative ones such as the increase in the tendency and violence of cybercrime. Cyber-attacks against enterprises, especially small- and medium-sized enterprises (SMEs), have become more frequent and sophisticated in recent years. Considering the increasing frequency and severity of cyber-attacks, the cyber insurance market is expected to continue to grow. In this context, the purpose of this study is to investigate the market practices of cyber insurance in Türkiye and to examine the cyber insurance market. In the study, qualitative research method was employed and semi-structured interview forms were used as data collection tool. As a result of the interviews with representatives from the non-life insurance companies participating in the research, the current situation of the cyber insurance market in Türkiye were examined under the headings of underwriting process and pricing, sector preference, requirements on the insured, insurance coverage, and response process when a cyber-incident is suspected. In addition, the effects of Covid-19 outbreak on the cyber insurance market and opportunities and/or obstacles to the cyber insurance market in Türkiye were tried to be revealed.

Keywords: *Cyber Risk, Cyber Insurance, Cyber Insurance Market, Qualitative Research, Semi-Structured Interview*

JEL Classification: *G22*

1. Giriş

Küresel düzeyde normal koşullarda yılları alması beklenen bir dijital dönüşüm süreci, Covid-19 salgını ile birlikte çok daha kısa bir süre içinde ve güvenlikten ziyade işlev odaklı olarak gerçekleşmiştir (Korucu, 2021: 45). Ekonomik ve sosyal hayatın dijitalleşmesi sadece gelişme fırsatlarının ve yeniliklerin değil aynı zamanda yeni risklerin de kaynağıdır. Maillart ve Sornette (2010: 357), internetin gelişmesiyle birlikte yeni tür büyük saldırılar, sanal çatışmalar ve suçlar ortaya çıktığını ifade etmektedir. Dünya daha fazla dijitalleşirken ve birbirine bağlanırken, siber güvenlik tehditleri de beraberinde artış göstermektedir. Hatta siber güvenlik tehditlerindeki artışın, bu tehditleri etkili bir şekilde önleme veya bunlara yanıt verme becerisini geride bıraktığını ifade etmek mümkündür (WEF, 2022a: 9). Dünya Ekonomik Forumu (WEF)'nun Küresel Riskler Raporu'na göre, 2020 yılında, kötü amaçlı yazılım saldırıları %358, fidye yazılımı saldırıları ise %435 oranında artış göstermiştir (WEF, 2022a: 9). Küresel Riskler Algı Araştırması 2021-2022 sonuçlarına göre ise, siber güvenlik başarısızlığı, Covid-19 salgını ile birlikte en çok kötüleşen ilk 10 risk arasında yer almıştır (WEF, 2022a: 24). Dijitalleşme arttıkça ve yeni teknolojiler ortaya çıktıkça, siber riskin de kaçınılmaz olarak büyümesi beklenmektedir (WEF, 2022b: 29).

Siber risk, Eling ve Schnell (2016: 483) tarafından *"veri veya hizmetlerin gizliliğini, kullanılabilirliğini veya bütünlüğünü tehlikeye atan BT kullanımından kaynaklanan herhangi bir risk"* olarak tanımlanmakta ve doğal olarak ya da insan kaynaklı olarak gerçekleşebileceği ifade edilmektedir. Siber riskler, faaliyete göre (örneğin suç niteliğinde ve suç teşkil etmeyen nitelikte), saldırı türüne göre (örneğin kötü amaçlı yazılım, içeriden saldırı, istenmeyen e-posta vd.) ve kaynağa göre (örneğin siber suç, siber savaş ve siber terörizm) sınıflandırılabilmektedir (Eling ve Schnell, 2016: 483). Birinci ve üçüncü taraf kayıplarına neden olabilmesi, hem kısa hem de uzun kuyruklu kayıplarla sonuçlanabilmesi, kayıpların birbirinden bağımsız olmaması (siber olaylar arasındaki korelasyonlar), verilere ve modelleme yaklaşımlarına ilişkin yüksek belirsizlik, tahmin edilmesi zor aşırı senaryolar (düşük sıklık, yüksek şiddet), değişim riski ve risk azaltma araçlarının yüksek önemi (ahlaki tehlike) siber riskin temel özellikleri arasında yer almaktadır (Eling ve Wirfs, 2016: 29). Söz konusu özellikleri sebebiyle siber riskin yönetimi oldukça zor bir süreç olup iş süreçlerinin dijitalleşmesine bağlı olarak daha da zorlaşmaktadır. Sağlam ve doğru bir siber risk yönetim süreci için, siber riskin sadece BT bölümünün sorumluluğunda görülmemesi, aynı zamanda farklı bölümlerin siber risk yönetim sürecinde birlikte hareket etmesi gerekmektedir (Eling ve Schnell, 2016: 479).

Risk yönetimi sürecinin temel bölümleri risk değerlendirmesi ve riske müdahale olup, risk değerlendirmesi, riskin tanımlanması ve analizi aşamalarını içermekte, riske müdahale ise, risklerle başa çıkmak için uygun tedbirlerin seçilmesi ve uygulanmasını kapsamaktadır (Marotta, Martinelli, Nanni, Orlando ve Yautsiukhin, 2017: 40). Risk yönetimi sürecinde ilk olarak risk tanımlama aşamasında potansiyel tehditler, mevcut güvenlik açıkları ve etkilenebilecek varlıklar belirlenmekte, daha sonra ise risk analizi aşamasında olayın olasılığı ve potansiyel etkisi belirlenerek risk tahmin edilmektedir (Marotta vd., 2017: 40). Ancak siber riskin nispeten yeni bir risk türü olması ve yeterli veri bulunmaması nedeniyle, doğru bir olasılık tahmini yapılabilmesi oldukça zordur. Ayrıca bu risk türü dinamik bir yapıda olduğundan önemli bir değişim riskine sahiptir ve bu durum geçmiş istatistiksel araştırmaların

geleceğe ilişkin değerlendirmelerinin de dikkatle incelenmesini gerektirmektedir (Eling ve Schnell, 2016: 480). Riske müdahale aşamasında ise, siber riski yönetmeye yönelik riskten kaçınma, riski kabullenme (riski tutma), riski azaltma ve riski transfer etme (bir ücret karşılığında) olmak üzere dört seçenek bulunmaktadır (Majuca, Yurcik ve Kesan, 2006: 2). Bireyler ve özellikle işletmeler açısından, riskten kaçınarak yani BT ürünlerini ve hizmetlerini kullanmayarak siber riskin yönetilmesi çoğu durumda ekonomik olarak mümkün olmayacağından, söz konusu riskin yönetilmesi sürecinde yönetimsel ve teknik süreçleri kullanarak riski azaltmaya yönelik adımlar atılması gerekli olmaktadır. Riski azaltmak amacıyla kullanılan araçların (yazılım güncellemeleri, antivirüs programları, verilerin sürekli yedeklenmesi, internet trafik yönetimi gibi) yeterli olmadığı durumlar için ise siber sigorta ile riski transfer etme olanağı bulunmaktadır (Eling ve Schnell, 2016: 480). Birey ve işletmeler genellikle bu seçenekleri bir arada kullanmakta yani siber riskin bir kısmını kabullenip üzerinde tutmakta, çeşitli teknoloji ve yöntemlerle bir kısmını azaltmakta ve geri kalanını da sigortalamayı tercih etmektedir (Schneier, 2001: 115). Siber risk, daha önce de ifade edildiği üzere, çok dinamik olduğundan ve önemli ölçüde değişim riskine maruz kaldığından, risk izleme de siber risk yönetim sürecinin önemli bir aşamasını oluşturmaktadır (Eling ve Schnell, 2016: 480).

Siber risk, mahiyeti gereği tüm işletmeleri etkilemektedir (Lloyd, 2020). Bunun sonucunda siber sigorta, her büyüklükteki işletme için siber risk tehdidini yönetmeye yönelik bir seçenek olarak ortaya çıkmakta ve günümüzde giderek daha çok tercih edilmeye başlamaktadır (Low, 2017). Bilgisayar suçlarına karşı özelleşmiş sigorta teminatı ilk kez 1970'lerin sonunda ortaya çıkmış olsa da, hacker saldırılarına karşı bilinen en eski ayrı bilgisayar korsanı sigorta poliçeleri ilk olarak 1990'lı yılların sonunda sunulmaya başlanmıştır (Majuca vd., 2006: 4-5). Zaman içinde, siber sigorta poliçeleri, siber risklerin sürekli gelişimi ve bilgi sistemlerinin karmaşıklığına uyum sağlamak için giderek daha sofistike hale gelmiştir (Marotta vd., 2017: 38). Ağ ve bilgisayar olaylarıyla ilişkili finansal risklerin üçüncü bir tarafa devrini sağlayan (Böhme ve Schwartz, 2010: 1) siber sigorta piyasalarının ana itici güçlerinden biri, büyük şirketlerde meydana gelen ve büyük kayıplara neden olan ciddi siber olaylar, diğeri ise veri korumaya ilişkin yasal düzenlemelerdir (Marotta vd., 2017: 38). Türkiye'de de 6698 sayılı Kişisel Verilerin Korunması Kanunu, 24 Mart 2016 tarihinde Türkiye Büyük Millet Meclisi'nde kabul edilmiş ve 7 Nisan 2016 tarihli ve 29677 sayılı Resmi Gazete'de yayımlanarak yürürlüğe girmiştir. Kişisel Verileri Koruma Kurumu (KVKK)'nun internet sitesinde ilan edilen veri ihlali bildirimlerinin sayısı, 2019 yılında 37 2020 yılında 30, 2021 yılında 50 ve 2022 yılında 47 olarak tespit edilmiştir (KVKK, 2023). Veri ihlali bildiriminde bulunan veri sorumluları arasında, başta teknoloji ve yazılım şirketleri olmak üzere, bankaların, sigorta şirketlerinin, sağlık kuruluşlarının, turizm şirketlerinin, havayolu şirketlerinin vd. yer aldığı görülmektedir.

Bireylerin ve işletmelerin BT kullanımları arttıkça, güvenlik açıkları ve siber saldırılar da artış gösterdiğinden, korunma önlemleri ve özellikle de siber sigortaya yönelik farkındalığın her geçen gün artması beklenmektedir. Munich Re tarafından yayımlanan Küresel Siber Risk ve Sigorta Araştırması 2022'de siber güvenlik ve sigortaya duyulan ihtiyacın istikrarlı bir şekilde arttığı ifade edilmekte ve 2022 yılı başında 9,2 milyar dolar olduğu tespit edilen küresel siber sigorta primlerinin 2025 yılına kadar yaklaşık 22 milyar dolara ulaşacağı tahmin edilmektedir. Araştırma bulgularına göre, siber saldırılardan en çok etkilenen BT, sağlık/ilaç ve finans sektörlerinde, hâlihazırda yürürlükte olan bir siber sigorta poliçesine sahip şirketlerin oranlarının daha yüksek olduğu tespit edilmiştir (Munich Re, 2022: 14).

Çalışmanın amacı, Türkiye'de siber sigortaya ilişkin piyasa uygulamalarının araştırılması ve Türkiye siber sigorta piyasasının incelenmesidir. Bu amaç doğrultusunda çalışmada ele alınan üç temel araştırma sorusu bulunmaktadır. Bunlardan birincisi Türkiye'de siber sigorta piyasasının mevcut durumunu, ikincisi Covid-19 salgınının siber sigorta piyasası üzerindeki etkilerini, üçüncüsü ise siber sigorta piyasasının önündeki fırsatları ve/veya engelleri ortaya koymayı amaçlamaktadır. Literatür incelendiğinde Türkiye'de siber sigorta piyasası ile ilgili çalışmaların sınırlı olduğu tespit edilmiştir. Bu nedenle çalışmanın siber sigorta ile ilgili literatüre katkı sağlaması beklenmektedir. Çalışma beş kısımdan oluşmakta olup, bir sonraki kısımda, dünyada ve Türkiye'de siber sigortaların ele alındığı önceki çalışmalar incelenmektedir. Üçüncü kısımda, çalışmada kullanılan görüşme sorularına ve veri toplama yöntemine yer verilmektedir. Dördüncü kısımda, araştırmanın bulguları ele alınmakta ve son kısımda ise sonuç ve değerlendirme sunulmaktadır.

2. Literatür İncelemesi

Siber risk, bireyler ve işletmeler için giderek büyüyen bir tehdit olup, yapısı gereği maliyetli ve tahripkâr etkilere sahiptir. Siber riskin yönetilmesi sürecinde siber sigortanın önemi her geçen gün artış göstermektedir. Siber riske ve siber sigortaya ilişkin artan farkındalığa rağmen, hem siber risk hem de siber sigorta ile ilgili araştırmaların sınırlı olduğu görülmüştür. Siber risk ve siber sigorta konularındaki araştırmaların sınırlı olmasının nedenlerinden biri, bu alanda güvenilir veri temin etmenin zor olmasıdır (Eling ve Wirfs, 2019: 1109). Mevcut çalışmalarda veri eksikliğinin ve modelleme zorluklarının vurgulandığı görülmektedir (Eling ve Schnell, 2016: 474, 478; Maillart ve Sornette, 2010: 363; Biener, Eling ve Wirfs, 2015: 149; Bouveret, 2018: 3). Bu kısımda, özellikle son on yılda sayılarında artış gözlenen, dünyada ve Türkiye'de siber sigortaların ele alındığı çalışmalar incelenmektedir.

1990'lı yılların sonlarından 2005 yılına kadar olan süreçte siber sigortanın zaman içindeki gelişimini inceleyen Majuca, Yurcik ve Kesan (2006), siber sigorta sektörünün büyük ölçüde düşük teminatlı birinci şahıs siber sigorta poliçelerinden daha yüksek teminatlı birinci ve üçüncü şahıs siber sigorta ürünleri sunan daha karmaşık, ürüne göre farklılaştırılmış poliçelere doğru olgunlaştığını ifade etmişlerdir. Ayrıca, siber risklerin sigortalanabilirliğindeki temel sorunları (ters seçim ve ahlaki tehlike gibi) ele aldıkları çalışmalarında, siber sigorta ürünlerinin interneti daha güvenli bir ortam haline getirdiği sonucuna varmışlardır. Siber sigorta piyasasının gelişiminin ele alındığı bir diğer çalışmada Baer ve Parkinson (2007), siber sigortanın faydalarını, ortaya çıkış sürecini, mevcut durumunu ve genişlemesinin önündeki engelleri (asimetrik bilgi, birbirine bağlı ve ilişkili riskler, yetersiz reasürans kapasitesi vd.) incelemiştir. Sigorta şirketleri halihazırda siber sigorta ürünleri sunuyor olsa da, siber sigorta poliçelerinin doğru fiyatlandırılıp fiyatlandırılmadığının hala açık bir soru olduğunu ifade eden Herath ve Herath (2011), siber sigorta primlerini belirlemek için copula metodolojisini kullanarak bir siber sigorta fiyatlandırma modeli geliştirdikleri çalışmalarında, üç tür sigorta poliçesi modeli kullanarak birinci şahıs kayıpları için prim tutarını copula tabanlı bir simülasyon yaklaşımı ile tahmin etmiştir. Biener vd. (2015) tarafından yapılan çalışmada ise siber riskin yönetiminde sigortanın yeterliliğinin araştırılması amacıyla 994 siber kayıp vakası incelenmiş ve bu vakaların istatistiksel özellikleri analiz edilmiştir. Elde edilen ampirik sonuçlar, siber riskin diğer operasyonel risklerle karşılaştırıldığında belirgin özelliklerini vurgulamakta ve bu risklerin sigortalanabilirliği ile ilgili birbiriyle yüksek oranda ilişkili kayıplar, veri eksikliği ve ciddi bilgi asimetrilerinden kaynaklanan önemli sorunlar olduğunu ortaya koymaktadır. Çalışmada, bu sorunların siber sigorta piyasasının gelişimini engellediği belirtilmiş, siber riske maruziyetin nasıl daha iyi yönetilebileceği tartışılmış ve gelecekteki araştırmalar için önerilerde bulunulmuştur.

Siber risk ve siber sigorta alanında bir literatür incelemesi gerçekleştiren Eling ve Schnell (2016), ulaştıkları araştırma bulgularını siber riskin tanımı ve sınıflandırılması, siber riskin neden olduğu maliyetler, siber riskle ilgili verilerin temini, siber riskin modellenmesi, siber risk yönetimi organizasyonu, siber riskin küresel ekonomi ve toplum için bir tehdit olup olmadığı ve siber sigorta piyasasının mevcut görünümü ve sigortalanabilirlik konusundaki başlıca zorluklar olmak üzere yedi başlık altında derleyerek siber risk ve siber sigorta alanlarındaki ana araştırma konularına genel bir bakış sunmuşlardır. Değişim riski, ahlaki tehlike, veri ve modelleme eksikliği gibi nedenlerle siber riski sigortalamada önemli zorluklar olduğunu ifade ettikleri çalışmalarında, bu zorlukların üstesinden gelmede zorunlu raporlama yükümlülükleri getirilmesi, riskin azaltılması için minimum düzeyde güvenlik sağlamaya yönelik asgari standartlar tanımlanması, özellikle verilere ve modellemeye ilişkin belirsizlikleri azaltmaya yönelik kamu-özel ortaklığı olabilecek anonim bir veri havuzu geliştirilmesi gibi çeşitli yolları ele almışlardır. Siber sigortayla ilgili mevcut literatürün kapsamlı bir araştırmasının sağlandığı bir diğer çalışma Marotta vd. (2017) tarafından yapılmış olup, çalışmada siber sigorta ile ilgili temel bilgiler özetlenmiş, siber sigorta piyasasının analizine yönelik mevcut bilimsel yaklaşımlar karşılaştırılmış, farklı teknolojik sistemlerde siber sigortanın uygulanabilirliği analiz edilmiş ve siber sigorta araştırmalarında daha fazla ilerleme için önerilerde bulunulmuştur. Yavaş bir başlangıca ve gelişme yolundaki bir dizi zorluğa rağmen siber sigorta piyasasının büyüdüğü, bu büyüme üzerinde konu ile ilgili yasal düzenlemelerin de etkili olduğu ve siber sigortanın siber riskin yönetiminde önemli bir fırsat olduğu ifade edilmiştir.

Katastrofik kayıplara yol açabilecek aşırı siber risk senaryolarının sigortalanabilirliği ile ilgili olarak Eling, Elvedi ve Falco (2022) tarafından yapılan çalışmada, yaygın olarak tartışılan altı "aşırı" siber risk

senaryosunun ekonomik etkileri analiz edilmiş ve tahmin edilen potansiyel ekonomik kayıpların sigortalanabilir bir aralıkta kaldığı ve geleneksel sigorta ve reasürans piyasası tarafından karşılanabileceği ifade edilmiştir. Söz konusu çalışmada elde edilen bulgular, sigorta ve reasürans şirketlerinin aşırı siber kayıp senaryoları için teminat sağlama kapasiteleri konusunda olumlu olarak değerlendirilmiştir. Siber risk için sigortanın uygulanabilirliğini ele alan başka bir çalışma, Malavasi, Peters, Shevchenko, Trück, Jang ve Sofronov (2022) tarafından, Advisen tarafından sağlanan siber olaylara ilişkin bir veri seti kullanılarak Amerika Birleşik Devletleri (ABD)'nde siber sigorta sektörü üzerine yapılmıştır. Çalışmada ilk olarak, siber kayıp olaylarının sıklığını ve şiddetini açıklayabilecek değişkenler ve bu değişkenlerin siber risk kategorilerine göre heterojen olup olmadığı araştırılmıştır. İkinci olarak da, siber riskin, gerekli primler ve risk havuzu büyüklükleri açısından sigortalanabilir olup olmadığı ve bu kararın sigortalı şirketlerin sektöründen ve büyüklüğünden etkilenip etkilenmediği ele alınmıştır. Araştırma sonucunda, şirket büyüklüğünün ve sektörünün siber olay sıklığı ve şiddeti üzerindeki etkisinin siber riske göre değiştiği belirlenmiştir. Ayrıca, siber sigorta primlerinin de siber risk türüne göre farklılık gösterdiği tespit edilmiştir.

Siber riski, siber sigortayı ve siber riskin sigortalanabilirliğini ele alan çalışmalar yanı sıra siber sigorta piyasasına ve özellikle siber sigorta sunan şirketlere odaklanan çalışmalar da bulunmaktadır. Franke (2017), İsveç sigorta piyasasında faaliyet gösteren 10 sigorta şirketiyle yapılan yarı-yapılandırılmış görüşmelere ve ayrıca iki reasürans şirketi ve üç sigorta aracısıyla yapılan ek görüşmelere dayanan çalışmasında, İsveç'teki siber sigorta piyasasının mevcut durumunu ortaya koymuştur. Yapılan görüşmeler neticesinde, araştırmanın gerçekleştirildiği dönemde, İsveç'te siber sigortanın çoğunlukla nispeten büyük şirketler tarafından satın alındığı, daha küçük şirketlerin ise siber sigortayı ancak iş yapabilmeleri için olmazsa olmaz bir unsur olması durumunda talep ettiği tespit edilmiştir. Siber sigorta piyasasında, özellikle büyük müşterilere özel karmaşık bir sigortalama sürecinin söz konusu olduğu, ancak bazı niş sigorta şirketlerinin giderek daha küçük müşterileri hedefleyen daha basit poliçeler sunmaya yöneldiği ifade edilmiştir. Söz konusu dönemde tarihsel verilere dayalı aktüeryal bir fiyatlandırma olmadığından, siber sigortanın doğru fiyatlandırılmasının zor olduğu, ancak uzun vadede, piyasa aktörleri arasında fiyatların daha doğru hale geleceğine dair bir düşünce olduğu belirtilmiştir. Sigorta şirketlerinin BT güvenliği zayıf olan müşterileri sigortalamaktan kaçındıkları, dolayısıyla siber sigortanın uygulamada sadece bir risk transfer aracı olmadığı, riskten kaçınma ve riski azaltma yönlerini de içerdiği vurgulanmıştır. Ayrıca sigorta şirketleri arasındaki farklılıkları da içerecek şekilde siber sigorta kapsamında sunulan teminatlar da ele alınmıştır. Çalışma, İsveç siber sigorta piyasası ile sınırlı olsa da, elde edilen bulguların bazı yönleriyle daha geniş bir ilgi alanına sahip olabileceği ifade edilmiştir.

Xie, Lee ve Eling (2020) çalışmalarında; ABD siber sigorta piyasasında, sigorta şirketlerinin siber sigorta piyasasına girme motivasyonunun, halihazırda siber sigorta sunan şirketlerin siber teminat miktarının ve siber sigorta şirketlerinin performansının belirleyicilerini ampirik olarak incelemiştir. Analiz sonuçları, sigorta şirketlerinin siber sigorta piyasasına yalnızca işlerinin büyümesi üzerindeki kısıtlamaların üstesinden gelmek için katılmadıklarını, daha ziyade siber riskleri anlama ve fiyatlandırma konusundaki potansiyel rekabet avantajlarından yararlanmak için siber sigorta sunduklarını göstermiştir. Sigorta şirketleri tarafından sunulan kapsamın türünün (tek başına veya paket halinde) ve miktarının, şirketin özelliklerine göre önemli ölçüde farklılık gösterdiği tespit edilmiştir. Ayrıca, çalışmada reasüransın sunulan teminat miktarını önemli ölçüde etkilediği ve siber reasürans piyasasının gelişiminin bir bütün olarak siber sigorta piyasasının sağlıklı büyümesi için zorunlu olduğu ifade edilmiştir. Siber sigorta şirketlerinin performansı ile ilgili olarak ise siber sigorta hasar prim oranlarındaki değişimlerin prim artışından değil, hasar sıklığı ve şiddetindeki artıştan kaynaklandığı tespit edilmiştir.

ABD siber sigorta piyasasına ilişkin yapılan bir başka çalışmada, Cole ve Fier (2021), sigorta şirketlerinin hem siber teminat yazma kararını hem de siber sigorta piyasasına ne ölçüde katıldığını etkileyen faktörleri bir panel veri seti kullanarak incelemiştir. Ayrıca, sigorta şirketlerinin ABD siber sigorta piyasasındaki performansı da ampirik olarak araştırılmıştır. Modellerin her birinde, sigorta şirketlerinin siber sigorta piyasasına katılma kararını, siber sigorta piyasasına dahil olma derecesini ve siber sigorta piyasasındaki performansını etkileyen hem finansal hem de operasyonel değişkenlere yer verilmiştir. Çalışmada elde edilen bulgular, ABD siber sigorta piyasasının oldukça yoğunlaştığını ve

büyüklük, iş karması, reasürans kullanımı ve organizasyon yapısı gibi firmaya özgü özelliklerin hem piyasaya katılımı hem de katılımın kapsamını etkileme eğiliminde olduğunu göstermiştir. Ayrıca, şirket büyüklüğü, reasürans kullanımı, çeşitlendirme, grup üyeliği, organizasyon yapısı gibi faktörlerin her birinin performansı farklı ve önemli şekillerde etkilediğine dair kanıtlar elde edilmiştir.

Türkiye'de siber sigortayı inceleyen çalışmaların ise daha sınırlı olduğu görülmektedir. Kuru ve Bayraktar (2017) tarafından yapılan çalışmada, ABD, İngiltere ve Türkiye arasında karşılaştırma yapılarak siber sigorta ve sosyal refah arasındaki ilişki analiz edilmiş ve siber sigortanın, interneti tüm kullanıcılar için daha güvenli hale getirerek sosyal refah üzerinde olumlu bir etkiye sahip olabileceği ifade edilmiştir. Altuntaş, Kara, Soylu ve Kırkbeşoğlu (2018) tarafından yapılan çalışmada, Türk sigorta sektörünün siber risklere güvence sağlama konusundaki etkinliği analiz edilmiştir. İki farklı veri toplama tekniğinin seçildiği çalışmada, ilk olarak belirlenen üç şirketin (elementer sigorta şirketi, brokerlik ve acente) siber sigorta konusunda deneyimli (siber sigorta teminatı sunmuş veya buna aracılık etmiş) yöneticileriyle yarı-yapılandırılmış görüşmeler gerçekleştirilmiş ve öncelikli olarak siber sigortanın Türkiye'deki yeri ve önemi tespit edilmeye çalışılmıştır. Çalışmada kullanılan bir diğer veri toplama tekniği ise söylem analizidir. Çalışma neticesinde, Türkiye'de siber riske ilişkin farkındalığın ve risk algısının henüz düşük düzeyde seyrettiği tespit edilmiştir. Ayrıca çalışmada Türkiye'de siber sigorta satışının söz konusu dönem itibarıyla pek yaygın bir uygulama olmadığı ifade edilmiştir. Bu durumun gerekçesi olarak, sigorta şirketlerinin işletmelerde konu ile ilgili yeterli teknik bilgiye sahip personel olmaması ve işletmelerin üst yönetimi ve çalışanlarının farkındalığının yetersiz olması sebebiyle bu sigorta ürününü sunmaktan kaçındıkları belirtilmiştir.

Siber sigortanın Türkiye özelinde incelendiği bir başka çalışmada Cebeci (2021), siber sigortanın önemini ve Türkiye'deki mevcut durumunu ele almıştır. Çalışmada siber saldırılar neticesinde ortaya çıkan veri ihlallerinin, finansal zararların ve itibar kayıplarının işletmeler için ciddi sorunlar olduğu ifade edilmiştir. Saldırıların ağırlıklı olarak küçük işletmeleri hedef aldığı ve bu işletmelerle faaliyette bulunan büyük işletmelerin de bu saldırılardan etkilendiği tespit edilmiştir. Türkiye'de sigorta sektöründe siber risklere karşı sunulan ürünlerin var olduğu ancak hem bireysel hem de kurumsal anlamda bu ürünlere yönelik farkındalığın artırılması gerektiği belirtilmiştir.

3. Veri ve Yöntem

Çalışmanın bu kısmında, görüşmelerde kullanılan sorular ve veri toplama yöntemi incelenmektedir.

3.1. Görüşme Soruları

Görüşme soruları, araştırmacılar tarafından bu çalışmanın temel araştırma soruları doğrultusunda ve Franke (2017)'nin çalışmasından yararlanılarak hazırlanmış olup, iki uzman (sigortacılık alanında çalışan bir akademisyen ve sigorta sektöründe çalışan bir uzman) görüşü ile yeniden gözden geçirilip düzenlenmiştir. Yarı-yapılandırılmış görüşmelerde kullanılan sorular şunlardır:

1. Siber risk olaylarına karşı sigorta sunuyor musunuz? Sunulan bu sigortayı bireylere mi yoksa işletmelere mi sunuyorsunuz? Sunduğunuz ürün, siber sigorta mı? Yoksa siber risklere karşı da teminat sağlayan farklı bir sigorta mı sunuyorsunuz?
2. Türkiye'de siber sigorta pazarı ve pazar payınız ne kadar büyük? Siber sigortaya ilişkin poliçe sayınıza, toplam prim üretiminize, sunulan sigorta bedeline ve ödenen hasar tutarına ilişkin bilgi verebilir misiniz? Müşterilerinizin ölçeği (küçük, orta ya da büyük ölçekli işletme) hakkında bir değerlendirme yapabilir misiniz?
3. Siber sigorta fiyatlandırma süreciniz hakkında bilgi verebilir misiniz? Örneğin, fiyatlandırma sürecinde hangi veri ve/veya yöntem(ler)i kullanıyorsunuz?
4. Fiyatlandırma, siber sigorta talebinde bulunan işletmelerin faaliyet gösterdiği sektör, aktif büyüklüğü, yıllık ciro gibi faktörlerden etkileniyor mu? İşletmeleri değerlendirmek için belirli yöntemler kullanıyor musunuz?
5. Siber sigorta talep eden bir işletmenin yerine getirmesi gereken şartlar var mı? Sigortayı sunmaya yönelik ön koşullarınız bulunuyor mu? Varsa bu şartların sağlanması sürecinde işletmelerle birlikte çalışıyor musunuz?
6. Siber sigorta kapsamında sunduğunuz teminatlar nelerdir? İsteğe bağlı teminatlar bulunuyor mu?

7. Siber sigorta poliçesine sahip bir sigortalı bir siber olay şüphesi olduğunda ne yapmalı? Sigorta şirketi olarak hangi aşamada müdahil oluyorsunuz? Bu süreçte birlikte çalıştığınız iş ortaklarınız var mı?
8. Dijital ticaretin ve işlemlerin artış gösterdiği Covid-19 salgını süreci siber sigorta talebini, prim üretimini ve siber olaylara yönelik hasarları nasıl etkiledi? Bu konudaki görüşlerinizi paylaşabilir misiniz?
9. Siber riske yönelik sigorta sürecinde yaşanan zorluklar nelerdir? Türkiye'de siber sigorta pazarının önündeki fırsatlar/engeller nelerdir? Bu konuda bir değerlendirme yapabilir misiniz?

Görüşme sırasında alınan cevaplar doğrultusunda konuyu daha derinlemesine inceleyebilmek amacıyla araştırmacılar tarafından görüşme sorularını tamamlayıcı ek sorular da yöneltilmiştir. Örneğin birinci soruya ek olarak "Hangi tarihten bu yana ya da ne kadar süredir siber riske yönelik sigorta sunuyorsunuz?" veya "Ürünü sunmaya yönelik çalışmalarınız var mı?", dördüncü soruya ek olarak "Siber sigorta ürününü sunmaktan kaçındığınız sektör(ler) var mı?", yedinci soruya ek olarak "İş ortaklarınız yerli firmalar mı?" gibi ek sorular ihtiyaç olması durumunda yöneltilmiştir.

3.2. Veri Toplama Yöntemi

Nitel araştırma yönteminin kullanıldığı bu çalışmada, nitel araştırmalarda sıklıkla kullanılan veri toplama tekniklerinden biri olan görüşme (mülakat) tekniği tercih edilmiştir. Görüşmenin çok çeşitli türleri bulunmakla birlikte, genellikle görüşme üzerindeki kontrol düzeyine göre, yapılandırılmamış görüşme, yarı-yapılandırılmış görüşme ve yapılandırılmış görüşme olarak sınıflandırılmaktadır (Gürbüz ve Şahin, 2018: 184). Nitel görüşmenin temel amacı araştırma konusunu katılımcıların bakış açısıyla ele almak olduğundan, nitel görüşmelerin daha az yapılandırılmış olması ve daha açık uçlu sorularla yürütülmesi gerektiği ifade edilmektedir (Gürbüz ve Şahin, 2018: 430). Bu doğrultuda çalışmada, Franke (2017) tarafından yapılan çalışma da takip edilerek, veri toplama aracı olarak yarı-yapılandırılmış görüşme tekniğinden yararlanılmıştır. Yarı-yapılandırılmış görüşme, araştırmacıya hem görüşme rehberi doğrultusunda ilerleme, hem de gerektiğinde daha derinlemesine gidebilme imkânı sağlamaktadır (Gürbüz ve Şahin, 2018: 184). Türkiye'de siber sigorta piyasasının arz tarafını sigorta şirketleri, sigorta aracıları (sigorta acentesi ve brokeri) ve reasürörler oluşturmaktadır. Türkiye siber sigorta piyasasına ilişkin ilk elden deneyimlerin ve görüşlerin elde edilmesi amacıyla arz yönlü aktörlerden biri olan hayat dışı sigorta şirketlerinin siber sigorta konusunda uzman yöneticileriyle yarı-yapılandırılmış görüşmeler yapılmıştır.

Türkiye'de siber sigorta sunan şirketlere ilişkin bilgi alabilmek amacıyla Ağustos 2022'de Türkiye Sigorta Reasürans ve Emeklilik Şirketleri Birliği (TSB) ile e-posta aracılığıyla iletişime geçilmiş ancak siber sigorta sunan sigorta şirketlerinin bir listesi temin edilememiştir. Sigortacılık Muhasebe Sistemi'nde her bir branş altında ihdas edilen alt branşlar için bir defter-i kebir hesabı oluşturulmaktadır. Alt branşlara ilişkin teknik gelir ve giderlerin takip edilebilmesi için ise Sigortacılık Hesap Planı'nda her bir alt branşa ilişkin yardımcı, alt ve tali hesaplar açılmaktadır. Türkiye'de siber sigorta sunan sigorta şirketlerinin listesinin verilememesinin ve siber sigortaya ilişkin yazılan primler, ödenen hasarlar gibi istatistiki bilgilerin paylaşılamamasının gerekçesi olarak, Sigortacılık Hesap Planı'nda henüz siber sigorta için açılmış bir hesabın bulunmaması gösterilmiştir.

Türkiye'de siber sigorta ürünü sunan toplam şirket sayısını tam olarak tespit etmek mümkün olmadığından, hayat dışı alanında faaliyet gösteren sigorta şirketlerinin (yurt dışında kurulmuş sigorta şirketlerinin Türkiye'deki şubeleri dahil) kurumsal web siteleri incelenerek sundukları ürünler arasında bireysel ve/veya kurumsal siber sigorta bulunan şirketler ile e-posta ve/veya telefon aracılığıyla iletişim kurulmuştur. Bu şekilde toplam on altı sigorta şirketi ile temasa geçilmiş ve bunlardan altı hayat dışı sigorta şirketi görüşmeyi kabul etmiştir.

Yedi görüşmenin tamamı online görüşme yoluyla gerçekleştirilmiştir ve görüşmelerin tamamına her iki yazar da katılmıştır. Yedi görüşmede altı şirketten on iki katılımcı ile görüşme gerçekleştirilmiştir. Altı şirket olmasına rağmen yedi görüşme yapılmasının nedeni, bir şirketi temsil eden iki katılımcı ile ayrı ayrı zamanlarda görüşme yapılmış olmasıdır. Görüşmelerin başında katılımcılara, şirket ve katılımcı bilgilerinin gizli tutulacağı ifade edilmiştir. Görüşülen kişilerin yarısı genel müdür yardımcısı olup, diğer yarısı ise başkan yardımcısı, müdür, direktör ya da uzman pozisyonlarındaki kişilerdir. Her bir şirket ile yapılan görüşmeler yaklaşık olarak birer saat sürmüştür. Çalışmada görüşülen şirket ve kişi

bilgilerinin gizli tutulmasına yönelik olarak şirketler; Şirket 1 (Ş1), Şirket 2 (Ş2), Şirket 3 (Ş3), …, Şirket 6 (Ş6) olarak kodlanmıştır. Görüşülen şirketlerden biri (Ş6), yapılan görüşmenin ardından e-posta aracılığıyla görüşme sorularına ilişkin özet niteliğindeki cevaplarını yazılı olarak da göndermiştir. Söz konusu görüşmelere ek olarak, Türkiye'de siber sigorta konusunda deneyimli iki sektör temsilcisi ile de ayrı ayrı görüşme gerçekleştirilmiş ve araştırma soruları çerçevesinde genel olarak Türkiye siber sigorta piyasası ile ilgili görüş ve değerlendirmeleri alınmıştır.

Tüm görüşmelerin tamamlanmasının ve çalışmanın taslağının hazırlanmasının ardından, özellikle çalışmanın bulgular kısmını gözden geçirmeleri ve gerek verdikleri cevaplarla ilgili varsa yanlış anlaşılan kısımları, gerekse şirketlerinin ve kendilerinin gizliliğini açığa çıkaracak bir bilgi paylaşıldıysa bunları tespit etmeleri için, e-posta aracılığıyla çalışmanın taslağı katılımcılara gönderilmiştir. Görüşme gerçekleştirilen tüm şirketler için çalışmanın taslağı ile ilgili olarak geri bildirimde bulunulmuştur. Katılımcıların büyük bölümü gizliliği açığa çıkaracak bir bilgi paylaşılmadığını teyit etmişler ve bulgular kısmının görüşmelerde verdikleri cevapları yansıttığını ifade etmişlerdir. Bazı katılımcılar ise düzeltme önerilerinde bulunmuş olup, söz konusu geri dönüşler doğrultusunda, gerekli düzeltmeler yapılmıştır.

4. Bulgular

Çalışmanın bu kısmında, üç temel araştırma sorusu çerçevesinde, yarı-yapılandırılmış görüşmeler neticesinde elde edilen temel bulgular sunulmaktadır.

4.1. Türkiye'de Siber Sigorta Piyasasının Mevcut Durumu

Türkiye'de siber sigorta piyasasının mevcut durumunun ortaya koyulmaya çalışıldığı ilk araştırma sorusuna ilişkin özet bulgulara Tablo 1'de yer verilmektedir. Tablo 1'de katılımcılar yerli ve yabancı şirket ayrımında incelendiğinde, görüşme gerçekleştirilen şirketlerin üçünün yabancı sermayeli şirket, kalan üçünün ise yerli sermayeli şirket olduğu görülmektedir. Ş3, Ş4 ve Ş6, Türkiye hayat dışı sigorta sektöründe faaliyet gösteren yabancı sermayeli; Ş1, Ş2 ve Ş5 ise yerli sermayeli şirketlerdir. Katılımcılar ile yapılan görüşmeler neticesinde elde edilen veriler incelendiğinde, Türkiye'de siber sigorta piyasasında,

- bireylere yönelik paket poliçe olarak sunulan bireysel siber sigorta,
- küçük ve orta büyüklükteki işletme (KOBİ)'lere yönelik paket poliçe olarak sunulan kurumsal siber sigorta ve
- büyük ve orta boy işletme (BOBİ)'lere "müşteriye özel" (terzi usulü) olarak sunulan kurumsal siber sigorta

olmak üzere üç tür siber sigorta ürünü sunulduğunu ifade etmek mümkündür. Görüşme gerçekleştirilen tüm şirketler (Ş6 haricinde) paket poliçe niteliğinde bireysel siber sigorta sunmaktadır. Ş2, Ş4 ve Ş5 KOBİ'lere yönelik siber sigorta paket poliçe hazırlıklarının devam ettiğini ve kısa vadede satışa sunmayı planladıklarını ifade etmektedir. Ş6, büyük ve orta boy işletmelere 2015 yılından bu yana müşteriye özel kurumsal siber sigorta sunmaktadır. Diğer dört şirket (Ş1, Ş2, Ş3 ve Ş5) ise az sayıda büyük ölçekli kurumsal siber sigorta poliçelerinin olduğunu ifade etmektedir. Sundukları siber sigorta ürünleri ve Tablo 1'de özetlenen poliçe sayıları göz önüne alındığında, mevcut durumda Ş1'in ana pazar bölümünün bireyler ile küçük ve orta büyüklükteki işletmeler, Ş6'nın ana pazar bölümünün büyük ve orta boy işletmeler, diğer şirketlerin (Ş2, Ş3, Ş4 ve Ş5) ana pazar bölümünün ise bireyler olduğu ifade edilebilir.

Görüşmelerde Ş2 siber sigortanın ayrı bir ürün olarak sunulduğunu, siber risklerin yer aldığı ve teminat verildiği farklı bir sigorta ürünü sunulmadığını belirtmektedir. Ş3, kurumsal siber sigortanın ayrı bir ürün olarak sunulduğunu, ancak bireysel siber sigorta ürününün sadece siber saldırılar ile sınırlı olmayıp, daha geniş kapsamlı bir paket ürün şeklinde sunulduğunu ifade etmektedir. Ş4, sundukları farklı bir sigorta ürününe siber risk teminatlarının eklendiğini ve bireysel siber sigortanın bu şekilde sunulduğunu belirtmektedir. KOBİ'lere yönelik kurumsal siber sigorta ürünü hazırlıklarının devam ettiğini ifade eden Ş5, bu ürünü hem ayrı bir ürün olarak hem de KOBİ'lere yönelik farklı sigorta ürünleri ile birleştirerek sunmayı planlamaktadır. Ş5 tarafından sunulan bireysel siber sigorta ürünü ise yine geniş kapsamlı bir paket ürün olup siber risk teminatlarına ek teminatlar (isteğe bağlı) da içerebilmektedir.

Tüm görüşmelerde, TSB tarafından yayımlanan istatistiki veri olmaması sebebiyle, Türkiye'de siber sigorta pazarının büyüklüğünü ve şirketlerin pazar payını tahmin etmenin zor olduğu ifade edilmektedir. Bununla birlikte, Ş4, Türkiye'de siber sigorta yıllık toplam prim üretiminin yaklaşık 250-300 milyon TL arasında; Ş6 ise, Türkiye'de siber sigortaya ilişkin doğrudan teminat sağlayan şirketlerin prim üretiminin yaklaşık 10 milyon $ olduğunu tahmin etmektedir. Ayrıca, görüşmelerde, 2022 yılı için bazı şirketler poliçe sayılarına, bazı şirketler ise prim üretimlerine ilişkin bazı yaklaşık veriler sunmuşlardır. Ş1, KOBİ'lere yönelik kurumsal siber sigorta paket poliçe sayılarının 10.000'i aştığını ve az sayıda büyük ölçekli kurumsal siber sigorta poliçelerinin olduğunu; Ş2, bireysel siber sigorta paket poliçe sayılarının yaklaşık 100.000 adet olduğunu ve 15-20 adet büyük ölçekli kurumsal siber sigorta poliçelerinin bulunduğunu ifade etmektedir. Ş2'nin siber sigorta prim büyüklüğü 60 milyon TL'nin üzerinde olup, yaklaşık olarak yarısı bireysel yarısı ise büyük ölçekli kurumsal siber sigorta poliçelerine aittir. Ş3, siber sigorta prim üretimine ilişkin net bir veri paylaşmamakla birlikte, toplam prim üretimleri içinde siber sigortaların payının henüz çok küçük olduğunu ifade etmektedir. Ş4'ün siber sigortalara ilişkin yaklaşık bir milyon TL prim üretimi, Ş5'in ise 2.000-3.000 adet bireysel siber sigorta paket poliçesi ile az sayıda büyük ölçekli kurumsal siber sigorta poliçesi bulunmaktadır. Ş6, poliçe sayısına ilişkin bir veri paylaşmamakla birlikte, siber sigorta prim büyüklüğünün 5-6 milyon $ olduğunu ifade etmektedir.

Tablo 1. Türkiye'de Siber Sigorta Piyasasının Mevcut Durumuna İlişkin Özet Bulgular

Sigorta Şirketi	Sahiplik Yapısı	Sunulan Siber Sigorta Ürünü	Ana Pazar Bölümü	Poliçe Sayısı	Prim Üretimi	Hasar Tutarı/Sayısı
Ş1	Yerli sermayeli	- Bireysel Siber Sigorta (paket poliçe) - Kurumsal Siber Sigorta ▪ Az sayıda büyük ölçekli poliçe ▪ KOBİ'lere yönelik paket poliçe	Bireysel ve KOBİ	- Bireysel: Veri yok - KOBİ'lere yönelik paket poliçe>10.000 - Az sayıda büyük ölçekli poliçe	Veri yok	En çok karşılaşılan hasar türü siber şantaj
Ş2	Yerli sermayeli	-Bireysel Siber Sigorta (paket poliçe) (2022) - Kurumsal Siber Sigorta ▪ Az sayıda büyük ölçekli poliçe ▪ KOBİ'lere yönelik paket poliçe hazırlığı	Bireysel	- Bireysel: Yaklaşık 100.000 adet - Kurumsal: 15-20 adet büyük ölçekli poliçe	>60 milyon TL (yaklaşık olarak yarısı bireysel, yarısı kurumsal)	Hasar sıklığı ve hasar tutarı düşük
Ş3	Yabancı sermayeli	-Bireysel Siber Sigorta (paket poliçe) - Kurumsal Siber Sigorta	Bireysel	- Bireysel: Net veri yok ancak yüksek satış adedi - Kurumsal:	Bireysel: Veri yok Kurumsal: Toplam prim üretimindeki	Bireysel: Küçük ölçekli gerçekleşen hasarlar Kurumsal: Hasar gerçekleşmedi

		(az sayıda büyük ölçekli poliçe)		3-4 büyük ölçekli poliçe	payı çok küçük	
Ş4	Yabancı sermayeli	-Bireysel Siber Sigorta (paket poliçe) (2022) - KOBİ'lere yönelik paket poliçe hazırlığı	Bireysel	Veri yok	Bir milyon TL	Bireysel: Küçük ölçekli gerçekleşen hasarlar (Prim büyüklüğünün %10-15'i kadar)
Ş5	Yerli sermayeli	-Bireysel Siber Sigorta (paket poliçe) (2019) - Kurumsal Siber Sigorta ▪ Az sayıda büyük ölçekli poliçe ▪ KOBİ'lere yönelik paket poliçe hazırlığı	Bireysel	- Bireysel: 2.000-3.000 poliçe - Kurumsal: 2-3 büyük ölçekli poliçe	Veri yok	Siber sigortalarda hasar gerçekleşmedi
Ş6	Yabancı sermayeli	Kurumsal Siber Sigorta (2015)	Büyük ve orta boy işletmeler	Veri yok	5-6 milyon $	Tazminat ödemesi gerçekleşen ve takip süreci devam eden hasarlar mevcut

Yapılan görüşmelerde hasar tutarı ile sayısına ilişkin bir veri paylaşılmamakla birlikte, Ş1, mevcut durumda siber sigortada çok büyük boyutlu tazminat ödemeleriyle henüz karşılaşılmadığını ve KOBİ'lere yönelik paket poliçe niteliğinde sunulan kurumsal siber sigortada en çok karşılaşılan hasar türünün siber şantaj olduğunu; Ş2, siber sigortaya ilişkin hasar sıklığı ve hasar tutarının düşük olduğunu; Ş3, bireysel siber sigortada gerçekleşen küçük ölçekli hasarlar olduğunu, ancak kurumsal siber sigorta poliçelerine ilişkin henüz bir hasar ile karşılaşmadıklarını; Ş4, bireysel siber sigortada gerçekleşen hasarın prim büyüklüğünün %10-15'i kadar olduğunu; Ş5, henüz siber sigortaya ilişkin bir hasarla karşılaşmadıklarını ifade etmektedir. Ş6 ise, siber olaya müdahale teminatının ve siber şantaj teminatının ödendiği hasarlar gerçekleştiğini, hala takip süreci devam eden hasarlar olduğunu, ancak siber sigorta poliçesinin %100 teminatının tetiklendiği, tüm teminatın bir anda ödendiği bir durumun henüz yaşanmadığını belirtmektedir.

- *Sigortalama Süreci ve Fiyatlandırma*: Türkiye'de siber sigortaya ilişkin fiyatlandırma sürecinin ve bu süreçte kullanılan veri ve yöntemlerin sunulan siber sigorta ürününün türüne ve siber sigortaya ilişkin sunulan teminatın doğrudan sigorta şirketi tarafından mı yoksa küresel ölçekte faaliyet gösteren büyük reasürörlerden teminat temin edilerek mi sunulduğuna bağlı olarak değişiklik gösterdiğini ifade etmek mümkündür. Yapılan görüşmeler doğrultusunda, paket poliçe niteliğinde sunulan bireysel siber sigortanın, her iş bazında bir yazım, risk ve fiyatlandırma (underwriting) sürecine gerek kalmadan, yani her iş bazında sigorta şirketine yeniden bilgi akışına ve yeniden fiyatlandırma sürecine gerek kalmadan, satış kanalları üzerinden satışı gerçekleştirilebilmektedir. Bununla birlikte, bireysel siber sigortanın satışı sürecinde bireylerin doldurması gereken birkaç sayfalık bir bilgi formu (poliçenin genel sorularını, bireyin teminat altına alınmasını istediği hizmet listesini vb. içeren) olduğu anlaşılmaktadır. KOBİ'lere yönelik paket poliçe niteliğindeki kurumsal siber sigorta ürünlerinin, verilen siber risk teminatlarına

ilişkin çeşitli alternatifler içeren standart poliçeler olması ve fiyatlarının da önceden belli olması sebebiyle, yazım süreci bakımından bireysel siber sigortaya benzer olduğu ifade edilebilir.

Büyük ölçekli kurumsal siber sigorta poliçelerinde ise "terzi usulü" her işe özel yazım süreci söz konusudur. Fiyatlandırma sürecinde, diğer siber sigorta ürünlerinde olduğu gibi yine soru formlarından yararlanıldığı ancak çok daha detaylı soru formlarının kullanıldığı, daha kapsamlı risk inceleme ve değerlendirmelerinin yapıldığı, gerekli olması durumunda ek sorular sorulabildiği ve belge talep edilebildiği ifade edilmektedir. İşletmenin cirosu, faaliyet gösterdiği sektör, talep ettiği teminatlar ve teminat limitleri, veri gizliliği ve güvenliği, yedekleme mekanizmaları, uzman bilgi güvenliği ekibinin varlığı, sistemsel altyapının konumu ve kimlerin erişebildiği, siber saldırılara yönelik müdahale ve kurtarma yeteneği, bilgi güvenliği alanında sahip olduğu uluslararası sertifika(lar), geçmişte bir siber saldırı ya da saldırıya bağlı hasar gerçekleşip gerçekleşmediği gibi bilgilerin talep edildiği soru formlarını siber sigorta talep eden işletmelerin BT yetkilileri ile finans uzmanları doldurmakta, formların doldurulması sürecinde siber sigorta alanında uzman brokerler da işletmelere destek olmakta, soru formlarına dayalı risk inceleme ve değerlendirmesi neticesinde, siber sigorta teklifi sunulabilmekte, işletmenin bazı eksiklerini gidermesi istenip yeniden değerlendirilebilmekte ya da teklif sunulması uygun görülmeyebilmektedir. Yapılan görüşmelerden, siber sigortaya ilişkin doğrudan teminat sağlayan şirketlerin yazım sürecini de kendisinin yürüttüğü, küresel ölçekte faaliyet gösteren büyük reasürörlerden teminat temin edilerek teklif sunulması durumunda, reasürör ile birlikte fiyatlama sürecinin söz konusu olduğu anlaşılmaktadır. Ş6, yazım sürecini kendilerinin yürüttüğünü, bu süreçte sadeleştirilmiş soru formları kullandıklarını, siber sigorta talep eden işletmenin BT yetkililerine formların doldurulması sürecinde hem kendi ekiplerinin hem de sürece aracılık eden sigorta brokerlerinin destek verebildiğini, formlara verilen yanıtlar doğrultusunda detaylı raporlar hazırladıklarını, müşteriye özel hazırlanan veriler doğrultusunda teminat limitlerini, şartları, muafiyetleri ve primi birlikte değerlendirerek kapsamlı bir rapor şeklinde teklif hazırladıklarını belirtmektedir. Görüşme gerçekleştirilen diğer katılımcılar, büyük ölçekli kurumsal siber sigorta poliçelerinin yurtdışına (yurtdışı reasürörlere) bağlı olduğunu, bu poliçelerin %100 reasüransla sunulabildiğini (%0 konservasyon), dolayısıyla bunun bir reasürans ürünü olduğunu ve risk kabul kararının reasüröre bağlı olduğunu ifade etmektedir.

Büyük bir işletmeden siber teminat talebi geldiğinde, sigorta şirketinin talebin yönetilmesi sürecinde aktif rol aldığı, reasürörün soru formlarının brokerler aracılığıyla sigorta talep eden işletmeye doldurtulması, doldurulan formların reasüröre ulaştırılması, reasürörün teklifinin (teklif vermesi durumunda) sigorta talep eden işletmeye sunulması gibi süreçleri yönettiği, bir nevi aracı gibi faaliyet gösterdiğinden bahsedilmektedir. Ancak düzenlenmesi durumunda kurumsal siber sigorta poliçesi, süreci yöneten sigorta şirketinin poliçesi olmaktadır. Ürün yurtdışına bağlı bir ürün olması sebebiyle, kurumsal siber sigorta primleri, küresel siber sigorta piyasasındaki gelişmelere (artan siber saldırılara, yaşanan hasarlara, siber sigorta talebine ve arzına) bağlı olarak değişiklik göstermektedir.

Ş2, bireysel siber sigorta poliçelerinde de reasürans desteği ile ürünü sunduklarını belirtmektedir. Ş5 ise, hâlihazırda sunmakta oldukları bireysel siber sigorta ürününü, %100 konservasyon oranıyla sunduklarını, KOBİ'lere yönelik sunacakları siber sigorta ürününü ise ilk yıl çok küçük bir konservasyon oranıyla sunmayı planladıklarını, kârlılık durumuna göre sonraki yıllarda konservasyon oranını artırabileceklerini ifade etmektedir.

- *Sektör tercihi*: Gerçekleştirilen görüşmeler doğrultusunda siber sigorta teminatı sağlama konusunda temkinli yaklaşılan sektörler olduğu anlaşılmaktadır. KOBİ'lere yönelik olan daha küçük ölçekli siber sigorta ürünlerinde, fiyatlar standart olduğundan ve bazı sektörlerde faaliyet gösteren işletmelerin maruz kaldığı siber risklerin paket poliçe kapsamında sigortalanabilmesi mümkün olmadığından, hâlihazırda bu ürünleri sunmakta olan veya sunmak üzere hazırlıklar yapan şirketler (Ş1, Ş2, Ş4 ve Ş5), bu işletmelere paket poliçe kapsamında teminat sağlanamadığını/sağlanamayacağını belirtmektedir. Siber risklere maruziyetin çok yüksek olarak değerlendirildiği sektörler arasında finans, sağlık, e-ticaret, BT, denizcilik, havacılık gibi sektörler yer almaktadır. Bununla birlikte gerek bu sektörlerde faaliyet gösteren işletmelerden gelen, gerekse büyük ölçekli işletmelerden gelen siber sigorta taleplerinin (reasürörler ile birlikte) kendi özelinde değerlendirildiği ve münferit siber sigorta poliçeleri ile teminat altına alınabildiği ifade edilmektedir. Ayrıca Ş5, finansal kuruluşlardan, çağrı merkezlerinden, sağlık hizmeti sunan kuruluşlardan gelen siber sigorta talepleri için reasürörlerden

teminat bulmanın zor olabildiğini, e-ticaret firmaları için ayrı özel kabul şartları olabildiğini ifade etmektedir. Bu sektörlere ek olarak Ş3, ödeme sistemlerine aracılık yapan yazılım firmalarının ve enerji şirketlerinin siber sigorta teminatı sağlama konusunda tercih edilmeyen grupta yer aldığını belirtmektedir. Ş6 ise, her ne kadar siber sigorta teminatı sağlama konusunda temkinli yaklaşılsa da finansal kuruluşların, özellikle de bankaların aslında güvenlik sistemlerine en fazla yatırım yapan grupta yer aldığını, asıl temkinli yaklaşılması gerekenin, siber risklere maruziyeti yüksek olmasına rağmen BT sistemlerine gerekli yatırımları yapmayan işletmeler olduğunu ifade etmektedir. Bununla birlikte, ödeme sistemleri, bulut teknolojileri, sağlık, hava yolu ve enerji sektörlerinden gelen siber sigorta taleplerine teminat sağlamaya istekli olmadıklarını, ancak gelen her talebi değerlendirmeye aldıklarını belirtmektedir.

- *Sigortalıda aranan şartlar*: Tüm katılımcılar, fiyatlama sürecinde kullanılan soru formlarında siber sigorta talep eden işletmenin BT sistemleri ile ilgili kapsamlı sorular yer aldığını ve işletmelerin BT sistemlerinin belirli uluslararası güvenlik sertifikalarına (bilgi güvenliği yönetim sistemleri ve gereksinimleri için dünyanın en iyi bilinen standartlarından biri olan ISO/IEC 27001 gibi) sahip olması gerektiğini ifade etmektedir. Reasürörlerin de teminat sağlama hususunda BT sistemlerine ilişkin güvenlik sertifikalarını talep ettiği, siber sigorta talep eden işletmenin BT güvenlik sistemlerinin yetersiz olması durumunda, siber sigorta talebine ilişkin bir teklif çalışılmadığı belirtilmektedir. Ayrıca Ş6, siber sigorta talep eden işletmenin BT sistemlerinin güvenliğine ve müşteri bazında oluşabilen diğer şartlara ilişkin eksiklikler olması durumunda, belirli bir süre içinde eksikliklerin giderilmesini önerdiklerini ve süre sonunda süreci yeniden değerlendirdiklerini ifade etmektedir.
- *Sigorta kapsamı:* Kurumsal siber sigorta kapsamında sunulan teminatların temel olarak birinci şahıs (sigortalı şirket) siber sigorta teminatları ve üçüncü şahıs (sorumluluk) siber sigorta teminatları olmak üzere iki gruba ayrıldığı görülmektedir. Birinci şahıs siber sigorta teminatları, bir siber saldırı nedeniyle sigortalı işletmenin uğrayacağı zararlara, üçüncü şahıs siber sigorta teminatları ise, sigortalı işletmenin siber saldırıya maruz kalması durumunda üçüncü kişilerin göreceği zararlara yöneliktir. Birinci şahıs siber sigorta teminatları arasında genellikle siber olaya müdahale (veri koruma mevzuatına uyum ve yasal bildirim masrafları, yasal savunma masrafları ve idari para cezaları, kredi izleme veya kimlik hırsızlığı hizmetlerine ilişkin masraflar, işletme itibarının korunmasına yönelik halkla ilişkiler masrafları vb.), veri ve yazılım kurtarma (siber saldırı nedeniyle kaybedilen ya da zarar gören veri ve yazılımların tekrar yerine getirilmesi ile ilgili masraflar), siber şantaj (fidye talepli siber saldırılar nedeniyle ortaya çıkan ve işletmenin sistemlerinin zarar görmemesi için ödenen siber şantaj giderleri) ve siber iş durması (siber saldırılar sonucu maruz kalınan iş durması ve kâr kaybı) teminatları yer almaktadır. Sorumluluk siber sigorta teminatları arasında ise genellikle bilgi gizliliği ve ağ güvenliği sorumluluğu (siber saldırı nedeniyle üçüncü kişilere ait gizli ya da kişisel verilerin ihlal edilmesi veya üçüncü kişilerin bilgisayar sistemlerinin etkilenmesi sonucunda üçüncü kişilerden gelebilecek tazminat talepleri) ile medya sorumluluğu (sigortalı işletmenin internet sitesi veya sosyal medya hesaplarındaki içerikler sebebiyle karşılaşabileceği tazminat talepleri) teminatları yer almaktadır.

Bireysel siber sigorta kapsamında sunulan başlıca teminatlar arasında ise kimlik hırsızlığı, şifre çalınması, çevrim içi saygınlığa zarar verilmesi, kimlik yenileme, ödeme araçlarının hileli kullanımı ve elektronik alışverişte yaşanan anlaşmazlıklar yer almaktadır. Ayrıca şirketlerin bireysel siber sigorta paket poliçelerine ATM hırsızlığı koruması gibi teminatlar ekleyebildiği ve/veya isteğe bağlı teminatlar verilebildiği görülmektedir.

- *Siber olay şüphesi olduğunda müdahale süreci:* Kurumsal siber sigortalara ilişkin hasar yönetimi süreçlerinde hukuki destek, adli bilişim, halkla ilişkiler, çağrı merkezi, kriz iletişimi gibi konularda deneyimli hizmet sağlayıcıları ile işbirliği yapıldığı ifade edilmektedir. Sigortalı işletmenin bir siber olay yaşandığını fark ettiği anda siber sigorta poliçesi üzerinde bulunan hasar hattına bildirimde bulunması gerekmekte olup, hasarın hangi aşamada olduğu, nasıl bir yol izleneceğini ve hangi iş ortağı/ortakları ile çalışılacağını belirlemektedir. Bu süreçte, sigortalı işletmenin sistemine uzaktan bağlanılabildiği gibi, daha büyük kriz anında yerinde müdahale de yapılabilmektedir.

Ş1, sigortalı işletmenin sistemlerine uzaktan bağlanılarak ve/veya yerinde müdahale edilerek zararı azaltıcı hatta önleyici bir hizmet sunulduğunu belirtmektedir. Ş6, anlık olarak sürece müdahale edebilen siber olaylara müdahale ekipleriyle (vendorlar) çalıştıklarını, önceden programlanan ve saatlik takip edilen süreçler söz konusu olduğunu, sigortalı işletmenin bir siber olay şüphesi olduğunda poliçe

üzerinde bulunan hasar hattı yanı sıra mobil aplikasyon ile de bildirimde bulunabileceğini, bir dakikalık bir süre içinde ilgili uzmanın sigortalı işletme ile iletişime geçtiğini, işletmeye sorduğu sorular ile risk seviyesini belirlediğini, poliçe numarası ile sigortalı işletmenin sistemine uzaktan bağlanılabildiğini ifade etmektedir. Ş6 ayrıca, hasar yönetimi sürecinde hizmet aldıkları ekiplerin, 12-24 saat içinde riskin ne kadar büyük olduğunu ölçümlemek, 48 saat içinde riske ilişkin raporu hazırlamak gibi yükümlülükleri olduğunu da belirtmektedir. Ş2, sigortalı işletmeden bir siber olay şüphesi olduğuna dair bildirim aldıkları anda bu durumu poliçenin teminatını sağlayan reasüröre de hemen bildirdiklerini, hasar yönetimi sürecinin reasürörün yönlendirmesi ile ilerlediğini, hatta hasarın çok büyük boyutlu olduğunun öngörülmesi durumunda reasürörün kendi hasar uzmanlarını da yönlendirebildiğini ifade etmektedir. Ş5 ise, reasürörlerin poliçeye hasar yönetimi süreçlerinde hizmet alınacak sağlayıcılara ilişkin özel şartlar (yurt dışı uzman ekip şartı, Türkiye'de belirli bir uzman ekip şartı gibi) koydurabildiğini belirtmektedir. Ş2 ayrıca KOBİ'lere yönelik kurumsal siber sigorta paket poliçe hazırlıklarının tamamlanmasının ardından siber sigorta hasar yönetimi süreçlerinde uzman firmalar ile vendor anlaşmaları yapılmasını planlamaktadır. Benzer bir şekilde, Ş3 de mevcut durumda küresel ölçekte hizmet aldıkları ekiplerin olduğunu ancak Türkiye'de henüz bu tür anlaşmaları bulunmadığını, ürünün gelişmesi ve yaygınlaşması durumunda anlaşmalar yapılabileceğini belirtmektedir.

Katılımcılar, Türkiye'de de siber olaylara müdahale sürecinde destek verebilecek firmaların bulunduğunu ifade etmekte ve siber sigorta piyasası geliştikçe bu tür firmaların nicelik ve niteliğinin de artış göstermesini beklemektedir. Ş6, Türkiye'de sigortalı işletmelere yerel hizmet sağlayabilmek adına son dönemde yerli hizmet sağlayıcıları ile de vendor anlaşmaları yaptıklarını ve siber olaylara müdahale ekipleri arasında yerli firmalar da bulunduğunu belirtmektedir.

4.2. Covid-19 Salgınının Türkiye'de Siber Sigorta Piyasası Üzerindeki Etkileri

İkinci araştırma sorusu Covid-19 salgınının siber sigorta piyasası üzerindeki etkilerini ortaya koymayı amaçlamakta olup, Ş1, özellikle işletmelerde uzaktan çalışmanın artmasına bağlı olarak, siber risklerin ve siber sigortaya olan talebin arttığını, ancak hasarlarda henüz alarm verici bir artış gerçekleşmediğini belirtmektedir. Bununla birlikte, özellikle küresel ölçekte siber risklerle ilgili hasarların büyüyeceğine, sigorta sektörünün gerekli kapasiteyi sağlayamayacağına dair ciddi endişelerin olduğunu ancak, Türkiye'de siber sigorta piyasasında henüz bu endişelerin tam olarak hissedilmediğini ifade etmektedir. Ş2'de benzer bir şekilde online işlemlerin ve uzaktan çalışmanın büyük artış gösterdiğine ve artık işletmelerin sadece işletmenin BT altyapısını değil personelinin de kişisel BT altyapısını koruması gerektiğine dikkat çekmektedir. Salgın ve sonrasındaki sürecin hem siber saldırıları, hem de korunma ihtiyacını artırdığını ifade etmektedir.

Ş3, salgın sürecinin ve salgına bağlı yaşanan gelişmelerin Türkiye'de siber sigorta talebini henüz etkilemediğini, siber sigortanın Türkiye'nin gündeminde yeterince yer almadığını ifade etmektedir. Benzer bir şekilde Ş4 de salgının siber sigorta talebinde kalıcı bir artış yaratmadığını, Ş5 ise salgın döneminin küresel ölçekte siber sigortalara talebi artırmış olabileceğini, ancak Türkiye'de talebe henüz bir olumlu etkisi olmadığını, hasar üzerinde de bir olumsuz etkisini görmediklerini ifade etmektedir.

4.3. Türkiye'de Siber Sigorta Piyasasının Önündeki Fırsatlar ve/veya Engeller

Temel araştırma sorularından üçüncüsü ise Türkiye'de siber sigorta piyasasının önündeki fırsatları ve/veya engelleri ortaya koymayı amaçlamaktadır. Ş1, hem dünyada hem de Türkiye'de siber sigorta piyasasında büyük bir potansiyel olduğunu öngörmektedir. Ancak olumsuz öngörülen risk artışı sebebiyle reasürörlerin teminat kapasitesini daraltma eğiliminde olduğunu, bunun da primlerde ciddi artışlara neden olduğunu ifade etmektedir. Ayrıca özellikle hasara müdahale sürecinde iş ortaklarının çok önemli olduğunu, Türkiye'de bu firmaların da henüz gelişme aşamasında olduğunu, büyük boyutlu hasarlar yaşanmadığından verdikleri hizmetin kalitesinin yeterince sınanmadığını, hasarların sigorta sektörü ve iş ortakları için önemli tecrübeler sağladığını ifade etmektedir.

Ş2, küresel ölçekte siber risklerin her geçen gün çeşitlendiğini ve artış gösterdiğini, hem artan riskler nedeniyle hem de bilgi güvenliği ile ilgili standartların ve düzenlemelerin çeşitli ülkelerde yürürlüğe girmesi nedeniyle siber sigortaya olan talebin çok hızlı artış gösterdiğini, ancak reasürans kapasitesinin bu talebi karşılayacak düzeyde aynı hızda artmamasının fiyatlarda sürekli artışa neden olduğunu ifade etmektedir. Türkiye'de siber sigortaya ilişkin gerek talebin gerekse arzın henüz istenen seviyede

olmadığını, Türkiye'de siber sigorta piyasasının önündeki en önemli engellerden birinin işletmelerin bilinç eksikliği olduğunu, ancak siber risklere ilişkin farkındalık arttıkça bunun sektör için bir fırsata da dönüşeceğini belirtmektedir. Türkiye'de de veri güvenliği konusunda önemli mevzuat düzenlemeleri yapıldığı, işletmelerin farkındalığı ve BT olgunluk seviyesi arttıkça arz tarafında da olumlu gelişmeler yaşanacağı beklenmektedir. Türkiye'de siber sigortaların gelişmesinin küresel reasürans piyasası için de aslında olumlu bir gelişme olacağı öngörülmektedir.

Ş2 ayrıca özellikle orta ve büyük işletmelere yönelik olan siber sigortanın bir reasürans ürünü olduğunu, sigorta şirketlerinin riski kendi üzerinde tutmasının, kendi kapasitelerini kullanmasının mümkün olmadığını, soru formları üzerinden fiyatlandırma sürecinin reasürörler tarafından yürütüldüğünü ve teminat verilmesine ilişkin kararın reasürör tarafından verildiğini ifade etmektedir. Reasürör kapasitesinin kısıtlı olması durumunda bunun bir engel gibi görülebileceğini, ancak sigorta şirketlerinin yazım sürecini yönetecek siber sigorta konusunda uzman personelinin yetersizliği göz önüne alındığında, küresel ölçekte faaliyet gösteren büyük reasürörlerden teminat temin etme sürecinde, siber sigortalara ilişkin bilgi ve birikimlerinden de faydalanıldığını ve tecrübe aktarımı gerçekleştirildiğini belirtmektedir.

Ş3, Türkiye'de siber sigorta talep eden şirketlerle yapılan görüşmelerde, şirketlerin BT sistemlerine yatırım yapmaları gerektiği, BT sistemlerinin belirli güvenlik sertifikalarına sahip olması gerektiği ifade edildiğinde, şirketlerin bu yatırımları yapmaları durumunda siber sigortaya ihtiyaçlarının kalmayacağı şeklinde bir yaklaşım içinde olduklarını ve taleplerin poliçelere dönüşemediğini ifade etmektedir.

Ş4 yurtdışı reasürörler teminat sağladığından, kurumsal siber sigortada talep edilen soru formlarını şirketlerin doldurmakta ve gerekli bilgileri sağlamakta zorlandığını, çok katı bir belgeleme söz konusu olduğunu belirtmektedir. Ürünü talep eden şirketlerin büyük bir bölümünün gerekli belgelemeyi sağlayamadığına, formları doldurup gerekli belgeleri sağlayan şirketlerin de önemli bir kısmının siber sigorta teklifi alamadığına dikkat çekmektedir. Burada yurtdışı reasürörlerin, AB normlarına göre belgeleme talep ettiğini ancak Türkiye'de henüz AB normlarına uygun bir veri güvenliğine erişilemediğini, bu nedenle şirketlerin gerekli belgelemeyi sağlamakta zorlandığını ve bu durumun kurumsal siber sigortaların önündeki en büyük engel olduğunu ifade etmektedir. Veri güvenliğine ilişkin yeni yasal düzenlemelerin bu engelin aşılmasına katkı sağlaması beklenmektedir. Ayrıca kurumsal siber sigorta için yurtiçinden reasürans teminatı temin edilebildiğinde, kurumsal siber sigorta primlerinin düşeceği ancak bunun beş yıl gibi bir vadede gerçekleşebileceği öngörülmektedir.

Ş5 gerek küresel ölçekte, gerekse Türkiye'de son yıllarda siber risklerin gündemde önemli bir yer tuttuğunu ifade etmekte ve gelecek yıllarda daha da fazla gündeme geleceğini öngörmektedir. Mevcut ekonomik koşullarda reasürörlerden teminat bulmanın kolay olmadığını, ancak daha istikrarlı bir ekonomik ortamda siber sigortanın sektörde daha fazla yer edinmesini beklediklerini ifade etmektedir.

Ş6 ise siber sigortaya ilişkin teknik bilginin çok zayıf olduğunu, sigorta talep eden işletmenin istekleri ile sigorta sağlayıcısının sundukları arasında orta noktayı yakalamanın kolay olmadığını, ancak siber sigortaya ilişkin bilinirliğin ve müşterilerin bilincinin her geçen gün arttığını, bu artışın da zorlukların aşılmasına katkı sağladığını ifade etmektedir. Siber sigorta genel şartları ile ilgili Türkiye'de çalışmalar yapıldığını belirtmekte ve genel şartların çıkmasıyla birlikte siber risklerin daha ölçülebilir hala geleceğini öngörmektedir.

5. Sonuç ve Değerlendirme

Siber güvenliğe yönelik tehditlerin arttığı günümüzde, siber sigortaya ilişkin farkındalığın her geçen gün artması ve siber sigorta piyasasının gelişmeye devam etmesi beklenmektedir. Türkiye'de siber sigortaya ilişkin piyasa uygulamalarının araştırılmasının ve siber sigorta piyasasının incelenmesinin amaçlandığı bu çalışmada üç temel araştırma sorusu ele alınmıştır. Araştırma sorularından birincisi Türkiye'de siber sigorta piyasasının mevcut durumunu, ikincisi Covid-19 salgınının siber sigorta piyasası üzerindeki etkilerini ve üçüncüsü ise siber sigorta piyasasının önündeki fırsatları ve/veya engelleri ortaya koymayı amaçlamaktadır. Nitel araştırma yönteminin kullanıldığı bu çalışmada, Franke (2017) tarafından yapılan çalışma takip edilerek, veri toplama aracı olarak yarı-yapılandırılmış görüşme formlarından yararlanılmıştır. Araştırma kapsamında altı hayat dışı sigorta şirketinin siber sigorta konusunda uzman yöneticileriyle yarı-yapılandırılmış görüşmeler gerçekleştirilmiştir.

Sigortacılık Hesap Planı'nda henüz siber sigorta için açılmış bir hesabın bulunmaması ve buna bağlı olarak TSB tarafından yayımlanan istatistiki veri olmaması sebebiyle, Türkiye'de siber sigorta piyasasının büyüklüğü ve şirketlerin pazar payı tam olarak bilinmemekte, gerçekleştirilen görüşmelerde tahmin etmenin de zor olduğu belirtilmektedir. Yapılan görüşmeler neticesinde, Türkiye'de siber sigorta piyasasında hem bireysel hem de kurumsal siber sigorta ürünlerinin sunulduğunu, kurumsal siber sigorta ürünlerinin küçük ve orta büyüklükteki işletmelere yönelik paket poliçe olarak sunulan kurumsal siber sigorta ve büyük ve orta boy işletmelere "müşteriye özel" olarak sunulan kurumsal siber sigorta olmak üzere iki başlıkta incelenebileceğini ifade etmek mümkündür. Kurumsal siber sigorta kapsamında sunulan teminatlar arasında hem birinci şahıs siber sigorta teminatları hem de üçüncü şahıs siber sigorta teminatları yer almaktadır. Mevcut durumda kurumsal siber sigorta genellikle ayrı bir ürün olarak sunulmakta ve fiyatlandırma sürecinde soru formlarından yararlanılmaktadır. Soru formları ile temin edilen bilgilere dayalı bir fiyatlandırma olması sebebiyle, siber sigortanın doğru fiyatlandırılmasının zor olduğunu ifade etmek mümkündür. Fiyatlama sürecinde kullanılan soru formlarında siber sigorta talep eden işletmenin BT sistemleri ile ilgili kapsamlı sorular yer aldığı ve BT güvenlik sistemlerinin yetersiz olması durumunda siber sigorta talebine ilişkin bir teklif çalışılmadığı belirtilmektedir. Buna bağlı olarak, siber sigorta talep eden işletmede aranan bu şartların işletmeleri BT güvenlik sistemlerine yatırım yapmaya yönlendireceği, dolayısıyla siber sigortanın riskin transfer edilmesi yanı sıra kaybın meydana gelme olasılığının ve/veya şiddetinin azaltılmasına da katkı sağlayabileceği ifade edilebilir.

Türkiye'de siber sigorta piyasasında sunulan kurumsal siber sigorta ürünlerinin hem birinci şahıs hem de üçüncü şahıs siber sigorta teminatlarını kapsaması, büyük işletmelere özel karmaşık sigortalama sürecinin olduğu kurumsal siber sigorta ürünleri yanı sıra daha küçük işletmeleri hedefleyen her iş bazında yeniden yazım sürecine gerek kalmadan sunulabilen daha basit poliçelerin varlığı, geçmiş verilerin eksikliği sebebiyle fiyatlandırma sürecinin zorluğu ve siber sigortanın bir risk transfer aracı olması yanı sıra riskten kaçınma ve riski azaltmaya da katkı sağlaması bakımından Türkiye'de siber sigorta piyasası için elde edilen bulguların, Franke (2017) tarafından yapılan çalışmada elde edilen bulgularla benzer olduğunu ifade etmek mümkündür.

Covid-19 salgını ve sonrasındaki sürecin hem siber saldırıları, hem de korunma ihtiyacını artırdığı konusunda bir fikir birliği bulunmaktadır. Ancak görüşmeler neticesinde elde edilen bulgular, salgın sürecinin ve salgına bağlı yaşanan gelişmelerin Türkiye'de siber sigorta talebini henüz önemli ölçüde etkilemediğini, hasarlar üzerinde de bir olumsuz etkisinin mevcut durumda hissedilmediğini göstermektedir.

Türkiye'de siber sigorta piyasasının önündeki engellerin başında siber sigortaya ilişkin bilinç eksikliği gelmektedir. BT güvenliğine yapılacak yatırımlar işletmeler için yüksek maliyetler doğurabildiğinden, işletmeler bu yatırımları yapmaları durumunda siber sigortaya ihtiyaçlarının kalmayacağı şeklinde bir yaklaşım içinde olmaktadır. Bunun yanı sıra siber sigorta için gerekli olan bilgileri sigorta şirketi ve/veya sigorta aracısı ile paylaşmanın da bir risk olarak görülebildiği belirtilmektedir. Bu durum var olan talebin poliçeye dönüşme oranının düşük kalmasına neden olmaktadır. Siber sigortaya ilişkin bilincin oluşması için somut örneklere, yaşanmışlıklara ihtiyaç olduğu, düzenleyici otoritelerin bu farkındalığı artırmaya yönelik adımlar atması gerektiği ifade edilmektedir. Ayrıca sigorta sektörünün siber sigorta çözümlerini piyasaya daha iyi anlatmasına da ihtiyaç bulunmaktadır.

Geçmiş verilerin eksikliği, hasar oranlarının öngörülemezliği, fiyatlamada yaşanan zorluklar, yetersiz reasürans kapasitesi ve suistimale çok açık oluşu (ahlaki tehlike), Türkiye'de siber sigorta piyasasının gelişmesinin önündeki diğer önemli zorluklar olarak dikkat çekmektedir. Ayrıca Türkiye'de henüz siber sigorta genel şartlarının bulunmaması da, piyasanın önündeki engellerden biri olarak değerlendirilmektedir. Ancak yapılan görüşmelerde siber sigorta genel şartları ile ilgili olarak Türkiye'de çalışmaların devam ettiği belirtilmekte ve genel şartların çıkmasıyla birlikte siber risklerin daha ölçülebilir hale geleceği öngörülmektedir. Siber sigortaya ilişkin bilinç eksikliği ve bahsi geçen diğer engeller sebebiyle ortaya çıkan düşük sigortalılık oranlarının, bu engelleri aşmaya yönelik adımlar atıldıkça bir fırsata dönüşeceği belirtilmektedir. Dolayısıyla siber sigorta alanında genel şartlar bağlamında bir mevzuat oluşturulmasının ve bir an önce yürürlüğe konulmasının gerekli olduğu düşünülmektedir.

Çalışmada Türkiye'de siber sigorta piyasasının arz tarafını oluşturan aktörlerden yalnızca hayat dışı sigorta şirketleri ile görüşmeler gerçekleştirilmiştir. Sigorta aracıları (sigorta acentesi ve brokeri) ile reasürörlerin de katılımcılar arasında yer alacağı bir çalışma ile Türkiye siber sigorta piyasasına ilişkin daha kapsamlı değerlendirmeler yapılabilmesi mümkündür. Ayrıca bu çalışmada mevcut ve/veya potansiyel siber sigorta müşterilerinden veri temin etmeye yönelik bir talep tarafı araştırması yapılmamıştır. Talep tarafına yönelik bir araştırma yapılmasının da, Türkiye'de siber sigorta piyasasının olgunlaşma sürecine katkı sağlayacağı düşünülmektedir.

Sigortacılık Hesap Planı'nda siber sigorta için bir hesabın oluşturulması ve böylelikle Türkiye'de siber sigorta sunan şirketler, siber sigortaya ilişkin yazılan primler, hasarlar gibi istatistiki bilgilerin temin edilebilmesi durumunda, sigorta şirketlerinin siber teminat yazma kararını, siber sigorta piyasasına hangi kapsamda katıldığını ve siber sigorta piyasasındaki performansını etkileyen faktörleri ampirik olarak araştırma imkanı söz konusu olabilecektir.

Etik Kurul İzni: Ankara Hacı Bayram Veli Üniversitesi Etik Komisyonu'nun 14.12.2022 tarih ve 13 sayılı toplantısında etik kurul izni alınmıştır.

Kaynakça

Altuntaş, E., Kara, E., Soylu, A.B. ve Kırkbeşoğlu, E. (2018). Siber Sigortalar: Son Gelişmeler, Uygulamalar ve Sorunlar, *Bankacılık ve Sigortacılık Araştırmaları Dergisi*, (12), 8-22. https://dergipark.org.tr/tr/download/article-file/610968

Baer, W.S. ve Parkinson, A. (2007). Cyber-insurance in IT security management. *IEEE Security and Privacy, 5(3),* 50-56. https://doi.ieeecomputersociety.org/10.1109/MSP.2007.57

Biener, C., Eling, M. ve Wirfs, J.H. (2015). Insurability of Cyber Risk: An Empirical Analysis. *The Geneva Papers on Risk and Insurance - Issues and Practice, 40*, 131-158. https://doi.org/10.1057/gpp.2014.19

Böhme, R. ve Schwartz, G. (2010). "Modeling Cyber-Insurance: Towards A Unifying Framework". *Workshop on the Economics of Information Security (WEIS).* Erişim adresi: https://www1.icsi.berkeley.edu/pubs/networking/modelingcyber10.pdf

Bouveret, A. (2018). "Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment". *International Monetary Fund Working Paper, WP/18/143*. Erişim adresi: https://www.imf.org/en/Publications/WP/Issues/2018/06/22/Cyber-Risk-for-the-Financial-Sector-A-Framework-for-Quantitative-Assessment-45924

Cebeci, İ. (2021). Türkiye'de Siber Risk Sigortalarına İlişkin Bir Değerlendirme. *Üçüncü Sektör Sosyal Ekonomi Dergisi, 56*(1), 163-188. http://dx.doi.org/10.15659/3.sektor-sosyal-ekonomi.21.02.1520

Cole, C.R. ve Fier, S.G. (2021). An Empirical Analysis of Insurer Participation in the U.S. Cyber Insurance Market, *North American Actuarial Journal, 25(2),* 232-254. https://doi.org/10.1080/10920277.2020.1733615

Eling, M. ve Schnell, W. (2016). What do we know about cyber risk and cyber risk ınsurance? *Journal of Risk Finance, 17*(5), 474-491. https://doi.org/10.1108/JRF-09-2016-0122

Eling, M. ve Wirfs, J.H. (2016). "Cyber risk: too big to insure? Risk transfer options for a mercurial risk class". Erişim adresi: https://www.ivw.unisg.ch/_/media/internet/content/dateien/instituteundcenters/ivw/studien/cyberrisk2016.pdf

Eling, M. ve Wirfs, J. (2019). What Are The Actual Costs of Cyber Risk Events? *European Journal of Operational Research, 272*(3), 1109-1119. https://doi.org/10.1016/j.ejor.2018.07.021

Eling, M., Elvedi. M. ve Falco, G. (2022). The Economic Impact of Extreme Cyber Risk Scenarios, *North American Actuarial Journal,* https://doi.org/10.1080/10920277.2022.2034507

Franke, U. (2017). The cyber insurance market in Sweden. *Computers & Security, 68*, 130-144. https://doi.org/10.1016/j.cose.2017.04.010

Gürbüz, S. ve Şahin, F. (2018). *Sosyal Bilimlerde Araştırma Yöntemleri Felsefe-Yöntem-Analiz*, Ankara: Seçkin Yayıncılık.

Herath, H.S.B. ve Herath, T.C. (2011). Copula Based Actuarial Model for Pricing Cyber-Insurance Policies, *Insurance Markets and Companies: Analyses and Actuarial Computations, 2(1),* 7-20. Erişim adresi: https://www.businessperspectives.org/images/pdf/applications/publishing/templates/article/assets/3934/IMC_2011_1_Herath.pdf

Korucu O. (2021). Yeni Normal Dünya Düzeninin Siber Güvenlik ve Bilgi Güvenliğine Etkileri, *Yönetim Bilişim Sistemleri Dergisi, 7(1),* 44-60. https://dergipark.org.tr/tr/pub/ybs/issue/63606/908082

Kuru, D. ve Bayraktar, S. (2017). The effect of cyber-risk insurance to social welfare, *Journal of Financial Crime, 24(2),* 329-346. http://dx.doi.org/10.1108/JFC-05-2016-0035

Kişisel Verileri Koruma Kurumu (KVKK). (2023). *Veri İhlali Bildirimleri*. 02.01.2023 tarihinde https://www.kvkk.gov.tr/veri-ihlali-bildirimi/ adresinden alındı.

Lloyd, G. (2020). The business benefits of cyber security for SMEs, *Computer Fraud & Security, 2020(2),* 14-17. https://doi.org/10.1016/S1361-3723(20)30019-1

Low, P. (2017). Insuring against cyber-attacks, *Computer Fraud & Security, 2017(4),* 18-20. https://doi.org/10.1016/S1361-3723(17)30034-9

Maillart, T. ve Sornette D. (2010). Heavy-tailed distribution of cyber-risks, *The European Physical Journal B, 75,* 357-364. https://doi.org/10.1140/epjb/e2010-00120-8

Majuca, R.P., Yurcik, W. ve Kesan J.P. (2006). The Evolution of Cyberinsurance. Erişim adresi: https://arxiv.org/ftp/cs/papers/0601/0601020.pdf

Malavasi, M., Peters, G.W., Shevchenko, P.V., Trück, S., Jang, J. ve Sofronov, G. (2022). Cyber Risk Frequency, Severity and Insurance Viability. *Insurance: Mathematics and Economics, 106*, 90-114. https://doi.org/10.1016/j.insmatheco.2022.05.003

Marotta, A., Martinelli, F., Nanni, S., Orlando, A. ve Yautsiukhin, A. (2017). Cyber-insurance survey, Computer Science Review, *24*, 35-61. https://doi.org/10.1016/j.cosrev.2017.01.001

Munich Re. (2022). Munich Re Global Cyber Risk and Insurance Survey 2022. https://www.munichre.com/landingpage/en/global-cyber-risk-and-insurance-survey-2022.html

Schneier, B. (2001). Insurance and the Computer Industry, *Communications of the ACM, 44(3),* 114-115. https://doi.org/10.1145/365181.365229

World Economic Forum (WEF). (2022a). *The Global Risks Report 2022, 17th Edition.* In partnership with Marsh McLennan, SK Group and Zurich Insurance Group. 03.11. 2022 tarihinde https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf adresinden alındı.

World Economic Forum (WEF). (2022b). *Global Cybersecurity Outlook 2022: Insight Report.* In collaboration with Accenture. 03.11.2022 tarihinde https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf adresinden alındı.

Xie, X., Lee, C. ve Eling, M. (2020). Cyber insurance offering and performance: an analysis of the U.S. cyber insurance market. *The Geneva Papers on Risk and Insurance - Issues and Practice, 45*, 690-736. https://doi.org/10.1057/s41288-020-00176-5

Research Article

Türk Sigorta Sektöründe Siber Sigortalara İlişkin Değerlendirme: Sektörel Bir Araştırma

Assessment of Cyber Insurance in the Türk Insurance Sector: A Sectoral Research

Nuriye VAROL GÖNEN	Emine ÖNER KAYA
Arş. Gör., Ankara Hacı Bayram Veli Üniversitesi	Doç. Dr., Ankara Hacı Bayram Veli Üniversitesi
Bankacılık ve Sigortacılık Yüksekokulu	Bankacılık ve Sigortacılık Yüksekokulu
nuriye.varol@hbv.edu.tr	emine.oner@hbv.edu.tr
https://orcid.org/0000-0001-9159-5983	https://orcid.org/0000-0002-4247-0866

Extensive Summary

The digitalization of economic and social life is a source not only of development opportunities and innovations, but also of entirely new risks. Due to the increasing digitalization all over the world, cyber risk is also inevitably growing (WEF, 2022b: 29). The management of cyber risk is a very difficult process due to its characteristics such as risk of change, high uncertainty regarding data and modeling approaches, and extreme scenarios that are difficult to predict. For individuals and especially businesses, managing cyber risk by avoiding risk, in other words by not using IT products and services, will not be reasonable in most cases. Therefore, it is necessary to take steps to prevent and/or reduce losses by using managerial and technical processes in the management of this risk. In cases where the tools used to mitigate the risk (such as software updates, antivirus programs, continuous backup of data, internet traffic management) are not sufficient, there is the opportunity to transfer the risk with cyber insurance (Eling and Schnell, 2016: 480). Individuals and businesses generally prefer to use these options together in the management of cyber risk. In other words, individuals and especially businesses accept some of the cyber risk, reduce some of it with various technologies and methods, and insure the rest (Schneier, 2001: 115). The importance of cyber insurance is increasing day by day in the process of managing cyber risks. Munich Re Global Cyber Risk and Insurance Survey 2022 states that the need for cyber security and insurance is increasing steadily and expects that global cyber premiums will reach approximately $22 billion by 2025.

Despite the growing awareness of cyber risk and cyber insurance, research on both cyber risk and cyber insurance is limited. One of the reasons why research on cyber risk and cyber insurance is limited is that it is difficult to obtain reliable data (Eling and Wirfs, 2019: 1109). Numerous studies highlight the lack of data and modeling challenges (Eling and Schnell, 2016: 474, 478; Maillart and Sornette, 2010: 363; Biener, Eling and Wirfs, 2015: 149; Bouveret, 2018: 3). This is also the reason why there are few quantitative analyses of cyber risk (Bouveret, 2018: 3). The existing studies often emphasize the challenges in managing and insuring cyber risk (Eling and Schnell, 2016: 474). In addition, studies have been conducted in recent years focusing on the cyber insurance market and insurance companies offering cyber insurance products. The purpose of this study is to investigate the market practices of cyber insurance in Türkiye and to examine the cyber insurance market. For this purpose, there are three main research questions addressed in this study. The first of these aims to reveal the current situation of the cyber insurance market in Türkiye, the second the effects of the Covid-19 outbreak on the cyber insurance market, and the third one aims to reveal the opportunities and/or obstacles in front of the cyber insurance market.

In this study, following the study by Franke (2017), qualitative research method was employed and semi-structured interview forms were used as data collection tool. The semi-structured interview provides the researcher with the opportunity to progress according to the interview guide and to examine it in more depth when necessary (Gürbüz and Şahin, 2018: 184). The interview questions were prepared by the researchers in line with the basic research questions of this study and based on the study by Franke (2017). Before conducting the interviews, the interview questions were revised by two experienced experts. According to the answers received during the interviews, additional questions were also asked by the researchers in order to explore the subject in more depth. Insurance companies, insurance intermediaries (insurance agents and brokers) and reinsurers constitute the supply side of the cyber insurance market in Türkiye. In the study, interviews were conducted with six non-life insurance companies active on the cyber insurance market in Türkiye. In order to keep the interviewed company information confidential, these six insurers are anonymously referred to as Company 1 (Ş1), Company 2 (Ş2), Company 3 (Ş3), …, Company 6 (Ş6) in this study. All of the interviews were conducted through online interviews and both authors participated in all of them. Each interview lasted approximately one hour. Additionally, interviews were held with two sector representatives experienced in cyber insurance in Türkiye and their opinions and evaluations on the cyber insurance market were collected within the framework of the research questions.

As a result of the interviews with representatives from the non-life insurance companies participating in the research, the current situation of the cyber insurance market in Türkiye were examined under the headings of underwriting process and pricing, sector preference, requirements on the insured, insurance coverage, and response process when a cyber-incident is suspected. In addition, the effects of Covid-19 outbreak on the cyber insurance market and opportunities and/or obstacles to the cyber insurance market in Türkiye were tried to be revealed.

There is a consensus that the Covid-19 outbreak has increased both cyber-attacks and the need for protection. However, the findings show that the Covid-19 outbreak did not cause a permanent increase in cyber insurance demand in Türkiye. One of the main obstacles to the cyber insurance market in Türkiye is the lack of awareness regarding cyber insurance. Lack of historical data, unpredictability of loss rates, difficulties in pricing, and insufficient reinsurance capacity stand out as other important challenges to the development of the cyber insurance market in Türkiye. It is predicted that low insurance coverage rates, which are caused by the lack of awareness regarding cyber insurance and the other obstacles mentioned, will turn into an opportunity as steps are taken to overcome these obstacles.

In the study, interviews were conducted with only non-life insurance companies, which are among the actors that constitute the supply side of the cyber insurance market in Türkiye. A study in which insurance intermediaries and reinsurers will be among the informants may enable more comprehensive assessments of the cyber insurance market. In addition, it is expected that a research on the demand side of cyber insurance will contribute to the development of the cyber insurance market in Türkiye. In case of the availability of data on cyber insurance in Türkiye, it will be possible to empirically investigate the factors affecting the cyber insurance market participation of insurance companies, and their performance in the market.