togübil TOGÜ - Turhal Uygulamalı Bilimler Fakültesi Dergisi
Journal of Applied Sciences Faculty of TOGÜ-TURHAL

TOGÜ- TURHAL UYGULAMALI BİLİMLER FAKÜLTESİ DERGİSİ
Journal of Applied Sciences Faculty of TOGÜ-TURHAL
Dergi web sitesi: https://dergipark.org.tr/tr/pub/togubil

E-ISSN: *Yıl:2023* *Cilt: 1* *Sayı: 1* *Sayfa: 41-50* *Makale Türü: Araştırma Makalesi*

Sigorta Sektöründe Siber Riskler

Aylin Mercan Alkan[1]

M a k a l e B i l g i s i

Makale Süreci:

Geliş Tarihi: *09/ 11/ 2023*
Kabul Tarihi: *18/ 12/ 2023*

Anahtar Kelimeler:
Sigortacılık, Siber Riskler, Siber Sigorta

Jel Kodları: *G22, G20, G32*

Ö z e t

Siber riskler, iş dünyasının dönüşümü ve teknolojinin ilerlemesi ile büyük bir tehdit haline gelmektedir. Bu riskler, sınırları ortadan kaldıran küreselleşme ve hızla gelişen teknolojilerle birlikte katastrofik boyutlara ulaşmıştır. İşletmelerin bu yeni riskleri yönetebilmesi şirketlerin varlıklarını sürdürebilmesi için büyük önem taşımaktadır. Siber sigorta, siber tehditlere karşı koruma sağlayan bir poliçedir ve işletmeler için kritik bir araç haline gelmiştir. Siber riskler, siber saldırılar ve veri ihlalleri yoluyla işletmelere maddi kayıpların yanı sıra itibar kaybı gibi birçok farklı zararlara yol açabilir. Siber sigorta, bu risklerin karşılanmasında etkili bir çözüm sunar. Siber riskler, işletmeler ve bireyler için büyük bir tehdit oluştururken, siber sigorta ürünleri bu risklerin etkili bir şekilde yönetilmesinde yardımcı olabilir. Siber sigorta, siber tehditlere karşı finansal koruma sağlayarak iş dünyasının dijital dönüşümünü desteklemektedir. Bu nedenle, siber sigorta pazarının büyümeye devam etmesi beklenmektedir. Bu çalışmada Siber Sigorta ürünlerinin ve Siber Sigortacılıkla alakalı gelişmelerin güncel durumunu ortaya koymak amaçlanmaktadır. Çalışmayla sektörün siber sigortalar konusunda teorik kaynak eksiklerini tamamlamak hedeflenmiştir.

[1] Araştırma Görevlisi, Tokat Gaziosmanpaşa Üniversitesi, Turhal Uygulamalı Bilimler Fakültesi, Bankacılık ve Sigortacılık Bölümü, aylin.mercan@gop.edu.tr,

ORCID: 0000-0001-7611-8724

togübil TOGÜ - Turhal Uygulamalı Bilimler Fakültesi Dergisi
Journal of Applied Sciences Faculty of TOGÜ-TURHAL

TOGÜ- TURHAL UYGULAMALI BİLİMLER FAKÜLTESİ DERGİSİ
Journal of Applied Sciences Faculty of TOGÜ-TURHAL
Dergi web sitesi: https://dergipark.org.tr/tr/pub/togubil

E-ISSN: *Year:2023* *Vol: 1* *No: 1* *Pages: 41-50* *Submission Type: Research Article*

Cyber Risks in the Insurance Industry

ArticleInfo

Article Proces:

Received: *09/ 11/ 2023*
Accepted: *18/ 12/ 2023*

Keywords: *Insurance, Cyber Risks, Cyber Insurance*

JEL Codes: *G22, G20, G32*

Abstract

Cyber risks have become a significant threat to the business world with the transformation of businesses and the advancement of technology. These risks have reached catastrophic proportions in tandem with globalization, which erases borders, and rapidly evolving technologies. Managing these new risks is of paramount importance for companies to sustain their existence. Cyber insurance is a policy that provides protection against cyber threats and has become a critical tool for businesses. Cyber risks can lead to various damages for businesses, including financial losses and reputational damage, through cyber attacks and data breaches. Cyber insurance offers an effective solution to address these risks. While cyber risks pose a significant threat to businesses and individuals, cyber insurance products can help effectively manage these risks. By providing financial protection against cyber threats, cyber insurance supports the digital transformation of the business world. Therefore, the cyber insurance market is expected to continue to grow. This study aims to present the current state of Cyber Insurance products and developments related to Cyber Insurance. The study aims to complete the theoretical resource deficiencies of the sector on cyber insurance.

1. Giriş

Geleceğimiz artık dijital gelişmelere ve dijital altyapılara giderek bağımlı hale gelmektedir. Yaşanılan Covid 19 salgını birçok sektörde dijital kanallara geçişi hızlandırarak odak noktası haline getirmiştir. Pandemi sonucunda tedarik zincirlerinde yaşanan aksamalar, mallara ve hizmetlere olan ulaşımın gecikmesi ve zorlaşması kuruluşların dijital altyapıya olan bakışlarını değiştirmelerine yol açmıştır. Küreselleşme ve giderek gelişen teknolojilerle birlikte sınırların ortadan kalktığı günümüzde işletmelerin karşı karşıya kaldığı riskler de değişim göstermektedir. Sigorta şirketlerinin gelişmekte olan bu riskleri tespit etmesi, analiz etmesi ve yönetebilmesi yeni iş dünyasına etkili çözümler sunabilmek ve varlıklarını sürdürebilmek için büyük önem taşımaktadır. Yeni riskler belirsiz bir risk alanı içinde faaliyette bulunan sigorta şirketleri için gelecekte olası hasar talepleri doğurabilecektir. Bu çerçevede dünyada son gelişmelerle birlikte siber riskler, iklim değişikliği, nanoteknoloji, genetiği değiştirilmiş ürünler yeni riskler arasında sıralanabilmektedir.

Son 10 yılda bilgi teknolojilerinin yeri gerek işletme altyapısında gerek toplumsal altyapıda artış göstermektedir. Finansal sistemlerden devlet altyapılarına kadar ülkelerin tüm sistemleri bilgi teknolojilerine bağımlı hale gelmektedir. Çoğu şirket için bu sistemlere ve sistemlerindeki hassas bilgilere yönelik siber riskleri yönetmek öncelikli konuma gelmiştir. Siber saldırılar ile veri ve sistemlere zarar verilebilmekte veya kişisel bilgiler gibi hassas bilgiler çalınabilmektedir. Bu saldırıların büyüklüğü ve yol açtığı maliyetlerin artması sigorta şirketlerinin siber riskleri yönetme konusunda etkili bir araç olabileceğini düşündürmektedir.

Güvenlik ihlallerinin ve siber saldırıların giderek artması işletmeler için siber riskin bir katastrofik risk boyutuna gelmesine neden olmuştur. Çoğu işletme için siber risklerin doğurabileceği kayıplar doğal afet risklerinden daha ciddi boyutlara ulaşmıştır. Şirketlere yapılan siber saldırılarda maddi kayıpların yanında şirkete karşı güvensizlik oluşması ve itibar kaybı da riskin şiddetini artırabilmektedir. Şirketler marka değeri ve müşteri ilişkilerinin karlılık kadar önem taşıdığı bu dönemde karşılıklı güveni zedeleyebilecek siber risklere karşı ciddi önlemler almaktadır. Özellikle dijital dönüşümün oldukça hızlı bir ivmeyle ilerlediği sigorta sektöründe kullanılan yazılım teknolojilerinin (bulut teknolojisi ve yapay zekâ gibi) çeşitliliği arttıkça karşılaşılabilecek saldırıların da değişerek artabileceği göz önünde bulundurulmalıdır. Şirketlerin siber risklerden kaynaklanabilecek zararları önleyici ve azaltıcı risk planları oluşturması risk yönetim sürecinde büyük önem taşıyabilmektedir.

2. Kavramsal Çerçeve

2.1 Siber Risk Nedir?

Bilgisayarın ve internetin icadı tüm dünyada devrim olarak nitelendirilebilecek gelişmelere yol açmış, bireyler, işletmeler ve hatta ülkeler arasında sınırlar adeta yok olmuştur. Teknoloji birçok alanda kolaylıklar ve fırsatlar sunarken bir taraftan da yeni bir suç türünün doğmasına neden olmuştur. “Siber uzay, tüm dünyaya ve uzaya yayılmış durumda bulunan bilişim sistemlerinden ve bunları birbirine bağlayan ağlardan oluşan veya bağımsız bilgi sistemlerinden oluşan sayısal ortamdır (T.C. Ulaştırma Bakanlığı, 2023). Bu sebeple siber kavramını sadece internet olarak algılamamak gerekmektedir (Clarke, 2011). Siber ortam bilginin yaratıldığı, saklandığı, paylaşıldığı bir sistem ve altyapıları içeren tüm alan olarak değerlendirilebilir.

2009 tarihinde ABD Ulusal Araştırma Konseyi siber saldırıyı: “Bilgisayar sistemleri, ağlar veya bilgiyi ve/veya bunlarda yerleşik olan ya da bunları taşıyan programları değiştirmek, bozmak, aldatmak, küçük düşürmek veya yok etmek için yapılan kasıtlı hareketler olarak” tanımlanmıştır (Singer, Friedman, 2015). Bilişim sistemleri ilk olarak 1970’li yıllarda muhasebe ve arşivleme işlemlerini yapmak üzere işletmelere girmiştir. Günümüzde ise satış kanalından tüm operasyonel süreçlere kadar ağ bağlantılı sistemlere geçilmiştir. E-posta ve elektronik imza ile birçok iş faaliyeti, sözleşme ve anlaşmalar online ortamda düzenlenebilmektedir. Pazarlama faaliyetleri için sosyal medya, web sitesi gibi gelişmiş dağıtım kanalları kullanılmaya başlanmıştır. Bu geniş yayılımın beraberinde getirdiği riskler siber riskleri oluşturmaktadır (Ünal, 2014).

Siber riskler şirketlerin üretim ve operasyonel süreçlerinde öngörülemeyen zararlara yol açabilmektedir. Yeterince test yapılmadan gerçekleştirilen bir yazılım güncellemesi sonucunda oluşabilecek küçük bir hata tüm üretimin durdurulması noktasına kadar gelebilmektedir. Tüm önemli ve gizli bilgilerin bilgisayar ortamında depolandığı düşünüldüğünde bigdata teriminin önemi ortaya çıkmaktadır. Günümüzde en değerli şirket varlıklarından birisi de bu büyükveri ve bu verinin işlenmesidir. Siber saldırıların artması kuruluşların bu değerli varlıkları ve verileri için bir tehdit unsuru olabilmektedir. Siber risklerle mücadeleyi zor hale getiren ise dijitalleşmenin oldukça hızla gerçekleşmesidir.

2.2. Siber Risk Türleri

Siber risklerde uygulanan birçok farklı saldırı yöntemi bulunmaktadır. Savunma Teknolojileri Mühendislik ve Ticaret A.Ş. (STM)’nin 2019 Ekim-Aralık Siber Tehdit Durum Raporu’na göre Türkiye’de en çok sahte

uygulamalar üzerinden sosyal mühendislik saldırıları gerçekleşmiştir. Bunlardan en çok tehlike oluşturan zararlı yazılım hemen her vatandaşın kullandığı E-Devlet'in sahte uygulaması olmuştur. Diğer en çok görülen saldırılar ise Kişisel Verilerin Güvenliği ve Veri Sızıntıları, Sosyal Medya Üzerinden Siber İstihbarat, Sağlık ve Ulaşım Sektöründeki Tehditler, IoT ve Akıllı Sistemlere Yönelik Tehditler olarak karşımıza çıkmaktadır (Savunma Teknolojileri Mühendislik ve Ticaret A.Ş., 2023).

2.2.1 Bilgisayar Korsanlığı

Bir bilgisayar sistemine yetkisi bulunmadığı halde sistemin güvenlik duvarlarını etkisiz hale getirerek girmeye çalışmaktır. Bu işleme hack, saldırıyı gerçekleştiren kişilere ise hacker adı verilmektedir. Hackerler sistemin içindeki güvenlik açıklarını tespit ederek bu açıklardan faydalanabilmektedir (Emniyet Genel Müdürlüğü, 2023). Birçok firma ağlarındaki bu güvenlik açığını yakalayabilen bilgisayar korsanları hakkında şikayetçi olmak yerine büyük ödüller vermeyi ve hatta iş teklifinde bulunmayı tercih etmektedir. Örneğin en popüler sosyal medya platformlarından biri olan Facebook'u hackleyerek güvenlik açıklarından birini bulan Andrey Leonov isimli hacker için şirket 40,000 dolar ödül ödemiştir (Vatan Gazetesi, 2023).

2.2.2 Zararlı Yazılımlar

Kötü amaçla oluşturulan her türlü yazılım zararlı yazılım olarak değerlendirilebilmektedir. Bilişim sistemleri için büyük tehlike oluşturan bu yazılımların farklı türleri bulunmaktadır. Virüsler, Truva atı, rootkitler, casus yazılımlar, solucanlar bunlardan bazılarıdır.

Virüsler internet ortamından, e-posta, bağlantı linkleri, usb (flash bellek) gibi aygıtlardan bilgisayara bulaşabilen zararlı yazılım kodlarından oluşmaktadır. Diğer yazılımlardan farklı olarak kendilerini diğer programlara kopyalayabilmekte ve bu şekilde yayılabilmektedirler (Akarslan, 2015). Virüslerin diğer bir özelliği de kullanıcı tarafından bir linke tıklanarak aktifleştirilmeye ihtiyaç duymasıdır. Mantık bombaları adı verilen yazılımlar da bir tür virüs programıdır. Bu programlar yaratıcıları tarafından belirlenen bir tarihte aktifleşmek üzere çalışmaktadırlar. Belirlenen tarihe kadar faydalı bir yazılım olarak işlem yapan ve fark edilmeyen bu virüs aktifleştiğinde bilgisayardaki tüm dosyaları, verileri ve bilgileri silebilmekte ve hatta sistemi tamamen çökertebilmektedir. Mantık bombası olarak bilinen en popüler zararlı virüslerden biri 'çernobil virüsü'dür. CIH (Çernobil Virüsü), 1998 yılında ortaya çıkmış, ana kartların Eprom (Erasable Programmable Read Only Memory) hafızasına veri yazarak kalıcı olarak donanıma zarar veren ilk virüs olmuştur (Ulusal Siber Olaylara Müdahale Merkezi (USOM), 2014).

Solucanlar tıpkı virüsler gibi kendini bilgisayarlar arasında kopyalayabilen ancak virüslerden farklı olarak ağ üzerinden otomatik olarak yayılabilen zararlı yazılımlardır. Solucanlar genellikle P2P dosya paylaşımı, virüslü web siteleri ve e-posta eklerinin indirilmesi yoluyla yayılmaktadır (Gönen, Kaya, 2023).

Truva atı veya trojenler herhangi bir yasal program yüklenirken arka planda kullanıcının bilgisi dışında işlem yapan kötücül yazılımlardır. Lisanslı ve ücretli bir programın internet üzerinden ücretsiz olanını yükleyerek bilgisayara bulaşımı sağlayabilmektedir. Örneğin bilgisayarına flash player yüklemek isteyen bir kullanıcı güvenli yükleme alanı olan Adobe yerine başka bir kaynak kullandığında Truva atını yükleyebilmektedir. Bulaştığı sistemde cihazın kontrolünü ele geçirme, farklı kötücül programları indirme, kullanıcıların verilerine erişme gibi zararlar verebilmektedir (Denning, 1988).

2.2.3.Yemleme (Phishing)

İllegal yöntemlerle kullanıcıların kimlik, şifre, kullanıcı adı, kart numarası, hesap numarası gibi hassas kişisel bilgilerini ele geçirmeye çalışan saldırılardır. Şifre avcılarına yemleyici adı verilir ve yemleyiciler güvenilir bir kaynak gibi gözükerek kullanıcıdan birçok kişisel veriyi isterler. Örneğin bir banka e-posta adresi gibi görünerek e-posta atabilir ve kullanıcının şifre, kredi kartı gibi bilgilerini ele geçirebilirler. Google Play gibi ödeme yapılabilen bir hesap üzerinden sanki yüksek tutarlı bir harcama yapılmış gibi e-posta gönderebilirler. Daha sonra 'bu harcamayı yapan siz değilseniz şu linke tıklayınız' şeklinde bir link göndererek Google Play'in kendi adresine çok benzeyen bir linke tıklanmasını sağlarlar. Tutarın iadesi için T.C. kimlik numarasından anne kızlık soyadına kadar tüm bilgilerin girilmesini isteyebilirler. Son dönemde en yaygın yapılan saldırılardan biri olan phishing sosyal mühendislik saldırılarının bir türü olarak bilinmektedir (Whitetaker, Ryner & Nazif, 2010).

2.2.4.Siber Casusluk ve İstihbarat Saldırıları

Devletler veya şirketler tarafından yapılabilen sosyal mühendislik saldırılarıdır. Şirketler açısından bakıldığında genellikle rakip firmanın hassas bilgilerine ulaşmak, finansal planlarını ele geçirmek için yapılabilmektedir. Örnek olarak iki yazılım devi olan Microsoft ve Oracle şirketleri arasında gerçekleşen siber casusluk olayları verilebilmektedir.

Siber casusluk bir devletin diğer bir devlete zarar vermek amacıyla yapabileceği siber eylemlerden biridir. Bu saldırılar siber savaşa neden olabilecek boyutlara ulaşabilmektedir. Diğer devlete ilişkin sırlar ele geçirilebileceği gibi zaman ve emek harcanan değerli bir buluşun çalınması gibi sanayi alanında birtakım bilgiler de ele geçirilmeye çalışılabilmektedir. Artan rekabet, teknoloji ve ticaret savaşları düşünüldüğünde devletlerin bu siber saldırılar ile üstünlük sağlamaya çalışmaya devam edebileceği düşünülmektedir (Yayla, 2013). APT (Advanced Persistent Threats) adı verilen Çinli bir tehdit grubu siber casusluk yaparak finansal kazanç sağlamayı amaçlamaktadır. 2012'den beri aktif olan bu grubun 4 ülkenin sağlık, telekom, teknoloji ve video oyun endüstrilerine saldırdığı tespit edilmiştir. Bu 14 ülke arasında Türkiye de bulunmaktadır (STM, 2019).

STM raporuna göre Türkiye'de 28 Ekim- 27 Kasım 2019 arasında Türk bankalarına ait 455.000'den fazla kart bilgisinin çalındığı ifade edilmiştir. Bu kart bilgileri "Joker's Stash" isimli underground sitesinde, farklı gruplar halinde 3 dolar veya 1 dolara satışa çıkarılmıştır. Sitedeki kart bilgileri detaylı olarak incelendiğinde sadece kart bilgileri değil ayrıca kart sahibinin adı soyadı, telefon numarası, e-posta adresi gibi bilgilerin de yer aldığı görülmüştür (STM, 2019).

2.3. Siber Risklerin Yönetimi

Siber risk belirli bir tehdidin, sistemin herhangi bir açığını yakalayarak zarar verme ihtimalidir. Gerekli önlemler alınmadan önce oldukça büyük olan bu risk, karşı önlemler geliştirildikçe azalmaktadır. Güvenlik önlemleri alındıktan sonra oluşabilecek risklere arta kalan risk adı verilirken önlem alınmamış haldeki risklere taban riski denilmektedir. Siber risklerin yönetim sürecinde sistemin karşılaşabileceği belirsizliklerin tespit edilmesi, analizi, ortadan kaldırılması, ya da minimum seviyeye indirilmesi hedeflenmektedir. Risk yönetimi; tehditlerin neler olabileceği, bu tehditlerin denetimi, risk analizi yapılması, güvenlik sistemlerinin oluşturularak gözden geçirilmesi gibi süreçler ile zararı yok etmeyi veya en aza indirmeyi hedefler. Siber risklerin yönetiminde değişime ne kadar hızlı bir şekilde ayak uydurulabilirse o kadar etkili sonuçlar alınabilecektir. Risk sıfıra indirebilmek mümkün olmasa da risk yönetimi ile azaltılabilmektedir. Örneğin internet ortamında müşteri ile etkileşim halinde olunan bir uygulama varsa ve bu uygulamanın karşılaşabileceği tehditlere karşı önlem alınmıyorsa durum çok büyük zararlarla sonuçlanabilmektedir. Dolayısıyla kurumların ve kişilerin siber risklere karşı bilinçlenmesi, siber güvenliğin önemini kavrayarak bunu sistemin bir parçası olarak görebilmesi büyük önem taşımaktadır (Marsh & McLennan, 2020).

Tehditlere karşı her şirket kendi sektörüne ve kritik envanterine göre bir yönetim sistemi oluşturmalıdır. Önemlerin alınması hususunda güncel siber saldırıları takipte olmalıdır küçük önlemlerle bile büyük siber saldırıların önüne geçilebileceğinden siber güvenliğe gereken önemi saldırı sonrasında değil, öncesinde vermek gerekmektedir (KPMG, 2023).

Siber risklerin yönetiminde şirket veya organizasyonların sistem üzerindeki tüm veri ve hassas bilgilerin envanterinin çıkarılması ve bu bilgilerin kaybedilmesi veya kötü amaçlı kullanılması durumunda şirkete verebileceği zararlar değerlendirilmelidir. Şirketin varlıklarında meydana gelebilecek kayıplar, finansal tüm zararlar, 3. şahıs veya şirketlere karşı doğabilecek sorumluluklar analiz edilmelidir. Şirketler yazılım konusunda dışarıdan hizmet alıyorsa bilgi teknolojileri konusunda üçüncü şahıslara ne kadar bağımlı olduğunu belirlemelidir. Güvenlik sistemlerini oluşturan antivirüs ve güvenlik duvarı gibi sistemleri olası risklere karşı güncel tutmalıdır. Riskin önemli bir kaynağı da insan faktörü olduğundan çalışanların şirket hesapları ve özellikle sosyal medya üzerinden yaptıkları işlemlerin herhangi bir itibar kaybına ve yasal tazmin yükümlülüğüne yol açmaması konusunda dikkatli olunmalıdır. Bu hususta şirket çalışanlarının aktiviteleri sırasında uyması gereken kurallar belirlenmeli ve yazılı olarak iletilmelidir (Ünal, 2014)

Şirketlere 4. Sanayi devrimi ile gelen akıllı telefon, yapay zekâ, sosyal medya, makine öğrenmesi, nesnelerin interneti, kripto para, bulut gibi teknolojiler siber saldırılar için siber uzayın genişlemesi anlamına gelebilmektedir. Her yeni uygulama veya cihazda bilinmeyen güvenlik açıkları olacağından siber saldırılar için uygun ortam bulunabilmektedir. Ayrıca zamanla hackerlerin bilgi düzeyi ve yetenekleri gelişecek buna istinaden yapılan saldırılar da profesyonelleşecek ve daha yaygın yapılabilecektir (Orbis, 2018).

Şirketin siber güvenlik ihlali olaylarını önlemek, tespit etmek ve bunlara müdahale etmek için hangi araçları, süreçleri ve kontrolleri kullandığı belirlenmelidir. Önleme, tespit etme ve müdahale konusundaki öncelikler ve yatırımlar değerlendirilmelidir. Şirketin sisteme herhangi bir tehdit söz konusu olduğunda uyarı sisteminin bulunması ve proaktif siber savunma programlarına entegre edilebilir olması gerekmektedir. Bilinen saldırı türlerine ve onu hedefleyebilecek tehdit aktörleri tarafından kullanılan araçlara karşı güvenlik açıklarını değerlendirebilmeli ve potansiyel tehditleri anlayabiliyor olmalıdır. Hangi verilerin rakip şirketler için değerli olabileceği belirlenmeli ve güvenlik yatırımlarının bu varlıkların çalınması veya tehlikeye atılmasına karşı koruma konusunda yeterliliği sağlanmalıdır. Şirket yöneticilerinin, tehditler, saldırılar, savunma teknolojileri ve risk

azaltma stratejileri konusunda siber güvenlik uzmanları ile güçlü iletişim halinde olmaları gerekmektedir (Allianz Risk Barometer, 2022).

2.4. Siber Risklerin Sigortalanması

Munich Re 'Cyber insurance: Risks and Trends' 2023 raporuna göre 2023 yılı itibariyle dünya çapında 4,7 milyon uzman siber güvenlik alanında çalışmaktadır. 2022 yılında 8,44 trilyon ABD doları olan siber suç maliyetinin 2023 yılında yaklaşık 11 trilyon ABD doları olması beklenmektedir. 2027 yılında ise bu rakamın 24 trilyon ABD dolarına ulaşabileceği düşünülmektedir. Cybersecurity Workforce Study (ISC)'nin çalışmasına göre işletme ve kuruluşları artan bu maliyet tehditinden koruyabilecek yeterli nitelik ve bilgi düzeyine sahip 3,4 milyon çalışan açığı bulunmaktadır. Ayrıca gittikçe kompleks hale gelen yeni bilgi teknolojilerinin açıklarına güvenlik sağlayabilecek nitelikte iş gücünün olmaması da gelecekte siber saldırıların daha kaotik olabileceği düşüncesine yol açmaktadır.

Günümüzde siber riskler, teknolojiler ve güvenlik açıkları yıldırım hızında gelişmektedir. Siber tehditler ve müdahalelerle ilgili kamu ve özel kuruluşlar arasında bilgi paylaşımı güçlü bir siber güvenlik programının temel gerekliliği haline gelmiştir. Bu karmaşık risk ortamına çözüm olarak, şirketler siber risk hakkında bilgi edinmek ve daha iyi yönetmek için yeni fırsatlar aradıkça sigorta ürünleri pazarı da gelişmektedir. Şu anda, bir şirketin müşterilerinin siber kaynaklı bir kayıp nedeniyle uğradıkları zararları karşılamak için önemli bir sigorta pazarı bulunmaktadır (AON, 2021). Bununla birlikte, sigorta endüstrisi, kaybedilen fikri mülkiyet, itibar ve markanın değerini kapsayan birinci taraf politikaları ve siber altyapı hatalarını kapsayan ürünler gibi yeni siber risk alanlarına doğru genişlemeye çalışmaktadır. Bu gelişmenin önündeki çeşitli zorluklar bulunmakla birlikte bunlardan birisi de siber saldırılardan kaynaklanan kayıp olasılıklarını doğru tahmin edebilmek için geçmişteki verilerin yetersiz olmasıdır. Bu veri eksikliği nedeniyle uygun primin hesaplanmasında zorluklar yaşanmaktadır (Odell, Fauntleroy & Wagner, 2015).

2023 Munich Re raporunda 2022 yılında siber saldırıların rekor seviyeye ulaştığı ifade edilmiştir. Aynı zamanda dijital verilerin ele geçirilmesine yönelik saldırılarda artış olmuştur. Fidye yazılımları ve tedarik zinciri saldırıları 2022 yılının en çok gerçekleşen saldırı türleri olmuştur. Gelecekteki siber saldırıların ChatGPT gibi yapay zekâ tabanlı uygulamalar, 'metaverse' veri tabanı ve operasyonel teknoloji (OT) dünyaları gibi önemli teknoloji trendleri ile birlikte farklılaşarak artması beklenmektedir. Tüm bu teknoloji evreninin bireyler, işletmeler ve devletler için önemli fırsatlar sunarken aynı zamanda yeni birçok riski de beraberinde getirebileceği ifade edilmektedir. Yeni saldırı ortamlarının oluşması, oluşabilecek yeni güvenlik açıkları ve yeni sistemik riskler bu risklerden bazılarıdır.

İşletmeler siber sigortayı siber risk yönetimi stratejisinin etkili bir bileşeni olarak görmelidir. İlk adım olarak işletmeler, mevcut siber sigorta ürünlerini proaktif olarak değerlendirmeli ve fiyatlandırmayı anlamalıdır. Şirketler, teklifleri tanımlamak için aktif olarak çalışan sigorta şirketlerinin gelişimlerine katılma fırsatına sahip olabilirler. Şirketler ürünleri değerlendirip seçerken, sigorta şirketleri ile risk kontrol unsurlarını yönlendiren iyi güvenliğin temellerini ve bu uygulamaların benimsenmesinin kapsamı ve primleri nasıl etkileyebileceğini tartışmalıdırlar (PwC, 2014).

İlk olarak 1990 yılında Amerika Birleşik Devletleri'nde kullanılan siber sigorta ürünleri 2000'lerin başında Avrupa ve ilk kez 2012 yılında Türkiye'de teminat sağlamaya başlamıştır. Önceleri yalnızca veri kaybıyla sınırlı olan poliçenin kapsamı doğan ihtiyaçlarla birlikte genişlemektedir. World Economic Forum 2019 raporunda Avrupa'daki top 10 risk arasında siber riskler birinci olmuştur (World Economic Forum, 2019).

Siber saldırıların bazı etkileri aşağıdaki gibidir (KPMG, 2018):

- Müşteri bilgilerinin ifşası; Finansal kayıp, cezai yaptırım ve itibar kaybı
- Fikri mülkiyetin çalınması; Rekabet dezavantajı ve finansal kayıp
- Kurumsal verinin çalınması; Finansal kayıp, itibar kaybı
- Servislere ulaşılamaması; Müşteri erişiminin kesilmesi, finansal kayıp, itibar kaybı
- Tedarik hizmetlerinin zarar görmesi; kesintiler, finansal kayıp, itibar kaybı
- IP fikri mülkiyetinin çalınması

Siber sigortalar yukarıda sıralanan risklerin transferi açısından önemli bir araçtır. Siber sigorta ürünleri ile veri ihlalleri, iş durması ve sistem hasarlarının neden olabileceği kayıplar azaltılmaya çalışılmaktadır. Dijital teknolojilere olan güvenin artması, dijital güvenlik ve gizlilik risklerinin artmasına ve poliçe sahiplerine bu risklerin çoğuna karşı finansal koruma sağlamak için bir siber sigorta pazarının ortaya çıkmasına neden olmuştur. OECD raporuna göre poliçelerin kapsama aldığı temel altı siber olay aşağıdaki şekilde gösterilmiştir (Organisation for Economic Co-operation and Development (OECD), 2020).:

- Siber dolandırıcılık ve hırsızlık
- Siber zorbalık
- Teknoloji bozulması
- Ağ güvenliği yükümlülüğü
- İletişim ve medya sorumluluğu
- Veri gizliliği ihlalleri

Siber risklerin sigorta kapsamı belirlenirken mülk için mi veya sorumluluk için mi yapılacakları düşünüldüğünde sunulan teminatların türü oldukça farklılaşabilmektedir. Bu durum şirketlerin siber risk havuzunu oluştururken zorlanmasına neden olabilmektedir. Siber risklerin underwriting ve fiyatlandırma süreçlerinin karmaşık olması da zorluklardan birisidir. Siber sigortaların yaygınlaşması için sigorta sisteminin çalışmalarının yanında hükümetin, regülasyonların, teknoloji şirketlerinin, broker gibi aracıların da iş birliği gerekmektedir (OECD, 2020).

Siber sigortaların ilk alıcısı olan şirketlere bakıldığında medya ve telekomünikasyon sektörü başta gelmekteyken sonrasında finansal kurumlar ve perakendeciler gelmektedir. Siber risk pazarının büyümesinde şirketlerin ve bireylerin risk bilincinin artmış olması etkili olmuştur. Buna karşın OECD ülkeleri içinde siber sigorta primleri hayat dışı branşın %0,5'ini oluşturmaktadır. Bu oran siber sigortanın büyüme potansiyeli olan bir pazar durumunda olduğunu göstermektedir. Nitekim yapılan araştırmalar 2025 yılında prim üretimi tahminlerinin 20 milyar ABD dolarını aşacağını ifade etmiştir (AON, 2017).

Örnek olarak Anadolu Sigorta A.Ş.'nin siber güvenlik ürünleri incelendiğinde Bireysel Siber Güvenlik Sigortası ve Ticari Siber Güvenlik Sigortası olmak üzere iki ürünü bulunmaktadır. Bireysel poliçenin teminatları; hukuki danışma, kimlik hırsızlığı, online saygınlığa zarar verilmesi, e-reputasyon, e-alışveriş, ödeme araçlarının hileli kullanımı ve kişisel şifre çalınması olarak düzenlenmiştir. Ticari siber güvenlik poliçesi teminatları; veri koruma hasarları, iş durması, siber fidye, bilgi güvenliği ve gizlilik sorumluluğu, kamu otoritesine karşı yapılan savunmalar ve para cezaları, veri ihlali, üçüncü kişilerden gelecek tazminat talepleri olarak düzenlenmiştir (www.anadolusigorta.com, 2023).

2.5. Siber Sigorta Verilerine Bakış

Tablo 1'de 2022 yılına ait toplam yazılan siber sigorta primlerinin yaklaşık 14 milyar dolar olarak gerçekleştiği görülmektedir. Yazılan primlerde en büyük üretim payına %71 ile Amerika'nın sahip olduğu, %29'luk payın Avrupa ve Afrika'ya ait olduğu gözlemlenmektedir. Asya ise %1'den daha az bir prim üretimine sahiptir.

Tablo 1. Siber Toplam Yazılan Primler, bölgesel (milyar dolar)

	Toplam Yazılan Primler	Toplam Yüzde	Ülkeler	Kayıp Data
Amerika	**9,693.41$**	**71%**	**5**	**0**
Asya	**55.72 $**	**<1%**	**3**	**0**
Avrupa&Afrika	**3,947.67 $**	**29%**	**11**	**1**
Toplam	**13,696.80 $**	**%100**	**19**	**1**

Kaynak: Global Insurance Market Report (GIMAR), Special Topic Edition, Cyber, April 2023

Tablo 2'deki verilere göre 2022 yılı için gerçekleşen net hasar tutarlarına bakıldığında yaklaşık 4 milyar dolar bir hasar gerçekleşmiştir. Hasarların %63'ü Amerika'da gerçekleşirken %37'si Avrupa&Afrika ülkelerinde gerçekleşmiştir. Sigorta şirketlerine göre, en yüksek potansiyel sigortalama kayıplarına sahip siber tehditler fidye yazılımı ve toplu güvenlik açığı saldırıları olurken, bunu bulut veri kesintisi, veri ihlalleri ve üçüncü taraf hizmet sağlayıcılardan kaynaklanan güvenlik açıkları takip etmektedir.

Tablo 2. Bölgelere Göre Siber Hasar Tutarları (milyar dolar)

	Net Hasarlar	Toplam Yüzde	Ülkeler	Kayıp Data
Amerika	**$2,677.01**	**%63**	**5**	**0**
Asya	**$4.35**	**%0**	**3**	**0**
Avrupa&Afrika	**$1,575.93**	**%37**	**11**	**4**

Toplam	**$8,252.94**	**%100**	**19**	**4**

Kaynak: Global Insurance Market Report (GIMAR), Special Topic Edition, Cyber, April 2023

Siber riskler geniş çaplı etki alanına sahip, sürekli gelişen ve büyüyen özgün risklerdir. Siber riskler sigorta şirketleri için aynı zamanda hem operasyonel hem de ticari bir risk boyutundadır. Operasyonel anlamda sigorta ürününün hasar ve yönetimsel riskleri söz konusu olabilecekken, ticari anlamda da şirketin kendisi siber saldırıya uğrayabilir ve sonucunda hasar taleplerini karşılama, işleme koyma ve hizmet sunma hizmetleri en çok ihtiyaç duyulan anda sekteye uğrayabilmektedir.

Allianz'ın 2020 risk barometre raporunda 2022 yılı için en önemli top 10 risk sıralamasında siber riskler birinci sırada gelmektedir. Bu riskler 2021 yılındaki rapora göre %44 oranında bir artış göstererek zirveye yerleşmiş, tedarik zincirinde yaşanan riskler ve doğal afet gibi riskleri geride bırakmıştır. Siber riskin en yüksek görüldüğü ülkeler ise Avustralya, Belçika, Brezilya, Hindistan, Danimarka, Japonya, Nijerya ve Güney Afrika olarak belirtilmiştir.

Siber sigortaların yönetimi ve gelişimde çeşitli engeller bulunmaktadır. Bu zorluklardan birisi de verilerin yetersiz olması ve veri toplama zorluğudur. Bu durum doğrudan fiyatlandırma sürecinin kalitesini etkileyebilmektedir. Standardize edilmiş bir veri modelleme yapısının olmayışı ve kayıpların tahmininde belirsizlerin yüksek oluşu siber risklerin ölçümünü zorlaştırmaktadır. Sigorta ve reasürans şirketlerinin temel sigortacılık işlemleri ve hasar yönetimi anlamında gerek duyulan teknik ve aktüeryal beceriyi güçlendirebilmek adına siber iş gücüne de yatırımlar yapması önem taşımaktadır.

3. Sonuç

Teknoloji ve internete bağımlılık gerek bireysel gerek şirketler bazında artarken beraberinde yeni riskleri de getirmektedir. Siber riskler son dönemde tüm risklerin önüne geçerek bazı ülkeler için bir numaralı risk konumuna gelmiştir. Bu riskin en önemli özelliklerinden biri tek bir kişinin oturduğu yerden yalnızca bir bilgisayarla dünya çapında zarar verebilme olanağına sahip olmasıdır. Sınırların olmadığı ve hasarların giderek arttığı siber uzayda risklerin etkili bir şekilde yönetilmesi ihtiyacı doğmuştur. Siber krizleri yönetmek, yönetim araç setinin giderek daha önemli bir parçası haline gelmektedir.

İşletmelerin gerek değişen tehditlere gerekse sınır ötesi mevzuat gerekliliklerine uyma ihtiyacının bir sonucu olarak, gizlilik ve güvenliği çalışma biçimlerine dahil etmeye giderek daha fazla önem vermeleri beklenmektedir. Siber güvenliğin her iş kolunun, fonksiyonun, ürünün ve hizmetin ayrılmaz bir parçası haline gelmesi önem taşımaktadır. Herhangi bir ayrım yapılmaksızın, küçük işletmelerden büyük devletlere kadar herkes siber risklerle karşı karşıya kalabilmektedir. Siber saldırılar için gerekli önlemleri almak, güvenlik sistemleri oluşturmak ve gerçekleşen bir kayıp söz konusu olduğunda bu kayıpları karşılayabilmek gerekmektedir. Konusu risk olan sigortacılık sektörü, siber risklerin yönetiminde ve yol açabileceği risklerin en aza indirilmesinde etkin rol oynayabilecek bir sektör konumundadır. Nispeten yeni olan siber sigortaların önünde, veri eksikliği, büyük sayılara ulaşılamamış olması, bilgi eksikliği, risk bilincinin gelişmemiş olması gibi birtakım engeller bulunmaktadır. Ancak gelişmekte olan ekonomisi, özellikle finans sektöründe yaygın olarak kullanılan ileri bilgi teknoloji sistemleri, genç nüfusu ve yabancı yatırımlar için iyi bir pazar olması nedeniyle Türkiye siber sigorta ürünleri için avantajlı konumdadır. Etkili bir siber güvenlik için sigorta şirketleri, teknoloji şirketleri ve devletin iş birliği içerisinde olması büyük önem taşımaktadır.

Siber sigorta pazarının karşısındaki zorluklar ancak siber saldırı ve siber güvenlik hakkında yeterli bilgi ve farkındalık düzeyine ulaşıp primi doğru hesaplayabilecek düzeye gelerek azaltılabilecektir. Ayrıca asimetrik bilgi ve ters seçilim ortamının giderilebilmesi ile poliçe teminatları arasında karşılaştırmalar ve verimli düzenlemeler yapılabilecektir. Tıpkı trafik sigortalarındaki gibi suistimallerin veya hasarların kaydedildiği TRAMER gibi bir veri tabanı sisteminin oluşturulması hasar sürecinde ve yeni saldırıların tahmininde yardımcı olabilecektir. Şirketlere sektörü fark etmeksizin siber güvenlik konusunda bilgilendirme veya eğitimler düzenlenmesi, sigorta bilincinin artırılmasının sağlanması, şirket çalışanlarının bilgi teknolojileri ile koordine çalışması gibi düzenlemelerin siber sigortaların yaygınlığı konusunda olumlu yönde etkili olabileceği düşünülmektedir. Siber sigorta, siber tehditlerin hızla geliştiği bir ortamda işletmeler ve bireyler için önemli bir güvenlik ağı sağlayabilir. Dolayısıyla, siber sigorta ürünleri sağlayan şirketlerin sürekli olarak pazarın ihtiyaçlarına ve değişen tehdit manzarasına uyum sağlaması önemlidir.

Siber risk yönetimi dijitalleşen dünyanın temel rollerinden biridir. Siber sigorta bunun önemli bir parçası olduğu için siber sigortalara talebin güçlü bir şekilde artması beklenmektedir. Sürdürülebilir bir siber sigorta pazarının oluşturulması, sigorta sektörü için önemli bir görev olmaya devam edeceği düşünülmektedir.

Kaynakça

Akarslan, H. (2015). Bilişim Suçları, 2. Baskı, Seçkin Yayınları.

Allianz Risk Barometer (2022). Allianz Global Corporate & Specialty, January.

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

Anadolu Sigorta, Bireysel Siber Güvenlik Sigortası Bilgilendirme Formu, https://www.anadolusigorta.com.tr/i/content/45_1_SR906.0220.pdf. 07.11.2023

Anadolu Sigorta, Ticari Siber Güvenlik Sigortası, https://www.anadolusigorta.com.tr/tr/ticari-siber-guvenlik-paket-policesi 07.11.2023

AON Inpoint (2017). Uncovering the Hidden Opportunities, Global Cyber Market Overview.

AON, (2016). Cyber-The Fast Moving Target, Benchmarking Views And Attitudes By Industry.

AON, (2021). Cyber Security Risk Report, February.

Clarke, R., Robert K., (Nisan 2011). Siber Savaş, (Çeviren: Murat Erduran), İkü Yayınevi.

Denning, P., (1988). Computer Viruses, NASA Ames Research Center, RIACS Technical Report TR-88.10.

Emniyet Genel Müdürlüğü, https://www.egm.gov.tr/siber/sibersucnedir, 05.11.2023

Global Insurance Market Report (GIMAR). (2023). Special Topic Edition, Cyber, April.

KPMG, (2018). Siber Güvenlik Sigortası Risk Değerlendirme Hizmetleri.

KPMG, (2023). Cybersecurity considerations 2023.

Marsh & McLennan Insights, (2020). MMC Cyber Handbook 2020 Advancing Cyber Resilience.

Munich Re (2023). Cyber insurance: Risks and Trends.

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. 01.10.2023

Odell, L. A., Fauntleroy, J. C., & Wagner, R. R. (2015). Cyber Insurance–Managing Cyber Risk. Institute for Defense Analyses, April.

Organisation for Economic Co-operation and Development (OECD), (2020). Encouraging Clarity in Cyber Insurance Coverage, The Role Of Publıc Polıcy And Regulation.

OECD, Building a Sustainable Cyber Insurance Market, Insurance Policy Insights, https://www.oecd.org/daf/fin/insurance/Building-a-Sustainable-Cyber-Insurance-Market.pdf. 28.10.2023

Orbis Research (2018). Global Cyber Security Insurance Market, https://www.reuters.com/brandfeatures/venture-capital/article?id=36676. 27.09.2023

PwC, (2014). Managing Cyber Risks with Insurance, June.

Reeve, T. (n.d.), Cyber insurance not trusted by business, KPMG claims, SC Media, https://www.scmagazineuk.com/cyber-insurance-not-trusted-business-kpmg-claims/article/1478868. 27.08.2023

Singer, P.W., Friedman A., (2015). Siber Güvenlik ve Siber Savaş, (Çeviren: Ali Atav), Buzdağı Yayınevi, 1. Baskı, Mart.

STM, (2019). Siber Tehdit Durum Raporu, Ekim- Aralık.

Swiss Re, (2022). Cyber İnsurance: Strengthening Resilience for the Digital Transformation November.

T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, 2016-2019 Ulusal Siber Güvenlik Stratejisi, http://www.udhb.gov.tr/doc/siberg/2016-2019guvenlik.pdf (24.09.2023)

USOM, (2014). Siber Güvenliğe ilişkin Temel Bilgiler, Temmuz http://some.sdu.edu.tr/assets/uploads/sites/408/files/siber-guvenlige-iliskin-temel-bilgiler-22092017.pdf. 25.07.2023

Ünal, S. (2014). Siber Riskler, *Reasürör,* Sayı 91, Ocak.

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.

Vatan Gazetesi, http://www.gazetevatan.com/facebook-un-acigini-buldu-40-bin-dolar-kazandi-1031106-teknoloji/. 25.03.2023

Whittaker C., Brian R., Marria N., (2010). Large-Scale Automatic Classification of Phishing Pages, NDSS '10, *Google Research*.

World Economic Forum (WEF), (2022a). The Global Risks Report 2022, 17th Edition. In partnership with Marsh McLennan, SK Group and Zurich Insurance Group.

World Economic Forum, (2019). Insight Report, Regional Risks for Doing Business.

Yayla, M. (2013). Hukuki bir terim olarak siber savaş. *Türkiye Barolar Birliği Dergisi,* 104, s.177-202.

ETİK VE BİLİMSEL İLKELER SORUMLULUK BEYANI

Bu çalışmanın tüm hazırlanma süreçlerinde etik kurallara ve bilimsel atıf gösterme ilkelerine riayet edildiğini yazar(lar) beyan eder. Aksi bir durumun tespiti halinde Tokat Gaziosmanpaşa Üniversitesi Turhal Uygulamalı Bilimler Fakültesi Dergisi'nin hiçbir sorumluluğu olmayıp, tüm sorumluluk makale yazar(lar)ına aittir. Yazar(lar) etik kurul izni gerektiren çalışmalarda, izinle ilgili bilgileri (kurul adı, tarih ve sayı no) yöntem bölümünde ve ayrıca burada belirtmişlerdir.

Kurul adı:

Tarih:

No:

ARAŞTIRMACILARIN MAKALEYE KATKI ORANI BEYANI

1. yazar katkı oranı: %100