BSAD

Bankacılık ve Sigortacılık Araştırmaları Dergisi
Sayı 12, ss.8-22

Siber Sigortalar: Son Gelişmeler, Uygulamalar ve Sorunlar

Eda ALTUNTAŞ

Başkent Üniversitesi

Emine KARA

Başkent Üniversitesi

Abdullah Buğra SOYLU

Başkent Üniversitesi

Erdem KIRKBEŞOĞLU

Başkent Üniversitesi

Öz

Bu çalışmanın amacı Avrupa Birliği'ne uyum sürecini takip eden ve 2007 yılından bugüne bu süreci başarıyla yöneten Türk sigortacılık sisteminin, siber risklere güvence sağlama konusundaki etkinliğini sınamaktır. Bu kapsamda, Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı tarafından 2016 yılında gerçekleştirilen "Siber Sigortalar: Son Gelişmeler, Uygulamalar ve Sorunlar" isimli proje baz alınmıştır. İlgili projede kullanılan yöntem ve soru formu birebir paralel olarak Türkiye'de de araştırma ekibimizce uygulanmıştır. Bu kapsamda Türkiye'de siber riskler konusunda aktif olarak çalışan şirket yöneticileriyle yarı yapılandırılmış görüşme tekniği kullanılarak ve Risk Management Forum 2015: Siber Risklerin Yönetimi adlı forumda konuşmacıların söylem analizi yapılarak siber riskle mücadelenin etkinliğini sınayacak sorular yöneltilmiştir. Görüşmeler neticesinde elde edilen bulgular, Türkiye ve AB sigortacılarının risk algıları ve riski değerlendirme bakış açıları arasında çok büyük farklılıklar olmamasına rağmen Türkiye'deki siber risklerin yaratacağı olası sorunlara ilişkin işletmelerin farkındalığının AB'den farklılık gösterdiğini göstermektedir.

Anahtar Sözcükler

Siber risk, siber sigorta.
JEL Sınıflaması: Z00.

Cyber Insurance: Recent Developments, Applications, and Problems

Abstract

The aim of this study is to examine the effectiveness of the Turkish insurance system following the harmonization process of the European Union and managing this process successfully from 2007 on the issue of securing the cyber risks. This is based on the project titled "Cyber Insurance: Recent Developments, Implementations and Challenges" conducted by the European Union Network and Information Security Agency in 2016. This project used the same methodology and questionnaire was administered by our research team in Turkey. In this context, Turkey cyber risks are actively working company managers with a semi-structured interview technique using and Risk Management about the Forum 2015: Cyber Question Risks Management Analyzing the discourse of speakers

at the forum called to test the effectiveness of cyber risk struggles were directed. At the end of the study, a significant level of risk perception and assessment styles of Turkey and the EU insurers have not shown differences. However, it was observed that low levels of awareness about the negative consequences of cyber risks in Turkey.

Keywords

Cyber risk, cyber insurance.
JEL Classification: Z00.

GİRİŞ

Günümüzde teknoloji, hemen her kesim tarafından yaşantımızın vazgeçilmezi olarak kabul edilmektedir. Teknolojinin önemi sadece insanlar için değil kurum ve kuruluşların tüm faaliyetlerinin ayrılmaz bir parçası olarak görülmektedir. Fayda sağlayan birçok durumun olumlu yanlarının olabileceği gibi kötüye kullanım sonucu birçok zararı da beraberinde getireceği bilinmektedir. Bilgi ve teknoloji hayatımızın en büyük kurtarıcısı gibi görünse de kötü niyetli kişi ve kuruluşların kendi menfaatleri uğruna yaptıkları birçok işin sonucu beklenmeyen zararlar oluşabilir. Dolayısıyla teknolojik sistemlerin kullanımı, gerek kamu kurumları ve işletmeleri gerekse de bireyleri siber risklerle karşı karşıya bırakmaktadır.

Günümüzde dünya çapında yaklaşık 6 milyar akıllı cihaz bulut üzerinden birbirine bağlanmış durumdadır. 2020 yılında ise bu rakamın 20 milyar olması beklenmektedir. Bu kapsamda siber tehditlerin önemi özellikle son yıllarda gündeme gelmiştir.

Bilgi teknolojisi alanında güvenlik ihlalleri giderek artmaya devam etmekte, işletmeler ise artık siber güvenlik riskini, doğal afet riskinden çok daha ciddiye aldıkları bir dönemdedirler. Son zamanlarda sıkça duymaya başladığımız siber risk aslında insanların geleneksel güvenlik anlayışında büyük bir değişimi ortaya çıkarmıştır. Bu değişim insanların güvenle kullandıkları telefondan, kişisel bilgisayarlarına kadar birçok teknolojinin parçası olarak görülen elektronik aletlerin daha dikkatli kullanılması gerektiğine de dikkat çekmiştir. Ancak ne kadar dikkat edilse de birçok kurumun siber risk yüzünden piyasada çok sayıda büyük risklerle karşı karşıya kaldıkları göz ardı edilmemelidir.

Günümüzde güvence kavramının en güzel karşılığı sigortadır. Sigortanın temeli güven esasına dayalıdır. Her geçen gün daha fazla şirket, verilerini ve markalarını tehdit eden riskleri minimuma indirmek için sigorta güvencesi arama yoluna gitmektedirler. Gelişmiş ülkelerde siber güvenlik ihlallerine karşı, sigortası olanların oranı %31'i geçmemektedir (Ekonomist Dergisi, 10.10.2016). Bu oran gelişmiş ülkeler için bir başarı göstergesi olarak tanımlanmasa da son yıllardaki artış göz önüne alındığında küçümsenemeyecek bir pazar payını temsil ettiği de söylenebilir. Ancak gelişmekte olan piyasalar için benzer bir seyrin olmadığı görülmektedir. Sigortacılığın büyük sayılar kanunu çerçevesinde etkin bir şekilde yürütülebildiği göz önüne alındığında özellikle siber risk sigortaları gibi uygulama sayısının az olduğu ülkelerde sigorta şirketlerinin etkin bir güvence sağlamasını beklemek imkânsızdır. Zira sigorta edilebilir bir riskten bahsedebilmek için sigorta şirketinin geçmiş yıllarda o risk grubunda yeterli veriye sahip olması gerekmektedir. Gerek prim gerekse de beklenen hasar tazminatlarının gerçekçi bir şekilde tahmin edilmesinin temelinde bu yatmaktadır.

Bu noktada temel sorun Türkiye gibi gelişen sigorta piyasaları için siber risklere karşı güvence sağlamadaki tecrübe eksikliğidir. Dolayısıyla bu çalışmanın amacı Avrupa Birliği'ne uyum sürecini takip eden ve 2007 yılından bugüne bu süreci başarıyla yöneten Türk sigortacılık sisteminin, siber risklere güvence sağlama konusundaki etkinliğini sınamaktır. Daha açık bir ifadeyle, Avrupa Birliğine uyum politikasıyla hareket eden devlet politikası, siber riskler gibi spesifik tehditlere karşı ne derece teminat sağlamada etkin çalıştığı sorgulanacaktır. Bu soruya cevap bulabilmek adına Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı tarafından 2016 yılında gerçekleştirilen "Siber Sigortalar: Son Gelişmeler, Uygulamalar ve Sorunlar" isimli proje baz alınmıştır. İlgili projede kullanılan yöntem ve soru formu birebir Türkiye'de araştırma ekibimizce

uygulanmıştır. Bu kapsamda Türkiye'de siber riskler konusunda aktif olarak çalışan şirket yöneticileriyle yarı yapılandırılmış görüşme tekniği kullanılarak ve Risk Management Forum 2015: Siber Risklerin Yönetimi adlı forumda konuşmacıların söylem analizi yapılarak siber riskle mücadelenin etkinliğini sınayacak sorular yöneltilmiştir. Görüşmeler neticesinde elde edilen bulgular, AB raporundakilerle karşılaştırılarak, Türk sigortacılık sisteminin etkinliği ve farklılığı çalışma sonunda ortaya konulmuştur.

1. SİBER RİSKLER VE SİGORTA GEREKSİNİMİ

Gerek bilginin hızlı bir şekilde yayılımı gerekse teknolojinin gelişimi risklerin çeşitliliğini artırmaktadır. Yıllara göre risklerin çeşitlendiğini gözlemlediğimizde farklı risk gruplarıyla karşılaşmak mümkündür. 2017 yılının ön planda olan risklerini sıralayacak olursak terör, siber saldırılar, doğal afetler, göç, bölgesel çatışmalar ve iklim değişikliği gibi risk unsurlarının yer aldığı görülmektedir. Bu risklerden bir tanesi olan siber saldırılar göz ardı edilemeyecek kadar çok tehlikenin başlangıcını oluşturmaktadır. Siber saldırı sonucu olası riskler bu tehditlerin en önemlileri olarak kabul edilmektedir. Devlet kamu kurum ve kuruluşlarının yanı sıra KOBİ'lerden çok uluslu şirketlere kadar tüm ticari kuruluşlar finansal kayıplarla sonuçlanabilecek siber risklerin tehdidi altında bulunmaktadır. Türkiye en çok siber saldırıya uğrayan ülkeler arasında 9'uncu ırada yer alırken, dünyada yılda 556 milyon siber saldırı gerçekleşmektedir (Milliyet gazetesi, 2016). Siber saldırıların her yıl %50 oranında arttığı ifade edilmektedir. Ayrıca siber suçların global ekonomiye maliyeti yıllık 445 milyar USD'dir (Habertürk, 2016). Türkiye'de yılda 10 milyondan fazla kişinin mağdur olduğu ve bunun toplam net maliyetinin 556 milyon USD olduğu tahmin edilmektedir (Sigorta gündem, 2016).

Siber saldırılar bugün o noktaya gelmiştir ki gerek kamu kuruluşlarının gerekse özel şirketlerin en büyük kâbusu olmuştur. Yapılan araştırmalara göre, ülkemizde 2017'nin ilk üç ayında gerçekleşen siber saldırı sayısı, geçen yılın ilk üç ayına göre %50 artmış durumdadır (Sigorta.com.tr, 01.09.2017). Ülkemizde günde ortalama 75 bin siber saldırı gerçekleşmektedir ve bu sayı artan oranda yükselmektedir. Siber atak sayısında Türkiye, dünyada 5'inci, Avrupa'da 4'üncü sıradadır (Hürriyet Gazetesi, 21.05.2017). Yapılan siber saldırıların çeşitlerine bakıldığında ise, veri sızdırma teşebbüsleri %40, Truva atı saldırıları ise %30 civarındadır. En fazla siber saldırıların nereye yapıldığına bakıldığında da üniversiteler ve Millî Eğitim Bakanlığı başı çekmektedir (Sigorta.com.tr, 01.09.2017). Bu ciddi rakamlar aslında siber risklerin önemini daha da dikkate değer hale getirmektedir.

Bu tür riskin gerçekleşmesi durumunda kişiler ve kuruluşlar farklı yöntemlerle zarar görebilmektedirler. Kişisel olarak yapılan saldırılarda kişisel bilgilerin ele geçirilmesi birçok sorunu beraberinde getirmektedir. Kurumlar açısından baktığımızda bir bankaya yapılan siber saldırıda birçok müşteri hesabının etkilenmesi muhtemeldir. Kurumlara yapılan siber saldırı sonucu yaşanılan maddi kaybın yanında kurum itibarının zedelenmesi ve güvensizlik durumunun oluşması gerçekleşen riskin etkilerini arttırmaktadır. Zira işletmelerin temel amacı yalnızca mal veya hizmet sunmak değil, aynı zamanda güven ortamı içinde müşteri portföyü oluşturmaktır. Bu güvenin sarsılması, uzun vadede işletmenin hayatta kalmasını etkileyecek bir durum yaratabilir.

Siber risk için birçok saldırı türü bulunmaktadır. Türkiye'de en çok karşılaşılan beş siber saldırı çeşidi şunlardır: Fidye yazılımları, Olta saldırıları, Kredi kartı dolandırıcılıkları, DOS/DDOS saldırıları, Mobil tehditler (Trend Micro, 2014).

Fidye yazılımları iki tür olarak karşımıza çıkar: şifreleyiciler ve kilitleyicilerdir. Şifreleyiciler bilgisayarlara ulaştıkları zaman bilgisayarda bulunan her türlü veriyi şifre ile korumaya alırlar. Bu koruma ile kişiler kendi bilgisayarlarındaki dosyaları açamaz ve dosya içinde bulunan verilere ulaşamazlar. Kilitleyiciler ise cihazı kilit altına alırlar. Bu kilit sadece verilere ulaşmayı değil tüm erişimi engeller. Böylelikle sisteme giriş erişilmez olur ve son olarak fidye talebinde bulunurlar.

Olta saldırıları ise zaman zaman bankalardan ve birçok finansal kuruluşlardan gelmiş gibi görünen sahte e-postalar olarak örneklendirilebilir. Bireyler gelen bu e-postaları acil ve çok önemli hissi yaratan başlıklar halinde görünmesinden dolayı dikkate almaktadır. Böylelikle SMS yoluyla gizli olması gereken bilgiler, kişilerin kart numaraları ve şifrelerinin ele geçirilmesi mümkün olabilmektedir.

Kredi kartı dolandırıcılıklarında ise siber suçluların kullanıcılara, özellikle herkesin ilgi gösterdiği ürünler için çeşitli kampanya, fırsat ve indirimler içeren sahte sipariş sayfalarını kapsayan e-postalar yolladıkları görülmektedir. Bu e-postalar özellikle sevgililer günü, anneler günü, babalar günü ve yıl başı gibi birçok kişinin birbirine özellikle online alışveriş yaparak hediye aldığı dönemlerde yoğunlaşmaktadır. Bu e-postalardaki bağlantılara tıklayıp sahte sipariş sayfalarından alışverişini yapan kişilerin kredi kartı bilgileri bilgisayar korsanları tarafından çalınabilmektedir (Trend Micro, 2016).

DOS/DDOS saldırıları adı verilen saldırı türü sistemin çalışmasını engellemek ve bu sistemin hizmet verememesi için yapılan saldırı türüdür. Bu saldırı türü 2016 yılının siber saldırı olaylarında en çok gündemde yerini almıştır.

Son olarak mobil tehditler adından anlaşılacağı üzere mobil cihazlara gelecek siber saldırı türüdür. Sayıları ve teknolojileri her gün gelişim gösteren mobil cihazların ürettikleri veri miktarı küçümsenemeyecek düzeydedir. En temel mobil tehditler; SMS gönderme, bilgi çalma ve reklam gösterimidir. Mobil cihazlar bilgisayar kullanımına göre daha korunmasız durumdadır. Bunun nedeni ise mobil cihazlarda anti virüs korumalarının bilgisayara oranla çok daha az olmasıdır.

Elbette her tehdit gibi siber riskler için de alınabilecek önlemler vardır. Özellikle kurumlar açısından baktığımız zaman siber güvenlik açısından üç temel yetkinlik bulunmaktadır. Birinci yetkinlik; bir kurumun güvenli bir siber altyapıya sahip olmasıdır. NART Sigorta ve Reasürans Brokerliği A.Ş. tarafından düzenlenen "2015 Risk Management Forum" konuşmacılarından Deloitte Türkiye Siber Güvenlik Hizmetleri Lideri Ali Yılmaz Kumcu'ya göre, siber güvenlik sistemleri günümüzde kurumların kaleleri gibidir. Orta Çağ döneminde insanoğlunun kendini korumak için kaleler inşa etmesi, hendek kazması gibi güvenlik amacıyla alınan önlemler, günümüzde yerini güvenli bir siber altyapıya bırakmaktadır. Bu kapsamda ilk olarak bilgi güvenliğinin bilgi işlemden ayrı olması gerekmektedir. Yine Kumcu'ya göre siber güvenlikte bir sonraki adım, özellikle son yıllarda daha çok gündeme gelen farkındalık olarak ön plana çıkmaktadır. Kurumların gelişen ve değişen siber tehditlere hazırlıklı olmaları için tehditlerin farkında olmaları gerekmektedir. Bu kapsamda kendi siber güvenlik sistemlerini güncelleyebilmeleri ve bu konuda dinamik davranış sergileyebilmeleri gerekmektedir. Ayrıca bilgi güvenliğinin sorumluluğu şirketlerde sadece bilgi güvenlik çalışanlarının değil her çalışanın sorumluluğu olacak şekilde farkındalık kazanılması gerekmektedir. Ancak bu iki yetkinlik her zaman yeterli olmamaktadır. Kurumların, siber saldırıya maruz kaldıklarında müdahale edebilecek hem operasyonel teknik hem de yönetimsel kabiliyete ihtiyaçları vardır. Kriz esnasında ve kriz sonrasında gerçekleşebilecek riskler açısından kurumların risk yönetimi anlamında destek almaları da onların yararına olacaktır (NART, 2015: 34-38).

Siber saldırı sonucunda meydana gelebilecek olaylar data kayıpları, veri silinmesi manipülasyonu, iş durması, üretimin durması, şantaj, çalınmış bilgilerin ifşasıyla ilgili tehditler ve itibar kaybı olarak sıralanabilir. İtibar kaybı burada rizikoların en büyüğü olarak değerlendirilmektedir. Ancak siber saldırıya uğramış şirketlerin, saldırının etkilerini azaltmak amacıyla karşılaştıkları masraflara bakıldığında; kriz yönetimi maliyeti toplam masrafların %48'ini, avukatlık masrafları %15'ini, kredi kartlarıyla ilgili maliyetler %11'ini, kanuni maliyetler %10'unu, uzlaşma masrafları %10'unu, ceza maliyetleri ise %6'sını oluşturmaktadır (NART, 2015: 43-46).

Kurumların ve şahısların siber tehditlerin sonuçlarından korunma yöntemlerinden biri sigortadır. Yukarıda bahsedildiği gibi pek çok kurum günümüzde siber saldırıya uğrayabilmekte

veya hali hazırda siber saldırıya uğramış durumdadır. Bu kapsamda siber sigorta, diğer adı ile veri güvenliği sigortasının önemi ön plana çıkmaktadır.

2. SİBER RİSK SİGORTASI

İnsanlar doğumlarından ölümlerine kadar çok sayıda ve değişik türlerde risk ile karşı karşıyadır. Bu riskler yalnız gerçek kişiler için değil tüzel kişiler ve organizasyonlar için de söz konusudur. Risklerin sonuçlarından korunmak için sigorta güvencesinden yararlanılır. Sigorta şirketlerinin gündeminde yer alan siber risk sigortası, kurumları ve sigortalıyı siber saldırılardan oluşan kayıplara karşı korumayı hedeflemiştir. Bu koruma yönteminin geliştirilmesi ve piyasanın daha iyi anlaşılması siber risk sigortasındaki bazı soru işaretlerinin ortadan kalkmasını sağlayacaktır. Bu ürünü sunan birçok sigorta şirketi, ürünün piyasada yaygınlaştırılmasında sorunlar yaşamaktadır. Bunun en önemli nedeni, poliçenin hangi amaca yönelik olduğuna dair yeterli farkındalığın ve bilgi birikiminin henüz sağlanamamış olmasıdır. Siber risk sigortası için Mesleki Sorumluluk Genel Şartları geçerlidir.

Şirketler bu verilerin ne derecede değerli olduğu ve nasıl korunması gerektiği hakkında; dahası bu verilerin kaybolması ya da çalınması gibi durumlarda oluşabilecek tazminat talepleri hakkında yeterli bilgi ve tecrübeye sahip olmadıkları gözlemlenmiştir. Şirketlerin bu konuda yetersiz bilgiye sahip olması ve sigorta yaptıracak kişiyi yönlendirememesi sebebiyle muhtemel sigorta müşterileri, ihtiyaçlarına yönelik bir sigorta ürününün varlığından haberdar değildir. Bu sorun aslında siber risk sigortanın gelişmemesindeki en büyük etkendir.

Siber risk sigortasının gelişim sıralamasına bakacak olursak siber risk sigortası ürünü ilk olarak 1990'lı yılların sonunda Amerika Birleşik Devletleri'nde ortaya çıkmış ve 2000'li yılların başında da Avrupa'da siber risk sigorta teminatları sağlanmaya başlanmıştır. Türkiye'de ise ilk kez 2010 yılında siber risk sigortalarının bir ihtiyaç olduğu kanaati ortaya çıkmıştır. Türkiye bu sigorta talebi karşısında ilk zamanlarda teminatı yurtdışı piyasalardan sağlarken, 2012 yılı sonrası bazı küresel firmaların Türkiye ofisleri bu teminatı sunmaya başlamıştır. Böylelikle Türkiye'deki sigorta şirketleri 2012 yılından itibaren, yurt içinde teminat sunmaya başlamıştır. Türkiye'de siber risk kavramı, yalnızca "veri kaybı" olayları ile sınırlı olduğunu düşünülürken, zamanla gerçekleşen zararlar neticesinde siber risklerin ve sigorta teminatlarının çok daha kapsamlı olması gerektiği anlaşılmıştır. Saldırıların artması ve farkındalığın yükselmesi ile birçok şirket bu konu doğrultusunda çalışmalarını hızlandırmıştır. Bu çalışmaların ilk adımı olarak şartname ve teminatlarda genişletmeler yapmışlardır.

2013 yılında Kıta Avrupası'nda teminat sağlayan 8 pazar varken, bu rakam 2017 yılında 25 pazara yükselmiştir. Küresel ölçekte 50 civarı pazarın siber sigorta teminatı sağladığını söylemek mümkündür. Son 4 yılda Kıta Avrupası'ndaki seyre bakılırsa, önümüzdeki yıllarda bu sayının artacağını söylenebilir (Kayganacı, 2017).

Siber risk sigortasını diğer sigortardan ayıran en önemli özellik verinin silinmesi kaybolması ya da çalınması değildir. Çünkü siber risk sigortasında zarar görecek veri sigortalanmaz. Siber risk sigortasında verinin maddi bir değeri yoktur. Sigortalanan verinin kaybolmasından kaynaklı 3'üncü şahısların talebi sigortalanır. Siber risk sigortasını diğer sigortalardan farklı kılan bir diğer özellik ise, gerçekleşen riskin etki olarak kestirilebilmesinin güçlüğüdür. Çünkü zarar oluştuğunda bu zararı ölçmek çok zordur. Bütün bu karmaşık ve zor belirlemelerden dolayı sigortacıların bu alandaki ürünlerini kolay bir şekilde yaygınlaştırmaları ve uygun fiyatlı poliçelerini müşterilerine sunmaları hiç de kolay değildir. Siber risk sigortasında belirlenmiş paket bir poliçe yoktur. Bu yüzden her sigortalının talep ve ihtiyaçlarına göre ek teminat içeren poliçeler düzenlenmektedir. Siber risk sorumluluk poliçeleri, elektronik veri ve internet kullanımıyla ilişkili birçok riski kapsamaktadır.

2.1. Birinci Şahıs Riskleri

Birinci şahıs riskleri, sigortalıyı doğrudan etkileyen faktörlerdir. Yani firmanın kendini koruduğu kayıplar için geçerlidir. Birinci taraf kapsamı poliçe sahibinin kendi verilerine, gelir kaybına, bir veri ihlali veya siber saldırı sonucu poliçe sahibinin işine zarar verilmesi riskini güvence altına alır. Bir örnek verecek olursak, bir işletmenin elektronik veri dosyalarına bir bilgisayar korsanının neden olduğu hasardır. Birinci tarafa ilişkin risk türleri şu şekilde sıralanabilir (ENISA, 2016).

- Hırsızlık ve dolandırıcılık; işletmeye ait bilgi ve verilerin çalınması sonucunda işletmenin uğrayacağı maddi ve itibari kayıplardır. Bu gibi durumların yaşanması şirketin marka ve piyasa değeri üzerinde olumsuz bir etki yaratmaktadır.
- Adli soruşturma; riskin gerçekleşmesi neticesinde saldırının etkisini analiz etmek ve saldırıyı durdurmak için gerekli yasal, teknik ve adli hizmetlere ilişkin maddi kayıplardır.
- İş kesintisi; bir poliçe sahibinin siber risk olayıyla veya veri kaybı sebebiyle iş yapamaması durumunda ortaya çıkan gelir kaybını ve ilgili maliyetlerini içerir.
- Bilgisayar veri kaybı ve restorasyonu; veri, donanım, yazılım veya bir siber saldırının neden olduğu tahrip sonucunda varlıkların fiziksel olarak zarar görmesini ve kullanılamamasını kapsar. Hasar gören diğer bilgileri kurtarma masrafları da dâhil olmak üzere, bilgisayarla ilgili varlıkların olumsuz sonuçlarını da içerir.

2.2. Üçüncü Şahıs Riskleri

Üçüncü şahıs riskleri kapsamı, poliçe sahibinin bir veri ihlalinden veya siber saldırıdan kaynaklı üçüncü şahıslara (müşteriler ve devlet kurumları da dâhil olmak üzere) karşı yükümlülüğünü güvence altına alır. Yani üçüncü şahıs teminatları, sigortalı firmaya karşı üçüncü şahısların bir takım zarar taleplerini ifade etmektedir. Örneğin, bir müşteri çalıştığı şirketin bilgisayar sisteminden, kişisel bilgilerinin çalınıp çevrimiçi yayınlandıktan sonra kişisel verilerini koruyamamaktan dolayı bu şirketi dava edebilir. Kapsam, genel olarak elektronik verilerin oluşturulması, gönderilmesi, alınması veya depolanmasında işlediği iddia edilen hatalar ya da ihmallerin bir sonucu olarak firmaya karşı talep edilen zararlardan oluşmaktadır. Poliçeler, genellikle firmayı tazminat taleplerine karşı savunmanın maliyetini karşılar. Bu maliyetler sigorta limitini azaltabilir. Üçüncü taraf risk kapsam türleri şu şekilde sıralanabilir (ENISA, 2016; Mcguirewoods, 2013).

- Dava tazminatları; siber bir saldırıdan kaynaklanan sivil dava, yargı veya ceza ile ilgili maliyetlerini kapsar.
- Bildirim maliyetleri; bir siber risk olayından etkilenen mağdurların, kanunların gerektirdiği bir bildirimle alakalı masraflarını karşılar.
- Kriz yönetimi; siber riske maruz kalmış bir sigortalının, piyasadaki itibarını korumak adına müşterilerine ne tür bir çağrıda bulunması ve bu süreçte ne tür bir kriz yönetimi politikası sergilemesi için katlandığı kriz yönetimi ve halkla ilişkiler masraflarını kapsar.
- Kredi izleme; bir siber risk olayından etkilenen şirketin müşteri veya çalışanlarına, bir daha bu tip bir dolandırıcılıkla karşılaşmaması için neler yapması gerektiğini eğitme konusundaki masraflardır.
- Medya sorumluluğu; telif hakkı, ticari marka veya hizmet markası ihlalinin sigortalı tarafından çevrimiçi yayınlanmasından kaynaklanan medya sorumluluğunu kapsar.

- Gizlilik yükümlülüğü; gizli tutulması gereken bilgilerin çalışan veya müşterilerin gizlilik ihlali nedeniyle sorumluluk kapsamını içerir.

2.3. Teminat Dışı Haller

- Rekabet; rekabet ve ticaretin engellenmesi, haksız rekabete ilişkin yasaların ihlali teminat dışı haller kapsamındadır.
- Bedensel yaralanma ve maddi varlıkların hasarı; fiziksel yaralanma, hastalık, ölüm ve/veya veriler dışındaki maddi varlıkların kaybı gibi durumlar teminat dışı hal olarak nitelendirilmiştir.
- Sözleşme sorumluluğu; sigortalının bir sözleşme sonucunda sorumlu olduğu herhangi bir garanti, teminat veya sorumluluk istisnadır.
- Siber terörizm; bilgisayarlar aracılığıyla işlenmiş, kamunun kullanmakta olduğu iletişim, ulaşım, enerji tedariki, güvenlik sistemlerinin şiddete, ölüme, imhaya yol açacak şekilde bozulması gibi durumlarda hükümet politikalarını değiştirmeye zorlayan karışıklık ve terör gibi durumlar istisnai hallere dahil edilmiştir.
- İşverenin yükümlülükleri; çalışan emeklilik planları, çalışan istihdam planları, çalışan kâr paylaşım, sosyal güvenlik hakları, işyerinde sağlığı ve güvenliği koruyan sorumluluklar vb. gibi işverenin sorumlu olduğu durumlar istisnai haller dahilindedir.
- İcra bildirimi; icra bildiriminde tanınan süreye riayet edilmemesi gibi durumlar istisnai durumlar dahilinde değerlendirilmiştir.
- Altyapı veya güvenlik arızası; mekanizma arızası, voltaj dalgalanmaları, elektrik kesintileri, uydu sistem arızaları, bilgisayar sistemi güvenliğinin sağlanamaması teminat dışıdır.
- Fikri mülkiyet; patentler ve ticari sırlar gibi fikri mülkiyet dahilinde bulunan hakların ihlalinden ileri gelen hususlar teminat dışı hallerdir.
- Kasıtlı eylem; sigortalı aleyhine talepte bulunulmasına yol açacak kasıtlı, planlı eylemler istisna edilmiştir.
- Suç teşkil eden eylemler; mahkeme kararına ya da sigortalı itirafına dayanılarak suç ve dolandırıcılık teşkil eden eylemlerden kaynaklanan durumlar istisna edilmiştir.
- Önceki talepler ve olaylar; poliçe başlangıç tarihinden önce yapılmış talepler veya poliçe başlangıç tarihinden itibaren bir talebe neden olabileceği bilinen durumlar istisna edilmiştir.
- Menkul kıymet talebi; menkul kıymetlerin mülkiyeti, alımı, satımı ile bağlantılı bir yasanın ihlalinden kaynaklı haller istisna edilmiştir.
- Terörizm/savaş; herhangi bir savaş, kargaşalık ve terörizmden kaynaklı haller istisna edilmiştir.
- Ticari zarar; elektronik fon transferi veya işlemin parasal değerinin hesaplanmasında, hesaplar arasındaki transfer sırasında vb. gibi durumlarda sigortalının uğrayacağı ticari kayıplar istisna edilmiştir.
- Veri güvenliği sorumluğu; yöneticilerin veya sorumlu kişilerin şirket verilerinin sızdırılmasında kötü niyetli ve kasıtlı hareketlerinin bulunması durumlarında ortaya çıkan zararlar teminat dışı hal kapsamındadır.

3. UYGULAMA VE YÖNTEM

Çalışmanın amacı, Avrupa Birliği'ne uyum sürecini takip eden ve 2007 yılından bugüne bu süreci başarıyla yöneten Türk sigortacılık sisteminin, siber risklere güvence sağlama konusundaki etkinliğini sınamaktır. Bu soruya cevap bulabilmek adına Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı tarafından 2016 yılında gerçekleştirilen "Siber Sigortalar: Son Gelişmeler, Uygulamalar ve Sorunlar" isimli proje baz alınmıştır. İlgili projede kullanılan yöntem ve soru formu birebir Türkiye'de araştırma ekibimizce uygulanmıştır. Bu kapsamda Türkiye'de siber riskler konusunda aktif çalışan şirket yöneticileriyle yarı yapılandırılmış görüşme tekniği kullanılarak siber riskle mücadelenin etkinliğini sınayacak sorular yöneltilmiştir. 2015 yılında İstanbul'da düzenlenen Risk Management Forum 2015: Siber Risklerin Yönetimi adlı forumda konuşmacılara söylem analizi yapılarak aynı sorulara cevaplar aranmıştır.

3.1. Türkiye Uygulaması

Çalışmanın Türkiye ayağında niteliksel araştırma yöntemlerinden iki farklı veri toplama tekniği seçilmiştir. İlk yöntem olan yarı yapılandırılmış görüşme tekniği ile önceden hazırlanmış sorulara sadık kalarak görüşmecilerle derinlemesine mülakatlar gerçekleştirilmiştir.

Çalışmanın amacına ulaşmak adına üç şirket seçilmiş ve çalışmanın analiz ve bulgular kısmında raporlanmış konu başlılarına uygun sorular sorulmuştur. Bu şirketlerin her birinin sermaye yapısı birbirlerine göre farklıdır. Sermaye yapılarına göre görüşmeler; sigorta şirketi, brokerlik ve acente olarak sınıflandırılmıştır. Öncelikle siber risk sigortasının Türkiye'deki yeri ve öneminin tespiti hedeflenmiştir. Bu nedenle yalnızca siber risk sigortası teminatı sunmuş veya buna aracılık etmiş kişiler seçilmiştir. Dolayısıyla görüşmenin gerçekleştirildiği kişiler Türkiye'de siber risk sigortası konusunda gelişkin bilgiye sahip sınırlı sayıdaki kişilerdir.

Görüşmeciler:

- Elementer Sigorta Şirketi: İsminin beyanını istemeyen bu sigorta şirketi, siber saldırı sonucu oluşabilecek kayıpları 2012 yılından itibaren Veri Koruma Sigortası ile Türkiye'de teminat altına almaya başlamıştır. Bu veri koruma sigortası işletmelerin siber risk sonucunda yaşanılan kaybı teminat altına alarak işletmelerin herhangi bir sarsıntı etkisinde kalmadan rutin işlerine kaldıkları yerden devam edebilmelerini sağlıyor. Bu anlamda şirket, siber risk sigortası alanında atılım yapan ilk şirketler arasında bulunuyor. Bu şirket alanına göre özel şartlar sunması ve siber risk konusunda uzman hasar süreci yönetimi ile bu konuda farkındalığını ortaya koymaktadır.
- Marsh Brokerlik: Türkiye'de siber risk sigortası konusunda atılım yapan ilk şirketler arasında yer alıyor. Aynı zamanda dünyanın lider sigorta brokerliği ve risk yönetim şirketidir. Marsh sigorta brokerliğinin, siber risk sigortası alanında pazar payının oldukça büyük olduğu bilinmektedir. Aynı zamanda Marsh, sigortalıların siber ataklar ile karşı karşıya kalması durumunda ne yapmaları gerektiği hakkında eğitim ve danışmanlık hizmeti de vermektedir.
- ERN Sigorta Aracılık Hizmetleri: İlgili sigorta acentesi uzun yıllardır Ankara'da faaliyet gösteriyor, ürün portföyü anlamında yangın, mühendislik ve sorumluluk sigortalarının çeşitli türleri konusunda tecrübeye sahiptir. Şirket aynı zamanda siber risklere yönelik birkaç sigorta poliçesinin hazırlanmasına aracılık etmiş ve risk danışmanlığı desteği sunmuştur.
- Çalışmanın veri toplama ayağının ikinci kısmında söylem analizi tekniği kullanılmıştır. 2015 yılında İstanbul'da gerçekleştirilen "Siber Risklerin Yönetimi" temalı Nart Risk Yönetimi forumuna katılan araştırma ekibi, dünyada ve Türkiye'de siber riskler konusunda yüksek bilgi ve tecrübeye sahip panelistlerin söylemlerini analiz etmiştir. Panelistler:

- Levent Nart: Nart Sigorta ve Reasürans Brokerliği A.Ş. yönetim kurulu başkanı ve genel müdürü olarak görevine devam etmektedir. Risk Management Forum 2015'te siber risklerle ilgili açılış konuşmasında verilerin güvenliğinden bahsetmiştir. Birinci oturumda ise dijital ve global bir risk olan "siber risk"in işletmeler tarafından nasıl algılandığından, yapılması gerekenlerden ve siber sigortalardan bahsetmiştir.
- Steven Young: Alman-Türk Ticaret ve Sanayi Odası başkan yardımcısı olarak görevine devam etmektedir. Forum'un açılış konuşmasında, siber risklerin gelecek yıllarda öneminin artacağından ve güvenlik önlemleri alınması gerektiğinden bahsetmiştir.
- Faruk Eczacıbaşı: Türkiye Bilişim Vakfı yürütme kurulu başkanı olarak Risk Management Forum 2015'te oturum başkanlığı yapmıştır. Konuşmasında, dünya ve Türkiye'deki siber tehditlerin etkilerini incelemiştir.
- Halil Öztürkci: Adeo Bilişim Danışmanlık A.Ş.'nde white hat hacker olarak çalışmaktadır. Forum'daki konuşmasında, devletleri, şirketleri ve bireyleri bekleyen siber saldırıları örneklerle açıklamıştır. Uygulamada bu risklerin yönetimiyle ilgili yapılan çalışmaları aktarmıştır.
- Murat Lostar: Lostar Bilgi Güvenliği A.Ş.'nde genel müdür olarak çalışmaya devam etmektedir. Forum'da yaptığı konuşmada, en kötü güvenlik krizlerinin aslında insan hatası ve bilinçsizlik olduğunu vurgulamıştır. Farkındalığı yükseltmek ve eğitim düzeyini arttırmak için yapılması gerekenlerden bahsetmiştir.
- İlhami Koç: Türkiye Sermaye Piyasaları Birliği başkanı olarak Forum'da yaptığı konuşmasında siber risklerin finans sektöründeki yerini, önemini ve siber güvenlik uygulamalarını aktarmıştır.
- Av. Gönenç Gürkaynak: ELİG Ortak Avukat Bürosunda yönetici olarak çalışmaya devam etmektedir. Forum'da siber suçlara karşı internet hukukunun nasıl şekillendiğinden bahsetmiştir. Siber suçla karşılaşıldığı esnada kişi ve kurumların yükümlülüklerini açıklamıştır.
- Burak Sadıç: PwC Türkiye'de bilgi güvenliği ve siber güvenlik hizmetleri lideri olarak çalışmaktadır. Yönetim kurulları, şirket yöneticileri ve üst düzey yöneticilerin bakış açısından siber riski anlatarak, oluşturulması gereken farkındalığın önemini bir kez daha vurgulamıştır. Bununla birlikte, kendi müşterilerine yapılan saldırıların yıllar bazından arttığını rakamlarla açıklamıştır.
- Daniel Shepherd: S21sec Cybersecurity şirketinde yönetici olarak çalışmaktadır. İspanyol bir şirket olan S21sec şirketi, siber güvenlik alanında uzmanlaşmış ve şirketlere bu konuda risk yönetimi hizmeti sunan bir firmadır. Daniel Sepherd, Forum'da yaptığı konuşmada, tecrübelerini aktararak şirketlerin siber saldırı sonucunda mali açıdan büyük zarar gördüklerini belirtmiştir. Siber sigortanın öneminin ve kurumlar için gerekliliğinin altını çizmiştir.
- Karolina Vogelpohl: Allianz Global Corporate&Specialty şirketinde Kuzey, Orta ve Doğu Avrupa finansal riskler bölge başkanı olarak görev yapmaktadır. Forum'daki konuşmasında hangi risklerin hangi yollarla teminat altına alınabileceğini aktarmıştır.

3.2. Avrupa Birliği Uygulaması

Çalışmada referans alınan kaynak, Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı (ENISA) tarafından hazırlanan ve 2016 yılında tamamlanan "Siber Sigortalar: Güncel Gelişmeler, İyi Uygulamalar ve Sorunlar" isimli projedir. Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı (ENISA), AB, üye ülkeleri, özel sektör ve Avrupa vatandaşları için bir ağ ve bilgi güvenliği uzmanlığı merkezidir. ENISA, bilgi güvenliği konusunda başarılı uygulamalar için tavsiyelerde bulunmak

için çok sayıda paydaş gruplarla birlikte çalışmaktadır. AB üyesi ülkelere, ilgili Avrupa Birliği mevzuatının uygulanmasında yardımcı olmakta ve Avrupa'nın kritik bilgi altyapısının ve ağlarının dayanıklılığını geliştirmeye çalışmaktadır. ENISA, AB çapında ağ ve bilgi güvenliğini geliştirmeyi taahhüt eden sınır ötesi toplulukların geliştirilmesine destek vererek AB üye ülkelerindeki mevcut uzmanlığı geliştirmeye çalışmaktadır.

ENISA'nın raporu iki kısımdan oluşmaktadır. İlk kısımda siber risklerin sigortacılar tarafından yönetilmesi sürecinde başarılı uygulamalar tespit edilmeye çalışılırken ikinci kısımda yine aynı süreçteki zorluklar tespit edilmeye çalışılmıştır. Bu amaçla ajans, siber sigortalar konusunda faaliyet gösteren sigorta şirketlerinin yetkin temsilcileriyle yarı yapılandırılmış görüşme tekniği kullanarak görüşmeler gerçekleştirmiştir.

Avrupa Birliği uygulamasındaki toplam görüşmeci sayısı 37'dir. 28 sigortacı Birleşik Krallık'tan, 2 sigortacı Almanya'dan, 2 sigortacı Yunanistan'dan ve birer sigortacı da Finlandiya, Fransa, İtalya, İspanya ve Hollanda'dan seçilmiştir.

4. ANALİZ VE BULGULAR

4.1. İyi Uygulamalar

Yöneticilerin yalnızca bugünü değil geleceğe ilişkin örgütleriyle ilgili plan ve politikalar üretmeyi, hedefler belirlemeyi ve bu hedeflere ulaşmada stratejiler geliştirmeyi zorunlu kılmaktadır. Zira belirlenen hedeflere ulaşmak için birçok riskle baş edilmesi gerekecektir. Bu nedenle yöneticiler, mevcut faaliyet alanlarındaki risk seviyesini çok iyi çözümlemek zorundadır. Önemli risklerin, belirlenerek önceliklendirilmesi ve en zayıf kritik kontrollerin tanımlanması kurumlar için önemlidir. Dolayısıyla hedeflere ulaşma yolunda risklerin yönetilmesi gerekliliği, son yıllarda yöneticilerin temel görevleri arasında gösterilmektedir (Kırkbeşoğlu ve McNeill, 2015: 210).

Sigorta sözleşmesinin hazırlanmasından önceki süreç sigorta şirketi için çok önemlidir. Bu süreçte sigorta şirketi, teklifi yapan müşterisinin riskini analiz edip değerlendirmesi gerekir. Bu aşamada ilk olarak müşterisinin teklif formu veya beyan formu adı verilen formu doldurmasını ister. Bu formun amacı, olası risklerin müşteri tarafından iyi niyetli bir şekilde beyan edilmesidir. Sigortacı, sigorta konusuna ilişkin çeşitli sorular sorduğu bu formdan bir risk primi hesaplayacaktır. Zira sigortacılıkta risk ne kadar yüksekse müşteriden istenecek prim o kadar ağırlaşacaktır. Sigortacı sadece teklif formuyla yetinmek zorunda değildir. İsterse sigorta konusunu yerinde ziyaret edebilir. Sigortacının hatalı bir risk seçimi yapmaması için bu süreç oldukça önemli olsa da yine de hatalı risk seçimi ortaya çıkabilir. Hatalı risk seçimi, sigortacının ortalama hasar olasılığından yüksek olasılıktaki bir riski, dikkatsiz bir risk değerlendirme (underwriting) sürecinden sonra ortalama bir fiyatla sigorta kapsamına alması anlamına gelir (Rejda, 2005). Siber risk sigortası hizmeti sunan sigorta şirketleri için bu süreç çok daha hassastır. Her bir müşteriye ait risklerin farklı olarak değerlendirilmesi nedeniyle bu süreçte riskler sürekli değişim göstermektedir. Son zamanlarda Avrupa'da, çeşitli sigorta şirketleri, ortak uygulamaları geliştirmek ve pazarda daha yüksek bir tutarlılık kurmak için çaba sarf etmektedirler.

Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı'nın siber risk araştırması (2016) sonuçlarına göre AB sigorta şirketleri müşterilerin riskini değerlendirirken genel olarak aşağıdaki ana kategorilere odaklanması gerektiği sonucuna ulaşmıştır. Aşağıda tanımlanan bu unsurlar gerek sigortacıların riski ölçmede gerekse siber sigorta satın almak isteyen işletmelerin riski yönetmede sahip olması gereken özellikleri göstermektedir.

Gözetim mekanizması; şirket bünyelerinde yer alan bilgi güvenliği sorumluları (Chief Information Security Officer), diğer çalışanların rutin iş tempolarında bilgi güvenliğine ayırmak zorunda oldukları zamanı telafi etmektedir. Bu kişilerin varlığı aynı zamanda şirket içinde bilgi güvenliği risklerinin düzenli ve sistematik takibini zorunlu kılacağından uzun vadede siber

risklerin ortaya çıkma ihtimalini azaltır. Bu nedenle Avrupa ülkelerindeki sigorta şirketleri, bir şirkette bilgi güvenliği sorumlularının varlığına daha fazla önem vermekte ve siber risk sigortası satın almak isteyen işletmelerde bu yönde çaba sarf etmektedir.

Bilgi güvenliği politikaları ve prosedürleri; sigortacılar önceleri şirketlerin bilgi güvenliği ile ilgili yazılı politika ve prosedürleri genel hatlarıyla dikkate alırken, günümüzde bu politikaların ne şekilde olduğu detaylarıyla sorgulanmaktadır. Dolayısıyla Avrupa ülkelerindeki sigorta şirketleri kapsamlı ve resmi bir bilgi güvenliği programının varlığını sorgulamak, buna ek olarak siber güvenlik konusundaki olgunluğunu dikkate alacak noktadadır. Benzer şekilde Türkiye'deki sigorta şirketleri tüm dizüstü, cep bilgisayarları, akıllı telefonlar ve ofis içi/dışı kullanılmakta olan masaüstü bilgisayarlardaki yetkisiz erişimi engelleyen sürücü şifrelemeleri için kontrol prosedürleri olup olmadığını sorgulamaktadır. Ayrıca şirket bünyesinde doküman koruma, saklama ve imha etme prosedürlerinin varlığı sorgulanmaktadır.

Çalışan farkındalığı; insan faktörü, bir örgüt içerisinde önemli bir risk oluşturabilirken, doğru eğitimle değerli bir savunma mekanizması ve risk yönetimi aracı haline gelebilmektedir. Örneğin, şifre çalma amaçlı e-postaları tanıyamayan eğitimsiz bir çalışan uygulanabilecek her güvenlik önleminin en zayıf halkasıdır. Buna ek olarak farkındalığı yüksek olan bir çalışan sadece politikaları ve prosedürleri uygulamakla kalmaz aynı zamanda bunları yorumlayarak uygulamaya çalışır. Avrupa ülkelerindeki sigorta şirketlerinin bir şirkette insan faktörünü güvence altına almanın önemli bir unsuru olan resmi bir güvenlik farkındalığı programının mevcudiyetini artık sorgulamaktalar. Özellikle sigortacılar; çalışanların, sık karşılaşılan siber risklere karşı eğitilmesine yönelik bir şirket prosedürünün varlığını sorguladıkları dikkati çekmektedir. Benzer şekilde Türkiye'de veri güvenliği ve gizliliği, yasal yükümlülükler, sorunlar, toplum mühendisliği (örneğin şifre çalma, phishing vb.) konularında farkındalık eğitimlerinin şirketler tarafından yürütülüp yürütülmediği sorgulanmaktadır.

Olay tepkisi; olay tepkisi, bir güvenlik ihlalinin veya siber saldırının sonrasını ele almak ve yönetmek için önceden geliştirilmiş risk yönetimi programıdır. Amaç, ortaya çıkan zararı sınırlayacak bir şekilde ele almak ve iyileşme süresini ve masraflarını azaltmaktır. Olay tepki planında, olayı neyin oluşturduğunu belirli koşullarla tanımlayan ve olay oluştuğunda izlenmesi gereken adımlar ve politikalar yer alır ve tüm departmanların buna uyması beklenir. Avrupa ülkelerindeki sigorta şirketleri, risk yönetimi sürecinde, işletmelerin bu tür bir programa sahip olup olmadıklarını sorgulamaktadır. Benzer şekilde Türkiye'de de sigortacıların risk analizi sürecinde işletmelerin iş devamlılık planı (BCP), yıkım onarım (DR) ve kriz yönetimi planlarının varlığı sorguladıkları tespit edilmiştir. Ayrıca herhangi bir bilgisayar saldırısı veya diğer veri kaybı/ihlali sonrasında operasyonların düzeltilmesi ve yeniden işler hale gelmesi için ne kadarlık süre harcandığı da sigortacıların risk analizi sürecinde dikkat ettikleri bir husustur. Yine bunun bir parçası olarak personelin iç bilgisayar ağına ve sistemlerine erişim yetersizliği/engellenmesi durumunun ne kadarlık bir sürede işletme için kriz yaratacağının sigortacılar tarafından sorgulandığı gözlemlenmiştir.

Güvenlik ölçümleri; şirketlerin düzenli olarak sahip oldukları bilişim risklerine yönelik güvenlik açıklarını izlemeleri önemlidir. Periyodik süreçler dahilinde ağ saldırılarının sıklıkları ve güvenlik açıklarının tespiti gibi testlerin yapılıp yapılmadığı ve mevcut şifreleme sisteminin içeriği Avrupa ülkelerindeki sigorta şirketleri için değerli konuma gelmiştir. Benzer şekilde Türk sigorta şirketleri de tüm bilgisayar aygıtlarında, sunucularında ve ağlarında yazılım sağlayıcının önerileri ve gereklilikleri doğrultusunda güncellemeleri yapılan anti-virüs yazılımı olup olmadığını, kullanılan güvenlik duvarı ve işgal/sızıntı görüntüleme tespit sisteminin olup olmadığını sorguladıkları gözlemlenmiştir. Buna ek olarak bilgisayar ağlarında hassas veriye erişimin sadece yetkili kişilerce erişimine sınırlı olup olmadığının da sorgulandığı tespit edilmiştir.

Tedarikçi (dış kaynak) kontrolü; çok sayıda firmanın üçüncü şahıslardan aldıkları tedarik hizmeti (mal veya hizmet şeklinde olabilir) neticesinde siber risklerle karşı karşıya kalma

ihtimalleri bulunmaktadır. Bu durum çoğu zaman şirketlerin kontrolünün dışında gelişse de Avrupa ülkelerindeki sigorta şirketleri için son yıllarda büyük önem arz etmektedir. Bu nedenle şirketlerin mal veya hizmet tedarik ettiği firmalarla kurduğu ilişkilerden kaynaklı siber tehlikelere karşı sigortacıların dikkat etmesi gerekliliği doğmaktadır. Türkiye uygulaması ise benzer şekilde sigortacıların, network, bilgisayar sistemi veya bilgi güvenliği fonksiyonlarının herhangi birinden dış kaynak kullanımı sağlayıp sağlamadıklarını sorguladıklarını göstermektedir. Bunun yanı sıra Türkiye'de sigortacıların, veri işleme veya depolama işlemlerini outsource ettikleri tüm iş ortaklarının IT sistemlerinin yeterliliklerini de sorguladıkları gözlemlenmiştir.

Üst yönetim farkındalığı; önemli bilgi güvenliği konularıyla ilgili yönetim kurulunun farkındalığı riski ele almak için atılan ilk adımdır. Bir kurul kararsız veya gecikmiş bir şekilde bu gibi konulardan haberdar olursa düzeltme eyleminin yetkisiz, kötü zamanlanmış veya orantısız olma riski bulunmaktadır. Daha açık bir ifadeyle siber tehlikelerle karşı karşıya olacak işletmelerde yönetim kurulunun periyodik olarak bilgilendirileceği bir yapıya sahip olması önemlidir. Yönetim kurulları rutin toplantılarında sıklıkla bu tür konuları tartışmaya almazlar. Ancak Avrupa ülkelerindeki sigorta şirketleri son yıllarda, yönetim kurullarının siber risklere karşı bilgilendirilme sıklığını ve toplantılarda siber risklere ilişkin alınan kararları sorgulamaktadır.

Sorunlar

Sigortacılar için en büyük zorluk, risk değerlendirmesini destekleyen siber güvenlik olayı verilerinin henüz büyük sayılar kanunu destekleyecek boyutta olmamasıdır. Sigortacıların henüz az sayıda gözleme ve veriye sahip olması geleceğe yönelik risk hesaplama sonuçlarındaki başarıyı etkilemektedir. Bu durum aynı zamanda Türkiye'deki sigorta şirketleri için benzer şeklindedir.

Avrupa ülkelerindeki sigorta şirketlerinin özellikle dikkat çektikleri bir diğer sorun, günümüz işletmeler dünyasında birleşme ve satın almaların sayısının artması neticesinde ortaya çıkan siber risklerdir. Şirketlerin satın alma veya birleşme yoluyla kimi zaman aynı çatı altında kimi zamanda yeni bir işletme olarak ortaya çıktığı bu durumlarda birleşen şirketlerin teknolojileri arasında da bir uyumsuzluğun veya güvenlik açıklarının yaşanması mümkün hale gelmektedir. Bir şirket siber riskle mücadelede kusursuz bir sisteme sahip olsa bile birleştiği veya satın aldığı diğer şirketin sahip olduğu bilişim alt yapısının güvensiz olması, ortaya çıkacak riskin boyutunu birleşme sonrası artıracaktır.

Siber risklere yönelik bir diğer sorun bulut bilişim ile ilgilidir. Bilindiği üzere tüm uygulama, program ve verilerinizin sanal bir sunucuda depolanması sistemine bulut bilişim denmektedir. Yani internetin olduğu her yerde elektronik cihazların aracılığı ile çeşitli bilgi ve verilere bulut bilişim veya teknolojisi sayesinde ulaşılabilmektedir. Bu noktadaki sorun müşteri konumundaki işletmelerin hangi veriyi ne kadar sıklıkta veya yoğunlukta bulut teknolojisiyle koruduklarının tam olarak kestirilemiyor olmasıdır. Bulut teknolojisiyle verilerin geri dönüşünü garanti altına almak kolaylaşsa da bu teknolojinin işletmeler tarafından düzenli olarak kullanılıp kullanılmadığı tam kestirilememektedir. Bu durum aynı zamanda Türkiye'deki sigorta şirketleri için benzer şekilde yorumlanmaktadır.

Gerek Avrupa'da gerekse de Türkiye'deki sigorta şirketlerinin daha az sıklıkta müşteri farkındalığının olmamasını, siber risklere ilişkin işletme içindeki plan ve politikaların tüm çalışanlarca aynı şekilde anlaşılamamış olmasını ve yeterli sayıda teknik beceri gerektiren personelin istihdam edilmiyor olmasını siber riskle mücadelede sorun olarak ortak değerlendirdikleri tespit edilmiştir.

Özetle çalışmada her iki bağlamda gerçekleştirilen paralel uygulamalar neticesinde birbirine benzer veya farklı seyreden iyi uygulamalar ve sorunlar yarı yapılandırılmış mülakat tekniğiyle karşılaştırma yapılabilir boyuta indirgenmiştir. Yukarıda anlatılanları bir tablo altında özetlemek bulguların anlaşılırlığına katkı sağlayacaktır. Buna göre siber risklerin sigortacılar tarafından yönetilmesi noktasında, iyi uygulamalar ve sorunları şu şekilde özetlenebilir;

Tablo 1. Siber risklere ilişkin risk analizi sürecinde karşılaşılan başarılı uygulamalar ve sorunlar

	Avrupa Birliği	Türkiye
Başarılı Uygulamalar		
Gözetim mekanizması	✓	X
Bilgi güvenliği politikaları ve prosedürleri	✓	✓
Çalışan farkındalığı	✓	✓
Olay tepkisi	✓	✓
Güvenlik ölçümleri	✓	✓
Tedarikçi (dış kaynak) kontrolü	✓	✓
Üst yönetim farkındalığı	✓	X
Sorunlar		
Yetersiz veri	✓	✓
Birleşme ve satın almalar	✓	X
Bulut bilişim kullanımı	✓	✓
Zayıf müşteri farkındalığı	✓	✓
İşletme içinde farkındalığı genele yayamama	✓	✓
Teknik beceriye sahip personel eksikliği	✓	✓

SONUÇ VE DEĞERLENDİRME

Her iki bağlamda gerçekleştirilen yarı yapılandırılmış mülakatlar neticesinde Türkiye ve AB sigorta şirketlerinin risk algıları ve riski değerlendirme bakış açıları arasında çok büyük farklılıklar olmadığı gözlemlenmiştir. Ancak Türkiye'deki siber risklerin yaratacağı olası sorunlara ilişkin işletmelerin farkındalığı AB'den farklılık göstermektedir. Ülkemizde siber uygulamaların gelişimi her ne kadar gelişmiş ülkelerle paralel seyretse de bu siber uygulamalar neticesinde ortaya çıkacak risklere ilişkin farkındalık ve risk algısı henüz düşük düzeyde seyrettiği gözlemlenmiştir. Ülkemizdeki bireysel risk algısının görece düşük olmasından siber risklerin de payını aldığı söylenebilir. Risk algısının düşük olması, sigortacıların bu tür risklere teminat sunmasında birtakım kısıtlar yaratacağı açıktır. Riskin yönetimi veya olası zararlardan korunmak ve tedbir almak öncelikle sigortalı bilincinin ve risk farkındalığının gelişkin olmasına bağlıdır. Bu nedenle toplumsal olarak risk farkındalığı yaratılamadığı sürece sigortacılar için siber sigortaların sürdürülebilir olması zorlaşacaktır. Zira ülkemizde siber sigorta ürününe sahip sigorta şirketi sayısı 2 iken, bu sayı 2017 yılı içerisinde bu şirketlerden birinin başka bir sigorta şirketi tarafından satın alınması neticesinde 1'e düşmüştür. Daha açık bir ifadeyle siber sigorta satışı ülkemizde yaygın bir uygulama olmaktan uzaktır. Gerçekleştirilen mülakat gösteriyor ki sigortacılar gerek işletmeler içerisinde yeterli teknik beceriye sahip personel eksikliğinden gerekse üst yönetim ve diğer çalışanların farkındalığının yetersiz olmasından bu sigorta ürününü satmaktan çekinmektedirler. Oysa Avrupa Birliği ülkelerinin büyük bir kısmında bu sigorta ürününün satışı artmaktadır. Dolayısıyla ülkemizdeki çabaların henüz karşılığını bulduğu söylenemez.

Türkiye uygulamasından elde edilen sonuçlar özellikle risk analizinin sigortacının soru formuyla başladığını ve işletme sahiplerine yöneltilen sorularla risklerin ortaya çıkarılmaya çalışıldığı bir durumu ortaya koymaktadır. Bu konuda yakalanacak açıkların sabit kıymetlerinde, sorumluluklarında özellikle kâr kaybında yaratacağı hasarların sigortacılar tarafından işletme sahiplerine raporlanarak risk farkındalığı yaratılmaktadır. Bunun en zayıf tarafı, farkındalık analizinin müşterinin izin verdiği ölçüde gerçekleşebiliyor olmasıdır. Ancak tersine AB sigortacılık sistemi özellikle siber riske maruz kalacak işletmelerin hali hazırda bir risk yönetimi sistemine, politika ve prosedürlerine sahip olunmasını zorunlu kılmaktadır. Daha açık bir ifadeyle sigorta satılacak bir işletmenin öncelikle risk yönetimi ve politikasına sahip olması zorunludur.

Sigorta şirketlerinin kendi siber güvenliklerini sağlamadaki çabaları ve farkındalıkları açısından Türkiye ile AB karşılaştırıldığında, AB sigortacılarının bu konuda ciddi yatırımlar yaptıkları görülmektedir. AB sigorta şirketlerinin pek çoğu, bilişim teknolojileri yatırımlarının %8-12'sini güvenlik yatırımlarına yönlendirmektedir (O'Connor, 2017). Richard Clarke'a göre güvenlik yatırımı için ayrılan bütçenin %8-12'den düşük olması sonucu oluşacak hataları gidermek şirketler için hem zor hem daha pahalı olacaktır. Yine Clarke'a göre, siber güvenliğin sağlanmasında en önemli unsur çalışanların beceri ve farkındalıkları olmaktadır. Sigorta şirketlerinin siber güvenlik yazılımları ve güvenlik duvarları ne kadar iyi olursa olsun, bilgi işlem çalışanlarının yetersiz bilgi, beceri ve farkındalığa sahip olması durumunda güvenlik tam anlamıyla sağlanamayacaktır (O'Connor, 2017). Sigorta şirketlerinin siber güvenlikleri, kişisel verilerin korunması bakımından büyük önem arz etmektedir. Dolayısıyla, şirketlerin gelebilecek olası siber saldırılara karşı bugünden önlem alması aynı derecede önemlidir. Ülkemizde sigorta şirketlerinin bu boyutlarda ciddi altyapı, güvenlik ve eğitim yatırımları olmasa da gelecekte bu yatırımların doğru yönlendirilmesine yönelik farkındalığın gelişmekte olduğu görülmektedir.

Her ne kadar risk analizi sürecinde başarılı uygulamalar farklılaşsa da sorunlar AB ile Türkiye arasında benzerdir. Ancak bu ortak sorunların ne düzeyde gerçekleştiği ileriki çalışmalarda nicel yöntemler yardımıyla daha da netleştirilebilir ve düzeyleri ve etkileri daha somut ortaya konabilir.

KAYNAKÇA

http://blog.trendmicro.com.tr/turkiyede-en-cok-karsilasilan-bes-siber-saldiri-cesidi/

http://riskandinsurance.com/analyzing-cyber-risk-coverage/

http://www.burakavci.com.tr/2016/01/dos-ddos-cyber-attack.html

http://www.cio.com/article/3065655/cyber-attacks-espionage/what-is-cyber-insurance-and-why-you-need-it.html

http://www.millire.com/dergi/SAYI_91.pdf

http://www.nart.com/siber-riskler-nart-guvencesinde/

http://www.paraanaliz.com/2017/ekonomi/sigorta-sektorunde-yeni-akim-siber-sigortalar-11654/

http://www.pwc.com.tr/tr/risk-surec-teknoloji-hizmetleri/bilgi-guvenligi-ve-siber-guvenlik-yayinlari/siber-riskler-sigortalanirken-nelere-dikkat-edilmeli-pwc.pdf

http://www.sigortacigazetesi.com.tr/siber-riskler-dogru-analiz-edilmeli/

http://www.sigortagundem.com/haber/siber-saldirilara-karsi-sigorta-teminati-geldi/1125704

https://blog.kaspersky.com.tr/ransomware-for-dummies/2713/

https://www.abi.org.uk/products-and-issues/products/business-insurance/cyber-risk-insurance/

https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public//cyber-risk-10_key_questions.pdf

https://www.mcguirewoods.com/Client-Resources/Alerts/2013/10/Buyers-Guide-to-Cyber-Insurance.aspx

https://www.slideshare.net/CezeriSGACezeriSiber/abd-siber-gvenlik-stratejisi

https://www.stm.com.tr/documents/file/Pdf/Siber%20Tehdit%20Durum%20Raporu%20Ekim-%20Aral%C4%B1k%202016.pdf

https://www2.deloitte.com/content/dam/Deloitte/tr/Documents/risk/tr-web-kuresel-siber-guvenlik-yonetici-bilgilendirme-raporu.pdf

Amy O'Connor (2017), 5 Ways the Insurance Industry Can Improve Cybersecurity: Former U.S. Security Chief Clarke, Insurance Journal, https://www.insurancejournal.com/news/national/2017/11/15/471130.htm Erişim: 24.04.2018.

Kırkbeşoğlu E. ve McNeill, J. (2015). Risk Yönetimine Giriş. *Risk Yönetimi ve Sigortacılık* (der. Kırkbeşoğlu E.) Gazi Kitabevi. Ankara., 21-42.

NART Sigorta ve Reasürans Brokerliği (2015). Siber Risklerin Yönetimi, Risk Management Forum 2015, İstanbul.

Rejda, G.E. 2005. Principles of Risk Management and Insurance, 9th edition. Pearson.

Eda ALTUNTAŞ
Başkent Üniversitesi, Sigortacılık ve Risk Yönetimi Yüksek Lisans Öğrencisi
E-posta: edaaltuntas.00@hotmail.com
ORCID: http://orcid.org/0000-0003-2874-5728

Emine KARA
Başkent Üniversitesi, Sigortacılık ve Risk Yönetimi Yüksek Lisans Öğrencisi
E-posta: e.kara20@outlook.com
ORCID: http://orcid.org/0000-0003-1824-6538

Abdullah Buğra SOYLU
Başkent Üniversitesi, Ticari Bilimler Fakültesi, Sigortacılık ve Risk Yönetimi Bölümü
E-posta: absoylu@baskent.edu.tr
ORCID: http://orcid.org/0000-0001-8119-369X

Erdem KIRKBEŞOĞLU
Başkent Üniversitesi, Ticari Bilimler Fakültesi,
E-posta: erdemk@baskent.edu.tr
ORCID: https://orcid.org/0000-0002-6781-9753

Yazı Bilgisi:

Alındığı tarih: 11 Şubat 2018.
Yayına kabul edildiği tarih: 30 Nisan 2018.
E-yayın tarihi: 28 Aralık 2018.
Yazıcı çıktı sayfa sayısı: 15.
Kaynak sayısı: 21.

Hakemler:
Prof. Dr. Ali Köse (Marmara Üniversitesi – İstanbul)
Öğr. Gör. Mehmet İsel (Bandırma Onyedi Eylül Üniversitesi - Manyas/Balıkesir)