Siber Güvenlik Yatırım Kararları Üzerine Literatür İncelemesi

Hakan ŞENTÜRK*, Celal Zaim ÇİL ve Şeref SAĞIROĞLU*****

*Kara Harp Okulu Savunma Bilimleri Enstitüsü, Ankara

** Çankaya Üniversitesi Elektronik ve Haberleşme Mühendisliği Bölümü, Ankara

*** Gazi Üniversitesi Bilgisayar Mühendisliği Bölümü, Ankara

(Geliş / Received : 01.04.2015 ; Kabul / Accepted : 02.06.2015)

ÖZ

Karmaşıklığı ve sıklığı her geçen gün artan siber saldırıların yol açtığı yüksek ekonomik zararlar ile bu saldırılara karşı koruma sağlayan çok sayıda siber güvenlik teknolojisi ürünlerinin yatırım alternatifi olarak sunulduğu güvenlik sektörü, alanda yapılan çalışmaların odak noktasını siber güvenliğin ekonomik boyutuna yöneltmiştir. Kısıtlı kaynak şartları altında siber güvenlik yatırım kararlarının verilebilmesine yönelik kullanılabilecek yöntemlerin belirlenmesi ihtiyacı öne çıkmıştır.

Bu çalışmada siber güvenlik yatırım kararlarının verilmesi sürecinde uygulanabilecek yatırım stratejileri, siber güvenlik risklerinin belirlenmesi ve ölçülmesi, güvenlik saldırılarının maliyet ve etkisinin ölçülmesi, güvenlik teknolojilerinin etkinliğinin ölçülmesi ve güvenlik yatırımlarının en uygun seviyesinin belirlenmesi olmak üzere beş kategoride alanda son onbeş yılda yapılan akademik çalışmalar incelenmiş, literatürdeki boşluklar ortaya konularak sonraki araştırmalara yön verilmesi amaçlanmıştır.

Anahtar Kelimeler: Siber güvenlik ekonomisi, güvenlik yatırımı, yatırım kararları, karar analizi, oyun teorisi, reel opsiyonlar

Literature Review on Cyber Security Investment Decisions

ABSTRACT

Severe financial losses incurred by cyber security attacks with increasing complexity and frequency, as well as booming cyber security sector offering variety of products as investment options have led the focus of the research in the field to the economic dimension of cyber security. The need for determination of methods to be used when making cyber security investment decisions under budget constraints have become prominent.

In five sections as the cyber security investment strategies, risk identification and measurement, attack costs and impacts calculation, measurement of technology effectiveness and determination of optimum level of cyber security investments, this study reviews and evaluates the academic literature on economic aspects of cyber security for the last fifteen years and aims to provide research directions by pinpointing literature gaps.

Keywords: Cyber security economy, security investment, investment decisions, decision analysis, game theory, real options

1. GİRİŞ (INTRODUCTION)

1990'lu yılların basit virüs yazılımlarıyla başlayan siber saldırıların, günümüzde gelişmiş, hedefli kalıcı tehdit (Advanced Persistent Threat, APT) saldırıları örneğinde görüldüğü gibi karmaşıklığını ve ekonomik etkisini artırdığı bilinmektedir. Bu durumun getirdiği en büyük zorluk, altyapının güvenliğinin sağlanması, ekonomik yansıması ise güvenlik için gerekli en uygun yatırım maliyetlerinin belirlenmesi ihtiyacıdır. Bu amaçtan yola çıkarak, bu çalışmada siber güvenliğin ekonomik boyutu üzerine alanda yapılan akademik çalışmalar incelenmiştir.

Siber güvenliğin ekonomik boyutunun büyüklüğü hakkında birkaç örnek vermek yerinde olacaktır. Ağustos 2003'te çıkan Blaster solucanı, ilk haftasında yarım milyon bilgisayara bulaşmış, işletme başına 475 bin dolar maddi kayıp verdiği açıklanmıştır [1]. "I Love You" ve "Love Bug" virüslerinin, dünya çapında 10 milyar dolar, My Doom isimli truva atının 4.8 milyar dolar, Nimda solucan yazılımının ise yaklaşık 3 milyar dolar maddi zarara yol açtığı tahmin edilmektedir [2].2010 yılında Symantec ve Ponemon Enstitüsü tarafından hazırlanan ve 15 farklı sektörden 51 farklı firmanın katıldığı sızma maliyetleri raporunda firma başına 2010 yılı yıllık ortalama kayıp tutarının 7,24 milyon dolar olduğu rapor edilmiştir [3]. Ponemon Enstitüsü tarafından 2012 yılında yapılan çalışmada ise, son üç yılda haftalık başarılı siber saldırı sayısı ortalamasının 50'den 102'ye çıktığı, ortalama saldırılardan kurtarma süresinin 14'den 24 güne çıktığı,

** Sorumlu Yazar (Corresponding Author)*
e-posta: hakan.senturk@shape.nato.int
Digital Object Identifier (DOI) : 10.2339/2016.19.1 39-51

firma başına yıllık ortalama kayıp maliyetinin ise 6,5 milyondan 8,9 milyon dolara çıktığı belirtilmiştir [4].

Bu verilerden de görüleceği üzere, siber güvenliği elektronik ve bilgisayar bilimi yanında ekonomik açıdan da ele almak bir zorunluluk haline gelmiştir. Nitekim Anderson, bilgi güvenliğini, finansal açıdan çözümü zor bir problem olarak tanımlamaktadır [5]. Artık bilgi güvenliği probleminin odak noktası teknik olarak neyin yapılabileceğinden, neyin ekonomik olarak en uygun olduğu noktasına kaymaktadır. Mevcut durumda bu alandaki mevcut çalışmalar yetersiz kalmaktadır [6,7]. Bu çalışmanın amacı; siber güvenliğin ekonomik boyutu ve siber güvenlik yatırım kararlarının en uygun seviyesinin belirlenmesine yönelik, alanda son on beş yılda dünyada yapılan akademik çalışmaların incelenmesi ve siber güvenlik ekonomisi alanında araştırma yapılabilecek konulara dikkat çekilmesidir.

Siber güvenlik ekonomisi alanında yapılan çalışmalar, temel olarak üç konuyu ele almaktadır [8]:

- Güvenlik saldırılarının/sızmaların gerçekleşme sıklığı: Saldırıların sıklığını oluşturan göstergelerin belirlenmesi.
- Güvenlik saldırılarının/sızmaların maliyeti: Bir saldırının maliyetinin tahmin edilebilmesine yönelik problemin çözümü.
- Siber güvenlik teknolojilerine yapılan yatırımlar: Belirlenen güvenlik sistemlerinin tedarik edilmesi, kurulumu, bakım ve idamesi ile kullanılmasına yönelik harcama düzeyinin belirlenmesi.

Benzer şekilde Su, siber güvenlik ekonomisi alanındaki mevcut literatür çalışmalarını şu üç kategoride toplamıştır [9]:

- Güvenlik saldırılarının maliyet ve etkilerinin ölçülmesi
- Güvenlik teknolojilerinin fayda ve etkilerinin ölçülmesi
- Güvenlik yatırımlarının optimum seviyesinin belirlenmesi.

Bu çalışmada, yukarıda Su tarafından belirtilen üç kategoriye ilave olarak, siber güvenliğin bir risk yönetimi disiplini olduğu [10] ve yatırımların ekonomikliğinin analizinde işletme risklerinin yönetilmesinin gerekliliği düşüncesinden yola çıkarak, "güvenlik risklerinin belirlenmesi ve ölçülmesi" ve siber güvenlik yatırım stratejileri da dâhil olmak üzere toplam beş temel alanda inceleme yapılmıştır.

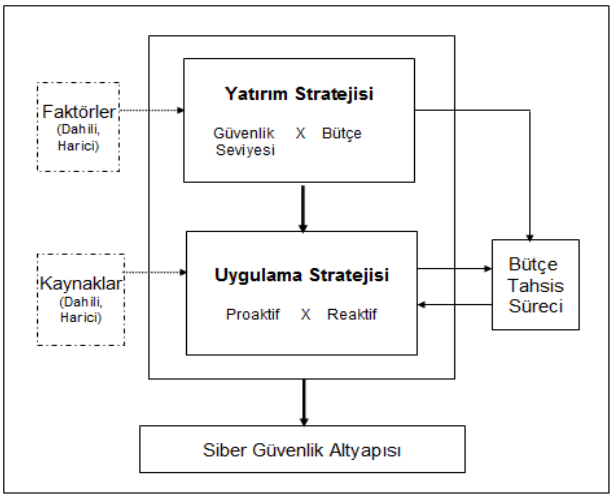
2. SİBER GÜVENLİK YATIRIM STRATEJİLERİ (CYBER SECURITY INVESTMENT STRATEGIES)

İşletmelerin siber güvenlik yatırımlarına yaklaşımının diğer yatırımlara olan yaklaşımıyla aynı olmadığını ortaya koyan çok yaygın bir görüş bulunmaktadır [11]. Siber güvenlik yatırımları, işletmeye doğrudan kar getirmeyen yatırımları gibi görülmektedir. Bir siber güvenlik yatırımının getireceği fayda, ancak işletmeye tehdit teşkil eden siber güvenlik risklerinin indirgenmesine bağlı olarak, aslında bir siber saldırı gerçekleşmesi durumunda yaşanacak maddi kaybın düşürülebildiği değer kadar olacaktır. Bu nedenle, yatırımın değerlendirilmesindeki ölçüt, diğer yatırımlardan farklı olarak, uygulanacak sistem çözümünün maliyeti düşüldüğünde, işletmeye sağlayacağı beklenen maddi kaybın azaltılması yönündeki marjinal fayda olacaktır [8].

İşletmelerin siber güvenlik yatırım kararları için kullandıkları strateji, genellikle Şekil 1'de görüldüğü üzere iki türlüdür [11]:

- Yatırım için gereken sabit bir bütçe miktarının belirlenmesi.
- Siber güvenlik gereksinimlerini ve önceliklerini karşılamaya yönelik hedeflenen güvenlik seviyesinin belirlenmesi.

İşletmeler, siber güvenlik yatırım karar sürecine, sabit bir bütçe belirleyerek ya da işletmenin güvenlik önceliklerini karşılamaya yönelik güvenlik seviyesi belirleyerek, diğer bir deyişle, yatırım stratejisini belirleyerek başlarlar. İşletmelerle yapılan görüşmeler sonucu ortaya konulan raporlarda, sabit bütçenin çoğunlukla işletmenin Bilgi Teknolojileri bütçesinin belirli bir yüzdesi (genellikle %1-%15 arasında) üzerinden belirlendiği görülmektedir [6,41]. Amaç, belirlenen sabit bütçeyle işletme risklerini minimize edebilecek teknolojileri edinecek güvenlik yatırımına karar vermektir. İşletmenin güvenlik gereksinimlerine odaklanan diğer yatırım stratejisinde ise güvenlik riskleri, öncelikleri ve hedeflenen güvenlik seviyesine ulaşabilmek için gerekli yatırım miktarı belirlenir. Yatırım stratejisinin belirlenmesine etki eden iç ve dış faktörler, işletmenin iş süreçleri gereksinimleri, önceki dönem tecrübe edilen saldırı olayları, uyulması gereken mevzuatlar, müşteri ya da tedarikçi talep veya koşulları olabilir [11].



Şekil 1. Siber Güvenlik Yatırım Karar Süreci [11].

İşletmenin yönetim seviyesinde belirleyeceği yatırım stratejilerinin, genellikle uygulama stratejilerini de şekillendirdiği görülmektedir. İki temel uygulama stratejisi; siber saldırıların gerçekleşmesinden sonra işletmenin güvenlik açıklarının giderilmesine yönelik reaktif ve kapsamlı risk analizleri sonucunda gerçekleşmesi muhtemel saldırıları önlemeye yönelik proaktif uygulama stratejileridir. Uygulama stratejilerinin belirlenmesine etki eden bilgi kaynakları; işletme içi/dışı güvenlik denetimleri, personel deneyimleri, saldırılara yönelik işletme içi toplanan ya da CSI/FBI, Ponemon, vb. enstitülerin çalışmaları kapsamında yayınlanan çeşitli istatistikî veriler, Ulusal/Uluslararası en iyi uygulamalar, ISO standartları usulleri, müşteri gereksinimleri, üretici tavsiyeleri olabilmektedir [11].

3. GÜVENLİK RİSKLERİNİN BELİRLENMESİ VE ÖLÇÜLMESİ (IDENTIFICATION AND MEASUREMENT OF SECURITY RISKS)

İşletmelerin güvenlik risklerinin analizi ve değerlendirilmesi amacıyla nicel, nitel ve karma teknikler kullanılmaktadır. Nicel tekniklerde risk sayısal değerlerle ifade edilirken, nitel tekniklerde ise genellikle düşük, orta, yüksek gibi tanımlayıcı sıfatlarla ifade edilir. Karma tekniklerde ise her iki yöntem de beraber kullanılır. Kullanılan yöntemler arasındaki en belirgin fark risk karar değişkenlerinin belirlenme ve hesaplanma farklılıklarıdır. Kullanılan risk karar değişenleri en azından aşağıdakilerden bir veya birkaçını kapsamaktadır [12]:

- Varlığın değeri,
- Zafiyetin kötü amaçlı kullanılma olasılığı,
- Etki seviyesi

Nicel tekniklerden en yaygınları, dördüncü bölümde açıklanacak olan Yıllık Kayıp Beklentisi metriği, Courtney, Livermore Risk Analizi Metodolojisi (LRAM), ISRAM (Information Security Risk Analysis Method), Stokastik Baskınlık tekniği, Hata Modları ve Etki Analizi (Failure Modes and Effects Analysis-FMEA) yöntemleridir [13]. Bu tekniklerin güçlü yanı işletmelere zafiyet altında olan varlıklarını ve değerlerini belirlemeye ve bu varlıkları korumak için gerekli olan tedbirleri almaya zorlamasıdır. Zayıf yanı ise bu değerlerin hesaplanmasında ihtiyaç duyulan fazla zaman ve işgücü gibi zorluklar ve belirsizliklerdir [6].

Nicel yöntemlerle birlikte kullanılan, risklerin sayısallaştırılması amacıyla kullanılan teknikler Tablo 1'de gösterilmiştir:

Tablo 1. Risk Sayısallaştırma Teknikleri [14].

Süreç Yaklaşımı	Faktör Yaklaşımı	Aktüeryal Yaklaşım
Sebep-Sonuç	Risk göstergeleri	Ampirik kayıp dağılımları
Bayesian İnanç Ağları		
Bulanık Mantık	Sermaye Varlık fiyatlandırma modeli (Capital Asset Pricing model –CAPM)	Geçmiş veri tabanı bilgileri kullanılan parametrik dağılımlar
İstatistik Kalite Kontrol ve Güvenilirlik Analizi		
Bağlantı	Tahminsel modeller	Aşırı-Değer Teorisi
Sistem Dinamikleri		

Risk analizinde kullanılan nitel teknikler ise, senaryo analizi, beyin fırtınası, hata ağacı analizi (Fault Tree Analysis-FTA), olay ağacı analizi (Event Tree Analysis-ETA), neden-sonuç analizi, olasılık ve etki matrisleri, kontrol listeleri, bulanık metrikler, uzman görüşlerine başvurulan görüşme ve anket yöntemleridir [6,15]. Bu yöntemlerin zayıf yanı uzman personelinin öznel görüşlerinden faydalanılarak belirlenen risklerin genellikle düşük, orta, yüksek vb. sayısal olmayan değerlendirmeler içermesidir. Genellikle bu tür yöntemlerin kullanılması esnasında ortaya çıkan farklı algılar ve riskler arasındaki bağlantılar, fayda maliyet analizlerinde kullanılabilmek amacıyla oluşturulan risk matrislerinin hazırlanmasını daha da karmaşıklaştırmakta, hatta imkânsız kılabilmektedir [16].

Günümüzde yaygın olarak bilinen ve ticari yazılımıyla beraber kullanılan nitel yöntemlerden birisi CRAMM (United Kingdom Central Computer and Telecommunication Agency's (CCTA) Risk Analysis and Management Method)'dir. Yöntem, BS7799 standardı ile ve ITSEC ile tam uyumludur [17]. Nitel yöntemleri kullanan bir diğer yazılım Cobra (Consultative, Objective and Bi-functional Risk Analysis)'dır. Bu yöntem de CRAMM gibi ISO 17799 uygunluğunu ölçebilmektedir. Varlıklar, tehditler ve zayıflıklar arasındaki ilişkileri ve riskin bulunduğu ortam arasındaki bağlantıları göstermek için görsel diyagramlar (UML) kullanan bir diğer nitel yöntem ise CORAS (Construct a platform for Risk Analysis of Security Critical Systems)'dır [18]. OCTAVE (The Operationally Critical Threat, Asset and Vulnerability Evaluation) da yaygın olarak bilinen ve kullanılan bir başka nitel risk değerlendirmesi modeli ve aracıdır [19].

Nitel ve nicel risk analiz yöntemlerinin avantaj ve dezavantajlarıyla birlikte ifade edildiği karşılaştırmalı analiz Tablo2 ve Tablo 3'de görülmektedir. Nitel yöntemler, genellikle uzman değerlendirmelerine dayandığından uygulaması daha basit olmaktadır. Nicel değerlendirmeler ise risklere özgü çoğu zaman ulaşılması zor istatistiki verilere ihtiyaç duymakta, ancak kaliteli verinin bulunması durumunda uygulanabildiği takdirde gerçeğe daha yakın sonuçlar verebilmektedir.

Tablo 2. Nitel ve Nicel Risk Analiz Yöntemlerinin Karşılaştırmalı Analizi - Avantajlar [19].

Nicel Risk Analizi/ Değerlendirmesi	**Nitel Risk Analizi/ Değerlendirmesi**
Ölçütler, hesaplamalar ve elde edilen sonuçlar; nesnel, somut, bağımsız gözlemlerden elde edilen istatistiksel verilere dayanır.	Hesaplamalar basittir.
Bilgi varlıklarının parasal değerleri ve risk yaklaşımı kavramları çok ayrıntılı ve belirgindir.	Bilgi varlıklarının ve risklerin parasal değerlerini bilmeye veya ölçmeye gerek yoktur.
Güvenlik çözümlerinin kar zarar analizini yapma, üst yönetimin; güvenlik yatırımlarının verimliliğini irdeleme olanağı vardır.	Tehditlerin yoğunluğunu sayısal olarak ölçerek belirlemeye gerek yoktur.
Üst yönetimi tatmin edecek şekilde tüm bilgiler ve tüm sonuçlar parasal ve gerçek sayılarla ortaya konabilir.	Teknik bilgi becerisi yetersiz olan veya güvenlik konusunda bilgisi olmayan kişiler de risk değerlendirme sürecine katkı yapabilir.
Otomatik bir süreç biçimine getirilebilir.	Raporlama, sonuçları değerlendirme ve iş süreçleri ile bütünleştirmede esnektir. İstatistiksel verilere gerek duymaz. Parasal değerin ölçülemediği veya ön bilginin hiç olmadığı koşullarda da kullanılabilir.

Aktaş ve Soğukpınar, risk analiz ve değerlendirme için uygun yöntem seçimi amacıyla bir yaklaşım önermiş, önerdikleri yaklaşımı dört adet risk analizi yöntemi üzerinde test ederek sonuçları yorumlamıştır [18].

Nitel ve nicel tekniklerin beraber olarak kullanıldığı karma yöntemlere örnek olarak, Countermeasures Inc., şirketi tarafından geliştirilen The Buddy System risk analiz aracı verilebilir [17].

Siber güvenlik risk yönetimi, bilgi varlıklarının bütünlük, gizlilik ve erişilebilirlik niteliklerini tehdit eden risklerin gerçekleşme olasılığının ortadan kaldırılması veya azaltılması sürecidir. ISO/IEC 27005, kurumların bilgi güvenliği risklerini değerlendirmek amacıyla genel bir çerçeve sunmakta, bilgi güvenliği risklerinin tanımlanması, adlandırılması, gruplanması, analizi, değerlendirilmesi, hesaplanması, ölçümü ve işlenmesine ilişkin adımları belirlemekte, bilgi güvenliği risklerinin sürekli ve güncel şekilde izlenmesi, denetimi ve yönetimine ilişkin kuralları ve yöntemleri tanımlamaktadır.

ISO 27005'e ilave olarak ABD Standartlar ve Teknoloji Enstitüsü'nün NIST 800-30, ISACA'nın RiskIT gibi bilinen diğer metodojiler de işletmelere bilgi güvenliği risklerini tanımlamaları, analiz ederek yönetebilmeleri amacıyla rehberlik sunmaktadır.

Her bir bilgi varlığına yönelik riskin ölçülmesinden sonra uygulanan risk yönetim metodolojisi kapsamında, riskten kaçınmak, riski devretmek, riski azaltmak ve riski kabul etmek alternatifleri arasından biri seçilerek uygulanır. Gerçekleşme olasılığı ve ekonomik değeri düşük bilgi varlığı riskleri için riskin kabullenilmesi seçilebileceği gibi, bazı durumlarda riskin transferi, diğer bir deyişle, işletme dışında bir unsurla paylaşılması (örneğin siber güvenlik sigortası yaptırmak) söz konusu olabilir.

Tablo 3. Nitel ve Nicel Risk Analiz Yöntemlerinin Karşılaştırmalı Analizi - Avantajlar – Dezavantajlar [19].

Nicel Risk Analizi/ Değerlendirmesi	**Nitel Risk Analizi/ Değerlendirmesi**
Hesaplamalar karmaşıktır.	Öznellik ve taraflı yargıda bulunma sorunu vardır.
Genelde, ilgili bir bilgi bankasıyla ve uygun araçlarla birlikte kullanılırsa başarılı sonuç verebilir. Çok fazla sayıda ön çalışmaya ve ön bilgiye gerek duyulur.	Bilgi varlıklarının gerçek parasal değerlerini sürece katma olanağı kısıtlıdır. Güvenlik çözümlerinin kar-zarar analizini yapma olanağı yoktur.
Üst yönetime veya uzman olmayan kişilere sunulacak kadar yalınlaştırılması çok zordur.	Tahmine dayalı olduğu için başarılı kestirimler yapılması zorunludur.
Risk değerlendirme sürecine katılan kişilerin yönlendirilmesi zor ve karmaşık bir işlemdir.	Otomatik bir biçime gelmesi çok zordur, otomasyona elverişliliği düşüktür.
Risk değerlendirme süreci sırasında karar değiştirmek çok zor ve zahmetlidir.	
Kapsam dışı bırakılan riskleri sonradan hesaba katmak genelde çok	

zordur.	

ABD'de 2013 yılı itibariyle siber-sigorta hizmeti sağlayan otuzun üzerinde sigorta şirketi olduğu, mevcut sigorta primlerinin genellikle 10 bin dolar ile 25 bin dolar arasında olmakla birlikte kapsama durumuna göre 50 milyon dolara kadar çıkabildiği [20], poliçe kapsamlarının birbirlerinden farklılık gösterdiği belirtilmiştir [15]. Riskin transferi amacıyla siber güvenlik sigortası kullanılmasının, hem akademisyenler hem de uygulayıcılar tarafından önerildiği, sigorta primlerinin hesaplanabilmesine yönelik ise farklı yaklaşımlar tavsiye edildiği görülmektedir [21-24]. Siber sigorta uygulamasının, birbirine bağımlı sistemlerde gereğinden az yatırım yapılması problemine karşı potansiyel bir çözüm olarak da düşünüldüğü belirtilmiştir [20].

Herath ve diğerleri, Tablo 1'de görülen aktüeryal bir yaklaşım ile ilişki (copula) tabanlı bir siber sigorta risk modeli ve fiyatlandırması yöntemi önermişlerdir [22]. Geçmiş yılların virüs maliyetleri kullanılarak oluşturulan modelin zayıf tarafı, yazarlarca da belirtildiği üzere, istatistikî olarak geçmiş saldırı ve maliyet bilgilerinin kullanılmasına olan bağımlılıktır ki, bu tür bilgilerin bulunmasındaki zorluklar pek çok çalışmada dile getirilmiştir [22,25,26,27].

Bandyopadhyay, siber güvenlik risklerinin indirgeme ve transferi amacıyla siber sigorta kullanımını incelemiş, sonraki çalışmalar için deneysel analizlerin yapılmasını önermiştir [28].

Jourdan, bilgi güvenliği uzmanlarıyla yaptığı görüşmelerden faydalanarak bilgi güvenliği risk analizi süreçlerini incelemiş, sonuç olarak risk analiz süreçlerinin dinamiklerini daha iyi anlamak ve uygulamalarını iyileştirmek yönündeki akademik çalışmaların devamını önermiştir [15].

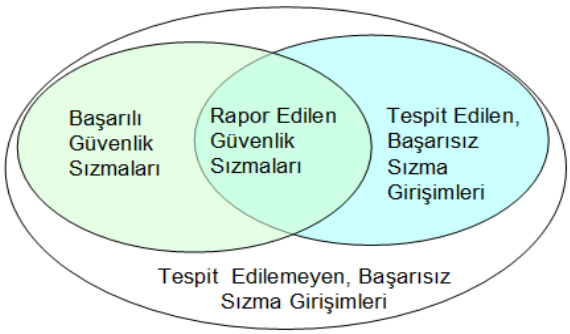
Wang, aşırı değer teorisi ile riske maruz değer (Value at Risk) yöntemini kullanarak risklerin belirlenmesi, ölçülmesi ve yatırımların fayda-maliyetinin artırılması üzerine bir yaklaşım önermişlerdir [29]. Claunch ve McMillan, son yıllarda siber saldırılardan kaynaklanan kayıp maliyetlerinin, tıp sektörü için 2010-2011 döneminde %10 olan genel sektör ortalamasının %32 oranında artış gösterdiği istatistiğine dikkat çekerek, Wyoming Tıp Merkezi'nde gerçekleştirdikleri vaka çalışmasında işletmenin tüm varlıklarını kapsayan bir risk analizi yaklaşımıyla, ilgili tıp merkezinin optimum siber güvenlik yatırımıyla, güvenlik seviyesini önemli derecede artırabildiğini belirtmiştir [30].

4. GÜVENLİK SALDIRILARININ MALİYET VE ETKİLERİNİN ÖLÇÜLMESİ (MEASUREMENT OF COST AND IMPACT OF SECURITY ATTACKS)

Thomas ve diğerleri, siber güvenlik saldırılarının maliyet ve etkilerinin ölçülmesindeki problemlerin; saldırı bilgilerini paylaşmama eğilimi, saldırı sonuç ve maliyetlerinin sağlıklı ölçülememesi, soyut varlıkların değerlemesindeki zorluklar, yanlış tahminler, orantısız sonuçlar, belirsizlik, bilgi yetersizliği, saldırı analizlerinde işletme içi birimlerin farklı ilgi, algı ve çıkarları ile kutuplaşmadan kaynaklandığını belirtmişlerdir [31].

Güvenlik saldırılarının maliyet ve etkilerinin ölçülmesi konusundaki bir diğer problem ise, saldırıların tespit edilebilmesindeki yetersizliklerdir. Örneğin APT saldırılarının, tespit edilmeyi önleyerek uzun süre ağda kalıp dışarıya yüksek değerli bilgi sızdırmayı sağlayabildiği, amacına ulaştıktan sonra kendini temizleyerek geride saldırıya yönelik iz bırakmadığı geçmiş saldırı analizlerinin sonucunda ortaya çıkmıştır [32,33]. Bunun dışında eğitim yetersizliği, zayıf güvenlik altyapısı, güvenlik ürünlerinin uygun yapılandırılmaması gibi sebeplerle de saldırılar çoğu zaman tespit edilememektedir.

Soo Hoo çalışmasında, Şekil 2'de görüldüğü üzere sızma girişimlerini birbiriyle örtüşebilen dört kümeye ayırmış, tespit edilen ve rapor edilen sızmaların ölçülebildiğini belirterek tespit edilemeyen başarılı ve başarısız sızma girişimlerinin görece oranlarının yüksek derecede belirsiz olduğunu ifade etmiştir [26].



Şekil 2. Sızma Girişimi Kümeleri [26].

Güvenlik saldırılarının işletmeye olan maliyet ve etkileri finansal, operasyonel, müşteriler ve çalışanlar ile ilgili somut ya da soyut etkilere yönelik doğrudan, dolaylı ya da fırsat maliyetlerini kapsamaktadır [9,34,35]. İngiltere Bilgi Güvenliği Forumu (Information Security Forum, ISF), bir güvenlik saldırısının işletmeye olan maliyet ve etkilerini aşağıdaki şekilde kategorize etmektedir [34]:

- Finansal etkisi
  - Satış, sipariş veya yeni sözleşme kayıpları
  - Somut varlıkların kayıpları
  - Cezalar, hukuki sorumluluklar
  - Öngörülmeyen maliyetler
  - İşletmenin düşen hisse değeri
- Operasyonel etkisi
  - Yönetim kontrolünün kaybı
  - Rekabetçiliğin kaybı
  - Yeni girişimlerin beklemeye alınması
  - Uygulamada olan iş standartlarının ifşa edilmesi
- Müşteriler ile ilgili etkiler

  - Geciken teslimatlar
  - Müşteri kayıpları
  - Güven kaybı
  - İşletme ününe gelen zarar
- Çalışanlar ile ilgili etkiler
  - Çalışanların moral durumunda ve verimliliğinde düşüş
  - Yaralanma veya ölüm.

Yukarıda belirtilen olumsuz etkilerin tespit edilebilmesi genellikle iş etki analizi yöntemiyle gerçekleştirilir [6]. Ancak risklerin ölçülmesinde bulunan problemler gibi, güvenlik saldırılarına ilişkin, rakamlarla ifade edilemeyen soyut etkilerin ve bu etkilerin seviyelerinin belirlenmesinde de problemler bulunmaktadır. Bu tür etkilerin boyutları, değerleme puanlaması gibi öznel yöntemlerle belirlenebilmekte [6]; ancak, ulaşılan sonuçların üzerinde sayısal analiz yapılarak, bu analiz sonuçlarına göre karar verebilecek doğrulukta olup olmadığı konusunda tereddütler yaşanmaktadır [36]. Literatürde, dolaylı maliyetlerin belirlenmesine yönelik çalışmalar, genellikle saldırı açıklanma bilgileri ile hisse senedi değerleri arasındaki ilişkilerin incelemesi üzerine olmaktadır.

Çavuşoğlu ve diğerleri, pazar değerleme tabanlı bir yaklaşımla, sızmaya maruz kalan işletmelerin piyasa değerinin açıklanmasının ilk iki günü içinde ortalama %2,1 kayba uğradığı, buna paralel olarak da bilgi güvenliği firmalarının ise aynı dönemde ortalama %1,36 değer kazandığını gözlemlemişlerdir [37].

Hovav ve D'Arcy, virüs ve hizmet dışı bırakma saldırılarına maruz kalan işletmelerin hisse senetlerinin borsadaki durumunu incelemiş, olayların açıklanmasının ardından bahse konu işletmelerin borsa senetlerinin değer kaybına uğradığını gözlemlemişlerdir [2] ve [38]. Ayrıca, saldırıların türüne göre etkilerin de farklı olduğu görülmektedir. Campbell ve diğerleri, yaptıkları deneysel çalışmada, halka açıklanan sızmalardan gizli bilginin ifşası özelliğinde olanların, işletmenin piyasa değerine negatif etkisini tespit ederken, yine halka açıklanan ancak gizli bilginin ifşa edilmediği sızmalara borsanın ve piyasanın aynı negatif etkiyi vermediğini gözlemlemişlerdir [39].

Gordon ve diğerleri, 2011 tarihli çalışmalarında, 1995-2007 arasındaki dönemde siber saldırıların işletmelerin hisse senetleri üzerindeki etkilerini incelemişler, saldırılar ile hisse senet değerleri arasındaki ters yönlü etkileşimin yüksek olduğunu, saldırıların bilgi güvenliğinin gizlilik, bütünlük ve erişilebirlik kıstaslarına göre sınıflandırılması durumunda, hisse senetleri üzerindeki en fazla olumsuz etkinin erişilebilirliği hedef alan saldırılar olduğunu tespit etmişlerdir [40].

Telang ve Wattal, yazılım sektöründe faaliyet gösteren üretici şirketler üzerine yaptığı çalışmada, yazılım zafiyetlerine ilişkin haberlerin medyada çıktığı gün, şirketlerin piyasa değerlerinin % 0.63 düştüğünü, yazılım zafiyetinin türüne göre etkinin de farklı olduğunu tespit etmişlerdir [41].

Wang, medyada çıkan sızma haberleriyle işletmelerin hisse senedi değerleri arasındaki ilişkiyi incelemiş, Campbell'ın çalışmasının sonuçlarıyla uyumlu olarak genel saldırı ve sızma haberlerinin farklı etkilere yol açtığı, ancak gizli bilgi içeren belirli sızma haberlerinin piyasada firmanın gelecekteki başarısı üzerinde daha negatif etkiye yol açtığını tespit etmiştir [42].

Conrad, zafiyetler, sızma sıklığı, kayıp maliyet tahminleri gibi güvenlik modeli parametreleri kapsamına belirsizliği de katabilmek için Monte Carlo simülasyonu yöntemini kullanmıştır [9,43].

İşletmelerin genel eğilimi, kötü reklâm olabileceği ve sektördeki konumuna zarar verebileceği düşüncesiyle maruz kaldıkları siber güvenlik saldırıları ve beraberinde gerçekleşen kayıplara ilişkin bilgileri paylaşmama yönündedir [26,28,31,44]. Bu sebeple pek çok makalede deneysel analizlerin artması gerektiğine işaret edilmekte, genellikle çalışmalarda ABD'de düzenli olarak yapılmakta olan ve çeşitli sektörlerden çok sayıda işletmenin katıldığı veri toplama çalışma sonuçlarından faydalanıldığı görülmektedir [6,35].

Gerçekleşen sızmaların kayıp maliyetlerine yönelik istatistikî veri sağlayan bu tür çalışmaların en yaygın örnekleri, CSI/FBI, Ponemon Enstitüleri ile Verizon'un yıllık yayınlanan raporlarıdır. Bu raporlarda, çalışmaya katılan işletmeler kapsamında, sektör bazlı saldırı türleri, saldırıların gerçekleşme sıklıkları ve saldırılardan kaynaklanan kayıp maliyetleri, kullanılan teknolojiler, uygulanan standartlar gibi çeşitli istatistiki veriler sunulmaktadır [3,4,36,45,47]. Örneğin, Ponemon Enstitüsü'nün 2014 yılı Mayıs ayında yayınladığı küresel veri sızma araştırması raporunda, araştırmaya katılan işletmelerin işletme başına ortalama kayıp maliyetlerinin bir önceki yıla oranla %15 artarak 3,5 milyon dolara çıktığı belirtilmektedir [46].

Hoo [46], sızma olaylarının sıklığı ve sonuçların etkilerinin sağlıklı şekilde ölçülmesi amacıyla sonraki çalışmalar için;

- Risk yönetimi faaliyetini destekleyici bilgi güvenliği istatistiklerinin toplanmasına yönelik metrik ve araçların geliştirilmesi,

- Saldırı paternlerinin ve saldırganların davranışlarının gözlemlenmesi amacıyla bilgisayar ağlarının simüle edildiği yazılım araçlarının geliştirilmesi gerektiğini önermiştir [26].

5. GÜVENLİK TEKNOLOJİLERİNİN ETKİNLİĞİNİN ÖLÇÜLMESİ (MEASUREMENT OF EFFECTIVENESS OF SECURITY TECHNOLOGIES)

Normal şartlarda, güvenlik teknolojilerinin fayda ve etkinliği, fayda-maliyet analizi yöntemleri ile ölçülebilir. Faydaları, korudukları bilgi varlıklarının değerleri ve indirgedikleri riskin derecesi ile, maliyetleri ise yazılım/teçhizatın tedarik maliyeti, kurulum, eğitim ve bakım-idame maliyetlerini kapsayan toplam sahiplik maliyetleri ile ölçülebilir. Ancak, seçilen güvenlik

teknolojilerinin etkinliğinin ölçülmesi hususunda problemler mevcuttur [35]. Laboratuvar ortamında yapılan etkinlik testlerinde toplam saldırılardan ne kadarının önlenebildiğine yönelik yüzdesel değerler elde edilebilmekte ancak, gerçek şartlarda saldırı girişimlerinin tamamının sayısının belirlenememesi sebepleriyle teknolojilerin toplam saldırıların yüzde kaçını önleyebildiğinin tespiti mümkün olmamaktadır [26]. Kullanılan güvenlik teknolojilerini etkinlikleri açısından birbirleriyle kıyaslamak için mevcut formal bir metodoloji de bulunmamaktadır. Zorluklar, saldırgan profilinin ve işletmenin güvenlik politikasına uyum durumunun tahmin edilmesindeki belirsizliklerin ölçülememesinden kaynaklanmaktadır [9].

Güvenlik teknolojilerinin etkinliği, o teknolojinin ilgili riski ne kadar azaltmakta olduğunun değerlendirilmesi ile de ölçülür [9,26]. Riskin azaltılması ise, riskin tamamen önlenmesi veya gerçekleşme olasılığının azaltılmasıdır. Güvenlik teknolojilerinin etkinliğinin değerlendirilmesinde, mevcut olması durumunda test ortamlarında gerçekleştirilen ürün deneme çalışma sonuçları ve geçmişte gerçekleşen olaylara ait istatistikî veriler kullanılabilir, bu tür tarihi verinin mevcut olmaması durumunda ise güvenlik teknolojilerinin etkinliğinin tahmin edilmesi için uzman görüşlerinden, işletmenin bilgi güvenliği uzman personelinden faydalanılabilir. Butler, uzman görüşlerinin varsayım ve tahminlerinin, alınan kararlara ne kadar duyarlı olduğunun belirlenebilmesi için duyarlılık analizi yapılmasının doğru yaklaşım olduğunu belirtmiştir [47].

Diğer bir konu ise, güvenlik teknolojilerinin birbirinden bağımsız olarak çalışmaması sebebiyle etkinliklerinin de bağımsız ölçülmemesi gerektiği [27], dolayısıyla birden fazla güvenlik teknolojisinin kullanılması durumundaki etkileşimin ölçülmesidir. Belirlenen risk için kullanılacak birden fazla teknolojinin riski ne kadar azaltacağı, toplam faydanın, ilgili teknolojinin tek tek kullanıldığında alınacak faydadan büyük olup olmayacağı konularının da incelenmesi gerekmektedir [3,47].

Yatırım yapılan güvenlik teknolojileri kullanılarak oluşturulan güvenlik sistemi altyapısının teknik açıdan etkinliğinin değerlendirilmesi amacıyla ise zafiyet tarama, sızma testleri vb. amaçlı çok sayıda ürün rafta hazır şekilde bulunmaktadır. Ayrıca bu amaçla işletmeler, gerek iç denetimler gerekse de dış kaynak kullanımıyla danışman şirketlerin denetlemesi yöntemine de başvurmaktadırlar; ancak, bu yaklaşım sistemin geneline ilişkin değerlendirme olup, siber güvenlik teknolojilerinin bireysel olarak değerlendirilmesi konusunda yardımcı olamamaktadır.

Gordon ve diğerleri, siber güvenlik denetimlerinin arttığına işaret ederek, denetimlerin siber güvenlik risklerinin indirgenmesinde ve yatırım kararlarında iyileştirmeler yapabildiğini belirtmiştir [48].

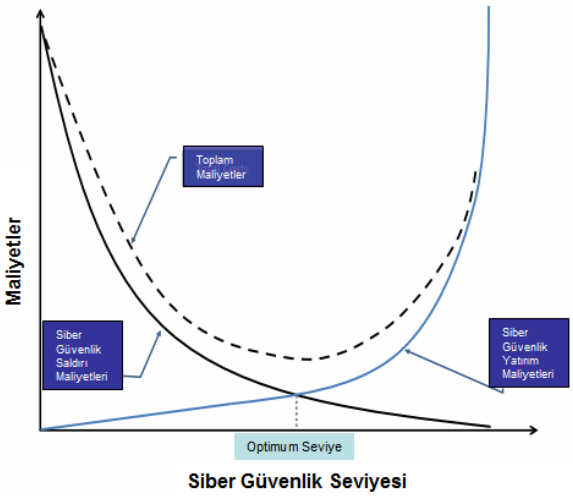
6. GÜVENLİK YATIRIMLARININ OPTİMUM SEVİYESİNİN BELİRLENMESİ (IDENTIFICATION OF OPTIMUM LEVEL OF SECURITY INVESTMENTS)

Rodewald, siber güvenlik yatırımlarına ilişkin iki ön kural belirlemiştir. Birincisi, tek başına hiçbir güvenlik kontrolünün belirli bir riski tamamıyla ortadan kaldıramayacağı, ikincisi ise her bir güvenlik kontrolünün bir maliyeti bulunduğudur [49]. Bu iki kurala, risklerin yüzde yüz gerçekleşip gerçekleşmeyeceğinin bilinemeyeceği gerçeği de eklenince, bir işletme için hangi güvenlik teknolojilerinin yatırıma değer olduğu ve güvenlik için ne kadar yatırım yapılması gerektiği soruları önem kazanmaktadır [6].

Şekil 3'e bakıldığında mavi çizgiyle gösterilen siber güvenlik yatırımları arttıkça siyah çizgi ile gösterilen olası saldırı maliyetlerinin azaldığı görülmekle, ancak optimum seviye olarak gösterilen belirli bir noktadan sonra yapılan siber güvenlik yatırımlarının saldırı maliyetlerini aynı oranda düşüremediği, dolayısıyla kesikli çizgi ile gösterilen toplam maliyetlerin arttığı görülmektedir [50]. Bu nedenle siber güvenlik yatırımlarının işletme risklerinin de minimizasyonu hedeflenerek [51], bütçe, güvenlik öncelikleri gibi kıstaslar da dikkate alınmak suretiyle yatırımların optimum seviyesinin belirlenmesi gerekmektedir.

Crume, bilgi güvenliğinin ilk kuralını, bir varlığı korumak için değerinden fazla yatırım yapmama gerekliliği olarak tanımlamıştır [52]. Bu nedenle, yapılması gereken yatırım seviyesinin belirlenebilmesi için işletmenin sahip olduğu bilgi varlıklarının değerlerinin belirlenmesi gerekmektedir. Poore, bilgi varlıklarının değerlerinin belirlenmesi aşamasında rehber olarak kullanılabilecek öneriler sunmuştur [53].

Güvenlik yatırımlarının analizi ve optimum yatırım seviyesinin belirlenebilmesi için önceki bölümlerde belirtilen risk, saldırı ve teknoloji etkinlik ölçümlerinin sonuçlarından faydalanılır ve yatırım kararları alınır.



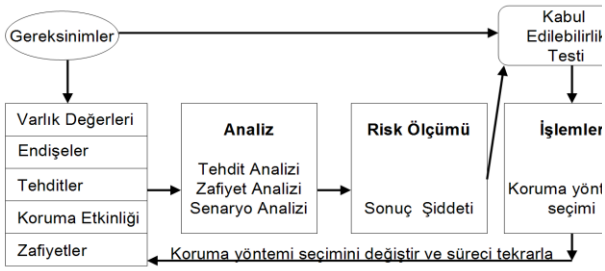
Şekil 3. Siber Güvenlik Yatırımları Olurluk İncelemesi [50].

Literatürde bu alanda kullanılan üç genel yaklaşım bulunmaktadır [9] :

- Karar Analizi Çerçevesi
- Oyun Teorisi
- Reel Opsiyonlar Teorisi.

6.1. Karar Analizi Çerçevesi (Decision Analysis Framework)

Bu yaklaşımın temelleri 1980'li yılların ortasında ABD Ulusal Standartlar Bürosu ve ABD Ulusal Bilgisayar Güvenlik Merkezi'nin önderliğinde gerçekleştirilen bir dizi bilgi güvenliği risk yönetim modelleme çalıştayına dayanmakta olup, ortaya çıkan birinci nesil siber güvenlik risk yönetim modellerinin en temeli Şekil 4'de görülen Ortak Çerçeve olmuştur [26].



Şekil 4. Ortak Çerçeve Süreç Diyagramı [26].

Ortak Çerçeve; Gereksinimler, Varlıklar, Güvenlik Endişeleri, Tehditler, Koruma Yöntemleri, Zafiyetler ve Sonuçlar olmak üzere yedi temel bileşenin tekrarlamalı bir süreç içerisinde analizini önermektedir. Ortak çerçevenin uygulama karmaşıklığı ve kaliteli verinin bulunamaması zorluklarının aşılabilmesi amacıyla, Entegre İş Risk Yönetim Çerçevesi, Değerleme-tabanlı metodolojiler, Senaryo Analizi Yaklaşımları ve En İyi Uygulamalar olmak üzere dört genel başlık altında ikinci nesil siber güvenlik risk yönetim modelleri ortaya çıkmıştır. Bu yaklaşımlar, her ne kadar veriye bağımlılık problemini kısmen aşmış olsalar da daha çok iş süreçlerine ve organizasyonel dinamiklere yoğunlaşmış, özellikle belirsizlik problemlerini aşamamıştır. 2000'li yıllardan itibaren yapılan pek çok çalışmada atıfta bulunulan Soo Hoo, belirsizlikleri de içine alan karar analizi ve risk yönetimi tabanlı bir model önerisinde bulunmuştur [26].

Gordon ve Loeb, optimum yatırım seviyesinin belirlenmesi amacıyla yapılan yatırımın marjinal faydasının marjinal maliyete eşitlenme prensibine dayalı bir ekonomik model önermiş, bir işletmenin sahip olduğu varlıkların değerinin %36,8'inin optimum yatırım seviyesi olduğu sonucuna varmışlardır [54]. Willemson ise, Gordon ve Loeb tarafından önerilen model üzerinde düzeltmeler yapılarak, yapılan hesaplamalarda optimum seviyenin varlık değerlerinin %50'sine çıkması gerekebildiğini iddia etmiştir [55].

Mercuri, fayda maliyet analizinin, açık anahtar kriptografisi, ağ sızma tespit sistemleri vb. sistemlerin değerlendirilmesinde kullanılabildiğini belirtmiştir [16]. Xie ve Mead, fayda-maliyet analizi yöntemiyle küçük işletmelerin bilgi güvenliklerinin geliştirilmesine yardımcı olacak tahmin metodolojisi geliştirmiştir [56]. Bodin ve diğerleri tarafından, Analitik Hiyerarşi Prosesi (AHP) kullanılarak çok ölçütlü bir karar verme modeli önerisi yapılmış [57], ancak karar seçimi alternatiflerinin belirlenmesi üzerinde durulmamıştır. Aynı yazarlar sonraki çalışmalarında önerdikleri AHP yaklaşımını risk metrikleriyle birleştirerek yatırım alternatiflerinin sıralanmasına yönelik bir model önermişlerdir [20].

Rue ve diğerleri tarafından ise farklı siber güvenlik yatırım modellerin analiz edilerek karşılaştırıldığı bir çerçeve model önerisi yapılmıştır, sonraki çalışmalar için, istatistikî verilerin bu karar modelinde uygulanan değerlendirme sürecine dâhil edilmesini önermişlerdir [35].

Behara ve diğerleri, sistem dinamikleri yaklaşımını kullanarak siber saldırı sürecinde yapılan yatırımların analizi için bir karşılaştırma ve analiz modeli önermişlerdir [58]. Ionnidis ve diğerleri, fayda teorisini kullanarak siber güvenlik yatırımlarının doğru zamanlamasının belirlenmesi konusunda çalışmışlardır [59]. Chai ve diğerleri, güvenlik teknolojilerinin dolaylı getirisinin belirlenmesi kapsamında 1997-2006 yılları arasındaki ABD borsa verilerini temel alarak yaptıkları çalışmada, siber güvenlik yatırımı yaptıklarına dair medyada çıkan haberler sonrasında işletmelerin borsa değerlerinde aşırı yükselme olduğunu kaydetmişlerdir [60].

6.2. Oyun Teorisi (Game Theory)

Sosyo-ekonomik değişkenleri içinde barındıran, ekonomik kararların alınmasında, karşılıklı etkileşimle optimal karar vermeye yönelik bir yaklaşım olan modern oyun teorisinin temelleri 1928 yılında John Von Neumann tarafından atılmıştır. Oyun teorisinde bir diğer önemli çalışma 1950 yılında John Nash tarafından gerçekleştirilen "Nash dengesi" teorisi olmuştur [61].

Oyun teorisinin siber güvenlik yatırımlarının değerlendirilmesindeki uygulamaları kapsamında; saldırganların stratejileri arasındaki etkileşim ve sızma başarısının artırılması, karşı tarafta ise işletmenin kazancının maksimize edilmesi amacıyla yapılan yatırımların sonucunda saldırıların engellenmesi, sistemdeki zafiyetlerin azaltılması ile saldırganlar üzerinde caydırıcılık etkisi vb. etkiler incelenmektedir [62].

Alpcan, işletmenin bölümler arası güvenlik ve bilgi teknolojileri risklerini optimum yatırımlarla indirgeyebilmeleri için dinamik teşvik mekanizmaları geliştirme konusundaki çalışmasında, oyun teorisini kullanmıştır [63]. Huan, oyun teorisi ile öğrenme teorisini birleştirmiş, oyun teorisinde genellikle ele alınmadığını iddia ettiği zaman unsurunu da dikkate alan stokastik bir oyun modeli önererek yatırımların

optimum seviyesinin belirlenmesi konusunda çalışmıştır [64].

Çavuşoğlu, oyun teorisi tabanlı bir yaklaşım kullanarak güvenlik yatırımlarını değerlendirme ve farklı faktörlerin yatırımlar üzerindeki etkisini inceleme amaçlı bir model önermişlerdir [65]. Grossklags, toplam çaba, en zayıf link, en iyi savunma, en zayıf hedef tiplerinden oluşan güvenlik oyunlarıyla siber güvenlik ve yatırım türleri ilişkilerinin ekonomik analizini yapmıştır [66]. Bommannavar ve diğerleri, saldırganlar ile koruyanlar arasındaki etkileşimi modellemek amacıyla sıfır toplamlı bir güvenlik oyunu tasarlamış, oyun teorisini, pekiştirmeli öğrenme ve markov modeli ile birleştirmek suretiyle karar vericilere yardımcı olacak nicel bir risk yönetimi çerçevesi önermişlerdir [67].

Zeshuang ve Jing, oyun teorisi ile işletmelerin siber güvenlik yatırım kararlarını analiz etmişlerdir [62]. Liu ve diğerleri, bu yaklaşımla, iki işletmenin bilgi güvenliğine ilişkin bilgi paylaşımı ve yatırım kararlarına ilişkin eğilimlerini incelemiştir [68]. Naghizadeh ve Liu, oyun teorisini kullanarak kullanıcıların, siber sigorta tercihlerini analiz etmiştir [69]. Gao ve diğerleri, bu yaklaşımla tüketim modellerinden Cournot ve Bertrans modellerini siber güvenlik yatırım kararlarının analizi amacıyla kıyaslamıştır [70]. Ashok ve diğerleri, enerji sektörüne yönelik kritik altyapıların geniş alan ağında izleme, koruma ve kontrolünün sağlanması amacıyla siber güvenliğinin belirlenmesinde oyun teorisi yaklaşımını kullanmışlardır [71].

6.3. Reel Opsiyonlar Teorisi (Real Options Theory)

Proje ortamındaki değişimlere tepki gösterme yeteneği olarak bilinen "reel opsiyon", finansal opsiyon teorisinin, yatırım projelerinin değerlendirilmesi ve firma stratejisinin belirlenmesi gibi finansal olmayan, diğer deyişle reel alanlara uyarlanmış halidir [72]. İşletme varlıklarının değerlendirilmesinde kullanılan bu teorinin [73] diğer önemli faydası belirsizlikler altında verilmesi gereken yönetimsel yatırım kararları sürecine, esnekliği dâhil etmesidir [74]. Bu sayede yatırım kararının ertelenmesi, beklenenden önce veya sonra sona erdirilmesi, küçültülmesi veya genişletilmesi gibi durumları karar vericilere seçenek olarak sunabilmektedir [72].

Gordon ve diğerleri, siber güvenlik yatırımları için uygulanan bekle-gör politikasını ve saldırıların gerçekleşme sayısının artmasıyla orantılı olarak siber güvenliğe daha fazla yatırım yapıldığı düşüncesini bu yaklaşımı kullanarak açıklamışlardır [75]. Tatsumi ve Goto, Gordon modelinden yola çıkarak, reel opsiyonlar yöntemiyle ne kadar ve ne zaman yatırım yapılması gerektiği sorularına cevap aramıştır [76]. Daneva ise önerdiği karar destek modelinde, belirlediği reel opsiyonların karar verme sürecinde gerekli esnekliği sağladığını iddia etmiştir [77]. Herath ve Herath, yığın e-posta üzerine gerçek verilerin kullanıldığı çalışmalarında reel opsiyonlar teorisi ile Bayes teoremi istatistikleri ve analizler sonrası öğrenmeyi içeren bir model önermişlerdir [78].

6.4. Kullanılan Metrik ve Yöntemler (Metrics and Methods Used)

Genel anlamda yatırımların ekonomikliğinin tespit edilmesi ya da yatırım projelerinin değerlendirilmesi maksadıyla kullanılan genel kabul görmüş yöntemleri, paranın zaman değerini dikkate alan ve almayan yöntemler şeklinde sınıflandırılmak mümkün olup, bu yöntemler aşağıda gösterilmiştir.

- Paranın Zaman Değerini Dikkate Alan Yöntemler:
  - Net Bugünkü Değer Yöntemi
  - İç Kar Oranı Yöntemi
  - Eşdeğer Maliyet Yöntemi
  - İndirgenmiş Geri Ödeme Süresi Yöntemi.
- Paranın Zaman Değerini Dikkate Almayan Yöntemler:
  - Basit Karlılık Oranları
  - Geri Ödeme Süresi Yöntemi
  - Nakit Girişinin Yatırım Maliyetlerine Oranı Yöntemi
  - Net Karın Yatırım Maliyetlerine Oranı Yöntemi
  - En Düşük Ortalama Maliyet Yöntemi
  - Kara Geçiş Analizi.

Siber güvenlik yatırımlarının analiz edilmesi amacıyla yaygınlıkla kullanılan yöntemler ise paranın zaman değerini dikkate alan "Net Bugünkü Değer" ve "İç Kar Oranı" metrikleri ile, paranın zaman değerini dikkate almayan, fayda maliyet analizi tabanlı, nakit girişinin ya da net karın yatırım maliyetlerine oranının farklı formüllerle ifade edildiği "Güvenlik Yatırımının Geri Dönüşü" yöntemidir [9,16,45,54,79].

6.4.1. Güvenlik Yatırımının Geri Dönüşü (Return on Security Investment-ROSI)

En basit anlamda bir yatırımın geri dönüşü, aşağıdaki formülün [80] sağında görüldüğü üzere, yapılan yatırımdan elde edilen faydanın yapılan yatırım tutarına bölünmesiyle hesaplanır. Bu basit anlatımda, siber güvenlik yatırımı tutarı, somut bir sayıyı ifade eder, ancak siber güvenlik yatırımının faydasının hesaplanması kolay olmamaktadır, çünkü örneğin tedarik edilen bir güvenlik duvarının işletmeye doğrudan getirisi olmadığından, beklenen fayda, risklerden kaynaklanabilecek kayıp maliyetlerini indirgeme ya da farklı tanımlamalarla hesaplanabilmektedir.

$$ROSI = \frac{R - ALE}{T} = \frac{S - T}{T} \quad (1)$$

Yukarıdaki formülde; R (recovery), bir yılda gerçekleşen saldırıların sebep olduğu kayıplardan

kurtarma maliyeti; S (savings), yatırım yapıldığında önlenen kayıplardan tasarruf maliyeti; T (tool), güvenlik teknolojisinin maliyeti; ALE ise daha önce de açıklandığı gibi yıllık kayıp beklentisidir.

Aşağıdaki formülde ise ROSI, risk indirgeme oranı ile ilişkilendirilerek hesaplanmaktadır [27].

ROSI = ((Risk tutarı x İndirgenen risk yüzdesi) – Güvenlik çözümünün maliyeti) / Güvenlik çözümünün maliyeti

6.4.2.Net Bugünkü Değer (Net Present Value-NPV)

ROSI metriğinin öznel zayıflığına ilave olarak zaman özelliği de problem teşkil etmekte, bu zayıflıklar nedeniyle işletmeler, ROI ile NPV metriklerinin kullanımına yönelmektedirler. NPV, ilgili yatırım çözümünün getirdiği para akışını bulmak ve bu rakamı mevcut zamanın para değerine dönüştürmek suretiyle çalışır. Para akışı, hesaplanan tahmini maliyetler, maliyet tasarrufları ve karları da kapsayan gelirlerden oluşmaktadır [9].

6.4.3. İç Kar Oranı (Internal Rate of Return-IRR)

Bu metrik de, NPV metriğine benzer şekilde para akışının hesaplanmasına odaklanır, ancak NPV'den farkı IRR'de maliyet ve fayda arasındaki başa-baş noktasının bulunmasıdır [9].

Gordon ve Loeb, işletme içi yatırımların faydalarını, işletmenin diğer yatırımlarından ve faaliyetlerinden ayırt etmenin zorluğuna değinerek, gerçekleşen maliyet tasarrufları ile beklenen maliyet tasarruflarının karşılaştırıldığı gerek NPV gerekse de IRR metriklerinin yetersiz kaldıklarını belirtmişlerdir [54]. ROSI metriğinde olduğu gibi, NPV ve IRR metriklerinin hesaplanmasında da yatırım ve maliyetlere ilişkin faiz ve vergi unsurunun dikkate alınmamasının gerçek hayata uygun olmadığı, elde edilen değerlerin tam olarak gerçeği yansıtmayacağı belirtilmektedir [79].

6.4.4. Yıllık Kayıp Beklentisi (Annual Loss Expectancy- ALE)

1979 yılında ABD Ulusal Standartlar Bürosu, "Otomatik Veri İşleme Risk Analizi Rehberi" isimli 65 numaralı Federal Bilgi İşleme Standardını yayımlayarak bilgisayar-tabanlı risklerin ölçümünde kullanılması amacıyla aşağıda açıklanan ALE metriğini önermiştir [26]:

$$\text{ALE}=\sum_{i=1}^{n} I(Oi)Fi \qquad (2)$$

Yukarıdaki formülde;

$\{O_1, \ldots O_n\}$ = Maddi zararla sonuçlanan saldırı olay seti

$I(O_i)$ = i olayının ABD doları cinsinden etkisi

F_i = i olayının gerçekleşme sıklığı

Avrupa Ağ ve Bilgi Güvenliği Ajansı (European Network and Information Security Agency-ENISA) ise, ALE'yi benzer şekilde, Yıllık Gerçekleşme Oranı (Annual Rate of Occurrence-ARO) ile Bir Olayın Kayıp Beklentisi (Single Loss Expectancy-SLE) değerlerinin çarpımı olarak tanımlamıştır [81].

ALE metriğinin ilgi çekici yanı, riske yönelik olasılık ve sonuç niteliklerini tek bir rakamla ifade edebilme yeteneğidir. Zayıf yanı ise, yüksek sıklığa sahip düşük etkili olaylar ile düşük sıklıklı yüksek etkili olayları birbirinden ayıramamasıdır [26]. Diğer bir eleştirilen tarafı, sadece doğrudan maliyetleri ele alması, örneğin üretimin aksamasından kaynaklanan dolaylı maliyetlerin düşünülmemesidir [79]. ALE metriğinin pratikte uygulanmasındaki kritik unsur, saldırıların gerçekleşme sıklığı ve etkilerine yönelik deneysel verilere ihtiyaç duyulmasıdır ki çoğu zaman bu tür verilere kolay ulaşılamamaktadır; ancak, buna rağmen metrik, sağladığı fayda sebebiyle [16] yatırım kararlarına yönelik modellerde yaygınlıkla kullanılmaktadır.

7. SONUÇLAR (CONCLUSION)

Bu çalışmada, siber güvenlik yatırım kararlarının verilmesi sürecinde uygulanabilecek yatırım stratejileri, siber güvenlik risklerinin belirlenmesi ve ölçülmesi, güvenlik saldırılarının maliyet ve etkisinin ölçülmesi, güvenlik teknolojilerinin etkinliğinin ölçülmesi ve güvenlik yatırımlarının optimum seviyesinin belirlenmesi konularında literatür incelemesi yapılmış, işletmelerin siber güvenlik yatırım kararlarını vermeleri için gerekli olan adımlara yönelik aşağıda belirtilen boşluklar tespit edilmiştir:

- Güvenlik olayları ile ilgili olarak risklerin belirlenerek ölçülebileceği "standart", genel kabul görmüş bir model bulunmamaktadır.

- Yatırım yapılan güvenlik teknolojilerinin, riskleri ne oranda indirgediğinin, risk yönetimi açısından ne kadar etkili olduklarının belirlenmesine yönelik "standart", genel kabul görmüş bir yöntem bulunmamaktadır.

- Siber saldırıların kayıp maliyet hesaplamaları ile, yapılan güvenlik yatırımlarının işletmeye finansal açıdan faydalarının hesaplanmasında "standart", genel kabul görmüş bir yöntem bulunmamaktadır.

- Kullanılan finansal metriklerin farklı formüllerle siber güvenliğe uygulanabildiği görülmekte, dolayısıyla bu konuda da üzerinde uzlaşılmış, genel kabul görmüş bir yöntem ortaya konulamadığı anlaşılmaktadır.

Sonuç olarak çalışmada, siber güvenlik yatırımlarına yönelik farklı yaklaşımlar, kaliteli verinin eksikliği, risklerin belirlenmesinde ve ölçülmesindeki belirsizlikler, saldırıların meydana getirdiği dolaylı zararların ve siber güvenlik teknolojilerinin etkinliklerinin belirlenmesindeki zorluklar bulunduğu belirlenmiştir.

Bu zorlukların aşılabilmesi ve çalışma sonuçlarının gerçek hayatta kullanılabilir yöntemler ve standartlar haline getirilebilmesi için öncelikle incelenen beş kategoride de bilimsel çalışmaların artırılması [78], deneysel çalışma sonuçlarının doğrulanmasında kullanılabilecek kaliteli verinin kaydedilmesi,

saklanması ve paylaşımının sağlanması önem arz etmekte olup bu amaçla, kamu, kamu-özel sektör ve kamu-özel sektör ile üniversitelerin ortak girişimlerine ihtiyaç olduğu değerlendirilmektedir.

8. KAYNAKLAR (REFERENCES)

1) A. Hovav ve J. D'Arcy, "The Impact of Virus Attack Announcements on the Market Value of Firms", ***Information Systems Security***, June 2004.

2) M. Ünver, C. Canbay ve A.G. Mirzaoğlu, "Siber Güvenliğinin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler Raporu", Mayıs 2009.

3) Symantec and Ponemon Institute, "2010 Annual Study: US Cost of a Data Breach", March 2011.

4) HP Ponemon Study, "The Growing Cost of Cyber Crime", 2012.

5) Ross Anderson, "Why Information Security is Hard – An Economic Perspective", ***17th Annual Computer Security Applications Conference***, September 2001.

6) S.E. Aoufi, "Economic Evaluation of Information Security", VU University Amsterdam, ***PhD Thesis***, ISBN/EAN:978-90-9024326-9, 2009.

7) L.A. Gordon ve M.P. Loeb, "Economic Aspects of Information security: An Emerging Field of Research," ***Information System Frontiers***, Vol. 8, No. 5, 2006, pp. 335-337.

8) J.N. Sheen, "Information Security Investment Decision by Fuzzy Economics", ***3rd International Conference on Information Sciences and Interaction Sciences (ICIS)***, 23-25 June 2010.

9) X. Su, "An Overview of Economic Approaches to Information Security Management", Technical Report, June 2006.

10) B. Blakley, E. McDermott ve D. Geer, "Information Security is Information Risk Management", ***Communications of the ACM***, 2002, pp.97-104.

11) B.R. Rowe ve M.P.Gallaher, "Private Sector Cyber Security Investment Strategies: An Empirical Analysis", ***Workshop on the Economics of Information Security (WEIS)***, March 2006.

12) D.J.Landoll, "The Security Risk Assessment Handbook", Auerbach Publications", ISBN : 978-0-8493-2998-2, 2006.

13) R.K. Rainer, C.A. Snyder ve H.H. Carr, "Risk Analysis for Information Technology", ***Journal of Management Information Systems***, 1991, Vol.8 No.1, pp.129-147.

14) A. Mukhopadhyay, S. Chatterjee, D. Saha, A. Mahanti ve S.K. Sadhukhan, "e-Risk Management with Insurance: A framework using Copula aided Bayesian Belief Networks", ***Proceedings of the 39th Hawaii International Conference on System Sciences***, 2006.

15) S.Z. Jourdan, "An Investigation of Organizational Information Security Risk Analysis", Auburn University, ***Ph.D Thesis***, 2010.

16) R.T. Mercuri, "Analyzing Security Costs", ***Communications of the ACM***, Vol.46 No.6. June 2003.

17) B.Karabacak ve İ.Soğukpınar, "Bilişim Sistemlerinde Etkin Risk Analizi Yöntemleri", ***Bilgi Teknolojileri Kongresi***, Poster Sunum Bildirisi, Pamukkale Üniversitesi, Denizli, 06-08 Mayıs 2002.

18) F.Ö.Aktaş ve İ.Soğukpınar, "Bilgi Güvenliğinde Uygun Risk Analizi ve Yönetimi Yönteminin Seçimi İçin Bir Yaklaşım", ***Elektrik-Elektronik-Bilgisayar Mühendisliği Sempozyumu***, Bursa, 26-30 Kasım 2008.

19) M. Eminağaoğlu, "Özdevimli Öğrenme Yaklaşımı ile Bilgi Güvenliği Risklerinin Nitel Değerlendirilmesine Yönelik Bir Model", Trakya Üniversitesi Fen Bilimleri Enstitüsü, ***Doktora Tezi***, 2011.

20) L. Bodin, L.A. Gordon ve M.P. Loeb, "Information Security and Risk Management," ***Communication of the ACM***, Vol. 51, No. 4, 2008, pp. 64-68.

21) H. Cylinder, "Evaluating Cyber Insurance", CPCU eJournal, Vol. 61 No. 12, December 2008.

22) H.S. Herath ve T.C. Herath, "Cyber-Insurance: Copula Pricing Framework and Implications for Risk Management", ***Workshop on the Economics of Information Security (WEIS)***, 2007.

23) R. Böhme, "Cyber insurance Revisited", ***Workshop on the Economics of Information Security (WEIS)***, Harvard University, 2005.

24) R. Böhme ve G. Kataria, "Models and Measures for Correlation in Cyber-Insurance", ***Workshop on the Economics of Information Security (WEIS)***, UK, 2006.

25) L.A. Gordon, M.P. Loeb ve T. Sohail, "A Framework for Using Insurance for Cyber-Risk Management", ***Communications Of The ACM***, 2003.

26) K.S. Hoo, "How much is Enough? A Risk-Management Approach to Computer Security", Stanford University, ***Ph.D.Thesis***, June 2000.

27) W. Sonnenreich, J. Albanese ve B. Stout, "Return on Security Investment (ROSI) : A Practical Quantitative Model", ***Journal of Research and Practice in Information Technology***, Vol. 38, No. 1, February 2006.

28) T. Bandyopadhyay, "Mitigation and Transfer of Information Security Risk: Investments in Financial Instruments and Technology", The University of Texas, ***Ph.D Thesis***, 2006.

29) J. Wang, A. Chaudhury, and H. Raghav Rao, "Research note-A Value-at Risk Approach to Information Security Investment," ***Information Systems Research***, pp. 106–120, 2008.

30) D. Claunch ve M. McMillan, "Determining the right level for your IT Security Investment", ***Healthcare Financial Management***, pp. 100-103, May 2013.

31) R.C.Thomas, M. Antkiewicz , P.Florer, S.Widup ve M.Woodyard, "How Bad is it? – A Branching Activity Model to Estimate the Impact of Information Security Breaches", ***Workshop on the Economics of Information Security (WEIS)***, 2013.

32) McAfee White Paper, "Combating Advanced Persistent Threats", 2011.

33) ISACA Report sponsored by Trend Micro, "Advanced Persistent Threat Awareness Study Results", 2013.

34) ISF, Information Security Forum, "The Standard of Good Practice for Information Security", 2007.

35) R. Rue, S.L. Pfleeger ve D. Ortiz "A Framework for Classifying and Comparing Models of Cyber Security Investment to Support Policy and Decision-Making", ***Workshop on the Economics of Information Security***, 2007.

36) Ponemon Institute Report sponsored by HP Enterprise Security, "2012 Cost of Cyber Crime Study", October 2012.

37) H. Çavuşoğlu, B. Mishra ve S. Raghunathan, "The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers", ***Internal Journal of E-Commerce***, 2004.

38) A. Hovav ve J. D'Arcy, "The Impact of Denial of Service Attack Announcements on the Market Value of Firms", ***Risk Management and Insurance Review***, Vol.6,No.2, 97-121, 2003.

39) K. Campbell, L.A. Gordon, M. Loeb ve L. Zhou, "The Economic cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market", ***Journal of Computer Security***, pp. 431-448, 2003.

40) L.A. Gordon, M.P. Loeb, ve L. Zhou, "The Impact of Information Security Breaches: Has There Been a Downward Shift in Costs?" ***Journal of Computer Security***, Vol. 19, No. 1, 2011, pp. 33-56.

41) R. Telang, ve S. Wattal, "Impact of Software Vulnerability Announcements on the Market Value of Software Vendors – An Empirical Investigation", Working Paper, Carnegie Mellon University, 2006.

42) T. Wang, "Essays on Information Security from an Economic Perspective", Purdue University, ***Ph.D Thesis***, 2009.

43) J.R. Conrad, "Analyzing The Risks of Information Security Investments With Monte Carlo Simulations", ***Proceedings of the 4th Workshop on the Economics of Information Security (WEIS05)***, June 2005.

44) T.Sohail, "To Tell or Not To Tell: Market Value of Voluntary Disclosures of Information Security Activities", University of Maryland, ***Ph.D Thesis***, 2006.

45) CSI (Computer Security Institute), "Computer Crime and Security Survey", 2010.

46) Ponemon Institute, "2014 Cost of Data Breach Study: Global Analysis", May 2014.

47) S.A. Butler, "Security Attribute Evaluation Method: A Cost-Benefit Approach", ***Proceedings of the 24th International Conference on Software Engineering***, New York, USA, pp. 232-240, 2002.

48) L.A. Gordon, M.P. Loeb, T. Sohail, C. Tseng ve L. Zhou, "Cyber Security, Capital Allocations and Management Control Systems", ***European Accounting Review***, Vol.17, No.2, pp. 215-241, 2008.

49) G.Rodewald, "Aligning Information Security Investments with a Firm's Risk Tolerance", ***Proceedings of the 2nd Annual Conference on Information Security Curriculum Development (InfoSecCD)***, Georgia, 23-24 September 2005.

50) L.A. Gordon, M.P. Loeb ve W.Lucyshyn, "Reducing The Challenges to Making Cybersecurity Investments in the Private Sector", ***Presentation at Homeland Security Science and Technology Principal Investigators' Meeting***, 2012.

51) I.Winkler, Qualys White Paper, "Justifying IT Security", 2010.

52) J. Crume, "Inside Internet Security", Addison Wesley Professional Publications, 08 September 2000.

53) R.S. Poore, "Valuing Information Assets for Security Risk Management", ***Information Systems Security***, pp.13-23, October 2000.

54) L.A. Gordon ve M.P. Loeb, "The Economics of Information Security Investment", ***ACM Transactions on Information and System Security***, 438-457, November 2002.

55) J. Willemson, "On the Gordon&Loeb Model for Information Security Investment", 2006.

56) N. Xie ve N.R. Mead, "SQUARE Project: Cost/Benefit Analysis Framework for Information Security Improvement Projects in Small Companies", ***Networked Systems Survivability Program Technical Note***, CMU/SEI-2004-TN-045, November 2004.

57) L.D. Bodin, L.A. Gordon ve M.P. Loeb, "Evaluating Information Security Investments Using Analytical Hierarchy Process", ***Communications ACM***, pp. 78-83, 2005.

58) R. Behara, C.D.Huang ve Q.Hu, "A System Dynamics Model of Information Security Investments", ***European Conference on Information Systems (ECIS)*** Switzerland, 2007.

59) C. Ionnidis, D. Pym ve J. Williams, "Fixed Costs, Investment Rigidities and Risk Aversion in

Information Security: A Utility-theoretic Approach", ***Workshop on the Economics of Information Security (WEIS)***, 2011.

60) S. Chai, M. Kim ve R.H. Rao, "Firms' Information Security Investment Decisions: Stock Market Evidence of Investors' Behavior", ***Decision Support Systems***, Vol.50, pp. 651-661, 2011.

61) O. Orkan Özer, "Oyun Teorisi ve Tarımda Uygulanması", ***Ankara Üniversitesi Fen Bilimleri Enstitüsü Doktora Semineri***, Ankara, 2004.

62) L. Zeshuang ve L. Jing, "Study on the Organization Information Security Investment-Decision Making Based on the Limited Strategy Game Theory Perspective", ***Second International Conference on Computational Intelligence and Natural Computing*** (CINC), 2010.

63) T. Alpcan, "Dynamic Incentives for Risk Management", ***5th IEEE International Conference on New Technologies***, Mobility and Security (NTMS), 2012.

64) J. Huan, "Optimal Investment in IS Security: A Game Theoretical Approach", Morgan State University, ***Ph.D Thesis***, 2009.

65) H. Çavuşoğlu, B. Mishra ve S. Raghunathan, "A Model for Evaluating IT Security Investments", ***Communications ACM***, Vol 47. No.7, pp.87-92, 2004.

66) J. Grossklags, "Secure or Insecure: An Economic Analysis of Security Interdependencies and Investment Types", University of Berkeley, California, ***Ph.D Thesis***, 2009.

67) P. Bommannavar, T. Alpcan ve N. Bambos, "Security Risk Management via Dynamic Games with Learning", ***IEEE International Conference on Communications (ICC)***, 2011, pp. 1–6, 2011.

68) D. Liu, Y. Ji ve V. Mookerjee, "Knowledge Sharing and Investment Decisions in Information Security", Decision Support Systems", Vol. 52, pp.95-107, 2011.

69) P.Naghizadeh ve M. Liu, "Voluntary Participation in Cyber Insurance Markets", ***Workshop on the Economics of Information Security (WEIS)***, 2014.

70) X. Gao, W. Zhong ve S. Mei, "A Differential Game Approach to Information Security Investment Under Hackers' Knowledge Dissemination", ***Operations Research Letters***, Vol.41, Issue 5, pp:421-425, September 2013.

71) A. Ashok, A. Hahn ve M. Govindarasu, "Cyber-physical security of Wide-Area Monitoring, Protection and Control in a Smart Grid Environment", ***Journal of Advanced Research***, (2014) Vol.5, pp. 481–489, 2014.we

72) A.K.İkiz ve İ.D. Kocakoç, "Bilişim Teknolojisi Projelerinde Reel Opsiyonlar", ***Dokuz Eylül Üniversitesi, Sosyal Bilimler Enstitüsü Dergisi***, Cilt:11, Sayı:4, Syf.17-51, 2009.

73) G.C. Akkaya, "Yatırım Projelerinin Değerlendirilmesinde Alternatif Bir Yöntem: Reel Opsiyonlar", ***Muhasebe ve Finansman Dergisi (MUFAD)***, Sayı 28, Syf. 172-178, Ekim 2005.

74) A. Değer, "Patent Değerlemesi ve Reel Opsiyonlar", ***Business and Economics Research Journal***, Vol.2, No.1, Syf.153-172, 2011.

75) L.A. Gordon, M.P. Loeb ve W. Lucyshyn, "Information Security Expenditures and Real Options: A Wait and See Approach", ***Computer Security Journal***, 19(2), 2003.

76) K.Tatsumi ve M.Goto, "Optimal Timing of Information Security Investment: A Real Options Approach", ***Workshop on the Economics of Information Security (WEIS)***, March 2009.

77) M. Daneva, "Applying Real Options Thinking to Information Security", ***Centre for Telematics and Information Technology (CTIT) Technical Report***, 2006.

78) H.S. Herath ve T.C. Herath, "Investments in Information Security: A Real Options Perspective with Bayesian Postaudit", ***Journal of Management Information Systems***, Vol. 25 Issue 3, p337, December 2008.

79) K.K. Kommineni ve A.Y. Babu, "A Cost-Benefit Model for an Enterprise Information Security", ***International Journal of Innovative Technology and Exploring Engineering (IJITEE)***, Vol.2, Issue 3, February 2013.

80) J.V. Brocke, G. Strouch ve C. Buddendick, "Return on Security Investments – Design Principles of Measurement Systems Based on Capital Budgeting", ***In Proceedings of ISTA 2007***. pp.21-32, 2007.

81) ENISA (European Network and Information Security Agency, "Introduction to Return on Security Investment", ***Deliverable***, December 2012.

82) H.Şentürk, C.Z.Çil ve Ş.Sağıroğlu, "Siber Güvenlik Ekonomisi Üzerine Literatür İncelemesi", ***7'nci Uluslar arası Bilgi Güvenliği ve Kriptoloji Konferansı***, ISCTURKEY 14, İstanbul, 17-18 Ekim 2014.