İŞLETMELERDE SİBER RİSKLERİN ANALİZİNDE, HARİTALANMASINDA VE DEĞERLENDİRİLMESİNDE İÇ DENETİMİN ROLÜ

Prof. Dr. Seval Kardeş SELİMOĞLU*
Mustafa Hakan SALDI**

Makale Gönderim Tarihi : 12/02/2019 / Kabul Tarihi : 26/03/2019

ÖZ

Bu çalışmanın amacı, iç denetim perspektifinden siber risklerin analiz edilmesi, haritalanması ve değerlendirilmesi için hangi tekniklerin nasıl uygulanacağı ve kullanılacağı ele alınarak anlatılmıştır. Çalışmanın içeriği itibari ile işletmelerde hangi tip siber risklerle karşılaşılabileceği ve bunlara nasıl önlem alınacağı üzerine detaylı incelemeler yapılarak, iç denetimin, siber risklerin kontrolünde üstlendiği görevlerini neler olabileceği ele alınarak araştırılmıştır.

Çalışmanın esas amacına paralel olarak, bilgi teknolojilerinde pratik olarak kullanılan metotlar örnek olaylar ile açıklanmıştır. Özellikle, siber risklerin analizinde uygulanan niceliksel modeller teorik çerçeveden aktarılmaya çalışılarak, iç denetimin güncel hayattaki rolü ile ilişkilendirilmesi hedeflenmiştir.

Sonuç olarak, iç denetimin işletmelerdeki önemi ve rolü de teknolojik gelişmeler ile beraber değişime uğrarken, operasyonel ve yönetsel süreçlerdeki faaliyet alanları da genişlemektedir. Bu bağlamda, siber risklere karşı önlemlerin alınmasında iç denetimin rolü de en az bilgi teknolojilerininki kadar büyüktür.

Anahtar Kelimeler: Siber Riskler, Analiz Metotları, Risk Haritaları, İç Denetim

JEL Kods: M42,M49

* Prof. Dr. Seval Kardeş Selimoğlu, İİBF İşletme Bölümü, Muhasebe ve Finansman Ana Bilim Dalı Öğretim Üyesi sselimoğlu@anadolu.edu.tr, https://orcid.org/0000-0003-1185-9980

** Mustafa Hakan Saldı, Anadolu Üniversitesi Sosyal Bilimler Enstitüsü İngilizce İşletme Doktora Programı Öğrencisi, Endüstri Mühendisi hamusaldi@hotmail.com, https://orcid.org/0000-0001-5043-4606

THE ROLE OF INTERNAL AUDIT: ANALYSIS, MAPPING AND ASSESSMENT OF CYBER RISKS IN ENTERPRISES

ABSTRACT

The article is tried to transfer from the internal audit perspective on how techniques are used for analyzing, mapping and assessing cyber risks. With the content of the study, the missions of internal auditing on control of cyber risks are investigated by doing in-depth examinations on what types of cyber risks can be encountered in businesses and how to take precautions to these risks.

In parallel with the main purpose of the study, the methods used in information technologies are described with actual events. Particularly, the quantitative models applied in the analysis of cyber risks are aimed to be transferred from theoretical framework and associated with the role of internal control in the current llife.

As a result, the role of internal control in the enterprises is transforming with technological developments and its' activities on the operational and managerial processes are expanding. Because of the mentioned reasons, the role of internal control in taking actions against cyber risks is as much as information technology.

Keywords: Cyber Risks, Analysis Methods, Risk Maps, Internal Auditing

JEL Codes: M42, M49

1. GİRİŞ

Bu çalışmanın amacı, işletmelerde sıklıkla karşılaşılan siber risklerin analizinde, haritalanmasında ve değerlendirilmesinde kullanılan uygulamaların, iç denetimin geleneksel rolü üzerindeki etkilerini doğrudan ve dolaylı yollarla araştırarak, geleceğe yönelik sonuçlar çıkarmaktır. Çalışma, iç denetimin işletmelerdeki rolünün, teknoloji ile nasıl şekillendiğinin ve değişime uğradığının güncel yaklaşımlar ile aktarılması bakımından ön plana çıkmaktadır.

Öncelikle, literatür incelemesi yapılarak geçmiş çalışmaların içerikleri ve bulguları araştırılmıştır. Daha sonra, riskin genel tanımı teorik açıdan anlatılarak, siber çevrede hangi faktörlerin önemli rol oynadığı kavramsal pencereden gösterilmiştir. Siber risk kavramı, istatistiksel veriler ve güncel vakalarla açıklanmıştır.

Siber risklerin analizleri üzerine öne sürülen teorik modeller incelenerek, bu metotların güncel koşullara nasıl uyarlandığı gözlemlenmiştir. Risk matrislerinin veya ısı haritalarının siber çevrede nasıl kullanıldığı örnek olaylar ile birlikte gösterilmiştir. Son bölümde ise siber çevrede iç denetimin hangi rollere sahip olduğu açıklanmıştır.

2.LİTERATÜR İNCELEMESİ

Tablo 1: Literatür Taraması

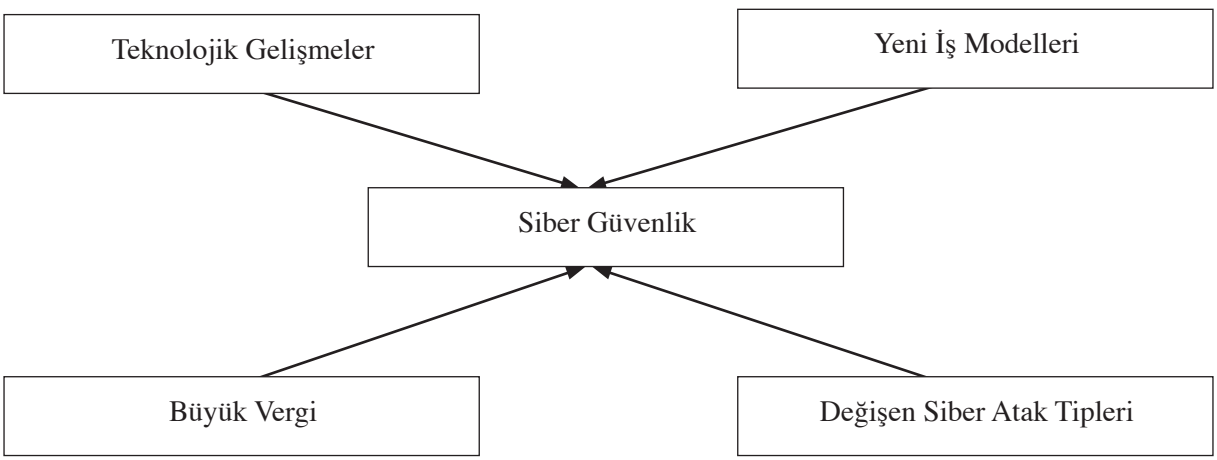
Yazar ve Yıl	Makale Adı	Konu Kapsam	Sonuç
Ralston, Graham ve Hieb(2007)	SCADA Ve DCS Ağları İçin Siber Güvenlik Risk Değerlendirmesi(Cyber Security Risk Assessment For SCADA And DCS Networks)	SCADA ve DCS ağlarındaki risklerin değerlendirilmesi için olasılık ve etki hesapları konuları temel alınmıştır.	FTA, ETA ve FEMA metodları kullanılarak herhangi bir siber tehditin ortaya çıkma olasılığı ve etkisi değerlendirilmiştir.
Spoonamore(2008)	CCLIF: Siber Operasyonların ve BT Mimarileri Riskinin Değerlendirilmesi İçin Nicel Bir Metodoloji(CCLIF: A Quantified Methodology System To Assess Risk Of IT Architectures And Cyber Operations)	CCLIF sürecinin organizasyonlardaki elektronik güvenlik uygulamalarında kullanımı konu edinilmiştir.	CCLIF süreci organizasyonların e-güvenlik fonksiyonlarına uyum açısından gerekli karakteristiklere sahiptir.
Guinta ve Frantz-ve(2010)	Siber Güvenlik Ve İşletmeler İçin Eleştirellik, Savunmasızlık Ve Risk Mantık Analizi Metodolojisi(Critically/Vulnerability/Risk Logic Analysis Methodology For Business Enterprise And Cyber Security)	Bilgi teknolojileri kaynaklı risklerin değerlendirilmesi matematiksel bir modele dayalı olarak yapılmıştır.	Önerilen metod ile risklerin tanımlanması, nicelikselleştirilmesi ve kabul edilebilir olup olmadığı anlaşılmıştır.
Kayrak(2012)	Bilgi Kriterleri Çerçevesinde Bilişim Teknolojileri Denetimi	Bilgi teknolojileri, denetimi ve yönetişimi konuları değerlendirilmiştir.	Bilgi kriterlerinin bilgi teknolojilerinin denetimindeki rolü ortaya çıkarılmıştır.
Yılmaz ve Sağıroğlu(2013)	Siber Güvenlik Risk Analizi, Tehdit ve Hazırlık Seviyeleri	Siber güvenlik kapsamında yer alan evrensel kurallar, siber kaynakların risk analizi, tehdit ve hazırlık seviyeleri incelenmiştir.	Siber güvenliğin sağlanabilmesi için bilgi varlıkları üzerinde risk analizleri yapılmalı ve siber tehdit araçlarına karşı hazırlıklı olunmalıdır.
Topaloğlu, 2013	Sosyal Güvenlik Suistimallerinin Tespiti ve Önlenmesi İçin Risk Analizi Ve Sürekli Denetim Yöntemleri	Gelişen teknoloji ve ekonomik aktiviteler ile birlikte denetim yaklaşımlarının reaktiften proaktife nasıl dönüşmeye başladığı değerlendirilmektedir.	Veri hacmindeki artışa bağlı olarak risk analizleri doğrultusunda denetim yöntemleri incelenmiştir.
Mukhopadhyay, Chatterjee, Saha, Mahanti ve Sadhukhan(2013)	Siber-Risk Karar Modelleri: BT'yi Güvence Altına Almak Veya Almamak(Cyber-Risk Decision Models: To Insure IT or Not)	Siber sigorta ürünlerinin organizasyonlara uygunluğuna ilişkin modeller önerilmektedir.	Siber risk sigortacılarına destek olmak ve daha verimli ürünler geliştirmek için UBPP modeli önerilmiştir.
Christiansen, D'angona ve Bell(2014)	Bilgi Teknolojisi Riskini Görüntelemek, Yönetmek ve Değerlendirmek İçin Metod Ve Sistem(Method And System For Assessing, Managing And Monitoring Information Technology Risk)	Veritabanları üzerinden bilgi teknolojileri risk faktörlerinin algılanması konusu üzerinde durulmuştur.	Bilgi teknolojilerinde ortaya çıkabilecek risklerin kontrol edilmesine yönelik bir metod önerilmiştir.
Kurnaz ve Dindaroğlu(2015)	İç Denetim Ve Bilgi Güvenliği İlişkisi: Bölgesel Bir Araştırma	İç denetim ve bilgi güvenliği fonksiyonları arasındaki ilişkinin doğasını etkileyen unsurların ortaya çıkarılması konusu değerlendirilmiştir.	İç denetim ve bilgi güvenliği arasındaki etkileşimin sonucunda tam güvenliğin sağlanması kesin olarak söylenemez.
Kurt ve Uysal, 2015	Siber Riskler ve COSO İç Kontrol Bütünleşik Çerçevesi	İşletmelerdeki risklerin çeşitliliği bilgi teknolojilerindeki gelişmelere bağlı olarak artış göstermektedir ve bu nedenle bu risklerin kontrol edilmesi konusu ön plana çıkmaktadır.	Bilgi güvenliğinin sağlanmasında COSO kurumsal risk yönetimi bütünleşik çerçevesinin siber tehditlere karşı rehberlik ettiği vurgulanmıştır.
Uludağ(2017)	Değişen Risk Algısı Ve İç Denetim	Değişen risk algısı iç denetim perspektifinden değerlendirilmiştir.	Değişen koşullar ile birlikte iç denetim açısından risk kavramına ilişkin unsurlar incelenerek risk odaklı iç denetim kavramı ortaya konmuştur.
Öztürk(2018)	Siber Saldırılar, Siber Güvenlik Denetimleri Ve Bütüncül Bir Denetim Modeli Önerisi	Siber güvenlik denetimindeki tüm süreçler bütüncül bir yaklaşımla değerlendirilerek bir model dahilinde gösterilmeye çalışılmıştır.	Önerilen denetim modeli ile birlikte denetim çevresine etki eden iç ve dış faktörler, siber saldırılar ve tehditler açıklanmıştır.

Literatür incelemesinde ortaya çıkan bulgulara göre siber risklerin analizi ve değerlendirilmesi iç denetime yeni teknikler ve bakış açıları kazandırmıştır. Özellikle, bilgisayar bilimleri kapsamında önerilen metotlar ve modeller iç denetim mesleğini profesyonel olarak yapan şahıslara ve kurumlara daha analitik boyutlar kazandırabilecektir.

3. SİBER RİSK TANIMI VE KAPSAMI

Risk, işletmelerin misyonlarına ve stratejik amaçlarına ulaşmak için gerçekleştirdiği fonksiyonların etkinliğindeki sapma potansiyeli olarak değerlendirilebilir. Risk tahmin edilebilir değildir, gelecek ile ilgili belirsizliği ve beklenen sonuçlardan sapma ihtimalini temsil eder. Stratejik, operasyonel, finansal ve yasal risklerin analizleri iç denetim ekibinin geleneksel sorumlulukları arasında yer alırken, dijitalleşme doğrultusunda ortaya çıkan yenilikler ile birlikte bu görevlere siber risklerin analizi ve değerlendirilmesi de eklenmiştir.

Siber güvenlik kavramı, enformasyon sistemleri kapsamında yer alan veri kümelerinin ve programların risklerden ve tehditlerden korunması amacıyla ortaya çıkmıştır. Enformasyon sistemlerinin işletmelerde anahtar role sahip olmasının altında dijital olarak depolanan, işlenen ve transfer edilen bilginin güvenliği ve denetlenmesi yer almaktadır. Modern çağın koşullarında organizasyonlar açısından en önemli varlığın bilgi olduğu tartışılmaz bir unsur haline gelmiştir. Bu nedenle, teknolojik uygulamalarla daha kıymetli bir araca dönüşen bilgi her daim çeşitli tehditlerle karşı karşıya kalabilmektedir. Bu tehditlerin amacı genel olarak enformasyon sistemlerindeki verileri uygunsuz olarak elde etmeye ve bozmaya yönelik olmaktadır. Siber tehditlerin başında bilgisayar ve yazılım korsanlığı gelmektedir.



Şekil 1: Siber Çevre

Kaynak: International Professional Practices Framework Global Technology Audit Guide

Temel olarak, enformasyon güvenliği verilere erişilme, verileri işleme ve verilerin kayıt altında tutulması fonksiyonlarını kapsamaktadır. Kişisel kullanıcılar açısından durum, sadece bilgi güvenliği şifreleri, güvenlik duvarları ve anti-virüs programları ile sınırlıdır. Ancak, diğer taraftan, işletmelerin veya kurumların veri güvenliği mekanizmaları bilgi işlem cihazları, sunucular, yönlendiriciler, telekomünikasyon ekipmanları ve birbirleriyle elektronik olarak bağlı makineleri bütünüyle kapsamaktadır.

Bilhassa, işletmeler açısından verilerin güvenliğinin sağlanmasında karşılaşılan siber risklerin ortaya çıkardığı tahribat geri dönüşü olmayan finansal kayıplara ve piyasa itibarının ciddi anlamda zedelenmesine neden olmaktadır. Bundan dolayı, mevcut ve gelişmekte olan siber risklerin analiz edilerek değerlendirilmesi iç denetim ekiplerini önemli oranda ilgilendirmektedir.

Ayrıca, dinamik olarak değişen teknoloji çevresi iç denetim mesleğine de çeşitli sorumluluklar yüklemektedir. Dijital ortamda korunan verilerin risklere karşı güvence altında tutulmasını sağlamak amacıyla çeşitli risk analizi araçları geliştirilmektedir. Stratejik planlama, proje yönetimi, rutin operasyonlar ve kaynaklama faaliyetleri doğrultusunda iç denetim kapsamına giren risk analizi teknikleri işletmelerde uygulanmaktadır.

Aslında, şirketler iş akışlarını ve süreçlerini dijital ortamda denetlemek için algoritmalar vasıtasıyla siber fiziksel sistemleri ve akıllı sensörleri kullanarak siber risklerin seviyesini de artırmaktadırlar. Bu nedenle, fabrikaların dört duvarı arasında yer alan fiziksel makineler, araçlar ve robotlar tehditlere karşı daha kırılgan bir hale gelmektedirler.

Siber riskler dijital dönüşümün yaşanmakta olduğu bu dönemde işletmeler tarafından en ciddi tehdit kaynakları olarak algılanmaktadır. Şirketler her geçen gün yeni siber ataklara maruz kalarak hem maddi hem de manevi açıdan büyük kayıplara uğramaktadırlar. Siber ataklar, organizasyonların veya şahısların bilgi ve iletişim teknolojisi araçlarına ve uygulamalarına doğrudan veya dolaylı yollarla gerçekleştirilen, sistemler içerisinde korunan verilerin bütünselliğine, gizliliğine ve mevcudiyetine tehdit unsuru oluşturan saldırıları kapsamaktadırlar.

Tablo 2: Risk Dağılımları

2018 Yılında Orta Ölçekli Şirketlerin Önemsediği En Ciddi 5 Risk		
Sıra	Risk	Yüzde
1	Siber Vakalar(Örn. Siber Suçlar, BT Hataları, Veri İhlalleri)	39%
2	İş Aksamaları	37%
3	Doğal Felaketler(Örn. Fırtına, Sel, Deprem)	32%
4	Yangın, Patlama	23%
5	Piyasa Gelişmeleri	21%

Kaynak: Allianz Global Corporate&Specialty

Siber ataklar nedeniyle ortaya çıkan risk senaryoları sonucunda kritik verilerin kaybı ile birlikte marka değerinin azalması, müşterilerin çekilmesi ve hisse fiyatlarının düşmesi gibi durumlarla karşılaşılır. Orta ölçekli şirketler kapsamında yapılan Allianz Global'in yaptığı araştırmaya göre, 2017 yılına kıyasla 2018 yılında siber risklere karşı duyulan endişenin oranı %29'lardan %39'lara kadar ulaşmıştır. Bu durum da tehlikenin boyutunun önem derecesini niceliksel olarak açıklamaktadır.

Tablo 3: Siber Saldırı Maliyetleri

Ağustos 2017 İtibariyle Gelişmiş Ekonomiler Kapsamında Seçilen Ülkelerin Yıllık Ortalama Siber Atak Maliyetleri(Milyon Amerikan Doları)	
Birleşmiş Milletler	21,22
Almanya	11,15
Japonya	10,45
Birleşik Krallık	8,74
Fransa	7,9
İtalya	6,73
Avustralya	5,41

Kaynak: Statista

2017 yılının Ağustos ayı itibariyle Birleşmiş Milletler'in siber ataklar sonucunda karşılaştığı maliyet 2.122.000.000 Amerikan doları olmuştur. Bu miktar Amerika'nın gayri safi yurt içi hasılasının yaklaşık olarak 0,0001'lik kısmına denk gelmektedir. Bu oran ihmal edilebilecek kadar küçük olsa da siber atakların maddi olmayan varlıkları uğrattığı hasar dikkate alınmamıştır. Bunlar, önceden de bahsedildiği üzere müşteri kayıpları, marka güvenilirliğinin ve değerinin azalması gibi faktörler ile ortaya çıkan, proaktif olarak hesaplanması neredeyse olanaksız ve doğrusal olmayan biçimde değişkenlik gösteren bilançodaki itibar(goodwill) kalemleridir.

Tablo 4: Siber Risklerin Sonuçları

Siber Riskler Nedeniyle İşletmeleri Kayba Uğratan Farklı Vakalar	
Fikri mülkiyet hırsızlığı	Fikri mülkiyet varlığının değerinin kaybolması sonucunda pazar payının azalması ve gelirlerin düşmesi
İşlerin aksaması	Siber saldırılar sonucunda bilgi sistemlerinde oluşan hasarlar ve arızalar nedeniyle yaşanan ekstra giderler ve zararlar
Verilerin ve programların bozulması	Veri kümelerinin ve programların bozulması sonucu ortaya çıkan giderler

Siber yağmacılık	Siber yağmacılık nedeniyle verilerin dışarı sızdırılması sonucu karşılaşılan kurtulma giderleri
Siber hileler	Organizasyonların maddi ve manevi haklarını ihlal ederek varlıklarına gasp girişiminde bulunulan faaliyetler sonucunda karşılaşılan kayıplar
Gizlilik etkinliği ihlali	Gizlilik etkinliği ihlali sonucu yasal çevreden alınan cezalar
Ağ hataları kaynaklı yükümlülükler	Siber saldırılar nedeniyle şebekelerde hasarların oluşması ve beklenmedik yükümlülüklerle karşılaşılması
İtibar etkisi	Siber güvenlik mekanizmasının ihale uğraması sonucunda eldeki müşterilerin korunamaması ve gelir kaybının yaşanması
Fiziksel kıymet hasarı	Siber ataklar sonucunda ortaya çıkan ve fiziksel varlıklarda gözlenen birincil şahıs kayıpları
Ölüm ve bedensel yaralanmalar	Siber ataklar nedeniyle üçüncül şahıslarda gözlenen ölüm ve bedensel yaralanmalar
Olay araştırmaları ve maliyetleri	Siber saldırılar sonucu ortaya çıkan kazaların ve ihlallerin araştırılması için gereken finansal kaynaklar

Kaynak: MMC Cyber Handbook 2018

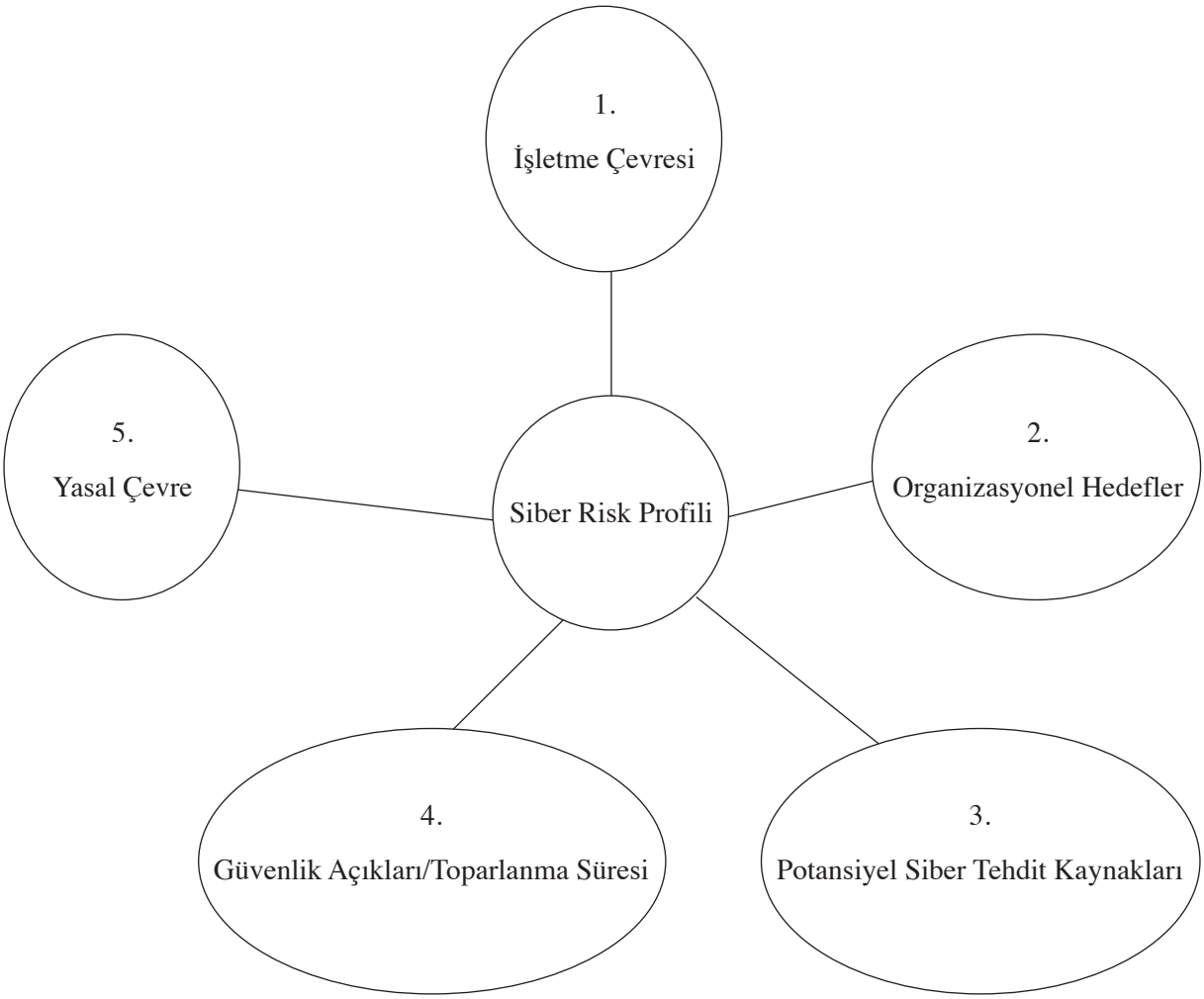
Siber saldırılar nedeniyle ortaya çıkan ve tablo üçte yer alan fırsat maliyetlerinin ulusal ekonomileri uğrattığı doğrudan kayıplar raporlarda bahsi geçen miktarlardan bir hayli fazladır. Örneğin, herhangi bir işletmede gizlilik ihlali dolayısıyla müşteri güveninin ve sadakatinin sarsılması sonucunda hisse fiyatlarının düşmesi ve rakiplerin müşterileri kendine çekmesi ile oluşan kayıplar ve zararlar hiçbir şekilde göz ardı edilemez. Ayrıca, siber riskler sonucunda ülkelerin uğradığı kayıpları ulusal bazda incelemek net sonuçlar çıkarmayacaktır, çünkü siber tehditlerin esas amacı küresel ekonomiyi zedelemektir.

İşletmeler dijital sistemlerindeki kırılganlıkları değerlendirirken konuya sadece iş akışlarındaki teknolojik parçalar ve yazılımlar açısından bakmadan, insan faktörünü de konuya dahil edip, gerçekçi yaklaşımları kullanarak bütünsel risk tespitleri ve analizlerinde bulunmalıdırlar.

4. SİBER RİSKLERİN ANALİZ YÖNTEMLERİ

Organizasyonlar siber risklerin tespit ve analiz edilmesinde çevik ve yapısal yaklaşımları tercih etmektedirler. İşletmelerin siber risklerden korunmaları ve bu riskleri bertaraf etmeleri için öncelikle kendi kurum kültürlerine ve varlıklarına uygun risk profilleri oluşturmaları daha etkin ve uygulanabilir tekniklerin geliştirilebilmesine olanak sağlamaktadır. Bu nedenle, işletmenin iç ve dış çevresi, aktif olduğu sektörler, dijital sistemlere olan bağlılığı, değer zinciri içerisindeki hedefleri, teknik ve insan kaynaklı güvenlik açıkları, siber riskler sonrasındaki toparlanma seviyesi, herhangi bir siber saldırı sonucunda iş-

lerin normal seviyesine gelme periyodu ve siber güvenlik çatısı altındaki yasal gereksinimleri karşılama yeteneği risk profilinin tespit edilmesinde dikkate alınacak konulardır.



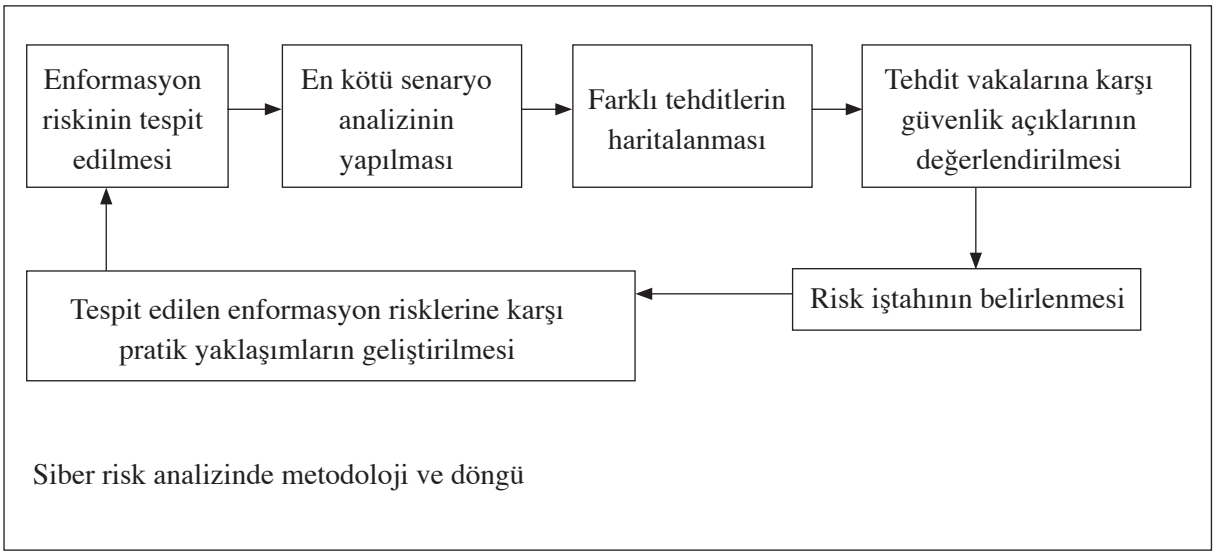
Şekil 2: Siber Risk Profiline Etki Eden Faktörler

Kaynak: Deloitte

5 görünümden tespit edilen risk profili doğrultusunda organizasyonun kabul edebileceği risk miktarı da belirlenerek siber güvenlik ölçümleri yapılır. Ancak tabi ki hiçbir koşulda ve süreçte %100 güvenlik sağlanamayacaktır ve her zaman kabul edilebilir bir risk seviyesi olacaktır.

Dijital platformlardaki verilerin gizliliği, bütünselliği ve mevcudiyeti siber risklerin analiz edilmesi ile güvence altına alınmaya çalışılır. Bilgi teknolojilerinde risklerin analizleri ve değerlendirmeleri hem kantitatif hem de kalitatif teknikler ile yapılabilmektedir. Yıllık kayıp beklentisi tekniği(Annual Loss

Expected)(ALE), Fisher yöntemleri, Courtney metotları, bilgi güvenliği risk analizi metodu(Information Security Risk Analysis Method)(ISRAM) ve diğer türev oranları kantitatif yöntemler olarak risk analizlerinde kullanılabilmektedir. Merkezi bilgisayar ve iletişim ajansı risk analiz ve yönetim metodu(Central Computer and Telecommunications Agency Risk Analysis and Management Method)(CRAMM), NIST SP 800-30 yöntemi, hata modu ve etkileri analizi (Failure Mode and Effects Analysis)(FMEA) ile hata modu ve etkileri kritiklik analizi (Failue Mode and Effects Criticality Analysis)(FMECA) kalitatif metotlar olarak risk analizlerinde uygulanabilmektedir(Rot, 2008: p.9).



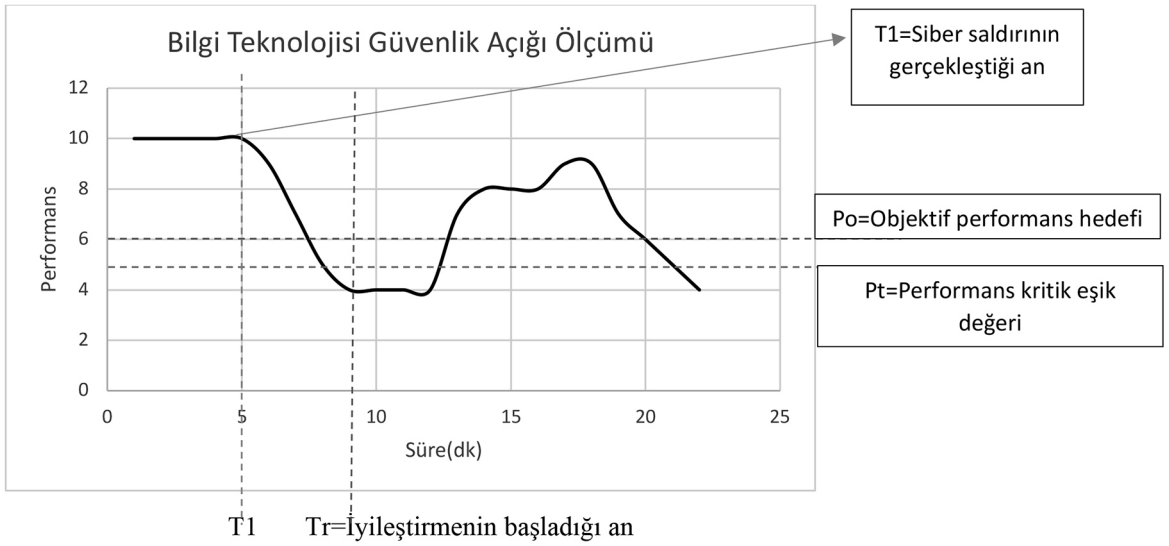
Şekil 3: Siber Risk Analizi Yapısal Modeli

Kaynak: Marsh&McLennan

Siber risklerin niceliksel değişkenlere dönüştürülmesinde, belirli bir zaman periyodu içerisinde maruz kalınan siber saldırıların şiddeti ve ortaya çıkma olasılığı kullanılır. Örneğin, bir işletmenin gelecek 12 ay içerisinde bir siber saldırıya maruz kalması olasılığı yüzde bir ve siber saldırı sonucu karşılaşacağı maliyet 10 milyon dolar iken, benzer şekilde karşılaşacağı daha ciddi bir siber saldırının ortaya çıkması olasılığı binde bir ve saldırı sonucu uğrayacağı kayıp ise 100 milyon dolar olabilmektedir. Daha açık bir ifadeyle saldırının ortaya çıkma olasılığı veya karşılaşılma sıklığı ile meydana getirdiği tahribat ters orantılı olarak gelişmektedir. Bu durum da riskin geleneksel formülü kapsamındaki; herhangi bir riskin ortaya çıkma olasılığı ile etkisinin çarpılması sonucunda ortaya çıkan değerin dengeli olmasını sağlamaktadır.

Herhangi bir siber saldırının şiddeti ve ortaya çıkma olasılığı, aslında işletmelerin risk profillerini oluşturarak, frekans(sıklık)-şiddet dağılımları veya kayıp derece olasılık eğrileri ile siber risklerin ölçülmesini sağlamaktadırlar. Bu sayede risk yöneticileri siber risklerin işletmeler açısından hangi anlamlara geldiklerini nicel olarak ölçebilmektedirler. Ayrıca, risk profili, herhangi bir işletmenin karşılaşabileceği

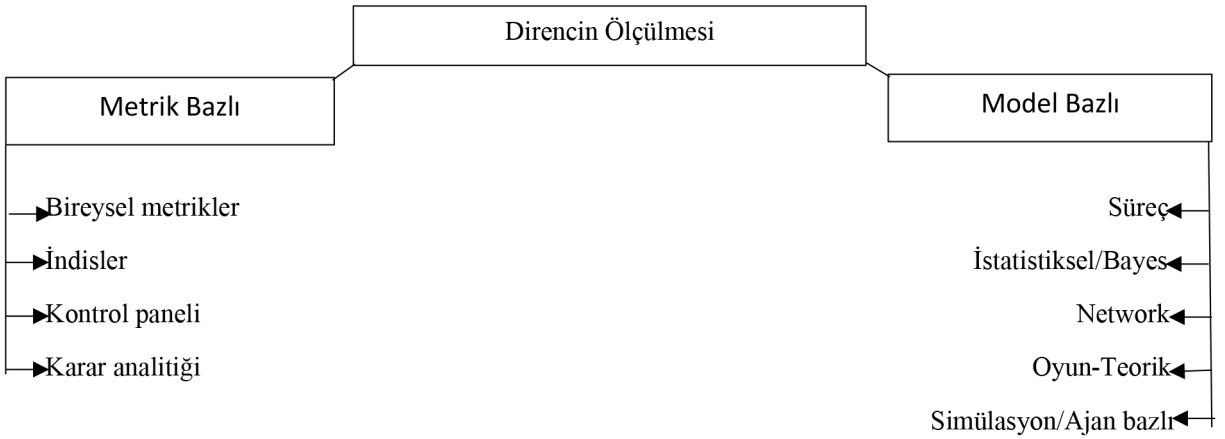
farklı siber saldırıların olasılığının ve şiddetinin hesaba katılmasına ve ortalama kayıp oranının analiz edilmesine olanak sağlamaktadır. Siber risklere maruz kalınması sonucunda beklenen kayıp miktarı proaktif bir yaklaşımla belirlenir ve bu maliyetleri karşılayacak tasarruflar önceden sağlanarak, risk toleransı oluşturulur.



Şekil 4: Metrik bazlı bilgi teknolojileri performans eğrisi

Kaynak: Cyber Resilience of Systems and Networks

Herhangi bir işletmenin siber saldırılara karşı direncini ve bağışıklığını gösteren bir vaka figür 2'de gösterilmiştir. Bu vakada esas amaç riskin etkisinin süreç açısından incelenmesini sağlamak ve siber riskin ölçümünü nicel değişkenler ile ifade etmektir. Spesifik olarak T1 bozucu eylemin ortaya çıkış anını belirtmektedir. Sistem operatörü çoğu zaman bu anı önceden bilemez veya tahmin edemez, bu durum da siber güvenlik mekanizmalarının en zayıf olduğu noktadır. Siber riskin analizi yapılırken dijital sistemlerdeki performansın düşmeye başladığı an orijin olarak alınır. Tr anından itibaren ise işletmenin siber güvenlik sistemi devreye girerek dijital operasyonların iyileştirilmesi sağlanmaktadır. Bu gibi vakaların analizlerinin elde edilmesinde siber saldırının gerçekleştiği an, siber atak sonrasında objektif performans hedefinin altına düşmesi için geçen süre ile kritik eşik performans değerinin altına inmesi için geçen zaman ve sistemin tekrar eski performans seviyelerine ulaşması için geçen periyod değişkenleri kullanılmaktadır. Bu yöntemle işletmelerin siber saldırılara karşı toparlanma süresi tespit edilmiş olur. Özetle, siber risklerin analizleri bu vakada kullanılan performans eğrileri ile yapılabilmektedir.



Şekil 5: Siber risklerin analizlerinde kullanılan teknikler

Kaynak: Cyber Resilience of Systems and Networks

Siber risklerin analiz edilmesinde kullanılan yöntemlerin esas amacı bilgi sistemlerinin bu risklere karşı oluşturduğu bağışıklığı tespit etmektir. Metrik bazlı yaklaşımlar sistem parçalarının bireysel özelliklerini veya sistem performansının bütününü değerlendirmeye yönelik olarak geliştirilmişken, model bazlı yaklaşımlar enformasyon teknolojisinin karşılaşabileceği siber riskleri sistem konfigürasyonu modellemeleri ve senaryo analizleri ile belirlemeye çalışmaktadır. Bu bağlamda model bazlı teknikler daha öngörülü yaklaşımları kullanmaktadırlar.

Metrik metotlar, uygulandığı sistemler için hayati öneme sahip veriler temin ederlerken, bazı araştırmacılar ve meslek sahibi kişiler tarafından ise ölçü ve metrik kavramları ayrı kavramlar olarak değerlendirilmekte ve hatta performans ölçümlerinin aslında birer metrik olduğunu iddia eden şahıslara da rastlanılmaktadır(Collier et al. 2016: p.7). Siber atakların şiddetine ve ortaya çıkma olasılığına yönelik evrensel olarak uygulanabilir metriklerin eksikliği ve siber risklere bağlı iş aksamaları ile ilgili değer sistemlerinin biçimselleştirilmesinde karşılaşılan problemler metrik bazlı metodolojilerin kullanım alanını kısıtlamaktadır.

Model bazlı yaklaşımlar ise matematiksel ve fiziksel kavramlar kullanılarak bilgi teknolojisi sisteminin direncinin tanımlandığı, gerçek dünyanın temsiline odaklanılarak risk analizlerinin yapıldığı tekniklerdir. Süreç modellemesi, siber riske maruz kalınmasından, tepki verilmesine ve sistemin kabul edilebilir performansına ulaşmasına kadar geçen evreleri detaylı bir biçimde incelemek için etkin bir tekniktir. İstatistiksel yaklaşımlar, sistem performansının ve direncinin ölçülmesinde yüksek hacimli veri potansiyelini kullanmaktadır. Bayes modeli, süreçleri ve istatistiksel metotları birleştirir. Network modelleri sistem içerisinde birbiriyle bağlantılı düğümlerin, siber riskin ortaya çıkması ile gösterdiği davranışları siber alanda denetlemektedir. Alternatif olarak, oyun, teorik/ajan-bazlı yaklaşımlar ise tanımlanmış kural kümelerine göre sistemin performansını kontrol etmektedirler. Ancak, bu gibi teknikler sınırlı

koşullarda ve sistem iyileştirilmesinde kullanılacak modellemenin net ve kesin olduğu durumlarda uygulanabilmektedir(Ganin et al. 2016: p.8, 2017b: p.2; Gao et al. 2016: p.5; Cohen et al. 2000: p.15).

5. SİBER RİSKLERİN HARİTALANMASI VE DEĞERLENDİRİLMESİ

Diğer alanlarda olduğu gibi, bir bilgi teknolojisi sisteminin herhangi bir siber riske maruz kalması ardından iyileşme kapasitesi o sistemin tehditlere karşı gösterdiği direnci ve bağışıklığı temsil etmektedir. İngilizce "cyber resilience" olarak isimlendirilen bu kavram işletmelerin enformasyon sistemlerinin siber risklere karşı geliştirdiği iyileşme periyodunun ve performansının metrik değişkenler olarak incelenmesini sağlamaktadır. Örneğin, A ve B adlarında aynı performansı gösteren iki eşit sistemin olduğu varsayımı yapılsın. Aynı siber saldırıya maruz kalan bu iki sistemden A objektif performans seviyesine t1 ve B ise t2 süre sonunda erişebilsin. Eğer t1<t2 ise A sisteminin "cyber resilience" seviyesi B'ninkinden daha iyi olarak algılanmaktadır.

Genel olarak, risk herhangi bir durum içindeki tehdit veya tehlike olarak değerlendirilir. Eğer, risk uygun yöntemler ile analiz edilerek yönetilebiliyorsa, sistemin güvenli koşullara ulaşması gerçekleştirilebilir. Ayrıca, sistemlerin karşılaştığı beklenmedik vakalar sonucunda yeniden optimal performansın yakalanması için gereken yetkinlik, riskin yönetilebilme kapasitesini de göstermektedir. Bilgi teknolojisi sistemlerinde de bahsedilen kavramlar uygulanabilmektedir. Özellikle, siber saldırının öncesindeki ve sonrasındaki sistem performansları ile sistemin çevikliği arasındaki ilişki siber riskin nasıl kontrol edildiğinin göstergeleridir.

Geleneksel olarak riskin değerlendirilmesinde geniş ölçekli olarak kullanılan formül "risk=tehdit*güvenlik açığı*sonuç" olarak belirlenmiştir. Risk analizinin tanımında adı geçen tehditlerin standart açıklamaları, NIST SP 800-53(Birleşmiş Milletler kapsamında yayını gerçekleştirilen ve ulusal güvenlik için dizayn edilen tüm federal enformasyon sistemlerinin güvenliğini korumak için öneriler getiren bildirgedir.) içerisinde belirtildiği gibi siber saldırı ihtimali, etkisi ve güvenlik açığı parametreleri üzerinden değerlendirilmiştir. Eğer siber risk ifadesi altında geçen tehditlerin olasılığı ve şiddeti nicel olarak belirlenebiliyorsa, risk değerlendirme matrisleri veya ısı haritaları siber risklerin analizlerinde kullanılabilmektedir.

Tablo 5: Siber Risk Haritası

Beş Ölçekli Risk Hesaplama Isı Haritası			**Siber Riskin Etkisi**				
			Çok Düşük	Düşük	Orta	Yüksek	Çok Yüksek
			1	2	3	4	5
Siber Risk Olasılığı	Çok Yüksek	5	5	10	15	20	25
	Yüksek	4	4	8	12	16	20
	Orta	3	3	6	9	12	15
	Düşük	2	2	4	6	8	10
	Çok Düşük	1	1	2	3	4	5

Kaynak: Risk Centric Threat Modeling(Process for Attack Simulation and Threat Analysis)

Örnek olarak gösterilen risk haritasında, siber riskin olasılığı ve etkisinin çarpımı sonucu elde edilen niceliksel değişkenler bilgi sisteminde meydana gelebilecek kaybın boyutunu ifade etmektedir. Siber saldırılara karşı alınacak önlemler değerlendirilirken ısı haritalarındaki renkler kullanılır. Burada kullanılan haritada kırmızı renk 9'dan yüksek olan değerleri temsil etmektedir.

Siber güvenlik uygulamalarında deneysel olarak kullanılan bir diğer risk formülü ise tehdit olasılığı, güvenlik açığı ve siber atağa maruz kalan işletme varlığının değeri parametrelerini kapsamaktadır.

Risk=Tehdit olasılığı*Güvenlik Açığı*Varlık Değeri

Formülde yer alan varlık değeri parametresi işletmenin herhangi bir datasının kaybolması, bozulması veya el değiştirmesi sonucu ortaya çıkabilecek hasarı temsil etmektedir.

Tablo 6: Varlık Değeri Bazlı Siber Risk Haritası

Tehdit-Güvenlik Açığı-Varlık Risk Hesaplama Isı Haritası	**Siber Tehdit Olasılığı**	Düşük			Orta			Yüksek		
	İstismar Seviyesi	Düşük	Orta	Yüksek	Düşük	Orta	Yüksek	Düşük	Orta	Yüksek
Varlık Değeri	Düşük	0	1	2	1	2	3	2	3	4
	Orta	1	2	3	2	3	4	3	4	5
	Yüksek	2	3	4	3	4	5	4	5	6
	Çok Yüksek	3	4	5	4	5	6	5	6	7
	Kritik	4	5	6	5	6	7	6	7	8

Kaynak: Risk Centric Threat Modeling(Process for Attack Simulation and Threat Analysis)

Tablo 7'de gösterilen siber risk haritası modelinde üç değişken ile analizler yapılabilmektedir. İstismar seviyesi veya güvenlik açığı olarak da bilinen parametrenin metrik dönüşümü herhangi bir işletmenin bilgi varlıklarının gizliliği, bütünselliği ve mevcudiyeti üzerinde tahribat unsuru oluşturabilecek davranışlar ve insan etmeni hesaba katılarak elde edilmektedir. Varlık değerlerinin skalası ise herkesçe bilinen/umumi(düşük), kuruma özel(orta), gizli/hassas(yüksek), kişisel olarak tanımlanabilir bilgi(çok yüksek) ve hizmete özel/çok gizli(kritik) olarak değerlendirmeye alınmıştır.

İşletmeler için bilgi teknolojisi uygulamalarının kritikliği de diğer siber risklerin değerlendirilmesinde incelenen bir diğer önemli faktördür. Örneğin, finansal hizmet amacıyla geliştirilen web tabanlı uygulamanın işlevsellik açısından taşıdığı mali değer uygulama üzerinden gerçekleştirilen finansal işlemlerin boyutu ile belirlenebilir.

6. İÇ DENETİMİN SİBER RİSKLERİN ANALİZİNDE, HARİTALANMASINDA VE DEĞERLENDİRİLMESİNDE ROLÜ

Kuruluşların yönetimleri, iş stratejilerini geliştirmek ve sürdürmek amacıyla hedeflerini açıkça tanımlamak zorundadırlar. Denetim perspektifinden ise, operasyonların yönlendirildiği işletme süreçlerinin

kontrol edilmesinde birincil rol oynayan standartlar ve politikalar takip edilerek sürekli analizler ve değerlendirmeler ile gözlemlenmelidir. Bu nedenle, organizasyonel hedeflerin ve stratejik amaçların açık ve net bir biçimde ifade edilmesi daha verimli ve uygun denetim aktivitelerinin oluşmasını sağlamaktadır. Özellikle, her işletmede, yönetimlerin ana görevi standartların tanımlanması ve kurumun yapısına entegre edilmesidir. Genel anlamda, denetçilerin organizasyonlarda üstlendiği rol, organizasyonel hedefler ve stratejiler doğrultusunda gerçekleştirilen operasyonların standartlara uygunluk gösterip göstermediğini araştırmak ve kontrol etmektir. Siber risklerin analiz edilmesinde ve değerlendirilmesinde de işletmelerin hedefleri, stratejileri ve standartları ön plana çıkmaktadır.

Risk yönetimi yaklaşımlarının dijital çevre kapsamındaki uygulamaları kurumun kültürüne ve yapısına göre değişkenlik göstermektedir. Bundan dolayı, bir işletmenin dijital ortamdaki varlıklarının neler olduğu ve hangi tip siber riskler ile karşılaşılabileceği süreçlerin analizleri ve testleri doğrultusunda belirlenebilmektedir. Sonrasında ise, işletmenin politikaları, standartları, operasyonları ile risk analizi araçları ve teknikleri birleştirilmektedir. Genel olarak, organizasyonların mülkiyetlerinin denetlenmelerinde izleme ve raporlama süreçlerinin verimli işlemesi gerekmektedir.

2013 yılının ocak ayında İç Denetim Enstitüsü tarafından işletmelerde risk ölçümünün ve kontrolünün sağlanması ve bu işlemlerdeki verimliliğin geliştirilmesi için "Etkin Risk Yönetimi ve Kontrolü için Üç Savunma Sınırı"(Three Lines of Defense in Effective Risk Management and Control) adında bir metodoloji sunulmuştur. Bu adımla birlikte siber güvenlik uygulamalarında iç denetimin rolü değerlendirilmiştir.

Üç savunma sınırı veya hattı mekanizması veri güvenliğinin sağlanması amacıyla siber saldırılarla mücadele etmede sıklıkla kullanılan bir yaklaşım olmuştur. Enformasyon güvenliğine yönelik ortaya çıkan siber risklerin kontrol edilmesinde etkin olan işletmeler, bu metodu organizasyonlarının en üst seviyesinden en alt seviyesine kadar entegre etmeyi başarmışlardır. Bu noktada, iç denetim, şirketlerin siber riskleri nasıl değerlendirdiğini ve kontrol ettiğini yönetim kurullarına ve üst yönetimlere objektif bir biçimde sağlayabilmektedir.

Tablo 7: Birincil Siber Güvenlik Sınırı

Savunma Aktivitelerinin Birinci Hattı
Güvenlik prosedürlerinin oluşturulması ve çalışanlara eğitimlerin verilmesi
Cihazlarda güvenlik yapılarının oluşturulması, güncel yazılımların kurulması ve düzenli olarak bakımlarının yapılması
Siber risk denetleme sistemlerinin cihazlara entegre edilmesi ve periyodik olarak testlerinin yapılması
Ağın akışının yönetilmesi ve korunması için yapısal modellerin kurulması
Bilgi varlıklarının, teknolojik ekipmanların ve ilgili yazılımların korunması
Verilerin korunması ve siber risklerin önlenmesi için programların takip edilmesi ve denetlenmesi
Bilgi güvenliğini sağlayacak seviyede eğitime ve tecrübeye sahip şahısların istihdam edilmesi

Kaynak: IIA Position Paper: The Three Lines of Defense In Effective Risk Management and Control

Siber risklere karşı oluşturulan birincil güvenlik hattında operasyonel yöneticiler riski sahiplenir ve yönetir. Ayrıca, süreç ve kontrol hataları için düzeltici aksiyonların uygulanmasında da sorumluluk operasyonel yöneticilerdedir. Siber güvenlik hattının birincil kısmında, günlük bazdaki kontrol prosedürlerinin iç denetimlerinin yapılması ve risklerin analizleri de yer almaktadır. İşletme içi politikaların ve stratejilerin tespit edilmesi, değerlendirilmesi ve kontrol edilmesi bu hat kapsamında gerçekleştirilmektedir. Operasyonel yönetim doğal olarak birincil güvenlik sınırında rol oynamaktadır. Bunun nedeni ise, sistemler ve süreçler içindeki kontrol mekanizması operasyonel yöneticilerin rehberliğinde tasarlanmaktadır.

Tablo 8: İkincil Siber Güvenlik Sınırı

Savunma Aktivitelerinin İkinci Hattı
Siber güvenlik politikalarının tasarlanması ve kontrol edilerek güncellenmesi
Siber risk değerlendirmelerinin düzenli olarak yapılması
Siber tehditlere yönelik istihbaratların toplanması
Risk göstergelerinin ve vakaların izlenmesi
Tedarikçiler ve hizmet sağlayıcılar ile ilişkilerin kurulması

Kaynak: IIA Position Paper: The Three Lines of Defense In Effective Risk Management and Control

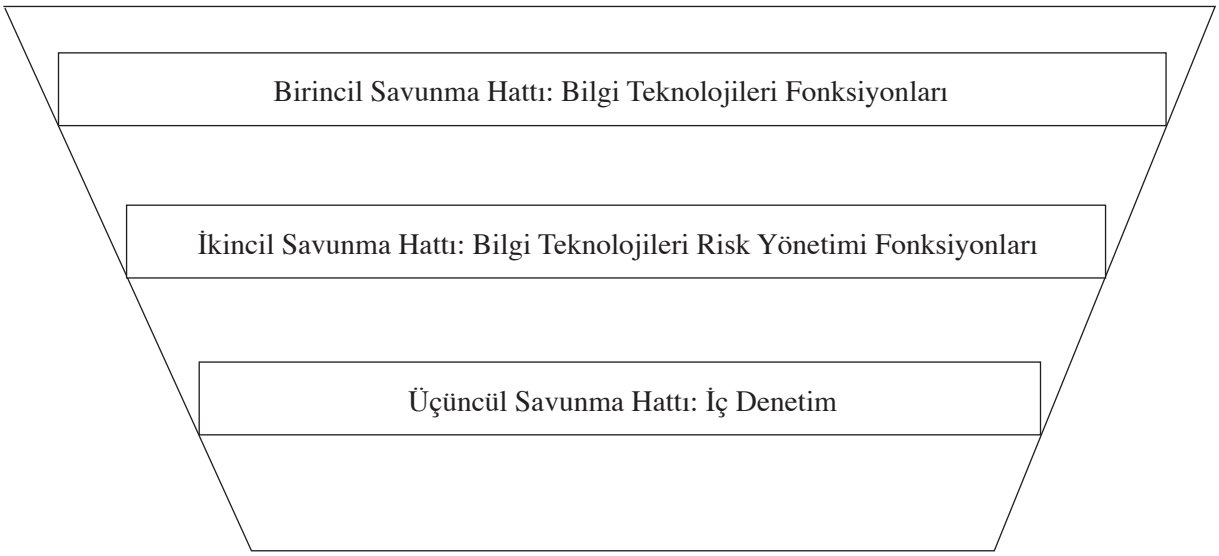
Mükemmel şartların sağlandığı bir ortamda, risklerin kontrol edilmesi için sadece birincil savunma sınırı yeterli olabilmektedir. Ancak, gerçek dünya koşullarında, birincil savunma hattı tek başına yeterli olamamaktadır. Bu yüzden, ikincil güvenlik sınırı geliştirilmiştir. Yönetim fonksiyonları açısından risklerin işletmenin iç çevresinden bağımsız olduğu düşünülerek, kanunlar ve regülasyonlar çerçevesinde, iç denetim mekanizması bu kısımda oluşturulmaktadır. Risk yönetimi çatısının kurulması, gelişen teknolojik süreçlerde yönetsel aktivitelerde rollerin belirlenerek yetki hiyerarşisinin oluşturulması, bilinen ve gelişmekte olan siber risklerin teşhis edilmesi gibi faaliyetler güvenlik sınırlarının bu bölümünde yapılmaktadır.

Tablo 9: Üçüncül Siber Güvenlik Sınırı

Savunma Aktivitelerinin Üçüncü Hattı
Önleme ve denetleme amacıyla siber güvenlik faaliyetlerinde bulunulması
Standart güvenlik konfigürasyonlarının değerlendirilerek, sorunlu web sitelerine ve kötü amaçlı yazılımlara karşı bilgi varlıklarının güvence altında tutulması

Kaynak: IIA Position Paper: The Three Lines of Defense In Effective Risk Management and Control

İç denetçilerin görevlerini verimli bir biçimde sürdürmelerinde organizasyonun objektifliği ve bağımsızlığı önemli rol oynamaktadır. İkincil savunma hattında yüksek seviyede bağımsızlık sağlanamamaktadır. Bu yüzden, iç denetim, yönetişimin ve risk yönetimi araçlarının en etkin olarak devreye girmesi için üçüncül savunma sınırında tam anlamıyla fonksiyonlarını göstermektedir.



Şekil 6: Roller ve Sorumluluklar

Kaynak: Deloitte

Teknik olarak dijital ortamlardaki tehditlerin doğası gereği siber risklerin analiz edilmesi, değerlendirilmesi ve kontrol edilmesi süreçleri şekil 4'teki yapı üzerinden takip edilmektedir. İç denetimin bu mekanizma içerisindeki esas rolü ise birincil ve ikincil savunma sınırında yürütülen faaliyetlerin verimini kontrol etmek ve üst yönetime objektif bir biçimde bildirmektir.

7. SONUÇ

Yakın geçmişe kadar, yönetim kurullarının siber riskleri yönetmesi çok nadir rastlanılan bir durum iken, teknolojideki hızlı gelişmeler ve siber suçların çeşitlenmesi ile birlikte denetim komiteleri ve işletmeler daha öngörülü yaklaşımlara yönelmektedir. Organizasyonlar için siber risk algısı birçok konunun önüne geçmektedir. Siber güvenlik risklerinin analiz edilmesi, değerlendirilmesi ve kontrol edilmesi süreçlerinin tümünü kapsayan siber risk yönetimi kavramı sadece bilgi teknolojilerine ait olmayıp, işletme çevresini bütünüyle ilgilendirmektedir.

İç denetim, siber risk yönetiminin verimliliğini değerlendirmek ve güçlendirmek için sistematik ve teknik yaklaşımları kullanarak, güvenlik mekanizmasında liderlik rolünü üstlenmektedir. Ayrıca, insanlar, süreçler ve teknolojiden oluşan işletme çevresinin siber risklerden uygun metotlarla korunup korunmadığının kontrolü de iç denetim tarafından sağlanmaktadır. İşletmelerin varlıklarını korumak için oluşturulan stratejilerin ve planların işlerliğinin kontrol edilmesi, organizasyonun siber atak sonrası etkilenme derecesi, güvenlik açıklarının tespit edilmesi, dijital enformasyonun nasıl kullanıldığı ve nerelere transfer edildiği konuları da iç denetimin rolleri arasındadır.

Siber saldırılar sonucunda ortaya çıkan tahribat çoğunlukla geri dönüşü olmayan zararlara yol açmaktadır. Finansal risklerin yönetiminde olduğu gibi siber çevredeki tehditlerin de disiplinli bir şekilde takip edilmesi ve kontrol altında tutulması gerekmektedir. Bu nedenle, teknolojideki gelişmeler ışığında iç denetimin rolü daha kapsamlı hale gelerek dijital sistemlere adapte olmaktadır.

KAYNAKÇA

Akhtar, Tafseer ve Gupta, B.B., "Towards a Framework for Analyzing Cyber Attacks Impact Against Smart Power Grid on SCADA System", International Conference on Communication and Signal Processing(ICCSP), 2018, s. 1087-1093.

Guinta, LR. ve Frantzve, LA., "Critically, Vulnerability, Risk Logic Analysis Methodology for Business Enterprise and Cyber Security", 2010, s. 983.

Gusmão, A., Silva, M., Paleto, T., Thiago, P., Silva, L., "Cybersecurity Risk Analysis Model Using Fault Tree Analysis and Fuzzy Decision Theory", International Journal of Information Management, 2018, Volume 43, Number 6, s. 248.

Haimes, Y.Y., "On The Definition of Resilience in Systems", Society For Risk Analysis, 2009, Volume 29, Nuımber 4, s. 498-504.

Kayrak, M., "Bilgi Kriterleri Çerçevesinde Bilişim Teknolojileri Denetimi", Journal of Turkish Court of Accounts/ Sayıştay Dergisi, Ekim 2012, Cilt 23, Sayı 87 s. 143-167.

Kurnaz, N. ve Dindaroğlu, A.K., "İç Denetim ve Bilgi Güvenliği İlişkisi: Bölgesel Bir Araştırma", Bilgi Ekonomisi ve Yönetimi Dergisi, 2015, Cilt 10, Sayı 1, s. 51-63.

Kurt, G. ve Uysal, T.U., "Siber Riskler ve COSO İç Kontrol Bütünleşik Çerçevesi", Muhasebe ve Denetime Bakış, 2015, Cilt 46, Sayı 15, s. 1-10.

Linkov, I., Eisenberg, D.A., Plourde, K., Seager, T.P., Allen, J., Kott, A.(2013), "Resilience Metrics for Cyber Systems", Environment Systems and Decisions, 2013, Volume 33, Number 4, s. 471-476.

Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., Sadhukhan, S., "Cyber-risk decision models: To insure IT or not?", Decision Support Systems, 2013, Volume 56, s. 11-26.

Öztürk, M.S., "Siber Saldırılar, Siber Güvenlik Denetimleri ve Bütüncül Bir Denetim Modeli Önerisi", Muhasebe ve Vergi Uygulamaları Dergisi, 2018, s. 208-232

Ralston, P.A.S. ve Graham, J.H. & Hieb, Jeffrey., "Cyber security risk assessment for SCADA and DCS networks", ISA transactions, 2007, Volume 46, Number 4, s. 583-594.

Rot, A., "IT Risk Assessment: Quantitative and Qualitative Approach", The World Congress on Engineering and Computer Science, 2008.

Spoonamore, S., "CCLIF: A Quantified Methodology System to Assess Risk of IT Architectures and Cyber Operations", 2008, s. 716.

Topaloğlu, S., "Sosyal Güvenlik Suiistimallerinin Tespiti ve Önlenmesi için Risk Analizi ve Sürekli Denetim Yöntemleri", TISK Akademi, 2013, Cilt 8, Sayı 16, s. 204-219.

Uludağ, S., "Değişen Risk Algısı ve İç Denetim", Muhasebe ve Denetime Bakış, 2017, Cilt 17, Sayı 51, s. 93-101.

Yılmaz, S. ve Sağıroğlu, Ş., "Siber Güvenlik Risk Analizi, Tehdit ve Hazırlık Seviyeleri", 6. Uluslararası Bilgi Güvenliği ve Kriptoloji, 2013, s. 158-166.