SİBER GÜVENLİK RİSKLERİNDEN KORUNMADA KÖPRÜ VE KATALİZÖR OLARAK İÇ DENETİM

(INTERNAL AUDIT AS A BRIDGE AND CATALYST IN THE PROTECTION OF CYBER SECURITY RISKS)

Seval SELİMOĞLU* / Mehtap ALTUNEL**

ÖZ

Günümüz iş ortamına bakıldığında hem kamu hem de özel sektörde işlemlerin gerçekleştirilmesi için dijital alt yapıya sahip oldukları ve bu kapsamda bilginin depolanması, işlemlerin yapılması ve raporlamanın elektronik ortamda gerçekleştiği görülmektedir. Bu dijital alt yapı internet, bilgisayar sistemi, yazılım, donanım ve hizmetler yani dijital ortamın tamamı siber alan olarak ifade edilmektedir. Bu alt yapının faaliyetlerin gerçekleştirilmesinde fırsatlar sağlamanın yanında büyük tehdit ve riskleri de beraberinde getirmektedir. Yakın zamanda yaşanan önemli siber saldırılar (WannaCry, BadRabbit, NotPetra vb.) göz önünde bulundurulduğunda ciddi zararlara ve maliyetlere sebep olmuştur. Bu kapsamda hem özel sektörde hem de kamu sektöründe siber saldırılara karşı önlemlerin alınması ve etkilerinin azaltılması önemlidir. Bu kapsamda üçlü savunma hattının siber riskleri kapsayacak şekilde tasarlanması ve iç denetim biriminin siber güvenlik risklerine yönelik çalışmalar yürütmesi, siber güvenlik risklerinin azaltılmasında etkili olacaktır. Bu çalışmada siber riskler ve siber risklerin yönetilmesine ilişkin bilgi verilmekle birlikte, siber güvenliğin sağlamasında iç denetimin rolü ortaya konulmaya çalışılmıştır.

Anahtar Kelimeler: Siber Risk, Siber Güvenlik, Üçlü Savunma Hattı, İç Denetim

JEL Kodlaması: M40, M42, O30

ABSTRACT

When we look at today's business environment, it is seen that they have digital infrastructure for the realization of transactions in both public and private sectors and in this context, information storage, transactions and reporting are realized in electronic environment. This digital infrastructure is expressed as the internet, computer system, software, hardware and services. In addition to providing opportunities for the realization of these activities, this infrastructure brings with it great threats and risks. Considering the recent cyber attacks (WannaCry, BadRabbit, NotPetra, etc.), it has caused serious damages and costs. In this context, it is important to take measures against cyber attacks in both the private and public sectors and to reduce their impact. Therefore, the design of the three lines of defense covering cyber risks and the internal audit unit's work on cyber security risks will be effective in reducing cyber security risks. In this study, information is given on the management of cyber risks and cyber risks, but the role of internal audit in providing cyber security is tried to be explained.

Keywords: *Cyber Risks, Cyber Security, The Three Lines of Defense Model, Internal Audit.*

JEL Classification: *M40, M42, O30*

* Prof. Dr., Anadolu Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, Eskişehir, Orcid:0000-0003-1185-9980, sselimoglu@anadolu.edu.tr
** Doktora Öğrencisi, Anadolu Üniversitesi, İşletme Anabilim Dalı, Muhasebe Bilim Dalı, Eskişehir, Orcid: 0000-0003-3149-7753 altunelmehtap@hotmail.com, Yazı Gönderim Tarihi: 19.03.2019, Yazı Kabul Tarihi: 26.03.2019

1. GİRİŞ

Bilgi teknolojisindeki gelişmeler, işletmeleride bu gelişmeler ile paralel yönde hareket etmeleri yönünde gerekli kılmıştır. Böylece artık bütün dünya bilginin herkes tarafından hızlı şekilde erişildiği küresel bir oluşum içinde yer almaktadır. Bu oluşum birçok fırsatı beraberinde getirmekle birlikte kötü amaçlı kullanımlara da ortam hazırlamaktadır. Bu kötü amaçlı kullanımlar siber suçlar olarak nitelendirilmektedir. Siber suçlar sadece birebir kişilere karşı yapılan bir eylem olmanın dışında işletmelere hatta ülkelere karşı eylemleri içermektedir. Dolayısıyla siber suçların etkileri hem mikro hem de makro seviyede kişilere ve kurumlara zarar verdiği söylenebilir.

Bilgi teknolojilerinde yaşanan gelişmelerin sunduğu fırsatlar ve beraberinde gelen siber suçlar ile mücadeleye ilişkin veri tabanlarının, bilgi sistemi ve uygulamaların güvenliğinin sağlanmasının önemi artmıştır (Öztürk, 2018: 209).

Siber güvenliğin sağlanması adına yapılan denetimler, ülkemizde finansal tabloların güvenirliliğini sağlamak adına yapılan denetimler kadar önemli bir yere sahip olduğunu söyleyebiliriz. Çünkü siber güvenlik risklerine ilişkin önlem alınmaması ile birlikte işletme hem büyük maliyet kayıpları ile karşı karşıya kalacaktır hem de itibari zedelenecektir. Bu anlamda siber güvenlik risklerine karşı farkındalık oluşturmak ve mücadele etmek adına yurtiçinde ve yurtdışında düzenlemeler ve akademik çalışmalar yapılmaya başlanmıştır. Siber güvenliğe ilişkin yapılan en önemli düzenlemelerden biri 2015 yılında COSO, Deloitte ile birlikte *Siber Çağda COSO* (COSO in theCyber Age) isimli rapor yayınlamıştır. Bu rapor kapsamında siber riskin işletmedeki değerlendirilmesi süreçleri üzerine bir çerçeve sunulmaktır (COSO, 2015). Diğer bir çalışmada Uluslararası İç Denetçiler Enstitüsü tarafından *Küresel Teknoloji Denetim Rehberi: Siber Risklerin Değerlendirilmesi: Üçlü Savunma Hattının Rolü* (Global Technology Audit Guide (GTAG): AssesingCybersecurity Risk: Roles Of The Three Lines Of Defense) yayınlanmıştır. Bu rehber iç denetçilerin siber güvenlik riskleri konusunda güvence sağlamaları adına yetkinliklerini geliştirmelerine yardımcı olması için tasarlanmıştır. Ayrıca bu rehber iç denetimin siber güvenlikteki rolünü ele almıştır (IIA, 2016). Bu düzenlemelerin yanında ISACA (Information SystemAnd Control Association) tarafından *Denetim: Siber Güvenlik* (Auditing: Cyber Security- Evaluating Risk and Auditing Controls) raporu yayınlanmıştır. Bu rapor siber güvenlik kontrollerini, risk değerlendirme ve yönetim incelemelerini içerir(ISACA, 2017). Bunların yanında siber risklerin yönetilmesinde kullanılan COBIT (Control Objectivesfor Information andRelatedTechnology), ISO 27000, NIST (NationalInstitute of StandardsandTechnology) diğer düzenlemelerdir (COSO, 2015).

Diğer taraftan ülkemizde yapılan çalışmalara bakıldığında Sermaye Piyasası Kurulu tarafından Ocak 2018 tarihinde *Bilgi Sistemleri Yönetim Tebliği* ve *Bilgi Sistemleri Bağımsız Denetim Tebliği* yayınlanmıştır. Bu tebliğler kapsamında bilgi sitemi yönetimi ve denetimine ilişkin açıklamalar sunulmuştur (SPK, 2018).

Akademik çalışmalara incelendiğinde, çalışmamızın kapsamı itibariyle denetim ve siber güvenlik ile ilgili çalışmalara yeni başlandığı görülmektedir. Fakat bilgi teknolojilerindeki gelişmeler ile birlikte, siber riskleri azaltmak ve önlemek adına denetime olan ihtiyacın artmasından kaynaklı bu yönde çalışmaların artacağı düşünülmektedir.

Türkiye'de siber risk ve siber güvenliğe ilişkin birçok çalışma bulunmakla birlikte, denetim kapsamında siber güvenlik risk değerlendirmesi adına çok çalışma bulunmamaktadır. Yayınlanan çalışmalara bakıldığında; Öztürk(2018) tarafından yapılan çalışmada siber güvenlik denetiminde sürecin bütüncül bir biçimde ele alınması suretiyle bir model gösterilmiştir. Bu kapsamda çalışmada siber güvenlik denetim sürecine ilişkin açıklamalar akış şeması ile açıklanmıştır. Kurt ve Uysal (2015) tarafından yapılan çalışmada güncellenen COSO ve yeni yayınlanan Siber Çağda COSO raporu doğrultusunda siber risklere yönelik nasıl bir iç kontrol sistemi geliştirilmesi gerektiği ele alınmıştır.

Yurtdışında yapılan akademik çalışmaların bir kısmına bakıldığında; Kahyaoğlu ve Çalıyurt (2018) tarafından yapılan çalışma kapsamında, iç denetim ve risk yönetimi perspektifinde anahtar konuları ve zayıflıkları belirlemek amacıyla siber güvenlik güvence yaklaşımı analiz edilmiştir. Mukhopadhyay ve diğerleri (2013) tarafından yapılan çalışmada siber riske karşı alınacak önlemler incelenmiştir. Shackelford (2012) tarafından yapılan çalışmada ise işletmelerin

siber saldırıları önlemede daha çok siber risk sigortasına yöneldiklerine ulaşılmıştır. Ayrıca bu çalışmada siber saldırıların firmalar üzerindeki etkisi, veri ihlallerine yönelik ABD'deki yasalar ve siber risk sigortalarının siber tehditleri azaltmaya yardımcı olmadaki boyutu ele alınmıştır. Nijerya'da banka sektöründe Ojeka ve diğerleri (2017) tarafından yürütülen çalışmada denetim komitesi etkinliği ve siber güvenlik arasındaki ilişki değerlendirilmiştir. Değerlendirme sonucunda denetim komitesinin denetim ve gözetim konusunda yetersiz olduğuna ulaşılmıştır. Sabillon ve diğerleri (2017) yürüttükleri çalışmada siber güvenlik güvencesi ve denetim alanında küresel liderlerin en iyi uygulamaları ve metodolojileri incelenmiştir. American Accounting Association tarafından 2017 yılında yapılan çalışmada, siber güvenliğin en baskın konuları ve siber güvenlik güvencesi için yeni yaklaşımların gerekliliği açıklanmıştır (American Accounting Association, 2017:1).

Bu çalışmada, siber güvenlik riskinin engellenmesinde bir barikat olan iç denetimin rolü ortaya koymak amaçlanmıştır. Bu amaçla çalışmanın ikinci bölümünde siber risk kavramının ciddiyetini ortaya koymak için yakın zamanda yaşanmış siber saldırılardan bahsedilmiş ve siber riske ilişkin genel açıklamalar yapılmıştır. Üçüncü bölümde siber risklerin belirlenmesi ve yönetilmesi konuları ele alınmıştır. Dördüncü bölümde siber güvenlikte üçlü savunma hattına ilişkin Uluslararası İç Denetim Enstitüsü'nün yayınladığı rehber çerçevesinde açıklama yapılmıştır. Son bölümde ise siber güvenlikte iç denetimin rolü ortaya konulmaya çalışılmıştır.

2. SİBER RİSK KAVRAMINA GENEL BAKIŞ

Artan rekabet koşulları ile küresel ortama ayak uydurmak için hem özel sektör hem de kamu sektöründe bilgi teknolojileri yaygın şekilde kullanılmakta, işlemler elektronik ortamda gerçekleştirilmekte ve raporlama yapılmaktadır. Bilgi teknolojileri hem kamu hem özel sektörde birçok kolaylık sağlayarak fırsat yaratmanın yanında riskleri de beraberinde getirmektedir(Öztürk, 2018: 208). Günümüzde teknolojinin gelişmesi ile birlikte bu riskler arasında ön plana çıkanı siber risklerdir. Siber riskin artışı ve buna bağlı olarak siber güvenliğin önemini vurgulamak adına PWC tarafından yürütülen 2018 yılına ait "Küresel Ekonomide Suçlar ve Hile Araştırmaları" başlıklı çalışma incelendiğinde hile beş kategoride ele alınmıştır. Bu çalışmada en sık yapılan hilelerden biri de "siber suçlar" olarak ifade edilmektedir (PWC, 2018:8). Dolayısıyla işletmenin karşılaştığı hileler arasında sıralanan siber suçların ifade edilmesi, siber risklerin işletmeler açısından önemini ve bu risklere yönelik işletmelerin önlemler alması gerektiğini göstermektedir.

Siber risk kavramını anlamak adına en bilindik siber saldırılardan bahsederek konunun önemliliğini ortaya koyduktan sonra siber, siber risk ve siber güvenlik kavramını tanımlamanın yararlı olacağı düşüncesindeyiz.

Yapılan araştırma sonucunda en ses getiren siber saldırının 12 Mayıs 2017 tarihinde ağırlıklı olarak Avrupa ülkelerinde etkisinin görüldüğü "WannaCry" adlı siber saldırıdır. Uzmanlara göre bu tarihe kadar gerçekleştirilmiş en yaygın ve en büyük saldırı olarak görülmektedir. Hastaneler başta olmak üzere birçok kuruluş bu siber saldırıdan etkilenmiştir. WannaCry siber saldırıların en yaygın şekli olan fidye yazılım saldırısıdır. Sisteme kullanıcı erişimi engellenerek karşılığında, 300 dolar değerinde Bitcoin fidye istenmiştir. Bu fidyenin üç gün içinde ödenmemesi halinde iki katına çıkacağı; bir hafta içinde ödenmediği takdirde ise sistemdeki tüm bilgilerin silineceği yönündedir (Burca, 2017). Diğer bir siber saldırı da Ekim 2017'de gerçekleşen "BadRabbit" dir. Bu siber saldırıdan en çok etkilenen ülkeler arasında Türkiye, dördüncü sırada yer almaktadır. BadRabbit zararlı yazılım olarak bilgisayara bulaşarak WannaCry'da olduğu gibi fidye istenmektedir (Burca, 2017). Bunun gibi diğer siber saldırılar Burca tarafından şöyle özetlenmiştir (Burca, 2017):

- Amerika'nın en büyük kredi bürosu "Equfax"ın kayıtlarına sızılarak 145.5 milyon Amerikalı'nın kişisel bilgileri çalınmıştır (Temmuz, 2017).
- "Yahoo"nun ana şirketi olan Verizon, Yahoo'nun 3 milyar kullanıcısının hesabının saldırıya uğradığını açıklamıştır (Ekim, 2017).
- ShadowBrokers adlı anonim grup, Amerikan Ulusal Güvenlik Merkezi'nin "hacking" araçlarını sızdırmıştır (Nisan 2017).

- 64 ülkede, Petya (NotPetya) fidye siber saldırısı gerçekleştirilmiştir (Haziran 2017).
- Amazon'un bulut hizmetinin güvenlik ayarındaki bir açık nedeniyle, 200 milyon Amerikan seçmeninin kimlik bilgileri açık hale getirilmiştir (Haziran 2017).
- 57 milyon Uber müşterisinin verilerinin 2016 yılında çalındığı açıklanmıştır (Kasım 2017).

Siber risk kavramına bakacak olursak öncelikle siber kavramını açıklamanın konunun anlaşılması açısından yararlı olacaktır. Siber kavramı, hayatımızın birçok noktasında karşımıza çıkmasına karşın TDK (Türk Dil Kurumu) tarafından nasıl bir açıklama yapıldığı incelendiğinde kurum tarafından herhangi bir açıklamanın mevcut olmadığı tespit edilmiştir. Oxford sözlüğünde ise siber, "bilgisayar, bilgi teknolojisi ve sanal gerçeklik ile ilişkili veya özelliği" şeklinde tanımlanmıştır (Oxford Dictionaries, 1857). Sağıroğlu (2018: 23-24) tarafından siber, tanım itibarıyla "elektronik ortamları" ifade etse de içerisinde çok farklı unsurları barındırdığı ifade edilmiştir. Bu unsurların bulunduğu, işletildiği, yönetildiği ve geliştirildiği ortamlarda bulunan veriler; "bilgisayar, sunucu, cihaz, donanım, yazılım, protokol, algoritma, işlem, politika, süreç, laboratuvar ve sistem" gibi unsurları içermektedir. Ayrıca insan, siber dünyanın önemli unsurlarından birisi olduğuna vurgu yapılmıştır.

Siber risk ise, bir kuruluşun bilgi teknolojisi sisteminin bir tür başarısızlık nedeniyle finansal kayıp, işleyişini durdurma veya itibar kaybına sebep olan tüm riskleri kastetmektedir. Böyle riskler aşağıdaki sınıflandırılmış eylemler sonucu ortaya çıkmaktadır (The Institute of Risk Management, 2014: 8):

- Casusluk, dolandırıcılık veya para sıkıntısı sebebiyle bilgi sistemlerine erişmek için kasıtlı veya yetkisiz güvenlik ihlalleri,
- Kasıtsız veya kazara güvenlik ihlali,
- Zayıf sistem bütünlüğü ve diğer faktörlerden dolayı operasyonel BT riskleri.

Siber güvenlik "siber ortamlarda karşılaşılabilecek tehdit ve tehlikeler ile oluşabilecek riskleri önceden öngörüp bunlara karşı önceden önlem alma girişimi" veya "siber varlıkların tehdit ve tehlikelerden korunması için doğru teknolojiler, yöntemler, çözümler, önlemler, politikalar, standartlar, testler gibi girişimlerin doğru amaç, hedef veya şekilde kullanılarak siber varlıkların veya sistemlerin istenilmeyen kişiler/sistemler tarafından elde edilmesini önleme girişimi" olarak ifade edilmektedir (Sağıroğlu, 2018: 26).

Geçmişte yaşanan siber saldırılar ve tanımsal ifadelerin ardından bilgi sistemlerine yönelik gerçekleştirilen yaygın siber tehditler aşağıdaki şekildedir (Kumar, Srivastava, & Lazarevic, 2005: 5-6):

Kimlik Doğrulama Suçları (AuthenticationViolations): Şifreler çalındığında kimlik doğrulama suçları ile sonuçlanır. Bu sorunun çözümü için birçok şifre ve ek bilgiye sahip olmak gereklidir.

İnkar Edememe (Nonrepudiation): Mesaj gönderen kişi çok iyi bir biçimde mesaj gönderdiğini inkar edebilir. İnkar edememe teknikleri ile göndericinin mesajları takip edilerek inkar edilmesi engellenebilmektedir. Ancak web sayfasına erişen kullanıcının yerini belirlemek zordur.

Truva Atları ve Virüsler (Trojan Horses and Viruses): Truva atı ve virüsler, birçok etkiye neden olan kasıtlı programlardır. Virüsler makineden makineye yayılır ve çeşitli bilgisayarlardaki dosyaları silebilir. Truva atları, yüksek seviyeden düşük seviyeye bilgi sızdırabilir. Bunlar için çeşitli virüs paketleri geliştirilmiştir.

Sabotaj (Sabotage): Bilgisayar korsanları sistemleri kırarak uygun olmayan mesajlar gönderebilir.

Hile (Fraud): Ticaret ve işlerin çoğu, uygun kontroller olmadan internet üzerinden yürütülmektedir ve internet hileleri işletmelere milyon dolar kayıplara neden olmaktadır. Suçlular yasal kullanıcıların kimlik bilgilerinin elde edebilir ve banka hesaplarını boşaltabilir.

Hizmet ve Altyapısal Engellemelere Yönelik Saldırılar (Denial of Service and InfrastructureAttacks): Korsanlar tarafından alt yapılar kırılarak zarar görmektedir. Altyapılar, telekomünikasyon sistemleri, güç sistemleri ve sıcaklık sistemlerinden oluşur. Böyle saldırılar hizmet engellemelerine neden olacaktır.

Doğal Afetler (Natural Disasters): Siber terörizme ek olarak kasırga,deprem, yangın gibi doğal felaket-

lerde bilgisayarların ve ağların zarar görmesine neden olabilmektedir. Bu durumlara yönelik önlemler, verilerin korunması ve veri tabanlarının iyileştirilmesidir.

Yukarıdaki sıralanan tehditlerin yanında Aslay (2017: 25-26) tarafından; sosyal mühendislik, web sayfası hırsızlığı ve yönlendirme, hukuka aykırı içerik sunulması, sistem güvenliliğinin kırılarak içeri sızılması, yerine geçme, çöpe dalma, istem dışı alınan elektronik postalar, bukalemun, oltalama, mantık bombaları, zararlı yazılımlar, bilgi ve veri aldatmacası, salam tekniği ve süper darbe gibi siber saldırı türleri sıralanmıştır.

Davenport ve Amjad tarafından 2016 yılında yayınlanmış olan "Siber Güvenliğin geleceği adlı çalışmada bir istatistik sitesinin 2016 yılında 22.9 milyar cihazın birbirine bağlı olduğunu ve 2020'de bu rakamın 50 milyara çıkacağı tahmin edilmektedir. Milyarca cihazın çevrim içi olmasıyla birlikte siber riskler artacaktır ve siber güvenliği karmaşık ve zorlu hale getirecektir(Davenport & Amjad, 2016). Davenport ve Amjad'ın yapmış olduğu çalışmadan da görüldüğü üzere siber riskler her geçen gün artmaktadır. Bu nedenle siber risklerin belirlenmesi ve yönetilmesi önemli hale gelmektedir.

3. SİBER RİSKLERİN BELİRLENMESİ VE YÖNETİLMESİ

İşletmelerin siber risklerini belirlenmesi ve siber riskleri yönetmesi işletme hedeflerine ulaşılması, zarara uğramama ve itibar kaybının yaşanmaması adına önemlidir. Hem özel sektörde hem de kamu sektöründe bilginin korunması önemlidir. Bu noktada öncelikle farkındalık düzeyinin artırılması öncelikli adımdır. Türkiye'de farkındalık düzeyini değerlendirmek adına yapılan bir çalışmada 501 kullanıcının %96.3'ü bilgi güvenliğinin önemini farkında olmasına rağmen aynı kullanıcıların %51.5'lik kısmı kullandıkları teknolojik cihazlara ilişkin tehditleri farkında değillerdir. Dolayısıyla bireysel, kamu kurumu ve özel sektör olarak öncelikle siber tehditlerin konusunda farkındalığın olması gereklidir. Bu nokta işletmeler tarafından çalışanlarına siber risklere ilişkin farkındalık eğitimi verilmesi önemli ölçüde etkili olmanın yanında hızlı değişim nedeniyle farkındalığın etkin yönetim ile süreklilik sağlanacağı göz ardı edilmemelidir (Erol & Sağıroğlu, 2018:107-109). IIA (The Institute Of Internal Auditing- İç Denetim Enstitüsü) tarafından yapılan çalışma incelendiğinde, siber ile ilişkili riskleri aşmak ve çözümlemek için, liderlik ekibinin önleyici tedbirler geliştirmesi, bu tedbirleri eğitim ve bilinçlendirme programlarıyla birlikte uygulamaya konmasının öneminden bahsedilmiştir. Dolayısıyla farkındalığı artırmak adına çalışanlar, tedarikçiler, ortaklar ve yükleniciler de aynı şekilde eğitilmeli ve siber güvenlik tedbirleri ve protokolleri konusunda onlardan neyin beklendiğini tam olarak anlamaları sağlanmalıdır (IIA, 2018:7).

Siber güvenlikte temel hedef; güvenliğin makul seviyede sağlanmasıdır. Burada yüzde yüz bir güvenliğin hiçbir zaman sağlanamayacağı yaklaşımı göz önünde bulundurulmalıdır. Bu noktada siber güvenliğin sağlanması için siber risklerin belirlenmesi ve doğru yönetilmesi önemli bir faktördür. Dolayısıyla risklerin iyi belirlenmesi, giderilmeye çalışılması için iyi bir risk yönetimi yapılmalı, mevcut teknikler, teknolojiler, politikalar, standartlar ve çözümler uygulanarak siber güvenlik kapsamında çalışmalar yürütülmelidir. Siber güvenlikte aşağıdaki unsurlar yer almaktadır:

- Bir güvenlik politikası oluşturulmalı ve uygulanmalıdır.
- Gereği kadar koruma prensibi uygulanmalıdır.
- İyi bir risk analizi ve yönetimi yapılmalıdır.
- Sistemlere belirli periyotlarla hataları, eksiklikleri, açıklıkları ve zafiyetleri gidermek amacıyla testler (sızma testleri) yapılmalıdır.
- Sistemleri kullanan her kullanıcıya en az hak verme yaklaşımı benimsenmelidir.
- Siber güvenliğin sağlaması adına düzenleme ve standartlar (Siber Çağda COSO, ISO 27000 vb.) takip edilmeli ve uygulanmalıdır.
- Elektronik ortamlarda her zaman güvensiz bir ortam olduğu göz önünde bulundurulmalıdır. Bu bağlamda bilgi varlığının yedeklenmesi ve kurtarılmasına yönelik sistemler kurulmalı ve işletilmelidir.
- Güncel tehdit ve tehlikeler takip edilerek giderilmelidir.
- Olası tehdit ve tehlikeler öngörülmeli ve önlem alınmalıdır bu amaç doğrultusunda mekanizma ve yapılar kurularak işletilmelidir.

- Güvenli bileşenleri tanımlama ve güvenlik gerektiren bileşenlerin sayıları en aza indirme temel amaç olmalıdır.
- Siber güvenlik sistemleri ile ilgilenen uzmanların kendilerini geliştirmeleri konusunda fırsat verilmelidir (Sağıroğlu, 2018: 44).

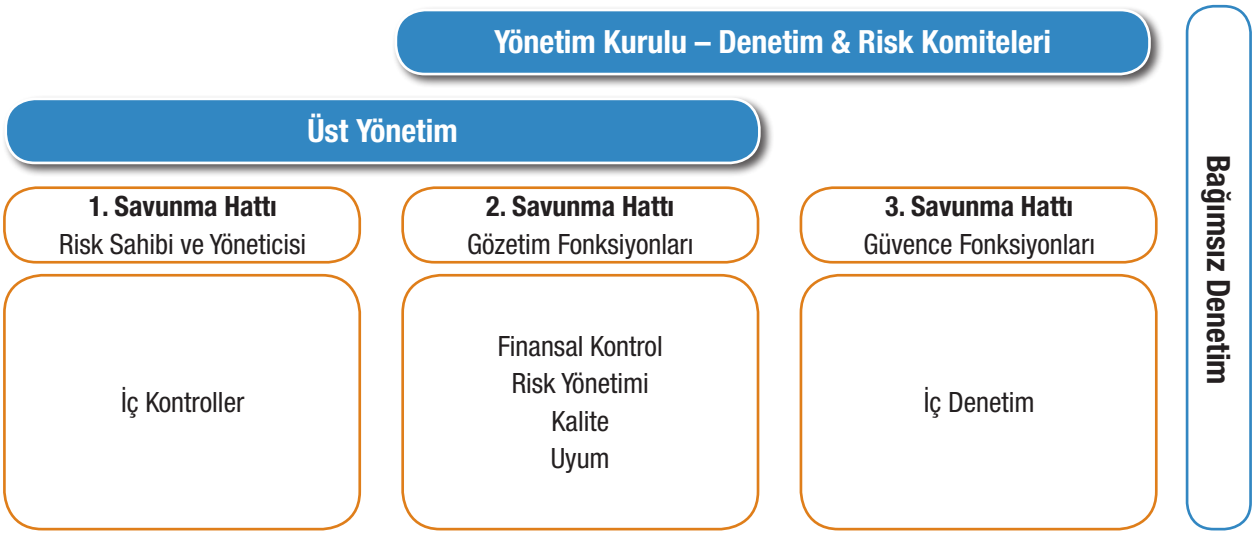
Son olarak KPMG tarafından siber güvenliğin sağlanması dolayısıyla siber risklerin belirlenmesi ve yönetilmesi şöyle özetlenmiştir (KPMG, 2016: 7):

- İşletmelerin sahip olduğu ağları korumak amacıyla gerekli anti-virüs yazılımlarını kurmak, güvenlik duvarı oluşturmak, siber olay yönetimi politikası oluşturmak ve kullanıcı eğitimine ve farkındalığa önem vermek gibi temel konuları ele almak,
- Siber güvenlik önlemlerinin merkezinde, yönetim kurulunun sorumluluğunda olan bilgi riski yönetimi yatmaktadır. Bu nedenle şirketin en önemli bilgi varlıklarının neler olduğunu anlamak ve bu varlıklara yönelik riskleri yönetmek,
- Siber güvenliği artırma projelerinde, insan faktörünü, kültürü, iş süreçlerini ve teknik güvenlik tedbirlerini birlikte ele alacak bütüncül bir yaklaşım benimsenmesi,
- Siber güvenlik sadece teknik bir konu olmadığı; siber güvenliğin sağlanması için siber olaylara karşı hazırlıklı olmayı, korunmayı, böyle olayları tespit etmeyi ve gerektiğinde tepki vermeyi içeren entegre bir yaklaşımın benimsenmesi,
- Çalışanlar kasıtsız şekilde en büyük güvenlik açığını oluşturuyor olabilirler, bu yüzden doğru davranışlara teşvik etmek için teknik eğitim ve farkındalık eğitimi verilmesi,
- Siber güvenlik sisteminin etkinliğini takip edecek bir yönetim yapısının oluşturulması ile siber tehditleri takip ederek daha iyi risk kararlarının alınmasını sağlayacak bir araştırma sisteminin kurulması.

4. SİBER GÜVENLİKTE ÜÇLÜ SAVUNMA HATTI

Geçmişte yaşanan muhasebe skandalları, başarısızlıklar, bilgi hırsızlığı, ve doğal afetler gibi küresel olaylar risk yönetimini yatırımcılar, ortaklar, yönetim kurulları, paydaşlar ve müşteriler açısından yeniden önemli hale getirmiştir (KPMG, 2016: 7). Bu kapsamda işletmelerin risk yönetimi görevlerini sistematik bir yaklaşımla atamaları ve koordine olmalarına yardımcı olacak en iyi uygulama üçlü savunma hattı modelidir. Dolayısıyla işletmelerin siber güvenliği sağlamada organizasyondaki tüm taraflara önemli görevler düşmektedir. Bu kapsamda işletmenin tüm süreçlerine atamalar yapılması, rol ve sorumlulukların net şekilde belirlenmesi, sahiplenilmesi ve zamanında, eksiksiz

Şekil 1. Üçlü Savunma Hattı



(Erdemir Grubu, 2015: 2)

şekilde yerine getirilmesi tüm risklerde olduğu gibi siber güvenlik yönünden de kritik öneme sahiptir.

Üçlü savunma hattı, Uluslararası İç Denetçiler Enstitüsü tarafından işletmelerin karşılaşabileceği birçok riske yönelik bir model olmakla birlikte çalışmamızın konusu itibariyle Enstitünün yayınladığı rehber (Global Technology Audit Guide (GTAG): Assessing Cybersecurity Risk: Roles of the Three Lines of Defense) kapsamında siber risklerin değerlendirilmesinde üçlü savunma hattının rolü ortaya konulmaya çalışılmıştır.

Rehber çerçevesinde üçlü savunma hattına ilişkin açıklamalar aşağıdaki başlıklarda sırasıyla özetlenmiştir (IIA, 2016: 6-15).

4.1. Birinci Savunma Hattı

Birinci savunma hattı, yönetim kontrollerinden oluşmaktadır. Bu savunma hattı Kaya (2017) tarafından *"riske karşı çarpışmanın en şiddetli yaşandığı cephe"* olarak ifade edilmiştir. Diğer bir ifadeyle şirketlerin tüm süreçlerine yönelik risklerin ilk kontrol altına alındığı hattır. Birinci savunma hattında yönetim, otomasyon, süreç, manuel vb. kontrollerin tasarlandığı kısımdır. Siber güvenlik açısından bakıldığında GTAG rehberinde ilk savunma hattı,riskleri kontrol eden ve yöneten ve süreçleri ve kontrol eksikliklerini gidermek için düzeltici eylemler uygulayan operasyonel yöneticilerden meydana geldiği ifade edilmiştir. Bu bağlamda işletmelerde teknolojiden sorumlu genel müdür (CTO, Chief Technology Officer), bilgi güvenlik yöneticileri (CISO, Chief Information Security Officer), bilgi yöneticisi (CIO, Chief Information Officer) veya BT (Bilgi Teknolojisi)'den sorumlu başka bir sorumluyu işe alabilir. Teknolojiden sorumlu genel müdür genellikle kuruluşun misyonunu yürütmek için mevcut teknolojiler hakkında bilgi ve yön sağlamaktan sorumludur ayrıca kuruluşun fikri mülkiyetini korumaktan sorumludur. Diğer sorumlu kişiler ise kuruluşun varlıklarının ve paydaş verilerinin uygun şekilde korunduğunu doğrulamak için sık sık gözetim programları geliştirmede liderlik ederler. Rehberde birinci savunma hattına ilişkin faaliyetler aşağıdaki şekilde sıralanmıştır:

- Güvenlik prosedürlerinin yönetimi, eğitimi, testi.
- Düzenlemelerin/konfigürasyonların güvenli araçlarla sürdürülmesi, uygulamaların güncellenmesi, yamaların yapılması,
- Saldırı tespit sistemini etkin kullanmak ve penetrasyon (sızma) testlerinin yürütülmesi,
- Network trafik akışını yeterli seviyede yönetmek ve korumak için güvenli şekilde network yapılandırılması,
- Bilgi varlıklarının, teknolojik araçların ve ilgili yazılımların envanteri,
- İzleme/gözetim ile ilgili veri koruma ve kayıp önleme programlarının etkin kullanımı,
- Erişim kısıtlaması,
- Gerekli yerlerde verilerin şifrelenmesi,
- İç ve dış taramalar ile zafiyet yönetimi uygulamaları,
- Sertifikalı IT, IT riski ve bilgi güvenlik personelinin işe alımı ve devamlılığı.

4.2. İkinci Savunma Hattı

İkinci savunma hattına baktığımızda finansal kontrol, kalite yönetimi, risk yönetimi, uyum gibi güvence fonksiyonlarından oluşmaktadır. Birinci savunma hattını aşarak yakalanan ve ciddi boyuttaki risklerin takip edildiği savunma hattıdır. İkinci savunma hattında oluşacak bir hata işletmeyi ciddi zararlara uğratabilir (Kaya, 2017). İkinci savunma hattının, siber güvenliğe ilişkin bir takım sorumlulukları vardır. Bunlar:

- Siber güvenlikle ilgili risklerin değerlendirilmesi ve risklerin kuruluşun risk iştahına uygun olup olmadığını belirlemek,
- Mevcut ve ortaya çıkan riskleri izleme, yasalarda ve düzenlemelerdeki değişiklikleri izlemek,
- Uygun kontrol tasarımı sağlamak için birinci savunma hattı fonksiyonları ile işbirliği yapmak.

Uluslararası İç Denetçiler Enstitüsünün yayınlamış olduğu rehberde ikinci savunma hattında siber güvenlikle ilgili yaygın faaliyetler şöyle sıralanmıştır:

- Siber güvenlik politikaları, eğitimi ve testlerinin tasarlanması,
- Siber risk değerlendirmelerinin yapılması,
- Siber tehdit bilgilerinin toplanması,
- Verilerin sınıflandırılması ve kısıtlı erişim rollerinin tasarlanması,

- Olayların anahtar risk göstergelerinin izlenmesi ve iyileştirilmesi,
- Sertifikalı IT risk personelinin işe alınması ve devamlılığı,
- Üçüncü taraflarla, tedarikçilerle ve hizmet sağlayıcılar ile ilişkilerin değerlendirilmesi,
- İş sürekliliği planlarının yapılması/test edilmesi ve olağanüstü durumları iyileştirme uygulamaları ve testlerine katılım.

Savunma hattının son aşamasında iç denetim yer almaktadır. İç denetim, bir kurumun faaliyetlerini geliştirmek ve onlara değer katmak amacını güden bağımsız ve objektif bir güvence ve danışmanlık faaliyetidir. İç denetim, kurumun risk yönetim, kontrol ve yönetişim süreçlerinin etkililiğini değerlendirmek ve geliştirmek amacına yönelik sistemli ve disiplinli bir yaklaşım getirerek kurumun amaçlarına ulaşmasına yardımcı olur (Türkiye İç Denetim Enstitüsü, 1994). Üçlü savunma hattının en önemli kısmıdır. Çünkü üçüncü savunma hattını geçen riskler organizasyonlar için yıkıcı sonuçlara neden olabilir. Bu nedenle iç denetim üçlü savunma hattında önemli sorumluluğa sahiptir (Kaya, 2017). Bu kapsamda üçüncü savunma hattına ilişkin açıklamalar aşağıda kısaca yapılmıştır.

4.3. Üçüncü Savunma Hattı

Üçüncü savunma hattı olarak iç denetim faaliyeti üst yönetime ve yönetim kuruluna yönetişim, risk yönetimi ve kontroller konusunda bağımsız ve objektif bir güvence sağlar. Bu, siber güvenlik risklerini ve tehditlerini yönetme ve azaltmada birinci ve ikinci savunma hattının gerçekleştirdiği faaliyetlerin genel etkinliğinin değerlendirilmesini içerir. İç denetim faaliyeti aşağıdaki konularla ilgili danışmanlık yapabilir:

- Siber güvenlik ve organizasyonun riskleri arasındaki ilişki,
- Tepkilere ve kontrol faaliyetlerine öncelik vermek,
- Organizasyonun tüm ilgili yönlerinde siber güvenlik riskinin azaltılması için denetim. Örneğin, ayrıcalıklı erişim, ağ tasarımı, satıcı yönetimi, izleme ve daha fazlası.
- İyileştirme faaliyetlerinde güvence,
- Risk farkındalığını artırmak ve özellikle ikinci savunma hattı olmayan veya yeterince olgun olmayan işletmelerde risk yönetimi aktivitelerinin koordinasyonuna yardımcı olur,
- Siber risklerle ilgili konuların iş sürekliliği planları ve olağanüstü olayların iyileştirilme testleri kapsamına dahil edilip edilmediğini doğrular.

Üçüncü savunma hattı yani iç denetim tarafından gerçekleştirilen ortak faaliyetler şöyledir:

- Siber güvenlikle ilgili önleyici ve tespit edici önlemlerin sürekli bağımsız değerlendirilmelerini sağlamak,
- Standart güvenlik yapılandırmaları, sorunlu web siteleri, kötü amaçlı yazılımlar ve veri sızıntıları için kısıtlı erişime sahip kullanıcıların BT varlıklarını değerlendirmek,
- İyileştirme tedbirlerini takip etmek,
- Hizmet kuruluşları, üçüncü şahıslar ve tedarikçilerin siber risk değerlendirmelerini yapmak.

5. İÇ DENETİMİN SİBER GÜVENLİK AÇISINDAN ÖNEMİ

5.1. Siber Güvenlik Gereksinimi

Siber güvenlik, her yıl şirketler, organizasyonlar ve hükümetler için daha önemli bir konu haline gelmeye başlamıştır. Siber saldırılar nedeniyle, birçok şirket hem bilgi hem de maddi kayıplarla da karşılaşabilmektedir. Bunların en büyük sebepleri arasında, birçok şirketin halen eski teknolojiler kullanıyor olmaları ve yeni teknolojilerini, eski ve kalabalıklaşmış olan güvenlik sistemlerinin üzerine kuruyor olmalarıdır. Güvenlik sistemlerinin güncellenmemesi ve eski teknolojilerin kullanılıyor olması, internet korsanlarının işini biraz daha kolaylaştırmaktadır.

Dijital dünyada iş yapan firmaların siber güvenlik konusuna özellikle önem vermeleri ve güvenlik sistemlerini geliştirmeleri, bu saldırılardan korunmalarını sağlayacak çalışmaların başında gelmektedir. Her geçen gün büyümekte olan saldırı hacimleriyle aynı olmadığı için de, bu saldırıları önlemek için siber güvenlik harcamalarına yapılan yatırımlar her yıl biraz daha artma eğilimindedir.

Siber güvenlik süreçleri hem iç hem de dış denetçiler tarafından denetimin amacı ve kapsamı çerçevesinde ele alınmalıdır. Çünkü işletmelerde artık siber riske

maruz kalmayan hiçbir süreç bulunmamaktadır. Endüstri 4.0, akıllı şehirler, yapay zeka ve büyük verinin (big data) alanının etkileri göz önüne alındığında, finansal, operasyonel veya sistematik tüm süreçler siber riske maruz kalmaktadır.

Her denetimde olduğu gibi siber güvenliğe yönelik yapılan denetiminde bir amaç bulunmaktadır. Bu amaç şöyle ifade edilmiştir: *Yönetimin siber güvenlik süreçlerini, politikalarını, prosedürlerini, yönetişim ve diğer kontrollerin değerlendirilmesini saptayarak yönetime sistematik ve bilimsel güvence ve danışmanlık hizmeti sunmaktır.* Denetimde siber güvenlik standartlarına, iç kontrollere uygunluğun değerlendirilmesine odaklanılmaktadır (Efe, 2018: 351).

5.2. Siber Güvenlik ve İç Denetimin İlişkisi

Yapay zekanın benimsenmesi ve gelişimi kamu kuruluşları ve özel sektörün kendi siber kapasitelerine yeniden daha dikkatli şekilde önem vermeye zorlamıştır. Yapay zekanın güçlenmesi ve büyük veri sistemlerini kullanmak ve bu sistemleri kurum dışı ve kötü niyetli güçlerden korumak başarı açısından kritik bir önem kazanmıştır (IIA, 2017: 10). Her ne kadar siber güvenlik gibi karmaşık ve hızlı değişen bir konu hakkında mutlak bilgi sahibi olunması mümkün olmamakla birlikte bir iç denetçi yöneticisi (İDY) veya iç denetim birimi başkanının siber güvenlik konusunu yakından takip etmesi ve konu hakkında bilgi sahibi olmasının önemi artmaktadır. Ayrıca yukarıda belirtildiği üzere siber riskler sadece bir teknoloji riski olmanın ötesinde bir iş riskidir. Dolayısıyla iç denetçiler bu konuda kritik rol oynamaktadır. Bu noktadaki başarı, yönetim ve denetim komitesinin bu konuya ne kadar önem verdiğine ve İDY'nin benimsediği yaklaşımla ilişkilidir. İDY, yalnızca siber güvenlik denetimlerinin yürütülmesi ile ilgili sorumluluklara değil aynı zamanda kuruma, ileriye dönük ve stratejik düşünce liderliği sunmak suretiyle kurum için güvenilir danışmanlık hizmeti sunmaya da fırsat vermektedir (IIA, 2016: 4).

Siber güvenlik konusunu oluşturan karmaşıklık arasında iç denetimin doğrudan etki edebileceği dört önemli alan bulunmaktadır. Bunlar:

- Siber tehditlere karşı hazırlık ve müdahale hakkında güvence vermek,
- İcrai yönetime ve kurula kurumun karşı karşıya olduğu risk seviyesini ve bu risk seviyelerine cevap vermek için sarf ettiği çabanın düzeyini bildirmek,
- Etkili savunma ve müdahale mekanizmalarını temin etmek için BT ve diğer taraflarla birlikte çalışmak,
- Risklerle ilgili olarak organizasyonlarda bulunan taraflar arasında iletişimi ve koordinasyonu sağlamak ve kolaylaştırmak (IIA, 2017: 10).

Uluslararası İç Denetçiler Enstitüsü'nün 2016 yılında "Global Perspektif ve Anlayışlar: Güvenilir Siber Danışmanlık İçin İç Denetim" kitapçığında belirtildiği üzere siber güvenlik bütüncül bir bakış açısıyla ve sistemli bir şekilde ele alınması gereklidir. Aksi durumda, siber güvenliğin sağlanamaması halinde, işletmenin en temel faaliyetlerinin bile yürütülemeyeceği, fikri mülkiyet haklarının kaybedilmesine ve hatta itibar kaybına uğrayacağı belirtilmiştir. Bu sebeple siber güvenlikte iç denetimin sorumluluğu yüksektir. İç denetim bu kadar önemli bir noktada kilit taşı olmasına karşın E&Y (Ernst&Young) tarafından 2016 yılında "Dijital Dünyada Güven Yaratmak" başlıklı rapor incelendiğinde birçok işletmenin siber güvenliği önemsemediği tespit edilmiştir. Ayrıca pek çok işlemenin bu sorunu ciddiye almayan bir yaklaşım sergilediği, mevcut zafiyetin etkisini daha da artırdığı konusunda raporda uyarıda bulunulmaktadır.

Yukarıdaki açıklamalar neticesinde siber risklere karşı bilinçli ve hazırlıklı olmanın gerekli olduğu söylenebilir. Bu noktada birçok kuruluş bilinçli olmasına karşın hazırlıklı değildir. Hazırlıklı olmak için işletmelerin bir siber saldırıları önleme, siber saldırılara direnme veya en az zararla kurtulma yeteneğine sahip olmaları gereklidir. Tüm bunların sağlanmasında iç denetimin etkisinin önemli olduğunu, işletmelerdeki iç denetim birimlerinin kendilerini siber güvenlik alanında geliştirmesi gerektiğini tekrar ifade edebiliriz.

Siber risklere (bilgisayar korsanlığı/izinsiz girişler, şifre avcılığı, ekonomik casusluk vb.) ilişkin endişeler artıkça paydaşlar siber güvenlik risk programlarını takip etmektedir ve yönetim kurulu iç denetim biriminden siber güvenlik konusunda güvence talep etmektedir. Bu sebeple iç denetim birimi siber riskler konusunda bilgi sahibi olmalı ve siber risklere karşı dirençli olmada rol üstlenmeli ve oynamalıdır.

İç denetim biriminin risk değerlendirme stratejileri, siber güvenliğe özgü tüm riskleri içerecek şekilde geliştirilmeli, politika ve iç kontrollere uyulması konusunda güvence vermelidir. Dolayısıyla iç denetim birimi paydaşlara gerekli güvenceyi vermek adına siber sorunlarla ilgili denetim programı geliştirmesi gereklidir. Bu denetim programının etkinliği için kontrol ortamı, kontrol faaliyetleri, risk değerlendirme, iletişim ve izleme süreçlerinin kurulması ve siber güvenlik tedbirlerinin değerlendirilmesi için bir çerçevenin kurulması gereklidir.

Üçüncü savunma hattı olarak iç denetim, kuruluşun siber risklerini tespit etme ve azaltma yeteneğini geliştirmek için siber güvenlik stratejileri ve politika geliştirme çalışmalarını yönetim ve yönetim kurulu ile iş birliği içinde gerçekleştirmelidir. İç denetim birimi gelişmekte olan teknoloji ve trendler kuruluşun siber güvenlik risk profilini etkileyeceğinden sürekli teknolojiden haberdar olmalıdır. Ayrıca kuruluşun kırılganlık seviyesini değerlendirmeli ve işletmenin risk faaliyetlerini tercih edilen siber güvenlik planına kıyasla gözden geçirmelidir (IIA, 2018: 6-9).

Son olarak iç denetim faaliyetleri ilk savunma hattındaki kontrollerin etkinliğini değerlendirir. BT genel kontrollerinin temel olduğunu ancak siber güvenlik riskini azaltmak için tam bir çözüm sunmadığını göz önünde bulundurmak önemlidir. Siber güvenliğin karmaşıklığı dolayısıyla risklerin izlenmesi, suiistimallerin ortaya çıkartılması ve düzeltici faaliyetlerin başlatılması gibi ilave kontrol katmanlarına ihtiyacı olduğu unutulmamalıdır (IIA, 2016).

6. SONUÇ VE ÖNERİLER

Endüstri 4.0, yapay zeka, bigdata, nesnelerin interneti gibi kavramların hayatımıza girmesi birçok bilgiye kolaylıkla ulaşmamızı ve işlememizi sağlarken, diğer taraftan birçok bilgisayarın birbirine bağlı olduğu bir dünyada tehlikelere açık bir ortamın olması kaçınılmaz hale gelmektedir.

Kuruluşlar birçok riskle karşı karşıya olmakla birlikte bilgi teknolojisindeki yaşanan gelişmeler kuruluşları yeni bir risk ile mücadele etmek zorunda bırakmaktadır. Bahsedilen bu yeni risk siber güvenlik riski olarak adlandırılmaktadır. Siber güvenlik riski, kuruluşların dijital ortamda işlemlerini gerçekleşmesi sonucu bir takım tehditlerle karşılaşma riski olarak kısaca ifade edilebilir.

Siber saldırıların artışıyla birlikte birçok düzenleyici kurumun bu konu üzerine yoğunlaşmasına neden olmuştur. Çünkü siber saldırılar ile kuruluşların değerli varlıkları ve verilerine tehdit altındadır. Kuruluşların karşılaştıkları siber tehditler müşteri bilgilerinin açıklanması, fikri mülkiyetlerin çalınması, işletmeye ait verilerin çalınması ya da işletmelerin sahip olduğu uygulamaların veya tedarik zincirlerinin zarar görmesi şeklinde özetlenebilir. Tüm bu tehditlerin etkileri finansal kayıp ve itibar kaybı şeklinde yansımaktadır. Dolayısıyla kuruluşların siber güvenlik risklerine odaklanmaları, bu riskleri tespit etmek, azaltmak veya en az zararla kurtulmak için özel çalışmalar gerekmektedir. Siber güvenlik riskleri ile mücadelede öncelikle kuruluşta farkındalık düzeyinin artırılması önemlidir. Bu yönde hem işletme içinde hem de işletme dışındaki tarafların siber güvenlik riski konusunda bilinç seviyelerini artırmaya yönelik eğitimler, programlar düzenlenmelidir.

Kuruluşların siber güvenlik riskine ilişkin farkındalığın oluşmasının ardından risklerin yönetilmesinde kullanılan, önemli bir model olan, üçlü savunma hattı modeli oluşturulmalıdır. Bu kapsamda kuruluşların birinci savunma hattında siber güvenlikten sorumlu kişilerin tanımlandığı ve kontrol faaliyetleri ele alınmaktadır. İkinci savunma hattı, risklerin değerlendirilmesi, risklerin kuruluşun risk iştahına uygun olup olmadığının izlenmesi, risklerin ve risk değerlendirmeleri kapsamında düzenlemelerin izlenmesi, risklerin azaltılmasında birinci savunma hattıyla işbirliği yapılması sorumluluğuna sahiptir. Üçüncü savunma hattı yani iç denetim, yönetişim, risk yönetimi ve kontroller konusunda bağımsız ve objektif güvence sağlar. Dolayısıyla siber güvenlik konusunda önleyici ve tespit edici kontrollerin bağımsız ve objektif şekilde iç denetiminin yapılması, işletmenin sahip olduğu BT varlıklarının saldırılara karşı etkinliğinin değerlendirilmesi, iyileştirme çalışmalarının takibi ve üçüncü tarafların siber değerlendirilmelerinin yapılması gibi sorumluluklara sahiptir.

Son olarak, siber güvenlik risklerinin engellenmesinde önemli role sahip olan iç denetimin değişen dünya karşısında geri kalmaması gerektiğini vurgulamak faydalı olacaktır. Bu değişen dünya karşısında hazırlıklı olmak adına yapay zeka, big data, siber saldırılar vb. konularda iç denetçilerin bilgi sahibi olması bir zorunluluktur. Ayrıca iç denetçiler, gelişen dünya karşısında rollerinin ne olacağının, kurum ve işletmelere ne gibi katma değerler sağlayacaklarının farkında olarak kendilerini geliştirmeli ve çalışmalarını yürütmelidirler.

Kaynakça

American Accounting Association. (2017). Cybersecurity and Continuous Assurance. *Journal Of Emergıng Technologıes In Accountıng* , 1-12.

Aslay, F. (2017). Siber Saldırı Yöntemleri ve Türkiye'nin Siber Güvenlik Mevcut Durum Analizi. *International Journal of Multidisciplinary Studies and Innovative Technologies* , 24-28.

Burca, N. (2017, Aralık 29). *2017 Siber Saldırıları 2018 Beklentileri ve İç Kontroller*. Mart 5, 2019 tarihinde https://nazifburca.com adresinden alındı

Burca, N. (2017, Haziran 3). *İç Kontrolleriniz Etkin Mi? «WannaCry» Siber Saldırısında Sorumluluk Kime Ait?* Mart 5, 2019 tarihinde https://nazifburca.com adresinden alındı

Burca, N. (2017, Ekim 25). *Yeni Bir Siber Saldırı: BadRabbit*. Mart 2019 tarihinde https://nazifburca.com adresinden alındı.

COSO. (2015). *COSO in the Cyber Age: Report Offers Guidance on Using Frameworks to Assess Cyber Risks.*

Davenport, T., & Amjad, A. (2016). *The Future Of Cybersecurity.* Mart 8, 2019 tarihinde Deloitte Insight: ttps://www2.deloitte.com adresinden alındı.

Efe, A. (2018). Siber Güvenlik Denetimi. Ş. Sağıroğlu, & M. Alkan içinde, *SiBer Güvenlik ve Savunma-Farkındalık ve Caydırma* (s. 349-370). Ankara: Grafiker Yayıncılık.

Erdemir Grubu. (2015, Mayıs 9). *İç Denetim Sistemi*. Mart 7, 2019 tarihinde https://slideplayer.biz.tr/slide/4870511/ adresinden alındı.

Erol, S. E., & Sağıroğlu, Ş. (2018). Siber Güvenlik Farkındalığı, Önemi Ve Yapılması Gerekenler. Ş. Sağıroğlu, & M. Alkan içinde, *Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık* (s. 105-134). Ankara: Grafiker Yayınları.

IIA. (2016). *Assessing Cybersecurity Risk Roles of the Three Lines of Defense.* The Institute of Internal Auditors. https://www.aicpa.org.

IIA. (2018). *Global Bakış AÇıları ve Anlayışlar: 2018 Global Risk Raporu-İç Denetim Yöneticilerinin Karşılaştığı En Büyük Riskler.* The Institute Of Internal Auditing.

IIA. (2016). *Global Perspektifler ve Anlayışlar: Güvenilir Bir Siber Danışman Olarak İç Denetim.* The Institute of Internal Auditors.

IIA. (2017). *Küresel Bakış Açıları ve Anlayışlar Yapay Zeka - İç Denetim Mesleğine İlişkin Dikkate Alınması Gerkenler.* The Institute of Internal Auditors.

ISACA. (2017). *Auditing: Cyber Security Evaluating Risk and Auditing Controls.*

Kahyaoglu, S. B., & Caliyurt, K. (2018). Cyber security assurance process from the internal audit perspective. *Managerial Auditing Journal*, 360-376.

Kaya, B. (2017, 4 9). 3 10, 2019 tarihinde Şirketlerin Güvencesi Üçlü Savunma Hattı: http://bertankaya.net adresinden alındı.

KPMG. (2016). *Denetim Komiteleri İçin Siber Güvenlik.*

KPMG. (2016). GRC Gündemi: Yönetişim, Risk ve Uyumluluğu Anlamak.

Kumar, V., Srivastava, J., & Lazarevic, A. (2005). *Manager CyberThreats Issues, Approaches and Challenges.* U.S.A.: Springer.

Kurt, G., & UysaL, U. T. (2015). Siber Riskler ve COSO İç Kontrol Bütünleşik Çerçevesi. *Muhasebe ve Denetime Bakış dergisi* , 1-10.

Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., & Sadhukhan, S. K. (2013). Cyber-risk decision models: To insure IT or not? *Decision Support Systems* , 11-26.

Ojeka, S. A., Ben-Caleb, E., & Ekpe, E.-O. I. (2017). Cyber Security in the Nigerian Banking Sector: An Appraisal of Audit Committee Effectiveness. *International Review of Management and Marketing* , 340-346.

Öztürk, M. S. (2018). Siber Saldırılar, Siber Güvenlik Denetimleri Ve Bütüncül Bir Denetim Modeli Önerisi. *Muhasebe ve Vergi Uygulamaları Dergisi*, 208-232.

PWC. (2018). Global Economic Crime and Fraud Survey 2018.

Sabillon, R., Serra-Ruiz, J., Cavaller, V., & Cano, J. (2017). A Comprehensive Cybersecurity Audit Model to Improve

Cybersecurity Assurance: The CyberSecurity Audit Model (CSAM). *International Conference on Information Systems and Computer Science*, 253-259.

Sağıroğlu, Ş. (2018). Siber Güvenlik Ve Savunma: Önem, Tanımlar, Unsurlar Ve Önlemler. Ş. Sağıroğlu, & M. Alkan içinde, *Siber Güvenlik ve Savunma-Farkındalık ve Caydırıcılık* (s. 21-45). Ankara: Grafiker Yayınları.

Shackelford, S. J. (2012). Should your firm invest in cyber risk insurance? *Business Horizon*, 349-356.

SPK. (2018). Bilgi Sistemleri Bağımsız Denetim Tebliği. Sermaye Piyasası Kurulu.

SPK. (2018). Bilgi Sistemleri Yönetimi Tebliği. Sermaye Piyasası Kurulu.

The Institute of Risk Management. (2014). *Cyber Risk Executive Summary.*

İnternet kaynakları

Oxford Dictionaries. (1857). Mart 2019, 8 tarihinde https://en.oxforddictionaries.com adresinden alındı.

Türkiye İç Denetim Enstitüsü. (1994). Mart 2019, 10 tarihinde https://www.tide.org.tr adresinden alındı.