SİBER HİJYENİN SAĞLANMASINDA İÇ DENETİMİN ROLÜ[1]

(THE ROLE OF INTERNAL AUDITING IN PROVIDING CYBER HYGIENE)

Alptuğ GÜLER* / Ali Kasım ARKIN**

ÖZ

Dünya tarihinde en yıkıcı savaşlar olarak 1. ve 2. Dünya Savaşları kabul edilmektedir. Ancak bu durum artık değişmektedir. Siber dünyadaki siber savaşların siber saldırganları, kendilerini 7 gün / 24 saat hazırlamakta ve çok uzun olmayan bir gelecekte bir ameliyathanenin enerji sistemlerini kesintiye uğratma, metro hattındaki trenleri çarpıştırma, fabrikaların üretim hatlarını durdurma gibi teknolojik saldırı potansiyeline sahip olma yolunda ilerlemektedirler. Ülke, kurum ve kişisel kullanıcı olarak, teknolojik araçların sahip olduğu siber riskler göz önünde bulundurulduğunda bu risklerin kontrolü için siber güvenlik ve siber güvenlik risk yönetimi temelli yaklaşım önem kazanmaktadır. Siber hijyen, siber bilgi güvenliği ile ilgili temel bir ilkedir ve kişisel hijyenle benzerlik gösterdiği gibi, siber tehditlerden kaynaklanan riskleri en aza indirgemek için basit rutin önlemler almanın eşdeğeridir. Bu bağlamda, bir olgunluk modeli olarak siber hijyen, kişisel hijyen ile aynı önemde görülmeli ve bir kuruma düzgün şekilde entegre edildiğinde, kurumsal siber bağışıklık sistemleri ve sağlıklarının en iyi durumda olacağı göz önünde bulundurulmalıdır. Günümüz kurumları için bu denli kritik olan risk yönetimi ve siber güvenlik sitemleri için gerekli bağımsız güvence, iç denetim tarafından benzersiz bir şekilde sağlanabilir. İç denetçiler bu süreçte önemli danışmanlar olabilir. Bu bakımdan, siber güvenliğin oluşturulması sürecinde siber hijyenden başlayarak üçüncü savunma hattına kadar iç denetim faaliyetinin siber rolü her geçen gün artmaktadır.

Bu makalede, siber güvenlik ve siber hijyen bağlamında iç denetçilerin ve iç denetimin siber rolü değerlendirilmektedir.

Anahtar Kelimeler: Siber Güvenlik, Siber Hijyen, İç Denetim, Siber Güvenlik Yönetişimi, Siber Güvenlik Olgunluk Modeli

JEL Kodlaması: G32, M42

ABSTRACT

The most destructive wars in the history of the world are accepted as the first and second world wars. However, this situation is changing now. The cyber attackers of cyber wars in the cyber world prepare themselves for 7 days / 24 hours, and in the not too long future, they are on the way to interrupt the energy systems of an operating room, collide the trains in the subway line, and have the potential of technological attacks such as stopping the production lines of the factories. As a country, organization and personal user, the cyber security and cyber security risk management based approach is important for controlling these risks when the cyber risks of technological tools are taken into consideration. Cyber hygiene is a fundamental principle of cyber information security and is equivalent to personal hygiene and is equivalent to taking simple routine measures to minimize the risks associated with cyber threats. In this context, cyber hygiene as a model of maturity should be seen as of the same importance as personal hygiene, and when integrated properly into an organization, it should be considered that organizational cyber immune systems and health are in the best condition. The independent assurance for risk management and cyber security systems that are so critical for today's organizations can be uniquely provided by internal audit. Internal auditors may be important consultants in this process. In this respect, starting from cyber hygiene in the process of cyber security creation the cyber role of internal audit activity is increasing day by day until the third line of defense.

In this article, the cyber role of internal auditors and internal audit is evaluated in the context of cyber security and cyber hygiene

Keywords: *Cyber Security, Cyber Hygiene, Internal Auditing, Cyber Security Governance, Cyber Security Maturity Model*

JEL Classification: *G32, M42*

---

*) İç Denetçi (CGAP), Düzce Üniversitesi, Orcid: 0000-0001-8439-9511, alptugguler@duzce.edu.tr

**) İç Denetçi (CGAP,CCSA), Düzce Üniversitesi, Orcid: 0000-0002-6826-0998, aliarkin@duzce.edu.tr

Yazı Gönderim Tarihi: 21.03.2019, Yazı Kabul Tarihi: 11.04.2019

1) Bu çalışmaya görüş ve önerileriyle katkıda bulunan Gençlik ve Spor Bakanlığı İç Denetçisi Sayın Ahmet Kebeli'ye teşekkür ederiz.

1. GİRİŞ

Günümüzde dijital teknolojilere bağımlılığın artması ve dijital araçların hayatımızın her anını kapsaması, ülkeleri, kurumları, sıradan insanları siber dünyaya ve buna bağlı olarak siber güvenlik risklerine karşı daha duyarlı hale getirmiş durumdadır. Siber kavramı, toplumun tamamında üretkenlik gelişimini ve bilgileri tam zamanında dağıtımını sağlaması yönüyle vazgeçil(e)mez bir olgu haline gelmiştir. Siber kavramı ile hangi endüstrinin veya uygulamanın tanıtıldığı önemli değildir, odak noktasında verimlilik artışı yer almaktadır. Bununla birlikte, bilginin siber alana hızlı bir şekilde iletilmesi genellikle genel sistem güvenliğini azaltmaktadır. Siber dünya hayatımıza birçok kolaylıklar getirirken, yanında belirsizlikleri ve kırılganlıkları da getirmektedir. Bu belirsizlikler ve kırılganlıkların önemli kısmı, bilgisayar korsanları ve siber saldırganların yaşam alanı buldukları ülkeleri, kurumları, kurum çalışanlarını, sıradan insanları tehdit ederek adeta siber terör estirmelerinden kaynaklanmaktadır.

Teknolojik gelişmeler, son on yılda altyapı gelişimi ile ilgili riskleri kökten değiştirmiştir. Bir ülkenin elektrik sistemine yapılacak başarılı bir siber saldırı yıkıcı etkileri tetikleyebilir (WEF, 2019: 83). Hizmet sektörünün enerji sistemlerini siber saldırılara karşı korumak için 2017 yılında 1,7 milyar ABD doları harcadığı tahmin edilmektedir (Nhede, 2017). Modern, birbirine bağlı olan küresel ekonomide, siber sistemler sürekli saldırı altındadır. Bugün milyarlarca kullanıcı ve internet cihazının (nesnelerin interneti) beslediği çok boyutlu bir bağlanabilirlik ortamı, saldırganların artık daha fazla kişiyi daha fazla cihaz üzerinden rahatsız edebilecekleri ve her yıl daha fazla ihlal, daha fazla etkilenen kurum ve kullanıcı ve daha fazla hasar olduğu anlamına gelmektedir[2] (GAC 16, 2016: 4).

Siber saldırganlar her gün daha sofistike ve daha yıkıcı olmaktadırlar. Bu durum karşısında kurumlar kendilerine "asla başımıza gelmez" demeye devam edemezler. Artık tüm kurumların bilgi güvenliği operasyonlarını modernize etmeleri ve daha da gelişmiş tehditlerle dolu bir geleceğe hazırlanma zamanı gelmiştir (Ling, 2017: 286). Hiç kimsenin siber saldırılara karşı kesin bir bağışıklık kazanmadığı açıkça anlaşılmaktadır. Artan sayıda bilgisayar ve ağ güvenliği ihlali rapor edildiğinden, genellikle binlerce hatta milyonlarca vatandaşı etkileyen, siber güvenliğe olan ilgi artmıştır. Aynı zamanda, tüm sektörler, güvendikleri kritik siber altyapılara bağımlılıklarını anlamaya çalışmaktadırlar. Dolayısıyla, her geçen gün daha fazla kurum, artan tehdidi ele almak için siber güvenlik programları geliştirmeye çalışmaktadır. Devletler ve topluluklar, uygulanabilir ve sürdürülebilir siber güvenlik programları oluşturmaya çalışan kurumlar arasındadır. Ancak devletler ve topluluklar, hem kamu hem de özel kurumlara dayanan ve hizmet veren karmaşık organizasyonlar olarak, siber riskleri güvence altına alma yönünde nasıl ve nereden başlayacakları konusunda kafa karışıklığı içerisindedirler. Kurumlardaki kafa karışıklığının giderilmesi için ele almaları gereken öncelikli soru(n)lardan biri, tam olarak ne tür bir siber olaya hazırlıklı olmaları gerektiğidir (Whit, 2011: 173).

İşlerinin kesintiye uğramasını istemeyen hemen hemen her ölçekteki kurum için bütünsel bir siber güvenlik sistemi kaçınılmaz bir gerçeklik haline gelmiş durumdadır. Kurumların kuracağı herhangi bir siber güvenlik programının temel hedeflerinden biri, olası saldırıların çekiciliğini sınırlandırmak olmalıdır. Zira bir saldırganın bir sisteme girmesi ne kadar uzun sürerse hedef o kadar az arzu edilir hale gelir. Bahsedilen siber tehditlere dur demek için; ister ülke çapında olsun, ister bir kurum çapında olsun, isterse de sıradan bir bilgi teknolojisi kullanıcı olsun bir siber güvenlik kalkanına ihtiyaç vardır. Bu kalkanı bir siber mücadele aracı yapacak olan kavram ise etkin bir siber hijyen anlayışıdır.

Çalışmanın konusunu siber güvenlik çalışmalarında kurum bazında önem kazanması beklenen siber hijyen kavramı ve iç denetim faaliyetinin siber rolü oluşturmaktadır. Çalışmanın ana amacı; odağına siber güvenliği alarak iç denetimim siber dünyada üstlenmesi gereken rolü ile siber hijyenin kurumlara sağlayacağı katkının çerçevesini çizmek ve bunun temelini oluşturmaktır. Çalışmada yöntem olarak,

2) 2016 itibariyle, 1.789.393 maruz kalma kaydında 1.093 veri ihlali açığa çıkarılmıştır (ITRC, 2017: 4). 2017 yılında 197.612.748 maruz kalma kaydında 1.632 veri ihlali açığa çıkarılmış ve buna karşılık 2018 yılında 446.515.334 maruz kalma kaydında 1.244 veri ihlali açığa çıkarılmıştır (ITRC, 2019: 2).

siber uzayın artık yadsınamaz bir gerçekliği olan siber güvenlik temelinde siber hijyen olgusu literatür üzerinden irdelenmekte, iç denetçilerin ve iç denetimin siber rolüne ilişkin çıkarımlar yapılmaktadır. Çalışma üç bölümden oluşmaktadır. İlk bölümde siber güvenliğin tanımı ve içeriği açıklanmıştır. İkinci bölümde, kurumların sürdürülebilir bir siber hijyen için siber olgunluk modelleri işlenmiş ve atılması gereken adımlar açıklanmıştır. Son olarak üçüncü bölümde iç denetim faaliyetinin siber güvenlik ve siber hijyende rolü ile siber güvenlik denetiminin kavramsal içeriği paylaşılmıştır.

2. SİBER GÜVENLİK

Siber güvenlik son birkaç yıldır ön plana çıkmıştır. Siber olayların artan sayısı ve ciddiyeti ile medyanın bu tür olaylara odaklanması her yerde kurum yöneticilerinin dikkatini çekmektedir (Hermans ve Diemont, 2017: 109). Son yıllarda siber teknolojinin hızla gelişmesi nedeniyle; kurumlarda, kuruluşlarda ve cihazlarda bilgisayar sistemlerinin korunması sağlanmış, tehditlere ve saldırılara güçlendirme sağlanmıştır. Veri sızmasından ağ çöküşüne kadar değişen siber güvenlik ve gizlilik olayları geçmiş yıllara göre daha sık yaşanmakta ve bunlar günümüz toplumunda en büyük tehditler haline gelmektedir (Li, Chen ve Susilo, 2019a: ix). Günümüzün bilgi teknolojisi, hızlı değişen, artan bağlantı (örneğin, nesnelerin interneti, bulut bilişim, mobil ağ) ve sürekli artan veri hacmi ile karakterize edilmektedir. Birbirine daha bağlı ve birbirine bağımlı bir bilgi teknolojisi ortamı, siber güvenlik olaylarından kaynaklanan ticari etkilerin artmasına neden olmaktadır. Böyle dinamik bir ortamda riski azaltmak için, güçlü bir yapılanma yoluyla siber güvenlik, bilgi sistemleri geliştirme yaşam döngüsünde olmazsa olmaz bir unsur haline gelmiştir (Wyatt, 2017: 336).

Siber güvenlik, Information Systems Audit and Control Association (ISACA) tarafından; bilgi işlemlerinin işlenen, depolanan ve internet üzerinden çalışan bilgi sistemleri tarafından taşınan bilgilere yönelik tehditleri (ve riskleri) ele alarak koruma olarak tanımlanmaktadır. Siber riskler, bilgi ve iletişim teknolojisi (BİT) sistemlerinin birbirine bağlanmasından kaynaklanan risklerdir. Modern kurumlar için bu bağlantılar kurum içinde, tedarikçileri ve müşterileri arasında ve çalışanlarıyla veya çalışanın kendi cihazlarında mevcuttur (Sunde, 2017: 271). Siber güvenlik, bir kurumun operasyonlarının etkinliği ve etkililiği, iç ve dış raporlamanın güvenilirliği ve geçerli yasal ve düzenlemelere uygunluğu ile ilgili hedeflerini destekleyen sistemlerle ilgilidir (GTAG, 2016: 5). Diğer bir tanım olarak siber güvenlik, kurumların bilgi varlıklarını iç ve dış tehditlere karşı korumak için kullanılabilecekleri araçlar, politikalar, güvenlik kavramları, güvenlik önlemleri, kurallar, risk yönetimi yaklaşımları, eylemler, eğitim, en iyi uygulamalar, güvence ve teknolojilerin toplanması olarak tanımlanmaktadır (SAMA, 2017: 5). Siber güvenlik, kurumun ve kullanıcı varlıklarının siber ortamdaki ilgili güvenlik risklerine karşı güvenlik özelliklerinin elde edilmesini ve bakımını sağlamayı amaçlar. Genel güvenlik hedefleri aşağıdakileri içerir (ITU-T X.1208, 2014: 2):

1- Erişilebilirlik (Kullanılabilirlik)
2- Bütünlük (doğruluğu ve reddedilmemeyi içerebilecek)
3- Gizlilik

Siber güvenlik, büyüklüklerinden veya faaliyet gösterdikleri sektörden bağımsız olarak, birçok kurumun yönetimi ve üst düzey yöneticileri için büyük bir endişe haline gelmiştir. Çoğu kurum için, siber güvenlik, kurumun karşı karşıya olduğu diğer ticari risklerle birlikte tanımlanması, değerlendirilmesi ve yönetilmesi gereken önemli bir iş riskidir ve kurum içindeki yalnızca bilgi teknolojisinde olanların değil tüm çalışanların ve yönetimin sorumluluğundadır. Bu iş sorununu yönetmek özellikle zordur, çünkü oldukça karmaşık bir siber güvenlik risk yönetimi programına sahip bir kurum bile maddi bir siber güvenlik ihlalinin ortaya çıkması ve zamanında tespit edilememesi riskini taşımaktadır (AICPA, 2017: 1). Siber suçun görülme sıklığı, kapsamı ve etkisi, bu konuyu Bilgi Teknolojisi (BT) departmanının sınırlarından üst düzey yöneticilerin ve kurumların, hükümetlerin ve diğer işletmelerin ofislerine kadar yükseltmiş durumdadır. Bir siber saldırının ciddi finansal, operasyonel ve kurumsal itibara zarar verme potansiyeli ortaya çıktıkça, siber güvenlik bir kurumun en üst düzeyde yönetilmesi gereken kritik bir risk olarak kabul edilmektedir (IIAC, 2015: 4).

Veri olaylarının büyüklüğü artmaya devam ederken, en dikkat çekici gelişme bu olayların arkasındakilerin

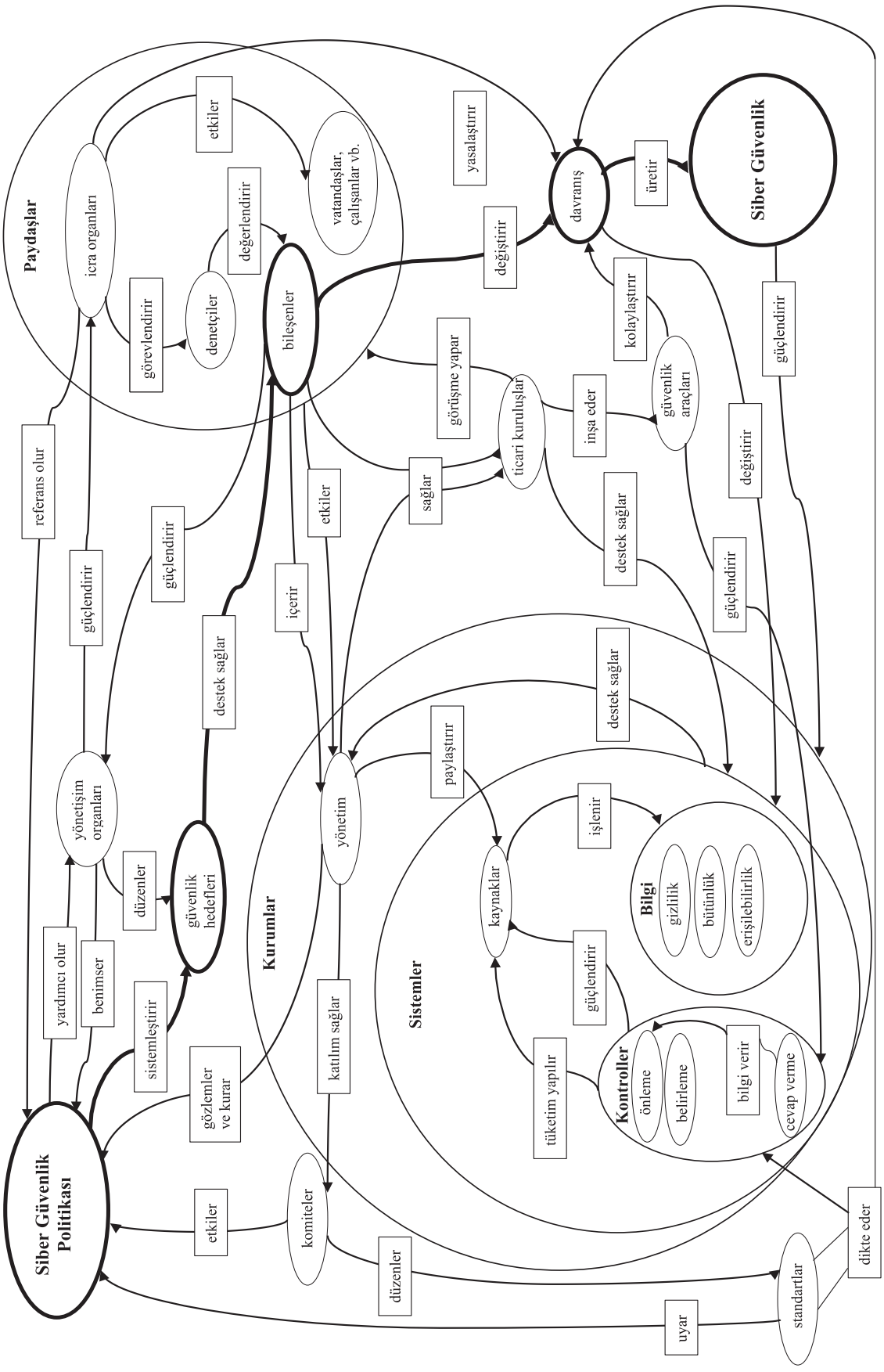
artan karmaşıklığıdır. Siber saldırganların iş modelleri gelişmiş ve daha karmaşık yöntemler kullanmanın yanı sıra, hedefleri de değişmiştir (McCarthy Tétrault, 2017: 4). Kurumlara yönelik saldırıları planlarken ve uygularken bilgisayar korsanları ve siber saldırganlar genellikle bütünsel bir yaklaşım sergilemektedirler. Bilgisayar korsanları ve siber saldırganlar, kurumların hassas işlerini, kurumsal bilgilerini ve kritik kaynaklarını korumak için inşa ettikleri önemli savunmaların üstesinden nasıl gelinebileceğini en iyi şekilde düşünmektedirler. (Hale, 2017: xxviii). Saldırganlar yaklaşımlarında yenilikçidir ve hedefleri genellikle savunma duruşunu bozmaya yöneliktir. Bu sebeple kurumlar için belki de siber güvenlikten daha önemli olan siber esnekliktir. Esneklik, "bilinmeyen ve bilinen tehditlere karşı hızlı bir şekilde dayanma ve kurtarma yeteneği" ile ilgilidir (Linkov vd., 2013: 471). Siber esnekliğe sahip olmak, saldırıları önlemek ve gerekli kurumsal işlevleri sürdürmek veya hızla eski duruma gelmek anlamına gelmektedir. Siber tehditler giderek daha karmaşık hale geldikçe, kurumlar sadece siber güvenliği ele almaya değil, aynı zamanda aşırı bağlantılı dünyamızda başarılı olmak için siber esnekliğe odaklanmalıdır (Keys ve Shapiro, 2019: 69). Siber esnekliğin arttırılması, kamu ve özel sektörlerin yeni ve yenilikçi yollarla işbirliği yapmalarını gerektirmektedir (WEF, 2018: 5).

Siber güvenlikte temel zorluk, sistemlerinizin bütünlüğünü ve gizliliğini korurken dijital hizmet kullanılabilirliğini sağlamaktır. Siber risklerin temel özelliği, risk azaltıcı kontrollerin etkinliğinin devamlı ve sürekli izlenmesini gerektirmeleridir. Sistemler çevrimiçi ve birbirine bağlı olmak üzere 7 gün / 24 saat olarak çalışmaktadır. Bu durum daha organize ve yüksek vasıflı siber saldırganların artan tehditleriyle bir araya geldiğinde, sistemleri korumak için gereken çabayı çok zorlaştırmaktadır. Bu nedenle koruma, herhangi bir kurumun farklı tarafları veya farklı savunma hatları tarafından birleştirilmiş bir çaba olmalıdır (Sunde, 2017: 272).

Verimlilik geliştirmeleri yapan teknoloji uzmanları için, güvenlik önlemleri, kullanıcının erişimini azaltan, engelleyen veya geciktiren önleme önlemleri, hayati önem taşıyan sistem kaynaklarını tüketen tespit önlemleri ve yönetim dikkatini sağlayan sistem özelliklerinden yönlendiren yanıt gereksinimleri nedeniyle, ilerlemeye doğrudan karşı çıkıyor gibi görünmektedir. Siber işlevsellik talebi ile güvenlik gereksinimleri arasındaki mevcut bu gerilim, "siber güvenlik politikası" ile ele alınmaktadır (Bayuk vd., 2012: 3). Yöneticiler, yönetimin siber güvenliğe yönelik kurumsal çapında uygun bir yaklaşım benimsendiğine dair güvence sağlamalıdır (NACD, 2017: 16). Bu güvence bir siber güvenlik politika belgesine bağlanmalıdır. Siber güvenlik politikasının tek bir tanım yoktur, ancak siber güvenlik terimi bir politika açıklamasına sıfat olarak uygulandığında ortak bir tema vardır. Genel olarak, "siber güvenlik politikası" terimi, siber güvenliği korumak için tasarlanmış yönergeleri ifade etmektedir (Bayuk vd., 2012: 4).

Şekil 1'de gösterildiği gibi, politikanın rolünün, siber güvenliğe ulaşması beklenen davranış kuralları için kuralların belirleneceği bir temel sağlamak olduğu unutulmamalıdır. Çok farklı politika bildirimlerine ve ilgili kurallara sahip olan çok çeşitli siber alanlar vardır. Siber güvenlik hedefleri doğrudan davranışa dönüşmemektedir, ancak siber güvenlik hedeflerine dayanan bir siber güvenlik stratejisinin daha iyi bir siber güvenlik politikası ile sonuçlanması beklenmektedir. Kurumlar, teknoloji kontrolleri ve ilgili operasyonel süreçleri uygulamak için standartlar oluşturmakta ve kurucular bu standartları politikaya uymak için kullanmaktadırlar. Standartların kendileri politika değildir. Aksine, politika hedeflerinden bir dizi teknolojiye ve operasyonel sürece yapılan çevirilerdir (Bayuk vd., 2012: 6).

Herhangi bir siber güvenli politikasının başarısında özellikle yönetimin, genel kurumsal bilgi güvenliği stratejisini desteklemek için yeterli kaynakları tahsis etmesi önemlidir (ITGI, 2006: 17). Ancak toplam siber güvenlik gerçekçi olmayan bir amaçtır. Siber güvenlik (genel olarak güvenlikte olduğu gibi) bir son durum değil bir sürekliliktir ve güvenlik de uyumun bir eşdeğeri değildir (NACD, 2017: 18). Bu sürekliliği sağlayacak ana kavram ise siber hijyen olacaktır. Bir kurum için siber güvenlik politikasının siber hijyen odağıyla bağlantılı olarak donanım ve yazılımların düzenli olarak doğrulanması, güvenlik sisteminin yapılandırılması, kurum içerisindeki kullanıcı ayrıcalıklarının kontrol edilmesi, denetlenmesi, kullanıcıların eğitilmesi vb. unsurlar siber başarının temel adımları olmalıdır.



Şekil 1. Siber Güvenlik Politikasına Bakış

(Bayuk vd., 2012: 5)

3. SİBER HİJYEN

Siber saldırıların hem sıklığı ve hem de etkisi her geçen gün artmaktadır. En başarılı saldırılar bilinen güvenlik sorunlarından yararlanmaktadır. Siber saldırıların yaklaşık % 80'inin kurban kurumlarında zayıf siber alışkanlıkların olduğu görülmektedir. Bu durumu ele almak için, düzenli, etkili güvenlik önlemleri almanın önemini vurgulayan bir siber hijyen stratejisi uygulanmalıdır. Bu, bir siber saldırının kurbanı olma veya bir siber saldırının etkisini diğer kurumlara yayma risklerini en aza indirecektir. Bu bağlamda siber hijyen bir kuruma düzgün şekilde entegre edildiğinde, kurumların çevrimiçi sağlık durumunun en iyi durumda olduğundan emin olmak için günlük rutinler, iyi davranışlar ve düzenli yapılan kontrollerin uygulanması yeterli olacaktır (ENISA, 2016: 6). Siber hijyen, bilgi güvenliği ile ilgili temel bir ilkedir ve kişisel hijyenle benzerlik gösterdiği gibi, siber tehditlerden kaynaklanan riskleri en aza indirgemek için basit rutin önlemler almanın eşdeğeridir. Altta yatan varsayım iyi siber hijyen uygulamalarının, savunmasız bir kurumun saldırılara maruz kalma riskini azaltarak, kurumlar arasında artan bağışıklık kazanabileceği yönündedir (ENISA, 2016: 14).

Geleneksel bilgi güvenliği modelleri bugünün gerçeklerine hitap edememektedir. Bu modeller, ofisin arkasını emniyet altına almayı hedeflerken, hala büyük ölçüde teknoloji odaklı, uyum temelli ve çevre odaklı bir yaklaşıma ihtiyaç vardır. BT siber güvenlik hijyeni genellikle eksiktir ve etkin olmayan erişim kontrolleri, 2015 yılında kaybedilen veya çalınan yarım milyar kişisel kayıtlara doğrudan katkıda bulunmuştur (Villiers, 2017: 321). Siber hijyen, birçok siber güvenlik olayından sorumlu olan az sayıdaki kök nedeni için önerilen önlem alma uygulamalarını açıklamaktadır. Birkaç basit uygulama bu yaygın kök nedenleri ele alabilir. Örneğin bir yama, siber hijyenin özellikle önemli bir bileşenidir, ancak mevcut araçlar ve işlemler çoğu zaman bu ortamlarda ve durumlarda bu riski hızla azaltmak için yetersizdir (Souppaya vd., 2018: 2). Bu nedenle sağlam bir siber güvenlik "Çin Seddi" kurulmalıdır, ancak özellikle insan faktörlerinden kaynaklanan güvenlik açıkları nedeniyle güvenlik cihazlarının ve sistemlerinin en iyileri tehlikeye girebilir. Bilgi sistemleri kurumdaki herkes tarafından kullanıldığından, bilgi güvenliği hijyenine uyma sıkıntısı da beraberinde gelir. İyi tasarlanmış güvenlik sistemleri, uygun kurum kültürü, eğitim, farkındalık, uyum ve denetim, güvenli davranış sergileyen kullanıcılarda çok önemli bir rol oynamaktadır (Totade ve Godbole, 2017: 243). Siber hijyen uygulamaları saldırganların başarılı olmalarını zorlaştırmakta ve saldırıların sebep olabileceği hasarı azaltabilmektedir (Souppaya vd., 2018: 4).

Önümüzdeki yıllarda ulusal düzeydeki tüm savunma paydaşları arasında, en karmaşık ve en güçlü siber savunma sistemleri kadar temel siber hijyen becerilerini ve farkındalığını arttırmak öncelik olacaktır. Çeşitli ülkelerde siber temelli güvenlik programları; özellikle küçük kurumlara yönelik olarak en temel kontrol ve güvenlik uygulamalarını benimsemelerini teşvik etmek amacıyla oluşturulmuştur ve iyi siber hijyenin işletmelerin karşılaştığı tehditlerin yüzde 80›ini karşılayacağı prensibi üzerine çalışmaktadır (Caravelli ve Jones, 2019). Bununla beraber kurumsal risk yönetimi sistemi yetenekleri de yıllar geçtikçe olgunlaşmaktadır. Aynı durum siber risk yönetim sistemi için de geçerlidir (Antonucci ve Verstichel, 2017: 375-376). Etkin bir siber risk yönetimi kurum bünyesinde içselleştirilmiş bir modele dayanmalıdır. Bu model siber hijyeni kurum bünyesinde hem yatay ve hem de dikey olarak yayabilmeli ve çalıştırabilmelidir.

3.1. Siber Hijyen İçin Siber Güvenlik Olgunluk Modeli

Olgunluk modeli, belirli bir disiplinde yetenek ve ilerlemeyi temsil eden bir dizi özellik, gösterge veya yapıdır. Model içeriği tipik olarak en iyi uygulamaları örneklendirir ve standartları veya disiplinin diğer uygulama kurallarını içerebilir. Dolayısıyla bir olgunluk modeli, bir kurumun uygulamalarının, süreçlerinin ve yöntemlerinin mevcut yetenek seviyesini değerlendirebileceği ve iyileştirme için hedef ve öncelikleri belirleyebildiğine dair bir kıyaslama sağlamaktadır (ONG-C2M2, 2014: 5).

Mevcut durumu analiz etmek için, diğer siber güvenlik kontrolleri değerlendirilirken ve yeni teknoloji, insanlar veya süreç kontrolleri uygulanırken istenen duruma yönelik bir siber güvenlik programı olgunluk modeli de uygulanabilir. Farklı kurum ve çerçevelerin artan olgunluk seviyeleri için çeşitli isimleri var-

dır; bununla birlikte çoğu, olgunluğu göstermek için bir olgunluk modeline bağlı kalır (ISACA, 2017: 12). Siber (güvenlik) hijyen seviyesi, önceden tanımlanmış bir siber güvenlik olgunluk modeli ile ölçülebilir. Siber güvenlik olgunluk modeli aşağıdaki Tablo 1'de özetlenen 6 olgunluk seviyesi ile (0, 1, 2, 3, 4 ve 5) belirlenmektedir. Seviye 3, 4 ya da 5'e ulaşmak için, bir kurumun öncelikle önceki olgunluk seviyelerinin (ölçütlerinin) tüm kriterlerini karşılaması gerekmektedir (SAMA, 2017: 10).

Tablo 1. Siber Güvenlik Olgunluk Modeli-1

Olgunluk Seviyesi	Tanım ve Kriterler	Açıklama
0 (Mevcut Değil)	• Herhangi bir dokümantasyon yoktur. • Bazı siber güvenlik kontrolleri için farkındalık veya dikkat yoktur.	• Siber güvenlik kontrolleri yerinde değildir. Belirli bir risk alanı hakkında herhangi bir farkındalık olmayabilir veya bu siber güvenlik kontrollerini uygulamak için mevcut planlar olmayabilir.
1 (Geçici)	• Siber güvenlik kontrolleri tanımlanmamış veya kısmen tanımlanmıştır. • Siber güvenlik kontrolleri tutarsız bir şekilde gerçekleştirilmektedir. • Siber güvenlik kontrolleri tam olarak tanımlanmamıştır.	• Siber güvenlik kontrol tasarımı ve uygulaması ilgili bölüme veya kuruma göre değişir. • Siber güvenlik kontrol tasarımı, tespit edilen riski sadece kısmen azaltabilir ve uygulama tutarsız olabilir.
2 (Tekrarlanabilir ancak gayri resmi)	• Siber güvenlik kontrolünün yürütülmesi, standartlaştırılmış olsa da, gayri resmi ve yazılı olmayan bir uygulamaya dayanmaktadır.	• Tekrarlanabilir siber güvenlik kontrolleri yerindedir. Bununla birlikte, kontrol hedefleri ve tasarımı resmi olarak tanımlanmamış veya onaylanmamıştır. • Yapılandırılmış bir gözden geçirme veya kontrolün test edilmesi konusunda sınırlı bir değerlendirme vardır.
3 (Yapısal ve resmileştirilmiş)	• Siber güvenlik kontrolleri, yapılandırılmış ve resmileştirilmiş bir şekilde tanımlanır, onaylanır ve uygulanır. • Siber güvenlik kontrollerinin uygulanması gösterilebilir.	• Siber güvenlik politikaları, standartları ve prosedürleri oluşturulmuştur. • Siber güvenlik belgelerine uyum, yani politikalar, standartlar ve prosedürler, tercihen bir yönetişim, risk ve uyum (GRC)[3] aracı kullanılarak izlenir. • Uygulamanın değerlendirilmesi için kilit performans göstergeleri tanımlanır, izlenir ve raporlanır.
4 (Yönetilebilir ve ölçülebilir)	• Siber güvenlik kontrollerinin etkinliği periyodik olarak değerlendirilir ve gerektiğinde geliştirilir (iyileştirilir). • Bu periyodik ölçüm, değerlendirmeler ve iyileştirme fırsatları belgelenmiştir.	• Siber güvenlik kontrollerinin etkinliği ölçülmekte ve periyodik olarak değerlendirilmektedir. • Siber güvenlik kontrollerinin etkinliğini belirlemek için temel risk göstergeleri ve trend raporlaması kullanılmaktadır. • Ölçme ve değerlendirme sonuçları, siber güvenlik kontrollerinin iyileştirilmesine yönelik fırsatları belirlemek için kullanılır.
5 (Uyarlanabilir)	• Siber güvenlik kontrolleri sürekli bir iyileştirme planına tabidir.	• Kurumsal çapta siber güvenlik programı, siber güvenlik kontrollerinin sürekli uyumu, etkinliği ve iyileştirilmesine odaklanmaktadır. • Siber güvenlik kontrolleri, kurumsal risk yönetimi çerçevesi ve uygulamaları ile entegredir. • Siber güvenlik kontrollerinin performansı, emsal ve sektör verileri kullanılarak değerlendirilir.

(SAMA, 2017: 10)

3) GRC- Governance, Risk and Compliance

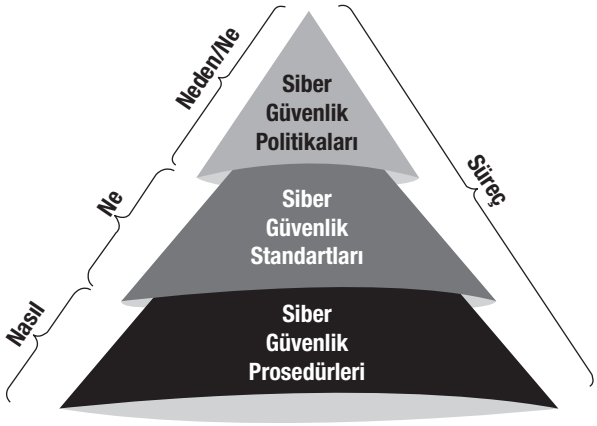
Modelin amacı, siber güvenliği ele almak ve siber güvenlik risklerini yönetmek için etkili bir yaklaşım oluşturmaktır. Uygun bir siber güvenlik olgunluk seviyesine ulaşmak için, kurumlar en azından aşağıda açıklanan 3 veya daha yüksek olgunluk seviyelerinde çalışmalıdır (SAMA, 2017: 10). Bu seviyeler aşağıda kısaca açıklanmıştır.

3.1.1. Olgunluk Seviyesi-3 (Yapısal ve Resmileştirilmiş)

BT faaliyetlerinin gözetimi ve yönetimi için bir kurum / süreç çerçevesi tanımlanmış ve kuruma BT yönetişiminin temeli olarak tanıtılmıştır. Yönetim birimleri, temel yönetişim faaliyetlerini kapsayan özel prosedürler geliştirerek rehberlik yapmıştır. Bunlar arasında düzenli hedef belirleme, performansın gözden geçirilmesi, planlanan ihtiyaçlara karşı yetenek değerlendirmesi, gerekli BT iyileştirmeleri için proje planlama ve fonlama yer almaktadır (ITGI, 2003: 48-49). Orta vadede detaylı, resmi işlemler tanımlanır. Kontroller onaylanmış ve tutarlıdır. Risk yönetimi uygulamaları ve analizleri işletme stratejilerine entegre edilmiştir (FFIEC, 2015: 7).

Seviye 3 olgunluğa ulaşmak için bir kurum, siber güvenlik kontrollerini tanımlamalı, onaylamalı ve uygulamalıdır. Ek olarak, siber güvenlik dokümantasyonuna uyumu da izlemelidir. Siber güvenlik dokümantasyonu "neden", "ne" ve "nasıl" siber güvenlik kontrollerinin uygulanması gerektiğini açıkça göstermelidir. Siber güvenlik dokümantasyonu Şekil 2'de gösterildiği gibi siber güvenlik politikaları, siber güvenlik standartları ve siber güvenlik prosedürlerinden oluşmaktadır (SAMA, 2017: 10).

Şekil 2. Siber Güvenlik Dokümantasyon Piramidi



(SAMA, 2017: 11)

Siber güvenlik politikası, kurumun yönetimi tarafından onaylanmalı ve siber güvenliğin kurum için neden önemli olduğunu belirtmelidir. Politika hangi bilgi varlıklarının korunması gerektiğini ve siber güvenlik ilke ve hedeflerinin belirlenmesi gerektiğini vurgulamalıdır. Siber güvenlik politikasına dayanarak, siber güvenlik standartları geliştirilmelidir. Bu standartlar, güvenlik ve sistem parametreleri, görevlerin ayrılması, şifre kuralları, olayların izlenmesi ve yedekleme kuralları gibi uygulanması gereken siber güvenlik kontrollerini tanımlamalıdır. Standartlar; siber güvenlik politikasını destekler ve güçlendirir. Siber güvenlik prosedürlerinde personel veya kurumun paydaşları tarafından yapılması gereken görevler detaylandırılmıştır. Bu prosedürler siber güvenlik kontrollerinin, görevlerinin ve faaliyetlerinin kurum ortamında nasıl yürütülmesi gerektiğini ve kurumun bilgi varlıklarının siber güvenlik politikası ve standartlarına göre korunmasını, desteklemesini öngörmektedir. Uygulamadaki gerçek ilerleme, siber güvenlik kontrollerinin performansı ve uyumu, anahtar performans göstergeleri (KPIs)[4] kullanılarak periyodik olarak izlenmeli ve değerlendirilmelidir (SAMA, 2017: 11). Anahtar performans göstergesi, bir kurumun hedeflere karşı nasıl performans gösterdiğini değerlendiren bir ölçümdür. Tanımlanmış bir hedef (tipik olarak) bir KPI metriğinin değerlendirilmesinde bir ölçüt sağlar (Rodriguez, 2017: 160).

3.1.2. Olgunluk Seviyesi-4 (Yönetilebilir ve Ölçülebilir)

Hedef belirlemede, iş açısından sonuçlar ile hedefler arasındaki ilişkilerde oldukça karmaşık bir aşamaya gelinmiş ve BT süreç iyileştirme önlemleri şimdi daha iyi anlaşılmaktadır. Gerçek sonuçlar, yönetime bir karne kartı şeklinde iletilmektedir. Kurumun yönetimi bu seviyede BT değer sunumunu en üst düzeye çıkarmak ve BT ile ilgili riskleri yönetmek için ortak bir amaç için birlikte çalışmaktadır. BT yeteneklerinin düzenli olarak değerlendirmeleri yapıl-

4) KPIs-Key Performance Indicators

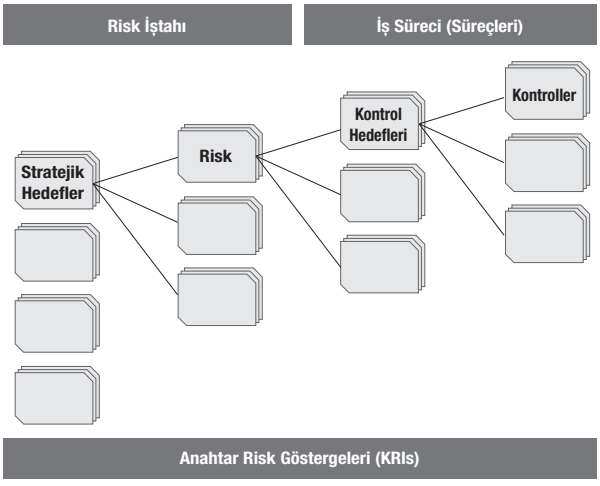
makta ve BT'nin performansında gerçek gelişmeler sağlayan projeler tamamlanmaktadır (ITGI, 2003: 49). Olgunluk, iş kolları arasında entegre olan siber güvenlik uygulamaları ve analitiklerle karakterize edilmektedir. Risk yönetimi süreçlerinin çoğunluğu otomatiktir ve sürekli süreç iyileştirmeyi içermektedir (FFIEC, 2015: 7).

Kurum, 4. olgunluk seviyesine ulaşmak için uygulanan siber güvenlik kontrollerinin etkinliğini periyodik olarak ölçmeli ve değerlendirmelidir. Siber güvenlik kontrollerinin etkili olup olmadığını ölçmek ve değerlendirmek için, anahtar risk göstergeleri (KRIs)[5] tanımlanmalıdır. Bir KRI, etkinlik ölçümü için normu gösterir ve gerçek ölçüm sonucunun hedeflenen normun altında mı yoksa üstünde mi olduğunu belirlemek için eşikleri tanımlamalıdır. KRI'ler eğilim raporlaması ve potansiyel iyileştirmelerin tanımlanması için kullanılır (SAMA, 2017: 11-12).

Her kurumun kendine özgü bir iş stratejisi, risk iştahı ve kurum kültürü vardır. Dijital çağda faaliyet gösteren bu faktörlerden bağımsız bir dizi siber risk de bulunmaktadır. Bunlar, web sitelerinin, e-postaların ve dijital cihazların neden olduğu ve bunlara zarar verebilecek riskleri içerir. Bu nedenle bir kurumun karşılaştığı belirli siber riskler, program ve ilgili KRI'ler gibi değişecektir. Tüm KRI'lerde olduğu gibi, daha geniş faaliyet risklerine bağlantı sağlayan KRI'lerin tasarlanması önemlidir (Rodriguez, 2017: 160-161).

Bir KRI programı oluştururken risk taksonomisine sahip olmak çok önemlidir. Kontrol düzeyindeki ölçüm ölçütler ile düşürülen riskler, sonuçta Şekil 3'de görüldüğü gibi stratejik hedeflerle olan ilişkisini destekler. Taksonomi aynı zamanda KRI'leri kullanan bir paydaş aralığında bir kuruluş içinde hesap verilebilirlik, cevap verme ve karar verme tutarlılığı konusunda netlik sağlar (Rodriguez, 2017: 161). KRI tasarımı kurumun karşılaştığı risklerin net bir görüntüsü ile başlar ve bu risklerin kontrol amaçlarına ve kilit kontrollere daha fazla sentezlenmesiyle devam eder (Şekil 3'deki gibi). Risk taksonomisinin bu unsurları, kurumun, endüstrinin en iyi uygulamalarının yanı sıra geçerli yasalar ve düzenlemeler tarafından yönlendirilen politika ve programlarla başlayan kapsamlı siber güvenlik programında daha belirgindir (Rodriguez, 2017: 162-163).

Şekil 3. Anahtar Risk Göstergeleri (KRIs) İçin Risk Taksonomisi



(Rodriguez, 2017: 162)

3.1.3. Olgunluk Seviyesi-5 (Uyarlanabilir)

BT yönetişim uygulamaları, etkili ve verimli teknikler kullanılarak karmaşık bir yaklaşım haline gelmiştir. Bu seviyede, BT faaliyetlerinde şeffaflık söz konusudur ve yönetim BT stratejisinin kontrolünü ele geçirmektedir. BT faaliyetleri en iyi şekilde gerçek iş öncelikleri için yönlendirilmekte ve önemli sapmaların veya problemlerin düzeltilmesi için zamanında önlem alınabilmektedir. Risk yönetimi (ve genel olarak BT yönetimi faaliyetleri) için harcanan çaba, standart ve mümkünse otomatikleştirilmiş süreçlerin benimsenmesi ile kolaylaştırılmıştır. BT yetkinliğinin sürekli iyileştirilmesi uygulaması kurum kültürüne dahil edilmiştir (ITGI, 2003: 49). Bu olgunluk seviyesindeki siber güvenlik kapasitesinin Şekil 4'te gösterildiği gibi beş boyuttan oluştuğu düşünülebilir (CMM, 2016: 5):

1- Siber güvenlik politikası ve stratejisinin geliştirilmesi,
2- Kurum içinde sorumlu siber güvenlik kültürünün teşvik edilmesi,
3- Siber güvenlik bilgisinin geliştirilmesi,
4- Etkili yasal ve düzenleyici çerçeveler oluşturulması ve
5- Standartlar, kurumlar ve teknolojiler aracılığıyla risklerin kontrol altına alınması.

5) KRIs-Key Risk Indicators

Şekil 4. Siber Güvenlik Kapasite Boyutları

(CMM, 2016: 5)

Bu beş boyutta, siber güvenlik kapasitesini arttırmaya çalışırken göz önünde bulundurulması gereken alanlar bir ülke kapsamında ele alınmıştır. Bu boyutların belirli konularda birbirleriyle örtüşebileceği kabul edilir ve aslında siber güvenlik kapasiteleri arasındaki karşılıklı bağımlılık mevcuttur. Her boyutta, her biri aşağıdaki gibi tanımlanmış çeşitli faktörler, yönler, olgunluk aşamaları ve siber güvenlik kapasitesi göstergeleri vardır (CMM, 2016: 5):

1. Boyut: Siber Güvenlik Politikası ve Stratejisi

Bu boyut ülkenin, siber güvenlik stratejisini geliştirme ve sağlama kapasitesini ve olay tepkisini, kriz yönetimini ve kritik altyapı koruma kapasitelerini geliştirerek siber güvenlik direncini arttırıyor. Siber güvenliğin sağlanması, erken uyarı, caydırıcılık, direnç ve toparlanma kabiliyetini içermektedir. Bu boyut, ulusal savunma ve esneklik kabiliyetini sağlamada etkili güvenlik politikasını göz önünde bulundurarken, genel olarak devlet, uluslararası ticaret ve toplum için hayati bir siber ortamın faydalarını korur (CMM, 2016: 14).

2. Boyut: Siber Kültür ve Toplum

Bu boyut, toplumdaki siber risklerin anlaşılması, internet servislerine güven düzeyi, e-devlet ve e-ticaret hizmetleri ve kullanıcıların kişisel bilgilerin korunmasını çevrimiçi olarak anlama gibi sorumlu bir siber güvenlik kültürünün önemli öğelerini incelemektedir. Ayrıca, bu faktör, kullanıcıların siber suçları rapor etmeleri için kanal olarak işlev gören raporlama mekanizmalarının varlığını araştırmaktadır. Ayrıca, bu faktör medya ve sosyal medyanın siber güvenlik değerlerini, tutumlarını ve davranışlarını şekillendirmedeki rolünü gözden geçirir (CMM, 2016: 25).

3. Boyut: Siber Güvenlik Eğitimi, Eğitimi ve Becerileri

Bu boyut, hem kamuoyu hem de yöneticiler için siber güvenlik bilinci artırma programlarının mevcudiyetini gözden geçirmektedir. Ayrıca, çeşitli hükümet paydaş grupları, özel sektör ve bir bütün olarak nüfus için eğitim ve öğretim tekliflerinin mevcudiyetini, kalitesini ve alımını değerlendirir (CMM, 2016: 32).

4. Boyut: Yasal ve Düzenleyici Çerçeveler

Bu boyut, hükümetin, BİT güvenliği, gizlilik ve veri koruma konularında ve diğer siber suçlarla ilgili konular üzerinde özellikle durularak doğrudan ve dolaylı olarak siber güvenlikle ilgili ulusal mevzuatı tasarlama ve çıkarma kapasitesini incelemektedir. Bu tür yasaları uygulama kapasitesi kanun uygulama, kovuşturma ve mahkeme kapasiteleriyle incelenir. Ayrıca, bu boyut, siber suçla mücadeleye yönelik resmi ve gayri resmi işbirliği çerçeveleri gibi konuları da gözlemlemektedir (CMM, 2016: 39).

5. Boyut: Standartlar, Kuruluşlar ve Teknolojiler

Bu boyut, bireyleri, kuruluşları ve ulusal altyapıyı korumak için siber güvenlik teknolojisinin etkin ve yaygın bir şekilde kullanılmasına yöneliktir. Boyut, siber güvenlik standartlarının ve iyi uygulamaların uygulanmasını, süreçlerin ve kontrollerin yayılmasını ve siber güvenlik risklerini azaltmak için teknolojilerin ve ürünlerin geliştirilmesini özel olarak incelemektedir (CMM, 2016: 49).

Olgunluk seviyesi 5, siber güvenlik kontrollerinin sürekli iyileştirilmesine odaklanmaktadır. Şekil 5'teki modelde gibi sürekli iyileştirme, siber güvenliğin amaç ve kazanımlarının sürekli analiz edilmesi ve yapısal iyileştirmelerin belirlenmesi ile sağlanır. Siber güvenlik kontrolleri, kurumsal risk yönetimi uygula-

Şekil 5. Siber Güvenlik Olgunluk Modeli-2

(KPMG, 2018: 2)

malarına entegre edilmeli ve otomatik gerçek zamanlı izleme ile desteklenmelidir. İş süreci sahipleri, siber güvenlik kontrollerinin uygunluğunu izlemek, siber güvenlik kontrollerinin etkinliğini ölçmek ve siber güvenlik kontrollerini kurumsal risk yönetimi çerçevesine dahil etmekten sorumlu olmalıdır. Ek olarak, siber güvenlik kontrollerinin performansı, emsal ve sektör verileri kullanılarak değerlendirilmelidir (SAMA, 2017: 12).

5. olgunluk seviyesi, kurumun ve endüstrinin siber riskleri yönetmesi için insanlarda, süreçlerde ve teknolojide yeniliğe yol açmasıyla karakterize edilmektedir. Bu durum yeni kontroller, yeni araçlar geliştirmek veya yeni bilgi paylaşım grupları oluşturmak anlamına gelebilir (FFIEC, 2015: 7). Siber hijyen için ulaşılması hedeflenen bu son seviye siber güvenlik anlayışın kurum kültürüne eklenmekten ziyade içselleştirme anlamına gelmektedir. Bu seviyede artık kurum her türlü siber saldırıya karşı hazırdır ve siber bağışıklık kazanılmıştır. Kurumun bu bağışıklığı kazanmasında kullanabileceği kurumsal araçlar çok çeşitlidir. Bu çeşitlilik içerisinde kurumun siber güvenlik politikalarına net bir bakış açısı sunabilecek en etkin araçlardan biri olarak iç denetim faaliyeti görünmektedir.

4. İÇ DENETÇİNİN VE İÇ DENETİMİN SİBER ROLÜ

Büyük veri, akıllı cihazlar, nesnelerin interneti, robotik proses otomasyonu, davranışsal analitik, üç boyutlu baskı gibi kavramlar kurumların artan dijitalleşmesine paralel olarak verimlilik ve maliyet etkinliği açısından önem kazanmaktadır. Ancak bu gelişmelerin kurumların operasyonlarına getirdiği artan riskler ve bunların kurumlara zarar vermesinin nasıl önleneceği iyice anlaşılmadır. Yalnızca BT sistemlerinin güvenlik açıklarına değil, kurum ortamına derinlemesine bakarak bu sistemlerin ürettiği verilere de ilişkin fikir edinilmesi gerekir. Mevcut portföydeki risklerin nasıl tespit edildikleri ve onları iyileştirmek için kurumun hangi stratejileri izlemesi gerektiği anlaşılır ve akıcı hale getirilmedir. Kurumlar bu konuda bilgi güvenliği uzmanlarına ve ekiplerine bu çabanın sorumluluğunu üstlenmesini isteyebilir. Siber risklere karşı güvenlik duvarları ve virüs koruma yazılımları yeterli çözüm değil midir? Keşke bu kadar basit olsaydı. Siber güvenlik, görünürlükle başlayan ve iç görü sağlayan, kapsamlı bir kurumsal çapta organizasyon çözümü gerektiren bir kurum sorunudur. Tehditleri ortaya çıkarmak, çözümün sadece bir parçasıdır. Kurumların BT uzmanları, tehditlerin nasıl ortaya çıka-

cağını tahmin etmesi ve bunlara yönelik stratejileri bildirmesi gerekir (Holmes ve Phillippe, 2017: 309-310). Teknolojinin hızla ilerlediği zamanımızda, BT uzmanları bile teknolojik değişimin nabzını tutmakta zorlanmaktadır. Öyleyse, iç denetçilerin bu siber çağda ortaya çıkan çeşitli riskleri yeterince değerlendirmeleri ve incelemeleri ve etkileriniz azaltmaları nasıl mümkün olabilir? Bu sorunun cevabı kısaca "bütüncül bir bakış açısıyla siber güvenlik sisteminin güçlendirilmesine yardımcı olmak" şeklinde verilebilir.

Bir kurumun iç denetim birimi, kurumun yönetişiminin, risk yönetiminin ve iç kontrol süreçlerinin etkinliğini değerlendirmek ve iyileştirmek için tasarlanan güvence ve danışmanlık faaliyetlerini yerine getirir. Bir iç denetim işlevi tarafından gerçekleştirilenlere benzer faaliyetler, bir kurum içindeki diğer unvanlar ile gerçekleştirilebilir. Bir iç denetim biriminin faaliyetlerinin bir kısmı veya tamamı bir üçüncü taraf servis sağlayıcıya dış kaynaklı olabilir. Örneğin, bir işletme (a) penetrasyon testini gerçekleştirmek için bir servis sağlayıcıyı çalıştırabilir; (b) İç denetim biriminin, işlevin yerine getirebilecek yetkinlik veya niteliklere sahip olmadığına dair sorumlulukları (örneğin, BT iç denetim işlevini yerine getirme) veya (c) yönetimin talebi üzerine tek seferlik özel bir değerlendirme yapabilir (AICPA, 2017: 46).

Kurumların bilgi sistemlerine ve yeni teknolojilerin geliştirilmesine dayanması, BT genelinin ve uygulama kontrollerinin geleneksel değerlendirmelerini siber güvenlik konusunda güvence sağlamak için yetersiz kılmaktadır. Siber güvenlik, bir kuruluşun bilgi varlıklarını (bilgisayarları, ağları, programları ve verileri) yetkisiz erişime karşı korumak için tasarlanmış teknolojiler, işlemler ve uygulamalar anlamına gelir. İç denetim faaliyeti, aşağıdakileri dikkate alarak bir kuruluşun siber güvenlik risklerini değerlendirmede çok önemli bir rol oynar (GTAG, 2016: 3):

1- Kuruluşun en değerli bilgilerine kim erişebilir?
2- Hangi varlıklar siber saldırılar için en olası hedefler?
3- Hangi sistemler tehlikeye girerse en önemli bozulmaya neden olur?
4- Yetkisiz kişilerce elde edilmesi durumunda hangi veriler finansal veya rekabetçi zararlara, yasal sonuçlara veya kurumun itibarına zarar verir?
5- Bir siber güvenlik olayı meydana gelirse, yönetim zamanında tepki vermeye hazır mıdır?

Kurumlar ve devlet kurumları için bilgilerin, iş süreçlerinin, uygulamaların ve sistemlerin mevcudiyeti, gizliliği ve bütünlüğüne yönelik artan tehditleri önlemek için uygulamaya konulan bilgi güvenliği yönetiminin önemli bir parçası iç denetim tarafından yerine getirilen **Siber Güvenlik Denetimi**dir. Uygulanan güvencelerin ve bilgi güvenliği sürecinin düzenli aralıklarla gözden geçirilmesiyle, bunların etkinliği, güncelliği, eksiksizliği ve uygunluğu ve dolayısıyla bilgi güvenliğinin mevcut durumu hakkında fikir vermek mümkündür. Bu nedenle, iç denetim, bir kurumda uygun bir güvenlik düzeyi belirlemek, elde etmek ve sürdürmek için bir araçtır. İç denetiminin temel görevi, bilgi güvenliğini uygularken ve optimize ederken yönetime, kurum yöneticilerine ve özellikle de BT'den sorumlu üst yöneticiye destek sağlamaktır. Denetimler bilgi güvenliği seviyesini iyileştirmek, yanlış bilgi güvenliği tasarımlarından kaçınmak ve güvenlik önlemlerinin ve güvenlik işlemlerinin verimliliğini optimize etmek için tasarlanmıştır. Bilgi güvenliği denetiminin bir sonucu olan denetim raporu, kurumun güvenlik durumunu, mevcut güvenlik eksikliklerine dayanarak yapılması gerekenler ile birlikte gösterir ve sonraki siber güvenlik optimizasyon sürecinde yardımcı olarak kullanılır. Denetim raporu, yönetim için bir bilgi kaynağı ve güvenlikten sorumlu herhangi biri tarafından kullanılabilecek bir araçtır (BSI, 2008: 5).

Teknoloji gelişmeye devam ettikçe, iç denetim de gelişmek zorundadır. Uzun yıllar boyunca, iç denetim birimleri, entegre denetimlerde ortak olarak BT denetim uzmanlarına güvenmiştir (Fountain, 2019: 19). Siber güvenlik için bağımsız güvence rolü, iç denetim tarafından benzersiz bir şekilde oynanabilir (Antonucci, 2017: 215). Dolasıyla günümüzde iç denetimin güncel çalışma portföyüne bir de siber rol eklenmektedir. İç denetçilerin siber güvenlik riskleri konusunda güvence sağlamak için güncellenmiş bir yaklaşıma ihtiyaçları vardır. BT genel kontrol değerlendirmeleri yararlı olsa da, siber güvenlik güvencesini sağlamada yetersizdirler, çünkü bunlar ne zamanında gerçekleştirilebilmektedir ne de tam değildirler. Bütünlük, doğruluk ve yetkilendirme gibi temel denetim hedefleri hala geçerlidir. Bununla birlikte, ortaya çıkan birçok faktör, siber güvenlik iddiaları hakkında değerli

sonuçlar sağlayan güncellenmiş bir iç denetim yaklaşımına ihtiyaç duymaktadır (GTAG, 2016: 4).

4.1. İç Denetim İçin Siber Güvenlik Risklerini ve Kontrollerini Değerlendirmeye Yönelik Bir Yaklaşım

Siber güvenlik yönetişimi, stratejik yönlendirme sağlayan, hedeflere ulaşılmasını sağlayan, riskleri uygun şekilde yöneten, kurumsal kaynakları sorumlu bir şekilde kullanan ve kurumsal güvenlik programının başarısını veya başarısızlığını izleyen bir kurumsal yönetim alt kümesidir (ITGI, 2006: 17). Şekil 6'da gösterilen çerçevenin birbirine bağlı altı bileşeni, yönetim siber güvenlik kontrollerinin ve yönetişiminin tasarım ve işletme etkinliğini değerlendirmek için kullanılabilir. Herhangi bir bileşendeki eksiklikler, siber güvenliğin genel etkinliğini etkileyeceğinden, her birinin diğerleriyle nasıl tasarlanıp işletildiğini değerlendirmek, iç denetime (iç denetim yöneticisine) kurumun siber güvenlik risklerini ele almak için ne kadar iyi hazırlandığını belirlemek için bir temel oluşturur. Bileşenler birlikte tasarlanmadığında veya iyi çalışmadığında, kurum siber tehditleri ve ortaya çıkan riskleri ele almak için hazır değildir demektir (GTAG, 2016: 17). Bu çerçevede, iç denetimin değerlendirmek durumunda olduğu bileşenler aşağıda açıklanmaktadır.

4.1.1. Siber Güvenlik Yönetişimi Bileşeni

Siber güvenlik yalnızca bir bilgi teknolojisi riski değildir. Kurum genelinde bir risktir ve bir yönetimin kurumsal risk yönetimi yetkisinin parçası olmalıdır (McCarthy Tétrault, 2017: 8). Siber güvenlik yönetişimi, güvenlik çabalarını tanımlayarak, yöneterek ve destekleyerek siber güvenlik yönetimi ve kontrolleri için gündem ve sınırları belirler (CBN, 2018: 3). İç denetim faaliyeti kurumun siber güvenlik yönetişimini anlamalıdır. 2100 numaralı IIA Standardı: yönetişim, risk yönetimi ve kontrol süreçlerinin iyileştirilmesine yönelik değerlendirme ve katkı sağlayan bir iç denetim faaliyetini gerektirmektedir.

Güçlü bir siber güvenlik yönetişimi şunlara bağlıdır (ITGI, 2006: 18; GTAG, 2016: 18):

Şekil 6. Siber Güvenlik Risk Değerlendirme Çerçevesi

(GTAG, 2016: 17)

1- Risk iştahı ve toleransı belirleme

2- Bir kesinti durumunda iş sürekliliği ve afet kurtarma için planlama

3- Güvenlik ihlallerine derhal yanıt verme

4- Bilgi güvenliği risk yönetimi metodolojisi

5- İş ve BT hedefleriyle açıkça bağlantılı kapsamlı bir güvenlik stratejisi

6- Etkili bir güvenlik organizasyon yapısı

7- Korunan ve sunulan bilgilerin değeri hakkında konuşan bir güvenlik stratejisi

8- Strateji, kontrol ve düzenlemenin her yönünü ele alan güvenlik politikaları

9- Her politika için eksiksiz bir güvenlik standardı seti

10- Siber güvenlik politikası ve politikalara uygun prosedürler

11- Uyumluluk sağlamak ve riskin etkililiği ve azaltılması konusunda geri bildirim sağlamak için kurumsallaşmış izleme süreçleri

12- Güvenlik politikalarının, standartlarının, prosedürlerinin ve risklerinin sürekli değerlendirilmesini ve güncellenmesini sağlayan bir süreç

13- Siber güvenlik riskleri ve tehditleri konusunda farkındalık kültürü

Güçlü bir siber güvenlik programı uygulamak, en son siber güvenlik araçlarını kullanmaktan daha fazlasını içerir. Önde gelen güvenlik araçlarının bile kısıtlamaları vardır ve eski sistemlerle entegrasyon zor olabilir. Siber güvenlik meselesi, son kullanıcıları ve BT uzmanlarını içeren bir olgudur. Ek olarak, güçlü siber güvenlik kurum kültürü, üst yöneticinin yanı sıra üst düzey risk yöneticisi, üst düzey işletme görevlisi, üst düzey bilgi yöneticisi ve diğer üst düzey liderlerin katılımını gerektiren kurumun başında başlayan bir kavramdır. Güçlü yönetici desteği olmadan, siber güvenlik, bir uyumluluk egzersizidir veya daha da kötüsü, kurumsal risk yönetimi meselesinden ziyade, sadece bir BT problemidir (Wyatt, 2017: 336-337).

Etkili bir yönetişim açıkça tanımlanmış politikalarda, ilgili araçlarda, yeterli personel ve konuya uygun eğitimle kanıtlanır. Farklı bakış açıları olan çok sayıda paydaş, yönetişimin kalitesini güçlendirmektedir. Bir siber güvenlik yönetişim komitesi, genellikle birinci, ikinci ve üçüncü savunma hattından üst yönetim ve temsilciliği içerir; teknoloji ve süreç sahipleri, müşteriler, servis sağlayıcılar ve tedarikçiler gibi potansiyel olarak kilit dış paydaşlardır. Olay müdahale ekipleri düzenli olarak yönetime rapor eder ve daha önce bilinmeyen boşluklara ek iç görü sağlamak için karşılaşılan ihlal türlerini bildirir. Yönetim daha sonra tespit edilen sorunları iyileştirme yoluyla izleyebilir (GTAG, 2016: 18).

4.1.2. Bilgi Varlıkları Envanteri Bileşeni

BT departmanı tüm bilgi varlıklarının güncel bir envanterini tutmalı ve kurumun amaçlarını ve sürdürme operasyonlarını ilerletmek için en gerekli olanları önceliklendirmelidir. Stratejik kurumsal hedef ve girişimleri karşılamak için, bu varlıklar geleneksel BT genel kontrollerinden ve periyodik değerlendirmelerden daha fazlasını gerektirir. En değerli varlıkları korumak için tasarlanmış önleyici ve izleyici kontrollerin devamlı bir etkinliğini sağlamak için sürekli izlenmesi gerekir (GTAG, 2016: 18).

Kuruluşun bilgi varlıkları değerlendirilirken aşağıdakiler göz önünde bulundurulmalıdır (GTAG, 2016: 18-19):

1-Veri

Türler (örneğin, işlemsel, BT yapılandırması, yapılandırılmamış)

Sınıflandırma (standardizasyon ve önceliklendirme sağlar)

Ortamlar (örneğin, veri ambarları, temel veri tabanları)

2-Teknoloji varlıklarının altyapı deposu

Sunucular

Ağ cihazları

Depolama

Son kullanıcı cihazları (örneğin dizüstü bilgisayarlar, mobil cihazlar)

3-Uygulamalar

4-Dış ilişkiler

Üçüncü tarafça barındırılan ortamlar

Veri dosyalarının dış kuruluşlarla paylaşılması (örneğin, satıcılar, düzenleyici kurumlar, hükümetler)

Hangi yazılım ve cihazların ağ üzerinde etkileşime girdiğini belirleme yeteneği siber tehditlere karşı savunma yapabilmek için esastır. Kurum bilinmeyen aygıtlara ve yazılımlara yapılan ağ saldırılarına karşı savunma yapamaz. Çalışanların kendi cihazlarını getirmelerine izin veren kurumlar, kurumsal ağ üzerinden verilere erişen daha büyük bir hacim ve çeşitli cihaz ve yazılımlar deneyimlemektedir. Çalışanların sahip olduğu cihazları kontrol etmek ve ağa olan bağlantı, yönetimin kilit odağını oluşturmalıdır. Giderek artan bir şekilde, daha fazla sayıda çalışanın kurumsal bilgilere rutin bir 8 saatlik çalışma süresini aşan belki de 24 saat süreyle erişebilmeleri gerektirmektedir. Bilinmeyen aygıtları algılama, doğrulama ve envanter oluşturma, kurumun, genel siber güvenlik stratejisinin etkili olmasını sağlamak için bu aygıtlardaki değişiklikleri izlemesine ve ölçmesine olanak sağlamaktadır (GTAG, 2016: 19).

4.1.3. Standart Güvenlik Yapılandırmaları Bileşeni

Birçok kurum, yüksek riskli sistemlerin daha sık test edildiği bir risk değerlendirmesine dayanarak test

Şekil 7. Fiziksel Güvenlik Risk Yönetim Sistemi

(Vandijck ve Lerberghe, 2018: 290)

edilecek sistemleri ve bunların test edilme sıklığını belirler. Yüksek riskli sistemlerin belirlenmesinde göz önünde bulundurulan faktörler, bu sistem tarafından içerilen veya erişilen verilerin hassasiyetini, sistemin operasyonel önemini ve bilinen tüm güvenlik açıklarının varlığını içerir (FINRA, 2018: 13).

Yönetim yazılımı kullanmak, sistemleri manuel olarak veya standart olmayan bir şekilde yönetmekten daha etkilidir. Bilgi güvenliği ve iç denetim faaliyeti, riske dayalı ortamların doğru bir şekilde değerlendirilebilmesini sağlamak için temel yapıları gözden geçirmelidir (GTAG, 2016: 19). Tipik bir siber rol olarak kurumun fiziksel güvenlik risk yönetim sistemi gözden geçirilebilir. Bunun için bir fiziksel güvenlik yönetim sisteminin nasıl planlanacağı uygulanacağı, izleneceği ve gözden geçirileceği Şekil 7'deki gibi belirlenmelidir. Bir **iç denetçinin yönetime raporlama yaparken izlemesi gereken adımlar** (Vandijck ve Lerberghe, 2017: 290-291):

1- Fiziksel güvenlik tehdidi alanı hakkında siber güvenlik ile ilgili net bir görüş edinin.
2- Fiziksel güvenlik sisteminin kurumun özellikle siber güvenlik ile nasıl ilişkili olduğunu anlayın: Kim ne yapar? Kaynaklar ve yeterlilikler nelerdir?
3- Siber güvenlikle ilgili olan güvenlik kontrollerini tanımlayın.
4- Bir kesinti olasılığını hesaplayarak kontrollerin etkinliğini değerlendirin.
5- Kontrollerin maliyet etkinliğini, toplam güvenlik maliyetlerine dayanarak haritalayın ve değerlendirin.
6- Fiziksel güvenlik risk yönetim sisteminin ne kadar olgun olduğu, siber güvenliği nasıl desteklediği, artırdığı ve uygulanabilir yasal ve düzenlemelere (örneğin veri odaları için katman gereksinimleri) ne kadar olgun olduğu konusunda net bir görüş edinin.

4.1.4. Bilgi Erişim Yönetimi Bileşeni

Yönetim, kullanıcılara iş rollerini temel alarak onaylama ve erişim sağlama süreci gibi önleyici kontroller

uygulamayı düşünmelidir. Ek olarak, çalışanların kurum içinde ne zaman hareket ettiğini tespit etmek için bir işlem, kullanıcı erişiminin ayarlanması ve yeni rolle ilgili olmasını sağlamak için yardımcı olacaktır. İç denetim faaliyeti, erişim seviyelerinin mevcut roller için haklı olduğunu doğrulamak için kilit verilere ve sistemlere kullanıcı erişimini gözden geçirebilir (GTAG, 2016: 19).

Ayrıcalıklı idari erişim özellikle önemlidir. Bilgiye erişme ve bilgileri salıverme özelliğine sahip kullanıcılar, siber güvenlik riskine karşı en hassastır. Yanlışlıkla kimlik avı denemelerinin bir sonucu olarak parolalarını yanlışlıkla bildirerek veya kötü amaçlı yazılım yükleyerek, kullanıcılar yetkisiz erişimi engellemek için tasarlanmış sistematik kontrol katmanlarını aşabilirler. Erişimi olan kişiler kuruluşun içinde ve dışında bulunur, bu nedenle verilerin içeride mi yoksa dışarıda mı barındırıldığına bakılmaksızın, anahtar verilere erişimi olan çalışanlara, danışmanlara ve satıcılara dikkat edilmelidir. Ayrıcalıklı erişime sahip kullanıcıların duyarlılık ve davranışlarını değerlendirmek ve erişimi sağlamak ve iptal etmek için önleyici kontrol faaliyetlerini onaylamak, kuruluşun siber güvenlik programının etkinliğinin öncü bir ölçüsüdür (GTAG, 2016: 20).

4.1.5. Ani Cevap ve İyileştirme Bileşeni

Uygulanan risk değerlendirmesi ve politika reçetelerinin sonucuna dayanarak, kurum uygun güvenlik özelliklerini ve kontrollerini tanımlayabilir veya tasarlayabilir. Güçlü bir siber güvenlik, derinlemesine savunma ilkesine dayanır. Beklenen koruma seviyesine ulaşıldığı ilgili kontroller katmanı (örneğin, erişim kontrolü, şifreleme ve izleme) eklenerek gerçekleştirilir. Böylece güvenlik tasarımı daha geniş güvenlik mimarisi ve sistem bağlantısı dikkate alınarak yapılır. Ek teknik olarak odaklanmış risk değerlendirmeleri (örneğin, teknik mimari, sistem ara yüzleri ve programlama dili) ilk uygulanan risk değerlendirmesini destekleyebilir (Wyatt, 2017: 338).

Kurumun riskleri hızla iletebilmesi ve düzeltebilmesi, programın etkinliğini ve olgunluk seviyesini gösterir. Olgun programlar, yönetim yanıtına verilen zamanı sürekli olarak kısaltabilir. Bu savunma hattının yansımaları şunlar olacaktır (GTAG, 2016: 20):

1- Önemli riskleri iletimi,

2- İyileştirmenin kabulü,

3- Çözüm için belirlenen sorunların takibi,

4- Kurum genelinde çözüme dair eğilim ve rapor.

4.1.6. Devam Eden İzleme Bileşeni

Bu çerçevenin son bir bileşeni olarak, yukarıda açıklanan beş bileşenin her birinin sürekli denetlenmesi, riskin nasıl yönetildiğini ve düzeltici faaliyetin ne kadar iyi çalıştığını belirlemeye yardımcı olacaktır. Etkili bir değerlendirme yaklaşımı rutin bir kontrol listesinden daha fazlasını gerektirir. İkinci savunma hattının, aşağıdakileri içeren davranışsal değişiklik üretmek için tasarlanmış bir izleme stratejisi uygulaması beklenir (GTAG, 2016: 20-21):

1- İlgili siber güvenlik riskini ölçmek için hassas bilgilere erişimi olan kişilerin izlenmesini içeren erişim seviyesi değerlendirmesi ve taraması: Kritik işlemler gerçekleştiren bir kullanıcı grubu için, ilgili BT varlıkları, güvenlik yapılandırmaları, sorunlu web siteleri, kötü amaçlı yazılım olayları ve veri sızma durumları arasındaki açıkları bulmak için sistematik bir yol geliştirmek yararlı olacaktır.

2- Güvenlik açığı değerlendirmesi yapılması: Düzenli olarak tarama sistemleri, ortamdaki güvenlik açıklarını tespit etmek için kritik öneme sahiptir. Güvenlik açıkları tanımlandıktan sonra, kategorize (örneğin kritik, büyük, orta) ve ele alındıktan sonra (örneğin, 30 gün içinde yüksek riskli sistemlerdeki tüm kritik güvenlik açıklarını ele alın), tespit edilen güvenlik açıkları için düzeltme etkinlikleri başlatılmalıdır.

3- Dış kaynak kullanımı genellikle kurumlar için en yüksek riskleri oluşturur ve öncelik almalıdır**:** Bununla birlikte, iyileştirme faaliyetleri sadece dışarıya bakan ortamlarla sınırlı değildir. Birinci ve ikinci hat kaynakları, Hizmet Seviyesi Anlaşmaları (SLAs)[6] tanımlamak ve üzerinde anlaşmak için

6) SLAs-Service Level Agreements

kurum genelinde çalışabilir ve iç denetim, yönetimin tanımlanmış SLA'lara uygun olup olmadığını değerlendirerek yardımcı olabilir.

4- Üçüncü taraf risk değerlendirmeleri ve izleme: Programlar, üçüncü taraf satıcıların risklerini ve verilen hizmetlere dayanarak kuruma verilen güvenlik risk düzeyini değerlendirmede yardımcı olabilir.

5- Olay izleme ve müdahale: Bu süreçlerin birleşimi bir kuruluşun ihlal durumunda tespit etmesine, yanıt vermesine, düzeltmesine, kurtarmasına ve yönetime rapor vermesine olanak tanır. Bu kontrollerin karşılanma hedeflerinde başarılı olmasını sağlamak için kayıt ve izleme teknolojilerinin yanı sıra yüksek eğitimli bir yanıt ekibi de gereklidir.

4.2. Siber Güvenlik Denetimi

Kurumlar birçok nedenden dolayı denetimler yaparlar. Denetim kurumun etkin operasyonlar gerçekleştirmesine, idari ve yasal düzenlemelere uygunluğunun kanıtlanmasına yardımcı olabilir. Yönetim için kurumun iyi çalıştığını ve olası zorlukları karşılamak için hazır olduğunu doğrulayabilir. Belki de en önemlisi, kuruluşun mali, operasyonel ve etik refahını paydaşlarına garanti edebilir. Siber güvenlik denetimleri, tüm kurumların ve kamu kurumlarının rekabet avantajı için dayandığı bilgi ve ilgili sistemlere özel olarak odaklanarak, tüm bu sonuçları desteklemektedir. Etkili bir denetim ile birçok faydanın başarılması, denetim faaliyetinin doğru ve tam olarak planlanmasına bağlıdır. Denetimin kapsamı ve amacı hem denetçi hem de denetlenen alan tarafından anlaşılmalı ve kabul edilmelidir. Denetimin amacı açıkça tanımlandıktan sonra, denetim sonuçlarını almak ve desteklemek için ilgili prosedürleri kapsayacak olan denetim planı oluşturulmalıdır. Denetim planının önemli bir bileşeni, çalışma programı olarak da bilinen denetim programıdır. Denetim programı, kontrol etkinliğini test etmek ve doğrulamak için kullanılacak özel prosedürleri ve adımları belgelemek için yaygın olarak kullanılır. Denetim programının kalitesi, denetim sonuçlarının tutarlılığı ve kalitesi üzerinde önemli bir etkiye sahiptir. Bu nedenle iç denetçilerin kapsamlı denetim programlarının nasıl geliştirileceğini anlamaları zorunludur (ISACA, 2016: 3). Plan ve program temelinde bir siber güvenlik denetimi için iç denetçinin / iç denetimin yapabilecekleri şu şekilde sıralanabilir (Frazıer & Deeter, 2015: 17-18; ISPG-SM01, 2017: 34):

1- Mevcut güvenlik politikasına, standartlarına, yönergelerine ve prosedürlerine uyumu kontrol edin.

2- Yetersizlikleri belirleyin ve mevcut politika, standartlar, kılavuzlar ve prosedürlerin etkinliğini inceleyin.

3- İlgili yasal, düzenleyici ve sözleşmeye bağlı gerekliliklerı belirleyin ve gözden geçirin.

4- Mevcut güvenlik açıklarını tanımlayın ve anlayın.

5- Risk ve azaltma stratejisi konusunda tartışmayı yönlendirin

6- Siber riskleri diğer kritik kurumsal risklere karşı bağımsız olarak değerlendirin ve önceliklendirin

7- Siber sorunları önlemek veya tespit etmek için kontrollerin optimize edilmesine yardımcı olun

8- Değişen siber riskin devamlı izlenmesini sağlayın

9- Operasyonel, idari ve yönetsel konulardaki mevcut güvenlik kontrollerini gözden geçirin, güvenlik önlemlerinin etkin bir şekilde uygulanmasını ve asgari güvenlik standartlarına uygunluğunu sağlayın.

10- İyileştirmeler için öneriler ve düzeltici eylemler sağlayın.

Dijital dönüşüm, iç denetim faaliyetine hem zorluklar hem de fırsatlar sunmaktadır. Verilerin hacmi, çeşitliliği ve kırılganlığı arttıkça, iç denetimin izlemesi gereken risklerin kapsamı da artmaktadır. Aynı zamanda, iç denetim birimlerinin performans ve farkındalığını arttırması için "son sınır"ın ne olabileceği konusunda çeşitli fırsatlar vardır. Teknoloji etkin denetim araçları, süreçleri ve uygulamaları, iç denetçilerin örnekleme ve varsayımlar yapmak yerine tüm verileri ve süreçleri sürekli olarak izlemelerini ve anormallikleri tespit edebilmelerini mümkün kılmıştır. Veri analizi ve bilgisayar destekli denetim araçları, iç denetçiler için yeni ufuklar açmaktadır (Ahıa ve Protıvıtı, 2016: 11).

Birçok iç denetim faaliyeti, kurumun siber güvenlik hazırlığına ilişkin bileşenleri değerlendirerek ilgili prosedürleri gerçekleştirmiştir. Saldırı ve sızma pro-

sedürleri gibi hedefli denetimler değerlidir, ancak siber güvenlik riskleri yelpazesinde yeterli güvenceyi sağlamazlar. İç denetimin siber güvenliğin kapsamlı bir görünümünü sağlaması ve yalnızca hedeflenen denetimleri yaparak yanlış bir güvenlik duygusu sağlamasından kaçınmak için geniş bir yaklaşım kullanılmalıdır (Deloitte, 2017: 2). Siber güvenlik amaçları ve denetim hedefleri kurumun siber güvenlik ihtiyacını göz önünde bulundurmalıdır. Siber güvenlik amaçları ve ilgili denetim hedefleri için Tablo 2'de gerekli açıklamalar yapılmıştır.

Tablo 2. Siber Güvenlik Amaçları ve İlgili Denetim Hedefleri

Siber Güvenlik Amacı	Denetim Hedefleri
Siber güvenlik politikaları, standartları ve prosedürleri yeterli ve etkilidir.	❏ Belgelerin eksiksiz ve güncel olduğunu doğrulayın. ❏ Resmi onay, onay ve uygulamanın yerinde olduğunu onaylayın. ❏ Belgelerin tüm siber güvenlik gereksinimlerini karşıladığını doğrulayın. ❏ Yan denetimlerin politikalarda, standartlarda ve prosedürlerde yapılan tüm hükümleri kapsadığını doğrulayın.
Ortaya çıkan risk güvenilir bir şekilde tanımlanır, uygun bir şekilde değerlendirilir ve uygun şekilde iyileştirilir.	❏ Risk tanımlama işleminin güvenilirliğini onaylayın. ❏ Kullanılan araçları, yöntemleri ve teknikleri içeren risk değerlendirme sürecini değerlendirin. ❏ Tüm risklerin sonuçların değerlendirilmesine göre ele alındığını onaylayın. ❏ İyileştirmenin yeterli olduğunu veya iyileştirilmemiş riske karşı resmi risk kabullerinin bulunduğunu doğrulayın.
Siber güvenlik dönüşüm işlemleri tanımlandı, konumlandırıldı ve ölçüldü.	❏ Dönüşüm sürecinin ve ilgili rehberliğin varlığını ve eksiksizliğini doğrulayın. ❏ Dönüşüm sürecinin, işletmenin tüm bölümleri tarafından uygulandığını ve takip edildiğini doğrulayın. ❏ Dönüşüm hedefleri, risk ve performans ile ilgili kontrolleri, metrikleri ve ölçümleri onaylayın.
Ataklar ve ihlaller zamanında ve uygun bir şekilde tespit edilir ve iyileştirilir.	❏ İzlemeyi ve belirli teknik saldırı tanıma çözümlerini onaylayın. ❏ Güvenlik olayı yönetimi ve kriz yönetimi süreçleri ve planları ile ilgili ara yüzleri değerlendirin. ❏ (Geçmiş saldırılara dayanarak) saldırı müdahalesinin zamanlamasını ve yeterliliğini değerlendirin.

(ISACA, 2017: 11)

Güvenlik yeteneklerini korumak ve geliştirmek, siber tehditleri azaltmaya yardımcı olabilir ve kurumu istenen siber güvenlik olgunluk seviyesine taşıyabilir. İç denetim kapsamlı bir siber risk değerlendirmesi yaparak, denetim komitesi ve yönetime objektif bakış açıları ve bulgular sunabilir. Bu bulgular, Kurumun siber risk alanlarını göz önüne alan geniş bir iç denetim planı geliştirmek için kullanabilir (Deloitte, 2017: 4). Bunun dışında siber güvenliğin iç denetim değerlendirmesi Tablo 3'de gösterildiği gibi tüm alanları, ilgili yetenekleri kapsamalı ve uygun olduğunda konu uzmanlarını içermelidir (Deloitte, 2015: 8).

Tablo 3. Siber Güvenliğin İç Denetim Değerlendirmesi

Aşama	I. Aşama: Planlama ve Kapsam Belirleme	II. Aşama: Mevcut Durumu Anlama	III. Aşama: Risk Değerlendirmesi	IV. Aşama: Boşluk Değerlendirmesi ve Öneriler
Anahtar Faaliyetler	**Faaliyetler:** • Özel iç ve dış paydaşları tanımlayın: BT, UYgunluk, Yasal Risk vb. • Örgütün görev ve hedeflerini anlayın • Endüstri gereksinimlerini ve yasal düzenlemeleri belirleyin • Endürstri ve sektör riski profili oluşturma (endüstri raporlarını haberlerini, trendlerini, risk vektörlerini gözden geçirme) • Kapsam içi sistemleri ve varlıkları tanımlayın • Satıcıları ve üçüncü tarafların katılımını tanımlayın	**Faaliyetler:** • Mevcut profili anlamak için görüşmeler ve atölye çalışmaları yapın • Mevcut kontrolleri anlamak için kapsam içi sistem ve süreçlerin adım adım gerçekleştirilmesi • Uygulanabilir raporların incelemeleri de dahil olmak üzere üçüncü tarafların kullanımını anlayın • Hem iç hem dış paydaşlar için güvenlik ortamı, stratejik planlar ve yönetişim dahil olmak üzere ilgili politika ve prosedürleri gözden geçirin • Öz değerlendirmeleri inceleyin • ÖNceki denetimleri inceleyin	**Faaliyetler:** • Kapsam dahilindeki tüm yetenekler arasındaki potansiyel risk listesini belgeleyin • Ortaya çıkan riskleri katmanlaştırmak ve potansiyel etkiyi belgelemek için konunun uzmanları ve yönetim ile işbirliği yapın • Risklerin olasılığını ve etkisini değerlendirin • Örgütün hedeflerine, yeteneklerine ve risk iştahına göre riskleri önceliklerindirin • Risk değerlendirme sonuçlarını yönetimle gözden geçirin ve doğrulayın, ayrıca kritikliği belirleyin	**Faaliyetler:** • Yetenek değerlendirme sonuçlarını belgeleyin ve değerlendirme puan kartı geliştirin • Belirli paydaşlarla değerlendirme sonuçlarını inceleyin • Boşlukları tanımlayın ve potansiyel şiddeti değerlendirin • Olgunluk analizine haritalama yapın • Önerileri belgelendirin • Çok yıllı siber güvenlik / BT denetim planı geliştirin
Dağıtımlar	**Dağıtım:** • Değerlendirme hedefleri ve kapsamı • Yetenek değerlendirme puan kartı çerçevesi	**Dağıtım:** • Çevre ve mevcut durumun anlaşılması	**Dağıtım:** • Öncelikli risk sıralaması • Yetenek değerlendirme bulguları	**Dağıtım:** • Olgunluk analizi • Değerlendirme puan kartı • İyileştirme önerileri • Siber güvenlik denetim planı

(Deloitte, 2015: 8)

4.3. Üçüncü Savunma Hattı Olarak İç Denetim Faaliyetinin Siber Hijyen Rolü

Üçüncü savunma hattı olarak iç denetim, siber güvenlik çabalarının, riskleri doğru bir şekilde tanımlayan ve önceleyen, doğru bilgileri toplayan ve uygun yanıtlar veren bir risk temelli yaklaşım olduğunu doğrulamaktan sorumludur. Gerçekte, iç denetim mevcut programın değerlendirilmesinde kaynak ve altyapıdan yoksundur. Bunun yerine birçok iç denetim birimi, siber güvenlik programlarını değerlendirmek için siber güvenlik uzmanlarına ve dış paydaşlara yönelir (Jamison, Morris ve Wilkinson, 2018: 11). İç denetim BT risk evreninin en kritik bileşenlerine odaklanarak kurumun siber hassasiyetini değerlendirmelidir. BT risk evreninin BT ile ilgili en kritik kavramları; (1) güvenlik ve mahremiyet, (2) altyapı ve (3) veri kategorisinde olduğunu görünmektedir (EY, 2011: 10). Aşağıdaki şekil risk evrenini değerlendirmede; iç denetime risk odaklı bir ileri görüş sağlamada yardımcı olacaktır (Sadek ve Close, 2015: 6).

Siber risklerin sıklığı ve çeşitliliği artarken, kurumlara verebilecekleri potansiyel zararları da devamlı artmaktadır. Çoğu kurum bu riskleri ciddiye almaktadır, ancak hem tehlikelerle mücadele etmek hem de kurum yöneticilerinin siber güvenlik hazırlıklarından haberdar olmasını sağlamak için daha fazlası yapılabilir. İç denetimin mevcut ve ihtiyaç duyulan kontrollere bağımsız bir değerlendirme sağlayarak; siber tehditleri yönetme mücadelesinde kurumlara yardım etmesinde, yönetimin birbirinden farklı siber riskleri anlamalarına ve ele almalarına yardımcı olma konusundaki kritik rolleri Tablo 4'te listelenmiştir (Deloitte, 2017: 6). Teknoloji geliştikçe, iç denetçilerin de görevleri gelişmektedir. İç denetçiler mesleğin, mevcut bölgesinden çıkmalı ve uzmanlığını siber riskleri ele almak için kullanması gerekmektedir (Fountain, 2019: 21). İç denetçilerin ve iç denetim yöneticilerinin öncelikleri ve sahip olması gereken siber dünyaya özgü iç denetim yetenekleri ve bilgisi Tablo 5'te görülmektedir.

Bu yeteneklerin haricinde, iç denetim ve iç denetçiler için göz önünde bulundurulması gereken siber hijyen (güvenlik) eylemleri (Ahıa ve Protıvıtı, 2016: 6; Protıvıtı, 2016: 6) şunlardır:

Şekil 8. BT İç Denetim Evreninin Gelişimi

(Sadek ve Close, 2015: 6)

1- Bir siber güvenlik stratejisi ve politikası geliştirmek için yönetim ile birlikte çalışın.
2- Kurumun siber güvenlik riskini kabul edilebilir bir düzeyde tutması için risk belirleme, değerlendirme ve azaltma yeteneğini geliştirme fırsatlarını belirleyin ve harekete geçirin.
3- Siber güvenlik riskinin yalnızca dış nedenlere bağlı olmadığını bilin (bir çalışanın, satıcının veya iş ortağının davranışlarından kaynaklanabilecek potansiyel tehditleri değerlendirin ve azaltın).
4- Denetim komitesi ve yönetimle olan iç ilişkileri (a) siber tehditlere ilişkin farkındalık ve bilgiyi arttırın ve (b) yönetimin siber güvenlik meseleleriyle yüksek derecede bağlı kalmasını ve siber güvenlik riskinin değişen doğası hakkında güncel kalmasını sağlayın.
5- Siber güvenlik riskinin resmi olarak denetim planına entegre edilmesini sağlayın.
6- Gelişen teknolojilerin ve trendlerin kurumu ve siber güvenlik risk profilini nasıl etkilediğine dair bir anlayış geliştirin ve güncel tutun.
7- Kurumun siber güvenlik programını, NIST Siber Güvenlik Çerçevesi, ISO 27001/27002 veya HITRUST CSF gibi uygun bir çerçeveye göre değerlendirin.
8- Siber güvenlik konusunda en güçlü önleme yeteneğinin insan ve teknoloji güvenliğinin eğitim, farkındalık, dikkat ve teknoloji araçlarının tamamlayıcı bir birleşimini gerektirdiğini yönetime iletme fırsatlarını araştırın.
9- Siber güvenlik izlemenin ve siber olay tepkisinin üst yönetim önceliği olması gerektiğini vurgulayın (net bir yükseltme protokolü, bu önceliğin ortaya çıkmasına (ve sürdürülmesine) yardımcı olabilir).
10- Her ikisi de siber güvenlik riskini etkin bir şekilde yönetme çabalarını engelleyebilecek her türlü IT / denetim personeli ve kaynak sıkıntısı ile destekleyici teknoloji araçlarının bulunmamasına yöneliktir. Bu farkındalığa sahip olun.

İç denetim faaliyetinin kurum süreçlerine olan hakimiyeti nedeniyle siber güvenlik uygulamalarına ve politikalarına artı değer katması beklenmektedir. İç denetim Siber hijyenin olgunluk seviyelerinin yükseltilmesinde danışmanlık ve güvence sağlama; kurumsal yönetim içerisinde siber güvenliğin farkındalığının arttırılması ve buna bağlı olarak kuramsal risk yönetiminde siber risklerin daha görünür şekilde değerlendirerek, etkin kontrolleri sağlamada üçüncü savunma hattının kritik bir öğesi olarak proaktif bir rolü ve potansiyeli vardır. İç denetimin siber güvenliğe bakışı ve alacağı rol ile kurumun siber bağışıklığı sağlamasında önleyici ve özellikle de yönlendirici bir tarafı olacaktır. Bu roller aşağıdaki tabloda gösterilmektedir.

Tablo 4. Öncelikler - İç Denetim Yetenekleri ve Bilgisi

Tüm İç Denetçiler	İç Denetim Yöneticileri (Birim Başkanları)
Veri analizi araçları - istatistiksel analiz	Veri analizi araçları - istatistiksel analiz
Çevik risk ve uyum	Veri analizi araçları - veri manipülasyonu
Sürekli denetim	Çevik risk ve uyum
Büyük veri / iş zekası	Sürekli denetim
Sürekli izleme	Sürekli izleme

(Ahıa ve Protıvıtı, 2017: 7)

Tablo 5. İç Denetim Faaliyeti İçin Siber Hijyen Rol

	İÇ DENETİMİN SORUMLULUK ALANI	İÇ DENETİMİN HESAPVEREBİLİRLİK ALANI	İÇ DENETİMİN DESTEK KAYNAKLARI	İÇ DENETİMDEN DANIŞMANLIK ALANLAR	İÇ DENETİME BİLGİ SAĞLAYAN KAYNAKLAR
Siber krizden önce	• Siber risk yönetim sisteminin etkinliği konusunda yönetim kurulu ve yönetime bağımsız güvence verme • Önemli riskler için siber kontrolleri ve iyileştirme planlarını değerlendirme • Yönetim kurulu düzeyindeki danışman siber komitenin denetimleri ve/veya incelemeleri	• Tavsiyeler yoluyla yüksek düzeyde bağımsız ve objektif güvence	• Yönetim Kurulu ve Denetim komitesi yönetişimi, gözetimi, görevi, tonu • Üst yönetici (CEO) ve yöneticiler • Siber risk yönetim sisteminin arkasındaki ilkeler	• Yönetim kurulu ve üst düzey finansal yönetici (CFO-chief financial officer) • Siber risk yönetimi sisteminin olgunluğunun etkinliği	• Diğer birimlerden birleşik güvence • Tüm üst düzey yöneticilerin ve toplantıların planlama, tartışma ve eylemlerinin kayıtları • Düzenli incelemelerin yönetim kurulu düzeyinde denetim süreci • Siber risk yönetimi iyileştirme planları ve faaliyetleri • Siber güvenlik politikaları ve prosedürleri • Siber strateji ve stratejik performans yönetimi • Siber standartlar ve çerçeveler • Siber güvenlik olay ve kriz yönetimi • İş sürekliliği yönetimi
Siber kriz sırasında / sonrasında	• Siber risk yönetim sistemi ve yönetim kurulu düzeyindeki danışman siber komite sürecindeki değişiklikler konusunda kriz sonrası yeni güvence verme	• Gözden geçirilmiş güvence	• Yönetim Kurulu ve Denetim komitesi • Üst yönetici (CEO) ve yöneticiler	• Yönetim Kurulu ve üst yönetici (CEO)	

(Antonucci, 2017: 222)

5. SONUÇ

İster kişisel olsun isterse bir kurum içeresinde olsun eğer teknolojik bir araç kullanacaksak bunun kolaylıklarının yanında zorluklarını da göz önünde bulundurmalıyız. 21. yüzyılın baş döndürücü değişim hızı siber dünyada çok daha net görülmektedir. Bu hız beraberinde kırılganlıkları, belirsizlikleri, tehditleri ve riskleri de getirmektedir. Özellikle siber riskler yaygın olarak kurumlar için en büyük risk kaynağı olarak kabul edilmektedir. Tüm sektörlerde kurumların güvenlik açığı artmaktadır. Sürekli bir av peşindeki bilgisayar korsanları ve siber saldırganlar için bu av herhangi bir ülkenin elektrik şebekesi, herhangi bir şirketin web sitesi veya sıradan bir kişinin banka hesabı olabilmektedir. Endişe verici bir şekilde siber saldırılar potansiyel zararlarıyla karşılaştırıldığında, orantısız bir şekilde çok ucuzdurlar. Siber saldırıların zaman aralığı 7 gün / 24 saattir. Bir siber saldırının başarılı olması siber saldırganlarının motivasyonuna bağlı olarak sadece bir zaman meselesidir. Bu nedenle sürdürülebilir bir siber hijyen ve siber güvenlik yönetimi anlayışı kurumların kaçınılmaz bir gerçekliğidir. Hiçbir kişi, hiçbir kurum, hiçbir ülke siber uzayda bir ada değildir ve siber saldırı için bir alarm verildiğinde, herkes için bir mücadele alanı vardır, ister siperde olsunlar isterse olmasınlar. 2. Dünya Savaşında öncü bir rol oynayan Winston Churchill'ün bir sözünü ödünç alıp bunu siber mücadeleye aktarırsak *"herhangi bir kurumun siber savunmasında yer alacak olan; en cesur yöneticilerini, en gözü pek bilgi güvenliği uzmanlarını, en donanımlı BT'cilerini, en cüretkar beyaz şapkalı hackerlarını bir masada toplarsanız, ne elde edersiniz? Bütün korkularının toplamını…"* şeklinde durumu özetleyebiliriz.

Küresel ekonominin artan bağlantı ve otomatik sistemlere bağımlılığı göz önüne alındığında, siber güvenlik, herhangi bir kurum veya devlet operasyonunun kritik bir bileşeni haline gelmiştir. Siber güvenliğin ön aşaması olarak siber hijyen, siber bilgi güvenliği ile ilgili temel bir ilkedir. Siber hijyen kişisel hijyenle benzerlik göstermekte ve siber tehditlerden kaynaklanan riskleri en aza indirgemek için basit ve rutin önlemler almayı ifade etmektedir. Ne yazık ki bir siber saldırı, güvenlik hijyeninin sağlanmasından daha kolaydır. Kurumların bir siber saldırının kurbanı olmalarını önleyebilmeleri veya bir siber saldırının risklerini en aza indirebilmeleri için en güçlü silahları, bir siber hijyen stratejisi uygulamalarıdır. Bu bağlamda, bir olgunluk modeli olarak siber hijyen kişisel hijyen ile aynı işlevde görülmeli ve bir kuruma düzgün şekilde entegre edildiğinde, kurumsal siber bağışıklık sisteminin güçlenerek kurumsal sağlığın korunabileceği dikkate alınmalıdır.

İç denetim faaliyeti tüm siber korkularının ötesine geçme potansiyeline sahiptir ve bu potansiyel kullanılmalıdır. İç denetçiler ve iç denetim faaliyeti için bu siber dünyadaki siber savaşın siber cephesinin siperlerinde yadsınamaz bir rol görünmektedir. Risk yönetimi, siber hijyen ve siber güvenlik için bağımsız güvence rolü, kendini buna göre yapılandıran iç denetim fonksiyonu tarafından benzersiz bir şekilde oynanabilir. İç denetçiler bu süreçte önemli danışmanlar olabilir. Siber hijyenin kurumların mevcut savunma hatlarında konumlanmasında kritik görevler üstlenebilirler. Bu yönüyle değerlendirildiğinde, üçlü savunma hattının üçüncü sırasındaki **iç denetim faaliyetinin siber rolünün (ve sorumluluğunun) her geçen gün arttığı sonucuna varılabilir.** Günümüzde -tüm meslekler gibi- iç denetimin de zorluğu, kritik iş bilgilerinin güvenliğini ve kullanılabilirliğini sağlamadaki (güvence sağlama) rolünü eşzamanlı olarak genişletirken, kendi risklerini kontrol ederek siber olaylar karşısında güncel kalabilmekle ilgilidir.

Kaynakça

Ahıa ve Protıvıtı, (2016) *Cybersecurity, IT Transformation and Analytics - Addressing Priorities for Internal Auditors in U.S. Healthcare Provider Organizations*, Ahia and Protiviti.

Ahıa ve Protıvıtı, (2017) *Cybersecurity, Data Analytics and Other Priorities for Internal Auditors in U.S. Healthcare Providers*, Ahia and Protiviti.

AICPA, (2017) *Reporting on an Entity's Cybersecurity Risk Management Program and Controls*, American Institute of Certified Public Accountants Inc.

Antonuccı D,, (2017) "Internal Organization Context", *The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities*, Ed.: Domenic Antonucci, John Wiley & Sons, Inc.: Hoboken, New Jersey.

Antonuccı D. ve Verstıchel D., (2017) "Epilogue", *The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities*, Ed.: Domenic Antonucci, John Wiley & Sons, Inc.: Hoboken, New Jersey.

Bayuk J. L., Healey J., Rohmeyer P., Sachs M. H., Schmıdt J. ve Weıss J., (2012) *Cyber Security Policy Guidebook*, John Wiley & Sons, Inc.: Hoboken, New Jersey.

BSI, (2008) *Information Security Audit (IS audit): - A Guideline for IS Audits Based on IT-Grundschutz*, German Federal Office for Information Security.

Caravellı J. ve JONES N., (2019) *Cyber Security: Threats and Responses for Government and Business*, Praeger Security International.

CBN, (2018) *Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Service Providers*, Central Bank of Nigeria.

CMM, (2016) *Cybersecurity Capacity Maturity Model for Nations (CMM) Revised Edition*, Global Cyber Security Capacity Centre University of Oxford.

DELOITTE, (2015) *Cybersecurity: The Role of Internal Audit*, Deloitte.

DELOITTE, (2017) *Cybersecurity and the Role of Internal Audit: An Urgent Call to Action*, Deloitte.

ENISA, (2016) *Review of Cyber Hygiene practices*, European Union Agency For Network and Information Security.

EY, (2011) *The Evolving IT Risk Landscape: The Why and How of IT Risk Management Today*, Ernst & Young.

FFIEC, (2015) *FFIEC Cybersecurity Assessment Tool*, Federal Financial Institutions Examination Council.

FINRA, (2018) Report on Selected Cybersecurity Practices - 2018, Financial Industry Regulatory Authority https://www.finra.org/sites/default/files/Cybersecurity_Report_2018.pdf Erişim Tarihi: 12.02.2019.

Fountaın L., (2019, February) "Internal Audit's Evolving Cybersecurity Role", *Internal Auditor*, 19-21.

Frazıer & Deeter, (2015) *Cybersecurity: Considerations for Internal Audit*, IIA Atlanta Chapter Meeting, Frazier & Deeter.

GAC 16, (2016) *Global Agenda Council on Cybersecurity*, White Paper, World Economic Forum: Geneva.

GTAG, (2016) *Assessing Cybersecurity Risk: Roles of the Three Lines of Defense,* The Institute of Internal Auditors.

Hale r., (2017) "Foreword The State of Cybersecurity", *The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities*, Ed.: Domenic Antonucci, John Wiley & Sons, Inc.: Hoboken, New Jersey.

Hermans J. ve Dıemont T., (2017) "Treating Cyber Risks", *The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities*, Ed.: Domenic Antonucci, John Wiley & Sons, Inc.: Hoboken, New Jersey.

Holmes C. ve Phıllıppe J., (2017) "Cybersecurity for Operations and Communications", *The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities*, Ed.: Domenic Antonucci, John Wiley & Sons, Inc.: Hoboken, New Jersey.

IIAC, (2015) *IIAC Cybersecurity Guidebook*, Investment Industry Association of Canada.

ISACA, (2016) *Information Systems Auditing: Tools and Techniques- Creating Audit Programs*, ISACA.

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

ISPG-SM01, (2017) *Information Security: Practice Guide for Security Risk Assessment & Audit*, Office of the Government Chief Information Officer-The Government of the Hong Kong Special Administrative Region.

ITGI, (2003) Board Briefing on IT Governance, 2nd ed., IT Governance Institute.

ITGI, (2006) Information Security Govenance for Board of Directors and Executive Management, 2nd ed., IT Governance Institute.

ITRC, (2017) *Data Breach Reports: 2016 End of Year Report*, Identity Theft Resource Center.

ITRC, (2019) *Data Breach Report: 2018 End of Year Report*, Identity Theft Resource Center.

ITU-T X.1208, (2014) *Series X: Data Networks, Open System Communıcations and Security: Cyberspace Security – Cybersecurity*, International Telecommunication Union.

Jamıson J., Morrıs L. ve Wılkınson C., (2018) *The Future of Cybersecurıty in Internal Audit*, The Internal Audit Foundation.

KPMG, (2018) *Siber Güvenlik Olgunluk Değerlendirmesi*, KPMG.

Lı K. C., Chen X. ve SusılO W., (2019a) "Foreword I-II", *Advances in Cyber Security: Principles, Techniques, and Applications*, Ed.: Kuan-Ching Li, Xiaofeng Chen, Willy Susilo, Springer Nature Singapore Pte Ltd.: Singapore.

Lıng C., (2017) "Information Asset Management for Cyber", *The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities*, Ed.: Domenic Antonucci, John Wiley & Sons, Inc.: Hoboken, New Jersey.

Lınkov I., Eısenberg D. A., Plourde K., Seager T. P, Allen, J. ve Kott A., (2013) "Resilience Metrics for Cyber Systems", *Environment Systems and Decisions*, 33(4), 471-476.

Keys B. ve Shapıro S., (2019) "Frameworks and Best Practices", *Cyber Resilience of Systems and Networks*, Ed.: Alexander Kott, Igor Linkov, Springer International Publishing AG, part of Springer Nature: Switzerland.

Mccarthy Tétrault, (2017) *Cybersecurity Risk Management: A Practical Guide for Businesses*, McCarthy Tétrault.

NACD, (2017) *Cyber-Risk Oversight*, Director's Handbook, National Association of Corporate Directors.

Nhede N., (2017) "Grid Automation Drives Increase in Utility Cybersecurity Investments: Report". Smart Energy International. 10 August 2017, https://www.smart-energy.com/industry-sectors/smart-grid/cybersecurity-technologies-navigant-research/, Erişim Tarihi: 19.02.2019.

ONG-C2M2, (2014) *Oil and Natural Gas Subsector Cybersecurity Capabılity Maturity Model*, U.S.Department of Homeland Security-Department of Energy.

Protıvıtı, (2016) *Cybersecurity, IT Transformation and Analytics – Addressing Priorities for Internal Auditors in U.S. Healthcare Provider Organizations*, Assoc. of Internal Auditors.

Rodrıguez A,, (2017) "Monitoring and Review Using Key Risk Indicators (KRIs)", *The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities*, Ed.: Domenic Antonucci, John Wiley & Sons, Inc.: Hoboken, New Jersey.

Sadek K. ve CLOSE C., (2015) *The Changing IT Risk Landscape: Understanding and Managing Existing and Emerging Risks*, Deloitte.

SAMA, (2017) *Cyber Security Framework*, Saudi Arabian Monetary Authority.

Souppaya M., Stıne K., Sımos M., Sweeney S. ve Scarfone K., (2018) *Critical Cybersecurity Hygiene: Patching The Enterprise*, National Institute of Standards and Technology.

Sunde S. J., (2017) "Assurance and Cyber Risk Management", *The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities*, Ed.: Domenic Antonucci, John Wiley & Sons, Inc.: Hoboken, New Jersey.

Totade A. ve Godbole S., (2017) "Culture and Human Factors", *The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities*, Ed.: Domenic Antonucci, John Wiley & Sons, Inc.: Hoboken, New Jersey.

VAndıjck I. ve Lerberghe P. V., (2017) "Physical Security", *The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities*, Ed.: Domenic Antonucci, John Wiley & Sons, Inc.: Hoboken, New Jersey.

Vıllıers S., (2017) "Access Control", *The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities*, Ed.: Domenic Antonucci, John Wiley & Sons, Inc.: Hoboken, New Jersey.

WEF, (2018) *Cyber Resilience Playbook for Public-Private Collaboration*, World Economic Forum: Geneva.

Whıt G. B., (2011) "The community cyber security maturity model", *2011 IEEE International Conference on Technologies for Homeland Security (HST)*, 173-178.

Wyatt M., (2017) "Cybersecurity Systems: Acquisition, Development, and Maintenance", *The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities*, Ed.: Domenic Antonucci, John Wiley & Sons, Inc.: Hoboken, New Jersey.