Mehmet Akif Ersoy Üniversitesi Uygulamalı Bilimler Dergisi
Journal of Applied Sciences of Mehmet Akif Ersoy University

İşletmelerde Siber Güvenlik Riskleri ve Bilgi Teknolojileri Denetimi: Bankaların Siber Güvenlik Uygulamalarının İncelenmesi

Özen AKÇAKANAT[1*], Ozan ÖZDEMİR[2], Mehmet MAZAK[3]

[1] Asst. Prof. Dr., Süleyman Demirel University, Faculty of Economics and Administrative Sciences, Department of Finance and Banking, Isparta, Turkey

[2] Asst. Prof. Dr., Süleyman Demirel University, Faculty of Economics and Administrative Sciences, Department of Finance and Banking, Isparta, Turkey

[3] Research Asst., Süleyman Demirel University, Faculty of Economics and Administrative Sciences, Department of Finance and Banking, Isparta, Turkey

Geliş Tarihi/Received: 03.08.2021
Kabul Tarihi/Accepted: 31.08.2021
Doi: 10.31200/makuubd.978263
Araştırma Makalesi/ Research Article

ÖZET

Günümüzde dijital veriler ve operasyonlar, pek çok işletmenin merkezinde yer almaktadır. Ancak bilgisayarlı sistemlere olan bu bağımlılık, çeşitli siber tehditleri de beraberinde getirmektedir. Bu riskler, çalışanlar ve yüklenicilerden kaynaklanan içsel riskler olabileceği gibi, siber suçluların ve hatta işletmenin müşterilerinin faaliyetleri sonucu da olabilir. Giderek artan bir şekilde ortaya çıkan, siber güvenlik riskleri yalnızca bir ağ veri ihlali riskini içermez aynı zamanda, açık dijital bağlantı ve erişilebilirliğe dayanan faaliyetler yoluyla tüm işletmenin zarar görmesi riskini de ortaya çıkarmaktadır. Bunun sonucu olarak siber güvenlik riskiyle nasıl başa çıkılacağını öğrenmek bir kuruluş için kritik öneme sahiptir. Bu kapsamda çalışmada öncelikle işletmeler için siber güvenlik riskleri ortaya koyularak, bu riskleri yönetmeye ilişkin bilgiler verilmiştir. Bu çalışmada aktif büyüklüğüne göre ilk on bankanın siber güvenlik ve bilgi teknolojileri faaliyetlerine ilişkin faaliyet ve entegre raporlarından elde edilen veriler incelenerek siber güvenlik uygulamalarının içeriğinin tespit edilmesi amaçlanmaktadır. Çalışmada kullanılan veriler bankaların 2019 ve 2020 faaliyet ve entegre raporlarından elde edilmiştir. Raporlardan elde edilen sonuçlara göre bankaların güncel mevzuat düzenlemelerine ve uluslararası standartlara uygun bir organizasyon yapılanmasına sahip oldukları, iç denetim çerçevesinde gerekli denetim faaliyetlerini gerçekleştirdikleri, bu çerçevede kapsamlı eğitim programları uyguladıkları, veri güvenliğini sağlamaya yönelik altyapı yatırımlarını yaptıkları ve teknolojiyi takip ettikleri tespit edilmiştir.

* Sorumlu yazar/Corresponding author
E-mail/e-ileti: ozenakcakanat@sdu.edu.tr

Anahtar kelimeler: Siber Güvenlik, Siber Güvenlik Riskleri, Bilgi Teknolojileri Denetimi, Bankalar.

Cyber Security Risks and Information Technology Audit in Businesses: Examination of Banks' Cyber Security Applications

ABSTRACT

Digital data and operations are at the center of many businesses today. However, this dependence on computerized systems causes various cyber threats and risks. These risks can be internal risks caused by employees and contractors, or they can be the result of the activities of cybercriminals and even customers of the business. Increasing cybersecurity risks include not only the risk of a network data breach but also carries the risk of harming the entire business through activities based on open digital connectivity and accessibility. Therefore, learning how to deal with cybersecurity risks is critical for an organization. In the study, first of all, cybersecurity risks for businesses have been revealed. Then, information on managing these risks is given. In the study, data has been obtained from 2019 and 2020 annual and integrated annual reports of Turkey's top 10 banks by asset size. It is aimed to determine the content of banks' cybersecurity applications. According to the results, it has been observed that the banks have an organizational structure in accordance with the current local regulations and international standards. It has been also observed that banks carry audit activities within the framework of internal audit. In this scope of internal auditing activities, banks arrange comprehensive education programs for their employees and invest in infrastructure and cutting-edge technology to ensure data security.

Keywords: Cybersecurity, Cybersecurity Risks, Information Technology Audit, Banks.

1. GİRİŞ

Bilgi sistemleri teknolojilerindeki son gelişmeler, çeşitli iş alanlarında birçok uygulamanın bilgisayarlar üzerinden yapılmasına neden olmaktadır. Bu süreçte veri birçok kuruluşta kritik bir kaynak haline gelmiş ve bu nedenle verilere etkin erişim, veri paylaşımı, veriden bilgi çıkarma ve bilgiden yararlanma acil bir ihtiyaç haline gelmiştir. 1990'ların ortalarında World Wide Web'in (www) ortaya çıkışı, veri, bilgi ve bilginin etkin bir şekilde yönetilmesinin önemini artırmıştır. Günümüzde gerek webde gerekse de bilgi teknolojilerinin içerisinde pek çok veri bulunmaktadır. Bu verileri ve bilgileri geleneksel araçlarla yönetmek

neredeyse imkânsız hale gelmektedir. Veri ve bilgi yönetimine olan talep arttıkça, veritabanlarının, uygulamaların ve bilgi sistemlerinin güvenliğinin sağlanması için de kritik bir ihtiyaç vardır. Veriler ve bilgiler, yetkisiz erişime ve kötü niyetli yolsuzluklara karşı korunmalıdır. Web'in ortaya çıkmasıyla birlikte, çok sayıda kişinin bu verilere ve bilgilere erişimi olduğundan, verileri ve bilgileri korumak daha da önemlidir. Bu nedenle, siber güvenlik risklerini yönetmek ve raporlamak, hemen hemen her şirketin yönetimi ve yönetim kurulu için öncellikli konular haline gelmiştir.

Özellikle müşteriler ve tedarikçilerle ilgili bilgiler de dâhil olmak üzere finansal ve finansal olmayan bilgiler ağlarda ve bulutta giderek daha fazla depolanmaktadır. Veri ihlallerinin yaygınlaşması, şirketlerin siber güvenlik risk yönetimi ve raporlamasına büyük yatırımlar yapmasına ve tüm şirketlerin ticari işlemler için güvenli bir dijital altyapıya sahip olmaya zorlamaktadır. Siber güvenlikle ilgili son raporlara göre, güvenlik ihlali yaşayan firmaların %20'sinden fazlası önemli bir gelir kaybı, müşteri tabanında bir azalma ve iş fırsatların da kayıplar yaşamışlar ve toplam maliyetler kişi başına yaklaşık 17 milyon ABD dolarını bulmuştur (Rosati vd., 2020, s.2).

İşletmeler, siber güvenlik tehditlerini yönetmek, ihlalleri ve diğer güvenlik olaylarını tespit etmek, yanıt vermek, azaltmak ve bunlardan kurtulmak için etkin süreçlere ve kontrollere sahip olduklarını gösterme baskısı altındadır. Bu noktada bu risklere karşı önlem alınması ve bu risklerin yönetilmesinde Bilgi Teknolojileri (BT) denetimi önem arz etmektedir. BT denetimi, bilgi varlıklarına ilişkin risklerin belirlenmesine ve bu risklerin azaltılması veya yok edilmesi için kontroller oluşturulmasına (risk yönetimi) odaklanmaktadır. Bilgi varlıklarının korunmasında BT denetiminin amaçlarından biri de işletmenin bilgi sistemlerinin uygunluğu, gizliliği ve bütünlüğünün gözden geçirilip değerlendirilmesidir.

Siber güvenlik risklerini azaltmak ve işletmeleri bu risklerden korumak için çeşitli uluslararası kuruluşlar birtakım düzenlemeler getirmiştir. Amerika Birleşik Devletleri Kamu Gözetimi Kurulu (PCAOB), 2018-2022 stratejik planına siber güvenlik risklerinin değerlendirmesini açıkça dahil etmiştir. Ayrıca, Menkul Kıymetler ve Borsa Komisyonu (SEC) yakın zamanda siber güvenlik risk açıklamaları hakkında raporlama yönergeleri yayınlamıştır. AICPA denetçilerin bir kuruluşun siber güvenlik risk yönetimi politikalarını ve prosedürlerini değerlendirmek için kullanmaları için bir güvence çerçevesi önermiştir (Janvrin & Wang, 2019, s.1).

2. SİBER GÜVENLİK

2.1. Siber Güvenlik Kavramı

Siber güvenlik son yıllarda küresel dünyanın ilgi odağı ve önem arz eden bir konusu haline gelmiştir (Von Solms & Van Niekerk, 2013, s.97). Literatürde birçok farklı tanımlamaya yer verilmesine rağmen siber güvenlik; internette olduğu gibi bir bilgisayarı ya da bilgisayar sistemini erişim izni olmayan kişilerden veya saldırılardan korumak adına alınan önlemler olarak tanımlanabilmektedir (Merriam-Webster, 2021). Bilgisayarların, elektronik iletişim sistemlerinin ve hizmetlerinin, kablolu ve elektronik iletişim ile bunların içerdiği bilgilerin; kullanılabilirliği, bütünlüğünü, kimlik doğrulamasını, gizliliğini ve inkâr edilememesini sağlamak amacıyla tüm bu iletişim kanallarının zarar görmesini engelleme ve korunmasını sağlama tedbirlerine siber güvenlik adı verilmektedir (NIST, 2021).

Bilgisayar tabanlı bilgi çağı, kurumların çalışma şekillerinin ve bilgi güvenliğine olan yaklaşımlarının değişmesine yol açmıştır. Günümüzde bilgi güvenliği kurumlar için; en az maddi fiziki varlıkların korunması kadar önemli bir hale gelmiştir (Gordon & Loeb, 2002, s.452). Bilgi güvenliği; bilginin gizliliğinin, bütünlüğünün ve kullanılabilirliğinin korunması anlamına gelmektedir (ISO/IEC 27000, 2018). Siber güvenlikle ilgili birçok güncel araştırma, siber güvenlik terimini bilgi güvenliği terimiyle dönüşümlü olarak kullanmaktadır. Eş anlamlı olarak değerlendirilebilen bu terimler, önemli derecede birbirleriyle örtüşmesine rağmen birbirlerinden farklılaştığı durumlar da olabilmektedir. Bilgi güvenliğinde; insan faktörüne yapılan atıflar genellikle insanların güvenlik sürecindeki üstlendikleri roller ile ilgiliyken, siber güvenlikte ise insan faktörü saldırıların temel hedefi olarak tanımlanmıştır, hatta bilmeden bile insanların siber saldırının bir parçası haline gelebileceğinden söz edilebilmektedir (Von Solms & Van Niekerk, 2013, s.100). Bir başka tanıma göre siber güvenlik; bilginin gizliliğinin, bütünlüğünün ve kullanılabilirliğinin siber uzayda (herhangi bir fiziksel biçimde bulunmayan, teknolojik araçlar ve bunlara olan bağlantılar vasıtasıyla internet üzerindeki insanların, yazılımların ve hizmetlerin etkileşim içinde bulundukları platform) korunması anlamına gelmektedir (ISO/IEC 27032, 2012). Bu nedenle, siber güvenlik ile bilgi güvenliği arasındaki fark, bilginin korunması siber güvenlikte siber alandaki bilgilerle sınırlandırılmışken, bilgi güvenliğinde ise bilginin her yerde korunması esastır. Bu durum; siber güvenliğin bilgi güvenliğinin içinde yer aldığını da göstermektedir. Ayrıca siber saldırılar, siber zararlar ve siber suçlar gibi siber güvenlik eksikliğinden kaynaklanan ve bireyleri, kurumları veya ulusal çıkarları etkileyebilen; ekonomik, fiziksel, psikolojik ve sosyal sonuçlar doğuran bu zararların

(Eva Ignatuschtschenko'dan aktaran Von Solms & Von Solms, 2018, s.3) siber güvenlik alanının dışında konumlandığı da belirtilmiştir (Von Solms & Von Solms, 2018, s.3).

2.2. Siber Güvenliğin Önemi

21. yüzyılda toplumun bilgisayarları ve bilgi çağını büyük bir hızla içselleştirdiği görülmüştür. Toplumun kullanmış olduğu; arabalardan trafik ışıklarına, su ve güç kaynakları gibi altyapı hizmetlerine kadar bilgisayarlar aktif olarak kullanılmaktadır. Toplumun, bilgisayar sistemlerinin getirmiş olduğu verimlilik artışına karşı duyduğu memnuniyeti, sistemin güvenliği ve aksamadan çalışmasıyla büyük ölçüde ilişkilidir. Fakat bilgisayar sistemlerinin nasıl çalışması istenildiği ve gerçekte nasıl çalıştığı arasındaki farkın, bilgisayar korsanlarınca keşfedilmesi milyarlarca dolarlık hacme sahip siber suçların doğmasına sebebiyet vermiştir (Tarter, 2017, s.213). 2015 yılında 3 trilyon dolarlık büyüklüğe sahip olan bu endüstrinin 2021 yılı sonunda 6 trilyon dolar seviyesine çıkması öngörülmektedir (Herjavec, 2020).

Dijital teknolojilerin yaygın bir şekilde benimsenmesiyle birlikte, alışveriş ve sosyal etkileşimlerden iş dünyasına, farklı sektörlere ve ne yazık ki suçlara kadar toplumun birçok yönü çevrimiçi hale gelmiştir (Lallie vd., 2021, s.1). Siber tehditler yalnızca bilgisayar sistemlerine verdikleri zararla kalmamakta, bir ülkenin ulusal çıkarları için önemli kabul edilebilecek haberleşme ve bilgisayar sistemlerine, enerji ve ulaşım ağlarına ve askeri sistemlere zarar verebilecek asimetrik bir harp çeşidi olarak düşünülmektedir. Bu sebeple, tüm dünyada önemli bir tehdit unsuru olarak değerlendirilmeye başlanmıştır (Aytekin, 2015, s.19).

Finansal sistem açısından incelendiğinde; bankalar, kredi kartı şirketleri ve yatırım fonları gibi finansal hizmet sağlayıcıların müşterilerinin kişisel olarak tanımlanabilecek bilgilerini (ev adresleri, sosyal güvenlik numarası, banka bilgileri, telefon numarası, e-posta adresi ve gelir bilgileri vb.) bünyelerinde barındırdığı bilinmektedir. Bu verilerin karanlık web üzerindeki yüksek değeri finans endüstrisini siber suçlular tarafından çekici bir hedef haline getirmektedir (Bowcut, 2021). 2013 yılının sonuna doğru kriminal suçlular tüm dünyada 100'den fazla bankayı hedef alarak global bir saldırı gerçekleştirmiştir. Toplamda 1 milyar dolara yakın bir seviyede kayıp gerçekleşmiş ve bu saldırıya 'Carbanak' saldırısı adı verilmiştir. Carbanak saldırısıyla beraber finansal endüstrideki siber güvenlik metodolojisi de değişime uğrayarak önceleri, son kullanıcı güvenliğine yoğunlaşan siber güvenlik faaliyetleri yaşanan bu krizle beraber ATM ve para transfer sistemleri (depozito hesapları) gibi banka ağ güvenliğinin önemini ortaya koymuştur. Bu nedenle 2015 yılında Obama hükümeti siber güvenlik yasasını

imzalamış ve yasaya göre finansal kurumların yaşamış oldukları siber güvenlik şoklarını federal hükümetle paylaşmasının önü açılmıştır (Johnson, 2016, s.278).

İçinde bulunduğumuz Covid-19 salgını küresel olarak milyarlarca vatandaşın hayatını değiştiren, toplumsal normlar ve yaşama ile çalışma şeklimiz açısından yaygın olarak yeni-normal olarak anılan duruma neden olan, dikkate değer, eşi görülmemiş bir olaydır (Lallie vd., 2021, s.1). Bu krizden diğer işletmelere göre daha az etkilenen, dijitalleşme sürecine zaman, çaba ve bütçe ayıranlardır. Başka bir ifadeyle, günlük faaliyetlerine bilgi teknolojisini önemli ölçüde yerleştirmiş olanlar, faaliyetlerine kesintisiz devam etmelerine imkân sağlamıştır. Bu kuruluşlar, teknolojik olarak ilkel rakiplerine kıyasla daha iyi koşullarda olsalar da çok belirgin olmayan başka bir Covid-19 yan etkisiyle yani artan siber suç oranlarıyla karşılaşmışlardır (Georgiadaou vd., 2021, s.2). Yapılan son araştırmalarda siber suçların sıklık ve şiddetinin arttığı görülmüştür. Amerika Birleşik Devletleri, İngiltere, İspanya, Hollanda, Almanya, Fransa, Belçika ve İrlanda'da bulunan firmalara yapılan anket çalışmasında; firmaların siber saldırılar sonucu kaybettikleri tutar 2019 yılına kıyasla 600 milyon dolar artarak 1,8 milyar dolar seviyesine ulaşmıştır (Hiscox, 2020).

2.3. Siber Güvenlik Riskleri ve Siber Saldırı

Siber güvenlik riski, harici saldırılar nedeniyle bilgi teknolojisi sistemlerinde bir arızanın sonucu olarak bir işletmenin finansal kaybı, kesintisi veya itibarının zedelenmesi riskidir (Florakis vd., 2020, s.2). Siber güvenliği tehdit eden en önemli unsur siber saldırılardır. Veri veya bilginin bütünlüğünün ya da gerçekliğinin bozulması siber saldırı ya da bilgisayar ağı saldırısı olarak adlandırılmaktadır (Uma & Padmavathi, 2011, s.390). Ayrıca, bir bilgi işlem altyapısını; kesintiye uğratmak, devre dışı bırakmak, yok etmek, kötü niyetle kontrol etmek veya kontrollü olarak bilgileri çalmak amacıyla bir kuruluşun siber uzay kullanımını hedef alan saldırılar da siber saldırı olarak tanımlanmaktadır (NIST, 2021). Siber saldırı süreci, zayıf güvenlik kontrolü içeren sistemleri internet üzerinden taramayı ve yanlış yapılandırılmış sistemleri arama süreciyle başlar. Bir bilgisayar korsanı sisteme bulaştığında virüslü sistemi uzaktan çalıştırabilir veya sisteme korsanlar için casusluk yapması üzerine komutlar gönderebilir. Ayrıca bilgisayar korsanları virüs bulaşan sistemlerin yazılımda bazı hatalar, anti-virüs eksiklikleri ve hatalı sistem yapılandırması gibi bazı kusurların var olmasını bekler ve böyle diğer sistemlere de virüs bulaştırabilmeyi amaçlar (Uma & Padmavathi, 2011, s.390).

Siber saldırı türlerinde yaygın olarak kullanılan yöntemler ise aşağıda verilmiştir (Butch vd. 2017; IBM, 2020):

• **Bilgi ve Veri Aldatmacası:** Bir bilgisayar sistemine giriş öncesinde veya giriş sırasında verilerin yetkisiz olarak değiştirilmesi ve işlem tamamlandıktan sonra tekrar eski haline getirilmesidir (Fraudfighting, 2021).

• **Salam Tekniği:** Siber suçluların her seferinde fark edilmeyecek boyutta kaynak veya maddi varlık çaldıkları bir tekniktir (Fraudfighting, 2021).

• **Hackleme:** İzinsiz bir şekilde bilgisayar sistemlerine erişilmesine denilmektedir (Butch vd., 2017).

• **Virüs Yayılması:** Saldırı altındaki sistemin yok edilmesi amacıyla başka bir sisteme eklenen kötü amaçlı yazılımlardır (Cybercrimechambers, 2021). Bir ağdaki diğer bilgisayarlara veya dosyalara yayılma özelliği gösterir (Butch vd., 2017).

• **Mantık Bombası:** Bu kötü amaçlı yazılım, saatli bombaya benzer şekilde çalışır. Bir mantık bombası, önceden programlanmış bir tarih ve saatte tetiklenen veya belirli mantıksal koşullar karşılanana kadar devre dışı kalır. Mantık bombası tetiklendikten ve etkinleştirildikten sonra veri bozulması, dosya silme veya sabit disk temizleme yoluyla saldırı bilgisayarına zarar verir (IBM, 2020).

• **Hizmet Engelleme Saldırıları (Denial of Services (DoS):** Bu saldırılar, bir sistemin kaynaklarını doldurur, onları bunaltır ve hizmet isteklerine yanıt verilmesini engeller ve sistemin gerçekleştirme yeteneğini büyük ölçüde azaltır. DoS saldırılarının amacı genellikle hizmet reddi veya farklı bir ikinci saldırı oluşturmaktır (IBM, 2020).

• **E-dolandırıcılık:** Meşru bir kuruluş gibi görünerek kredi kartı numaraları ve kullanıcı adı şifre kombinasyonlarını gibi gizli bilgileri çıkarmaya yönelik saldırılardır (Butch vd., 2017).

• **Solucan ve Truva Atı Saldırıları:** Solucanlar karmaşık yapıya sahip zararlı yazılımlardır ve genellikle e-posta ekleri ve çeşitli web siteleri üzerinde paylaşılan dosyalar üzerinden yayılırlar. Kullanıcının veri kaynaklarını kullanarak kendi kaynak dosyalarını diğer kullanıcılara ulaştırmayı denerler. Truva atı ise, kendilerini yararlı bir yazılım gibi göstererek karşıdan yüklenilmeyi beklerler. Truva atı yazılımları kullanıcının kişisel bilgilerini çalmak amacıyla kullanılmaktadır (İTÜBİDB, 2013).

2.4. Siber Güvenlik Risklerine Karşı Alınan Önlemler

1960 ve 1970'lerde yapılan ilk araştırmalar işletim sistemlerinin güvenliğinin sağlanması üzerine yapılmıştır. Bell ve LaPadula'nin güvenlik politikaları formulüze edilerek işletim sistemleri için uyarlanmıştır. Ardından Honeywell, SCOMP ve MULTICS gibi güvenli işletim sistemlerini geliştirmiştir. Günümüzde işletim sistemlerinin güvenliği oldukça önem arz etmekte ve Microsoft gibi firmalar ürünlerinin güvenliğinden emin olmak adına oldukça büyük kaynak ayırmaktadır. 1980'li yılların başı itibariyle veri tabanı sistemlerinin güvenliği üzerine çalışmalara başlanmıştır. Araştırmaların odak noktasının büyük bir bölümünü, çok düzeyli güvenli veritabanları (multilevel secure database) oluşturmaktaydı. Bunun nedeni ise veritabanı sistemlerinin veriler arasındaki ilişkiyi zorunlu kılması ve ek güvenlik önlemlerine ihtiyaç duymasıdır. Veriler üzerinde birden fazla sorgu oluşturma yoluyla hassas bilgilere ulaşılması bir endişe kaynağı haline gelmiştir (Thuraisingham, 2005, s.64).

Bu noktada siber güvenlik stratejileri veri bütünlüğünü koruma açısından büyük önem arz etmektedir. Örnek vermek gerekirse, polyinstantiation (çoklu somutlaştırma) çok düzeyli ilişkili veri modelleri içerisinde kullanılan önemli bir siber güvenlik stratejisidir. Polyinstantiation paylaşılan bir kaynağın farklı örneklerinin oluşturulup farklı kullanıcılara farklı örneklerinin gösterilmesi olarak tanımlanabilir (Di Vimercati & Samarati, 2011). Ayrıca doğru ayrıcalıklara sahip olmayan bir kullanıcının daha hassas bilgileri görmesini önlemek için paylaşılan bir kaynağın birden çok örneğinin oluşturulduğu bir siber güvenlik stratejisidir. Bu stratejinin temel amacı, bir nesnenin veya belgenin bir kopyasını yapmak ve orijinal belgeyi veya nesneyi el değmeden bırakarak ikinci kopyanın niteliklerini değiştirmektir (Mezquita, 2020).

Bilgisayar ağ sistemlerinin güvenliği ile dağıtılmış sistemlerin güvenliği (veri merkezleri, multimedya sistemleri gibi) tüm sistem güvenliğini oluşturan diğer iki temel ögedir. Şifreleme ve kriptografi üzerine yapılan araştırmalar, ağlar ve Web nedeniyle büyük önem kazanmıştır. Dağıtılmış sistemlerin güvenliği üzerine yapılan araştırmaların çoğu Web'in güvenliğinin yanı sıra dağıtılmış nesne yönetim sistemleri gibi sistemlerin güvenliğini sağlamaya da odaklanmaktadır. İşletim sistemlerinin güvenliği, veri tabanı sistemlerinin güvenliği, ağ sistemlerinin güvenliği ile dağıtılmış sistemlerin güvenliği sistem güvenliğini oluşturan dört temel unsurdur (Thuraisingham, 2005, s.65).

3. BİLGİ TEKNOLOJİLERİNİN DENETİMİ

Bilgi teknolojisi denetimi, bir kuruluşun bilgi teknolojisine ilişkin altyapının, faaliyetlerin, veri kullanımı ve yönetiminin, politikalarının, prosedürlerinin ve operasyonel süreçlerinin genel kabul görmüş standartlara veya yerleşik politikalara göre incelenmesi ve değerlendirilmesi olup (Harvard, 2021); mali denetim süreçleri ve denetim mesleği pratikleri ile büyük oranda benzerlikler içermektedir. Bilgi teknolojilerinin denetim süreçleri ile mali denetim arasında da gerekli hususlarda iletişim halinde olunması beklenirken; muhasebe tutarsızlıkları, uyumluluk açıkları ve iç kontroller konusunda denetçilere ve yönetime rehberlik edilir.

Birçok işletme bilgisayar sistemlerinin güvenliğini ve bütünlüğünü kontrol etmede büyük başarısızlıklar yaşayabilmektedir. Binlerce çalışan ve sistem arasında dağıtılan bilgisayar ağlarının büyüklüğü, potansiyel bir güvenlik açığı noktasını temsil etmektedir. Bu nedenle iç denetim sürecinin önemi büyük önem arz etmektedir (Romney & Steinbart, 2017, s.198). Denetim mesleği ve uygulamaları teknolojik gelişmelere kayıtsız kalmayarak günümüzde geldiği noktaya kadar birçok evrede değişimler yaşamıştır (Güneş vd., 2013). Bir iç kontrol sistemi geliştirmek ve kuruluşun kontrol hedeflerine ulaşabilmesi için bilgi teknolojileri konusundaki yeteneklerini ve risklerini kapsamlı bir şekilde analiz etmesi ardından denetçiler ve sistem geliştiricilerle birlikte etkili kontrol sistemleri tasarlaması gerekmektedir (Romney & Steinbart, 2017, s.198).

İş ortamlarının daha karmaşık hale gelmesi karar vericilerin güvenilir bilgiye ulaşma olasılığını azaltmıştır. Bu nedenle bilgi riski gündeme gelmiştir. Bilgi riski karar vericilerin karar süreçlerinde yanlış bilgiyi kullanma riskidir. Bilginin coğrafi mesafeler, organizasyonel katmanlar ve bir şirketin büyümesiyle ilişkilendirilen diğer faktörler nedeniyle karar vericilerin bilgiden uzaklaşması bir risk unsurudur. Ayrıca temel alınan verilerin hacminin ve karmaşıklığının artmasıyla beraber veri hazırlayıcıların karar vericilerden farklı amaçlara sahip olması karar verme süreçlerini etkileyen risk unsurlarıdır (Turner vd., 2017, s.216).

Bilgi teknolojileri (BT) denetimi, bilgisayar denetimi ya da elektronik veri işleme denetimi olarak da adlandırılabilmektedir. BT denetimi, bir işletmenin BT altyapısının kontrollerinin incelenme sürecinden oluşmaktadır. Bu incelemeler finansal denetim, iç denetim ve diğer güvence hizmetleri ile beraber koordine edilebilmektedir (Güneş vd., 2013). Bilgi

riskini azaltmak ve denetim sürecini sistematik bir süreç olarak inceleyebilmek adına otoritelerce belirli standartlar ve çerçeveler oluşturulmuştur.

Literatürde, siber denetim süreci üzerine yoğunlaşmış 4 ana standart ve çerçeve bulunmaktadır. Bunlar (Kahyaoğlu & Çalıyurt, 2018, s.362); Bilgi ve İlgili Teknolojiler için Kontrol Hedefleri (COBIT), Uluslararası Standardizasyon Örgütü (ISO), Amerikan Yeminli Mali Müşavirler Enstitüsü (AICPA) ve NIST'dir.

• **COBIT:** Yönetimin kontrol gereksinimleri, teknik sorunlar ve iş riskleri arasındaki boşluğu aynı anda kapatmasını sağlayan ISACA tarafından oluşturulan bir çerçevedir.

• **ISO:** Kuruluşların bilgi güvenliği ilkelerini desteklemek amacıyla süreçleri ve kontrolleri uygulamasını sağlayan standartları ele alan ISO 27000 serisi geliştirilmiştir.

• **AICPA:** Kuruluşların siber güvenlik risk yönetimi programlarının etkinliği hakkında ilgili ve faydalı bilgilere sahip olmalarına yardımcı olmak için AICPA tarafından bir siber güvenlik risk yönetimi raporlama çerçevesi oluşturulmuştur. Bu çerçeve, Sistem ve Organizasyon Kontrollerinin (SOC) önemli bir bileşenidir.

• **NIST:** Kritik Altyapı Siber Güvenliğini Geliştirme Çerçevesi'nin ilk sürümü Şubat 2014'te yayınlanmıştır. Çerçeve, siber risklerin potansiyel etkilerini azaltan uygulamalarda kuruluşlara rehberlik etmek için mevcut standartlar, yönergeler ve uygulamalar üzerine kuruludur.

Bahsedilen standartlar ve çerçeveler bilgi teknoloji denetiminde efektif risk yönetimini sağlayarak işletmelere yol haritası sunmaktadır. AICPA (2017) standartlarından yararlanılarak hazırlanan risk yönetimi aşamaları sırasıyla aşağıda sunulmuştur (Eaton vd., 2019).

• **Siber güvenlik risklerini tanımlama ve önceliklendirme:** Denetim firmaları, BT uzmanlıklarından ve mevcut siber güvenlik tehditleriyle ilgili bilgilerinden yararlanarak şirketlerin siber güvenlik risklerini belirlemelerine ve önceliklendirmelerine yardımcı olabilir.

• **Siber güvenlik kontrol sistemi tasarımı:** Denetim firmaları, şirketlerin aşama 1'de tanımlanan riskleri ele almak için siber güvenlik kontrolleri tasarlamalarına yardımcı olabilir. Ayrıca denetim firmaları, endüstrideki en iyi uygulamalar ve kontrol standartları (örneğin, AICPA'nın siber güvenlik kontrol kriterleri) dâhil olmak üzere önemli BT kontrol sistemi uzmanlığına sahiptir.

• **Siber güvenlik kontrollerinin çalışma etkinliğini test etme:** Denetim firmaları, şirketlerin siber güvenlik kontrollerinin çalışma etkinliğini, danışmanlık veya güvence kapasitelerinde test edebilir. Ayrıca mali tablo denetimleri ve BT danışmanlık hizmetleriyle birlikte BT kontrollerini test etme konusunda kapsamlı deneyime sahiptir. Harici bir hizmet olarak bildirilmemişse bu danışmanlık hizmeti iç denetim olarak kabul edilecektir.

• **Harici siber güvenlik raporlaması:** Denetim firmaları, şirketlerin dış kaynaklı kriterlere göre (örneğin, AICPA'nın kurum düzeyinde siber güvenlik raporlama çerçevesi) harici siber güvenlik raporları hazırlamasına yardımcı olabilir.

• **Harici siber güvenlik raporlaması konusunda güvence hizmeti:** Denetim firmaları, şirketlerin siber güvenlik risk yönetimi programının etkinliğine ilişkin resmi bir güvence sözleşmesine hazırlanmalarına ve hazır olup olmadıklarını değerlendirmelerine yardımcı olabilir. Hazırlık değerlendirmeleri Aşama 1-4'ün başarıyla tamamlanmasına dayanmalıdır. Denetim firmaları, bir şirketin siber güvenlik risk yönetimi programının etkinliğine ilişkin resmi bir güvence sözleşmesi sağlayabilir. Güvence raporları kamuya açık olarak paylaşılabilir veya paylaşılamaz. Kamuya açık olarak paylaşılıyorsa, denetim firması bağımsızlık amacıyla Aşama 1-4'te herhangi bir danışmanlık hizmeti vermemiş olmalıdır.

4. BANKACILIK SEKTÖRÜNDE BİLGİ TEKNOLOJİLERİ GÜVENLİĞİ VE SİBER GÜVENLİK

İş modelinin, yasaların, standartların, düzenlemelerin de bir gereği olarak bankacılık sektöründe bilgi teknolojilerine ilişkin güvenlik önlemlerinin alınması ve bu süreçlerin denetimi hayati bir fonksiyondur. Finansal kurumlar özellikle de bankalar denetim süreçlerine aşina olan kurumlar olup faaliyetlerinin doğası gereği ve güvence sağlama amacıyla denetim faaliyetlerine önem vermektedirler. Bilgi teknolojilerinin ve sistemlerinin denetiminde her ne kadar müşteri varlıkları ilk korunan varlıklar olarak öne çıksa da bankanın üstlendiği maliyet ve karşılaşılabilecek sorunlar açısından karmaşık ve dolaylı etkileri olan önemli bir yönetsel alandır. Bu kapsamda bu konuya ilişkin faaliyetlerin denetlenmesi ve raporlanması da banka ile ilgili paydaşlar açısından önem kazanmaktadır.

İşletmelerin finansal açıdan önemli sürdürülebilirlik bilgilerinin yatırımcılara ve kamuya açıklanmasına rehberlik edecek standartlar belirleyen bağımsız ve kar amacı gütmeyen bir kuruluş olan Sürdürülebilirlik Muhasebesi Standartları Kurulu (SASB), tarafından yayınlanan Ticari Bankalar Standardında ifade edildiği üzere kişisel finansal verilerin gizliliğini

ve veri güvenliğini sağlamak ticari bankalar endüstrisinin temel bir sorumluluğudur. Bu alandaki performansı yönetemeyen şirketler, azalan gelir ve tüketici güvenine duyarlıdır. Bu çerçevede yapılacak güvenlik ihlallerinin sayısı ve yönetim stratejilerinin niteliğine ilişkin daha fazla açıklama, hissedarların ticari bankaların hissedar değerini nasıl koruduğunu anlamalarını sağlayacaktır. Ticari bankaların sürdürülebilirlik raporlarında yayınlamaları öngörülen çerçevede siber güvenlik (veri güvenliği) ile ilgili sayısal sonuçlar ve diğer açıklamalar ilgili standartta açıklanmıştır. Bu kapsamda banka tarafından muhafaza edilen bilgilerin yetkisiz edinilmesi, erişilmesi, kullanılması veya ifşa edilmesi durumları olarak tanımlanan toplam veri güvenliği ihlali sayısı ve müşterilerin kişisel verilerinin ifşası ile ilgili yüzdesel hesaplamalar yapılacak ve açıklanacaktır. Sürdürülebilirlik raporlarında muhasebe metriği olarak ifade edilen sayısal bilgilerin yanında diğer açıklamalara da yer verilmelidir. Bu kapsamda; veri güvenliğine yönelik güvenlik açıklarını ve tehditleri belirlemeye ve ele almaya yönelik yönetim yaklaşımının tartışılması hakkında ifadeler de açıklanmalıdır (SASB, 2021b).

Bilgi sistemlerinin güvenliğinin sağlanması amacıyla Türkiye'de yakın dönemde çok sayıda düzenleme uygulamaya konulmuştur. Bankacılık sektörü ile ilgili ilk düzenlemeler arasında "Bankacılık Düzenleme ve Denetleme Kurumu (BDDK) tarafından yayımlanarak yürürlüğe giren "Bankalarda Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Bilgi Sistemleri Denetimi Hakkında Yönetmelik (2006)", "Bankalarda Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Bilgi Sistemleri Denetimine İlişkin Rapor Formatı Hakkında Tebliğ (2006)" ve "Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ (2008)" yer almıştır. 2010 yılında yayımlanan ve en son 2014 yılında değişikliğe gidilen "Bankalarda Bağımsız Bilgi Sistemleri ve Bankacılık Süreçleri Denetimi Hakkında Yönetmelik" 2006 yılında yayımlanan önceki düzenlemeyi yürürlükten kaldırmıştır. Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Banka Bilgi Sistemleri ve Bankacılık Süreçlerinin Denetimine İlişkin Rapor Hakkında Tebliğ de 2010 yılında yayımlanmış ve 2006'da yayımlanan tebliği yürürlükten kaldırmıştır (Bankacılık Düzenleme ve Denetleme Kurumu [BDDK], 2021).

Bilgi Sistemleri (BS) ile ilgili çok sayıda kurum ve kuruluş tarafından düzenlemeler yapılmıştır. Sayıştay tarafından 2013 yılında Bilişim Sistemleri Denetim Rehberi yayınlanırken, Gümrük ve Ticaret Bakanlığı tarafından 2013 yılında Gümrük İşlemlerini Kolaylaştırma Yönetmeliği kapsamında ihracatçı firmaların lisans almasında ISO27001 zorunluluğu getirilmiştir benzer bir kapsamda yapılan düzenleme ile 2016 yılında EPDK tarafından lisans sahiplerine ISO27001 zorunluluğu getirilmiştir. 2014 yılında BDDK ödeme

ve elektronik para kuruluşlarının bilgi sistemlerinin yönetim ve denetimini düzenleyen bir tebliğ yayınlanmış ve 2015 yılında Gelir İdaresi Başkanlığı yeni nesil ödeme kaydedici cihazlara ait güvenlik servis sağlayıcı merkezlerinin denetimine ilişkin teknik kılavuz yayınlamıştır. Türkiye Bankalar Birliği Risk Merkezi 2016 yılında üyelerinin bağımsız denetim kuruluşlarınca gerçekleştirilecek denetimi ve raporlamasına ilişkin bir genelge yayınlanmış bilgi sistemleri güvenliği ve denetimi konusunda yayınlanan düzenlemeler arasında yer almıştır (KPMG, 2021).

Kişisel Verilerin Korunması Kanunu (KVKK, 2016) toplumda verilerin işlenmesi ile ilgili güven sağlanması için diğer önemli bir adımdır. Kanunda, kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korunması ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlenmesi amaçlanmıştır. Kanunda özel nitelikli bilgilerin özelliği ile kişisel verilerin işlenmesi şartları da belirtilmiştir. Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi veri sorumlusu olarak ifade edilmekte olup, veri güvenliği ile ilgili veri sorumlusuna denetim yükümlülüğü de getirilmiştir.

2010 yılında yayımlanan yönetmelikte BS denetimi (BSD), bilgi sistemleri yönetimi kapsamında yer alan süreç, faaliyet, yazılım ve donanım gibi bilgi sistemi unsurları ve bankacılık faaliyetlerine ilişkin süreçler ile bu sistem ve süreçler bünyesinde tesis edilen iç kontrollerin değerlendirilmesi sonucunda görüş oluşturulması ve rapora bağlanması aşamalarından oluşan süreç olarak ifade edilmiştir. BS denetiminde, denetlenenin bilgi sistemleri ve bankacılık süreçlerinin ve bu sistem ve süreçlere ilişkin iç kontrollerinin uyumluluk, etkinlik ve yeterliliği hakkında görüş oluşturulması amaçlanmaktadır. Bilgi sistemleri ve bankacılık süreçleri denetimi ile bağımsız denetimin ilişkisine yönetmelikte yer verilmiş olup, Bağımsız denetim ile BSD; birbirlerinin kapsam ve sonucunu etkileyecek hususlar ihtiva etmeleri nedeni ile bütünsel bir yaklaşım içinde planlanması ve uygulanmasına yönelik hususlar yer almıştır. Denetim sonucunda denetimine ilişkin görüşün "şartlı", "olumsuz" ya da "görüşten kaçınma" şeklinde olması durumunda; görüş ve görüşe esas teşkil eden tespitler finansal denetçiye yazılı olarak iletilmesi yönetmelikte düzenlenmiş ayrıca BSD raporunun içeriğinin gizli bilgi niteliği taşıdığı ve herhangi bir ortamda yayımlanmaması hususu ifade edilmiştir (BDDK, 2010).

En önemli gelişmeler arasında BDDK Mart 2020'de yayımlanan Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik yer almıştır. Düzenlemede bilgi sistemlerinin yönetimi ile elektronik bankacılık hizmetlerinin sunulmasında ve bunlara ilişkin risklerin yönetiminde esas alınacak asgari usul ve esaslar ile tesis edilmesi gereken bilgi sistemleri kontrolüne ilişkin hükümler yer almaktadır. Yönetmelikte Bilgi Sistemlerine İlişkin Risk Yönetimi ve Kontrollerin Tesisi'ne ilişkin ayrı bir kısım bulunmakta olup; bu bölüm, bilgi sistemleri yönetişimi, bilgi güvenliği yönetimi, sistem geliştirme ve değişiklik yönetimi, bilgi sistemleri sürekliliği ve erişilebilirlik yönetimi, dış hizmet alımı ve bilgi sistemleri iç kontrol ve iç denetim faaliyetleri alt bölümlerinden oluşmaktadır (BDDK 2020).

5. YÖNETMELİK ÇERÇEVESİNDE TÜRK BANKACILIK SEKTÖRÜNDE BİLGİ SİSTEMLERİNE İLİŞKİN FAALİYETLERİN ANALİZİ

BDDK tarafından yayınlanan ve güncel mevzuat çerçevesini de oluşturan Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik çerçevesinde diğer işletmelerde de olduğu gibi bankaların da maruz kalabileceği riskleri önleme adına önemli birçok faaliyetin yürütülmesi beklenmektedir. Bu kapsamda bankaların faaliyetleri kamuya açık güncel kaynaklardan araştırılmış ve siber güvenlik risklerini önlemeye yönelik mevcut durumun analizi yapılmıştır.

5.1. Araştırmanın Yöntemi

Bu çalışmanın amacı, işletmeler için siber güvenlik risklerini ortaya koymak ve bu riskleri yönetmeye yönelik bilgi sunmaktır. Ayrıca çalışmada bankaların siber güvenlik ve bilgi teknolojileri faaliyetlerine ilişkin bilgileri incelenerek bu uygulamaların içeriğinin tespit edilmesi amaçlanmaktadır. Çalışmanın kapsamını aktif büyüklüklerine göre ilk 10 banka sıralamasına giren bankalar oluşturmaktadır. Bankaların 2019 ve 2020 faaliyet raporları ve entegre raporlarında siber güvenlik ile ilgili vermiş oldukları bilgiler, Bilgi Sistemleri (BS) ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik kapsamında incelenerek araştırma gerçekleştirilmiştir. Araştırmanın kısıtlarından ilki Türkiye'de faaliyet gösteren tüm bankaların araştırmaya dahil edilmemesidir. İkinci bir kısıt ise araştırma kapsamında yer alan 10 bankadan bazılarının hazırlamış olduğu raporlarda, çalışmanın amacına hizmet eden veriler bulunmamaktadır. Bu sebeple bazı bilgiler 10 bankanın tamamı için verilememiştir.

5.2. Bankaların Siber Güvenlik Faaliyetlerine İlişkin Bilgiler

5.2.1. Bilgi sistemleri komitesine ilişkin bilgiler

Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmeliğin 4. maddesi kapsamında; yönetim kuruluna verilen sorumluluklar çerçevesinde BS strateji planı, BS Strateji Komitesi ve BS Yönlendirme Komitesi oluşturulması gerekliliği, komitelerin nasıl oluşturulacağı ve faaliyetleri hakkında düzenlemeler mevcuttur (BDDK, 2020). Bahsi geçen yönetmelik kapsamında araştırmanın örneklemini oluşturan bankaların bilgi sistemleri faaliyet alanı ile ilgili oluşturdukları komitelerine ilişkin bilgilere Tablo 1'de yer verilmiştir.

Tablo 1. Bankalar ve bilgi sistemlerine ilişkin oluşturulan komiteler

Banka Adı	**Komitenin Adı**
Türkiye Cumhuriyeti Ziraat Bankası A.Ş.	Bilgi Sistemleri Strateji Komitesi Bilgi Güvenliği Komitesi
Türkiye Vakıflar Bankası T.A.O.	Bilgi Güvenliği Komitesi
Türkiye Halk Bankası A.Ş.	Bilgi Sistemleri Strateji Komitesi Bilgi Güvenliği Komitesi
Türkiye İş Bankası A.Ş.	Bilgi Güvenliği Koordinatörlüğü Bilgi Sistemleri Strateji Komitesi
Türkiye Garanti Bankası A.Ş.	Bilgi Teknolojileri Strateji Komitesi Bilgi Sistemleri Süreklilik Komitesi Bilgi Sistemleri Yönlendirme Komitesi Bilgi Güvenliği Komitesi Veri Güvenliği ve Verinin Korunması Komitesi
Yapı ve Kredi Bankası A.Ş.	Bilgi Sistemleri Yönlendirme Komitesi Bilgi Güvenliği Komitesi
Akbank T.A.Ş.	Bilgi Riski Yönetim Başkanlığı Bilgi Riski Yönetim Komitesi
QNB Finansbank A.Ş.	Bilgi Sistemleri Strateji Komitesi Bilgi Sistemleri Süreklilik Komitesi Bilgi Güvenliği Komitesi
Denizbank A.Ş.	İç Kontrol Merkezi ve Uyum Başkanlığı Kontrol Değerlendirmesi ve IT Kontrol Bölümü
Türk Ekonomi Bankası A.Ş.	Operasyonel Risk Komitesi

Kaynak: Bankaların faaliyet ve entegre raporlarından oluşturulmuştur

Tablo 1'de görülebileceği gibi bazı bankalarda tek bir komite oluşturulmuş iken bazılarında ise birden fazla komitenin oluşturulduğu tespit edilmiştir. Bu doğrultuda Garanti Bankası 5 komite ile en fazla bilgi sistemleri komitesi oluşturan banka konumundadır. Her bir bankanın bilgi sistemleri stratejileri kapsamında bu komiteleri farklı isimlerle oluşturduğu gözlemlenmiştir. Genellikle komiteler, bilgi güvenliği komitesi ve bilgi sistemleri strateji

komitesi adı altında kurulmuştur. Ziraat Bankası banka yönetiminde yer alan bilgi sistemleri strateji ve bilgi güvenliği komitelerinin BDDK tarafından düzenlenen mevzuattaki görev ve yetkileri yerine getirmek ve komitelerin ilgili alanlarındaki stratejik faaliyetleri düzenlemek olduğunu belirtmiştir (Ziraat Bankası, 2020).Yapı ve Kredi Bankası'nda faaliyet gösteren bilgi sistemleri yönlendirme komitesinin bilgi teknolojileri stratejik planlaması doğrultusunda yol haritasını belirlemekle sorumlu olduğu ve bankanın bilgi güvenliği komitesinin ise banka yönetim kurulu adına bilgi güvenliği politikası ve süreçlerinin oluşmasında ve denetimde görevli olduğu dile getirilmiştir (Yapı ve Kredi Bankası, 2020). Ayrıca Garanti Bankası ise, benzer şekilde faaliyetlerine devam eden bilgi teknolojileri strateji, bilgi sistemleri süreklilik ve bilgi sistemleri yönlendirme komiteleri de dâhil olmak üzere üst yönetimin komite faaliyetlerine katkıda bulunabilmesi amacıyla yönetim kurulu üyeleri bulunan komitelerin toplam komitelere oranını %90'na çıkardığını belirtmiştir (Garanti Bankası, 2020).

5.2.2. İç kontrol ve iç denetim tarafından bilgi güvenliği alanında yapılan kontrollere ilişkin bilgiler

Yönetmeliğin 30, 31 ve 32. maddelerinde bilgi sistemleri iç kontrol ve iç denetim faaliyetleri ayrıntılı olarak düzenlenmiştir. Bu çerçevede madde 30'da BS iç kontrol fonksiyonunun çerçevesi belirlenmiş olup, BS iç kontrol sorumlusu atanması ve BS iç kontrol faaliyetleri bu kişinin sorumluluğunda yürütülecek faaliyetlere ilişkin düzenleme belirtilmiştir. Bulguların takibi ve güvence sağlanması, personelin eğitimi ve kaynak tahsisi ile ilgili düzenlemelere de bu bölümde yer verilmiştir. 30. maddede banka ve bankanın dış hizmet sağlayıcıları nezdindeki BS yönetimine ilişkin faaliyetler, bu faaliyetleri destekleyen süreçler ve tesis edilen BS kontrollerinin mevzuata ve banka içi politika, prosedür ve standartlara uyumlu olduğu ve bilgi sistemlerine ilişkin iç kontrol ve risk yönetimi faaliyetlerinin etkinliği ve yeterliliği hususunda yönetim kuruluna güvence sağlamak üzere BS iç denetim fonksiyonu oluşturulacağı, BS iç denetim sorumlusu atanacağı ve BS iç denetim faaliyetleri bu kişinin sorumluluğunda yürütüleceği belirtilmektedir (BDDK, 2020).

Yönetmeliğin bu maddeleri kapsamında bankaların raporlarının incelenmesi neticesinde ulaşılan ve öne çıkan bilgiler aşağıda yer almaktadır.

Vakıfbank'ta, iç denetim faaliyetleri kapsamında denetime giren şube ve genel müdürlük birimlerinde ISO 9001 Kalite Yönetim Sistemi, 14001 Çevre Yönetim Sistemi, ISO 27001 Bilgi Güvenliği Yönetim Sistemi ve ISO 22301 İş Sürekliliği Yönetim Sistemi'ne

entegrasyona öncelik verildiği belirtilmiştir. Ayrıca Swift Customer Security Framework, Gelir İdaresi Başkanlığı ve Özel Entegratör Denetimi gibi denetimlerde başarıyla tamamlanmıştır (Vakıfbank, 2020). Benzer şekilde Halk Bankası'da ISO 20000 Bilgi Teknolojileri Hizmet Yönetim Sistemi çerçevesinde dijitalleşme ve bilgi güvenliği çalışmalarını yürütmektedir. Ayrıca raporda GRI 103 Yönetim Yaklaşımı 2016 ve GRI 418 Müşteri Gizliliği 2016 yaklaşımlarının uygulandığı belirtilmiştir (Halkbank, 2019). 2019 yılında Türkiye İş Bankası ise iç kontrol faaliyetleri açısından 36 adet kontrol noktasını ikinci seviye kontrol açısından günlük, haftalık ve aylık olarak gözden geçirmiş ayrıca bir dış denetim çalışması ile bir sızma testi çalışması da uygulanmıştır (İş Bankası, 2019).

Denizbank, banka kontrol süreçleri kapsamında risk kontrol matrisleri hazırlamakta ve yönetim beyanı testleri gerçekleştirmektedir. Denizbank COBIT çerçevesi dikkate alarak Bilgi Teknolojileri kontrollerini gerçekleştirmektedir. Ayrıca Denizbank; ITIL ile COBIT standartlarını temel alan ve her yıl bağımsız denetim sonucunda ISAE3402 raporuna sahip olan 'Intertech' firması tarafından dış kaynaklı hizmet alımı gerçekleştirerek bilgi güvenliği hizmetleri desteklenmektedir (Denizbank, 2020).

TEB bilgi teknolojileri denetimi kapsamında yapmış olduğu kontrol ve denetimlerde erişim güvenliği, değişiklik yönetimi ile veri merkezi ve ağ operasyonları başta olmak üzere 3 ana kategoride kontrollerini gerçekleştirmektedir (TEB, 2020).

Akbank Bilgi Riski Yönetim Başkanlığı tarafından gerçekleştirilen risk kontrolleri çerçevesinde BDDK mevzuatı ile beraber COBIT, ISP, ITIL, COSO, NIST, PCI ve DSS gibi uluslararası standartlar esas alınarak ilgili çalışmalar yürütülmektedir (Akbank, 2020). Yapı ve Kredi Bankası COBIT tarafından düzenli olarak her yıl denetlendiğini belirtmiştir (Yapı ve Kredi Bankası, 2020).

5.2.3. Düzenlenen bilgi teknolojileri ve siber güvenlik eğitimlerine ilişkin bilgiler

Yönetmeliğin 19. maddesinde banka genelinde bilgi güvenliği farkındalık seviyesini artırmak için kapsamlı bir bilgi güvenliği farkındalığı eğitim programı oluşturulması gerektiği belirtilmiştir. Aynı maddede eğitim programı, bilgi güvenliği politikaları ve standartları ile birlikte, bilgi güvenliği ve verilerin korunması konusundaki bireysel sorumlulukların neler olabileceği ve bilgi varlıklarını korumak için alınması gereken önlemlerin neler olacağı hususunda bilgiler içermesi gerektiği de ifade edilmektedir (BDDK, 2020). Bu kapsamda

sadece 3 bankanın eğitim faaliyetlerine ilişkin bilgilere raporlarda yer verdiği görülmüştür. Bu bankaların raporlarının incelenmesi neticesinde ulaşılan bilgiler aşağıda yer almaktadır.

Bankaların tüm çalışanlarına bilgi güvenliğine ilişkin farkındalığı artırmak adına verilen eğitimler büyük önem taşımaktadır. Bu kapsamda veri güvenliği ve gizliliği gibi konularda banka çalışanlarına eğitimler düzenlenmektedir. Yapı ve Kredi Bankası, 8.359 çalışanına 3.413 saat bilgi güvenliği eğitimi düzenlemiştir (Yapı ve Kredi Bankası, 2020). Vakıfbank, 2019 yılında 14.533 çalışanına bilgi güvenliği eğitimi düzenlerken 2020 yılında yaşanan pandemi koşulları nedeniyle 450 çalışanına bu eğitim verilmiştir (Vakıfbank, 2020). Garanti Bankası, 2020 yılında düzenlemiş olduğu siber güvenlik eğitimleriyle çalışanlarının %99'una eğitim vererek bir önceki seneye kıyasla çalışanlarının eğitime katılma oranını (%72) yaklaşık %38 oranında artırmıştır. Bu sayede tam zamanlı çalışan başına düşen siber güvenlik eğitim saati 2019 yılına kıyasla 1,19 saatten 1,73 saate çıkmıştır (Garanti Bankası, 2020).

5.2.4. Bilgi sistemleri risk yönetim işlemlerine ilişkin bilgiler

Yönetmeliğin 7. maddesi, varlık envanterindeki bilgi varlıklarına ilişkin tehdit ve güvenlik açıklarının tespit edilmesi suretiyle risklerin belirlenmesi, tespit edilen tehditlere ve güvenlik açıklarına göre bilgi varlıklarının riske maruz kalma olasılıklarının belirlenmesi, risklerin gerçekleşmesi durumunda ilişkili bilgi varlığının gizliliği, bütünlüğü, erişilebilirliği gibi kriterlerine olan etkilerin belirlenmesi suretiyle ilgili bilgi varlığına yönelik etki hesaplaması yapılması, bilgi varlıklarını tehdit eden risklerin belirlenen olasılık ve etki değerlerine göre risk derecelendirmesinin yapılması, risk analizinde gerçekleştirilen çalışmaların bütününü temsil eden özet risk değerlendirme raporunun hazırlanarak üst yönetime sunulması konularında düzenlemeler içermektedir (BDDK, 2020). Yönetmeliğin bu maddesi kapsamında bankaların raporlarının incelenmesi neticesinde ulaşılan bilgiler aşağıda yer almaktadır.

Yapı ve Kredi Bankası Basel II'nin ileri ölçüm yöntemlerine uyum çalışmalarının yürütüldüğünü belirtmiştir. Bu kapsamda bankanın operasyonel risk kayıpları ve önemli risk göstergeleri takip edilmekte olup her yıl bilgi sistemleri risk envanteri çıkarılmaktadır (Yapı ve Kredi Bankası, 2020). Akbank Bilgi Riski Yönetimi Başkanlığı banka içinde işlenen veya banka dışı paydaşlarla paylaşılan verilerin güvenilir, izlenebilir ve tutarlı olması amacıyla gerekli görülen politikaları belirleyen ve yürütülmesini sağlayan birimdir. Her türlü dış dolandırıcılığın (fraud) izlenmesi, tespiti ve önlenmesi bankanın risk yönetimi kapsamından

değerlendirilmekte olup Bilgi Riski Yönetimi Başkanlığı tarafından yürütülmektedir (Akbank, 2020). Denizbank Bilgi Güvenliği ve Bilgi Teknolojileri Risk Yönetimi Grubu; bilgi güvenliği yönetiminin merkezi bir yapı üzerinden işlemesine olanak yaratmak, bilgi güvenliği risklerine ilişkin departmanlar arası koordinasyon çalışmalarını yürütmek ve bilgi güvenliğine ilişkin risk bulgularının tespit ve takibini yaparak gerekli stratejik çalışmaları ve güvenlik politikalarını belirlemekle görevlidir. Bu kapsamda dolandırıcılık (fraud) yönetimi, veri yönetişimi ile bilgi güvenliği programı ve risk yönetimi çalışmaları titizlikle yürütülmektedir. Bilgi teknolojileri denetimi kapsamında; erişim güvenliği, değişiklik yönetimi, veri merkezi ve ağ operasyonları, finansal verilerin oluşum sürecine ilişkin verilere erişim yönetimi gibi alanlar denetim kapsamındaki başlıca kategorilerdir (Denizbank, 2020). Vakıfbank ise bilgi güvenliği risk yönetimi kapsamında dolandırıcılık (fraud) ve bilgi güvenliği konularının daha etkin yönetilebilmesi amacıyla Güvenli Bankacılık Başkanlığı'nı kurmuştur (Vakıfbank, 2020). Halkbank, ISO 9001: 2015 Kalite Yönetim Sistemi Standartları kapsamında risk odaklı bir bakış açısıyla yerinde denetim, merkezde denetim ve bilgi teknolojileri denetimi şeklinde 3 farklı denetim sürecini benimsemiştir. Bilgi teknolojileri denetimi çerçevesinde 85 adet uygulama denetimi gerçekleştirilmiştir (Halkbank, 2019).

5.2.5. Veri güvenliği ve gizliliğine ilişkin bilgiler

Yönetmeliğin 9. maddesinde, banka, bankacılık faaliyetlerinin yürütülmesinde kullanılan verilerin taşındığı, iletildiği, işlendiği, saklandığı ve yedek olarak tutulduğu ortamlarda gizliliğini sağlayacak önlemleri alması gerektiği belirtilmektedir. Aynı maddede ayrıca verilerin tutulduğu ortamın kâğıt veya elektronik ortam olmasından bağımsız olarak alınacak önlemlerin, gizliliği sağlanmaya çalışılan verilerin gizlilik derecesine uygun olması ve gerekli yerlerde ek kontrollerin tesis edilmesi esastır ibaresi de bulunmaktadır. Veri barındıran medya ya da cihazların kullanımdan kaldırılması durumunda, içerdikleri verilerin gizlilik derecesine uygun olarak güvenli bir şekilde imha edilmesi sağlanması gerektiği de belirtilmektedir (BDDK, 2020). Yönetmeliğin bu maddesi kapsamında bankaların raporlarının incelenmesi neticesinde ulaşılan bilgiler aşağıda yer almaktadır.

İş Bankası dijital dönüşüm kapsamında hizmetlerin ve süreçlerin dijitalleşmesi amacıyla banka kaynaklarının önemli bir kısmını bu kanala ayırmakta ve veri güvenliği kapsamında yalnızca yasal mevzuatı takip etmeyip iş süreçlerini sürekli olarak geliştirmektedir. Bu güncellemeler olası tehditlere karşı dirençlilik yaratarak bankanın istenmeyen durumlardaki hızlı karar verme kapasitesini geliştirmesine yardımcı olmaktadır. Bu çerçevede siber güvenlik

takibinin 7/24 yapılabilmesi, zararlı yazılımların engellenmesi amacıyla Güvenlik İstihbarat ve Savunma Merkezi (GİSM) kurulmuştur. Merkez sistemdeki açıkların tespit edilebilmesi amacıyla 2012 yılından beri düzenli olarak sızma testleri gerçekleştirmektedir (İş Bankası, 2019). Garanti Bankası veri güvenliği politikalarının belirlenmesi ve koordinasyonun sağlanması amacıyla Veri Güvenliği ve Verinin Korunması Komitesini hayata geçirmiştir. Komite veri güvenliği ve korunması kapsamındaki süreçlerin takibini ve olası iyileştirmelerini yapmak amacıyla 3 ayda 1 kez olmak üzere toplanmaktadır (Garanti Bankası, 2020).

Ziraat Bankası müşterilerin ve bankanın sır kapsamında değerlendirdiği bilgilerin korunması kapsamında veri güvenliği ekibini faaliyete geçirmiştir. Banka bünyesindeki istemcilerde Windows 10 işletim sisteminin hayata geçirilmesiyle beraber tüm bilgisayarlardaki verilerin dışarı sızmasını engelleyen yeni bir yazılım kurmuş ve taşınabilir bellek ile yazıcı kanalları verilerin dışarı aktarılması konusunda izlenmeye başlanmıştır (Ziraat Bankası, 2020). Vakıfbank günümüzde kurumların en değerli varlıklarının veri olduğu düşüncesiyle çok büyük boyutlardaki verinin depolanması ve yönetilmesi amacıyla sektörde çok az veri merkezinin sahip olduğu Tier 3 ve 4 sertifikalarına sahip Vakıfbank İstanbul Veri Merkezi (VIVEM)'i faaliyete geçirmiştir (Vakıfbank, 2020). Ek olarak TEB, 2020 yılında Euromoney 2020 Özel Bankacılık ve Varlık Yönetiminde En İyi Veri Yönetimi ve Veri Güvenliği ödülüne layık görülmüştür (TEB, 2020).

5.2.6. İleri teknolojinin siber güvenlik ve denetim sürecinde kullanılmasına ilişkin bilgiler

Yönetmelikte de belirtildiği üzere bilgi güvenliği yönetim sisteminin ulusal veya uluslararası standartları ya da en iyi uygulamaları referans alması gerekmektedir. Bu çerçevede bankaların güncel teknolojik gelişmelerin de uygulanmasıyla farklı teknoloji tabanlı faaliyetleri uygulamaya geçirdikleri görülmektedir. Bankaların raporlarından ulaşılan bu kapsamdaki uygulama örneklerine aşağıda yer verilmiştir.

Büyük veri, yapay zeka ve makine öğrenmesini temel alarak karmaşık tehditlere karşı daha etkili savunma ve tespit mekanizmalarını esas alan teknoloji platformların önemi bankaların dikkatini çekmiş durumdadır. Dijital dönüşüm kapsamında büyük veri, yapay zeka, veri analitiği, siber güvenlik, açık bankacılık, robot yazılım ve blok zincir teknolojisi bankalar tarafından dikkate alınmaktadır (Akbank, 2020; İş Bankası, 2020; Vakıfbank, 2020). Bu çerçevede Akbank Covid-19 döneminde uzaktan çalışma koşullarını verimli hale getirebilmek ve bu sayede dolandırıcılık ve siber tehditleri yönetebilmek amacıyla teknoloji kapasitesinde

artışa gitmiştir. Ayrıca uzaktan bağlantı altyapısının (VPN altyapısı) üst düzey güvenlik hizmeti ile hizmet verebilmesi için teknik değişiklikler tamamlanmıştır (Akbank, 2020). Vakıfbank dolandırıcılık önleme, anomali tespiti ve siber güvenlik alanlarında veri analitiği çalışmaları yürütmektedir (Vakıfbank, 2020). İş bankası siber güvenlik çalışmaları kapsamında ana yatırımcısı olduğu Maxis Yenilikçi Girişim Sermayesi Yatırım Fonu aracılığıyla, 2020 yılı Workshop mezunu siber güvenlik girişimi PCI Checklist firmasına 1.1 milyon TL tutarında yatırım gerçekleştirmiştir (İş Bankası, 2020).

Garanti bankası banka ve paydaşları için belirlemiş olduğu öncelikli konularda 8. Sırada siber güvenlik alanına dikkat çekmektedir. Bu kapsamda siber güvenlik risklerinin azaltılması ve veriye dayalı denetim süreçlerinin yaygınlaştırılabilmesi için veri mühendisleri istihdam edilmektedir. Her denetim çalışması için en az 1 veri uzmanı görevlendirilerek denetim sürecinde büyük veri ve makine öğrenmesi teknolojilerinden yararlanılması amaçlanmıştır. Bu sayede denetim sürecinde örneklem yerine verinin tamamının denetlenmesi ve güven aralığının artırılması hedeflenmektedir (Garanti Bankası, 2020).

Yapı ve Kredi Bankası veri güvenliği ve gizliliğini sağlamaya yönelik birçok kontrol mekanizması tasarlamış ve siber güvenlik yatırımlarına banka politikalarınca öncelik verilmiştir. Bu çerçevede son 3 yılda 190 milyon TL tutarından fazla siber güvenliğin sağlanması ve dolandırıcılığı önleme konularında yatırım yapıldığı belirtilmiştir (Yapı ve Kredi Bankası, 2020).

6. SONUÇ

Bilgi teknolojilerinde yaşanan gelişmeler işletmeler tarafından bilgi sistemlerinin ve internet teknolojilerinin yoğun biçimde kullanmasına, faaliyetlerinin büyük oranda bu sistemlerle yönetilmesine, bilgilerin dijital ortamda depolanmasına ve genel olarak tüm işletme faaliyetlerinin dijital dönüşümüne etken olmaktadır. Ancak bilgisayar teknolojilerinin ve internet teknolojilerinin geniş kitleler tarafından yoğun kullanımı ile birlikte, uygulamalardaki güvenlik açıkları, kötü niyetli uygulamalar (bilgisayar korsanlığı vb.) işletmeleri büyük mali zararlarla karşı karşıya bırakmaktadır. Güvenin çok önemli bir faktör olduğu bankacılık sektöründe güven kaybı, ekonomik sonuçlarla birlikte itibar kaybına da neden olabilmektedir. Aynı zamanda işletmenin kritik önemdeki bilgilerinin ve müşterilere ait kişisel verilerinin kurum dışındaki kötü niyetli kişilerce ele geçirilmesi ayrıca yasal olarak suç niteliği de taşımaktadır. Bankacılık sektörü yerine getirdiği fonksiyonlar ve yürüttüğü faaliyetlerle birlikte

dijitalleşmenin yoğun yaşandığı bir sektördür. Sektörün bu özelliğinin yanı sıra mali sektörün lokomotifi olması ve dolaylı olarak diğer sektörleri etkilemesi sektörü daha da önemli bir hale getirmektedir.

Siber güvenlik ile ilgili çok sayıda tehdit türü ortaya çıkmıştır, zaman içerisinde yeni tehditlerin de ortaya çıkması muhtemeldir. Bu dinamik süreçte işletmelerin de bu tehditlere karşılık güvenlik önlemlerini alması gerekmektedir. Güvenlik önlemlerinin alınmasında da çok sayıda önlem çeşidi uygulamaya konulmaktadır. Ancak işletmelerin bilgi sistemlerinin denetimi ve risk yönetiminde de standartlaşması genel kabul görmüş ilkeler çerçevesinde faaliyet göstermesi beklenmektedir. COBIT, ISO, AICPA ve NIST siber denetim süreçlerine ilişkin standartlar ve çerçeve oluşturmaktadır. AICPA standartlarına dayanarak oluşturulan risk yönetimi aşamalarında muhasebe ve denetim kuruluşlarının BT uzmanlıklarının sürecin her aşamasında etkililiği ön planda yer almaktadır. Mali tabloların bağımsız denetimi görevini üstlenen muhasebe ve denetim kuruluşları, risk yönetiminde sürecin her aşamasında olduğu gibi bilgi sistemleri denetiminin raporlanmasında da ilgili birimlerinin uzmanlıkları ile güvence hizmetlerinde yardımcı olmaktadırlar.

Türkiye'de bankacılık sektöründe bilgi sistemlerinin güvenliğine ilişkin gelişmeler incelendiğinde teknolojideki gelişmeleri ve uluslararası standartları karşılayan güncel mevzuat düzenlemelerinin yapıldığı ve bankalar tarafında da sürece hemen adapte olunduğu görülmektedir. Bu doğrultuda araştırma kapsamında incelenen banka bilgilerinden bilgi sistemlerine ilişkin komitelerin kurulduğu, iç kontrol ve iç denetim faaliyetlerine ilişkin yönetmelik ve standartlara uyumlu bir organizasyon yapılanmasına gidildiği görülmektedir. Araştırmadan elde edilen önemli bir sonuç da iç kontrol faaliyetleri açısından bankaların genel olarak BDDK mevzuatı ve uluslararası standartların gerekliliklerini karşılayan faaliyetler gerçekleştirdiği görülmektedir. Bankaların siber güvenlik farkındalığını artırma ve çalışanların sürece katılımını sağlamak adına önemli eğitim programları uyguladıkları araştırma kapsamında incelenen raporlardan elde edilen diğer bir sonuçtur. Bankalar bilgi sistemlerinden kaynaklı risklerin yönetilmesi için organizasyon yapısında prosedürleri tanımlayarak, ilgili önleyici faaliyetleri ve denetim faaliyetlerini yürütmektedirler. Bu kapsamda raporlarda da paydaşlara farklı düzeylerde kapsayıcılığı olan bilgi akışının sağlandığı görülmektedir. Bankacılık sektöründe bilgi sistemlerinin güvenliğinde önemli bir boyut verilerin taşındığı, iletildiği, işlendiği, saklandığı ve yedek olarak tutulduğu ortamlarda gizliliği sağlayacak önlemleri alması gerekliliğidir. Bankaların bu kapsamda aldıkları önlemler ve yürüttükleri faaliyetler, bankalar nezdinde kurmuş oldukları veri depolama merkezler, sahip oldukları

sertifikalar, almış oldukları ödüller vb. bilgilere bu çerçevede raporlarında yer verdikleri görülmektedir.

Sonraki çalışmalar kapsamında araştırmacılara, Türk bankacılık sektörünün tamamını içine alan bir örneklemle çalışmaları önerilmektedir. Ayrıca siber güvenlik riskleri ve bilgi teknolojileri denetimi sadece bankalar nezdinde önem arz eden bir konu olmayıp diğer tüm işletmeleri de ilgilendirmektedir. Bu sebeple takip eden çalışmalarda bankacılık harici sektörlerin de ele alınması önerilebilir. Son bir öneri ise düzenleyici otoriteler için verilebilir. BDDK çıkarmış olduğu yönetmeliklerle, bankacılık sektöründe bilgi güvenliği ve siber riskleri güvence altına alacak birtakım düzenlemeler getirmiştir. Kanun yapıcıların BDDK'nın yapmış olduğu düzenlemeleri örnek alarak, diğer sektörler için de siber güvenliği ve bilgi teknolojileri denetimini sağlamak adına adımlar atması önem arz etmektedir.

REFERENCES / KAYNAKLAR

Akbank (2020). Erişim tarihi: 02.08.2021, https://www.akbankinvestorrelations.com/tr/images/pdf/faaliyet-raporlari/2020_akbank_faaliyet_raporu_.pdf

Aytekin, A. (2015). *Türkiye'nin siber güvenlik stratejisi ve eylem planının değerlendirilmesi* (Basılmamış yüksek lisans tezi). Gazi Üniversitesi, Ankara.

BDDK. (2010). *Bağımsız denetim kuruluşlarınca gerçekleştirilecek banka bilgi sistemleri ve bankacılık süreçlerinin denetimi hakkında yönetmelik*. Resmî Gazete: 13.01.2010, Sayı: 27461.

BDDK. (2020). *Bankaların bilgi sistemleri ve elektronik bankacılık hizmetleri hakkında yönetmelik*. Resmî Gazete: 15.03.2020, Sayı:31069.

BDDK. (2021). Erişim tarihi: 15.04.2021, https://www.bddk.org.tr/Mevzuat/Liste/50

Bowcut, S. (2021). Erişim tarihi: 02.08.2021, https://cybersecurityguide.org/industries/financial/

Buch, R., Ganda, D., Kalola, P., & Borad, N. (2017). World of cyber security and cybercrime. *STM Journals, 4*(2), 18-23.

Cybercrimechambers. (2021). Erişim tarihi: 02.08.2021, https://www.cybercrimechambers.com/blog-bot-virus-dissemination--124.php

Denizbank. (2020). Erişim tarihi: 02.08.2021, https://www.denizbank.com/hakkimizda/_pdf/faaliyet-raporlari/2020-yili-faaliyet-raporu.pdf

Di Vimercati, S. D. C., & Samarati, P. (2011). Polyinstantiation. In H. C. A. van Tilborg & S. Jajodia (Eds.), *Encyclopedia of cryptography and security*. Boston, MA: Springer.

Eaton, T. V., Grenier, J. H., & Layman, D. (2019). Accounting and cybersecurity risk management. *Current Issues in Auditing, 13*(2), C1-C9. https://doi.org/10.2308/ciia-52419

Florakis, C., Louca, C., Michaely, R., & Weber, M. (2020). *Cybersecurity risk* (No. w28196). National Bureau of Economic Research.

Fraudfighting. (2021). Erişim tarihi: 06.04.2021, https://fraudfighting.org/data-diddling/

Garanti Bankası. (2020). Erişim tarihi: 02.08.2021, https://www.garantibbvainvestorrelations.com/tr/entegre-faaliyet-raporu/

Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021). Working from home during COVID-19 crisis: A cyber security culture assessment survey. *Security Journal.* https://doi.org/10.1057/s41284-021-00286-2

Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security, 5*(4), 438-457. https://doi.org/10.1145/581271.581274

Güneş, F., Kızıldeniz, S., Selçuk, S., Suna, B., & Coşkun, S. (2013). Erişim tarihi: 02.08.2021, 131.pdf (ab.org.tr)

Halkbank. (2019). Erişim tarihi: 02.08.2021, https://www.halkbank.com.tr/content/dam/halkbank/tr/dokumanlar/bankamiz/surdurulebilirlik/2019SurdurulebilirlikRaporu.pdf

Harvard. (2021). Erişim tarihi: 15.04.2021, https://rmas.fad.harvard.edu/faq/what-does-information-systems-audit-entail

Herjavec. (2020). Erişim tarihi: 02.08.2021, https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report.

Hiscox. (2020). Erişim tarihi: 02.08.2021, https://www.hiscox.co.uk/sites/uk/files/documents/2020-06/Hiscox_Cyber_Readiness_Report_2020_UK.PDF

IBM. (2020). Erişim tarihi: 02.08.2021, https://www.ibm.com/services/business-continuity/cyber-attack

ISO/IEC 27000. (2018). Erişim tarihi: 02.08.2021, https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en:term:3.10.

ISO/IEC 27032. (2012). Erişim tarihi: 02.08.2021, https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en

İş Bankası. (2019). Erişim tarihi: 02.08.2021, https://www.isbank.com.tr/contentmanagement/IsbankSurdurulebilirlik/pdf/2019EntegreRaporu.pdf

İş Bankası. (2020). Erişim tarihi: 02.08.2021, https://www.isbank.com.tr/contentmanagement/IsbankFinancialDocuments/Y%C4%B1ll%C4%B1k%20ve%20Ara%20D%C3%B6nem%20Faaliyet%20Raporlar%C4%B1/pdf/faaliyet2020.pdf

İTÜBİDB. (2013). Erişim tarihi: 02.08.2021, https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/vir%C3%BCs-solucan-ve-truva-at%C4%B1

Janvrin, D. J., & Wang, T. (2019). Implications of cybersecurity on accounting information. *Journal of Information Systems*, *33*(3), A1-A2. https://doi.org/10.2308/isys-10715

Johnson, A. L. (2016). Cybersecurity for financial institutions: The integral role of information sharing in cyber attack mitigation. *N.C. Banking Inst*., *20*(1), 277-310.

Kahyaoğlu, S. B., & Çalıyurt, K. (2018). Cyber security assurance process from the internal audit perspective. *Managerial Auditing Journal*, *33(*4), 360-376. https://doi.org/10.1108/MAJ-02-2018-1804

KPMG. (2021). Erişim tarihi: 15.04.2021, https://assets.kpmg/content/dam/kpmg/tr/pdf/2018/05/bt-denetim-standartlari-ve-uygulamalari.pdf

KVKK. (2016). *Kişisel verilerin korunması kanunu*. Resmî Gazete: 07.04.2016, Sayı: 29677.

Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during pandemic. *Computers & Security, 105*, 102248. https://doi.org/10.1016/j.cose.2021.102248

Merriam-Webster. (2021). Erişim tarihi: 02.08.2021, https://www.merriam-webster.com/dictionary/cybersecurity

Mezquita, T. (2020). Erişim tarihi: 02.08.2021, https://cyberhoot.com/cybrary/polyinstantiation/

NIST. (2021). Erişim tarihi: 02.08.2021, https://csrc.nist.gov/glossary/term/cybersecurity

QNB Finansbank. (2020). Erişim tarihi: 02.08.2021, https://www.qnbfinansbank.com/medium/document-file-3042.vsf

Romney, M. B., & Steinbart, P. J. (2017). *Accounting information systems*. New York: Pearson.

Rosati, P., Gogolin, F., & Lynn, T. (2020). Cyber-security incidents and audit quality. *European Accounting Review*, 1-28. https://doi.org/10.1080/09638180.2020.1856162

SASB. (2021b). Erişim tarihi: 15.04.2021, https://www.sasb.org/standards/download/

Tarter, A. (2017). Importance of cyber security. In P. Saskia Bayeri, R. Karlovic, B. Akhgar & G. Markarian (Eds.), *Community policing-A European perspective* (pp. 213-230). Springer.

TEB. (2020). Erişim tarihi: 02.08.2021, https://www.teb.com.tr/UPLOAD/PDF/2021/TEB-Faaliyet-Raporu-2020_final.pdf

Thuraisingham, B. (2005). *Database and applications security integrating information security and data management.* Boca Raton, FL: Taylor & Francis.

Turner, L., Weickgenannt, A., & Copeland, M.K. (2017). *Accounting information systems controls and processes*. Hoboken: John Wiley & Sons.

Uma, M., & Padmavathi, G. (2013). A survey on various cyber attacks and their classification. *International Journal of Network Security*, *15*(5), 390-396. https://doi.org/10.6633/IJNS.201309.15(5).09

Vakıfbank. (2020). Erişim tarihi: 02.08.2021, https://www.vakifbank.com.tr/documents/yiliski/VKF_FRAT_2020_UYG__uyg_65_SPREADS_NY.pdf

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97-102. https://doi.org/10.1016/j.cose.2013.04.004

Von Solms, B., & Von Solms, R. (2018). Cybersecurity and information security-what goes where? *Information and Computer Security*, *26*(1), 2-9. https://doi.org/10.1108/ICS-04-2017-0025

Yapı ve Kredi Bankası. (2020). Erişim tarihi: 02.08.2021, https://assets.yapikredi.com.tr/ResponsiveSite/_assets/pdf/arsiv/surdurulebilirlik/EFR_YKB_TR_2020.pdf?v2

Ziraat Bankası. (2020). Erişim tarihi: 02.08.2021, https://www.ziraatbank.com.tr/tr/yatirimci-iliskileri-ZB/finansal-bilgiler/Documents/2020_entegre_faaliyet_raporu.pdf