ERCİYES AKADEMİ, 2022, 36(2), 707-722
https://doi.org/10.48070/erciyesakademi.110135

İŞLETMELERDE BİLGİ SİSTEMLERİNİN DENETİMİNDE SİBER GÜVENLİK RİSKLERİNİN ÖNEMİ

Serkan AKIN[a] Ahmet TANÇ[b]

Özet

Bilgi sistemleri; sürekli gelişen ve değişen bilgi çağında işletmeler için maliyet azaltıcı, işlemleri kolaylaştırıcı ve zamandan tasarruf sağlayan önemli bir etken olmuştur. İşletmelere birçok alanda kolaylık sağlayan bilgi sistemlerinin aynı zamanda önemli bir risk unsuru olduğu görülmektedir. Bankacılık gibi bazı sektörler için hayati öneme sahip olan bilgi güvenliği için birçok standart yayınlanmış olunup, aslında tüm işletmeler için önemli ve dikkat edilmesi gereken bir konu olduğu açıkça ortadadır. Bu bağlamda çalışmanın amacı işletmelerde bilgi sistemlerinin denetiminde siber güvenlik risklerinin önemini ortaya koymaktır. Çalışma, nitel araştırma yöntemlerinden doküman analizi kullanılarak yapılmıştır. Elde edilen sonuçlara göre; yapılan araştırmalarda organizasyonların karşılaştığı en önemli beş riskin ilk sırasında "siber güvenlik ve veri güvenliği" risklerinin geldiği görülmektedir. Çalışmanın bir diğer sonucuna göre son yıllarda Türkiye'de toplamda bilişim suçlarına ilişkin 60.000 üzerinde olayın gerçekleştiği ve milyonlarca lira tutarında tedbir ve el koyma işlemlerinin yapıldığı ortaya konulmuştur. 2022 yılı mart ayında ise bir bankanın mobil yatırım uygulamasından 16 milyar TL'nin, bilgi sistemlerindeki açık sebebiyle kişisel hesaplara geçirildiği görülmektedir. Bu sebeple bilgi teknolojilerini aktif şekilde kullanan banka gibi diğer işletmelerin de güncel hayatta karşılaşabilecekleri siber risklere önem vermelerinin gereği ortaya konulmuştur. Aynı zamanda örnekler yaşanmış vakalardan alınarak bundan sonra karşılaşılabilecek siber risklere karşı iç ve dış bağımsız denetçilere, işletme yöneticilerine birtakım önerilerde bulunulmuştur.

Anahtar Kelimeler: Bilgi sistemleri, Siber güvenlik riskleri, Bağımsız denetim.

✵ ✵ ✵

THE IMPORTANCE OF CYBER SECURITY RISKS IN AUDIT OF INFORMATION SYSTEMS IN BUSINESSES

Abstract

Information systems; It has been an important factor in reducing costs, facilitating operations and saving time for businesses in the constantly developing and changing information age. Information systems, which provide convenience to businesses in many areas, are also seen to be an important risk factor. Many standards have been published for information security, which is of vital importance for some sectors such as banking, and it is clear that it is an important and important issue for all businesses. In this context, the aim of the study is to reveal the importance of cyber security risks in the control of information systems in enterprises. In this

[a] Öğr. Gör., Kayseri Üniversitesi, Pınarbaşı Meslek Yüksekokulu, Muhasebe ve Vergi Bölümü, serkanakin@kayseri.edu.tr
[b] Doç. Dr., Nevşehir Hacı Bektaşi Veli Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, İşletme Bölümü, atanc@nevsehir.edu.tr
Makale Geliş Tarihi: 10.04.2022, Makale Kabul Tarihi: 14.06.2022

study, which was carried out using document analysis, one of the qualitative research methods, the concepts of information and information systems were explained first. Afterwards, cyber security risks in information systems auditing were explained and some suggestions were made regarding the need to avoid related risks for businesses and those performing business audits. According to the results obtained; In the researches, it is seen that "cyber security and data security" risks come first among the five most important risks faced by organizations. According to another result of the study, it has been revealed that in recent years, more than 60,000 incidents related to cyber crimes have taken place in Turkey, and measures and seizures worth millions of lira have been made. In March 2022, it is seen that 16 billion TL from a bank's mobile investment application was transferred to personal accounts due to the vulnerability in their information systems. For this reason, it has been revealed that other businesses such as banks that actively use information technologies should also give importance to cyber risks that they may encounter in daily life. At the same time, some suggestions were made to internal and external independent auditors and business managers against cyber risks that may be encountered in the future, by taking examples from real cases.
Keywords: Information systems, Cyber security risks, Independent audit.



Giriş

İşletmelerde meydana gelen dijital değişim ve gelişim, denetim süreçlerinin bilgi teknolojileri bakış açısıyla düzenlenmesinin gereğini ortaya koymuştur. Yapılan literatür taramasında Gordon vd. yaptıkları araştırmada bilgi güvenliğinin ekonomik etkilerini araştırmak amacıyla bir model önerisine gittikleri görülmektedir (Gordon vd., 2003). Gansler ve Lucyshyn ise araştırmalarında bilgi güvenliğinin tesis edilmesinde ortaya çıkan zorlukları sıralarken atılacak adımlar hakkında da bilgi vermişlerdir (Gansler & Lucyshyn, 2005). Aktaş ve Soğukpınar tarafından yapılan araştırmada ise bilgi güvenliği risklerini önlemek için kullanılan modellerde, işletmenin ihtiyacını en iyi şekilde karşılayabilecek modelin belirlenmesi gereğine vurgu yapılarak örnek bir model önerisi test edilmiştir (Aktaş & Soğukpınar, 2010). Kurt ve Uysal tarafından yapılan çalışmada ise işletmelerin güncellenen COSO ve yeni yayınlanan raporu doğrultusunda siber risklerin tespitine ya da yönetilmesine yönelik nasıl bir iç kontrol sistemi geliştirmesi gerektiği üzerinde durulmuş ve çeşitli önerilerde bulunulmuştur (Kurt & Uçma Uysal, 2015). Selimoğlu ve Altunel tarafından yapılan araştırmada; siber riskler ve siber risklerin yönetilmesine ilişkin bilgi verilmekle birlikte, siber güvenliğin sağlamasında iç denetimin rolü ortaya konulmaya çalışılmıştır (Selimoğlu & Altunel, 2019).

Bu alanda yapılan araştırmalara bakıldığında bilgi sistemleri risk denetimine ilişkin farklı disiplinlerden de birçok çalışmanın literatüre kazandırıldığı görülse de bilgi sistemleri denetimi açısından siber güvenlik risklerini ele alan çalışmaların kısıtlı kaldığı görülmektedir. Çalışmanın bu bağlamda diğer çalışmalardan farklılaşacağı ve alanda yapılacak yeni çalışmalara ilham vereceği düşünülmektedir. Araştırmanın ilk kısmında bilgi ve bilgi sistemleri açıklanmıştır. Daha sonra bilgi sistemleri güvenliğinden bahsedilerek, işletmelerin karşılaştığı siber güvenlik riskleri ortaya konulmuştur. Çalışmanın son kısmında ise bilgi sistemleri denetimi siber güvenlik riskleri bakış açısıyla anlatılarak çeşitli öneri ve çıkarımlarda bulunulmuştur.

1. Literatür Taraması

Konuya ilişkin literatür taraması yapıldığında bilgi sistemleri denetimi ve siber güvenlik risklerine ilişkin birçok çalışmanın yapıldığı görülmektedir. Bu durum bizlere ilgili konuların denetim alanında ne denli önemli olduğuna işaret etmektedir. Bu bağlamda tekrara düşmemek adına girişte yapılan literatür taraması kapsam dışı bırakılarak ilgili alanda yapılan çalışmalar Tablo 1 yardımıyla sunulmuştur.

Tablo 1. Literatür Taraması

Yazar (Tarih)	Ülke	Çalışmanın Amacı	Sonuç/Öneriler
(Ertaş & Güven, 2008)	Türkiye	Denetçilerin günlük uygulamalarında teknolojik araçlardan faydalanma düzeylerinin belirlenmesi. Ayrıca, yeni teknolojilerin denetim sürecinde kullanılması ile elde edilen sonuçların belirlenmesine çalışılmaktadır.	Bilgi teknolojileriyle birlikte deneyimli çalışanların daha teknik ve riskli alanlara odaklanabildiği, denetim çalışanlarının iş tatmini ve moral düzeyinin arttığı ve denetim çalışmalarının daha kolay incelenebildiği belirlenmiştir.
(Önce & İşgüden, 2012)	Türkiye	Bilgi teknolojileri uygulamalarının iç denetim faaliyeti ile ilişkisini ve iç denetim birimlerinin bu ilişkileri değerlendirmesini araştırmaktır.	Finansal tabloların kısa zamanda hazırlanması ve yayınlanması, iç kontrol sisteminin denetlenmesi, eş zamanlı veri alışverişi ile sağlanan kaynak ve zaman tasarrufu, izleme faaliyetlerinin verimliliğinin artması gibi konularda BT' nin sağladığı faydalar görmezden gelinmemelidir.
(Kayrak, 2012)	Türkiye	Çalışmada BT denetiminin, diğer denetim türleri ile ilişkisi, standartlar, metodoloji, risk ve kontroller çerçevesinde genel bir değerlendirmesi yapılmış ve COBIT 4.1 çerçevesinde Avrupa Birliği Sayıştayı (ECA) tarafından uygulanan BT denetim yaklaşımına yer verilmiştir.	Çalışmada, BT denetiminde değerlendirilmesi gereken kontrollerin, bilgi kriterlerinden yola çıklarak belirlenebileceği tezi ortaya konulmuştur.
(Tuncer vd., 2014)	Türkiye	Teknolojik olarak hızla gelişen dünyamızda bilgi sistemleri denetimleri ile vergi denetimlerinde uygulanabilecek bilgi sistemlerin denetimlerinin ele alınması ile bilgisayar destekli denetim aracı kullanan meslek mensubu vergi denetçisinin, bilgi teknoloji denetimi algısı üzerine yapılan araştırma sonuçlarının irdelenmesidir.	Meslek mensuplarının genel olarak vergi denetimlerinde bilgi teknolojilerinden yararlanılmasının, denetim sürecine önemli ölçüde katkı sağlayacağı düşüncesinde oldukları tespit edilmiştir. Fakat yaptıkları denetim çalışmalarında kendilerine çok fazla bilgi teknolojileri ile ilgili destek sağlanmadığı anlaşılmaktadır.
(Serçemeli & Kurnaz, 2016)	Türkiye	Denetimde bilgi teknoloji ürünleri kullanımına yönelik eğilim sebeplerinin, Teknoloji Kabul Modeli aracılığıyla ortaya konması amaçlanmaktadır.	Vergi müfettiş ve yardımcılarının bilgi teknolojileri ürünlerini kullanıma yönelik algılanan fayda ve niyet eğilimlerinin oldukça yüksek olduğu görülmüştür. Ayrıca, denetim sürecinde algılanan kullanım kolaylığının, bilgi teknolojilerine yönelik tutumu ve algılanan faydanın da kullanıma yönelik niyeti pozitif yönde etkilediği, tutumun davranışa yönelik niyeti, algılanan faydanın davranışa yönelik tutumu ve niyetin de davranışın oluşmasını etkilemediği sonucuna ulaşılmıştır.

Tablo 1. devamı

Yazar (Tarih)	Ülke	Çalışmanın Amacı		Sonuç/Öneriler
(Kaban & Arslan, 2016)	Türkiye	Bankalarca, gelişmiş bir denetim yazılımı olan ACL (Audit Command Language) kullanılarak muhasebe hareketleri üzerinden olası bir zimmet eyleminin nasıl açığa çıkarılabileceğinin anlatılması amaçlanmıştır.		Bir zimmet vakasının ACL programı yardımıyla nasıl tespit edilebileceği senaryo analizi yöntemi ile ortaya konulmuştur. Akabinde söz konusu hilenin denetimine ilişkin yapılması gereken incelemeler izah edilmiştir.
(Öztürk, 2018)	Türkiye	Siber güvenlik denetimindeki tüm sürecin bütüncül bir biçimde ele alınması suretiyle bir model dâhilinde gösterilmesidir.		Yapılan çalışma ile siber güvenlik denetimleri bir bütün olarak ele alındığı için denetim faaliyetleri daha iyi açıklanmakta anlaşılmakta ve literatüre katkı sağlanmaktadır.
(Akçakan at vd., 2021)	Türkiye	İşletmeler 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		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.
(Ağdeniz, 2021)	Türkiye	Kamu iç denetçilerinin bilgi ve iletişim güvenliği denetimi konusunda yetkinliklerinin ve Türk Kamu Mali Yönetim sisteminin önemli aktörlerinden iç denetimin BT denetimi konusunda mevcut durumunun ortaya konması olarak belirlenmiştir.		Kamu iç denetçileri de yapılan düzenlemelerle birlikte yeni dönemde sürdürülebilirliklerini sağlamak adına, henüz çok yeterli bir düzeyde olmasa dahi, eğitimlere katılarak, uluslararası sertifikaları alarak, BT alanına ilişkin denetim faaliyetleri yürüterek uyum sağlamaya çalışmaktadır.
(Yel & Atasoy, 2021)	Türkiye	Bağımsız denetçilerin, dijitalleşmenin bağımsız denetime yansımalarını siber güvenlik yönünden nasıl değerlendirdiğini tespit etmektir.		Dijitalleşmenin bağımsız denetim mesleğine etkisi hakkında, yaş, eğitim durumları, bulundukları il, gelir düzeyi, mesleki unvan ve meslekte geçen süre gibi değişkenlere göre farklılıklar olduğu tespit edilmiştir.
(Atakan, 2021)	Türkiye	Siber güvenlik, siber tehdit ve siber saldırı gibi alanlarda COVİD-19 salgını etkisiyle görülen gelişmeler ile bunlara ilişkin olumsuzlukları kontrol etmek üzere ön plana çıkan " uzaktan denetim" alanında beklenen değişimler anlatılması		Teknolojik yeniliklerle çeşitlenen siber güvenlik riskleri ve tüm dünyada etkisini gösteren COVID-19 salgını sonrasında tüm şirketlerin ve kamu kurumlarının siber güvenliği sağlamak için uzaktan denetim prosedürlerinin yeterliliği ile ilgili yeniden bir
(Kestane, 2021)	Türkiye	Siber güvenliğin etkinleştirilmesine yönelik olarak sürekli süreç denetiminin etkisi" araştırılmıştır ve gelecekte yapılması gereken uygulamalara yönelik önerilerde bulunulması amaçlanmıştır.		Siber güvenlik mekanizmalarının işletmelerde oluşturulmasına yönelik iç kontrol sistemlerinin; özellikle, kontrol ortamının yeniden tanımlanması gerektiği büyük önem taşımaktadır.

Literatüre bakıldığında genel olarak bilgi sistemleri denetimi açıklanarak özellikle iç denetim faaliyetleri üzerinden birtakım çıkarımların yapıldığı görülmektedir. Aynı zamanda meslek mensuplarıyla birlikte kamu/özel iç denetçilerine birtakım önerilerde bulunan çalışmaların varlığından söz etmek mümkündür. Benzer şekilde siber güvenlik risklerinin bağımsız denetim ile bağını kuran çalışmaların varlığından söz etmek de mümkündür. Konu multidisipliner bir yapıda olduğu için bilgisayar mühendisliği alanında yapılan ve model önermeleri içeren birtakım çalışmalar da mevcuttur.

2. Bilgi ve Bilgi Sistemleri

Bilgi, farklı disiplinlerde birçok tanımlamanın yapıldığı bir kavram olarak ortaya çıkmaktadır. Felsefe alanında yapılan yazınlarda bilgi kuramı epistemoloji olarak geçmektedir. Bu çalışmalarda ortaya

konulan ilk husus bilgi denilen kavramın direkt insana ait olduğudur. Felsefi çalışmalarda bilgi akılsal ve zihinsel bir etkinlik olarak anlaşılmaktadır (Çüçen, 2003). Bilgi konusu ele alınırken kendi başına bütüncül bir şekilde tek bir olgu gibi anlatılmaya çalışılsa da konuyla ilişkili ve dolaylı sorularla, konunun dağılması beklenen bir durumdur (Pears, 2003).

Bu denli soyut bir kavram için farklı anlamlar çıkması kaçınılmazdır. Farklı bir bakış açısıyla bilgi; elde bulunan verilerin birtakım süreçlerden geçirilerek bir anlam ifade etmesini sağlayacak hale getirilmesi olarak da açıklanmaktadır (İnci, 2016).

Kurumsal anlamda bilgi en geniş tanımıyla; kurum için kıymetli olan dosya, evrak, bilgisayar, internet siteleri vb. her şeydir. Bilgi, kurumlar için çok değerli ve korunması gereken varlıklardır (Çubukçu, 2018). Bu yüzden üst yönetim tarafından işletmeye ait bilgilerin korunmasına yönelik birtakım prosedürlerin ve kuralların çalışanlara sözlü ve yazılı anlatılarak uygulanması önem arz etmektedir.

Bilgi kavramı anlatıldıktan sonra bilgi sistemlerinin de doğru şekilde anlaşılması gerekmektedir. Bilgi sistemleri, bir etkinliği yerine getirmek amacıyla ortaya konulan bilgisayar donanımı, çeşitli yazılımlar ve kaynak paylaşımını sağlamak amacıyla, bilgisayarların birbiriyle bağ kurmasını sağlayan ve bunları kullanan insan kaynağından oluşur (Sayıştay Yayınları [SAY], 2013). Bilgi sistemleri, işletmenin bilgi teknolojileri alt yapısını oluşturan ağlarla birlikte donanım, yazılım, veri toplama işlemlerinin tamamını içerisine almaktadır (Laudon & Laudon, 2011). İşletmede bulunan bilgi teknolojilerinin etkili yönetimi ve kullanımının sağlanması amacıyla hangi kararların alınması gerektiğini, bu kararların nasıl uygulanmasını ve denetlenmesini içeren sorunlar bilgi sistemlerinin çerçevesini oluşturmaktadır (Weill & Ross, 2009).

Günümüz dünyasında işletmelerin bilgi sistemlerinden faydalanmadığı bir alan kalmamıştır. İşletmelerdeki işlemlerin çoğalıp karmaşık bir hal alması bilgi sistemlerine duyulan ihtiyacı daha da artırmıştır. Otomasyon sistemlerine geçişler, bilgisayar sistemlerinin daha önemli bir hal alması özellikle üretim işletmelerinde genel üretim giderlerinin artarak direkt işçilik giderlerinin azalmaya başlaması dijital dönüşümün göstergelerinden biri olmuştur.

Örgütsel faaliyetlerini daha verimli bir şekilde yerine getirmek isteyen organizasyonlar, ilk olarak muhasebe departmanlarında bilişim sistemlerini kullanmaya başlamışlardır. Ortaya çıkan bu süreçte gelişmiş ülkelerdeki devlet ya da özel kuruluşlarda, iş süreçlerinin büyük bir kısmı bilişim destekli bir ortamda yerine getirilmekte ve bilginin ortaya çıkmasından yok olmasına kadar olan yaşam sürecinde bilişim sistemlerinden faydalanılmaktadır (Hinnsen, 2009).

2.1. İşletmelerde Bilgi Sistemleri

20. yüzyılın sonlarında bilişim teknolojilerinde meydana gelen büyük değişimler hayatın hemen her alanında yenilenme ihtiyacı doğurmuştur. İşletmeler bilişim teknolojilerinde meydana gelen bu değişimlerden en çok etkilenen organizasyonlardan biri olmuştur. İşletmelerin iş süreçlerini yerine getirebilmek adına bilişim teknolojilerini en etkin şekilde, sürekli olarak kullanmaları gerekmektedir. Bu bağlamda bakıldığında işletmelerin kullanmış olduğu bilişim teknolojileri; internet, intranet ve extranet, üretim otomasyonları, ofis bilgisayar ve ekipmanları, elektronik veri değişim sistemleri vb. şeklinde sıralanabilir. Bilgi sistemlerinde kullanılan araçlardan bazıları açıklanacak olunursa;

- İnternet: İnternet kelime anlamına bakıldığında, İngiliz literatüründe "international electronic network" olarak adlandırılan geniş alana yayılmış bilgi ağlarını birbirine bağlayan bir araç olarak tanımlanmaktadır (Paul, 1996). İnternet ilk bulunduğu günden itibaren dramatik bir biçimde değişmiştir. Az sayıda üniversite ve kurumların kullandığı bir araçtan üç milyardan fazla kullanıcıya sahip dünya çapında bir ağa dönüşmüştür. Kendini geliştirdiği bu süreçte insanların haberleşme ve iş yapma biçimlerini değiştirmiş, bu alanda birçok fırsat ve fayda sunmuştur. Bugün internet olarak bilinen şey hızlı bir şekilde nesnelerin internetine doğru genişlemekte ve yaşantımızı etkilemektedir (Kim, 2019). Önceleri bir kişinin hayali olarak ortaya çıkan internet şu anda 3 milyardan fazla kullanıcısı olan bir alan olmuştur.

-Donanım: Girdi, işleme ve çıktı faaliyetlerini yerine getiren bilgisayar ekipmanlarından oluşur. Girdiyi oluşturan araçlar, klavye, otomatik tarama araçları, manyetik karakterleri okuma araçları ve diğer birçok araçtan oluşur.

-Yazılım: Bilgisayarın donanımlarını harekete geçiren ve bilgisayarı kendi isteklerimiz doğrultusunda işlevsel hale getirmeye yarayan programların bütünüdür (Hoşcan, 2005). Yazılımlar; bilgisayarlara verilen program ve talimatlardan oluşur. Örneğin bordro işlenmesine, müşterilere fatura gönderilmesine yarayan programlardır (Gökçen, 2007). Bilgi sistemlerine yapılan saldırı ve ihlallerin birçoğu yazılımlar aracılığıyla yapılmaktadır. Bu yüzden bilgi sistemleri risklerinin önlenmesinde yazılımların korunması önemli rol oynamaktadır.

-Veri tabanı: Öncelikle veri kavramına bakılacak olunursa; kendi başına bir anlam ifade etmeyen ya da tek başına kullanılamamasına rağmen enformasyon ve bilginin temelini oluşturan ilişkilendirilmeye, gruplandırılmaya, yorumlanmaya, anlamlandırılmaya ve analiz edilmeye ihtiyaç duyulan ham bilgidir (Yılmaz, 2009). Veri tabanı ise verilerin toplanması ve bilginin organize edilmesini sağlamaya yarayan araçtır. Veri tabanları işletmenin sahip olduğu müşteri bilgileri, faturaların saklandığı otomasyon sistemleri, stok bilgileri, diğer işletme bilgileri gibi birçok bilgiyi içerebilir (Gökçen, 2007). İşletmeyle alakalı bu denli önemli bilgilerin korunması ve denetimi önemli bir araştırma alanı olduğu bir gerçektir. Özellikle Big Data olarak adlandırılan veri tabanlarının kullanılması, korunması ve denetimi alanında birçok yeni araştırmanın yapıldığı görülmektedir.

-Intranet: İşletmelerde kullanılan iç ağ olarak da bilinen intranet için farklı tanımlamalar mevcuttur. Hinrichs (Hinrichs, 1997) tarafından yapılan açıklamalarda intranet*; "internet teknolojisi, ağ hizmetleri ve çeşitli TCP/IP protokolleri kullanan, HTML üzerinden kurulu bir iç bilgi sistemi"* olarak bilinmektedir. Intranet sayesinde kurumsal, bölümsel, grup ve kişisel iletişim bir platformda toplanmaktadır. İşletme içerisinde tüm tarafların eriştiği kullanımı ve öğrenimi kolay bilgiyi yöneten önemli bir araçtır. Internet üzerinde bilgi erişimi herkese açık iken, intranet gibi uygulamalarda paylaşılan bilgi kurum içi kullanıcılara açıktır.

2.2. İşletmelerde Bilgi Sistemleri Güvenliği

Bilgi güvenliği; işletme faaliyetlerinin sürekliliğini sağlamak üzere, işletme bilgilerinin ortaya çıkabilecek her türlü tehlike ve tehdide karşı korunmasıdır (Çubukçu, 2018). Gelişen ve değişen rekabet ortamında işletmelerin otomasyon sistemlerini daha yaygın kullanmaları, bilgisayar teknolojilerinden en üst seviyede yararlanmaları, bir takım güvenlik sorunlarını da ortaya koymaktadır. İşletmeler, giderek karmaşık bir hal alan bu yapılarında bilgi güvenliğine çok daha fazla ihtiyaç duymaktadırlar. Bilgi teknolojilerinde meydana gelen büyük değişimlere rağmen işletmeler; içerisinde insan faktörü bulunan

birimlerdir. İnsan faktörünün olduğu bir birimde yüzde yüz hatasız ve güvenlikli bir ortamdan bahsedilmesi zor bir ihtimaldir.

İşletmenin sürekliliği kavramı, işletme faaliyetlerinin sahip ya da ortaklarının yaşam sürelerine bağlı olmaksızın süresiz olduğunu belirtir (Muhasebe Sistemi Uygulama Genel Tebliği). Bağımsız denetim raporlarında; *Yönetimin ve Üst Yönetimden Sorumlu Olanların Konsolide Finansal Tablolara İlişkin Sorumlulukları* kısmında da belirtildiği gibi işletmenin sürekliliğinden sorumlu olan bir yönetim anlayışı içerisinde olunması gereği muhasebe teorisinin de temel yapı taşlarından biridir. Bu sebeple bilgi güvenliğinin sağlanarak işletme sürekliliğine risk teşkil edecek durumları önleme faaliyetleri işletme yönetimi için önem arz etmektedir.

Bilgi sistemleri güvenlik yönetimi, politikalar, standartlar, yönergeler, rehber dokumanlar ve prosedürler yardımıyla bir bilgi sistemi içinde gizlilik, bütünlük ve sürekliliğin sağlanmasını hedefler. Bu sebeple de bilgi sistemleri içerisinde yer alan varlıklar sınıflandırılır. Bu varlıklara olan tehditler ortaya konularak, bu tehditlerin oluşturduğu riskler belirlenir ve bu riskleri en aza indirecek önlemler alınır (Kara, 2018).

Üst yönetim tarafından ilgili risklere ilişkin bir takım güvenlik politikalarının oluşturulması ve bunların ilgili personellere duyurulması önem arz etmektedir. Ortaya konulan bu politikalar, alt yapı ve sistemlere veya güvenliğe ilişkin değişimler yaşandığında, bu değişimlerin takibi yapılarak uygulanan güvenlik politikalarının mevcut kontrol yapısına etkinliğini değerlendirmelidir (Dayıoğlu, 2010).

İşletmelerde etkin bir bilgi sisteminin sağlanması işletme yönetimiyle doğrudan bağlantılıdır. Yönetim tüm çalışanlarına katılımcı bir yönetim anlayışıyla bilgi güvenliliğinin önemini çeşitli araçlarla anlatmalıdır. Tam anlamıyla bilgi güvenliği en alt çalışandan en üst yönetime kadar güvenlik bilincinin oluşturulmasıyla mümkün olacaktır. İşletmede bilgi güvenliğinin sağlanmasında dikkat edilmesi gereken hususlar şunlardır (Gökçen, 2007);

- İşletmede tüm çalışanların güvenlik prosedürlerinin neden var olduğunu ve neden uyulması gerektiğinin bilincinde olması,
- Hiçbir çalışana yetkisi olmadığı halde bilgi sistemlerine giriş izni verilmemesi
- Korsan yazılım kullanılmaması
- Virüs koruma programları kullanılması,
- Bilgi sistemlerinin düzenli aralıklarla yedeklenmesi
- Güvenlik testleri yapılarak güvenlik eksikliklerinin rapor edilmesi.

3. Bilgi Sistemleri Güvenliği ile İlgili Düzenlemeler

Bilgi güvenliği yönetimi; "Bilginin bir bütün içerisinde gizliliği ve elde edilen bilginin kullanılabilirliği ile tüm bunları destekleyen süreç ve sistemlerle alakalı risklerin yönetilmesi için ihtiyaç duyulan yönetim ortamının sağlanması olarak tanımlanmaktadır (Coles & Moulton, 2003). Dünya'da bilgi sistemleri güvenliği için birtakım standartlar üzerinde çalışmalar yapılmış ve işletmelere bunların uygulanması önerilmiştir. Belirlenen bu standartlarda bilgi güvenliği yönetim sistemlerinde ilk olarak güvenlik politikasının tanımlanması ve risklerin yönetilmesi gerektiği belirtilmektedir. İşletme varlıklarına yönelik risklerin ortaya konması ve oluşan bu risklere karşı savunma mekanizmasının kurulması önem arz etmektedir (Takçı vd., 2010).

3.1. COBIT

COBIT, işletme bütününe ait kurumsal bilgi ve teknolojinin, yönetilmesi ve yönetişim esaslarının sağlanması için bir çerçevedir. Kurumsal bilgi ve teknolojiler, işletmenin belirlediği amaçlarını yerine getirmek için, organizasyonun neresinde olursa olsun devreye sokulan tüm teknolojik araçlar ve işlenen bilgi olarak adlandırılabilir (Information Systems Audit and Control Association [ISACA], 2019).

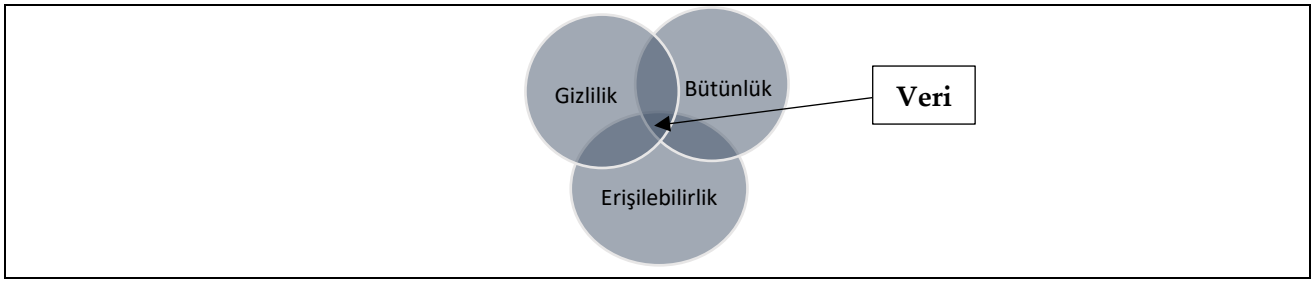
İlk sürümü 1996 yılında yayımlanan COBIT 1'in (Control Objectives for Information and Related Technology) çerçevesi denetim ile sınırlıydı. 1998 yılında ikinci defa yayımlanan COBIT 2'de kontrol kavramı ortaya çıktı. Yönetim kavramının bu çerçeve içerisine girmesi 2000 yılında yayımlanan COBIT 3 ile mümkün oldu ve bu şekilde COBIT bir bilgi teknolojileri yönetimi çerçevesi haline geldi. 2007 yılında yayımlanan COBIT 4 ve COBIT 4.1 sayesinde tamamen bilgi teknolojileri yönetişimi halini aldı. Serinin son sürümü olan COBIT 5 çerçevesinde ise "kurumsal bilgi teknolojileri yönetişimi" kavramı öne çıkarıldı (Cantürk, 2013).

3.2. ISO/IEC

Uluslararası bir standart olan ISO/IEC önsöz hariç beş bölümden meydana gelmektedir. Bunlar; kapsam, atıf yapılan standartlar veya dokümanlar, terimler ve tarifler, yönetim şartları ve teknik şartlardan oluşmaktadır (Bilgiç vd., 2013). Bilgi sistemlerinde risk yönetimi yapmaya yarayan bir çerçeveden oluşmaktadır. Örgüt içerisinde bilgi güvenliğinin yerine getirilmesi için gizlilik, bütünlük ve sürekliliğin bir arada bulunmasını sağlar. ISO/IEC bu birlikteliği sağlamak için şu adımları izler (Kara, 2018);

- Varlıkları tanımlama,
- Tehditleri tanımlama,
- Var olan önlemlerin belirlenmesi,
- Açıklıklar ve beklenen sonuçların ortaya konulması,
- Risk tahmini ve değerlendirilmesi.

ISO/IEC Standardı teknik bir standart olmayıp organizasyonların güvenlik için ihtiyaç duyduğu gereksinimleri tanımlarken gerçekleştirme yöntemlerini kurum, kuruluş ve işletmelere bırakır. İşletme iç ve dış çevresi tarafından bilginin, kötü amaçlı kullanımına karşı korunması için gerekli prosedürleri tanımlar. Bu amaçla TSE tarafından yayınlanmış olan ISO/IEC 270001 adlı yönergede bu standardın kullanım amacı; bilgi güvenliği yönetim sistemini kurmak, yerine getirmek, izlemek, gözden geçirmek, sürdürmek ve iyileştirmek için bir model ortaya konulması olarak belirlenmiştir (Ersoy, 2012). Bu modelde işletme bilgilerinin gizliliği, erişilebilirliği ve bütünlüğünün korunması amaçlanmıştır. (KPGM, 2017).



Şekil 1. ISO 27001 Bilgi Güvenliği Yönetim Sistemi
Kaynak: KPGM BT Denetim Standartları ve Uygulamaları Araştırma Raporu (2017, s. 22).

3.3. COSO İç Kontrol Modeli

COSO Komitesi 1985 yılında beş ayrı bağımsız meslek örgütü tarafından Amerika'da kurulmuştur (Türedi vd., 2014). COSO, organizasyonların iç kontrol sistemleriyle ilgilenmiş ve iç kontrolü; bir organizasyonda bulunan üst yönetim ve altında çalışanlar tarafından gerçekleştirilen faaliyetlerin, etkinlik ve verimliliğinin sağlanması, finansal raporların güvenilirliği ve ilgili kanunlara, düzenlemelere uygun olma hedefine ulaşmak amacıyla oluşturulan süreç olarak tanımlamıştır (Yılancı, 2006). COSO tarafından yayımlanan raporlarda iç kontrol sistemi beş bileşenden oluşmaktadır. Bunlar; kontrol çevresi, risk değerlendirme, kontrol faaliyetleri, bilgi ve iletişim ve izleme faaliyetleridir (Kaval, 2005).



Şekil 2. COSO Küpü
Kaynak: Sox Online.

1992 yılında ortaya konulan ilk COSO modelinin iç kontrol bütünleşik çerçevesinin üç ana başlığı ve beş bileşenine sadık kalınarak, COSO küpü; iç kontrol yapısında olması gereken nitelikler ve 17 adet yeni ilkenin eklenmesiyle 2011 yılında güncelleştirilerek yeniden yayımlanmıştır (Türedi vd., 2014). Şekil 1'de görülen COSO küpü son güncellemeleri içeren halidir. Aynı zamanda COSO, Deloitte ile birlikte 2015 yılında siber çağda COSO isimli bir rapor yayınlamıştır.

4. Siber Güvenlik

Siber güvenlik; organizasyonların ve kullanıcıların dijital ortamda sahip olduğu varlıkların korunması amacıyla ortaya konulan araçlar, politikalar, prosedürler, güvenlik teminatları ile kılavuz ve risk yönetimi faaliyetlerinin tamamı olarak adlandırılabilir (Choo, 2011). Günümüz bilgi ve iletişim çağında elektronik aygıtların, dijital ortamdaki verilerin siber saldırılara karşı korunması ve gerekli güvenlik önlemlerinin alınması olarak da tanımlanabilir. (Ertuğrul, 2020).

Hayatın hemen her alanında dijitalleşme çığır aşmışken, işletmelerin dijital dünyada kendini yenilemesi ve geliştirmesi kaçınılmaz olmuştur. Siber güvenlik tanımlarından anlaşılacağı üzere dijital dünyada işlerin kolaylaşması aynı zamanda birtakım zorlukları da beraberinde getirmektedir.

Ortaya çıkan siber güvenlik ihlallerinin sistematik ve sıradan bir hale gelmiş olması, yöneticilerin dikkatini bu yöne doğru çekmektedir. İşletmelerin bilgiye ve bilgilerin birbirine bağlılıklarına olan gereksinim arttıkça, siber risklere karşı dayanıklılık geliştirmek önemli bir hal almıştır. İşletmelerin siber güvenlik ihtiyaçlarını karşılamaları, işletme itibarı için de önemlidir. (Yıldırım, 2018).

4.1. Siber Güvenlik Riskleri

İşletmelerde meydana gelen hızlı dijital dönüşümün bir sonucu olarak, dikkat edilmesi gereken en önemli risklerden biri de siber güvenlik riskleri olmuştur. Siber güvenlik ihlallerinin işletmeler üzerindeki etkileri son derece yıkıcı olabileceğinden dolayı, siber güvenlik; günümüz işletmelerinin başa çıkması gereken en önemli sorunlardan biri olarak belirlenmektedir. Siber saldırı yapan suçluların günümüzde çok karmaşık ve özel yöntemler kullanması ve bu saldırıların yaygınlaşmasından ötürü, siber saldırılar önemli derecede finansal kayıplara, itibari zedelenmelere ve operasyonel zararlara neden olan ve yönetilmesi gereken önemli bir risk olarak karşımıza çıkmaktadır (City of Vancouver, 2016).

Her işletmenin karşılaşabileceği siber riskler farklı yoğunluk ve nitelikte olabilir. Dijital dünyanın farklı araçlarından yararlanan işletmeler için birbirinden farklı siber risk türleri karşımıza çıkmaktadır. Bu durum örnekle açıklanacak olunursa; operasyonlarının neredeyse tamamını dijital ortamda gerçekleştiren bankalar, işlemlerinin çok daha az bir kısmını dijital ortamda gerçekleştiren işletmelere nazaran farklı ve yoğun siber riskler ile karşılaşacaklardır. Siber güvenlik risklerinin yoğunluğu ve türü değişse de işletmelerin siber güvenlik risklerine karşı aynı disiplin ve bilinçle önlem almaları gerçeği değişmemektedir.

Günümüz bilişim çağında siber risklerin ardı arkası kesilmezken birçok siber saldırı çeşidi akademik çalışmaların konusu olmaktadır. Bu bağlamda işletmelerin karşılaşabileceği siber risklerin bazıları şunlardır;

Sahte Mail Göndermek: Oltalama yöntemi olarak da bilinen sahte mail gönderme yöntemi, işletmelerin karşılaştığı siber saldırılardan biridir. Bu yöntemde saldırıya uğrayan taraf, farkında olmadan işletme banka hesap parolasını, işletme e-posta parolasını veya işletmeye ait sosyal hesapların parolalarını kaybetme riskiyle karşı karşıya kalabilir. Kullanılan bu yöntemde sahte maili alan taraf bu konuda eğitilmediyse, aslında yasal bir kurumdan e-posta almış gibi hareket etmektedir. Bu yöntemde kullanım amacına göre e-posta içeriği değişmektedir. Son derece profesyonel şekilde hazırlanan e-posta içeriği sayesinde kurban, çalışılan bankadan, bir müşteriden ya da e-posta sunucusundan güvenliğine dair e-posta almış gibi bir sebeple kandırılabilir. E-posta açılıp ilgili linklere tıklandığında banka hesaplarından sorumlu personel, banka sayfası gibi hazırlanan sayfaya yönlendirilerek parola ve kişisel bilgilerinin çalınması sağlanacaktır.

Tablo 2. Siber Saldırıların Temel Yöntemleri

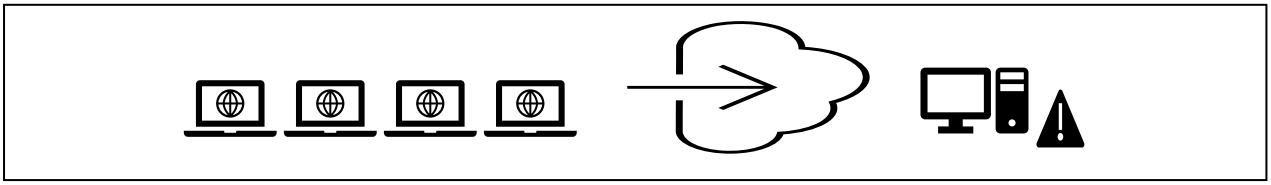
Saldırı türü	
Dos/DDoS (Denial of Service)	İşletme sunucularının normal çalışmasını kesintiye uğratmak için tasarlanmış saldırıları içerir
WEB ve Uygulamalara Yapılan Saldırılar	Web uygulamaları aracılığıyla yapılan saldırıları içerir.
Siber casusluk	Yetkisiz kişilerden yararlanma amacıyla yapılan saldırıları içerir.
Erişim Ayrıcalığının Kötüye Kullanımı	Yetkinin suiistimali veya yanlış kullanımdan kaynaklanan saldırıları veya olayları içerir
Ödeme kartını gözden geçirme	Bir cihazın, finansal veri okuma ekipmanına yerleştirilerek yapılan saldırıları içerir (ör. ATM'ler, POS terminalleri vb.).
Satış noktası Pos saldırıları	Verilere ve finansal işlemlere uzaktan erişim şeklinde yapılan saldırıları içerir.
Siber Suç	Siber casusluk dışında herhangi bir amacı olan saldırıları içerir ve başka bir kategoriye ayrılamayan tüm teknikleri içerir.
Spam Mailler	Bulunmayı önlemek için geniş bir IP adresi kümesinden küçük hacimlerde spam mail gönderen saldırıları içerir.
Kötü amaçlı yazılım	Bilgisayarlara ve bilgisayar sistemlerine zarar vermeyi veya devre dışı bırakmayı amaçlayan yazılımlarla yapılan saldırıları içerir.
Hatalar	Nedeni başka kategoriye girmeyen olayları içerir.

Kaynak: Popescu, C. R., & Popescu, G., (2018).

Dos/Ddos Saldırıları, s. Dijital çağda internet sitelerini en aktif kullanan organizasyonlardan biri de bankalardır. Ancak internet sitelerini sadece bankaların yoğun kullandığını söylemek uygun olmayacaktır. Farklı sektörlerin satış ve pazarlamada kullandığı en önemli araçlardan birisi de elektronik ticarettir. Elektronik ticaret kavramı, ABD'de bulunan Elektronik Ticaret Kaynakları Merkezi tarafından; elektronik olarak idare edilen teknik verilerle bütünleştirilmiş işletme faaliyetlerini tanımlayan bir kavram olarak tanımlanmaktadır (Tunca M. Z., 2018). Elektronik ticaret hacmi Türkiye'de 2020 yılında 226.200.000.000 TL rakamlarına çıkmıştır (eticaret.gov.tr). İşletmelerin elektronik ticaret yapmak için kullandığı araçların başında internet siteleri gelmektedir. Aynı zamanda internet siteleri kurumsal kimliğin yansıması olarak işletme hakkında bilgi veren bir araçtır.

Ticari ve kurumsal kimliğin yansıması olan internet siteleri, birçok dış etken tarafından saldırıya maruz kalmaktadır. Bu saldırılardan biri de DOS/DDOS atak olarak bilinen ve internet sitelerini çalışmaz hale getiren saldırılardır.

DOS/DDOS saldırılarında amaç, sistemi kaldırabileceği alanın üstüne çıkartarak hizmeti aksatmak veya sistemi çalışamaz hale getirmektir. Bu saldırılar birden fazla noktadan eş zamanlı olarak gerçekleştirilir. Bu saldırılar bir siber saldırı çeşidi olsa da bir hack yöntemi değildir (Ertuğrul, 2020).



Şekil 3. DDOS Saldırısı
Kaynak: Ertuğrul, İ. (2020).

Sistemin kullanılmaz hale gelmesi, işletmenin elektronik ticaretine ve kurumsal itibarına olumsuz etki yapacaktır. Bankalardan örnek verilecek olunursa; 1 saat boyunca banka internet sitesine ulaşılamaması durumu çok ciddi finansal sonuçlar doğurabilir. Covid-19 sebebiyle artan elektronik ticaret hacminde, satış operasyonlarının tamamını internet sitelerinden gerçekleştiren firmaların sistemlerine erişim sağlanamaması durumu da önemli finansal kayıplara sebep olacaktır. Bu sebeple internet sitelerinin güvenliğinin sağlanması, bilgi sistemleri güvenliği açısından son derece önemlidir.

5. Bilgi Sistemlerinin Denetimi Sürecinde Siber Güvenlik Risklerinin Önemi

Bilgi sistemlerinin işletmeler tarafından sıklıkla kullanılmaya başlanması ve yaygınlaşması sonucunda, işletme verilerinin elektronik ortamda saklanması ve işlenmesi sürecinde ortaya çıkabilecek problemlerin artan riski, bilgi sistemlerinin denetimini önemli hale getirmiştir. Bu bağlamda işletmeler belirli aralıklarla bilgi sistemleri risk değerlemesi yapmalı ve bu risklere karşı önlemler almalıdır.

Bilgi sistemleri denetimini ile finansal denetim arasında bir ilişki olmasına rağmen genel olarak birbirinden ayrılan noktaları bulunmaktadır. Bu duruma örnek verilecek olunursa; iç kontrollerin değerlendirilmesi bilgi sistemleri denetiminde ihtiyari bir durumdur, ancak finansal denetimde, denetim sürecinin iç kontrollere göre tasarlanması gerekir. Finansal denetimde denetçi, iç kontrollerin etkin bir şekilde kurulduğu işletmede, denetim testlerinin yoğunluğunu daha az seviyede tutabilecekken bilgi sistemleri denetiminde ise bilgi varlıklarına ilişkin risklerin belirlenmesi ve bu risklerin azaltılmasına ya da yok edilmesine ilişkin kontroller oluşturulmasına, yani risk yönetimine odaklanılmaktadır (Yalkın, 2011).

Denetçi, bilgi sistemleri riskleri üzerine yapacağı denetimin yürütülmesinde, çalışma alanı standartlarından ikincisine göre uygun denetim prosedürlerini ve bu prosedürler için gerekli kanıtların miktarını, testlerin kapsamını belirlemek amacıyla müşteri işletmenin iç kontrol sistemini gözden geçirmelidir. İç kontrol hedeflerine ulaşılması için müşteri işletmenin iç kontrol sistemini değerlendiren denetçinin, bilgi sistemlerinden iyi derecede anlaması beklenir. Bu durum da genel standartlar arasında yer alan mesleki eğitim ve yeterlilik standardının gereğidir (Kaya, 2012).

Finansal Tabloların Bağımsız Denetiminde Bağımsız Denetçinin Hileye İlişkin Sorumlulukları Standardında (BDS 240) "*denetçi, denetimde hukuk ve bilgi teknolojisi (BT) uzmanları gibi ihtisas gerektiren alanlarda bilgi ve beceri sahibi kişileri veya daha deneyimli ilave kişileri görevlendirerek, belirlenen hile kaynaklı "önemli yanlışlık" risklerine karşılık verebilir"* denilerek bilgi teknolojilerinin karmaşık süreçlerine uzman kişilerin görevlendirilmesi gerektiğine dikkat çekilmiştir. Bu bağlamda bilgi teknolojilerini tehdit eden doğal yapısı sebebiyle alanında uzman denetçiler tarafından siber güvenlik risklerinin değerlemesinin yapılması önem arz etmektedir.

Siber güvenlikle ile alakalı hangi denetim usullerinin finansal tablo denetimlerinde ve finansal raporlamada kullanılacağına ilişkin değerlendirme yapılırken, öncelikle denetçinin, işletmenin bilgi sistemlerini nasıl kullandığını ve bilgi sistemlerinin finansal tablolar üzerindeki etkisini anlaması gerekmektedir. Özellikle finansal tablolardaki, yetkisiz erişimden kaynaklanan bilgi sistemleri riskleri de dâhil olmak üzere, önemli yanlışlık riskleri değerlendirilirken, denetçiler şirketin bilgi teknolojisi sistemlerini ve kontrollerini anlamak zorundadırlar. Siber güvenlik denetiminde denetçinin öncelikli odak noktası, denetim verilerine en yakın olan kontrol ve sistemler, yani finansal tablolarla ilgili verileri barındıran sistemlere yöneliktir. Çünkü siber olaylar genellikle, işletmenin veri tabanı ve işletim sistemi gibi iç çevre ve ağ katmanları vasıtasıyla ortaya çıkmaktadır (Center for Audit Quality, 2019).

Sonuç

Günümüzde işletmelerin kullanmış olduğu geleneksel bilgi teknolojileri denetimi yöntemleri, siber saldırıları önlemek üzere belirli sınırlar ortaya koymayı hedeflemektedir. Ancak bilgi teknolojileri denetiminde ortaya konulan kontroller, ortaklar ve tedarikçilerle karmaşık ilişkiler ve dijitalleşen operasyonlardaki sayısız artış karşısında yetersiz kalmaktadır. İşletmelerin sahip olduğu bilginin değeri; bilginin nerede bulunduğu, bilginin kaybı ya da çalınması durumunda yaratacağı finansal etki ve muhtemel bir saldırı karşısında saldırganların bu bilgiyle ilgilenme ihtimalini göz önünde bulundurarak anlamaları gerekmektedir.

İç Denetçiler Enstitüsü (The Enstitute of Internal Auditors) tarafından yayımlanan raporda; organizasyonların karşılaştığı en önemli beş riskin ilk sırasında "siber güvenlik ve veri güvenliği" riskleri gelmektedir. Bilgi sistemlerini etkin şekilde kullanan işletmeler siber saldırılara açık bir hedeftir. Araştırmada işletmelerin karşılaşabileceği siber saldırılar anlatılmış olunup, bunlara karşı etkin bir savunma mekanizması kurulması gereği belirtilmiştir. Özellikle salgın dönemi uzaktan çalışma imkanlarının artmasıyla bilgi teknolojilerinden faydalanan işletme sayısında artış olmuştur. Bu durum aynı zamanda işletmelerin siber güvenlik kaygılarını daha da artırmıştır. Bilgi sistemleri denetimine ihtiyaç daha da belirgin hal almıştır. İlgili otoriteler tarafından yapılan araştırmalara göre COVID-19 döneminde siber saldırılar dünya genelinde %10 oranında artmıştır. Her bir veri ihlalinin ortalama maliyeti 1 milyon $ tutarını bulmuştur.

Türkiye'de açıklanan veriler ışığında son yıllarda bilişim suçlarına ilişkin 60.000 üzerinde olayın gerçekleştiği milyonlarca lira tutarında tedbir ve el koyma işlemlerinin yapıldığı ortaya konulmuştur. Siber saldırılar sonucu Türkiye'nin en büyük bankalarından birinde 4 milyon dolar kayba uğranmış olunup, banka ilgili kaybın sigorta tarafından karşılanacağını ve finansal tablolara etki etmeyeceğini bildirmiştir. 2022 yılı mart ayında ise bir bankanın mobil yatırım uygulamasından 16 milyar TL, bilgi sistemlerindeki açık sebebiyle kişisel hesaplara geçirilmiştir. Banka durumu sonradan fark ederek hesaplara bloke koymuştur. Bilgi sistemlerindeki açığı bulan şahıslar ilgili tutarı ilgili bankada tutmasalardı ne olurdu? İlgili tutarı kişisel kripto cüzdanlara aktarmış olsalardı banka bu işlemi nasıl geri alabilecekti? Böyle bir senaryoda bankanın nerdeyse 1,5 yıllık kârı buhar olabilirdi. Bilgi güvenliği zafiyeti olan işletmeler bu örnekte olduğu kadar şanslı olmayabilirler. Bu sebeple siber güvenlik risklerinin denetimine hem işletmeler hem denetim kuruluşları önemle yaklaşmalıdır. Tüm bu açıklamalar bilgi sistemleri denetiminde siber güvenlik risklerinin önemine atıf yapmaktadır. Sonuç olarak denetçi, bilgi sistemlerini etkin şekilde kullanan işletmenin denetimini planlarken, bilgi sistemleri riskini ortaya koyabilecek kanıtların ne şekilde ne kadar toplanacağına da karar vermelidir.

Aynı zamanda Popescu ve Popescu'nun (2020) belirttiği gibi mevcut denetim risk yaklaşımlarında olan; doğal risk, kontrol riski, bulgu riskinin yanında yeni bir bileşen olarak bilgi sistemleri riskinin getirilmesi kaliteli bir denetimin ortaya konulması için önem arz etmektedir. Bu sebeple denetçi mevcut denetim risk planlamasında ortaya çıkabilecek bilgi sistemleri risklerine uygun şekilde bir denetim planlayarak, toplanacak kanıtları işletme bilgi sistemleri kullanım oranına göre gözden geçirmelidir.

Sonuç olarak çalışma, literatürde bahsedilen çalışmalara benzer şekilde bilgi teknolojileri ve siber güvenlik konularına detaylı şekilde değinmiş olsa da hem işletmelere hem de denetçilere siber güvenlik risklerinin önemini hatırlatması sebebiyle farklı bir bakış açısı sunmaktadır. Bilgi teknolojilerinin yoğun kullanıldığı banka ve benzer iş alanlarında, siber güvenlik risklerinin sadece iç denetim departmanı tarafından bir risk unsuru olarak görülmesinin yeterli olmadığı bir gerçektir. Bu sebeple bilgiye ihtiyaç duyan tarafların kararlarını etkileyebilecek önemlilik düzeyinde, makul güvence sağlamak suretiyle bir görüş bildiren bağımsız dış denetçilerin, bilgi teknolojileri denetiminde siber güvenlik risklerine odaklanması zorunlu bir hal almıştır. Bağımsız denetçilerin ilgili alanda eğitimi zorunlu hale gelmiş, uluslararası sertifika programlarına katılarak ISACA gibi kurumların akredite ettiği sertifikaları almaları önem kazanmıştır. Denetimde yeni dijital yöntemlerin konuşulduğu bugünlerde, bilgi teknolojileri denetimi hakkında bilgi sahibi olmak tüm denetim departmanları için zorunlu hale gelmiştir. Geleceğin denetim mesleğinde dijital unsurların çok fazla yer bulacağı görülen bir gerçektir. Bunun sonucu olarak denetim firmaları ve işletmeler için siber güvenlik riskleri farkında olunması gereken önemli bir konudur.

Etik Kurul İzni

Bu çalışma etik kurul izni gerektiren bir çalışma grubunda yer almamaktadır.

Katkı Oranı Beyanı

Yazarlar makaleye eşit oranda katkı sağlamış olduklarını beyan eder.

Çıkar Çatışması Beyanı

Makale yazarları aralarında herhangi bir çıkar çatışması olmadığını beyan eder.

Kaynakça

Ağdeniz, Ş. (2021). Bilgi ve iletişim güvenliği denetiminde kamu iç denetçilerinin rolü ve yetkinliklerine ilişkin bir araştırma. *Alanya Akademik Bakış*, *5*(2), 525-545.

Akçakanat, Ö., Özdemir, O., & Mazak, M. (2021) İşletmelerde siber güvenlik riskleri ve bilgi teknolojileri denetimi: bankaların siber güvenlik uygulamalarının incelenmesi. *Mehmet Akif Ersoy Üniversitesi Uygulamalı Bilimler Dergisi*, *5*(2), 246-270.

Aktaş, F. Ö., & Soğukpınar, İ. (2010). Bilgi güvenliğinde uygun risk analizi ve yönetimi yönteminin seçimi için bir yaklaşım. *Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi*, *3*(1), 39-46.

Atakan, M. (2021). Siber güvenlik ve covid 19 salgınının uzaktan denetim üzerinde etkileri. *Denetişim,* (22), 27-39.

Bilgiç, E., Sadıkoğlu, E., & Turhan, S. (2013). TS EN ISO/IEC 17025 Standardı denetimlerinde teknik alanda tespit edilen genel bulgular. *Mühendis ve Makina*, 14-17.

Cantürk, S. (2013). Bilgi teknolojileri yönetişimi için yeni bir adım: COBIT 5. *KPMG Gündem Dergisi*, *17*, 36-37.

Choo, K.-K. R. (2011). The cyber threat landscape: challenges and future research directions. *Computers & security*, *30*(8), 719-731.

Coles, R. S., & Moulton, R. (2003). Operationalizing IT risk management. *Computers & security*, *22*(6), 487-493.

Çubukçu, F. (2018). *Bilgi Güvenliği Yönetim Sistemi ISO27001: 2013 Uygulama Kılavuzu*. Pusula.

Çüçen, A. K. (2003). Bilgi kuramına giriş. *Bilimname*, *2003*(2).

Dayioğlu, E. (2010). Kamu idarelerinde bilgi sistemi güvenlik risklerinin yönetimi. *Denetişim,* (4), 71-81.

Ersoy, E. V. (2012). *ISO/IEC 27001 bilgi güvenliği standardı: Tanımlar ve örnek uygulamalar*. ODTÜ Yayıncılık.

Ertaş, F. C., & Güven, P. (2008). Bilgi teknolojilerinin denetim sürecine etkileri. *Muhasebe ve Finansman Dergisi,* (37), 50-59.

Ertuğrul, I. (2020). *Ofansif ve defansif siber güvenlik*. Dikeyeksen.

Gansler, J. S., & Lucyshyn, W. (2005). Improving the security of financial management systems: What are we to do? *Journal of Accounting and Public Policy*, *24*(1), 1-9.

Gordon, L. A., Loeb, M. P., & Lucyshyn, W. (2003). Sharing information on computer systems security: An economic analysis. *Journal of Accounting and Public Policy*, *22*(6), 461-485.

Gökçen, H. (2007). *Yönetim bilgi sistemleri*. Palme Yayıncılık.

Hinnsen, P. (2009). *Business/IT fusion*. MachMedia.

Hinrichs, R. J. (1997). *Intranets: What's the bottom line?*. Prentice Hall.

Hoşcan, Y., Ortal, Ö., Hepkul, A., Kağnıcıoğlu, H., & Sevim, A. (2005). *Yönetim bilgi sistemi*. Anadolu Üniversitesi Yayınları.

İnci, A. (2016). *Bilgi sistemleri risk yönetimi ve denetimi standartlarının bankacılık sistemi üzerinde modellenmesi ve uygulanması*. Okan Üniversitesi.

Kaban, I., & Arslan, M. C. (2016). Bilgi teknolojileri destekli denetim uygulamaları kapsamında zimmet hilelerinin ortaya çıkarılması; bankacılık sektöründe bir uygulama. *Ege Akademik Bakis*, *16*(3), 415.

Kara, M. (2018). *Kurumsal bilgi güvenliği*. Papatyabilim Yayıncılık.

Kaval, H. (2005). *Muhasebe denetimi: Uluslararası finansal raporlama standartları uygulama örnekleriyle*. Gazi Kitabevi.

Kaya, İ. (2012). Bilgi işlem sistemlerinde muhasebe denetimi. *İstanbul Üniversitesi Siyasal Bilgiler Fakültesi Dergisi* (3-4-5).

Kayrak, M. (2012). Bilgi kriterleri çerçevesinde bilişim teknolojileri denetimi. *Sayıştay Dergisi,* (87), 143-167.

Kestane, Ü. A. (2021). Siber güvenliğin etkinleştirilmesinde sürekli süreç denetimi modeli. *World of Accounting Science*, *23*(4).

Kim, D., & Solomon, M. G. (2019). *Bilgi sistemleri güvenliğinin temelleri* (Çev. U. Can). Nobel Yayın.

Kurt, G., & Uçma Uysal, T. (2015). Siber riskler ve COSO iç kontrol bütünleşik çerçevesi. *Muhasebe ve Denetime Bakış,* (46), 1-10.

Laudon, K. C., & Laudon, J. P. (2011). *Yönetim bilişim sistemleri* (Çev. Ed. Prof. Dr. Uğur Yozgat). Nobel Akademik Yayıncılık.

Önce, S., & İşgüden Kılıç, B. (2012). İç denetim faaliyetinin gelişen ve değişen bilgi teknolojileri ortamı açısından değerlendirilmesi: İMKB 100 örneği. *Yönetim ve Ekonomi Araştırmaları Dergisi,* (17), 38-70.

Öztürk, M. S. (2018). Siber saldırılar, siber güvenlik denetimleri ve bütüncül bir denetim modeli önerisi. *Journal of Accounting and Taxation Studies*, 208-232.

Paul, P. (1996). Marketing on the internet. *Journal of Consumer Marketing*.

Pears, D. (2003). *Bilgi nedir?* (Çev. A. Güçlü). Bilim ve Sanat.

Popescu, C. R. G., & Popescu, G. N. (2018). Risks of cyber attacks on financial audit activity. *The Audit Financiar journal*, *16*(149), 140-147.

Selimoğlu, S., & Altunel, M. (2019). Siber güvenlik risklerinden korunmada köprü ve katalizör olarak iç denetim. *Denetişim*(19), 5-16.

Serçemeli, M., & Kurnaz, E. (2016). Denetimde bilgi teknoloji ürünleri kullanımının teknoloji kabul modeli (TKM) ile araştırılması. *İstanbul Üniversitesi İşletme Fakültesi Dergisi*, *45*(1), 43-52.

Takçı, H., Akyüz, T., Alper, U., Karabağ, R., Aktaş, F. Ö., & Soğukpinar, İ. (2010). Bilgi güvenliği yönetiminde risk değerlendirmesi için bir model. *Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi*, *3*(1), 47-52.

Tunca M. Z., & Hasköse, A. (2002). Global elektronik ticaret. *Erciyes Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, (18)*, 145-157.

Tuncer, Ö. T., Yüksel, O., Ergüden, E., & Sayar, Z. Bilgi sistemleri denetimi, vergi denetimlerinde uygulanabilecek bilgi sistemleri denetimleri ve uygulamalari-bilgi sistem denetimlerinin meslek mensuplarinin algisi üzerine bir araştirmA. *Muhasebe ve Vergi Uygulamaları Dergisi*, *7*(2), 37-62.

Tülay, Y., & Atasoy, A. (2021). Dijitalleşmenin Bağımsız Denetime Yansımalarının Siber Güvenlik Yönünden Değerlendirilmesi. *Muhasebe ve Finansman Dergisi*, 439-458.

Türedi, H., Gürbüz, F., & Alıcı, Ü. (2014). COSO modeli: iç kontrol yapisi-coso model: internal control structure. *Öneri Dergisi*, *11*(42), 141-155.

Weill, P., & Ross, J. W. (2009). *IT savvy: What top executives must know to go from pain to gain*. Harvard Business Press.

Yılancı, M. (2006). İç Denetim Türkiye'nin 500 Büyük Sanayi İşletmesi Üzerine Bir Araştırma, Ankara: Nobel Yayınları, 2. *Baskı, Eylül*, *2006*, 65.

Yildirim, E. Y. (2018). Bilişim Sistemlerine Yönelik Siber Saldırılar ve Siber Güvenliğin Sağlanması. *Mesleki Bilimler Dergisi (MBD)*, *7*(2), 24-33.

Yılmaz, M. (2009). Enformasyon ve bilgi kavramları bağlamında enformasyon yönetimi ve bilgi yönetimi. *Ankara Üniversitesi Dil ve Tarih-Coğrafya Fakültesi Dergisi*, *49*(1), 95-118.

