SİBER RİSKLER VE COSO İÇ KONTROL BÜTÜNLEŞİK ÇERÇEVESİ

Prof. Dr. Ganite KURT*
Doç. Dr. Tuğba UÇMA UYSAL**

ÖZET

Günümüzde işletmedeki risklerin yönetimi işletmenin yönetim felsefesinin bir parçası olarak tanımlanmaktadır. İşletmedeki risklerin çeşitliliği ise, bilgi ve iletişim teknolojisindeki gelişmelere bağlı olarak siber risklere kadar uzanmaktadır. İşletme içerisindeki siber riskleri değerlendirebilmek ve yönetebilmek için öncelikle iç kontrol unsurlarına siber risk açısından odaklanmak gerekmektedir. Siber risk kaçınılan bir durum değildir. Aksine yönetilebilen bir durumdur. Ayrıca siber tehdit durumunda, işletmelerde tüm verilerin korunması mümkün değildir. Bu nedenle de işletmelerin siber risklere hazırlıklı olması ve bir eylem planının işletme içerisinde hazır bulunması gerekmektedir. Bu çalışmada işletmelerin güncellenen COSO ve yeni yayınlanan raporu doğrultusunda siber risklerin tespitine ya da yönetilmesine yönelik nasıl bir iç kontrol sistemi geliştirmesi gerektiği üzerinde durulmakta ve öneriler sunulmaktadır.

Anahtar Kelimeler: Siber Risk, COSO, İç Kontrol Bütünleşik Çerçevesi

CYBER RISK AND COSO INTERNAL CONTROL INTEGRATED FRAMEWORK

ABSTRACT

Contemporarily, managing the risks in enterprises is accepted as a part of management philosophy. The diversity of risks in enterprises includes even cyber risks depending on developments in information and communication Technologies. To evaluate and manage cyber risks in enterprises, first internal control elements should be focused on cyber risks. Cyber risks are unavoidable but managable. In a cyber threat situation, it is not possible to protect all the information within enterprises. Consequently enterprises should be aware of this risk and be prepared to this threat with a plan of action. In this study it is aimed to guide enterprises about determination of cyber risks towards updated COSO and its current report and to setting up a proposal internal control system to manage risks.

Keywords: Cyber Risk, COSO, Internal Control Integrated Framework

* Gazi Üniversitesi, Bankacılık ve Sigortacılık Yüksekokulu Öğretim Üyesi, ganitekurt@gmail.com
** Muğla Sıtkı Koçman Üniversitesi, Turizm Fakültesi Öğretim Üyesi, ucmatugba@gmail.com

1. Giriş: İşletmeler Siber Risklerden Kaçınabilir Mi?

Son yıllarda bilgi teknolojilerinde yaşanan gelişmeler işletmelerin de bu gelişimlere paralel olarak hareket etmelerini gerektirmektedir. İşletme süreçleri açısından bilgi teknolojilerinin kullanımındaki artış, küresel pazar ortamı, iş süreçlerinin karmaşıklaşması, hata ve hilenin önlenmesi ya da tespit edilmesi güncellenen COSO[1] çerçevesinde de üzerinde durulan konular olmuştur. Böylece üzerinde durulması gereken konu hem güncellenen COSO çerçevesi hem de Kurumsal Risk Yönetimi Bütünleşik Çerçeveyi esas alan işletme içindeki uygulamaların siber güvenlik ile ilgili riskleri nasıl göstereceği ya da bu risklerden nasıl korunabileceğidir. Bu doğrultuda COSO, Deloitte ile birlikte Ocak 2015'de Siber Çağda COSO (COSO in the Cyber Age) isimli bir rapor yayınlanmıştır. Raporda siber risklerin işletmedeki değerlendirme süreçleri üzerinde güncellenen COSO bakış açısı sunulmaktadır. Bilgi teknolojileri kullanımının yaygınlaşması işletmelerdeki iş süreçlerinin izlenmesi ve raporlanması açısından bir taraftan kolaylık sağlamakta diğer taraftan da siber suçlara uygun ortamı hazırlamaktadır (COSO Raporu, 2015: 1-2). Çünkü siber riskler, bilgi teknolojilerindeki gelişmelere bağlı olarak siber ortam içerisinde ortaya çıkmaktadır. Türkiye Ulusal Siber Güvenlik Stratejisi 2013 – 2014 Eylem Planı içerisinde siber ortam, tüm dünyaya ve uzaya yayılmış durumda bulunan bilişim sistemlerinden ve bunları birbirine bağlayan ağlardan oluşan ortamı ifade etmektedir. Tanımlanan siber ortam içerisinde de kaçınılmaz bir durum şeklinde ortaya çıkan siber riskler ile karşılaşılmaktadır (http://www.resmigazete.gov.tr/). Bu tespiti destekler nitelikte Bilgi Güvenliği İhlali Anketi (2015 – Information Security Breaches Survey) sonuçlarına göre, büyük ve kurumsal işletmelerin % 90'ı bilgi güvenliği suçu raporlarken küçük ve orta büyüklükteki işletmelerin % 74'ü bilgi güvenliği suçu raporlamışlardır. Yine anket sonuçlarına göre, büyük işletmelerdeki suçların % 75'i çalışanlar ile ilişkilidir. Bilgi Güvenliği İhlali Anketini yürüten PWC Siber Güvenlik Direktörü de anketi yanıtlayan 10 işletmeden 9'unun işletmesinde bir siber suçu raporladığını belirterek her örgütün siber suçlar ile nasıl mücadele edeceğini bilmeye ihtiyacı olduğunu belirtmektedir (http://economia.icaew.com/). Siber suç temelinde kronik, örgüt çapında bir riski ifade etmektedir ve kamu işletmeleri açısından olduğu kadar diğer işletmeler açısından da önemli tehditler oluşturmaktadır. Son dönemde siber suçlar, Sony Pictures Entertainment gibi medya devlerinin de ararlarında bulunduğu birçok sektörü olumsuz etkileyen bir suç olarak karşımıza çıkmaktadır. Siber suçların oluşumunda etkili olan ve örgütlerin sıklıkla farkında olmadan karşılaştıkları siber saldırıların potansiyel maliyetleri işletmelerin entelektüel varlıklarının kaybedilmesi, müşteri gizliliğinin korunamaması, işletmenin fiziksel altyapısının hasar görmesi, marka değerinin kaybı, piyasa değerinin azalması vb. gibi sıralanmaktadır. Siber güvenlik konusu Amerikan Sermaye Piyasası Kurulu'nun (SEC) de öncelikli konuları arasında yer almaktadır. SEC, işletmelere örgüt seviyesinde siber risk yönetimi programına ek olarak örgütü tehdit eden siber saldırıların işaret edildiği kapsamlı bir plan geliştirilmesi gerekli-

1 COSO, İlk kez 1985 yılında Hileli Finansal Raporlama Ulusal Komisyonuna destek sağlamak amacıyla kurulmuş bir özel sektör girişimidir. Esas olarak hileli finansal raporlamaya yol açabilen ihmal edilmiş ya da dikkatten kaçan etkenler üzerinde çalışır ve halka açık şirketler, bağımsız denetçiler, Amerikan Sermaye Piyasası Kurulu (SEC) ve diğer düzenleyiciler ile eğitim kurumları için tavsiyeler geliştirir. İlk başkanının adı James C. Treadway olduğu için komisyon bu kişinin adıyla da anılmaktadır.

liğini de vurgulamaktadır. Bunu gerçekleştirmek için de COSO'nun yeni yayınladığı raporun temel alınarak güncellenen COSO çerçevesine uygun olarak bir planlama yapılması gerekmektedir. Bu planın özellikleri arasında aşağıdakilerin bulunması da büyük bir önem taşımaktadır (http://www.weil.com):

- Örgüt içerisinde siber saldırıların yönetim kurulu üyeleri de dahil bütün çalışanlar açısından nasıl belirlenebileceğini içeren bir plan hazırlanmalıdır. Plan esnek olmalıdır ve uygulama ile test edilmelidir. Üst yönetim tarafından kabul edilebilir seviyede olmalı ve işletmedeki tüm çalışanları içerisine almalıdır.
- İşletmenin yönetim kurulu üyeleri için bir siber risk eğitimi hazırlanmalıdır. İşletmenin faaliyetleri ve finansal raporlaması ile ilgili siber riskleri işaret eden düzenlemeler yapılmalıdır.
- Üst yönetim işletmenin siber güvenliğinden tam sorumlu olması durumunda, siber güvenlik önleme ya da anlama ölçümlerini gerçekleştirmeli ve değerlendirmelidir. Düzenli olarak siber güvenlik raporlarını almalı ve bu raporlar işletmenin bilgi teknolojilerine ilişkin riskleri ve siber ihlalleri içermelidir.
- İşletmelerde siber saldırılar genellikle normal bir mail şeklinde gerçekleştirildiğinden örgüt çapındaki ağı kapsayan şifrelerin koruma altına alındığı stratejiler gerçekleştirilmelidir.
- Örgüt içerisinde siber güvenlik sorumluluğunun genel kurul, yönetim kurulu ya da denetim komitesinden hangisine ait olduğunun belirlenmesi sağlanmalıdır. Paydaşların beklentilerini de göz önüne alan siber ihlallerin tanımlanması gerekmektedir.

Siber risk için yapılan açıklamalardan görülebileceği gibi siber risk kaçınılan bir durum değildir. Aksine yönetilebilen bir durumdur. Siber tehdit durumunda tüm verilerin korunması da mümkün değildir (COSO Raporu, 2015: 1-2). Bu nedenle işletmelerin siber risklere hazırlıklı olması ve yukarıda ifade edilen bir eylem planının işletme içerisinde hazır bulunması gerekmektedir. Bu çalışmada belirtilen gerekliliklerden yola çıkılarak işletmelerin güncellenen COSO ve yeni yayınlanan raporu doğrultusunda siber risklerin tespitine ya da yönetilmesine yönelik nasıl bir iç kontrol sistemi geliştirmesi gerektiği üzerinde durulmaktadır.

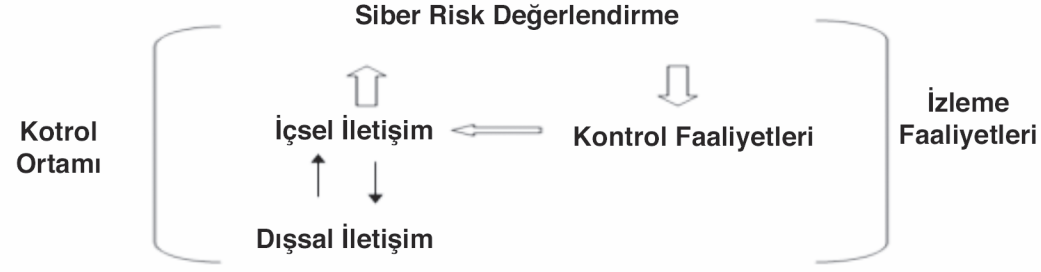
2. Siber Riskin COSO Gözüyle Değerlendirilmesi ve Yönetilmesi

Günümüzde işletmedeki risklerin yönetimi işletmenin yönetim felsefesinin bir parçası olarak tanımlanmaktadır. İşletmedeki risklerin çeşitliliği ise, bilgi ve iletişim teknolojilerindeki gelişmelere bağlı olarak siber risklere kadar uzanmaktadır. İşletme içerisindeki siber riskleri değerlendirebilmek ve yönetebilmek için öncelikle iç kontrol unsurlarına siber risk açısından odaklanmak gerekmektedir. Bunun temelinde de tüm iç kontrol bileşenleri açısından geçerli olan birtakım kritik soruların yanıtlanması gerekmektedir. Bu soruların her biri işletmenin iç kontrol sisteminin siber risklere veya siber saldırılara hazırlanmasına yardımcı olmaktadır. Örneğin (COSO Raporu, 2015:3):

- **Kontrol Ortamı:** İşletmenin yönetim kurulu örgütün siber risk profilini anlayabiliyor mu? İşletmenin yönetim kurulu siber riskin nasıl yönetebileceği konusundan haberdar mı?
- **Risk Değerlendirme:** Örgüt ve örgütün kritik paydaşları örgütün faaliyetleri, raporlaması, amaçlara uyum ve siber risklerin bu amaçlar üzerindeki etkisini anlayabiliyor mu?
- **Kontrol Faaliyetleri:** Örgüt teknoloji üzerindeki genel kontrol faaliyetlerini içeren örgüt seviyesinde kabul edilebilir siber riskleri de içeren kontrol faaliyetleri geliştirdi mi? Bu tür kontrol faaliyetleri örgüt içerisinde politika ve prosedür oluşturmaya uygun mu?

- **Bilgi ve İletişim:** Örgüt siber risk için iç kontrolü yönetebilecek bilgi gereksinimini tanımlamış mıdır? Örgüt iç kontrolün işlevini destekleyen iç ve dış iletişim kanallarını tanımlamış mıdır? Örgüt bir siber risk olayının nasıl cevap verebilir, yönetebilir ve iletebilir?
- **İzleme Faaliyetleri:** Örgüt siber riskleri işaret edecek olan iç kontrollerin etkili bir şekilde yürütülebilmesini, geliştirilmesini ve işletilebilmesini nasıl sağlayacak? Örgüt seviyesinde siber risk profilinin gözetlenmesi için ne yapılmalıdır?

Birçok örgütte bilgi sistemlerinin örgüt için önemin anlaşılması amacıyla çok fazla zaman harcanmaktadır. Bu durum bir taraftan her şeyin korunması çabalarına neden olmakta diğer taraftan da belirli bilgi sistemlerinin yetersiz korunmasına yol açmaktadır (COSO Raporu, 2015:5). Bu nedenle işletme içerisinde siber riskin iç kontrol sistemi bileşenlerine entegre edilerek değerlendirilmesi ve yönetilmesi sağlanmalıdır. Bunun için yukarıdaki iç kontrol bileşenlerine yönelik hazırlanan kritik sorunların yanıtlanması önceliklidir. Aşağıdaki şekil üzerinde belirtilen entegre sistem de sürece yardımcı siber riskin yönetilmesi ve değerlendirilmesi sürecine yardımcı olmaktadır.

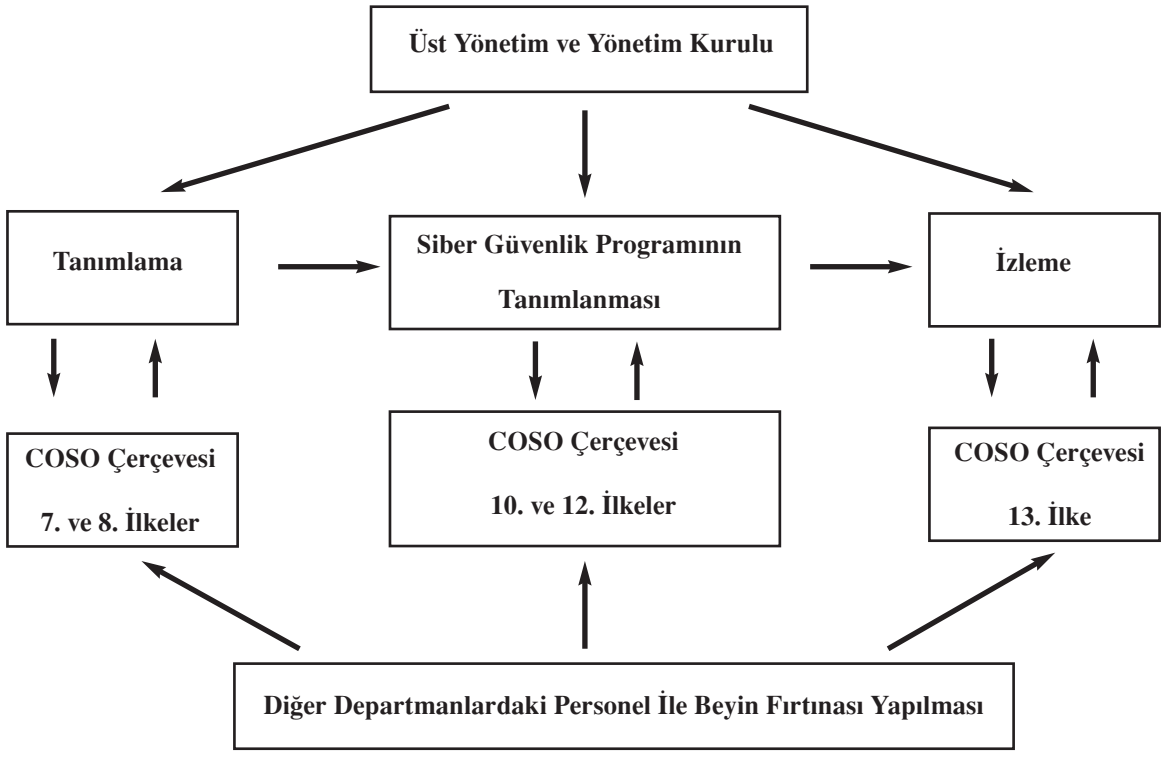


Şekil 1. Siber Riskin COSO Gözüyle Değerlendirilmesi

Kaynak: COSO Raporu, 2015: 4

Bir işletmede siber riskin COSO gözüyle değerlendirilmesi ya da yönetilmesi, yönetim kurulu ve üst yönetimin işletme amaçlarının daha iyi gerçekleştirilebilmesine imkan tanımaktadır. Yukarıdaki şekil üzerinde de görülebileceği gibi, içsel iletişim ve dışsal iletişim yolu ile sağlanan kritik bilgi sistemlerinin tanımlanması temelinde işletme içerisindeki riskin tolerans seviyesi ile ilgilidir. Bu durum örgüt içerisinde diğerlerinin de detaylı siber risk analizi uygulamasına olanak vermektedir. Sonuçta bu tür risklere işaret eden uygun kontrol faaliyetlerinin uygulamaya konması sağlanmaktadır. İç kontrol unsurlarından kontrol ortamı ve izleme faaliyetleri siber risklerin incelenmesi açısından temeldir. Örgütün güvenilir olması için, iç kontrol bileşenlerinin sunumu ve işlevi siber riskleri göz önüne alan ve onlar cevap verebilen nitelikte iç kontrol faaliyetleri esas alınarak tasarlanmalıdır (COSO Raporu, 2015:4). Çünkü COSO 2013 iç kontrol bütünleşik çerçevesi örgütün iyi tasarlanmış kontrol faaliyetlerine ilişkin ilkeleri ve noktaları üzerine odaklanmasını sağlar. Her örgüt farklı kişiler tarafından yönetilir ve iç kontrolü etkileyen beceri ve deneyimlerin şekillendirildiği mesleki yargılar tarafından yürütülür. Her ne kadar işletmede yönetimsel farklılıklar bulunsa da COSO 2013 çerçevesi her işletme açısından ortak noktalar sunmaktadır.

COSO 2015 raporuna ve denetim şirketlerinin yaptıkları araştırmalara göre, her örgüt iç ve dış kaynaklı siber risklerin çeşitleri ile karşılaşmaktadır. Siber riskler örgütün amaçlarına ulaşmasını engelleyebilecek belirsizliklerden oluşmaktadır. Siber saldırıların öncül belirleyicileri ve saldırıların arkasındaki teşvikler olarak tanımlanmaktadır. Siber saldırıların öncül belirleyicileri, çoğu zaman işletme içerisinde çoğu zaman fark edilememektedir. Bu nedenle işletme içerisindeki elektronik bilginin ve sisteminin korunabilmesi ya da sürekliliği risklerin koşullarının ve sonuçlarının yönetilmesine bağlı olarak ortaya çıkmaktadır (Caralli vd., 2010). Bu noktada da güncellenen COSO ilkeleri gerek üst yönetime gerekse de işletmenin ilişkili taraflarına detaylı açıklamalar sunmaktadır. Aşağıdaki şekil üzerinde anlatılanların sunumunu görmek mümkündür.



Şekil 2. COSO İlkelerinin İşletmedeki Siber Riskleri İzlemedeki Yeri

COSO 2013 çerçevesinde yer alan 6. ilke "Doğru ve uygun hedeflerin belirlenmesi" örgütün amaçları ile ilgili olan risklerin belirlenmesine ve tanımlanmasına yardımcı olan hedeflerin çeşitlendirilmesine olanak tanımaktadır. Bu ilke örgütün siber risk değerlendirme sürecine etki yapmakta ve amaçların nasıl gerçekleştirileceğine ilişkin yol göstermektedir. Bu noktada COSO 2015 raporunda tanımlanan kategoriler aşağıdaki gibidir (COSO Raporu, 2015:5):

- Faaliyetlere ilişkin amaçlar
- Dış finansal raporlama amaçları
- Dış finansal olmayan raporlama amaçları
- İç raporlama amaçları
- Yasalara ve düzenlemelere uygunluk amaçları

Bu kategorilere uygun olarak ve COSO çerçevesinde yer alan altıncı ilke ile bağlantılı olarak örgütün amaçları ile ilgili olan risklerin tanımlanmasını kolaylaştıran kontrol amaçlarının oluşturulması işletmede üst yönetim ve yönetim kurulunun gerçekleştireceği ilk faaliyet olarak karşımıza çıkmaktadır. Bununla birlikte yüksek seviyede siber güvenlik kontrol amaçları aşağıdakileri de içeren örgütün genel amaçları ışığında belirlenmelidir (http://www.bkd.com):

- Kabul edilebilir seviyede riskleri azaltmak, işletmenin prestijini ve markasını koruyarak tüketici beklentilerini karşılamak, gerekli düzenleyici gereklilikleri sağlamak ve finansal varlıkları korumak,
- Elektronik bilgi sürecinde işletme bilgisine erişebilirlik, bütünlük ve güvenilirlik sağlamaktır.

İfade edilen kontrol amaçları işletmenin genel amaçları ile uyumlaştırılarak yine COSO 2013 çerçevesinde siber risk yönetimi için bilgi sistemlerinin tanımlanması ve işletme varlıklarına ilişkin risk değerlendirmenin yapılması gerekmektedir. Özellikle COSO 6. İlke doğrultusunda yüksek seviyede yaklaşım ile bilgi sistemlerinin değerlemesinin yapılması gerekmektedir. Bunun için de örgüt içerisinde siber risklere ilişkin kontrollerin uygulanmasında kritik bilgi sistemlerinin tanımlaması aşağıdaki gibi yapılabilir.

Tablo 1. Kritik Bilgi Sistemlerinin Tanımlanması

Kritik Bilgi Sistemlerinin Tanımlanması	Bilgi Sistemlerinin Nerede Var olduğunun Tanımlanması	Bilgi Sistemleri ile İlgili Risklerin Anlaşılması
Aşağıdakileri kullanarak işletme amaçları üzerinde temellenen bilgi kategorilerinin tanımlanması: • Kurumsal politikalar • ISO Standartları • Düzenleyici Gereklilikler • İşletme Amaçları • Entelektüel Varlıklar • Finansal Bilgiler • Müşteri veya İşveren Bilgisi	• Bilginin nasıl toplandığı, kullanıldığı, transfer edildiği, depolandığı ve arşivlendiğinin tanımlanması • Bilgi varlıklarının kullanımını, işletmeyi ve bilgi sistemini tanımak • Hangi bilginin işletme süreçleri, sistemleri ve uygulamaları içerisinde hareket ettiğinin anlaşılması için uygun bilgi akışı oluşturmak	• Varlıkların envanterinin analizi ve kontrol risklerini tanımlayan bilgi akışının sağlanması • Siber saldırıların olası öncüllerinin değerlendirilmesi ve onların akış yöntemlerinin anlaşılması • Süreç, sistem ve uygulamaların risk profili üzerine odaklanan riskleri işaret eden kontrollerin tanımlanması

Kaynak: COSO Raporu, 2015:18

Değerlendirme sürecindeki tanımlama aşamasından sonra siber güvenlik programının belirlenmesine geçilmelidir. COSO 2013 çerçevesinde yer alan 7. ilke "Risklerin belirlenerek analiz edilmesi" ve 8. ilke "Suistimal riskine ilişkin değerlendirmelerin yapılması" ilkeleri işletme içerisinde daha derinlemesine risk değerlendirme yapılmasına imkan tanımaktadır. Bu aynı zamanda örgüt içerisinde siber risk etkilerinin değerlendirilmesine de imkan tanımaktadır. Risk değerleme sürecinin etkin olabilmesi için bireyler örgütün siber profilinin anlaşılmasına katkı yapmak zorundadırlar. Bu katılım siber saldırıların öncüllerinin belirlenmesine ya da anlaşılmasına yardımcı olmaktadır. Ayrıca örgüt içerisinde risk değerlendirme sürekli bir şekilde değişimleri yansıtabilecek şekilde güncellenmelidir. Bu durum örgütün en önemli bilgi sistemlerinin siber kontrollerinin korunmasına olanak tanır (COSO Raporu, 2015:7). Temelinde güncellenen COSO'nun 7. ve 8. ilkeleri örgütün amaçlarına ulaşmasındaki risklerin nasıl tanımlanacağını göstermektedir. Kritik ve hassas bilgi ile ilgili önemli işletme süreçlerinin nasıl yönetileceği ve analiz edileceğini gösterir. Değişik departmanlarda çalışan personel ile yapılan beyin fırtınası risk tanımlama ve analizleri açısından önemli olabilir. Aşağıda bu ilkeler ışığında işletme içerisinde yürütülebilecek olan faaliyetlere yer verilmektedir (http://www.bkd.com/articles/2015/coso-and-cybersecurity.htm):

- Kritik ve hassas bilgi ile ilgili risklerin tanımlanması ve öncelik verilmesi, bu bilgi ile ilgili işletme süreçlerinin tanımlanarak işletmenin risk haritasının çıkarılması, bilginin raporlanması ve depolanması süreçleri ile ilgili örgütün tüm paydaşlarını da içeren işlemlerin tanımlanması,
- Örgüt için kritik öneme sahip bilgi teknolojileri sistemlerinin tanımlanması,
- Kritik bilgi teknolojileri sistemlerinin değerlendirilmesi, en yüksek risk alanlarında düzenli olarak risk yönetimi kaynaklarının toplanmasıdır.

Önemli işletme süreçlerinin ve bilgi teknolojileri sistemlerinin tanımlanmasından sonra siber güvenlik risklerini izleyen, tanımlayan, öncelik veren bir program geliştirilmelidir. Ardından da izleme aşamasına geçilerek, işletme içerisinde her bir süreci gözlemlenmeli ve kontrol çatışmaları (control gap) tanımlanmalıdır. COSO bütünleşik çerçevede yer alan 10. ilke olan "Uygun kontrol faaliyetlerinin belirlenmesi ve geliştirilmesi" ve 12. ilke "Politika ve prosedürler aracılığıyla uygulanması" ile kontrol çatışmalarına uygun kontrol faaliyetlerinin nasıl geliştirileceği belirlenebilir. COSO çerçevesinde yer alan 9. ilkede ise "Kayda değer ve önemli değişikliklerin tespit edilmesi ve değerlendirilmesi" örgütün içerisinde izleme ve bilgi iletişim protokollerini içeren bir siber güvenlik programı hazırlanmasına ve izlenmesine doğrudan katkılar yapmaktadır. Başarılı siber risk güvenliği yönetim programı COSO'nun 13. ilkesi olan "İlgili bilgilerin kullanılması" ilgili zamanında sunum ve kaliteli bilginin iletilmesi için öneme sahiptir.

Sonuçta COSO gözüyle siber risklerin işletmede yönetilmesi ve değerlendirilmesi süreci sürekli faaliyeti içermektedir. Bilindiği gibi herhangi bir COSO bileşeninin etkili çalışması için kontrol ortamının çok güçlü olması gerekmektedir. Bu nedenle işletmede öncelikle kritik bilgi sistemlerini de içeren kontrol ortamının hazırlanması gerekmektedir. İşletmede kontrol ortamı içerisinde birtakım anahtar eylemlerin de bulunması gerekmektedir. Siber risklere uygun etkili kontrol ortamı ve izleme faaliyetlerini içeren anahtar eylemler aşağıdaki gibidir (COSO Raporu, 2015:17):

- Bilgi sistemlerini korumanın önemini göz önüne alan üst yönetimin bilinirliğinin olması

- Potansiyel siber riskleri azaltmaya yönelik olan etkili kontrollerin tasarlanmasını ve uygulanmasını sürekliliği olan bir program oluşturmak,
- Kalifiye risk uzmanlarından yardım alma ve onları sürece dahil etmek,
- Dış kaynaklı hizmet sağlayıcılar ile ilgili siber risk ve kontrollere uygun izleme faaliyetleri yerine getirmek,
- Siber zayıflıkların düzenli ve zamanında izlenmesini sağlamak,
- Bilgi sistemlerini korumaya yardımcı olan kontrol faaliyetleri uzmanlarının hesap verebilirliğini sağlamaktır.

Her bir anahtar eylem işletme içerisindeki siber risk değerlendirme ve yönetme sürecine doğrudan etki yapmaktadır. Ancak siber çağda COSO iç kontrol bütünleşik çerçevesinin rehberliğini açıklayan yeni raporda da belirtildiği gibi kurumsallık olmadan siber riskleri yönetmek mümkün değildir. Bunun için de temel olan işletmedeki kurumsal yönetim anlayışının bu sürecin sürekliliği ve başarısı üzerindeki etkisini anlayan üst yönetimin de tam desteğini alan bir çalışmanın yürütülmesidir.

3. Sonuç ve Tartışma

Bilgi güvenliği ya da bilgi güvenliği ihlalleri birçok ülkede olduğu gibi ülkemizde de ulusal güvenlik stratejisi içerisinde öncelikli konuların başında gelmektedir. Bu öncelikli konu modern finansal sistem içerisinde elektronik finansal bilgi açısından değerlendirildiğinde ise, işletmenin ilişkili tarafları ya da bilgi kullanıcıları açısından siber güvenliğin önemi daha da iyi anlaşılmaktadır. Siber suç ve risk üzerinde denetim şirketlerinin de her yıl yayınladıkları anket sonuçları birçok işletmenin siber suçlar karşılaştığını ve raporladığını göstermektedir. Bu gereklilik doğrultusunda Ocak 2015'de COSO, güncellenen iç kontrol çerçevesi ve COSO Kurumsal Risk Yönetimi Bütünleşik Çerçevesinin (2004) nasıl siber risklerin yönetimine rehberlik edeceğini açıklayan bir rehber yayınlamıştır. Bu araştırma raporunda COSO 2013'ün örgütün siber risk yönetimine nasıl yardımcı olacağını açıklamaktadır. Raporda COSO gözüyle işletmedeki siber riskleri yönetebilmek ya da değerlendirebilmek için, işletmedeki kurumsal yönetim anlayışına ve iç kontrol bileşenlerine önemli vurgular yapılmaktadır. İşletme içerisinde üst yönetim ve tüm çalışanların birlikte koordineli olarak hareket ettikleri bir siber risk değerlendirme programının varlığına işaret edilmekte ve programın işlerliği açısından iç kontrol bileşenlerinden kontrol faaliyetleri ve kontrol ortamına sıklıkla vurgu yapılmaktadır. İşletmelerin siber risklere hazır olup olamayacağı noktasında belirleyici olan ise, işletmelerin siber risklere tam anlamıyla hazır olamayacağı hatta bu tür risklerden kaçınmanın imkansız olduğu ancak yönetebilmek adına ya da siber saldırıların öncüllerini belirleyebilmek adına etkin bir eylem planına ihtiyaç duyduklarıdır. İşletme içerisinde siber risklere uygun kontrollerin tasarlanması ve uygulanması sağlanabilirse işletmedeki siber risklerin etkilerini minimize etmek mümkün olabilmektedir. Bununla birlikte modern finansal sistem içerisinde işletmelere yol gösterici olan güncellenen COSO dışındaki siber odaklı standartlar ve çerçeveler işletmelerin siber riskleri yönetebilmesine yardımcı olmaktadır.

KAYNAKÇA

Caralli, Richard A.; Allen, Julia H.; Curtis, Pamela D.; White, David W.; & Young, Lisa R. 2010. CERT® Resilience Management Model, Software Engineering Institute, Carnegie Mellon University, http://www.sei.cmu.edu/library/abstracts/reports/10tr012.cfm

Information Security Breaches Survey. 2015. https://www.gov.uk/information_security_breaches_survey_2015-full-report.pdf

COSO. 2015. COSO in the Cyber Age, http://www.coso.org Erişim Tarihi: 1 Mayıs 2015

COSO. 2013. Internal Control – Integrated Framework, Executive Summary, http://www.coso.org/documents/990025P_Executive_Summary_final_may20_e.pdf

COSO. 2006. Internal Control over Financial Reporting — Guidance for Smaller Public Companies, http://www.coso.org/documents/SB_Executive_Summary.pdf

IFAC. 2011. Global Survey on Risk Management and Internal Control: Results, Analysis and Proposed Next Steps, Published by the Professional Accountants in Business Committee, February, USA.

Kurt, Ganite ve Tuğba Uçma Uysal. 2015. KOBİ'ler İçin Risk Temelli İç Kontrol Modeli, İçinde: Bütünleşik Yaklaşımla KOBİ'lerde Risk Temelli İç kontrol, Editörler: Ganite Kurt ve Tuğba Uçma Uysal, Gazi Kitabevi, Ankara.

Kurt, Ganite ve Tuğba Uçma Uysal. 2013. Coso İç Kontrol-Bütünleşik Çerçeve Güncelleme Projesinin Yenilikleri, *World of Accounting Science*, Vol. 15 Issue 2, p99-109.

http://www.bkd.com/articles/2015/coso-and-cybersecurity.htm Erişim Tarihi: 20 Mayıs 2015

http://economia.icaew.com/news/june-2015/cost-of-cyber-security-breaches-more-than-doubles Erişim Tarihi: 20 Mayıs 2015

http://www.resmigazete.gov.tr/eskiler/2013/06/20130620-1-1.pdf Erişim Tarihi: 20 Mayıs 2015

http://www.weil.com/~/media/files/pdfs/pcag_sec_discl_alert_jan_2015.pdf Erişim Tarihi: 20 Mayıs 2015