TONE at the TOP®

Üst yönetim, yönetim kurulları ve denetim komitelerine yönetişim ile ilgili konularda özet bilgiler.

Sayı 113 | Ekim 2022

Siber Tehditlerin Hafifletilmesi

Siber güvenlik, modern risk ortamında kalıcı bir öğe haline gelmiştir ve yönetim kurulları, çok yönlü ve sürekli gelişen tehditlere uygun gözetim sağlamaya yönelik artan bir baskıyla karşı karşıyadır. NACD Yönetim Kurulu Anketinde yönetim kurulu yöneticilerinin toplam %70'i siber güvenliği "stratejik, kurumsal risk" olarak nitelendirmiştir.[1] Siber güvenlik şemsiyesi altında çok çeşitli sorunlar yer almaktadır — birkaçını saymak gerekirse mahremiyetin korunması; fidye yazılımı, kötü amaçlı yazılım ve hizmet dışı bırakma veya oltalama saldırıları; yetersiz siber güvenlik politikaları ve olay müdahale ve kurtarma planları da dâhil olmak üzere tümü kritik konulardır.

Kurumlar da tecrübe etmiş oldukları ihlâlleri rapor etmelerini gerektiren yeni düzenlemelerle karşı karşıyadırlar. Örneğin, Kritik Altyapı Yasası için Siber Olay Raporlaması (The Cyber Incident Reporting for Critical Infrastructure Act)[2], Federal Siber Güvenlik ve Altyapı Güvenliği Ajansının siber saldırılar esnasında kurbanlara yardımcı olmasına, trendleri tanımlamasına ve diğer potansiyel kurbanlarla bilgi paylaşmasına olanak tanıyabilecek raporlama gerektirmektedir. Ayrıca, Menkul Kıymetler ve Borsa Komisyonu kamu sektörü siber güvenlik risk yönetimi, strateji, yönetişim ve olay raporlaması ile ilgili açıklamaları standardize edebilecek düzenlemeler[3] teklif etmiştir.

Kurumlara bağımsız, tarafsız güvence ve tavsiye sağlayan iç denetim siber risklerin ele alınmasında yönetim kurulları için güçlü bir kaynak olabilir. Bir PwC raporuna[4] göre "birçok şirket dayanıklılık ve müdahale de dâhil olmak üzere siber süreçleri ve kontrolleri gözden geçirmek için iç denetimden faydalanmaktadır."

Geliştirilmiş Güvenliğe Giden Adımlar

Yönetim kurulları karşı karşıya kaldıkları siber güvenlik tehditlerini göz önünde bulundurduklarından dolayı, iç denetimin fark yaratabileceği çok sayıda alan bulunmaktadır.

Riskin fark edilmesi. Siber tehditler şirketlerin risk derecelendirmelerinde en üstlere taşınmıştır.İç Denetçiler Enstitüsünün (IIA) hazırladığı On Risk 2022[5] yayınına göre, "Siber saldırıların karmaşıklık derecesinin ve çeşitliliğinin giderek artması kurumların markalarına ve itibarlarına zarar vermeye devam etmektedir ve genellikle feci finansal etkilerle sonuçlanmaktadır." Yönetim kurulu üyeleri, tepe pozisyondaki yöneticiler ve iç denetim yöneticileri (İDY'ler) ile yapılan görüşmelere dayanan bu rapor bu yıl siber güvenliği en önemli risk olarak tanımlamıştır.

Ne yazık ki bazı şirket liderleri bu tehditleri her yönüyle fark edemeyebilir. Risk Hakkında raporunda, İDY'lerin, yönetim kurulu üyelerinin ve icracı yönetimin siber güvenliğe atadığı risk ilgisi arasındaki fark özellikle endişe vericiydi. İDY'lerin %97'si siber güvenliği kurumları için yüksek düzeyde ilgili bir risk olarak derecelendirmiştir (7 puanlık bir ölçekte 6 veya 7 olarak derecelendirmişlerdir); öte yandan, yönetim kurulu üyelerinin sadece %87'si ve tepe pozisyondaki yöneticilerin sadece %77'si böyle bir derecelendirme yapmıştır.

İDY'ler arasındaki güçlü ilgi derecelendirmesi, siber güvenlik sorunlarına ilişkin farkındalıklarının yüksek seviyede olduğunu akla getirmektedir. İç denetimin bir kuruma ilişkin bütüncül bilgisi göz önünde bulundurulduğunda bu durum şaşırtıcı değildir. Yönetim kurulları risk güvencesinden finansal ve uyum risklerinin ötesinde faydalanmak ve onu geliştirmek istediklerinden dolayı, siber güvenlik endişelerinin tarif edilmesine ve onların potansiyel etkisinin ölçülmesine yardımcı olması için iç denetime güvenebilirler. Bu durum, risk kapsamındaki başarısızlıkların vurgulanmasını, yeni ortaya çıkan risklerin izlenmesini ve siber güvenlik çaba ve çalışmalarında teknoloji araçlarından en iyi şekilde faydalanmayı içerebilir.

Üçlü Hat Modelinin değerinden faydalanılması. IIA'nın Üçlü Hat Modeli[6] kurumların hedeflerine ulaşmasına en iyi şekilde yardım edecek ve siber güvenliğe ilişkin olanlar da dâhil olmak üzere güçlü yönetişimi ve risk yönetimini kolaylaştıracak yapıları ve süreçleri tanımlamasını sağlamaktadır. Üçlü Hat Modeli aşağıdakiler tarafından oynanan temel roller tanımlamaktadır:

IIA Hakkında

The Institute of Internal Auditors, Inc. (IIA), 170'den fazla ülke ve bölgede 218.000'i aşkın üyesi bulunan küresel bir meslek örgütüdür. IIA, iç denetim mesleğinin baş savunucusu, uluslararası standart koyucusu ve baş araştırmacısı ve eğitmeni olarak hizmet verir.

IIA

1035 Greenwood Blvd.
Suit e 401
Lake Mary, FL 32746 ABD

Ücretsiz Abonelik

Ücretsiz abonelik kaydınızı yapmak için theiia.org/Tone adresini ziyaret ediniz.

Okuyucu Geri Bildirimi

Sorularınızı/yorumlarınızı Tone@theiia.org adresine gönderiniz.

» Kurumsal gözetim için paydaşlara karşı sorumlu ve hesap verebilir olan yönetişim organı.

» Kurumsal hedeflere ulaşmak için faaliyet gösteren yönetim.

» Bu hedeflere ulaşma konusunda bağımsız ve objektif güvence sağlayan iç denetim.

Araştırma, üç hat arasındaki iş birliğinin siber güvenlik risk yönetiminin etkinliği üzerinde olumlu bir etkisi olduğunu göstermiştir. *ISACA Journal*[7] yayınındaki bir makaleye göre, iç denetim değerli güvenceler sağlayabilir ve tehditler ile zafiyetleri tanımlayabilir. Bu, bir ilk siber risk değerlendirmesi yapmak ve etkili denetim kriterlerini tanımlamak suretiyle siber güvenlik trendlerinin ve paydaş beklentilerinin belirlenmesini içerebilir. Makalede, bulguları hakkındaki raporlama ve tavsiye verme faaliyetlerinde "denetçiler [yönetim kuruluna] gözetim görevini ifa ederken önemli ölçüde yardımcı olabilir," denmiştir.

İç denetimin sağladığı girdinin en yararlı hale getirilmesinin sağlanması. Birçok kurumda, denetim komiteleri siber tehditler de dâhil olmak üzere tüm risk tiplerini ele almaktan sorumludur.[8] Bununla birlikte, bazıları çeşitli nedenlerle siber konulara ilişkin endişeleri diğer komitelere devretmektedir. Kurumun büyüklüğü ile faaliyet gösterdiği endüstriye ve karşı karşıya kaldığı tehditlere bağlı olarak, siber sorunları gözetmekle görevlendirilen komite ayrı bir siber güvenlik komitesi, bir risk komitesi, bir teknoloji komitesi, aday göstermek ve yönetişim komitesi veya bir başka komite olabilir. Yönetim kurulları, diğer nedenlerin yanı sıra, denetim komitesinin zaten çok meşgul olduğunu ya da siber endişelerin gözetimi için gerekli uzmanlığa sahip olmadığını kararlaştırabilir.

İç denetim genellikle denetim komitesine rapor vermektedir ancak iç denetimin aynı zamanda siber güvenlikten sorumlu herhangi bir ayrı komiteye rapor sunmaması durumunda kurum değerli siber risk tavsiyelerini ve güvencesini gözden kaçırabilir. Siber sorunları denetleyen bir komiteyle bu ilişkiye sahip olmak, iç denetimin içgörülerinin anlaşılmasını ve etkili şekilde hareket edilmesini sağlamaktadır.

Gizli tehditlerin tanımlanması. Yönetim kurulları, siber güvenlik çaba ve çalışmalarına zarar verebilecek ve potansiyel olarak felakete sebep olabilecek görünüşte küçük kusurların sayısına şaşırabilirler. İç denetim, yönetim kurullarının kurumlarının denetim planının gözden kaçan tehditleri ne kadar iyi tanımlayabildiğini ve yeni ortaya çıkan riskleri ne kadar iyi fark edebildiğini belirlemesine yardımcı olacak içgörüler sunabilir. Deloitte tarafından yayınlanan bir rapora[9] göre, yönetimin normalde hafife aldığı siber tehditlerin bazıları aşağıda açıklananları içermektedir:

» Hâlâ sistemde oturum açabilen eski personelin sayısı ve çeşitliliği ve kurumsal sistemlere erişimi olan üçüncü taraf tedarikçilerin sayısı. Her iki durumda da şirketlerin ne kadar kimliği belirsiz ve yetkisiz dış kullanıcının giriş yetkisi elde edebileceğine ilişkin fikri çok az olabilir.

YÖNETİM KURULU ÜYELERİNE SORULAR

» Siber güvenlikle ilgili stratejik planlama sürecimizde iç denetim içgörüsü ve tavsiyesinden en iyi şekilde faydalanıyor muyuz?

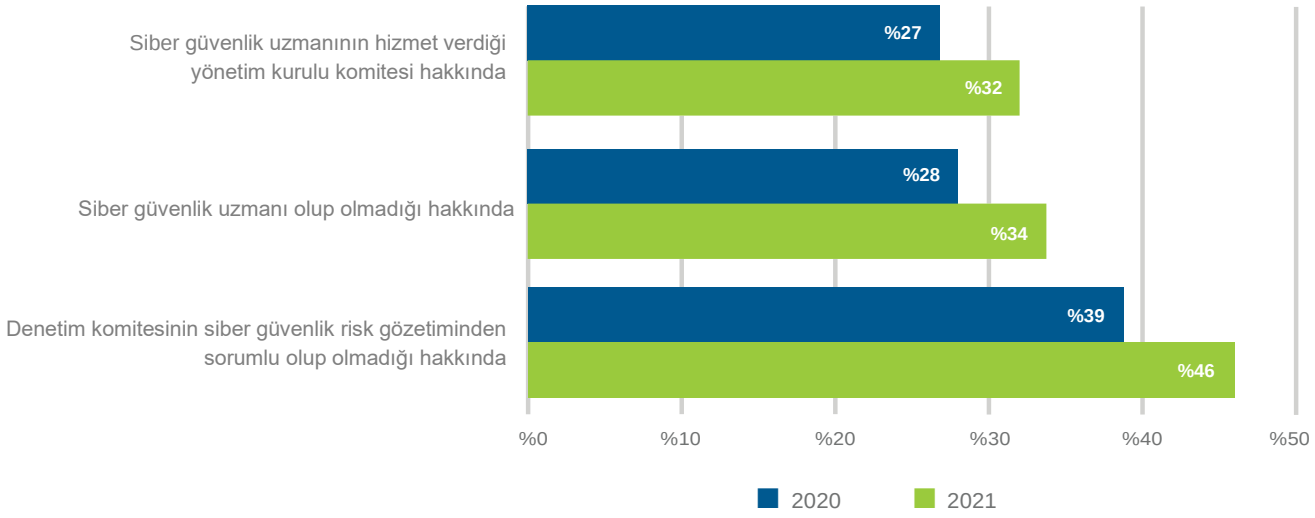
» Siber güvenlik çaba ve çalışmaları için yeterli kadro ve fonu sağladık mı?

» Kurum finansal açıdan siber güvenlik söz konusu olduğunda risk toleransını tanımladı mı?

» Siber güvenliğin gözetimi konusunda özel bir komite görevlendirildi mi?

» Yönetim kurulu üyeleri bir siber ihlâl durumunda şirketin prosedürlerini anlar ve ihlâlin gerçekleşmesi halinde rollerini bilir mi?

Aşağıdaki konularda açıklama yapan S&P 500 Şirketleri



Kaynak: 2021 Denetim Komitesi Şeffaflık Barometresi (2021 Audit Committee Transparency Barometer), Denetim Kalitesi Merkezi, Kasım 2021.

» Şirketin kullandığı bulut hesaplarının sayısı. Bulutta daha fazla etkileşim, siber saldırılar için daha fazla açıklık bırakabilir. Deloitte raporu, kurumların bulut sağlayıcılarına, mevzuata uygunluğun ve bağımsız kontrol değerlendirmelerinin yanı sıra altyapının dayanıklılığı, hizmet kesinti süresi, performans ve diğer ölçütler hakkında soru sormasını önermektedir.

» Kurumun tecrübe ettiği fiili siber ihlâllerin toplam sayısı. Zannedilenin aksine, şirketin çok az sayıda siber saldırı tecrübe etmesi olayların tespit edilmediğine ilişkin bir uyarı işareti olabilir. İç denetim ekibi bu tip uyarı işaretlerinin izlenmesini sağlamaya yardımcı olabilir.

İş ortağı ilişkilerindeki endişelerin ele alınması. Gartner[10], 2025 yılına kadar kurumların %60'ının üçüncü taraf işlemlerinde ve iş sözleşmelerinde siber güvenlik riskini dikkate alacaklarını öngörmektedir. Günümüzde, güvenlik ve risk yönetimi liderlerinin sadece %23'ü üçüncü taraf siber güvenlik maruziyetini gerçek zamanlı olarak izlemektedir ve tarama faaliyetlerini bütün tedarik zincirinden ziyade acil tedarikçilerle sınırlayabilirler.

Risk Hakkında 2022 yayınına göre, denetim liderleri, tepe pozisyondaki yöneticiler ve yönetim kurulu üyeleri bir kez daha aynı görüşleri paylaşmamaktadır. İDY'ler bu alanda kurumsal yeteneği %37 olarak derecelendirirken yöneticiler %53 ve yönetim kurulu üyeleri %57 olduğuna inanmaktadır. İDY'lerin bu alanda güveninin daha düşük olması, kısmen, bu riske atadıkları daha yüksek ilgi derecesinden kaynaklanıyor olabilir ki bu derece yönetim kurulu üyelerinden 17 puan daha yüksektir (%60'a kıyasla %77).

Her halükârda, yönetim kurullarının iç denetimin bu alandaki girdisinin ve deneyimlerinin tam değerini anladıklarından emin olmaları gereklidir. İç denetim kurum genelindeki ekiplerle birlikte çalıştığından dolayı, belirli bir tedarikçiyle ilgili olarak veya bütün tedarik zinciri genelinde ilişkilendirilen veya tanımlanan siber riskler konusunda yönetim kurullarını uyarabilir. Kurumun iş ortakları siber güvenlik tedbirleri hakkında güvence istediklerinde iç denetim talep ettikleri bu tür verileri ve güvenceyi sağlayabilir.

Kaynakların En Yararlı Hale Getirilmesi

Kurumlar göz korkutan siber güvenlik endişeleriyle boğuştukları için var olan tüm kaynaklarını en yararlı hale getirmeleri gerekecektir. Yönetim kurulları, iç denetçilerin verimlilik ve etkinliği artırmaya yönelik fırsatları tanımlayarak kurum genelinde katabildikleri değeri anlayarak ve ondan faydalanarak şirketlerinin güvenliğini iyileştirebilirler.

Hızlı Anket Sorusu

Kurumunuz için siber güvenlik risk yönetimi gözetiminden hangi yönetim kurulu komitesi sorumludur?

- ◯ Denetim komitesi
- ◯ Siber güvenlik komitesi
- ◯ Teknoloji komitesi
- ◯ Aday gösterme ve yönetişim komitesi
- ◯ Diğer

Cevaplamak ve diğer cevapları da görmek için theiia.org/Tone sayfasını ziyaret ediniz.

Son notlar

1 Siber Riske Yönelik Yönetim Kurulu Yönetişiminin Prensipleri (Principles for Board Governance of Cyber Risk), Ulusal Kurumsal Yöneticiler Birliği, İnternet Güvenliği Birliği ve Dünya Ekonomik Forumu, PwC'nin katkılarıyla, Mart 2021.

2 https://www.cisa.gov/circia

3 https://www.sec.gov/rules/proposed/2022/33 -17038.pdf

4 Siber Risk Gözetimi: Yönetim Kurulunun Rolü (Overseeing Cyber Risk: The Board's Role), PwC, Ocak 2022.

5 Risk Hakkında 2022: Riski Anlama, Hizalandırma ve Eniyileme Rehberi (OnRisk 2022: A Guide to Understanding, Aligning, and Optimizing Risk), The Institute of Internal Auditors, 2021.

6 IIA'nın Üçlü Hat Modeli: Üçlü Savunma Hattı Güncellemesi (The IIA's Three Lines Model: An Update of the Three Lines of Defense), İç Denetçiler Enstitüsü, Temmuz 2020.

7 " Siber Güvenlik Denetiminiz Ne Kadar Etkili? (How Effective Is Your Cybersecurity Audit?)" Matej Drascek, ve ark., ISACA Journal, 7 Haziran 2022.

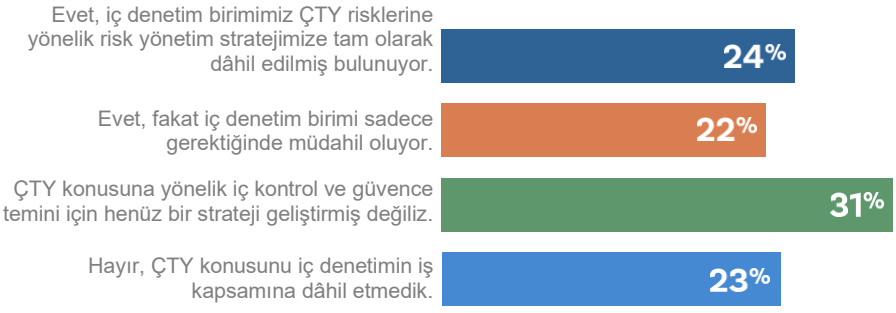
8 "Siber Güvenlik: Gelişmekte Olan Bir Yönetişim Sorunu (Cybersecurity: An Evolving Governance Challenge)," Harvard Law School Forum on Corporate Governance, Phyllis Sumner, ve ark., 15 Mart 2020.

9 İç Denetim: 2022 için Riskler ve Fırsatlar (Internal Audit: Risks and Opportunities for 2022), Deloitte, 2021.

10 2022 Öngörüleri: Siber Güvenlik Liderleri Dağıtılmış Ekosistemde Kontrolü Kaybediyor (Predicts 2022: Cybersecurity Leaders Are Losing Control in a Distributed Ecosystem), Sam Olyaei, ve ark., Gartner, 24 Ocak 2022.

HIZLI ANKET SONUÇLARI

Kurumunuz ÇTY konusunda güvence temin etmek için iç denetimden faydalanıyor mu?



Kaynak: Tane at *the Top* Haziran 2022 Anketi.

2022-4015