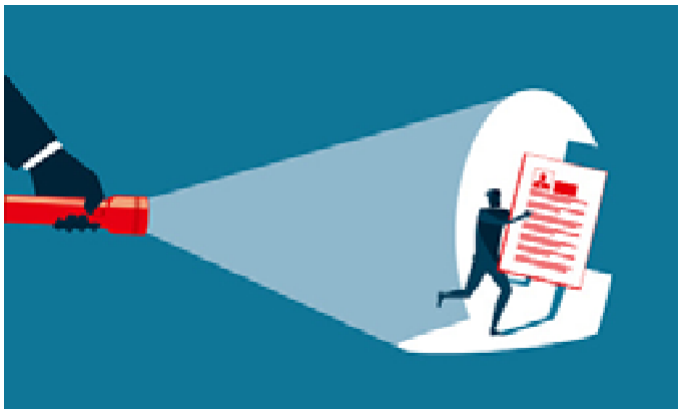
TONE at the TOP®

*Üst yönetime, yönetim kurullarına ve denetim komitelerine yönetişimle ilgili konular hakkında kısa ve öz bilgiler sunar.*

**106. Sayı | Ağustos 2021**

# Siber Güvenlik Canavarıyla Yüzleşmek



**Siber Güvenlik riski** her büyüklükte ve her sektörden kurumu etkilemektedir ve bizimle olmaya devam edecek gibi görünmektedir. Dünya çapındaki yönetim kurulları ve üst düzey yöneticilerle yapılan bir anket, 2021 yılında siber tehditleri ilk ondaki riskler arasında göstermiştir ve ayrıca anket katılımcıları bu risklerin 2030 yılında en önemli riskler arasında yer almasını da beklemektedir. Gerçekten de küresel siber suçların her yıl %15 oranında bir sıçrama yapması beklenmektedir ve Cybersecurity Ventures şirketine göre, bunların yıllık etkisinin 2025 yılına kadar 10,5 trilyon doları bulacağı tahmin edilmektedir. Bu siber araştırma şirketi buna "tarihteki en büyük mali servet aktarımı" adını vermektedir.

Siber güvenlik olayları fidye yazılımlar, uzaktan çalışma kaynaklarına yönelik saldırılar, tedarik zincirlerine yönelik saldırılar, oltalama veya suç arz eden diğer eylemler olarak karşımıza çıkabilir. Bunlar bir şirketin faaliyetlerini aksatabilir, önemli bir işletme değerini yok edebilir ve işletmeyi itibar zedeleyici bir sorumlulukla veya propagandayla karşı karşıya bırakabilir. IBM verilerini baz alırsak, veri ihlallerinin maliyeti yüksektir ve artmaya da devam etmektedir ve bu maliyet 2021 yılında ortalama 4,24 milyon dolara ulaşmış olup, bir yılda neredeyse %10 artmıştır.

Dahası, Covid-19 salgını da henüz tam manasıyla anlaşılamamış veya çözüme kavuşturulamamış yeni zafiyetler ortaya çıkarmıştır.

## Tehlikeleri Yönetmek

**Bu kadar çok şey tehlikede olmakla birlikte**, siber risklere ilişkin denetim ve gözetimi artırmak için yönetim kurullarının atabilecekleri birtakım adımlar vardır. Bu süreç boyunca iç denetim kritik bir ortak işlevi görebilir. İç denetim ekibi, kurumun siber güvenlik uzmanlarıyla iş birliği yaparak kurumun planlarının amaçlandığı gibi uygulandığına ve ilgili görev için uygun ve yeterli olduğuna dair objektif bir teyit sunabilir. Deloitte Risk ve Mali Danışmanlık emekli kıdemli ortağı ve CIA unvanına sahip Sandy Pundmann, "İç denetim, yönetim kuruluna, büyük çapta bir risk maruziyetinin mi yoksa yanlış bir güvenlik algısının mı söz konusu olduğunu söyleyebilir" diyor.

Yönetim kurullarının siber riski ele almalarına yardımcı olacak çeşitli stratejiler vardır. Pundmann ve diğerleri, kurumlarının güçlü yanlarını, zayıf yanlarını ve zafiyetlerini açık ve net şekilde anladıklarından emin olmak amacıyla, yönetim kurullarının kurumlarının siber risk profilini net şekilde anlamalarını, denetim ve gözetim görevlerine sahip çıkmalarını ve sağlıklı bir şüpheciliği uygulamaya koymalarını tavsiye etmekledir.

**Denetim ve gözetim rollerini belirleyin ve düzenli güncellemeleri bir programa oturtun.** Gartner, Inc. şirketinin bir anketine göre, bugün yönetim kurullarının %10'undan daha azında uzman bir yönetim kurulu üyesinin başkanlık ettiği özel bir siber güvenlik komitesi varken, bu sayının 2025 yılına kadar %40'a ulaşması beklenmektedir. Salgın döneminde dijital işletmenin kapsamının genişlemesi ve uzaktan çalışmanın ve onun beraberinde getirdiği ilave potansiyel risklerin kabul edilip benimsenmesi bu beklenen artışta itici bir güç olabilir.

## IIA Hakkında

The Institute of Internal Auditors, Inc. (IIA), 170'ten fazla ülke ve bölgede 200.000'i aşkın üyesi bulunan küresel bir meslek örgütüdür. IIA, iç denetim mesleğinin baş savunucusu, uluslararası standart koyucusu ve baş araştırmacısı ve eğitmeni olarak hizmet vermektedir.

## The IIA

1035 Greenwood Blvd.
Suite 149
Lake Mary, FL 32746, ABD

## Ücretsiz Abonelik

Ücretsiz abonelik için, www.theiia.org/Tone adresini ziyaret ediniz.

## Okuyucu Geri Bildirimi

Sorularınızı/yorumlarınızı Tone@theiia.org e-posta adresine gönderiniz.

Günümüzde, siber güvenlik denetim ve gözetim sorumluluğunun kime ait olduğunu kesin olarak belirlemek zor olabilir, çünkü bu sorumluluk çoğunlukla yönetim ve çeşitli komiteler arasında dağıtılmıştır, demektedir Pundmann. Bu sorumluluk bir komiteye verilmeli ve söz konusu komite bu konuyu her toplantıda ele almalıdır, diye de sürdürüyor sözlerini. Siber güvenlik, ayrıca, en az yılda iki kez yönetim kurulunun tamamının gündeminde yer almalıdır.

**Tehdit seviyesini bilin.** Siber güvenlik salt bir BT meselesinden çok daha fazlasıdır. McKinsey'in bir prodcast programında, Birleşik Krallık'ın Ulusal Siber Güvenlik Merkezi'nin eski müdürü John Noble, "İster bir olayın öncesinde olsun isterse olay esnasında olsun, [siber güvenliği] sadece bilgi teknolojilerinden sorumlu genel müdür yardımcısına ve teknik ekibe bırakmamalısınız" demiştir. "Kullanılabilirlik, güvenlik ve maliyet kıstasları arasındaki gerilimlerin nasıl yönetileceğine yöneticilerin karar vermeleri gerekir ve yönetim kurulunun sorgulama ve sınama süreçlerine ihtiyaç duyduğumuz nokta da çoğunlukla burasıdır."

**Daha derine inin.** Yönetim kurulları, kurumlarının siber risk değerlendirmelerini düzenli olarak gözden geçirip geçirmediğinden ve gerekli iyileştirmeleri yapıp yapmadığından haberdar olmalıdır. Çoğu durumda, iç denetim ekibinden bir başlangıç değerlendirmesini veya projesini uygulaması, muhtemelen bir saldırı ve sızma denetimi yapması talep edilir, fakat bu sadece ilk adımdır, diye uyarıyor Pundmann. Siber olayları önlemek, tespit etmek ve onlara müdahalede bulunmak için şirketlerin çok yönlü bir stratejiye ihtiyaçları vardır. Bu çaba, şirketin saldırıları anlamak amacıyla attığı devam eden adımlara, uygulanmakta olan tedbirlerin etkililiğine, olayların ve olaylara yönelik müdahalelerin nasıl izlendiğine ve şirketin müdahalesinin şekline ve başarısına ilişkin bir değerlendirmeyi de içermelidir. Tam strateji değerlendirmesi komite düzeyinde başlayabilir, ancak bu konu yönetim kurulunun tamamı tarafından tartışılmalı ve ele alınmalıdır, demektedir.

Bir Deloitte yayınında da belirtildiği gibi, siber riske karşı mücadelede ilk hat iş birimleri ve BT'den oluşmaktadır, zira bunlar günlük karar ve çalışmalarında riski ele almaktadırlar. Kurumun ikinci hattı, yönetişimi ve denetim ve gözetimi üstlenen bilgi ve teknoloji risk yönetim liderliğidir. İç denetim fonksiyonu giderek daha fazla durumda üçüncü hat olmaktadır ve güvenlik tedbirlerinin ve performansın bağımsız bir değerlendirmesini yapmaktadır.

**Bu riski farklı kılan şeyin ne olduğunu anlayın.** Kurumlar ve yönetim kurulları risklere aşinadır, fakat siber güvenlik birkaç sebeple diğer risklerden ayrılmaktadır. Birincisi, bu alanın yüksek düzeyde uzmanlık gerektirmesi ve tehditlerin sürekli değişmesidir ve bu da, bu konuyu pek çok yönetim kurulu üyesinin uzmanlık düzeyinin ötesine geçirmektedir. İkincisi, internet kullanımının pek çok kurumda yaygın olması neticesinde risklerin ve bu risklerin bırakabileceği etkinin çok yönlü ve karmaşık olmasıdır. Siber Risk Yönetici Ağı'nın bir panel tartışmasında katılımcılarından biri şöyle demiştir: "Kurumların internete erişimi üretilen değeri sunmada asli öneme sahiptir ve internete erişime bağlı olan tüm bu işlemler tabiatları gereği güvenli değildir". "Bu, yönetim kurullarının uğraştıkları diğer risk yönleri ve alanları için geçerli değildir, bu yönüyle onlardan ayrılır."

# YÖNETİM KURULU ÜYELERİNE SORULAR

» Yönetim kurulu, kurumun karşı karşıya olduğu siber güvenlik tehditlerini ve siber riskleri ele almak ve yönetmek için atılan adımlarla ilgili en güncel bilgileri ne sıklıkla almaktadır?

» Kurum, siber güvenliği sadece bir BT meselesi olarak değil de bir kurumsal risk meselesi olarak mı ele almaktadır?

» Yönetim Kurulu siber riskleri izleme konusunda proaktif bir rol oynuyor mu yoksa aksi söyleninceye kadar her şeyin yolunda olduğunu mu varsayıyor?

» Kurumun özel bir siber güvenlik komitesi var mı? Eğer yok ise, başka bir komitenin, örneğin denetim komitesinin siber güvenlik konusunda denetim ve gözetim sorumluluğu var mı?

**Gerçek hayata uygun bir örnek bulun.** Bir masa başı tatbikatında - *ki bunu iç denetim birimi, diğer yönetim kademeleri veya dışarıdan bir taraf yürütebilir* - kurumun saldırılara nasıl müdahale ettiğini, yatırımcıların konuyla ilgili nasıl bilgilendirildiklerini ve müşterilerin veya iş ortaklarının saldırılardan nasıl etkilendiklerini belirlemek maksadıyla yönetim kurulu ve yönetim simüle edilmiş bir saldırıyı izleyebilirler. (Tatbikatı mümkün olduğunca gerçekçi kılmak için durumun bir simülasyon olduğundan sadece CIO ve CEO'nun haberdar olmasını isteyen bir yönetim kuruluyla dahi çalışmış Pundmann). Kurum müdahaleyi değerlendirir değerlendirmez, yönetim kurulu yapılmış veya yapılmakta olan değişiklikler hakkındaki en güncel bilgileri alabilir.

İç denetim, önemli başka bir tatbikatta merkezi bir oyuncu rolünü de üstlenebilir; söz konusu tatbikat, tamamı uzman olmayan kişilerin anlayabileceği terimlerle ifade edilen, siber risklerin yüksek düzeyde bir kurumsal görünümünü sunan ve kurumun bulunduğu yer ile bulunması gereken yeri karşılaştıran bir olgunluk modeli canlandırmasıdır. Pundmann, tüm riskleri izlemek ve ele almak mümkün olmadığı için, bu tatbikatlar aynı zamanda hangi hedeflerin en kritik olduğunu açıklığa kavuşturarak kurumun o alanlarda önleme ve tespit faaliyetlerini iyileştirmesini sağlayabileceğini söylemiştir.

**Risklerin sizi gafil avlamasına izin vermeyin.** Teknolojinin benimsenme ve yaygınlaşma düzeyi arttıkça, bilinmeyen yeni teknolojilerle ilişkilendirilen riskler de aynı şekilde artmaktadır. Yeni bir ERP sistemi dahi gözden kaçırılmaması gereken güvenlik sorunları teşkil edebilir, diye belirtiyor Pundmann. Pek çok şirketin, yeni bir sistemde ortaya çıkabilecek sorunlarla nasıl baş edileceğini planlamak için sistemde sorun çıkmasını beklemesi hatalı bir davranıştır. "Siber ve kontrol stratejiniz için en başından itibaren bir güvenlik planınız olduğundan emin olun," demektedir.

Şirket birleşmelerinin ve satın almalarının tarafı olan kurumlar da yeni zafiyetlerle karşı karşıya kalabilirler. "Eğer bir şirketi satın alıyorsanız, işlerinizi ve işletmelerinizi birbirine bağlarken ne tür riskler aldığınızı sorun", tavsiyesinde bulunuyor. Tedarik zincirleri veya diğer üçüncü taraflarla iş yapan şirketler de o kaynaklardan gelebilecek risklere açık hale gelebilirler. İlaveten, uyum alanında, örneğin Menkul Kıymetler ve Borsa Komisyonu'nun siber güvenlik açıklamaları ile ilgili kuralları gibi ilgili düzenlemelerden kurumlar haberdar olmalıdırlar.

## İç Denetim Kaynaklarından İstifade Etmek

**Siber tehditler korkutucu olabilir,** fakat iç denetim, kurumun karşı karşıya olduğu riskler ve bu risklerin en iyi nasıl giderileceği konusunda benzersiz ve bağımsız bir bakış açısı sunabilir. Siber güvenlik sorunlarının izlenmesinde proaktif davranan ve iç denetimin sunabileceği değerden tam anlamıyla istifade edebilen yönetim kurulları siber güvenlik risklerini gidermek konusunda daha iyi ve avantajlı bir konumda olacaklardır.

## YÖNETİM KURULUNUZUN EKSİĞİ NE?

Kurumların **%60**'ında yönetim kurulu üyesi veya icrai yönetim düzeyinde görevli bir siber güvenlik yöneticisi yoktur.

Kurumların **%59**'u siber güvenlik birimi ile iş kolları arasındaki ilişkinin en iyi ihtimalle nötr olduğunu, diğer durumlarda ise güvensiz veya namevcut olduğunu söylemektedir.

Yönetim kurullarının **%20**'si, kendilerine sunulan siber güvenlik risklerinin ve risk azaltma tedbirlerinin kurumu büyük siber saldırılardan koruyabileceğinden aşırı derecede emindirler.

Kurumların **%36**'sı, henüz yeni iş inisiyatiflerini planlama aşamasından başlayarak siber güvenliği sürece dâhil ettiklerini söylemektedir.

Kaynak: *(Riskli Altılı: Yönetim Kurullarının Kurumsal Siber Dayanıklılığı Anlama Konusundaki Açıklarını Teşhir Etmeye Yönelik Kilit Sorular) "The Risky Six: Key Questions to Expose Gaps in Board Understanding of Organizational Cyber Resiliency,"* IIA Global ve EY, 30 Mart 2021.

1 *2021 ve 2030 Yılları için En Önemli Riskler Hakkında Yöneticilerin Görüşleri*, Protiviti ve NC State University ERM İnisiyatifi, 2021. *(Executive Perspectives on Top Risks for 2021 and 2030)*

2 *"Siber Suçların 2025 Yılına Kadar Dünyaya 10,5 Trilyon Dolara Mal Olması Bekleniyor"*, Steve Morgan, *Cybercrime Dergisi*, 13 Kasım 2020. *("Cybercrime to Cost the World $10.5 Trillion Annually by 2025")*

3 *Bir Veri İhlalinin Maliyeti Raporu*, IBM, 2021. *(Cost of a Data Breach Report)*

4 *"Gartner 2025 Yılına Kadar Yönetim Kurullarının %40'ında Özel Bir Siber Güvenlik Komitesinin Olacağını Tahmin Etmektedir"* Gartner basın açıklaması, 28 Ocak 2021. *("Gartner Predicts 40% of Boards Will Have a Dedicated Cybersecurity Committee by 2025,")*

5 *"Yönetim Kurulları ve Siber Güvenlik"* McKinsey and Company podcast yayını, 2 Şubat 2021. *("Boards and Cybersecurity")*

6 *"Siber Güvenlik ve İç Denetimin Rolü: Acil Harekete Geçme Çağrısı"* Sandy Pundmann, Deloitte, 2017. *("Cybersecurity and the Role of Internal Audit: An Urgent Call to Action")*

7 *"Siber Güvenlik: Değişen Bir Yönetişim Sorunu"*, Harvard Law School Forum on Corporate Governance (Harvard Hukuk Fakültesi Kurumsal Yönetişim Forumu), 15 Mart 2020. *("Cybersecurity: An Evolving Governance Challenge,")*

8 *"Halka Açık Şirketlerin Siber Güvenlik Açıklamaları Hakkında Komisyon Açıklaması ve Kılavuzu"*, 33-10459 ve 34-82746 sayılı Açıklamalar, Securities and Exchange Commission (Menkul Kıymetler ve Borsa Komisyonu), 26 Şubat 2018. *("Commission Statement and Guidance on Public Company Cybersecurity Disclosures,")*


## Hızlı Anket Sorusu

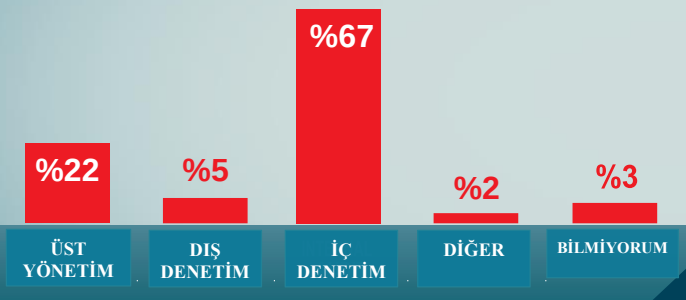
**Yönetim kurulunuzda siber güvenlik uzmanı bir üye var mı?**

- ❑ Evet
- ❑ Hayır
- ❑ Bilmiyorum

Soruyu cevaplamak ve başkalarının bu soruya ne cevap verdiğini öğrenmek için www.theiia.org/Tone adresini ziyaret ediniz.

## HIZLI ANKET SONUÇLARI

Yönetim kurulu, risk yönetimi ve iç kontrolün etkinliği konusunda güvence için birincil olarak kime itimat ediyor?




Kaynak: Tone at the Top, Haziran 2021