TONE at the TOP®

Üst yönetime, yönetim kurullarına ve denetim komitelerine yönetişimle ilgili konularda kısa ve öz bilgiler sunar.

Sayı 137 | Ekim 2026



Siber Güvenlik İhlalinden Yönetim Kurulu Gündemine:

Siber Güvenlik Gözetiminin Güçlendirilmesi

Şubat 2024'te UnitedHealth Group'un bir iştiraki olan Change Healthcare'e yönelik bir fidye yazılımı saldırısı, ABD sağlık sisteminin büyük bölümünde sigorta talepleri ile ödeme işlemlerini durma noktasına getirmiştir. Saldırının bilançosu ağır olmuştur: 32,2 milyar dolarlık doğrudan müdahale maliyeti, iş kesintisinden kaynaklanan 3867 milyon dolarlık ek zarar ve etkilenen yaklaşık 190 milyon kişi.

Saldırganlar, sisteme temel bir güvenlik kontrolü olan çok faktörlü kimlik doğrulamanın kullanılmadığı bir portal üzerinden girmiştir. Şirketin CEO'su Andrew Witty de ABD Senatosu Finans Komitesi önünde bu durumu onaylamıştır.
Komite Başkanı Ron Wyden ise açılış konuşmasında sorumluluğu en tepeye yüklemiş ve şirketin yönetim kurulunda gerçek anlamda bir siber güvenlik uzmanına ihtiyaç olduğunu savunmuştur.

Bu artık yalnızca konuşulmakla kalan bir görüş değildir. Delaware Hakkaniyet Mahkemesi (Delaware Court of Chancery), 2025 yılında verdiği bir dizi kararda siber güvenliğin, yönetim kurullarının öylece yönetime devredemeyeceği "kritik öneme sahip" bir risk olduğuna hükmetmiştir. Artık yönetim kurulu üyelerinin bu konuda düzenli olarak bilgilendirme alması beklenmekte; bu toplantılara ait tutanakların bulunmaması bile tek başına gözetim yükümlülüğünün yerine getirilmediğine işaret edebilmektedir.

Bu riskin yakın zamanda ortadan kalkması da beklenmemektedir. IIA'nın 2026/2027 Risk in Focus Raporuna göre iç denetim liderlerinin %80'i siber güvenliği, kurumlarının karşı karşıya olduğu en önemli beş risk

arasında göstermiştir. Bu oran 2025'e göre 7 puan artmış olup en çok seçilen ikinci risk olan köklü dijital dönüşümün (Yapay Zekâ dâhil) 22 puan üzerindedir.

Görüldüğü üzere siber güvenlik, kurumun en üst kademesinin azami ölçüde dikkat göstermesini gerektiren kritik bir alandır. Yönetim kurulu üyeleri, siber risklerin gözetimini görevlerinin bir parçası olarak ele almak ve bu görevi yerine getirebilecek yeterli uzmanlığı geliştirmekle yükümlüdür.

Tone at the Top'ın bu sayısında kurumların siber güvenlik çalışmalarındaki olası eksiklikler, siber güvenlik yönetişimine ilişkin kamuya yapılan açıklamaların giderek genişleyen kapsamı ve iç denetçilerin, yönetim kurullarının bu alandaki yönetişim sorumluluklarını yerine getirmelerine nasıl destek olabilecekleri ele alınmaktadır.

Devam Eden Bir Süreç

Siber güvenlik, sadece teknik bir mesele olmaktan çıkarak günümüz işletmelerinin karşı karşıya olduğu temel iş risklerinden biri hâline gelmiştir. CrowdStrike'ın Siber Güvenlik Risk Gözetimi: Yönetim Kurulu Üyeleri için Yönetişim Rehberi (Cybersecurity Risk Oversight: A Governance Guide for Board Directors) başlıklı raporunda belirttiği gibi, günümüzde yönetim kurulları siber güvenliğin "bir mevzuata uyum faaliyeti olmaktan çıkıp temel bir yönetişim sorumluluğuna" dönüştüğüne tanıklık etmektedir.

Kurumların siber güvenliğe ilişkin kamuya yapılan açıklamaları ele alış biçimi, bu dönüşümün açık bir örneğidir. ABD Menkul Kıymetler ve Borsa Komisyonu (SEC) siber güvenlik açıklamalarına ilişkin kuralları 2023 yılında belirlemiş olsa da pek çok kurum bunun da ötesine geçerek siber güvenlik gözetimi ve yönetim kurulunun bu alandaki uzmanlığı hakkında gönüllü olarak ayrıntılı bilgiler paylaşmaktadır.

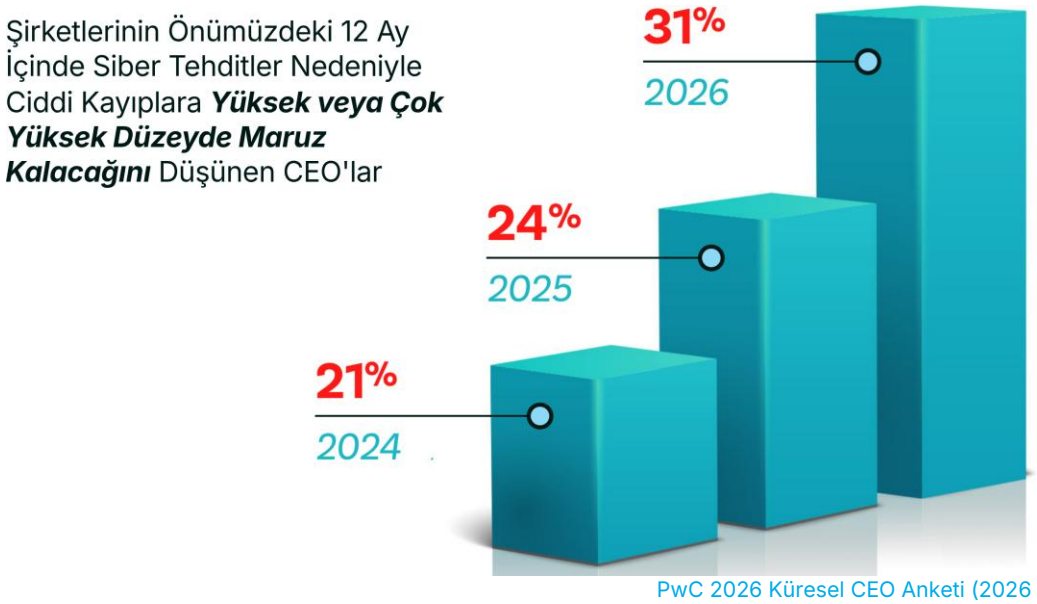
Nitekim yatırımcılar ve diğer paydaşlar siber güvenlik gözetimine ilişkin daha fazla bilgi talep etmeye devam ederken EY'nin piyasa değeri yüksek şirketler üzerinde yaptığı analiz, son yıllarda pek çok alanda yapılan kamuya yapılan açıklamalarda kayda değer artışlar olduğunu ortaya koymuştur. EY'nin araştırmasındaki başlıca bulgular şunlardır:

- Şirketlerin %78'i siber güvenlik gözetiminden denetim komitelerinin sorumlu olduğunu belirtmektedir.
- %86'sı siber güvenliği, yönetim kurulu üyelerinden birinin sahip olduğu ya da yönetim kurulunun aradığı bir uzmanlık alanı olarak açıkladığını belirtmektedir — bu oran 2019 yılında %53'tü.%73'ü siber güvenlik çalışmalarını NIST CSF 2.0 veya ISO 27001 gibi harici bir çerçeveyle uyumlu hâle getirmektedir.
- %58'i simülasyonlar, masa başı tatbikatları veya müdahaleye hazırlık testleri gibi siber güvenliğe hazırlık faaliyetleri yürütmektedir — bu oran 2019 yılında %3'tü.

Ancak kurumların siber riskleri ciddiye aldığı açıkça görülse de riskin hızına ayak uydurma konusunda kayda değer eksiklikler bulunmaktadır. Bu durum, örnek olarak kurumların yapay zekâyı kullanma ve anlama biçiminde kendini göstermektedir; bu alan, en iyimser değerlendirmeyle bile hâlâ gelişim aşamasındadır.

Workiva'nın 2026 Yıl Ortası Yönetici Kıyaslama Anketi (2026 Midyear Executive Benchmark Survey) sonuçlarına göre yöneticilerin %84'ü, herhangi bir insan incelemesinden geçmese bile yapay zekâ (YZ) çıktılarının doğruluğuna en azından bir ölçüde güvendiğini belirtmektedir. Öte yandan yöneticilerin %26'sı, iç denetimlerin kurum dışındaki kişilere veya yönetim kurulu üyelerine ulaşmış YZ hatalarını tespit ettiğini ifade etmektedir. Bu sonuçlar, yöneticilerin YZ'ye ilişkin varsayımları ile YZ'nin kendi kurumlarında fiilen nasıl işlediği arasında bir kopukluk olabileceğine işaret etmektedir.

Workiva'ya göre "YZ, işletmeleri benzeri görülmemiş bir hızla yeniden şekillendirirken yeni bir risk de ortaya çıkmaktadır. Dönüşüm, onu gözetmekle görevli liderlerin sezgilerini geride bırakıyor olabilir."



PwC 2026 Küresel CEO Anketi (2026 Global CEO Survey).

IIA Hakkında

İç Denetçiler Enstitüsü (IIA), 265.000'den fazla küresel üyeye hizmet veren ve 200.000'den fazla Sertifikalı İç Denetçi (CIA) sertifikası veren kâr amacı gütmeyen uluslararası bir meslek birliğidir. 1941 yılında kurulan IIA, dünya çapında iç denetim mesleğinin standartlar, sertifikalar, eğitim, araştırma ve teknik rehberlik alanlarındaki lideri olarak tanınmaktadır. Daha fazla bilgi için theiia.org adresini ziyaret edin.

IIA

1035 Greenwood Blvd.
Suite 401
Lake Mary, FL 32746 ABD

Ücretsiz Abonelik

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

Okuyucu Geribildirimi

Sorularınızı/Yorumlarınızı gönderin: **Tone@theiia.org**.



Siber Güvenlik Tartışmasında İç Denetçilerin Yeri

İç denetim fonksiyonu, kurumların siber güvenlik risklerini azaltma çabalarında değerli bir iş ortağıdır. IIA'nın Siber Güvenlik Konu Bazlı Gerekliliği (Cybersecurity Topical Requirement) ve buna ilişkin Kullanıcı Rehberi, siber güvenlik risk yönetimi planında iç denetimin rolünün ne olması gerektiğini, Uluslararası İç Denetim Standartlarına uyum için ise bu rolün asgari olarak neleri kapsaması gerektiğini açıkça ortaya koyan temel bir kaynak niteliğindedir.

Bu Gereklilik, "siber güvenlik yönetişimi, risk yönetimi ve kontrol süreçlerinin tasarımını ve uygulamasını değerlendirmeye yönelik tutarlı ve kapsamlı bir yaklaşım" sağlamak üzere tasarlanmıştır. Bu doğrultuda iç denetim, üç temel alanı değerlendirmekle yükümlüdür:

- **Yönetişim:** Kurumsal hedefleri, politikaları ve prosedürleri destekleyen, açıkça tanımlanmış temel siber güvenlik hedefleri ve stratejileri.
- **Risk Yönetimi:** Siber risklerin gecikmeksizin üst makamlara iletilmesine yönelik bir süreç de dâhil olmak üzere siber tehditleri belirleme, analiz etme, yönetme ve izleme süreçleri.
- **Kontroller:** Siber riski azaltmak amacıyla yönetim tarafından oluşturulan ve periyodik olarak değerlendirilen kontrol süreçleri.

Siber güvenlik yönetişimi bakımından Konu Bazlı Gereklilik, yönetişim gerekliliklerini ilgili çerçevelerle eşleştirmektedir. Bu çerçeveleri anlamak, denetim komitesinin ve yönetim kurulunun kurumun siber risk yönetimi planına ilişkin bilgi birikiminin kritik bir parçası olmalıdır. Ayrıca Gereklilik, iç denetimin yönetişim süreçlerinin siber güvenlik hedeflerine nasıl uygulandığını gözden geçirmesini ve bu kapsamda aşağıdakilerin mevcut olup olmadığını incelemesini gerekli kılmaktadır:

- Resmîleştirilmiş planlar ve hedefler.
- Siber güvenlik süreçlerini yönetmek için kullanılan politikalar, prosedürler ve diğer ilgili belgeler.
- Siber güvenlik hedeflerine ulaşılmasını destekleyen roller ve sorumluluklar ile siber güvenlik fonksiyonunun, yeterli destek ve görünürlük elde edebilecek kadar üst bir kademeye bağlı olup olmadığı.
- Kurum içindeki ve dışındaki ilgili paydaşlarla karşılıklı etkileşim kurulduğuna ve iletişim sağlandığına dair kanıtlar.

Bir bütün olarak ele alındığında bu gereklilikler, yönetim kurullarına ve denetim komitelerine siber güvenlik konusunda iç denetimden neler bekleyebileceklerine dair net bir tablo sunacaktır. Ayrıca bu gereklilikler Uluslararası İç Denetim Standartlarına uyum için zorunlu olduğundan, yönetim kurulu üyeleri Standartlara uygun çalışan bir iç denetim fonksiyonunun sağlayabileceği değeri azami düzeye çıkardığından emin olabilir.

Siber Güvenlik Endişelerine Artan İlgi

Telekomünikasyon sektörü, siber güvenlik riskiyle mücadele eden pek çok sektörden biridir. Bu alanda savunuculuk çalışmalarında son dönemde kaydedilen ilerlemeler, iç denetimin bu konuda ne denli değerli olabileceğini yönetim kurullarına göstermek açısından yararlı bir örnek olay niteliğindedir.

Telekomünikasyon sektörünü tehdit eden unsurlar arasında "makine hızında gerçekleşen siber saldırılar" ile güvenlik operasyonlarının yeni ortaya çıkan tehditlere genel olarak geç yanıt vermesi yer almaktadır. Bu tespitler, EY'nin "Telekom Şirketleri Yapay Zekâ Saldırıları Çağında Siber Güvenliği Nasıl Güçlendirebilir?" (How Telecoms Can Dial Up Cybersecurity in the Age of AI Attacks) başlıklı yayınında ortaya konmaktadır.

Kanada'da kısa süre önce kabul edilen bir yasa, hükümetin ülkenin telekomünikasyon sistemini bu tür tehlikelere karşı koruma kapasitesini güçlendirmektedir. Yasa, federal hükümetin düzenleme yetkisindeki sektörlerde kritik siber sistemleri işleten kuruluşların siber altyapılarını korumak için gerekli adımları atmasını zorunlu kılmaktadır.

IIA, daha sonra Kanada'nın Kritik Siber Sistemlerin Korunması Yasası (Critical Cyber Systems Protection Act) adını alacak düzenlemeye ilişkin görüşlerinde, kurumların olası siber riskleri belirleyip azaltmasına yönelik etkili süreçler geliştirilmesi ve uygun iç kontroller ile bağımsız güvence prosedürlerinin varlığının sağlanması gerektiğine dikkat çekmektedir. Yasa, "bu mevzuat uyarınca düzenlemeye tâbi olarak belirlenmiş bir operatörde iç denetim" yapılmasını öngörmektedir.

Diğer ülke ve bölgelerdeki siber güvenlik düzenlemelerinden bazıları şunlardır:

- ABD: 2022 tarihli Kritik Altyapılara Yönelik Siber Olay Bildirim Yasası (Cyber Incident Reporting for Critical Infrastructure Act of 2022).
- Avrupa Birliği: NIS2 Direktifi.
- Birleşik Krallık: 2018 tarihli Ağ ve Bilgi Sistemleri Düzenlemeleri (Network and Information Systems Regulations 2018).

Yönetim Kurullarının İç Denetimin Bakış Açısına İhtiyacı Var

Siber güvenlik, her kurum için son derece geniş kapsamlı ve zaman zaman içinden çıkılması güç bir konudur. İşin içindeki teknik ve sürekli değişen pek çok unsur düşünüldüğünde, yönetim kurullarının kendilerine mümkün olan en açık, en doğru ve en ilgili bilgilerin sunulduğundan emin olmak için sağlam yönetişim ve raporlama yapılarına güvenmeleri gerekecektir. Bu noktada tartışmaya etkili bir katkı sunabilecek konumda iç denetimden daha uygun konumlandırılmış bir fonksiyon bulunmamaktadır.



Uluslararası İç Denetçiler Enstitüsünün (Institute of Internal Auditors Inc., "IIA") Telif Hakkı © 2013 kesinlikle saklıdır. IIA isminin veya logosunun çoğaltılmasında ABD federal ticari marka tescil sembolü olan ® kullanılacaktır. Bu materyalin hiçbir kısmı IIA tarafından öncesinde yazılı izin verilmeksizin çoğaltılamaz. Değiştirildiği onaylanmadıkça tüm maddi yönlerden orijinali ile aynı olan bu çevirinin yayımlanması için telif hakkı sahibi olan Uluslararası İç Denetçiler Enstitüsü (Institute of Internal Auditors Inc., "IIA") 1035 Greenwood Blvd. Suite 401 Lake Mary, FL 32746, ABD isimli kurumdan izin alınmıştır. Bu belgenin hiçbir kısmı IIA tarafından öncesinde yazılı izin verilmeksizin çoğaltılamaz, bir geri alma sisteminde depolanamaz veya hiçbir formda veya elektronik, mekanik, fotokopi, kaydetme veya başka bir şekilde hiçbir suretle aktarılamaz. İşbu belge Türkiye İç Denetim Enstitüsü tarafından çevrilmiştir. Tone at the Top Ekim 2026 bülteni Sayın Tuğrul Bozbey ve Sayın Alp Buluç (SMMM, CIA, CRMA, CCSA), tarafından gözden geçirilmiş ve "edit" edilmiştir.

Uluslararası İç Denetçiler Enstitüsünün (Institute of Internal Auditors Inc., "IIA") Telif Hakkı © 2013 kesinlikle saklıdır. IIA isminin veya logosunun çoğaltılmasında ABD federal ticari marka tescil sembolü olan ® kullanılacaktır. Bu materyalin hiçbir kısmı IIA tarafından öncesinde yazılı izin verilmeksizin çoğaltılamaz. Değiştirildiği onaylanmadıkça tüm maddi yönlerden orijinali ile aynı olan bu çevirinin yayımlanması için telif hakkı sahibi olan Uluslararası İç Denetçiler Enstitüsü (Institute of Internal Auditors Inc., "IIA") 1035 Greenwood Blvd. Suite 401 Lake Mary, FL 32746, ABD isimli kurumdan izin alınmıştır. Bu belgenin hiçbir kısmı IIA tarafından öncesinde yazılı izin verilmeksizin çoğaltılamaz, bir geri alma sisteminde depolanamaz veya hiçbir formda veya elektronik, mekanik, fotokopi, kaydetme veya başka bir şekilde hiçbir suretle aktarılamaz. İşbu belge Türkiye İç Denetim Enstitüsü tarafından çevrilmiştir. Tone at the Top Ekim 2026 bülteni Sayın Tuğrul Bozbey ve Sayın Alp Buluç (SMMM, CIA, CRMA, CCSA), tarafından gözden geçirilmiş ve “edit” edilmiştir.