TONE at the TOP®

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

Sayı 119 | Ekim 2023

Yeni SEC Siber Güvenlik Açıklama Kuralları: *Yönetim Kurulları Gündemi Yakalamak için Ne Yapmalı?*

ABD Menkul Kıymetler ve Borsa Komisyonunun (SEC) yeni siber güvenlik açıklama kuralları, her yerde karşılaşılan bu risk konusunda güçlü bir yönetişimin önemini daha da artırmaktadır. NACD (Ulusal Yönetim Kurulu Üyeleri Derneği) tarafından hazırlanan bir makalede, bu kuralların yakın zamanda kesinleştiği göz önünde bulundurulduğunda, "her ölçekte halka açık şirketin açıkça belirlenen son tarihlerden önce uyum sağlama yarışı içinde oldukları" belirtilmektedir.[1] Yeni kuralların etkilerini anlamak ve uyumu sağlamak için adımlar atmak kurumlar için en önemli öncelik olmalıdır. Tone at the Top yayınının bu sayısında yeni yönetmelikler incelenmekte ve iç denetimin bir şirketin siber güvenlik çaba ve çalışmalarına yapabileceği önemli katkılar tartışılmaktadır. Ayrıca, yönetim kurulu üyeleri için yeni sorumluluklar ve başka önemli hususlar da vurgulanmaktadır.

Büyüyen Bir Tehdit

Siber güvenlik bilgisayarlar, ağ cihazları, yazılım ve veriler de dâhil olmak üzere bir kurumun bilgi kaynaklarının yetkisiz erişim, kesinti veya tahribata karşı korunmasıyla ilgilidir. Buna rağmen, her teknolojik gelişmeyle birlikte dolandırıcılar siber güvenlik saldırıları düzenlemek için yeni yollar bulmakta ve bu da siber riski tüm işletmeler için önemli bir konu haline getirmektedir.

Siber ihlallerin maliyeti yıkıcı olabilir: Cisco tarafından yapılan bir araştırmaya katılan özel sektör siber güvenlik liderlerinin yaklaşık %60'ı son 12 ay içinde bir siber güvenlik vakasıyla karşılaştıklarını ve etkilenenlerin %41'i için maliyetin en az 500.000$ olduğunu bildirmiştir.[2] Doğrudan finansal maliyetlere ilave olarak, siber suçlar ve saldırılar bir şirketin iş yapma kabiliyetini sekteye uğratabilir, gizli kurumsal ve müşteri verilerini ifşa edebilir ve itibarına zarar verebilir.

Bu nedenle SEC'in geçtiğimiz yaz halka açık şirketlerin kayda değer siber güvenlik ihlallerini nasıl raporlamak ve siber güvenlik risk yönetimi, stratejisi ve yönetişim uygulamalarına ilişkin bilgileri nasıl açıklamak zorunda olduklarına dair yeni kurallar yayımlaması şaşırtıcı değildir. Bu kurallar, 2022 yılında yayımlanan tasarıları güncellemekte ve nihai hale getirmektedir.

Siber Riskin Etkisi

Kurumlar siber olaylar ve ihlaller nedeniyle ne gibi olumsuz sonuçlarla karşılaşmıştır?

Etki	2021 YILI SIRASI	2023 YILI SIRASI	2023 YILI YÜZDESİ
İş kesintisi (tedarik zinciri ve/veya ortak ekosistemi de dâhil)	1	1	%58
Gelir kaybı	9	2	%56
Müşteri güveninin kaybı/olumsuz marka etkisi	4	3	%56
İtibar kaybı	5	4	%55
Stratejik bir girişimin fonlarının kesilmesi	İlgili değil	5	%55
Teknoloji bütünlüğüne olan güvenin kaybı	İlgili değil	6	%55
Olumsuz yetenek işe alma/kurumda tutma etkisi	8	7	%54
Fikri mülkiyet hırsızlığı	2	8	%54
Hisse fiyatında düşüş	2	9	%52
Mevzuat kaynaklı para cezaları	7	10	%52
Liderlikte değişim	5	İlgili değil	İlgili değil

Kaynak: 2023 Küresel Siber Gelecek Anketi (2023 Global Future of Cyber Survey), Deloitte, 2023
Not: 2021'de ilk iki sıralama sıklığına göre, 2023'te ilk iki kutu seçimi

IIA Hakkında

The Institute of Internal Auditors (IIA), 230.000'den fazla küresel üyeye hizmet veren ve dünya çapında 185.000'den fazla Sertifikalı İç Denetçi (CIA) sertifikası vermiş 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 ediniz.

The IIA

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

Ücretsiz Abonelik

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

Siber Güvenlik Yönetimi ve Olayları Hakkında Açıklamaların Kapsamının Genişletilmesi

SEC'in kuralları, Menkul Kıymetler Borsa Kanununun raporlama şart ve gerekliliklerine tâbi olan halka açık şirketlerin siber güvenlik açıklamalarını iyileştirmeyi ve standart hale getirmeyi amaçlamaktadır. Yeni kurallar, şirketlerin kayda değer olduğu düşünülen risk yönetimi, strateji, yönetişim ve siber güvenlik olayları hakkında raporlamak zorunda oldukları hususların kapsamını genişletmektedir. Yeni kurallar, kayıtlı kurumların aşağıdakileri yapmasını gerektirmektedir:

- Siber güvenlik tehditlerini nasıl değerlendirdiklerini, tespit ettiklerini ve yönettiklerini ve herhangi bir riskin iş stratejilerini, operasyon sonuçlarını veya mali durumlarını önemli ölçüde etkileyip etkilemediğini ya da önemli ölçüde etkileme ihtimalinin olup olmadığını açıklamak. Ayrıca, önemli siber güvenlik olaylarını açıklamak ve her bir olayın niteliği, kapsamı ve zamanlamasına ilişkin kayda değer hususları tarif etmek zorundadırlar.
- Yönetim kurulunun siber riskleri nasıl denetlediğini ve yönetimin önemli riskleri değerlendirme ve yönetme konusundaki rolünü ayrıntılı olarak açıklamak. SEC, yönetim kurulunun siber güvenlik uzmanlığının açıklanmasına ilişkin teklif edilen gerekliliklerden birini kabul etmemeye karar vermiştir.
- Yabancı özel ihraç kurumları da aynı kurallara tâbidir ve kamuya açıkladıkları veya açıklamak zorunda oldukları ya da yabancı bir ülkede veya hukuki ortamda, herhangi bir borsaya veya menkul kıymet sahiplerine açıkladıkları önemli siber güvenlik olayları hakkında bilgi vermek zorundadırlar.
- Bir kurumun bir siber olayının önemli olduğunu belirlemesinden itibaren genellikle dört iş günü içinde bir Form 8-K dosyası hazırlamak. (ABD Başsavcısının derhal açıklama yapmanın ulusal güvenlik veya kamu güvenliği için önemli bir risk oluşturacağını belirlemesi ve SEC'e yazılı olarak bildirmesi halinde, açıklamanın geciktirilmesine izin verilebilir.)

Yönetim Kurullarının Dikkate Alması Gereken Önemli Hususlar

Birçok kurum siber olayları şu anda ne kadar iyi tespit ettiklerini, analiz ettiklerini, yönettiklerini ve bunlardan ne kadar iyi toparlandıklarını anlamak için boşluk ve eksiklik değerlendirmeleri yapmaktadır. İç Denetçiler Enstitüsü (IIA) Standartlar ve Mesleki Rehberlik Direktörü George Barham (CIA, CRMA, CISA), yeni kurallar göz önüne alındığında, yönetim kurullarının var olan değerlendirme sürecinin dört günlük bir toparlanmayı destekleyip desteklemeyeceğini belirlediğinden emin olmaları gerektiğini söylemiştir. Ayrıca, olayları BT ekibi tespit edecek olmasına rağmen, kapsamlı bir bakış açısı kazanmak amacıyla bu olayların önemlilik derecesini belirleme sürecine mali, hukuki ve düzenleyici ekipler gibi diğer alanlardan da girdi sağlanması gereklidir.

Yönetim kurulu üyelerinin önemliliğin hem nicel hem de nitel unsurları olduğunun da bilincinde olmaları gereklidir. Barham "Parasal kayıplardan daha fazlası söz konusudur" demiştir. Bu durum aynı zamanda hukuki ve düzenleyici hususları da içermektedir. Örneğin, şirket Avrupa Birliğinde faaliyet gösteriyorsa, bir olay Genel Veri Koruma Tüzüğü (GDPR — General Data Protection Regulation) kapsamına girebilir. Örneğin, olayın ticari sırların veya kuruma rekabet avantajı sağlayan diğer bilgilerin ifşa edilmesini içermesi halinde, stratejik hususlar da önemlilik konusunda bir faktör olabilir. Barham, önemlilik tespitinin, bir yatırımcının şirket analizini etkileyebilecek her türlü hususu içermesi gerektiğini belirtmiştir.

Düzenlemenin 106. Maddesi yönetim kurulunun rol ve sorumluluklarını ele aldığı için, yıllık 10-K, kurumların siber güvenlik yönetişimlerini belgelemeleri gereken rapordur. Bu belge, örneğin yönetim kurulunun denetim komitesinin siber riski gözden geçirmekten sorumlu olduğunu raporlayabilir, ki genellikle böyledir ve yönetimin siber güvenlik konularında denetim komitesine veya yönetim kuruluna nasıl rapor verdiğini de kapsayabilir. Yönetim kurulu üyelerinin sorumluluklarının bir parçası olarak, siber güvenlik konularını yönetim düzeyinde kimin ele aldığını ve siber tehditlerin nasıl yönetildiğini ve hafifletildiğini anlamaları gereklidir.

İç Denetimin Katkısı

İç denetçiler, genellikle, yaygın olarak benimsenen kontrol çerçevelerine atıfta bulunmak da dâhil olmak üzere siber güvenlikle ilgili risklerin hafifletilmesine yardımcı olan anahtar iç kontrollerin belirlenmesinden ve test edilmesinden sorumludur. Yeni kurallar ışığında, kurumların yönetim organları ve üst yönetimleri, siber güvenlik müdahale ve kurtarma kontrollerinin etkinliğini ve verimliliğini doğrulamak için bağımsız, objektif ve bilgi içeren güvenceye ihtiyaç duyacaktırlar. İç denetim kendi mesleki standartlarının yanı sıra, özellikle kurumun BT ve bilgi güvenliği fonksiyonları tarafından kullanılanlar olmak üzere yaygın kabul gören kontrol çerçevelerine uygun olarak bu güvenceyi sağlayabilir. Şirketler siber risklere karşı en iyi nasıl korunacaklarını tespit ederken iç denetçiler danışmanlık hizmeti de sunabilirler.

Kurumlar yeni gereklilikleri nasıl ele alacaklarını belirlerken iç denetim yöneticisi ve iç denetim ekibi için bazı spesifik roller aşağıdakileri içerebilir:

• Kuralların finansal, stratejik planlama, uyum ve denetim planı açılarından beklenen etkileri konusunda yönetim kurulları, üst yönetim ve siber güvenlik risk yönetimi liderlerine danışmanlık sunmak.

• Yeni düzenlemelere uyumla ilgili risk değerlendirmelerini güncellemek ve kurumun gereklilikleri karşılamaya yönelik hazırlıklarını desteklemek. Eğer iç denetim birimi siber güvenlik risk değerlendirmelerine halihazırda katılmamışsa, bu sürece katkıda bulunmaya başlayabilir.

• Güncel siber güvenlik kontrollerinin kurumun yeni kurallara uyum sağlaması için uygun şekilde tasarlanıp tasarlanmadığına ve etkin şekilde işleyip işlemediğine ilişkin raporlama yapmak.

"Siber güvenlik genellikle kurumların yönetmek zorunda olduğu en yüksek risk alanlarından biri olarak kabul edilir," diye belirtmiştir Barham; dolayısıyla zaten iç denetimin radarında olduğu kesindir. Bu, iç denetimin ilgili risklerin ve bu riskleri hafifletmek için gerekli iç kontrollerin bilincinde olduğu anlamına gelmektedir. İç denetim, yönetim kurullarının yeni kurallar kapsamındaki siber güvenlik yönetişim sorumluluklarını yerine getirmek için ihtiyaç duydukları bilgi ve içgörüleri de sağlayabilir. Yönetimin sağladığı bakış açısına ilave olarak, iç denetim siber risklerin nasıl yönetildiği ve açıklandığı konusunda bağımsız ve objektif bir bakış açısı sunabilir. Denetim komitesine siber güvenlik riski ve düzenlemelerinin denetim planına dâhil edilmesi konusunda tavsiyelerde bulunabilir ve kurumun SEC kurallarına uymaya ne kadar iyi hazırlandığı ve bunları ileriye dönük olarak ne kadar iyi uyguladığı konusunda rapor verebilir.

Son Teslim Tarihinin Tutturulması

Olay açıklamaları veya 8-K Formları için, kurallar Federal Resmi Gazetede yayımlandıktan 90 gün sonra veya 18 Aralık 2023'te yürürlüğe girecektir (daha küçük raporlama şirketlerinin uyum için 180 güne kadar ilave süresi vardır). 10-K Formu açıklamaları, 15 Aralık 2023 tarihinde veya sonrasında sona eren mali yıllara ilişkin yıllık raporlardan itibaren yapılacaktır.

NACD, yeni kuralların yönetim kurulu üyelerinin niteliklerini ele almamasına rağmen, "yönetim kurulu, CEO'lar ve bilgi güvenliği yöneticileri de dâhil olmak üzere tüm liderlerin risk yönetimindeki rolünü artırdığını" belirtmiştir. Yönetim kurulu üyeleri yeni sorumluluklarını ele alırken, siber güvenlik endişelerini gidermek için ihtiyaç duyacakları değerli güvence ve içgörü için iç denetime başvurabilirler.

YÖNETİM KURULU ÜYELERİ İÇİN SORULAR

• Kurum, yeni SEC kurallarına uymaya hazırlıklı olunmasından nasıl emin olmaktadır?

• Siber saldırıları önlemek veya hafifletmek için halihazırda ne tür kontroller uygulanmaktadır? Bunlar ne kadar başarılı olmuştur?

• Yeni SEC kurallarını ele almak için yeni kontroller veya raporlama prosedürleri uygulanıyor mu? Eğer uygulanıyorsa, bunlar nelerdir?

• Kurum son iki yıl içinde herhangi bir önemli siber olay tecrübe etmiş midir? Bunlar nasıl ele alınmıştır ve ne gibi iyileştirmeler yapılabilmiştir?

• İç denetimden alınacak ne tür bir güvence veya tavsiye yönetim kurulunun siber risk gözetim sorumluluklarını yerine getirmesine yardımcı olabilir?

" SEC'in Onaylanan Siber Güvenlik Açıklama Kurallarında Zaman Çok Önemli (Time Is of the Essence with SEC's Approved Cybersecurity Disclosure Rules)," James Turgal, NACD, 12 Eylül 2023.
Cisco Siber Güvenlik Hazırlık Endeksi: Hibrit Bir Dünyada Yılmazlık (Cisco Cyber Security Readiness Index: Resilience in a Hybrid World), Cisco, Mart 2023.