KÜRESEL BAKIŞ AÇILARI VE ANLAYIŞLAR

2022 yılında Siber Güvenlik

KISIM 1: Yeni SEC Teklifleri Oyunu Nasıl Değiştirebilir?

KISIM 2: Kritik Ortaklar — İç Denetim ve CISO

KISIM 3: Siber Olay Müdahale ve Kurtarma

The Institute of Internal Auditors

İçindekiler

Kısım 1:

Yeni SEC Teklifleri Oyunu Nasıl Değiştirebilir?

Uzmanlar Hakkında

Andy Watkin-Child

Watkin-Child, 20 yıllık bir siber güvenlik, risk yönetimi ve teknoloji uzmanıdır ve ayrıca, siber güvenlik ve siber risk konularında yönetim, gözetim ve güvenceye yönelik çözüm sağlayıcı olan Augusta Group şirketinin kurucu ortağıdır. Mühendislik ve üretim, finansal hizmetler ve basın ve medya endüstrilerinde bilançoları 1 trilyon Euro'yu aşan şirketlerin liderlik ekipleriyle çalışarak siber güvenlik, siber risk yönetimi, operasyonel risk ve teknoloji konularında 1. ve 2. Savunma Hattında (LoD) uluslararası liderlik pozisyonlarında bulunmuştur. Yönetim kurullarının, küresel risk liderlik ekiplerinin ve siber güvenlik, operasyonel risk ve GDPR komitelerinin deneyimli bir üyesidir.

Manoj Satnaliwala

Satnaliwala, Caliber Home Loans şirketinde iç denetim yöneticisi ve SVP pozisyonundadır; tüm denetim faaliyetlerinden sorumludur ve doğrudan denetim komitesiyle çalışmaktadır. Şu anki rolünden önce, Amerika Birleşik Devletleri'ndeki en büyük üçüncü halka açık ipotek sigorta şirketi olan Radian Group Inc. şirketinde denetim fonksiyonuna liderlik etmiş ve PWC iç denetim fonksiyonu direktörü olarak, büyük bir banka holding şirketi için CCAR projesinin bir parçası olarak iç denetime yönelik kontrollerin validasyonunu yönetmiştir.

Giriş

Yeni düzenleyici tekliflerin devasa sonuçları olabilir

2022 yılındaki ve aslında son birkaç yıldaki haberler pek olumlu olmamakla birlikte ve Ukrayna krizi, kalıcı COVID-19 tehdidi ve giderek artan ABD-Çin gerilimini kapsayan bir ortamda siber tehditler de gölgelerin arasındaki tehditkâr ve korkutucu varlığını korumaktadır. Bu değişkenler ve daha fazlası bir araya gelerek siber güvenliği iç denetçi risk haritalarında önemli — ve hatta lider — bir odak haline getirmiştir.

Bununla birlikte, 2022 yılında geniş bir kurum yelpazesini etkileyecek gibi görünen, siber güvenlikle ilişkili gelişmeler de görülmüştür; bu gelişmeleri anlamak daha fazla efor gerektirecek ve olası etkilerini her yönüyle kavramak zaman alacaktır. ABD Menkul Kıymetler ve Borsa Komisyonu'nun (SEC) yaptığı iki düzenleyici teklif bunların başında gelmektedir. İkinci teklif özellikle önemlidir çünkü ABD'de faaliyet gösteren halka açık işletmelerin hem yönetim kurullarının siber güvenlik alanındaki — eğer varsa — bilgi ve deneyimini hem de siber güvenlik politikalarını, prosedürlerini ve yönetişim stratejilerini açıklamalarını ve rapor etmelerini gerektirecektir. Bu düzenleme uygulamaya konulursa (ki olasılıkla uygulamaya konulacak gibi görünmektedir), halka açık kurumlar faaliyet gösterdikleri endüstriye veya ne kadar büyük olduklarına bakılmaksızın bu yeni kurallara tâbi olacaktır. Bu gelişmelerin, siber güvenlik açısından, bu zorlu süreçte kurumlarını yönlendirmede kritik bir rol oynayacak olan iç denetim topluluğu için yeni bir sayfayı ve — tanıdık da olsa — yeni bir konuyu temsil ettiğini söylemek abartı olmaz.

Bu, hafife alınacak bir zorluk olmasa da iç denetim neyse ki bu gelişmekte olan risk alanında güvence sağlamak için ihtiyaç duyduğu araç ve becerileri anlamaktadır. IIA'nın siber güvenlik hakkında hazırladığı üç kısımdan oluşan Küresel Bilgi Özeti serisinin 1. Kısmı, yeni SEC tekliflerine ve onların hem ABD'de hem de diğer ülkelerde siber güvenlik raporlama yönetmeliği üzerindeki olası etkilerine genel bir bakış sunmaktadır. Ayrıca, iç denetçilerin yeni düzenlemelerin yakında yaratacağı değiştirilmiş uyum ortamını yönetirken kurumlarına yardım etmede nasıl önemli bir rol oynayabileceklerini de keşfetmektedir.

Sahnenin Hazırlanması

Risk ortamını domine eden siber güvenlik

Çağımızın en önemli riski

Siber güvenlik 2022 yılında tüm endüstrilerdeki tüm kurumların bütün kademelerinde birinci sırada yer almaya devam etmektedir ve bu endişe IIA'nın hazırladığı *2022 İç Denetimin Nabzı, Kuzey Amerika* (*Nabız*)[1] yayınında yer alan verilerde açıkça yansıtılmaktadır. Nabız anketine katılan iç denetim liderlerinden kurumları için risk seviyesini başlıca 13 risk arasında derecelendirmeleri istendiğinde, teknolojiyle ilgili riskleri ilk üç arasında derecelendirmişlerdir — siber güvenlik, BT ve (genellikle BT hizmetlerini içeren) üçüncü taraf ilişkileri. Bu ilk üç arasında bile siber güvenlik kolayca ilk sırayı almıştır; katılımcıların %85'i siber güvenliği yüksek veya çok yüksek bir risk olarak derecelendirmiştir ve bu, ikinci en yüksek derecelendirilen risk olan BT'nin derecelendirmesinden %24 daha yüksek bir puandır.

Bu tür bir endişenin olacağı garantidir. 2021 yılında, neredeyse her türden siber saldırı endişe verici marjlarda artmıştır. *2022 SonicWall Siber Tehdit Raporu*[2] yayınına göre, 2021 yılında şifreli tehditlerin sayısı %167 (10,4 milyon saldırı), fidye yazılım %105 (623,3 milyon saldırı), cryptojacking (kripto para madenciliği yapmak için bilgisayarlara yapılan saldırılar) %19 (97,1 milyon saldırı), izinsiz giriş girişimleri %11 (5,3 trilyon saldırılar) ve Nesnelerin İnternetini (IoT) hedef alan zararlı yazılımlar %6 (60,1 milyon saldırı) oranında artmıştır.

Dahası, tüm bu saldırıların sebep oldukları hasar açısından önemli bir maliyete yol açmaktadır. Cisco/Cybersecurity Ventures firmalarının hazırladığı 2022 Siber Güvenlik Yıllık Yayını[3]'nın son versiyonuna göre, 2025 yılına kadar siber saldırılardan kaynaklanan toplam yıllık maliyetin yıllar boyunca ortalama %15 oranında artarak 10,5 trilyon dolara ulaşması beklenmektedir.

Üstelik, bu beklenti jeopolitik ortamdaki siber güvenliği etkileyen dramatik değişiklikleri hesaba bile katmamaktadır. Rusya'nın Ukrayna'yı istilasından önce bile, yüksek seviyelerde karmaşık olan, devlet destekli olduğu şüphesi barındıran siber saldırıların etki ve sıklık açısından arttığı konusunda bol miktarda kanıt vardı. Söylenenlere göre[4] Rus Dış İstihbarat Servisi tarafından yönlendirilen bir bilgisayar korsanlığı grubu 2020 yılında Teksas merkezli SolarWind şirketinin sistemlerinin güvenliğini kırdığında Microsoft, Cisco, Intel, Deloitte, Pentagon'un bazı bölümleri, ABD İç Güvenlik Bakanlığı, Enerji Bakanlığı ve Ulusal Nükleer Güvenlik İdaresi de dâhil olmak üzere 18.000'e kadar müşterinin[5] dijital altyapısının tehlikeye açık olduğunu ve durumun aylarca fark edilemediğini görmüştür.

2021 yılında, ABD şirketlerine yönelik bir başka büyük şüpheli devlet destekli saldırı da Colonial Pipeline Co.[6] şirketinde görülmüştür. Bu saldırı, Doğu Kıyısına benzin ve jet yakıtı tedarikinin neredeyse yarısının akışını geçici olarak kesintiye uğratmıştır. En nihayetinde, Colonial şirketi ağı eski haline getirmek ve verileri kurtarmak amaçlarıyla DarkSide hack grubuna neredeyse 5 milyon dolar fidye ödemiştir.

---

1. The IIA, *2022 İç Denetimin Nabzı, Kuzey Amerika (2022 North American Pulse of Internal Audit)*, Mart 2022, https://www.theiia.org/en/content/research/pulse-of-internal-audit/2022/2022-north-american-pulse-of-internal-audit/
2. SonicWall, *2022 SonicWall Siber Tehdit Raporu (2022 SonicWall Cyber Threat Report)*, 2022, https://www.sonicwall.com/2022-cyber-threat-report/.
3. Steve Morgan, "2022 Siber Güvenlik Yıllık Yayını: 100 Olgu, Rakamsal Veri, Kestirim ve İstatistiksel Veri (2022 Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics)," Cybersecurity Ventures, Cisco, 19 Ocak 2022, https://cybersecurityventures.com/cybersecurity-almanac-2022/.
4. Joe Hernandez, "Microsoft, SolarWinds Saldırısının Arkasındaki Rus Hacker Grubunun Yine İş Başında Olduğunu Söyledi (The Russian Hacker Group Behind the SolarWinds Attack Is At It Again, Microsoft Says)," NPR, Güncelleme tarihi: 25 Ekim 2021, https://www.npr.org/2021/10/25/1048982477/russian-hacker-solarwinds-attack-microsoft.
5. Isabella Jibilian ve Katie Canales, "ABD, SolarWinds Siber Saldırısı Üzerine Rusya'ya Yaptırımlar Hazırlıyor. Büyük Hack'in Nasıl Gerçekleştiğine ve Neden Bu Kadar Önemli Olduğuna İlişkin Basit Açıklama (The US Is Readying Sanctions Against Russia Over the SolarWinds Cyber Attack. Here's a Simple Explanation of How the Massive Hack Happened and Why It's Such a Big Deal)," Business Insider, Güncelleme tarihi: 15 Nisan 2021, https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12.
6. Andrew Marquardt, "As Biden Warns of a Russian Cyberattack, What Are the Precedents? Here's What Happened When a Major Oil Pipeline Was Hacked Last Year," Fortune, March 22, 2022, https://fortune.com/2022/03/22/biden-warns-russian-cyber-attack-pipeline/.

Jeopolitik kırılma noktası

Bu saldırılardan beri, Rusya'yla ilgili endişeler giderek artmış ve Ukrayna'nın istilasıyla birlikte zirve noktasına ulaşmıştır. Gerçekten de Rusya'nın Ukrayna'ya yönelik saldırganlığı geleneksel savaşa ilave olarak siber savaşı da — Ukrayna'nın güç şebekesine[7] yönelik büyük ölçekli bir saldırı — içermektedir ve ayrıca, Rusya'nın NATO ve ABD tarafından uygulanan sayısız ekonomik yaptırıma misilleme yapabileceğine yönelik endişe de artmaktadır. Rusya'nın resmi olarak Ukrayna'ya girmesinden sadece bir hafta önce, Siber Güvenlik ve Altyapı Güvenliği Ajansı (CISA), büyüklüğü ne olursa olsun tüm ABD işletmelerini siber güvenlik ve kritik varlıkların korunması konusunda daha yüksek bir duruş benimsemeleri konusunda uyaran nadir bir "Kalkanlar Yukarı[8]" bildirisi yayınlamıştır. CISA, Rusya siber tehditlerini değerlendiren Mart 2022 beyanında[9] şunları belirtmiştir: "CISA ve diğer sınıflandırılmamış kaynaklar tarafından yayınlanan Son Tavsiye ve Uyarılar, Rus devlet destekli tehdit unsurlarının Amerika Birleşik Devletleri ve diğer Batı ülkelerinde sayılan şu endüstri ve kurumları hedef aldığını ortaya koymaktadır: COVID-19 araştırması, hükümetler, seçim kuruluşları, sağlık ve ilaç, savunma, enerji, video oyunları, nükleer, ticari tesisler, su, havacılık ve kritik üretim."

Mayıs 2021'de, Başkan Biden, ABD'deki ulusal güvenliğin durumunu iyileştirmek için tasarlanan bir yürütme emrini[10] imzalamıştır. Bu emir, hem devlet kurumlarının siber güvenliğe ilişkin rehber ve standartları gözden geçirmesi ve yenilerini geliştirmesine, hem de kurumların yazılım tedarik zinciri güvenliğini ve tehdit bilgisi paylaşımını geliştirmeye odaklanmasına duyulan ihtiyacı spesifik olarak ele almıştır. Yakın zamanda, Başkan Rus siber güvenlik tehdidini yineleyen ve CISA'nın konu hakkındaki gelişen rehberliğini[11] vurgulayan bir bildiri de yayınlamıştır.

Rusya, istikrar bozucu siber saldırıları desteklediği iddia edilen tek devlet değildir. Evanina Group şirketinin 2021 yılında hazırladığı bir rapora[12] göre, Çin özellikle de kişisel bilgilerin elde edilmesi ve veri gizliliği konusunda siber cephede giderek daha agresif hale gelmiştir.

Ulusal Karşı İstihbarat ve Güvenlik Merkezi'nin eski müdürü William Evanina "Çin'in Fikri Mülkiyet ve Ticari Sırlarımızı yasadışı, yasal ve karmaşık hibrit yöntemlerle bütüncül olarak elde etme yeteneği, şimdiye kadar tanık olduğumuz hiçbir şeye benzemiyor," demiştir.

Evanina 2017 Equifax siber ihlâli, dört Çin vatandaşının düzinelerce şirkete, üniversiteye ve devlet kurumuna izinsiz girmeye (hacklemeye) yönelik 2011-2018 kampanyası ve ABD petrol ve doğal gaz boru hattı şirketlerine saldıran, devlet destekli 2011-2013 siber kampanya (DOJ, Temmuz 2021'de bu olayla ilgili bir rapor yayınlamıştır) da dâhil olmak üzere Çin Komünist Partisi'yle bağlantılı çok sayıda siber olaya atıfta bulunmuştur. Ayrıca, Ulusal Güvenlik Ajansı (NSA), Federal Soruşturma Bürosu (FBI) ve CISA kurumları tarafından hazırlanan ve Çin devlet destekli bilgisayar korsanlarının ABD'ye karşı kullandığı 50'den fazla siber taktik ve aracı yayınlayan Temmuz 2021 tarihli rapora da atıfta bulunmuştur.

Bu karmaşık ve genel olarak tehlikeli siber ortamda, SEC, özellikle SEC'e ve (bazı durumlarda) kamuoyuna raporlama konusunda, kurumsal ortam genelinde siber sağlığı ve hazır bulunmayı ele almak amacıyla tarihi adımlar atmıştır. Bu tür adımlar türünün ilk örneğidir ve hem halka açık ABD şirketleri hem de dünya genelinde şirketler de önemli etkileri olabilir.

---

[7]. IANS, "Ukrayna, Güç Şebekesine Rusya Destekli Siber Saldırıyı Engelledi (Ukraine Foils Russia-backed Cyber Attack on Power Grid)," 14 Nisan 2022, https://www.nationalheraldindia.com/international/ukraine-foils-russia-backed-cyber-attack-on-power-grid.

[8]. Siber Güvenlik ve Altyapı Güvenliği Ajansı (CISA), "Kalkanlar Yukarı (Shields Up)," Erişim tarihi: 22 Nisan 2022, https://www.cisa.gov/shields-up.

[9]. Siber Güvenlik ve Altyapı Güvenliği Ajansı (CISA), "Rusya Siber Tehdidine Genel Bakış, Uyarılar ve Tavsiyeler (Russia Cyber Threat Overview and Advisories)," Ulusal Güvenlik Bakanlığı, Erişim tarihi: 22 Nisan 2022, https://www.cisa.gov/uscert/russia.

[10]. ABD Genel Hizmetler İdaresi (GSA), "14028 Sayılı Yürütme Emri: Ülkenin Siber Güvenliğinin İyileştirilmesi (Executive Order 14028: Improving the Nation's Cybersecurity)," 12 Mayıs 2021, https://www.gsa.gov/technology/technology-products-services/it-security/executive-order-14028-improving-the-nations-cybersecurity.

[11]. Siber Güvenlik ve Altyapı Güvenliği Ajansı (CISA), "Kalkanlar Yukarı (Shields Up)."

[12]. William Evanina, "Evanina Group CEO'su William R. Evanina'nın Çin Komünist Partisi'nin (CCP) Amerika'ya Yönelik Kapsamlı Tehdidine İlişkin Bir Duruşmada Senato Seçilmiş İstihbarat Komitesinin Karşısında Yaptığı Açıklama (Statement of William R. Evanina, CEO, The Evanina Group, Before the Senate Select Committee on Intelligence, at a Hearing Concerning the Comprehensive Threat to America Posed by the Communist Party of China (CCP)), The Evanina Group, 4 Ağustos 2021, https://www.intelligence.senate.gov/sites/default/files/documents/os-bevanina-080421.pdf.

Büyük Değişim

Siber olay raporlarına yönelik tarihi bir ilk adım

Teklifler

İki aylık bir süre içinde, SEC işletme sektöründe siber güvenliğe yönelik uzun zamandır beklenen iki teklif açıklamıştır. Şubat 2022'de yapılan birinci teklif[13] kayıtlı yatırım danışmanlarına, kayıtlı yatırım şirketlerine ve iş geliştirme şirketleri veya fonlarına odaklanmaktadır. Teklif edilen kural tahtında, danışmanların ve fonların aşağıdakileri yapması gerekecektir:

- Danışmanlık müşterilerine ve fon yatırımcılarına zarar verebilecek siber güvenlik risklerini ele almak için tasarlanan yazılı siber güvenlik politika ve prosedürlerini benimsemek ve uygulamak.
- Danışmanı veya onun fon veya özel fon müşterilerini etkileyen önemli siber güvenlik olaylarını yeni bir gizli formda SEC'e rapor etmek.
- Son iki mali yılda meydana gelen siber güvenlik risklerini ve önemli siber güvenlik olaylarını broşürlerinde ve izahnamelerinde kamuya açıklamak.

İlave olarak, bu teklif SEC teftiş ve yürütme kabiliyetlerini kolaylaştırmaya yardımcı olmanın yanı sıra, danışmanlar ve fonlar için siber güvenlikle ilgili bilgilerin kullanılabilirliğini iyileştirmek için tasarlanan yeni kayıt tutma şartları ortaya koymaktadır.

SEC Başkanı Gary Gensler bir basın bildirisinde[14] "Siber risk, SEC'in üç bölümden oluşan misyonunun her bir bölümüyle ve özellikle de yatırımcıları koruma ve piyasaları düzenli tutma amaçlarımızla ilgilidir. Teklif edilen kurallar ve değişiklikler, siber güvenlik hazırlığını geliştirmek için tasarlanmıştır ve yatırımcıların danışman ve fonların siber güvenlik tehdit ve saldırılarına karşı dayanıklı olduğuna ilişkin güvenini artırabilir," demiştir.

Bu kurallar denetlenen kuruluşların siber güvenlik risklerini nasıl yönetmesi ve siber güvenlik olaylarını nasıl raporlaması gerektiğine ilişkin SEC beklentilerini — dolaylı olarak da olsa — yansıtırken, ikinci teklif bu tür beklentileri açıkça ortaya koymaktadır. Tüm halka açık şirketlere yönelik olan ve Mart 2022'de çıkartılan ikinci teklif[15], "1934 tarihli Menkul Kıymetler Borsası Kanununun raporlama şartlarına tâbi olan halka açık şirketlerin siber güvenlik risk yönetimi, stratejisi, yönetişimine ilişkin açıklamaları ve siber güvenlik olay raporlamasını geliştirmeyi ve standart hale getirmeyi" amaçlamaktadır. Bu amaçla, yeni kurallar halka açık şirketlerin aşağıdakilerle ilgili açıklama ve raporları sunmasını gerektirecektir:

- Şirketin siber güvenlik risklerini tanımlayacak ve yönetecek politika ve prosedürleri. Kurallara aşağıda sayılanlar da dâhil olmak üzere raporlamaya tâbi olabilecek kapsamlı ancak detaylı olmayan bir risk yönetimi stratejileri, politikaları ve prosedürleri listesi de dâhildir:
    - Kayıt yapanın siber güvenlik risk değerlendirme programı olup olmadığı.
    - Kayıt yapanın herhangi bir siber güvenlik risk değerlendirme programıyla bağlantılı olarak değerlendirenler, danışmanlar, denetçiler veya diğer üçüncü taraflarla çalışıp çalışmadığı.

[13]. ABD Menkul Kıymetler ve Borsalar Komisyonu (SEC), "Yatırım Danışmanları, Kayıtlı Yatırım Şirketleri ve İş Geliştirme Şirketleri için Siber Güvenlik Risk Yönetimi (Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies)," 9 Şubat 2022, https://www.sec.gov/rules/proposed/2022/33-11028.pdf.
[14]. ABD Menkul Kıymetler ve Borsalar Komisyonu (SEC), "SEC, Kayıtlı Yatırım Danışmanları ve Fonlar için Siber Güvenlik Risk Yönetimi Kuralları ve Değişiklikleri Teklif Ediyor (SEC Proposes Cybersecurity Risk Management Rules and Amendments for Registered Investment Advisers and Funds)," basin bildirisi, 9 Şubat 2022, https://www.sec.gov/news/press-release/2022-20.
[15]. ABD Menkul Kıymetler ve Borsalar Komisyonu (SEC), "Siber Güvenlik Risk Yönetimi, Stratejisi, Yönetişimi ve Olay Raporlaması (Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure)," 9 Mart 2022, https://www.sec.gov/rules/proposed/2022/33-11038.pdf.

- Kayıt yapanın herhangi bir üçüncü taraf hizmet sağlayıcının kullanılmasıyla ilişkili siber güvenlik risklerini denetlemek ve tanımlamak için politika ve prosedürlerinin olup olmadığı.
- Kayıt yapanın siber güvenlik olaylarını önlemek, tespit etmek ve onların etkisini en aza indirmak için faaliyetler yürütüp yürütmediği.
- Kayıt yapanın siber güvenlik olayı durumunda iş sürekliliği, beklenmedik durum ve kurtarma planları olup olmadığı.
- Önceki siber güvenlik olaylarının kayıt yapanın yönetişim, politika ve prosedürlerinde veya teknolojilerinde yapılacak değişiklik için bilgi sağlayıp sağlamadığı.
- Siber güvenlikle ilgili risk ve olayların kayıt yapanın operasyonlarının sonuçlarını veya finansal durumunu etkileyip etkilemediği ya da etkilemesinin makul düzeyde muhtemel olup olmadığı.
- Siber güvenlik risklerinin kayıt yapanın iş stratejisinin, finansal planlamasının ve sermaye dağılımının bir parçası olarak kabul edilip edilmediği.

- Aşağıdakiler de dâhil olmak üzere yönetimin siber güvenlik politika ve prosedürlerinin uygulanmasındaki rolü:
  - Belirli bazı yönetim pozisyonları veya komitelerinin siber güvenlik risklerinin ölçülmesi ve yönetilmesinden sorumlu olup olmadığı.
  - Kayıt yapanın bilgi güvenliğinden sorumlu genel müdür yardımcısı veya denk bir pozisyonda olan birini atayıp atamadığı.
  - Bu kişi veya komitelerin siber güvenlik olaylarının önlenmesi, hafifletilmesi, tespit edilmesi ve düzeltilmesini izlemesi ve bu konularda bilgilendirilmesi için kullanılan süreçler.
  - Bu kişi veya komitelerin siber güvenlik risklerini yönetim kuruluna veya yönetim kurulunun bir komitesine rapor edip etmediği ve ayrıca, ne sıklıkta rapor ettiği.
  - Bütün kurulun, spesifik kurul üyelerinin veya bir kurul komitesinin siber güvenlik risklerinin denetlenmesinden sorumlu olup olmadığı.
  - Kurulun siber güvenlik riskleri hakkında bilgilendirilip bilgilendirilmediği ve bu tür riskler hakkında yaptığı tartışmaların sıklığı.
  - Kurulun veya kurul komitesinin siber güvenlik risklerini iş stratejisinin, risk yönetiminin ve finansal denetiminin bir parçası olarak görüp görmediği ve nasıl değerlendirdiği.

- Yönetim kurulunun siber güvenlik uzmanlığı – eğer varsa – ve siber güvenlik riskleri denetimi. Bu da aşağıdakiler hakkında bilgileri içermektedir:
  - Kurulun siber güvenlik konusunda çalışma tecrübesi olup olmadığı.
  - Kurulun siber güvenlik konusunda sertifikasyon veya derece alıp almadığı.
  - Kurulun siber güvenlik konusunda bilgisinin, becerisinin veya başka arka plan bilgisinin olup olmadığı.

İlave olarak, bu teklif halka açık şirketlerin siber güvenlik olaylarını, diğer herhangi bir planlanmamış önemli olay için zaten yapmaları gerektiği gibi, dört iş günü içerisinde rapor etmelerini gerektiren Form 8-K'de de değişiklik yapılmasını içermektedir. Bu tür raporlar aşağıda sayılanları içerecektir:

- Olayın ne zaman keşfedildiği ve sürekli devam edip etmediği.
- Olayın niteliği ve kapsamına ilişkin kısa tarif.
- Herhangi bir verinin çalınıp çalınmadığı, değiştirilip değiştirilmediği, erişilip erişilmediği veya herhangi başka bir yetkisiz amaç için kullanılıp kullanılmadığı.
- Olayın şirketin operasyonları üzerindeki etkisi.
- Şirketin olayı düzeltip düzeltmediği veya şu anda düzeltiyor olup olmadığı.

SEC'e göre, bu açıklama ve raporlar yatırımcılara "tutarlı, karşılaştırılabilir ve karar almada faydalı" bilgiler sağlayacaktır.

Gensler[16] “Günümüzde, siber güvenlik halka açık ihraççıların giderek daha fazla mücadele etmesi gereken yeni ortaya çıkan bir risktir. Ağlarımızın birbirine bağlılığı, kestirimci veri analitiğinin kullanılması ve veriye yönelik doyumsuz istek sadece hızlanmakta ve finansal hesaplarımızı, yatırımlarımızı ve özel bilgilerimizi riske atmaktadır. Yatırımcılar ihraççıların bu büyüyen riskleri nasıl yönettiği hakkında daha fazla bilgi almak istemektedir,” demiştir.

Tarihsel önemi

Birçok yönden, bu tarif edilen kuralların yapısı finansal koşullar ve faaliyet sonuçları (Sarbanes-Oxley), içeriden öğrenenlerin bilgisi ve kurumsal güçlü yönler, zayıf yönler, fırsatlar ve tehditler ile ilgili olanlar gibi diğer SEC raporlama kurallarını yansıtmaktadır. Bununla birlikte, siber güvenlik risklerinin bu tür raporlamalar gerektirecek noktaya çıkarılmasına yönelik ilave adımların atılması büyük ölçüde emsalsizdir.

The Augusta Group ve Parava Security Solutions şirketlerinin kurucu ortağı ve Cybersecurity Maturity Model Certification Europe şirketinin (CMMC Avrupa) kurucusu olan Andy Watkin-Child “ABD, muhtemelen, dünyada siber güvenliği düzenleyen ilk ve galiba tek ülkedir. ABD'deki şirketler, AB'nin Genel Veri Koruma Yönetmeliğine (GDPR) aşina olabilir ve bu teklifleri hızlı şekilde bir araya getirebilirler ancak veri koruma ve siber güvenlik iki farklı paradigmadır. Büyük bir fark söz konusudur ve muhtemelen – yabancı yüklenicilerin bile siber güvenlik zafiyetleri için Adalet Bakanlığı tarafından soruşturulmasıyla sonuçlanabilecek – Savunma Bakanlığı (DoD) Mali Yönetim Yönetmeliği dışında siber güvenlik alanında buna benzer başka bir uygulama yoktur,” demiştir

Watkin-Child, yeni kuralların öneminin yurt dışında nasıl güçlü dalgalanma etkileri olabileceğini de açıklamaktadır. “Ukrayna krizi, siber güvenliğin bir silah olduğunu kanıtlamıştır ve gerçekten de NATO 2016'dan beri bunu bir operasyon derecesi olarak görmektedir. Siber güvenlik, nükleer silahların yanı sıra saldırgan bir araçtır. Bir operasyon alanı olduğundan dolayı ulusal altyapılar için ciddi bir tehdit oluşturması bir sorundur. SEC teklifi ilk önce büyük oyuncuları — ticaret firmalarını — vuracaktır ancak SEC'in yetki alanı dışındaki kurumlara da uzanacağını umuyorum çünkü hem iş ortamı hem de federal ortam küresel düzeyde çok iç içe geçmiş durumda,” demiştir.

Watkin-Child, savaşta siber güvenliğin tek bir ordu bünyesinde düşünülemeyeceğini; eğer müttefiklerden biri savunmasızsa bu durumun tüm ortak operasyonları doğrudan etkileyeceğini söylemektedir. Siber güvenlik koruması halka açık — ve özel — şirketler için farklı değildir. Watkin-Child “Amerikan silah sistemleri hacklenemezken İngiliz sistemleri hacklenebiliyorsa korunmanın hiçbir anlamı yok. [ABD] başkanının NATO’yla diğer şeylerin yanı sıra ortak siber güvenlik standartları hakkında konuşmasının bir nedeni var. Yapılması gereken doğru şey budur çünkü Rusya gibi bir ülke iş sektörünü güç üreticilerine, örneğin suyunuza, elektriğinize, gazınıza, sağlık hizmetinize saldırmak için kullanırsa her şey bitmiş demektir,” demiştir.

Bu tür potansiyel sonuçların doğası gereği makro olduğu açıktır ancak kurum düzeyinde sonuçları da unutmamak önemlidir. Ayrıca, siber güvenlik açıklama ve raporlarına dâhil edilmesini garanti edebilecek kapsamlı listeleri gördüğünüzde hissedeceklerinize rağmen tüm sonuçlar olumsuz değildir.

Watkin-Child, “Elbette bu açıklama ve raporların yasal tarafları var. Bununla birlikte, tekliflerde de belirtildiği üzere, sadece SEC’e raporlama yapmıyorsunuz. İşinizi ve işletmenizi etkileyebilecek tüm piyasa katılımcılarına raporlama yapıyorsunuz. Yatırım topluluğu, kredi derecelendirme kuruluşları, sigorta şirketleri — tüm bu kurumlar, duruma göre siber güvenlikte ne kadar iyi olduğunuzu veya olmadığınızı SEC ile birlikte görecektir. Bu tür bir şeffaflık riske eşlik etse de aynı zamanda bir fırsatı da temsil etmektedir.”

[16]. Gary Gensler, “Zorunlu Siber Güvenlik Açıklamaları Teklifi Hakkında Beyan (Statement on Proposal for Mandatory Cybersecurity Disclosures),” ABD Menkul Kıymetler ve Borsalar Komisyonu (SEC), 9 Mart 2022, https://www.sec.gov/news/statement/gensler-cybersecurity-20220309.

İç Denetimin Rolü Tutarlıdır

Tanımla, değerlendir, rapor et

Araçlar mevcuttur

2002 Sarbanes-Oxley Kanunu (SOX), iç denetim fonksiyonlarının çalıştıkları kurumlara değer katması için ilave sorumluluklar getirmiş ve yeni fırsatların kapısını açmıştır. Gerçekten de kurumlar yeni mevzuata göre yön belirlerken birçoğu için iç denetim SOX uyumuyla eş anlamlı hale gelmiştir. Yeni SEC tekliflerinin doğası gereği siber güvenlik alanında da aynı şeyin olabileceğine düşünmek için sebepler vardır.

İlk bakışta, siber güvenlik alanının karmaşık yapısı nedeniyle bu en azından kısa vadeli bir imkânsızlık gibi görünebilir. Nabız anketi[17] katılımcılarına göre, siber güvenlik halka açık kurumlarda denetim planı tahsisinin ortalama olarak sadece %9'unu oluşturmaktadır; bu oran önceki üç yıl için kaydedilen %7 oranının üzerindedir ancak finansal raporlamaya ayrılan %35'in çok altındadır. Bu durumun, örneğin bütçe sınırlamaları, yeterli kaynakların olmaması ve bilgi veya tecrübe eksikliği gibi birden fazla sebebi olabilir.

Bununla birlikte, iç denetimin sağlayabileceği gerçek değer mutlaka siber güvenlik bilgisi yoluyla değil; riski tanımlama, riski rapor etme ve riski ele alacak kontrolleri değerlendirme bilgisiyle sağlanmaktadır. Gerçekten de bunlar SEC önerilerinin tek bir spesifik risk için vurgulamayı arzu ettiği şeylerdir.

Watkin-Child, "Bu önerilerin aslında siber güvenlikle ilgili olmadığını, siber güvenlik risk yönetimiyle ilgili olduğunu anlamak önemlidir. İnsanlar siber güvenliği düşündüklerinde kontrolleri uygulamayı ve bir şeyleri düzeltmeyi düşünmektedirler. SEC ise tamamen farklı bir şey, yani kurumların siber güvenlik risklerini değerlendirmelerini istemektedir. Kurumlardaki kurulların, hangi formda olursa olsun, siber güvenlik risk yönetim programlarını değerlendirmek ve onların denetimi konusunda güvence sağlamak için yönetişim yapılarına sahip olmalarını istemektedir," demiştir.

Caliber Home Loans, Inc. şirketinin iç denetim yöneticisi olan Manoj Satnaliwala, "SEC'in görmek istediği şey kurulların gözetim sorumluluğunu üstlenmesi ve geri kalanını güvence altına almasıdır. Aslında siber güvenlik standartlarında boşluk yoktur — NIST Siber Güvenlik Çerçevesi gibi kurumlara rehberlik edecek çerçeveler vardır. Asıl boşluk hesap verebilirliktedir – ki bu da hızlı bir şekilde sorumluluk tahterevallisi haline gelebilir," demiştir.

İç denetimin rolü bu tahterevallinin dengelenmesine yardımcı olabilir. Satnaliwala, "Kurulların ve yönetimin yardıma ihtiyacı var. İç denetim güvence yoluyla hesap verebilirlik sağlar ve kurum genelinde görünürlüğü arttırarak ortak risk sahipliğini teşvik eder. Risk farklıdır ancak iç denetimin rolü gerçekten tutarlıdır. Denetim fonksiyonları en baştan başlamak zorunda değildir ve her iç denetim görevinin siber güvenlik programının en can alıcı yerinde olmasını beklemek makul değildir ancak bu zorlukla ilgili olarak, görevlerde SEC önerilerine göz atıp 'SEC'in beklentileri nelerdir?' diye sormaktan biraz daha fazlasıdır. En azından bazı siber güvenlik kaynakları mevcut olduğu sürece, risklerin uygun şekilde kapsanmasını sağlayacak ince ayar yaklaşımları dışında ortalama iç denetim fonksiyonunda herhangi bir değişikliğe ihtiyaç olduğunu düşünmüyorum," demiştir.

Bununla birlikte, bu tür siber güvenlik kaynaklarına erişim sağlamak genellikle söylemesi kolay, yapması zor bir eylemdir. Siber güvenlik alanında herhangi bir derecede uzmanlık eğitim ve sertifikasyonlar aracılığıyla bir gecede geliştirilmeyecektir ve özellikle de maliyetli, yüksek talep gören yetenekleri istihdam etmek için bütçesi sınırlı olan küçük iç denetim fonksiyonları için, süreç odaklı uyumun ötesinde herhangi bir rolü yürütme seçenekleri sınırlıdır. Bu durumlarda, iç denetim bilgiye en iyi

[17]. The IIA, "2022 İç Denetimin Nabzı, Kuzey Amerika (2022 North American Pulse of Internal Audit),"

nereden erişim sağlayabileceği konusunda kapsamlı bir anlayışa sahip olmak zorundadır. Bu tür bir erişim aşağıda açıklanan şekillerde olabilir:

- **Kurumun kendi yetenek tabanında.** Daha geleneksel bir BT denetim kapasitesinde deneyimli olanlar, genellikle teknik siber güvenlik eğitimini nispeten hızlı şekilde tamamlayacak bilgi temeline sahiptir. İlave olarak, belirli bazı siber güvenlik temelleri değişim yönetimi, erişim kontrolleri, BT operasyonları ve felaketten kurtarma gibi alanların bünyesine dâhil edilebilir ve bu da uzun vadede dış kaynak kullanımını azaltabilir.
- **Hem ikinci hatla hem de güvenilir dış denetim fonksiyonlarıyla işbirliği yoluyla.** *Uluslararası İç Denetim Meslekî Uygulama Standartları*na (UMUÇ) uyum için iç denetimin bağımsızlığı ve objektifliğinin korunması zorunlu olsa da, BT gibi konuyla alakalı fonksiyonlarla daha fazla işbirliğine dayanan bir çalışma ilişkisi kurmak denetçilerin aksi takdirde elde edilmesi etmeleri zor veya maliyetli olabilecek teknik yetkinliklere dolaylı erişmesini sağlayabilir.

Varılan sonuçlar

Hazırlık zamanı

Kötü niyetli kişiler yaklaşımlarında yenilik yapmaya ve şirketler de onları engelleyecek yenilikleri yapmaya devam ettikçe siber güvenlik bir konu olarak her zaman gelişmektedir. Bununla birlikte, siber güvenliğin tarihi yazılmaya devam ederken 2022 yılı iş dünyasının genelinde görülen korkunç trendlere karşı koyma çabasında ulaşılan kilometre taşlarıyla hatırlanacaktır. Her iki SEC teklifinin de resmi kurallar yayınlanmadan önce yorumlar için 60 günlük süreyi tamamlaması zorunlu olmasına rağmen, halka açık şirketler ve onların iç denetim fonksiyonlarını sürpriz olacak çok az şey olmalıdır.

İç denetim, eğer daha önce yapmadıysa, kurumunun bir siber güvenlik stratejisinde hesaba katılması gereken varlıklarının tam kapsamlı envanterini çıkarmak için sahip olduğu zamanı kullanabilir ve kullanması gereklidir. İç denetçiler, bu bilgi olmadan, siber konularla ilişkili güncel kontrollerin, politikaların ve yönetişim stratejilerinin yeterli olup olmadığını değerlendirmekte zorlanacaktırlar. Bu tür değerlendirmeler sadece kurumsal güvenlik amaçları için değil, aslında bütün pazar topluluğu için önemlidir. Dünya her geçen gün birbirine daha da bağlanmaktadır ve bu da siber güvenlik gibi risklere yönelik sorumlulukların büyük ölçüde ortak olduğu anlamına gelmektedir. En nihayetinde, tarihin defalarca gösterdiği üzere, bir kurumun güvenliğinin kırılması bir başkasının güvenliğini çok gerçekçi bir şekilde etkileyebilir.

Zincir ancak en zayıf halkası kadar güçlüdür.

KISIM 2

Kritik Ortaklar — İç Denetim ve CISO

Uzmanlar Hakkında

Jerry Perullo

Jerry Perullo, büyüyen şirketlerin olgun siber güvenlik programlarını hızlı bir şekilde oluşturmasını sağlayan bir Siber Güvenlik Programı Strateji ve Yönetişim firması olan Adversarial Risk Management firmasının kurucusudur. Perullo, Adversarial firmasını kurmadan önce, 20 yıl boyunca New York Menkul Kıymetler Borsası da dâhil olmak üzere küresel bir kritik ekonomik altyapı ailesinde siber güvenlik programını inşa edip yönettikten sonra Intercontinental Exchange (NYSE:ICE) şirketinin Bilgi Güvenliğinden Sorumlu Genel Müdür Yardımcısı olarak emekli olmuştur. NACD Direktörlük Sertifikası® bulunan Perullo, ayrıca, 6 yıl boyunca Finansal Hizmetler Bilgi Paylaşım ve Analiz Merkezinin (FS-ISAC) Yönetim Kurulunda ve en son Başkan olarak görev yapmıştır. Perullo, Georgia Teknoloji Enstitüsünde Siber Güvenlik ve Gizlilik Okulunda Uygulama Öğretim Üyesi olarak ders vermekte ve deneyimlerini lifeafterCISO.com podcast'i aracılığıyla teknoloji risk liderleriyle paylaşmaktadır.

Hassan NK Khayal, CIA, CRMA, CFE

Hassan NK Khayal, Dubai'de yaşayan bir İç Denetim Yöneticisidir. Hassan, İç Denetçiler Enstitüsünün (IIA) dünya çapında 30 Yükselen Lider listesinde ilk 15'te yer almaktadır. Hassan'ın Orta Doğu Çalışmaları alanında BBA, MBA dereceleri ve bir sertifikası vardır. Hassan, aynı zamanda CIA, CRMA ve CFE'dir. Hassan'ın ayrıca Robotik Süreç Otomasyonu (RPA), Veri Analitiği, Nesnelerin İnterneti (IoT), Kalite Yönetimi, Sağlık ve Güvenlik, Çevre Yönetimi ve Risk Yönetimi alanlarında mesleki sertifikaları vardır.

Alan Maran

Alan, Chewy, Inc. şirketinde İç Denetim Yöneticisidir (İDY). Ocak 2019'dan beri bu şirkette çalışmaktadır. Bu rolde Çevik kurumsal risk değerlendirmeleri yapmak, Yönetimin desteklediği çeşitli faaliyetler için sürekli ve zamanında Danışmanlık desteği ve kurum için tanımlanan önemli risklere yönelik kontrollerin uygunluğu, şirket genelinde operasyonlar, kurumsal sistemler ve BT yönetişim, risk ve uyum (GRC) uyumu ve veri analitiği, siber güvenlik, veri gizliliğine daha fazla odaklanarak İç Denetim Ekibi üyelerinin gelişimine sürekli odaklanma konusunda Güvence sağlamak da dâhil olmak üzere İç Denetim Fonksiyonu için genel Stratejik ve Yürütme faaliyetlerinin gözetiminden sorumludur. Alan e-Ticaret, Fintech, Teknoloji ve Üretim Şirketlerinde 22 yılı aşan deneyime sahip olan ve öğrenme tutkusu devam eden deneyimli bir Denetim yöneticisidir. Chewy şirketine katılmadan önce, kariyerine Ernst & Young, LLC şirketinde başlayarak ilerici liderlik rolleri üstlenmiş ve ardından, çok uluslu Fortune 500 kurumlarında diğer çeşitli İç Denetim pozisyonlarında ilerlemiştir. MBA derecesi ve Washington Eyalet Üniversitesi'nden Finans Yüksek Lisansı vardır; Sertifikalı Suiistimal Denetçisidir (CFE); Sertifikalı Blockchain Uzmanıdır ve İç Denetçiler Enstitüsü'nün yerel Bölümlerine bağlıdır.

Srini Srinivasan, PMP, CBIP

Srini Srinivasan, Chewy, Inc. şirketinde Bilgi Güvenliği ve Verilerden Sorumlu Genel Müdür Yardımcısıdır. Srini, Güvenlik, Veri ve Kurumsal Sistemler Müdürü olarak işe girdiği Ekip 2019'dan beri bu şirkette çalışmaktadır. Bu rolde şirket genelinde bilgi güvenliği, veri ve analitik platformların yönetimi, kurumsal sistemler ve BT yönetişim, risk ve uyum (GRC) konularının gözetiminden sorumludur. Srini e-Ticaret, Bankacılık ve Finansal Hizmetler, Perakende ve Pazarlamayı kapsayan 25 yılı aşkın deneyime sahip deneyimli bir teknoloji yöneticisidir. Chewy şirketine katılmadan önce, Citizens Financial Group'ta liderlik rolleri üstlenmiştir. Bharathidasan Üniversitesi'nden Bilgisayar Bilimleri alanında yüksek lisans derecesi ve Bentley Üniversitesi'nden MBA derecesi vardır.

Giriş

Başarı açısından kritik siber güvenlik ortaklıkları

Siber güvenlik tüm kurumlar için en önemli riskler arasında olmaya devam etmektedir. Anketler, siber suçluların hassas verileri hacklemek için ya da eğitimsiz ve şüphelenmeyen kişileri hassas bilgileri ifşa etmeye veya kötü niyetli kişilerin onlara erişim sağlamasına izin vermeye ikna etmek için gösterdikleri bitmek tükenmez ve pişkin çabaları mütemadiyen yansıtmaktadır.

Örneğin, 2022 Verizon Veri İhlâli Soruşturmaları Raporu, 2021 yılında fidye yazılımıyla ilgili ihlâllerde %13 oranında – ki bu oran son beş yılın toplamından daha fazladır – şaşırtıcı bir artış olduğunu göstermektedir. Bununla birlikte, bu raporda, Verizon raporuna göre fidye yazılımı saldırılarının en başarılı yöntemlerinin hâlâ aynı olduğu gösterilmektedir — masaüstü paylaşımı ve uzaktan erişim yazılımının (%40) ve e-postanın (%35) kötüye kullanımı.[18]

IIA'nın yayınladığı yeni Siber Güvenlik Operasyonları Denetimi: Önleme ve Tespit Etme (GTAG) rehberi, kurumların siber güvenlik operasyonlarına ilişkin güvenceyi incelemesine ve önceliklendirmesine yardımcı olacak şekilde tasarlanmıştır. İç denetçilerin siber güvenlik operasyonlarını tanımlamasına, onun bileşenlerini belirlemesine, BT kontrol çerçevelerinin konuyla alakalı kontrol rehberliğini göz önünde bulundurmasına ve siber güvenlik operasyonlarının denetimine yönelik yaklaşımları anlamasına yardımcı olmayı amaçlamaktadır.

Siber güvenlik güvencesinin iyileştirilmesi konusunda bu rehberde yer almayan önemli unsurlardan biri, iç denetim müdürleri ve bilgi güvenliğinden sorumlu genel müdür yardımcıları (CISO'lar) arasında sağlıklı bir ilişki kurulmasıdır. Bu potansiyel olarak simbiyotik ilişki, hem iç denetim ve bilgi güvenliğinin çerçeveler, riskler ve kontroller konusunda uyumlu hale getirilmesine yardımcı olabilir hem de kapsamı genişleyen siber güvenlik risk profilinin yönetilmesini destekler.

Bu Küresel Bilgi Özeti iç denetim ve bilgi güvenliği yöneticileri arasındaki güçlü bir ilişkinin faydalarını inceler; iç denetim bağımsızlığını sağlarken bu tür ilişkileri kurmanın ve beslemenin yollarını inceler ve ayrıca, bu ortaklıkların kuruma nasıl değer katabileceğini değerlendirir.

18. "2022 Verizon Veri İhlâli Araştırmaları Raporundan 3 Çıkarım (3 Takeaways From the 2022 Verizon Data Breach Investigations Report)," J. Mack, Rapid7, 31 Mayıs 2022, https://www.rapid7.com/blog/post/2022/05/31/3-takeaways-from-the-2022-verizon-data-breach-investigations-report/.

Kolektif Siber Güvenlik

Siber risk kurum çapında yaklaşım gerektirir

Siber suçluların yaptıkları planların her yıl daha da karmaşıklaşıp çoğaldığı görüldükçe siber güvenlik büyüyen ve gelişen bir risk alanı olmaya devam etmektedir. Kurumların siber saldırılara karşı savunmasız kaldığını gösterecek bol miktarda istatistik veri vardır. Aynı zamanda, çeşitli endüstrilerde faaliyet gösteren kurumların bir yandan performansı ve kârlılığı iyileştirecek yeni teknolojiler kullanırken diğer yandan ağırlıklı olarak verilerin toplanmasına, yönetilmesine, analiz edilmesine ve kullanılmasına dayanan veri odaklı iş stratejilerini benimsemelerine yönelik baskı artmaktadır.

Diğer önemli risk alanlarında olduğu gibi, siber riskin de kurum genelinde anlaşılması ve yönetilmesi gereklidir. Yine de, sigorta brokerliği ve risk yönetimi şirketi Marsh ve Microsoft'un hazırladığı "Siber Dirençlilik Durumu" raporuna göre, siber güvenliği yönetmek için kurumsal bir yaklaşım benimseyen kurumların sayısı azdır. Siber risk konusunda karar verici 600'den fazla kişinin katıldığı bir anketi[19] esas alan bu raporda, her 10 kurumdan sadece 4 tanesinin siber risk planları yaparken yasal, kurumsal planlama, finans, operasyonlar veya tedarik zinciri yönetimiyle ilgilendiği görülmüştür.[20]

Bu rapora göre "Çoğu şirketin siber riske karşı kurum çapında bir yaklaşım, yani özünde geniş tabanlı iletişimle ilgili olan ve siber dirençlilik yolculuklarında önemli kararlar aldıkları anlarda paydaşlar arasında işbirliğini ve uyumu teşvik eden bir yaklaşım benimsememiş olması güven duygusunu kısıtlayan şeylerden biridir."[21]

Bu raporda tanımlanan anahtar risk trendleri arasında:

"Her kurum siber saldırı bekleyebileceğinden dolayı, sadece olayların önlenmesine kıyasla siber dirençlilik inşa etmek için siber güvenlik tedbirleri, sigorta, veri ve analitik ve olay müdahale planları da dâhil olmak üzere sibere özgü kurum çapında amaçların uyumlu olması gereklidir."[22]

İç denetim yöneticileri, kurum çapında etkili bir yaklaşımı desteklemek için CISO'larla ilişki kurmak ve var olan ilişkileri ilerletmek suretiyle önemli ölçüde katkıda bulunabilirler. Bu tür ilişkiler karşılıklı anlayış ve saygının yanı sıra ortak amaçlara dayanmak zorundadır.

NYSE'nin ana şirketi Intercontinental Exchange'den (NYSE:ICE) resmi olarak emekli CISO ve Adversarial Risk Management kurucusu olan Jerry Perullo, bilgi güvenliği ve iç denetim rolleriyle ilgili iletişimin zayıf olmasının ya da bunların açık ve net bir şekilde anlaşılmamasının siber güvenlik konusunda uyumu zedeleyebileceğini söylemiştir. Bunun aksine, iç denetim ve bilgi güvenliği yöneticileri arasında kurulan iyi bir ilişki amaçların, stratejinin, operasyonların ve politikaların daha derinden anlaşılmasını sağlayan kapıyı açmaktadır ve bu da iç denetimi — ve dolayısıyla onun bulgu ve tavsiyelerini — siber risk liderleri, icracı yönetim ve kurul için daha alakalı hale getirebilir, demiştir. Dahası, iç denetim ve bilgi güvenliği ekip arasında kurulan güçlü bir ilişki, her alanın kritik misyonu ve bu iki alanın genel siber güvenliği nasıl desteklediği hakkındaki bilgilerin kapsamını genişletmektedir.

Perullo "Günün sonunda, iç denetim bilgi güvenliği hakkında eğitilmek ister. Bunu yapmanın birçok yolu vardır ancak (bilgi güvenliği) ekibinin kendisinden öğrenmek gibisi yoktur," demiştir.

Perullo, start-up'larla yaptığı danışmanlık çalışmalarında genellikle siber güvenliğe yönelik yönetişim programlarını ayarlayarak başlamaktadır. Bu da tipik olarak icracı yönetimi, finans, hukuk ve bilgi güvenliği bölümlerini içerebilen bir çapraz fonksiyonel yönetişim komitesinin oluşturulmasını gerektirmektedir. Ayrıca, gözlemci olarak kıdemli iç denetim yöneticilerini de dâhil ettiklerini söylemiştir.

19. "2022 Marsh ve Microsoft Siber Risk Anketi (2022 Marsh and Microsoft Cyber Risk Survey)"
20. "Siber Dirençlilik Durumu (The state of cyber resilience)," Marsh Microsoft, 2022, https://www.marsh.com/us/services/cyber-risk/insights/the-state-of-cyber-resilience.html?utm_source=forbes&utm_medium=referral-link&utm_campaign=gl-cyber-risk-2022-the-state-of-cyber-resilience.
21. ibid.
22. ibid.

Başarının Beş Anahtarı

Sağlam bir iç denetim, CISO ilişkisinin faydaları

İç denetim ve CISO'lar iyi kurulmuş bir ortaklığın sayısız faydasını tanımlamaktadır. Bu tür ortaklıkların detayları ve karmaşıklığı kurumun büyüklüğüne, her endüstrideki düzenleme düzeyine veya bir kurumun siber güvenlik risk profiline bağlı olarak değişebilir. Bununla birlikte, kurumun büyüklüğü veya faaliyet gösterdiği endüstri ne olursa olsun, işbirliği ve dayanışmanın açık ve net faydalar yaratabileceği beş alan vardır.

Kurumun siber risk profili üzerinde anlaşma ve uyum

Risk profili, kurumun karşı karşıya kaldığı tehdit türlerinin nicel analizidir. Siber güvenlik açısından, bu tür bir analiz varlıkları ve siber riskleri tanımlar; bu riskleri yönetmek için tasarlanan politika ve uygulamaları inceler ve mevcut olabilecek her türlü güvenlik zafiyetini anlamaya çalışır. İç denetimin siber risk profilini anlaması, hem kurumun siber güvenliğe karşı genel yaklaşımını destekleyen hem de iç denetimin bu kritik alanda tesirini iyileştirebilen bir denetim planı oluşturması için temel sağlamaktadır.

Chewy, Inc. şirketinde iç denetim yöneticisi olan Alan Maran, evcil hayvan maması ve evcil hayvanlarla ilgili diğer ürünlerin çevrimiçi perakendecisinin halka açılmasından beri geçen üç yıl içinde kurumun CISO'su Srini Srinivasan ile güçlü bir ilişki geliştirmiştir. Srinivasan, şirketin siber risk profilini NIST Siber Güvenlik Çerçevesi temelinde kapsamlı şekilde değerlendirmek ve ölçmek için bilgi güvenliği bölümünün iç denetim, hukuk bölümü ve diğer paydaşlar ile işbirliği yaptığını söylemiştir.

Srinivasan "Bu bizim taban çizgimiz, dayanağımız. Daha sonra, siber güvenlik ve yönetişim için üç yıllık yol haritamızı belirledik ve onu yaptığımız siber güvenlik çerçevesi değerlendirmesine dayanarak uyarladık ve geliştirdik. Şu anda, söz konusu fırsat alanlarında ilerleme kaydedip kaydetmediğimizi görmek ve genel risk puanlarımızın kriterleri karşılayıp karşılamadığını değerlendirmek için her yıl değerlendirmeler yapmaktayız," demiştir.

Başlangıçtan itibaren iç denetimi de sürece dâhil eden bu işbirlikçi yaklaşım, Chewy şirketinin genel siber güvenlik duruşunu sürekli olarak iyileştirme amacını iç denetim güvence ve danışmanlık hizmetleriyle birleştiren ortak bir stratejiye olanak tanımıştır.

Maran "'BT ve güvenliği her zaman denetlemem gerekiyor' şeklinde bir bakış açımız yok. Aynı zamanda destek de sağlamalıyız. İç denetim açısından bakıldığında, bütün bir strateji geliştirilirken Srini ve ekibini destekleme zihniyeti güçlü olan bir ortak olduğumuzu görüyoruz," demiştir.

Bilgi güvenliği ve bağımsız güvence unsurlarının yeni projelerin bünyesine en baştan dâhil edilmesi, bu işbirliğinin ilave faydalarından biridir. Başka bir deyişle, bilgi güvenliği, iç denetim ve yönetişim kontrolleri artık sonradan akla gelen şeyler değildir, demiştir Srinivasan.

Srinivasan "Yaptığımız şey, proje girişimleri başlarken her iki ekibimizin de sürece dâhil olması ve mühendislik ekipleri, ürün ekipleri, iş ekipleri ile ortaklık kurmasıdır. . . Güvenlik açısından dikkate alınması gerekenler nelerdir? En iyi uygulamaları takip ediyor muyuz?" demiştir.

Srinivasan, bu yaklaşımın proje geliştikçe uygun süreç ve kontroller inşa etmek suretiyle siber riskleri tanımlamaya, en aza indirmeye ve mümkünse elimine etmeye yardımcı olduğunu söylemiştir. "Dolayısıyla, proje hayata geçtiğinde, her iki ekibimiz için de çok kolay oluyor çünkü sağlam bir anlayışımız var. Denetim kontrol değerlendirmelerini ya da erişim gözden geçirmelerini veya yönetişim kontrollerini takip ettiğimizde zaman çok daha fazla içgörü elde etmekteyiz," demiştir.

Rolleri anlama

Chewy şirketinin nispeten yeni bir halka açık şirket olmasının Maran ve Srinivasan'ın kurduğu ilişkiye büyük ölçüde yardımcı olmuştur çünkü bu durum ilişkinin sıfırdan şekillendirilmesi için fırsat sağlamıştır. Bu, aynı zamanda, Maran, Srinivasan ve onların ekipleri arasında açık ve sık iletişim beklentisi de oluşturmuştur.

Srinivasan “Önemli paydaşlar arasında bu şeffaflık ve güveni yaratmanın ideal yollarından biriydi; dolayısıyla bu fırsatın kaçmasını istemedik,” demiştir.

Bu, asla anlaşmazlıkların olmadığı anlamına gelmez. Bununla birlikte, çatışmalar doğduğunda, bu ilişkinin onları tartışmayı ve her iki tarafa da hizmet eden bir çözüm bulmayı kolaylaştırdığını söylemiştir Srinivasan.

Srinivasan “İç denetimden bir şeyler saklamamın bana hiçbir faydası yok. Yaptıklarımız hakkında ne kadar fazla bilgi sahibi olurlarsa… yaptıklarımızı o kadar çok takdir ederler. Aynı şekilde, iç denetimin de ‘Yakaladık seni’ tarzında bir bakışı olduğunu düşünmüyorum,” demiştir.

En nihayetinde, işbirlikçi yaklaşım iç denetimin eksikliklerin erkenden tespit edilip ele alınabildiği bir sürecin parçası olduğu çevik bir tarzda faaliyet göstermeye olanak tanımaktadır, demiştir Srinivasan.

Maran, samimi etkileşimin rollere ilişkin karşılıklı anlayışı doğruladığını ve güçlendirdiğini eklemektedir.

“Srini her şeyi bildiğimizi varsaymıyor ancak aynı zamanda, endişelerimize ve bakış açımıza saygı duyuyor,” demiştir.

Anlamlılık

Kritik konularda doğru zamanda güvence anlayışları ve bulguları sağlamak, iç denetimin herhangi bir risk alanında ama özellikle de siber güvenlik alanında karşılaştığı en büyük zorluklarından biridir. Sürekli gelişen ve hızlı ilerleyen bu risk güvencenin ilgili ve zamanında olmasını gerektirir.

Perullo, kurumun siber güvenlik misyonuyla uyumlu olmayan iç denetim görevlerinin ve onlarla ilgili tavsiyelerin faydadan çok zararı olacağı konusunda uyarmıştır. Bunlar, özellikle de iç denetimin emin olmadığı durumlarda iç denetimin ne görmek istediği konusunda bilgi güvenliğinde kafa karışıklığı yaratabilir.

Perullo “Başlangıçta iç denetimin ne görmek istediğine ilişkin iyi bir fikri olmayabilir. Denetimlerin misyonla uyumlu olmasını sağlamak için denetim öncesi süreçte işbirliği yapmak ve siber yönetişim sürecini gözlemlemek daha iyidir,” demiştir.

Siber uzmanlığa sahip bir iç denetim danışmanı olan Hassan Khayal, bu alanın iç denetimin eleştiriye özellikle açık olduğu bir alan olduğunu belirtmiştir. Genellikle, iç denetçiler iç denetim bağımsızlığını korumak bahanesiyle BT veya bilgi güvenliği ekiplerinde çalışanları tanımaya ve konu hakkında daha fazla şey öğrenmeye direnmektedirler.

“İlk görevlerimde utanıp sıkılmadan BT personeline gidip ‘Her şeyden çok sizden bir şeyler öğrenmek için buradayım’ derdim. Süreci anlayan veya teknik anlayışı olanları seçer ve öğle yemeğinde dostça sohbet ederdim; böylece yaptıklarının en kritik ve can alıcı parçalarını tam olarak öğrenmiş olurdum.”

Khayal, bu eğitim sürecinin iç denetçinin kurumun siber güvenlik olgunluğunu anlamasına da yardım ettiğini ve bunun konuyla alakalı tavsiyeler sunmanın kritik unsuru olduğunu söylemiştir.

Khayal “Eğer küçük ile orta ölçekli kurumlardan ya da hatta halka açık olmayan daha büyük bir kurumdan bahsediyorsak yapabileceğiniz veya yapmanız gereken çok şey vardır. Belirli bir noktada, tavsiyeler çok saldırgan olabilir ve dolayısıyla sunduğunuz tavsiyeler gerçekçi değildir,” demiştir.

İç denetim ve bilgi güvenliği ekipleri arasında güçlü bir ilişki kurmak, konuyla alakasız veya yanlış yola sapmış denetim görevleri ve tavsiyelerinin olasılığını düşürmektedir. Bu fayda, Chewy şirketinde teyit edilmiştir.

Srinivasan “Alan'ın ekibi ve Alan'ın kendisi teknoloji perspektifinden genel güvenlik stratejimizin ne olduğu, bu konuda ne yaptığımız ve en önemli risklerimizden bazılarının neler olduğu konusunda oldukça bilgilidir. Bu nedenle, risk derecelendirmeleri ve dâhili kabiliyetlerimiz arasında büyük bir fark yoktur. Bu durum, Chewy şirketinde hem ekibimizin veya ekip üyelerimizin hem de liderlik ekibimizin genel bilgisini arttırmak amacıyla daha iyi bir iş çıkarmamıza yardımcı olmaya devam edecektir,” demiştir.

Yönetim kuruluna ve icracı yönetime raporlama

Chewy şirketinin kurumsal kültürü, açık iletişimle desteklenen daha geniş kapsamlı bir risk görüşü sağlamaktadır. Maran ve Srinivasan, aralarındaki işbirliği ve onun sağladığı faydalar konusunda paydaşları — icracı yönetim ve kurul — eğitme rollerini üstlenmişlerdir.

“Birçok kurumda, insanlar ‘Bu konu BT güvenliğiyle ilgili, yani CISO’yla konuşacağız ve CISO ilgilenecek’ gibi izole ve etkileşimsiz bir yaklaşım benimsiyor. Ancak entegre risk yönetimi veya kurumsal risk yönetimi perspektifinde, şirket için gördüğümüz herhangi bir risk bütün kurum için geri döner,” demiştir Maran. “Siber saldırı operasyonlarınızı, çıktılarınızı ve finans raporlarınızı etkileyebilir. Srini, liderleri neler yaptığımız ve hafiflettiğimiz riskler hakkında eğitme konusunda da iyi bir iş çıkartmıştır. Dolayısıyla, o perspektiften bu bir işbirliğidir.”

Bu, değişen risk ve düzenleyici siber ortamlara zamanında ve çevik karşılıklar verme anlamına da gelmektedir. Örneğin, Maran ve Srinivasan’ın kurumun 2022 yılının ilk çeyreğinde açıklanan ve ABD Menkul Kıymetler ve Borsa Komisyonu tarafından teklif edilen siber güvenlik raporlama kurallarına karşılık verebileceğine yönelik güveni artmaktadır.

Bu işbirliği bilgi güvenliği ve iç denetimin de ötesine geçmektedir. Srinivasan “İşbirliği kurumun güvenliğiyle sınırlı değil. Muhasebe ekibi ve hukuk ekibi de dâhil olmak üzere benzer ortaklıklar kurduğumuz başka önemli paydaşlar da vardır. Bence bu tür şeffaf ilişkilerin kurulması, bu gelişen düzenlemeler ve ilave şartlar ortaya çıktığında çok iyi hazırlanmamızı sağlıyor.”

Chewy şirketinde liderler tutarlı ve birleşik mesajlaşmadan fayda sağlamaktadır; öte yandan, Khayal liderlerin kurumun siber güvenlik durumu ve ihtiyaçlarından haberdar olmaması durumunda önemli tehlikeler doğabileceği uyarısında bulunmaktadır. Liderlerin BT ve siber güvenlik hakkında bilgi sahibi ve eğitimli olmaması halinde bu alanların hızlı bir şekilde sadece maliyet merkezinden ibaret alanlar olarak görülebileceğini belirtmiştir. Khayal, iç denetimin bilgi güvenliğini anlamaktan kaçınması durumunda bu alanda değerli ve ilgili güvence sunma olasılığının daha düşük olduğunu söylemiştir. Bu da icracı yönetim ve kurulun siber güvenlik hakkındaki görüşlerini etkilemektedir.

Bağımsızlığı koruma ve ona saygı duyma

Sertifikalı bilgi sistemleri denetçisi (CISA) olmak için çalışan Khayal, bu sertifikayı alma konusundaki kararlılığının BT ve bilgi güvenliği uzmanları arasında güvenilirliğini şimdiden arttırdığını söylemiştir. Ayrıca, bu alandaki iş arkadaşlarıyla onların seviyesinde etkileşim kurmasına olanak tanımaktadır ve bu da sadece denetim görevini yürütürken iletişim kuran bir denetçi için çok ileri düzey veya kompleks görülebilecek bilgileri gönüllü olarak vermelerini daha olası kılmaktadır. Dahası, bu etkileşimi bağımsız ve objektif bir denetim görevi yürütme becerisi için bir tehdit olarak görmemektedir.

“Sonuçta işyerindesiniz,” demiştir. “Şahsen, denetçilere bağımsız olmalarını söylediğimizde ‘İşyerinde arkadaş edinemezsin; öğle yemeğini her zaman tek başına yemen gerekir,’ demediğimizi düşünüyorum.’”

Khayal, bu yaklaşımı kurumun tüm alanların benimsediğini belirtmiştir. Bilgisayar bölümü personeliyle Linux hakkında ya da pazarlama bölümü personeliyle sosyal medya hakkında konuşacaktır.

Khayal “Bir yandan ilişkileri sürdürürken diğer yandan kendinizi mesleki olarak geliştirmeniz için iyi bir fırsat. Tıpkı denetim müşterilerimize veya denetlenenlere ‘Süreç ve işlemlere bakıyoruz; insanları yakalamaya çalışmıyoruz,’ dememiz gibi. Dolayısıyla, insanları öğle yemeğine çıkardığınızda söz konusu süreç veya işlemi de yemeğe çıkarmıyorsunuz,” demiştir.

Maran, Chewy şirketinde Maran ve Srinivasan arasındaki yakın iş ilişkinin bağımsız doğrulamaya duyulan ihtiyacın karşılıklı olarak anlaşılmasını desteklediğini belirtmiştir.

“Mesleğimizin doğası güvenmek ama aynı zamanda doğrulamaktır. Objektiflik açısından bunu yapmakla yükümlüyüm,” demiştir. “Bundan dolayı, evet, test etmiş olduğumuz belirli, özelikle de değişen şeylere güveniyoruz. Çoğu durumda, değiştirmediğimiz şeyleri doğruluyoruz. Bununla birlikte, yönetimin verdiği bilgilerin bütünlüğünü test etmeye de devam ediyorum. Bir raporun sadece görünüşüne bakmıyoruz; tam ve doğru olmasını sağlamak amacıyla onlarla aynı sonuçları aldığımızdan emin olmak için raporun kaynağına dönüyoruz.”

Maran, en nihayetinde, birbirinin kurumdaki rolünü anlamanın işleri kolaylaştırdığını belirtmiştir.

“Burada bir anlaşma söz konusudur. İşte yapmam gerekenler. İşte üst yönetime — kurula, paydaşlara ve denetim komitesine sunmam gereken güvence,” demiştir. “Yıl boyunca yapacağımız denetimler konusunda uyum sağlıyoruz. Kapsam üzerinde uyum sağlıyoruz. Evet, bazen bakış açımız ve birbirimizin bu bakış açısını nasıl gördüğü hakkında konuşuyoruz ancak güvence sağlamamız gereken risk alanlarında nadiren anlaşmazlık yaşıyoruz.”

Srinivasan, siber güvenliğe karşı veri temelli bir yaklaşıma odaklanmanın bilgi güvenliği ve iç denetim arasında maddi olgular üzerinde bir anlaşma olacağını varsaydığını eklemektedir.

“Herhangi bir anlaşmazlık olursa üzerinde çalışmamız ve aynı maddi olgular setine ulaşmamız gereklidir,” demiştir. “Sonrasında, bireysel olarak 'Tamam, bunun orta derecede kritik veya yüksek kritik veya düşük kritik olduğunu hissediyorum,' diyebileceğimiz bir seviyede öznelliğe sahip olabilirsiniz. Bunun, ortak bir referans çerçevesi olmadan kafa patlatmaktansa sağlıklı bir tartışma ve netice sağladığını düşünüyorum.”

Değer Katma

Siber güvenlik dirençliliğini arttırma

Srinivasan, yaklaşımının başından beri Chewy şirketinin misyonuna sadık kalmak olduğunu söylemiştir. Bu da üç şeyi başarmak anlamına geliyordu: Şirketin dâhili işletme ilkelerini uygulamak, bilgi güvenliği ve iç denetim arasında uyumu sağlamak ve şeffaflık yoluyla güven inşa etmek.

“Bence uzun bir yol katettik ve bu ilerleme, ekip üyeleri ve liderlerin birbirlerini haberdar etmek ve bilgilendirmek yapması gerekenler açısından karşılığını fazlasıyla vermektedir,” demiştir.

Daha önce belirtildiği üzere, yüksek derecede iletişim, işbirliği ve yardımlaşma iç denetimi siber güvenlik sürecine sürekli olarak dâhil eden çevik bir yaklaşımı desteklemektedir. Srinivasan sürdürülebilirliğe odaklanmanın artması, tedarik zincirinde dikkate alınması gerekenler, piyasa koşulları, jeopolitik gelişmeler ve daha fazlası gibi başlıca kuvvetlerin siber güvenlik ve onunla ilgili güvence için esnek yaklaşımlar gerektirdiğini not etmektedir.

“Bence bu bizi uyanık, çevik, duyarlı ve ilgili olmaya zorluyor,” demiştir. “Daha uzun teslim süreleri olan klasik şelale yaklaşımıyla devam edersek fırsatı kaçıracağız. Bu nedenle, sahip olduğumuz etkileşim seviyesinden memnunum.”

Bilgiyi arttırma

Bu iki ekibin birbirinin aynı amaca ulaşmak – kurumu siber güvenli tutmak – için benimsediği yaklaşımı anlama ve takdir etme konusunda ilerlemesi ve büyümesi ortaklığın özündeki faydalardan bir diğeridir.

“'Buna baktık mı? Bunu hesaba kattın mı? Bu risk analizine bakış açım işte böyle – seninkiyle uyumlu mu?' gibi sorularla birbirimizin teknik bilgisini her zaman kontrol ediyoruz,” demiştir Maran. “Dolayısıyla, en başından itibaren nereye bakacağımızı düşünüyoruz ve Srini, başlangıç toplantılarına katılıyor. Biz denetime başlamadan önce de görüşmelere katılır. Gerçekten hiçbir sürpriz söz konusu değildir.”

Bununla birlikte, gerçek katma değer, denetim görevlerinin yürütülmesinden ve iç denetimin doğrudan doğruya BT ve güvenlik personeliyle ilgilenmesinden sonra yapılan işbirliğinden kaynaklanmaktadır.

Maran “Kariyer gelişim perspektifinden bakıldığında, özellikle de BT ve siber güvenlik zihniyetiyle aslında gerçekten cazip ve tatmin edicidir çünkü sadece kutuları işaretleyip ‘Bunu yaptınız mı?’ diye sormaktan çok daha fazlasını görüyorsunuz,” demiştir. “Dahası da var. Yorum da söz konusu; doğru olması gereken teknik uzmanlık var; bu yüzden bence burası ekibimin çok şey öğrendiği bir yer.”

Varılan Sonuçlar

İç denetim ve bilgi güvenliği arasında kurulan sağlıklı bir ilişki, kurumun siber risk profilinin uyumlu hale getirilmesi ve anlaşılması başta olmak üzere, güvenlik zafiyetleri ve fırsatlardan olgunluk ve sızma testine kadar kuruma birden fazla fayda sağlamaktadır.

Dahası, kurumun siber olaylara, siber güvenliği etkileyen faktörlerdeki değişikliklere ya da gelişen düzenleyici ortama karşılık vermesi gerektiğinde sağlam bir ilişki direnci ve çevikliği arttırabilir. Tepe pozisyondaki kişilere ve kurula siber güvenlik riskleri, ihtiyaçları, öncelikleri ve sağlığı hakkında tutarlı ve birleşik mesajlar verilmesine yardımcı olmaktadır. Her iki taraf da roller, yaklaşımlar ve görevler hakkında daha derin bir anlayış ve takdir kazandığında iç denetim bağımsızlığı başarıyla korunabilir ve hatta arttırabilir. Son olarak, denetim yöneticileri ve CISO'lar arasında kurulan sağlam bir ilişki siber güvenliğe yönelik kurum çapında yaklaşımı destekleyerek BT güvenliğini güçlendirebilir.

Maran "Zihniyet, sadece denetlemekten — 'Gelip değerlendirmem ve anlamlı gözlemler yapmam gerekiyor — 'Bu benim şirketim; bu gerçekten önemsediğim bir konu ve ekibin başarılı olmasına bu şekilde yardımcı olacağım,' demeye doğru değişmektedir," demiştir.

KISIM 3

Siber Olay Müdahale ve Kurtarma

Uzmanlar Hakkında

Brian Tremblay

Brian Tremblay, Onapsis şirketinde Uyum Uygulamasına liderlik etmektedir; burada, BT genel kontrolleri ve Sarbanes-Oxley (SOX) ve Genel Veri Koruma Yönetmeliği (GDPR) gibi düzenleme ve uyum konularıyla ilişkili uyum, siber güvenlik ve iş sürekliliğinin örtüştüğü noktaların artmasına bağlı olarak doğan zorluk ve fırsatları anlama ve yön bulmada müşterilere yardımcı olmaktan sorumludur. Onapsis şirketinden önce, yüksek teknolojili yarı iletken şirketi Acacia Communications'ta İDY olarak çalışıyordu. İç denetim fonksiyonunu oluşturmaya ve tüm faaliyetlerine liderlik etmeye ilave olarak, kurumun halka açılmak için hazırlanmasına (SOX'u uygulama dâhil) yardım etmiş ve kurumsal risk yönetimini (KRY) uygulamasını kolaylaştırmıştır. Tremblay, daha önce, Iron Mountain şirketinde İç Denetim Direktörüydü ve hem Kuzey Amerika'daki tüm denetim ve projeleri denetliyor hem de küresel kalite yöneticileriyle bağlantı kuruyordu. Öncesinde, Houghton Mifflin Harcourt şirketinde üst yönetici olarak iç denetim departmanı kurmuş ve SOX uygulamasını yürütmüştür. Kariyerinin başlarında Raytheon ve Deloitte şirketlerinde çalışmıştır.

DaMon Ross Sr.

2020 yılında, DaMon Ross Sr. Cyber Defense International şirketinde çalışmaya başlamıştır; burada, o ve ekibi gerekli kabiliyetleri kendileri oluşturma imkanları olmayan kurumlara ekonomik siber güvenlik çözüm ve hizmetleri sunmak amacıyla elit siber güvenlik operasyonlarından ve siber tehdit istihbarat kabiliyetlerinden faydalanmaktadırlar. Ross, Cyber Defense International şirketinde çalışmaya başlamadan önce, SunTrust Bank şirketinde Siber Güvenlik Operasyonları için Kıdemli Başkan Yardımcısıydı. Bı rolde, SunTrust şirketinin 24/7/365 siber güvenlik operasyonları merkezini oluşturmaktan sorumluydu. Ross, benzer şekilde, siber istihbarat, siber tehdit izleme, siber olay müdahale ve siber suç konularında uzmanlaşan ekipler oluşturmuştur. Bankanın ilk içerden öğrenen tehdit izleme programını oluşturmak için hukuk, insan kaynakları, kurumsal güvenlik ve kurumsal etik ve risk ortaklarıyla başarılı bir ortaklık kurduğunu da not etmek gerekir. Ross, Amerika Birleşik Devletleri Gizli Servisi Elektronik Suçlar Görev Gücü ve İç Güvenlik Bakanlığı ile olanlar da dâhil olmak üzere çok sayıda bilgi paylaşım ortaklığının kurulmasını da kolaylaştırmıştır.

Giriş

Öze dönüş

Siber güvenlik uzun zamandır kurulların ve onların iç denetim fonksiyonlarının önde gelen odak noktalarından biri olmuştur ve Menkul Kıymetler ve Borsa Komisyonunun (SEC'in) siber güvenlik risk yönetimi, strateji, yönetişim ve olay raporlamalarıyla ilgili yeni tekliflerinin sunulmasıyla birlikte 2022 yılı da istisna olmamıştır. Bunlar ve diğer düzenleyici tekliflere yönelik itici güç garanti edilmektedir. Kimlik Hırsızlığı Kaynak Merkezinin bir raporuna göre, 2021 yılında kaydedilen 1.862 yüksek profilli veri ihlâli vardır – ki bu, 2020 yılında kaydedilen toplamı %68 oranında aşan ve 2017 yılında kaydedilen tüm zamanların rekorunu kıran rakamdır. Bu trendden hiçbir endüstri kaçamamıştır.[23]

Bu ortamda, kurumlar kurul, yönetim ve iç denetim arasında iletişim ve uyumun yanı sıra risk ve onun ilişkili düzenlemeleri hakkında sürekli öğrenme de dâhil olmak üzere ana ilkeler üzerine inşa edilmiş net, sağlam siber güvenlik kontrolleri ve süreçleri arzu etmekte ve hatta buna ihtiyaç duymaktadır. IIA'nın hazırladığı "2022 yılında Siber Güvenlik" başlıklı üç kısımlık serinin 1. Kısmı düzenleyici unsurların potansiyel etkilerine odaklanırken 2. Kısım bilgi güvenliğinden sorumlu genel müdür yardımcıları (CISO'lar) ve iç denetim yöneticileri arasındaki simbiyotik ilişkinin faydalarını incelemektedir. Bu son kısım, kurumun siber olay müdahale stratejisini geliştirmesi ve uygulamasını ve daha spesifik olarak ifade etmek gerekirse, iç denetimin bir siber güvenlik ihlâlinden hızlı şekilde kurtulması için kritik nitelikteki kontrolleri değerlendirirken kurumsal değer sağlayabileceği alanları vurgulamaktadır.

[23]. Kimlik Hırsızlığı Kaynak Merkezi, "Kimlik Hırsızlığı Kaynak Merkezi'nin 2021 Yıllık Veri İhlâli Raporu, Riskli Durum Sayısında Yeni Rekor Kırdı (Identify Theft Resource Center's 2021 Annual Data Breach Report Sets New Record for Number of Compromises)," 24 Ocak 2022, https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/.

Anahtar Kontroller

İç denetime siber müdahalede rol verme

Olay müdahale yanılması

"Siber olay müdahale" ve "siber güvenlik müdahale ve kurtarma" terimleri doğru ve faydalı tanımlayıcılar olmalarına rağmen bu tür planların etkili olması için ihtiyaç duyulanlar hakkında kısmen eksik bir görüşü de ima etmektedirler.

İç denetim, en temel rolüyle kurumlara risk yönetimi hakkında bağımsız güvence sağlamaktadır. Bu da siber olaylara karşı uygun müdahaleye ilişkin güvence sağlamanın yanı sıra riskin ve onun etkilerinin hafifletilmesini veya ideal olarak önlenmesini sağlayacak kontrollerin uygun şekilde değerlendirilmesini içermektedir. Herhangi belirli bir risk üzerinde bu denli yüksek bir standarda ulaşmak için dikkatin sadece tek bir riske karşılık vermeye ayrılmaması gereklidir. Bunun yerine, siber olay müdahale faaliyetini etkin müdahale tedbirlerinin yanı sıra önleyici kontrollere öncelik veren bütüncül, döngüsel bir tarzda ele almak daha etkilidir.

Onapsis, Inc. şirketinde uyum uygulamaları lideri olan Brian Tremblay "Risk yönetimi bir çeşit çark gibidir," demiştir. "Çarkın başlangıcında, doğru kontrollerimiz vardır ve süreçler olması gerektiğini düşündüğümüz gibidir. Ardından, herhangi bir şey olduğunda bir anda 'Kontroller beklenen şekilde mi işledi ve olacağını düşündüğümüz şey oldu mu?' gibi sorular sorulmaya başlar. Sonrasında, buradan yola çıkarak nelerin değiştirilmesi gerektiğini öğreniriz ve döngü yeniden başlar. Bir olaya müdahale ettiğiniz an o olaydan sonrasıysa zamanınız ve kaynaklarınız açısından muhtemelen verimsizsiniz. Bugüne ve geleceğe de eşit ağırlık verilmesi gerekir çünkü biz sadece bugünün işini inşa etmiyoruz, geleceğin işini de inşa ediyoruz. Kurumlar bununla çok sık mücadele ettiğinden dolayı iç denetçilerin odaklanması gereken gerçekten önemli bir alandır."

Değişmeyen temeller

Risklerin daha az karmaşık hale geldiği zamanlar nadirdir ve siber güvenlik doğası gereği yüksek düzeyde teknik olduğundan dolayı hem riskin kendisini hem de onu hafifletmek için gerekli sistemleri anlamak için gerekli öğrenme eğrisi her yeni teknolojik ilerlemeyle birlikte daha da dikleşmiştir. Bununla birlikte, bu durum muhakkak siber olay müdahale planının temel yapısının ve kapsadığı kontrollerin önemli ölçüde değişeceği anlamına gelmemektedir.

Bu kontroller IIA'nın en son yayınladığı *Siber Olay Müdahale ve Kurtarma Denetimi* başlıklı Tamamlayıcı Rehberde ana hatlarıyla özetlenmektedir ve dört üst düzey iş amacında gruplanabilir:

- **Olay Müdahalesinin Planlanması.** Bir olay meydana gelip gelmediğinin ve bu olay hakkında ne yapılacağının belirlenmesi sürecine rehberlik etmesi için politika ve prosedürlerin hazırlanması gereklidir. Planlama faaliyetinin önemli paydaşları içermesi gereklidir; rol ve sorumlulukları tanımlamalı ve farkındalık ve uygulamayı desteklemek için uygun şekilde test edilmelidir.
- **Olayın Tanımlanması.** Tespit edici kontrollerden elde edilen verilerin analiz edilmesine yönelik süreçler, bir siber olayın mevcut olup olmadığının tespit edilmesini sağlamaktadır; bu da genelde bir veya daha fazla müdahale planının uygulamaya konulmasını tetiklemektedir.
- **İletişim.** Siber olaylarda birçok potansiyel paydaş söz konusudur; dolayısıyla, olayın etkilerinin ve çözüme yönelik çabaların uygun ve zamanında bildirilmesi için her müdahale planının bünyesinde bir iletişim stratejisi barındırması gereklidir.

- **Teknik Müdahale ve Kurtarma.** Olayın niteliği, dâhili ve harici çaba ve çalışmaların koordinasyonunu içeren gerekli teknik onarım ve restorasyon kontrollerini büyük ölçüde belirlemektedir.[24]

Bu iş amaçlarına ulaşmak ve örneğin Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) Kritik Altyapı Siber Güvenliğini İyileştirme Çerçevesi gibi bir yerleşik siber olay müdahale çerçevesine uyum sağlamak, söz konusu bilgi güvenliği ve bilgi teknolojileri ekiplerinin uygulama, bakım va iyileştirmeyle ilgili sunabileceği teknik bilgileri — yani iç denetimin sahip olabileceği veya olamayacağı bilgileri gerektirmektedir. Bununla birlikte, daha az teknik ama eşit derecede değerli disiplinlere sahip diğer birimlerin önemli değerler sağlaması için de yeterli alan vardır. Objektif güvence sağlamak için kritik düzeyde önemli olan bağımsız perspektifinin yanı sıra, tüm departmanlar genelinde kurumsal fonksiyonlara benzersiz erişimi ve onlara ilişkin benzersiz bir anlayışı olan iç denetim tam da böyle bir disiplindir.

Cyber Defense International, LLC. şirketinin kurucusu ve SunTrust şirketinde eski kıdemli başkan yardımcısı ve siber güvenlik operasyonları yöneticisi olan DaMon Ross Sr., "İç denetim perspektifinden bakıldığında, siber olay müdahalesine yönelik yaklaşım fiili sürece ve o sürecin çıktısına odaklanılması açısından diğer herhangi bir riskten farklı değildir," demiştir. "Materyallerin teknik doğasına rağmen, bir süreç alanında çalışmaya alışmış herhangi bir iç denetçi önemli olan şeyleri oldukça hızlı bir şekilde kavrayacaktır."

Bu tür bir süreç, iç denetimin Sarbanes-Oxley (SOX) uyum programlarında, kriz müdahale planlarında veya herhangi bir yerleşik risk yönetimi stratejisinde görebileceklerine geçici bir benzerlikten daha fazlasına sahiptir. "Farklı kurumların farklı terminolojileri vardır ancak siber olay planı esasen bir siber olayın ne zaman meydana geldiğini, tüm ilgili tarafların rol ve sorumluluklarının ne olduğunu ve karar alma sürecine kimlerin katılması gerektiğini ana hatlarıyla belirten bir yönetim politikasıdır," demiştir Ross.

Tremblay, benzer bir fikri ifade etmiştir. Siber risklerle ilgili kontroller de Sarbanes-Oxley ile ilişkili uyum risklerini yönetmek için kullanılan çerçevelerin bir parçasıdır demiştir.

Örneğin, bilgisayar korsanlarının herhangi bir teknolojiye sızarken attıkları ilk adımlardan biri amaçlarına ulaşmak için gerekli hak ve ayrıcalıklara erişim sağlamaktır. Büyük risk şemasında, bu eylem yetkisiz erişim riski altında yer almaktadır. Tremblay, bunun SOX veya siber risk için geçerli olup olmadığı konusunda hiçbir fark olmadığını söylemiştir. "En basit hallerine indirgendiğinde, riskler ve o riskleri hafifletecek kontroller esasen özdeştir."

Dokümantasyon kontrolleri

Tremblay'nin bahsettiği üzere, bu tür bir politikada yer alan kontroller de diğer kurumsal risklerle görülebilenlerle önemli ölçüde özdeştir. Etkili bir dokümantasyon sürecine sahip olmak buna örnektir. Ross da buna katılmaktadır. Kurumlar, siber olayları uygun şekilde belgeleyen iş akışlarının neye benzediğini ve paralel işleyen tüm hareketli parçaların nasıl bir bütün haline geldiğini anlamak zorundadırlar demiştir.

"Bu durum sadece büyük olaylar için geçerli değildir. Her kurumun bununla günlük olarak uğraşan bir fonksiyonu olması gereklidir. Bir bilgisayarda kötü amaçlı yazılım olduğunu düşünelim. Bunun gibi küçük olaylar daha büyük olaylara dönüşebilir ve en kötünün gerçekleştiği durumda, uygun dokümantasyon olayın nasıl tırmandığını anlamaya yardımcı olmaktadır. Bu fonksiyon kendi başına bir kontroldür."

Tespit ve fiziksel altyapı kontrolleri

Fiziksel altyapı, kritik kontrollerden bir diğeridir ve yetkisiz erişim riskleri kategorisine girmektedir. Her ne kadar bu tür kontroller siber güvenlik konusunu tartışırken hemen akla gelmese de Ponemon Institute tarafından hazırlanan ve IBM Güvenlik tarafından yayınlanan araştırmaya göre, hassas verilerin saklandığı sabit disk veya sunuculara yetkisiz erişim

[24]. The IIA, *Siber Olay Müdahale ve Kurtarma Denetimi (Auditing Cyber Incident Response and Recovery)*, Tamamlayıcı Rehber, Çalışma Rehberi, https://www.theiia.org/globalassets/documents/content/articles/guidance/gtag/2022/gtag_auditing_cyber_incident_response_and_recovery_final.pdf.

2020 yılında kaydedilen tüm kötü amaçlı ihlâllerin %10'undan sorumludur ve kurumlara her ihlâl için ortalama 4,36 milyon dolara mal olmuştur.

Bu tür altyapılar, tesis genelinde kilitli kapılar gibi daha temel güvenlik tedbirlerinin yanı sıra erişimin kısıtlı olduğu güvenli sunucu odalarını içerebilir. Altyapı güvenliği önemli olmasına rağmen, potansiyel olarak şüpheli faaliyeti tespit etmek ve belgelemek için kontrollerin bulunması daha önemli olabilir.

Tremblay "Fiziksel altyapıdan bahsettiğimde, kilitli kapıların yanı sıra gerçek riski yaratan eylemlerin bildirilmesi ve belgelenmesinden emin olmaktan da bahsediyorum. Bu, mezeye karşılık ana yemek gibidir," demiştir.

Ross, bu tür sistemlerin tanımlanması ve onlara ilişkin güvence sağlanması doğrudan iç denetimin yerleşik beceri setleri içinde yer almaktadır demiş ve eklemiştir: "İç denetim, kurumun hayatta kalması için en yüksek riskli veya kritik olan sistemleri tanımlayabilme becerisine sahiptir. Aslında, diğer risklerle ilgili federal kanun ve yönetmeliklere uyum konusunda güvence sağlamanın bir parçası olarak tanımlanan bu sistemlere iç denetimin halihazırda sahip olması muhtemeldir. Tek gereken, bu düşünceyi yüksek erişim sunabilecek yeni tedarik türlerini içerecek şekilde genişletmektir."

Kurtarma beklentilerinin uyumu

Siber olay müdahale planının tüm aşamalarında etkili dokümantasyon kritik düzeyde önemlidir. Bununla birlikte, bu tür dokümantasyonun sağladığı verilerin raporlanması ve kurumsal tespit ve kurtarma beklentilerinin uyumu da eşit düzeyde kritiktir.

Tremblay'a göre, bu, kurumların siber müdahale planlarında görmüş olduğu en büyük boşluklardan biridir — ve iç denetimin en fazla değeri sağlayabileceği alandır. "İç denetimin siber felaketten kurtarmadaki rolü iki aşamalıdır," demiştir. "Birincisi, olayın mevcut olduğundan emin olmaktır ve kullandığınız dokümantasyon veya herhangi bir teknoloji veya süreç aracılığıyla mevcudiyetini kanıtlayabilirsiniz. İkincisi ve yeterince yapılmadığını gördüğüm şey, gerçekçi kurtarma programının kurumun risk iştahı temelinde ne olacağını [belirlemek için] tüm önemli paydaşlarla görüşmektir."

Tremblay, bu programın kurumda söz konusu uygulamanın 'sahibi' – ki bu kişi, olayın nerede meydana geldiğine bağlı olarak CISO, tedarik zinciri yöneticisi veya herhangi başka bir lider olabilir – tarafından belirleneceğini söylemiştir. Günlük görevler için söz konusu uygulamaya bağlı olarak uygulamanın sahibi ve tüm diğer taraflar arasında bağlantı işlevi görmek iç denetim için önemlidir.

"Örneğin, CISO 48 saatlik programın kabul edilebilir olduğunu söyleyebilir ancak söz konusu teknolojinin hazır, çalışır durumda olmasına ve girdilerini almasına bel bağlayan CFO veya diğer lider veya fonksiyonlar ile görüşmezseniz kendinizi potansiyel bir karmaşaya hazırlıyorsunuz demektir," demiştir Tremblay. "Örneğin, hesapları kapattığımız dönemde olmamak şartıyla CFO 48 saatin uygun olduğunu söyleyebilir. Eğer hesapları kapattığımız dönemdeysek hiçbir kesinti kabul edilemez çünkü kurumun kamu piyasalarında gerçekten kötü görünecek bir uzatma başvurusu yapması gerekecektir."

Bu tür görüşmelerde bir tarafın diğerine baskın gelmesi şart değildir. Daha ziyade, böyle görüşmeler sayesinde iç denetim kurumun risk iştahı doğrultusunda fikir birliği sağlayabilir. "Uyuşmazlığın olduğu durumlarda, iç denetim 'Bunun olmasına gerçekten değer mi?' diye sorabilir. CEO ise 'Evet, değer çünkü bu sorunu çözmek bir milyon dolara mal olacak,' diyebilir. Gerçekten yaptığımız şey, bu planın teknolojinin ilgilendirdiği paydaşların etrafında tam anlamıyla geliştirildiğinden emin olmaktır," demiştir Tremblay.

Tremblay şu şekilde devam etmektedir: "Bence bu alan bir meslek olarak bizim özellikle iyi olmadığımız bir alan. Sanırım, belirli bazı şeyleri doğrulayan kutuyu 'Olay müdahalesine ilişkin kontrollerin gözden geçirilmesinin bir parçası olarak, belirli teknolojilerin paydaşları arasında gereksinimlerde bir boşluk belirledik' demeden işaretlemeye çalışıyoruz. Bu, oldukça geçerli. Bu, kurum açısından değerli olan ve daha önce tanımlanmayan bir iş riskini tanımlamaktadır."

Çapraz işlevsellik

Siber güvenlik müdahalesinden birincil olarak sorumlu olanın CISO ve güvenlik ekibi olduğunu düşünmek yaygın bir yanılgıdır. Bu düşünce sadece kısmen doğrudur. Siber güvenlik stratejisinin daha teknik yönlerini uygulamak için gerekli tecrübe ve uzmanlık çok büyük olasılıkla bahsi geçen departmanda bulunmasına rağmen, departmanın bu yükü kendi başına omuzlayacak kapasiteye – veya arzuya – sahip olacağını varsaymak tehlikelidir.

“Siber olay müdahalesi çapraz işlevsel bir süreçtir, en azından öyle olması gereklidir,” demiştir Ross. “Kurumsal müdahale sürelerindeki gecikmenin gördüğüm en büyük nedeni, bilgi açısından bilgi güvenliği departmanının kendisi değildir; daha ziyade, birincil sorumluluğu güvenlik olmayan departmanlarla çapraz işlevli rol ve sorumluluklar belirlenmesidir. Bu departmanların yapması gereken başka işler vardır.”

Ross’a göre, bu yanılgının düzeltilmesi ve tüm paydaşlar genelinde ortak sorumluluk fikrinin desteklenmesi iç denetimin odaklanması gereken önemli bir alan olmalıdır. “Muhakkak güvenlik ekibinin ve yaptıklarının üzerinde durulması gerekmez ancak onların yürüttüğü sürecin kurum genelinde o süreçte payı olan diğerleri tarafından nasıl desteklendiği vurgulanmalıdır. Güvenlik ekibi ne yapması gerektiğini bilir ancak BT ekibini ve arka uç geliştiricileri kritik şekillerde yardımcı olmaya zorlayamaz. İşin içinde birçok kurumsal politika vardır ve ben o pozisyondayken iç denetiminde değerli bir ortak bulmuştum. Güvenlik ekipleri bu savaşlarda tek başına mücadele edemez. Kurumda sürecin neresinde boşluklar olduğunu belirlemeye yardımcı olmak için kısmen de olsa nötr bir taraf bulabilirseniz bunun herkese yardımı olur.”

Ross, iç denetimin genellikle harici danışmanlarla işbirliği yapmak suretiyle masaüstü simülasyonları kolaylaştırmasının bu boşlukları vurgulamak ve rollere açıklık getirmek için kullanılacak faydalı bir strateji olduğunu söylemiştir. “Siber olay müdahale planınızın test edilebileceği bir yer olduğunda, masaüstü simülasyon CIO, CISO, BT liderleri, CEO, iç denetimi — yani tüm ilgili paydaşları — makul bir senaryoyu incelemek üzere bir konferans odasında veya Zoom görüşmesinde bir araya getirmektedir. İç denetim, kimin ne yaptığını sorarak ve bu sorumlulukların gerçekle uyumlu olup olmadığını değerlendirerek teknik uzmanlık olmadan da tartışmayı kolaylaştırabilir. ‘Bu noktada, planımıza göre ekibinizin X ve Y’yi yürütüyor olması gerekiyor ancak gerçekte Z’yi yapıyor olabilirsiniz,’ diyebilirler. İşte bu noktada duymak istemediklerinizi duyacaksınız. Çoğu kurum bu simülasyonu yılda en az bir kez yapmak zorundadır ancak iç denetimin bu simülasyonların sorumluluğunu gerçekten üstlenmesi gereklidir.”

Varılan Sonuçlar

Risk ortamıyla birlikte gelişme

İç denetim, kurumdaki benzersiz yeri sayesinde, kurumun siber olay müdahale planları söz konusu olduğunda masada bir yeri hak etmektedir. Ancak bu başarı iç denetimi siber güvenliği daha derinden keşfetme ve anlama çabasından muaf tutmamaktadır. Gerçekten de, bulut tabanlı teknoloji lehine fiziksel altyapıdan hızla vazgeçilen bir gelecekte, kaçınılmaz bir şekilde, iç denetimin daha fazla uzmanlaşması gerekli ve beklenir hale gelecektir.

“Kariyerime iç denetimde başladığımda, en çok hoşuma giden noktalardan biri çok kültürlü ve birçok konuda bilgili olmayı gerektiren bir rol olmasıydı,” demiştir Tremblay. “Uzman olmanız gerekmeyen birçok konu hakkında birçok şey görmek ve öğrenmek zorundasınız. Ancak teknoloji çevresinde o kadar büyük bir değişim oldu ki iç denetçinin bu kültürlü ve birçok konuda bilgili olduğu günlerin sayılı olup olmadığını merak etmeye başlıyorum. Bunun yerine, belki bir gün, iç denetim kurumlar için doğası gereği kritik olan şeyler hakkında daha çok bir konu uzmanı (SME) haline gelecektir. Bundan dolayı, kurumların 8-10 operasyon, uyum ve bilanço denetçisinden oluşan denetim ekipleri yerine bir siber güvenlik denetçisi, bir ESG denetçisi ve benzeri olacaktır.”

Ross da buna katılmıştır. “Gelişen teknolojiyle birlikte belirli bir noktada, o kadar derine inemezseniz müdahale sürecindeki boşlukları nasıl derinlemesine anlarsınız? Asla gerçekten yapamazsanız.”

Eldeki bilgi ve kaynaklarla başarılabilecek çok şey var ancak heyecan verici ve tamamıyla yeni bir gelecek kapımızda. İç denetimin bu geleceğin bir parçası olması gerekiyor.

Önceki sayılar

Küresel Bakış Açıları ve Anlayışlar'ın önceki sayılarına erişim sağlamak için şu adresi ziyaret ediniz: www.theiia.org/GPI.

Okuyucu Geribildirimleri

Soru veya yorumlarınızı gönderin: globalperspectives@theiia.org.

IIA Hakkında

İç Denetçiler Enstitüsü (IIA) dünya çapında 215.000'i aşkın üyeye hizmet eden ve dünya genelinde 180.000 Sertifikalı İç Denetçi (CIA) unvanı veren bir uluslararası meslek birliğidir. 1941 yılında kurulan IIA, dünya çapında standartlar, sertifikasyon, eğitim, araştırma ve teknik rehberlik konusunda iç denetim mesleğinin lideri olarak kabul edilmektedir. Daha fazla bilgi için, theiia.org adresini ziyaret ediniz.

Sorumluluğun Reddi Beyanı

IIA bu dokümanı bilgi ve eğitim amaçlı yayımlamaktadır. Bu materyalin spesifik münferit koşullara kesin ve nihai cevaplar vermesi beklenmemelidir ve sadece bir rehber olarak kullanılması amaçlanmıştır. IIA, herhangi bir spesifik durumla doğrudan ilgili konularda daima bağımsız uzman tavsiyesi almanızı önerir. IIA, herhangi bir kimsenin bu rehberi tek referans kaynağı olarak kullanması durumunda hiçbir sorumluluk kabul etmez.

Telif Hakkı

Ağustos 2022

The Institute of Internal Auditors

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101