آراء و رؤى عالمية

الأمن السيبراني في 2022

الجزء الاول : كيف يمكن لمقترحات هيئة الأوراق المالية والبورصات الأمريكية (SEC) الجديدة أن تغير اللعبة

الجزء الثاني: الشركاء المهمون - التدقيق الداخلي ومدير إدارة أمن المعلومات

الجزء الثالث : الاستجابة للحوادث السيبرانية والتعافي منها

قام بترجمة هذه الوثيقة الى اللغة العربية فريق عمل من جمعية المدققين الداخليين في لبنان برئاسة عضو مجلس الحكام ناجي فياض مؤلف من محمد شهاب، محمود غلاييني و داليا بوكروم

The Institute of
Internal Auditors

المعهد الدولي
للمدققين الداخليين

المحتويات

قام بترجمة هذه الوثيقة الى اللغة العربية فريق عمل من جمعية المدققين الداخليين في لبنان برئاسة عضو مجلس الحكام ناجي فياض
مؤلف من محمد شهاب، محمود غلاييني و داليا بوكروم

كيف يمكن لمقترحات لمقترحات هيئة الأوراق المالية والبورصات الأمريكية ***(SEC)*** الجديدة أن تغير اللعبة

عن الخبراء

Andy Watkin-Child

هو مخضرم في مجال الأمن السيبراني وإدارة المخاطر والتكنولوجيا لمدة 20 عامًا ، ومؤسس مشارك لمجموعة *The Augusta Group* ، وهي مزود حلول للإدارة والإشراف وضمان الأمن السيبراني والمخاطر السيبرانية. شغل مناصب قيادية دولية في خطي الدفاع الأول والثاني *(LoD)* للأمن السيبراني ، وإدارة المخاطر السيبرانية ، والمخاطر التشغيلية ، والتكنولوجيا ، حيث عمل مع فرق قيادية من الشركات ذات الميزانيات العمومية التي تزيد عن 1 تريليون يورو في مجالات الهندسة والتصنيع والمالية. الخدمات والصناعات الإعلامية والنشر. وهو عضو متمرس في مجالس الإدارة وفرق قيادة المخاطر العالمية ولجان الأمن السيبراني والمخاطر التشغيلية ولجان القانون العام لحماية البيانات *(GDPR)*.

Manoj Satnaliwala

هو الرئيس التنفيذي للتدقيق ونائب أول لرئيس التدقيق الداخلي لشركة *Caliber Home Loans* وهو مسؤول عن جميع أنشطة التدقيق ، ويعمل مباشرة مع لجنة التدقيق. قبل توليه منصبه الحالي ، قاد وظيفة التدقيق في *Radian Group Inc.* ، ثالث أكبر شركة تأمين على الرهن العقاري يتم تداولها علنًا في الولايات المتحدة ، وكان مديرًا للتدقيق الداخلي لشركة *PwC* ، حيث أدار التحقق من ضوابط التدقيق الداخلي. كجزء من مشروع *CCAR* لشركة قابضة لبنك كبير.

المقدمة

يمكن أن يكون للمقترحات التنظيمية الجديدة آثار ضخمة

شهدت دورة الأخبار في عام 2022 ، وفي الواقع ، في السنوات العديدة الماضية ، القليل من الإيجابية ، وتلوح التهديدات السيبرانية في الأفق بشكل كبير في مزيج يشمل أزمة أوكرانيا ، وتهديدات كوفيد -19 المستمرة ، والتوترات المتزايدة بين الولايات المتحدة والصين. لقد اجتمعت هذه المتغيرات وغيرها لإعطاء الأمن السيبراني مكانة مهمة - بل ورائدة بالفعل - على خرائط مخاطر المدقق الداخلي.

ومع ذلك ، شهد عام 2022 أيضًا تطورات متعلقة بالأمن السيبراني والتي تعد بالتأثير على مجموعة واسعة من المنظمات ، وسوف تتطلب مزيدًا من الجهد لفهمها ، وستستغرق آثارها وقتًا لفهمها بالكامل. من أهم هذه المقترحات التنظيمية المقدمة من هيئة الأوراق المالية والبورصات الأمريكية (***SEC***). الاقتراح الثاني جدير بالملاحظة بشكل خاص لأنه سيتطلب من الشركات المتداولة علنًا والتي تعمل في الولايات المتحدة الكشف عن سياسات وإجراءات واستراتيجيات الحوكمة الخاصة بالأمن السيبراني ، بالإضافة إلى معرفة مجلس الإدارة وخبرته - إن وجدت - في مجال الأمن السيبراني. إذا تم تنفيذها (حيث من المحتمل أن تكون في شكل ما) ، فإن المنظمات المتداولة علنًا ، بغض النظر عن القطاع أو الحجم ، ستخضع لهذه القواعد الجديدة. بدون المبالغة ، تمثل هذه التطورات فصلاً جديدًا للأمن السيبراني وموضوعًا جديدًا - إذا كان مألوفًا - لمجتمع التدقيق الداخلي ، والذي سيلعب دورًا حاسمًا في توجيه مؤسساتهم من خلال هذا التحدي.

على الرغم من أن هذا لا يمثل تحديًا يجب الاستخفاف به ، إلا أن التدقيق الداخلي لحسن الحظ يفهم الأدوات والمهارات التي يحتاجها لتقديم ضمانات بشأن منطقة المخاطر المتطورة هذه. يقدم الجزء الأول من سلسلة ملخصات المعرفة العالمية المكونة من ثلاثة أجزاء من المعهد العالمي للمدققين الداخليين حول الأمن السيبراني نظرة عامة على مقترحات هيئة الأوراق المالية والبورصات الجديدة ، بما في ذلك الآثار المترتبة على تنظيم تقارير الأمن السيبراني في الولايات المتحدة وكذلك في الخارج. كما يستكشف كيف يمكن للمدققين الداخليين أن يلعبوا دورًا مهمًا في مساعدة مؤسساتهم على إدارة مشهد الامتثال المتغير الذي يمكن أن تخلقه اللوائح الجديدة قريبًا.

تمهيد الطريق

الأمن السيبراني يهيمن على مشهد المخاطر

الخطر الأكبر في عصرنا

يبقى الأمن السيبراني على رأس أولويات جميع المنظمات في جميع الصناعات في عام 2022 ، وينعكس هذا القلق بوضوح في البيانات الواردة من المعهد الدولي للمدققين الداخليين (*IIA*) لعام 2022 في أمريكا الشمالية (***Pulse***)[1] . عندما طُلب منهم تصنيف مستوى المخاطر التي تتعرض لها مؤسساتهم من بين 13 خطرًا رئيسيًا ، صنف قادة التدقيق الداخلي الذين أجابوا على استبيان *Pulse* المخاطر المتعلقة بالتكنولوجيا ضمن المراكز الثلاثة الأولى - الأمن السيبراني وتكنولوجيا المعلومات وعلاقات الأطراف الثالثة (والتي غالبًا ما تتضمن خدمات تكنولوجيا المعلومات) . حتى بين هؤلاء الثلاثة الأوائل ، احتل الأمن السيبراني المرتبة الأولى بسهولة ، حيث صنفه 85 ٪ من المشاركين على أنه مرتفع أو مرتفع للغاية ، 24 نقطة مئوية أعلى من تصنيفات تكنولوجيا المعلومات ، ثاني أعلى تصنيف للمخاطر.

هذا القلق له ما يبرره. في عام 2021 ، زادت الهجمات السيبرانية من كل نوع تقريبًا بهوامش مقلقة. وفقًا لتقرير[2] ***SonicWall Cyber Threat*** لعام 2022 ، ارتفع عدد التهديدات المشفرة في عام 2021 بنسبة 167٪ (10.4 مليون هجوم) ، وارتفعت فيروسات الفدية بنسبة 105٪ (623.3 مليون هجوم) ، وارتفعت هجمات الـ *Cryptojacking* (الهجمات على أجهزة الكمبيوتر لتعدين العملات المشفرة) بنسبة 19٪ (97.1 مليون هجوم) ، وارتفعت محاولات التسلل بنسبة 11٪ (5.3 تريليون هجوم) ، وارتفعت البرامج الضارة الموجهة إلى إنترنت الأشياء (*IoT*) بنسبة 6٪ (60.1 مليون هجوم).

علاوة على ذلك ، فإن كل هذه الهجمات تحمل تكلفة كبيرة للأضرار التي تسببها. من المتوقع أن يصل إجمالي التكاليف السنوية للهجمات السيبرانية إلى 10.5 تريليون دولار بحلول عام 2025 ، بمتوسط نمو بنسبة 15٪ على أساس سنوي ، وفقًا لأحدث إصدار من 'Cisco/Cybersecurity Ventures 2022 Cybersecurity Almanac[3]

وهذا لا يؤثر حتى في التغييرات الدراماتيكية التي تطرأ على المشهد الجيوسياسي التي تؤثر على الأمن السيبراني. حتى قبل الغزو الروسي لأوكرانيا ، كانت هناك أدلة كثيرة على أن الهجمات السيبرانية المشتبه بها التي ترعاها الدولة ، بمستويات عالية من التطور ، كانت تتزايد من حيث التأثير والتكرار. شهد خرق عام 2020 لأنظمة *SolarWind* التي تتخذ من تكساس مقراً لها ، والذي يقال[4] ان من قام بها مجموعة قرصنة تم توجيهها من قبل وكالة الاستخبارات الأجنبية الروسية ، البنية التحتية الرقمية لما يصل إلى 18000 عميل[5] - بما في ذلك *Microsoft* و *Cisco* و *Intel* و *Deloitte* وأجزاء من البنتاغون ، وزارة الأمن الداخلي الأمريكية ووزارة الطاقة والإدارة الوطنية للأمن النووي - تعرضت للخطر ولم يتم اكتشافها لعدة أشهر.

في عام 2021 ، شوهد هجوم رئيسي آخر مشتبه به برعاية الدولة على شركة أمريكية هي شركة Colonial Pipeline Co.[6]. وأدى الهجوم إلى تعطيل تدفق ما يقرب من نصف إمدادات البنزين ووقود الطائرات إلى الساحل الشرقي. في النهاية ، دفعت Colonial فدية تقارب 5 ملايين دولار لمجموعة القرصنة *DarkSide* لاستعادة الشبكة واستعادة البيانات.

---

[1]. The IIA, *2022 North American Pulse of Internal Audit*, March 2022, https://www.theiia.org/en/content/research/pulse-of-internal-audit/2022/2022-north-american-pulse-of-internal-audit/

[2]. SonicWall, *2022 SonicWall Cyber Threat Report*, 2022, https://www.sonicwall.com/2022-cyber-threat-report/.

[3]. Steve Morgan, "2022 Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics," Cybersecurity Ventures, Cisco, January 19, 2022, https://cybersecurityventures.com/cybersecurity-almanac-2022/.

[4]. Joe Hernandez, The Russian Hacker Group Behind the SolarWinds Attack Is At It Again, Microsoft Says," NPR, updated October 25, 2021, https://www.npr.org/2021/10/25/1048982477/russian-hacker-solarwinds-attack-microsoft.

[5]. Isabella Jibilian and Katie Canales, "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, updated April 15, 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/.

نقطة الانهيار الجيوسياسي

منذ هذه الهجمات ، تصاعدت المخاوف بشأن روسيا ، وبلغت ذروتها مع غزو أوكرانيا. في الواقع ، يشمل العدوان الروسي على أوكرانيا الحرب السيبرانية - هجوم واسع النطاق على شبكة الكهرباء[7] الأوكرانية - بالإضافة إلى الحرب التقليدية ، وهناك قلق متزايد من أن روسيا قد تنتقم من العقوبات الاقتصادية التي لا تعد ولا تحصى التي فرضها عليها حلف شمال الأطلسي والولايات المتحدة. قبل الانتقال الرسمي لروسيا إلى أوكرانيا ، أصدرت وكالة الأمن السيبراني وأمن البنية التحتية *(CISA)* بيانًا نادرًا *"Shields Up"* يحذر الشركات الأمريكية من جميع الأحجام من تبني موقف مشدد فيما يتعلق بالأمن السيبراني وحماية الأصول الحيوية. "تكشف الاستشارات الأخيرة التي نشرتها *CISA* ومصادر أخرى غير سرية أن الجهات الفاعلة المهددة التي ترعاها الدولة الروسية تستهدف الصناعات والمنظمات التالية في الولايات المتحدة والدول الغربية الأخرى: أبحاث*COVID-19* ، والحكومات ، والمنظمات الانتخابية ، والرعاية الصحية والأدوية ، والدفاع ، كتب *CISA* في بيان[8] صدر في مارس 2022 لتقييم التهديدات السيبرانية الروسية.

في مايو 2021 ، وقع الرئيس بايدن أمرًا تنفيذيًا[9] مصممًا لتحسين حالة الأمن القومي في الولايات المتحدة. تناول الأمر تحديدًا الحاجة إلى قيام الوكالات الحكومية بمراجعة وتطوير إرشادات ومعايير جديدة للأمن السيبراني ، وللمؤسسات للتركيز على تعزيز توفير البرامج. الأمن المتسلسل ومشاركة معلومات التهديد. في الآونة الأخيرة ، أصدر الرئيس أيضًا بيانًا كرر فيه تهديد الأمن السيبراني الروسي وسلط الضوء على إرشادات[10] *CISA* المتطورة حول هذا الموضوع.

روسيا ليست الجهة الحكومية الوحيدة التي يُزعم أنها تدعم الهجمات السيبرانية المزعزعة للاستقرار. وفقًا لتقرير[11] عام 2021 من مجموعة *Evanina Group* ، أصبحت الصين عدوانية بشكل متزايد على الجبهة السيبرانية ، لا سيما فيما يتعلق بالحصول على بيانات المعلومات الشخصية وخصوصية البيانات.

قال ويليام إيفانينا ، المدير السابق للمركز الوطني لمكافحة التجسس والأمن: "إن قدرة الصين على الحصول بشكل شامل على ملكيتنا الفكرية وأسرارنا التجارية من خلال أساليب هجينة غير قانونية وقانونية ومعقدة لا تشبه شيئًا لم نشهده من قبل".

أشارت إيفانينا إلى العديد من الحوادث السيبرانية المرتبطة بالحزب الشيوعي الصيني ، بما في ذلك خرق *Equifax* الإلكتروني لعام 2017 ؛ حملة 2011-2018 من قبل أربعة مواطنين صينيين لاختراق عشرات الشركات والجامعات والهيئات الحكومية ؛ وحملة إلكترونية رعتها الدولة في الفترة 2011-2013 لمهاجمة شركات خطوط أنابيب النفط والغاز الطبيعي الأمريكية (أصدرت وزارة العدل تقريرًا عن هذه الحادثة في يوليو 2021). كما أشار إلى تقرير يوليو 2021 من وكالة الأمن القومي (*NSA*) ، ومكتب التحقيقات الفيدرالي (*FBI*) ، و *CISA* الذي أصدر أكثر من 50 تكتيكا وأدوات إلكترونية يستخدمها قراصنة صينيون ترعاهم الدولة ضد الولايات المتحدة.

في هذه البيئة السيبرانية المعقدة والخطيرة بشكل عام ، اتخذت لجنة الأوراق المالية والبورصات (*SEC*) خطوات تاريخية لمعالجة الصحة السيبرانية والتأهب عبر المشهد التنظيمي ، لا سيما فيما يتعلق بتقديم التقارير إلى لجنة الأوراق المالية والبورصات (في بعض الحالات) للجمهور. مثل هذه الخطوات هي الأولى من نوعها ويمكن أن يكون لها آثار كبيرة ليس فقط على الشركات الأمريكية المتداولة علنًا ولكن الشركات في جميع أنحاء العالم.

---

7. IANS, Ukraine Foils Russia-backed Cyber Attack on Power Grid," April 14, 2022, https://www.nationalheraldindia.com/international/ukraine-foils-russia-backed-cyber-attack-on-power-grid.
8. Cybersecurity and Infrastructure Security Agency (CISA), "Russia Cyber Threat Overview and Advisories," Department of Homeland Security, accessed April 22, 2022, https://www.cisa.gov/uscert/russia.
9. U.S. General Services Administration (GSA), "Executive Order 14028: Improving the Nation's Cybersecurity," May 12, 2021, https://www.gsa.gov/technology/technology-products-services/it-security/executive-order-14028-improving-the-nations-cybersecurity.
10. Cybersecurity and Infrastructure Security Agency (CISA), "Shields Up."
11. William Evanina, "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, August 4, 2021, https://www.intelligence.senate.gov/sites/default/files/documents/os-bevanina-080421.pdf.

التغيير الكبير

خطوة تاريخية أولى نحو الكشف عن الحوادث السيبرانية

المقترحات

في غضون شهرين ، كشفت *SEC* النقاب عن مقترحين طال انتظارهما يتناولان الأمن السيبراني في قطاع الأعمال. يركز الاقتراح الأول[12] ، الذي تم الكشف عنه في فبراير 2022 ، على مستشاري الاستثمار المسجلين ، وشركات الاستثمار المسجلة ، وشركات أو صناديق تطوير الأعمال. بموجب القواعد المقترحة ، ستكون هناك حاجة إلى المستشارين والأموال من أجل:

- اعتماد وتنفيذ سياسات وإجراءات الأمن السيبراني المكتوبة المصممة لمعالجة مخاطر الأمن السيبراني التي يمكن أن تضر العملاء الاستشاريين والمستثمرين في التمويل.
- الإبلاغ عن حوادث الأمن السيبراني الكبيرة التي تؤثر على المستشار أو عملاء صندوقه أو صندوقه الخاص إلى لجنة الأوراق المالية والبورصات في نموذج سري جديد
- الإفصاح علنًا عن مخاطر الأمن السيبراني وحوادث الأمن السيبراني الكبيرة التي وقعت في العامين الماليين الماضيين في الكتيبات وبيانات التسجيل الخاصة بهم

بالإضافة إلى ذلك ، سيحدد الاقتراح متطلبات حفظ السجلات الجديدة للمستشارين والأموال المصممة لتحسين توافر المعلومات المتعلقة بالأمن السيبراني ، فضلاً عن المساعدة في تسهيل فحص *SEC* وقدرات الإنفاذ.

قال جاري جينسلر رئيس المجلس الأعلى للتعليم في بيان صحفي[13]: "تتعلق مخاطر الإنترنت بكل جزء من مهمة *SEC* المكونة من ثلاثة أجزاء ، وعلى وجه الخصوص بأهدافنا المتمثلة في حماية المستثمرين والحفاظ على أسواق منظمة". "تم تصميم القواعد والتعديلات المقترحة لتعزيز الاستعداد للأمن السيبراني ويمكن أن تحسن ثقة المستثمرين في مرونة المستشارين والأموال ضد تهديدات الأمن السيبراني والهجمات."

بينما تعكس هذه القواعد - إذا كانت ضمنية - توقعات هيئة الأوراق المالية والبورصات (*SEC*) لكيفية إدارة الكيانات المنظمة لمخاطر الأمن السيبراني والإبلاغ عن حوادث الأمن السيبراني ، فإن الاقتراح الثاني يوضح هذه التوقعات. يهدف الاقتراح الثاني[14] ، الصادر في مارس 2022 ، والموجه إلى جميع الشركات المتداولة علنًا ، إلى "تعزيز وتوحيد الإفصاحات المتعلقة بإدارة مخاطر الأمن السيبراني والاستراتيجية والحوكمة والإبلاغ عن حوادث الأمن السيبراني من قبل الشركات العامة التي تخضع لمتطلبات الإبلاغ الخاصة ببورصة الأوراق المالية. قانون عام 1934. " للقيام بذلك ، تتطلب القواعد الجديدة من الشركات العامة تقديم إفصاحات فيما يتعلق بما يلي:

- سياسات وإجراءات الشركة لتحديد وإدارة مخاطر الأمن السيبراني. تتضمن القواعد قائمة واسعة ولكنها غير شاملة لاستراتيجيات وسياسات وإجراءات إدارة المخاطر التي قد تخضع للإفصاح ، بما في ذلك:
  - ما إذا كان لدى المسجل برنامج لتقييم مخاطر الأمن السيبراني.
  - ما إذا كان المُسجل يُشرك مُقيّمين أو مستشارين أو مدققين أو أطراف ثالثة أخرى فيما يتعلق بأي برنامج لتقييم مخاطر الأمن السيبراني.
  - ما إذا كان لدى المسجل سياسات وإجراءات للإشراف على وتحديد مخاطر الأمن السيبراني المرتبطة باستخدامه لأي مزود خدمة تابع لجهة خارجية.

12. U.S. Securities and Exchange Commission (SEC), "Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies," February 9, 2022, https://www.sec.gov/rules/proposed/2022/33-11028.pdf.
13. U.S. Securities and Exchange Commission (SEC), "SEC Proposes Cybersecurity Risk Management Rules and Amendments for Registered Investment Advisers and Funds," press release, February 9, 2022, https://www.sec.gov/news/press-release/2022-20.
14. U.S. Securities and Exchange Commission (SEC), "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure," March 9, 2022, https://www.sec.gov/rules/proposed/2022/33-11038.pdf.

- ما إذا كان المسجل يقوم بأنشطة لمنع واكتشاف وتقليل آثار حوادث الأمن السيبراني.
- ما إذا كان لدى المسجل خطط استمرارية الأعمال والطوارئ والاسترداد في حالة وقوع حادث للأمن السيبراني.
- ما إذا كانت حوادث الأمن السيبراني السابقة قد أبلغت عن تغييرات في حوكمة المسجل أو سياساته وإجراءاته أو تقنياته.
- ما إذا كانت المخاطر والحوادث المتعلقة بالأمن السيبراني قد أثرت أو من المحتمل بشكل معقول أن تؤثر على نتائج عمليات المسجل أو وضعه المالي.
- ما إذا كانت مخاطر الأمن السيبراني تعتبر جزءًا من إستراتيجية أعمال المسجل والتخطيط المالي وتخصيص رأس المال.

- دور الإدارة في تنفيذ سياسات وإجراءات الأمن السيبراني ، بما في ذلك:
  - ما إذا كانت بعض المناصب أو اللجان الإدارية مسؤولة عن قياس وإدارة مخاطر الأمن السيبراني.
  - ما إذا كان المسجل قد عيّن مسؤول أمن معلومات رئيسي أو شخصًا في منصب مماثل.
  - ما إذا كانت العمليات التي يتم من خلالها إبلاغ هؤلاء الأشخاص أو اللجان عن ومراقبة منع حوادث الأمن السيبراني والتخفيف من حدتها واكتشافها ومعالجتها.
  - ما إذا كان هؤلاء الأشخاص أو اللجان يقدمون تقاريرهم إلى مجلس الإدارة أو لجنة من مجلس الإدارة بشأن مخاطر الأمن السيبراني ، وكذلك مدى تكرار تقاريرهم.
  - ما إذا كان مجلس الإدارة بأكمله ، أو أعضاء معينين في مجلس الإدارة ، أو لجنة مجلس الإدارة هي المسؤولة عن الإشراف على مخاطر الأمن السيبراني.
  - ما إذا كان مجلس الإدارة على علم بمخاطر الأمن السيبراني وتواتر مناقشاته حول هذه المخاطر.
  - ما إذا كان مجلس الإدارة أو لجنة مجلس الإدارة ينظران في مخاطر الأمن السيبراني ، وكيفية ذلك ، كجزء من إستراتيجية الأعمال وإدارة المخاطر والرقابة المالية.
- خبرة مجلس الإدارة في مجال الأمن السيبراني ، إن وجدت ، وإشرافه على مخاطر الأمن السيبراني. يتضمن هذا معلومات عن:
  - ما إذا كان مجلس الإدارة لديه خبرة عملية في مجال الأمن السيبراني.
  - ما إذا كان المجلس قد حصل على شهادة أو درجة علمية في الأمن السيبراني.
  - ما إذا كان لدى مجلس الإدارة معرفة أو مهارات أو خلفية أخرى في مجال الأمن السيبراني.

بالإضافة إلى ذلك ، يتضمن الاقتراح تعديلاً على النموذج 8-K ، والذي سيتطلب من الشركات العامة الكشف عن حوادث الأمن السيبراني في غضون أربعة أيام عمل ، تمامًا كما هو مطلوب بالفعل لأي حدث جوهري آخر غير مجدول. تشمل هذه الإفصاحات ما يلي:

- متى تم اكتشاف الحادث وهل هو مستمر.
- وصف موجز لطبيعة ونطاق الحادث.
- ما إذا كانت أي بيانات قد تمت سرقتها أو تغييرها أو الوصول إليها أو استخدامها لأي غرض آخر غير مصرح به.
- تأثير الحادث على عمليات الشركة.
- ما إذا كانت الشركة قد عالجت الحادث أو تعمل حاليًا على إصلاحه.

ووفقًا للجنة الأوراق المالية والبورصات ، فإن هذه الإفصاحات ستزود المستثمرين بمعلومات "متسقة وقابلة للمقارنة ومفيدة لاتخاذ القرار". قال Gensler[15]: "اليوم ، يعد الأمن السيبراني خطرًا ناشئًا يجب على جهات الإصدار العامة التعامل معه بشكل متزايد". "إن الترابط بين شبكاتنا ، واستخدام تحليلات البيانات

[15]. Gary Gensler, “Statement on Proposal for Mandatory Cybersecurity Disclosures,” U.S. Securities and Exchange Commission (SEC), March 9, 2022, https://www.sec.gov/news/statement/gensler-cybersecurity-20220309.

التنبؤية ، والرغبة النهمة في البيانات تتسارع ، مما يعرض حساباتنا المالية واستثماراتنا ومعلوماتنا الخاصة للخطر. يرغب المستثمرون في معرفة المزيد عن كيفية إدارة المُصدرين لتلك المخاطر المتزايدة."

الأهمية التاريخية

من نواحٍ عديدة ، يعكس هيكل هذه القواعد الموصوفة قواعد إفصاح أخرى لـ *SEC* ، مثل تلك المتعلقة بالظروف المالية ونتائج التشغيل (Sarbanes-Oxley)، والمعلومات الداخلية ، ونقاط القوة والضعف والفرص والتهديدات التنظيمية. ومع ذلك ، فإن اتخاذ خطوة إضافية لزيادة مخاطر الأمن السيبراني للإشارة إلى ضرورة مثل هذه الإفصاحات أمر غير مسبوق إلى حد كبير.

يقول آندي واتكين تشايلد ، الشريك المؤسس لمجموعة أوغوستا وحلول بارافا الأمنية ومؤسس نموذج نضج الأمن السيبراني في أوروبا: "ربما تكون الولايات المتحدة هي الدولة الأولى ، وأود أن أقول الدولة الوحيدة في العالم التي تنظم الأمن السيبراني". (*CMMC* أوروبا). "قد تكون الشركات في الولايات المتحدة على دراية باللائحة العامة لحماية البيانات (*GDPR*) في الاتحاد الأوروبي وقد تكون سريعة في تجميع هذه المقترحات معًا ، ولكن حماية البيانات والأمن السيبراني نموذجان مختلفان. هناك فرق كبير ، بخلاف لائحة الإدارة المالية لوزارة الدفاع (*DoD*) - والتي يمكن أن تؤدي حتى إلى قيام وزارة العدل بالتحقيق في ثغرات الأمن السيبراني - لا يوجد شيء آخر مثله في مجال الأمن السيبراني ".

يشرح واتكين-تشايلد أيضًا كيف يمكن أن يكون لأهمية القواعد الجديدة تأثيرات مضاعفة قوية في الخارج. يقول: "لقد أثبتت أزمة أوكرانيا أن الأمن السيبراني سلاح ، وبالفعل اعتبره حلف الناتو درجة من العمليات منذ عام 2016". "الأمن السيبراني هو أداة هجومية إلى جانب الأسلحة النووية. المشكلة في ذلك لأنه مجال للعمليات ، فإنه يشكل تهديدا خطيرا للبنى التحتية الوطنية. إن اقتراح لجنة الأوراق المالية والبورصات (*SEC*) يصيب اللاعبين الكبار أولاً - الشركات التجارية - لكن إيماني هو أنه من المأمول أن يتدفق هذا إلى مؤسسات خارج نطاق اختصاص هيئة الأوراق المالية والبورصات لأن مشهد الأعمال ، فضلاً عن المشهد الفيدرالي ، متشابك للغاية على المستوى العالمي ".

في الحرب ، كما يقول واتكين تشايلد ، لا يمكن اعتبار الأمن السيبراني ضمن جيش واحد فقط. إذا كان أحد الحلفاء ضعيفًا ، فسيكون لذلك تأثير مباشر على العملية المشتركة بأكملها. لا تختلف حماية الأمن السيبراني للشركات العامة والخاصة. يقول: "إذا لم يتم اختراق أنظمة الأسلحة الأمريكية بينما يمكن للأنظمة البريطانية أن تتعرض للاختراق ، فلا فائدة من وجود حماية على الإطلاق". "هناك سبب تحدث الرئيس [الأمريكي] إلى الناتو فيما يتعلق ، من بين أمور أخرى ، بمعايير الأمن السيبراني المشتركة. إنه الشيء الصحيح الذي يجب فعله ، لأنه إذا استخدم كيان مثل روسيا قطاع الأعمال لمهاجمة مولدات الطاقة ، على سبيل المثال ، المياه والكهرباء والغاز والرعاية الصحية الخاصة بك - فقد انتهى كل شيء. "

من الواضح أن مثل هذه النتائج المحتملة هي ذات طبيعة كلية ، ولكن من المهم عدم استبعاد النتائج على مستوى المنظمة أيضًا. وعلى الرغم مما قد يشعر به المرء عند رؤية القوائم الشاملة للعناصر التي يمكن أن تضمن إدراجها في عمليات الكشف عن الأمن السيبراني ، فليست كل النتائج سلبية.

يقول واتكين تشايلد: "بالطبع ، هناك الجانب القانوني لعمليات الإفصاح ، ولكن ، كما تنص المقترحات ، فأنت لا تقدم تقارير إلى لجنة الأوراق المالية والبورصات فقط. أنت تقدم تقارير إلى جميع المشاركين في السوق الذين قد يكون لهم تأثير على عملك. المجتمع الاستثماري ، ووكالات التصنيف الائتماني ، وشركات التأمين - سوف يرون جميعًا جنبًا إلى جنب مع هيئة الأوراق المالية والبورصات (*SEC*) إلى أي مدى أنت جيد في مجال الأمن السيبراني ، أو لا ، حسب الحالة. تأتي هذه الشفافية مصحوبة بالمخاطر ، ولكنها تمثل أيضًا فرصة ".

دور التدقيق الداخلي لا يزال ثابتًا

التحديد والتقييم والتواصل

الأدوات في مكانها الصحيح

قدم قانون ساربينز أوكسلي لعام 2002 *(SOX)* مسؤوليات إضافية وفتح فرصًا جديدة لوظائف التدقيق الداخلي لإضافة قيمة لمنظماتهم. في الواقع ، مع اجتياز المنظمات للتشريع الجديد ، أصبح التدقيق الداخلي بالنسبة للكثيرين مرادفًا للامتثال *SOX* . نظرًا لطبيعة مقترحات *SEC* الجديدة ، هناك سبب للاعتقاد بأن الأمر نفسه يمكن أن يحدث في مجال الأمن السيبراني.

للوهلة الأولى ، قد يبدو هذا استحالة قصيرة المدى على الأقل بسبب الطبيعة المعقدة لمجال الأمن السيبراني. وفقًا للمشاركين في استطلاع Pulse survey[16]، يشكل الأمن السيبراني في المتوسط 9 ٪ فقط من تخصيص خطة التدقيق في المؤسسات المتداولة علنًا ، وهو ما يزيد عن 7 ٪ في السنوات الثلاث السابقة ولكن أقل بكثير من 35 ٪ المخصصة لإعداد التقارير المالية. هناك عدة أسباب وراء حدوث ذلك ، مثل قيود الميزانية ، ونقص الموارد الكافية ، ونقص المعرفة أو الخبرة.

ومع ذلك ، فإن القيمة الحقيقية التي يمكن أن يوفرها التدقيق الداخلي ليست بالضرورة من خلال المعرفة بالأمن السيبراني ، ولكن المعرفة بتحديد المخاطر ، والإبلاغ عن المخاطر ، وتقييم الضوابط لمعالجة المخاطر. في الواقع ، هذه هي الأشياء التي ترغب مقترحات هيئة الأوراق المالية والبورصات في التأكيد عليها لخطر واحد محدد.

يقول واتكين تشايلد: "من المهم أن ندرك أن هذه المقترحات لا تتعلق حقًا بالأمن السيبراني ، بل تتعلق بإدارة مخاطر الأمن السيبراني". "عندما يفكر الناس في الأمن السيبراني ، فإنهم جميعًا يفكرون في تنفيذ الضوابط وإصلاح الأشياء. ما تبحث عنه هيئة الأوراق المالية والبورصات هو شيء مختلف تمامًا ؛ إنهم يبحثون عن مؤسسات لتقييم مخاطر الأمن السيبراني لديهم. إنهم يريدون من مجالس الإدارة في المؤسسات أن يكون لديها هياكل حوكمة قائمة لتقييم وضمان الإشراف على برنامج إدارة مخاطر الأمن السيبراني ، مهما كان الشكل الذي قد يتخذه ".

يقول مانوج ساتناليوالا ، الرئيس التنفيذي للتدقيق في شركة *Caliber Home Loans، Inc*.: "ما تريد لجنة الأوراق المالية والبورصات الأمريكية رؤيته هو تحمل مجالس الإدارة مسؤولية الإشراف وضمان الباقي". توجيه المنظمات ، مثل *NIST Cybersecurity Framework*. الفجوة الحقيقية تكمن في المساءلة ، والتي يمكن أن تتحول بسرعة إلى تأرجح المسؤولية ".

يمكن أن يساعد دور التدقيق الداخلي في تحقيق التوازن لهذه التأرجح. "المجالس والإدارة ، يحتاجون إلى المساعدة. إن التدقيق الداخلي من خلال التأكيد يضمن المساءلة ، ومن خلال الرؤية المعززة عبر المؤسسة ، يعزز ملكية المخاطر المشتركة "، كما يقول ساتناليوالا. "الخطر مختلف ، لكن دور التدقيق الداخلي يظل ثابتًا حقًا. لا يجب أن تبدأ وظائف التدقيق بلبحث ببدايات الأمور ، ومن غير المعقول أن نتوقع أن تدخل كل إدارة تدقيق داخلي في التفاصيل الجوهرية لبرنامج الأمن السيبراني ، ولكن فيما يتعلق بهذا التحدي ، فإن الأمر لا يتعدى مجرد النظر في مقترحات لجنة الأوراق المالية والبورصات والسؤال ، "ما هي توقعات هيئة الأوراق المالية والبورصات الأمريكية؟" طالما أن هناك على الأقل بعض موارد الأمن السيبراني موجودة بالفعل ، لا أعتقد أن هناك حاجة إلى أي تغييرات في متوسط وظيفة التدقيق الداخلي بخلاف أساليب التغيير والتبديل لضمان التغطية المناسبة للمخاطر. "

ومع ذلك ، فإن الوصول إلى موارد الأمن السيبراني غالبًا ما يكون قولًا أسهل من فعله. لن يتم تطوير أي درجة من الخبرة في الأمن السيبراني من خلال التدريب والشهادات بين عشية وضحاها ، وخاصة بالنسبة لوظائف التدقيق الداخلي الصغيرة ذات الميزانيات المحدودة لتوظيف المواهب المكلفة والمطلوبة بشدة ، فإن خيارات أداء أي نوع من الأدوار بخلاف الامتثال القائم على العمليات محدودة. في هذه الحالات ، يجب أن يكون لدى التدقيق الداخلي فهم شامل لأماكن الوصول إلى المعرفة على أفضل وجه. هذا يمكن أن يكون:

- **ضمن قاعدة المواهب الخاصة بالمؤسسة** . غالبًا ما يكون لدى أولئك الذين لديهم خبرة في قدرات تدقيق تكنولوجيا المعلومات الأكثر تقليدية قاعدة المعرفة لإكمال التدريب التقني على الأمن السيبراني بسرعة نسبيًا. بالإضافة إلى ذلك ، يمكن دمج أساسيات معينة للأمن السيبراني في مجالات مثل

[16]. The IIA, “2022 North American Pulse of Internal Audit,”

إدارة التغيير ، وضوابط الوصول ، وعمليات تكنولوجيا المعلومات ، والتعافي من الكوارث ، مما قد يقلل من الحاجة إلى الاستعانة بمصادر خارجية على المدى الطويل.

- **من خلال التعاون مع كل من الخط الثاني ووظائف التدقيق الخارجي الموثوق بها**. بينما يجب الحفاظ على استقلالية التدقيق الداخلي وموضوعيته وفقًا للمعايير الدولية للممارسة المهنية للتدقيق الداخلي *(IPPF)* ، فإن إنشاء علاقة عمل أكثر تعاونًا مع الوظائف ذات الصلة مثل تكنولوجيا المعلومات يمكن أن يوفر للمراجعين إمكانية الوصول غير المباشر إلى الكفاءات الفنية التي قد يكون الحصول عليها صعبًا أو مكلفًا.

الاستنتاج

حان وقت الاستعداد

يتطور الأمن السيبراني ، كموضوع ، دائمًا مع استمرار الجهات المسيئة والمرتكبة في الابتكار في مناهجها واستمرار الشركات في الابتكار لإحباطها. ومع ذلك ، مع استمرار كتابة تاريخ الأمن السيبراني ، سيتم تذكر عام 2022 للمعالم التي تم تحقيقها في محاولة لمواجهة الاتجاهات الرهيبة التي شوهدت عبر عالم الاعمال . على الرغم من أن مقترحات لجنة الأوراق المالية والبورصات يجب أن تخضع لفترة 60 يومًا للتعليقات قبل إصدار القواعد الرسمية ، إلا أنه لا ينبغي أن يكون هناك الكثير من المفاجأة للشركات المتداولة علنًا ووظائف التدقيق الداخلي الخاصة بها.

يمكن للتدقيق الداخلي ويجب أن يستخدم الوقت المتاح له ، إذا لم يكن قد فعل ذلك بالفعل ، لتقييم النطاق الكامل لأصول مؤسسته التي يجب أن تؤخذ بعين الاعتبارلاحتسابها في استراتيجية الأمن السيبراني. بدون هذه المعرفة ، سيجد المدققون الداخليون صعوبة في تقييم ما إذا كانت الضوابط والسياسات واستراتيجيات الحوكمة الحالية المتعلقة بالفضاء الإلكتروني كافية. مثل هذه التقييمات ليست مهمة فقط لأغراض الأمن التنظيمي ، ولكن في الواقع لمجتمع العمل بأكمله. أصبح العالم أكثر ترابطا يوما بعد يوم ، وهذا يعني أن المسؤوليات المتعلقة بالمخاطر مثل الأمن السيبراني هي مشتركة إلى حد كبير. وكما هو معروف، وكما أظهر التاريخ مرارًا وتكرارًا ، يمكن أن يكون لخرق إحدى المنظمات تأثير حقيقي للغاية على أمن منظمة أخرى.

إن قوة السلسلة تعادل قوة أضعف حلقاتها.

الشركاء المهمون – التدقيق الداخلي ومدير إدارة أمن المعلومات

عن الخبراء

جيري بيرولو

جيري بيرولو هو مؤسس شركة*Adversarial Risk Management* ، وهي شركة لاستراتيجيات برامج الأمن السيبراني والحوكمة التي تمكن الشركات النامية من إنشاء برامج أمن سيبراني مناسبة بسرعة. قبل تأسيس*Adversarial* ، تقاعد بيرولو كرئيس تنفيذي لأمن المعلومات في *IntercontinentalExchange (NYSE: ICE)* بعد 20 عامًا من بناء وقيادة برامج الأمن السيبراني في مجموعة من أهم المجموعات الاقتصادية في العالم بما في ذلك بورصة نيويورك. بيرولو هو *NACD Directorship Certified®* ، عمل أيضًا في مجلس إدارة مركز تبادل وتحليل معلومات الخدمات المالية *(FS-ISAC)* لمدة 6 سنوات، كان آخرها رئيسًا. يحاضر بيرولو في معهد جورجيا للتكنولوجيا حيث يعمل أستاذًا للممارسة في كلية الأمن السيبراني والخصوصية ويشارك خبراته مع قادة مخاطر التكنولوجيا من خلال البث الصوتي لموقع *lifeeafterCISO.com*

حسن خيال، CIA, CRMA, CFE

حسن خيال هو مدير تدقيق داخلي في دبي. تم تصنيفه من قبل معهد المدققين الداخليين *(IIA)* كواحد من أفضل 15 قائدًا ناشئًا عالميًا تحت 30 عامًا. حاصل على بكالوريوس في إدارة الأعمال وماجستير في إدارة الأعمال وشهادة في دراسات الشرق الأوسط. وهو أيضًا *CIA* و *CRMA*و *CFE*. حاصل على شهادات مهنية في مكننة العمليات الروبوتية*(RPA)* ، وتحليلات البيانات، وإنترنت الأشياء*(IoT)* ، وإدارة الجودة، والصحة والسلامة، والإدارة البيئية، وإدارة المخاطر.

آلان ماران

ألان ماران هو رئيس قسم التدقيق الداخلي في *Chewy Inc.* يعمل في الشركة منذ يناير 2019. وفي هذا المنصب، هو مسؤول عن الإشراف على الأنشطة الاستراتيجية والتنفيذية الشاملة لوظيفة التدقيق الداخلي، بما في ذلك أداء تقييمات مخاطر المؤسسة، وتقديم الدعم الاستشاري المستمر وفي الوقت المناسب لمختلف الأنشطة التي تدعمها الإدارة ؛ والتأكيد على ملاءمة الضوابط على المخاطر الرئيسية المحددة للمؤسسة، والمواءمة مع العمليات وأنظمة الشركة وحوكمة تكنولوجيا المعلومات والمخاطر والامتثال *(GRC)* عبر الشركة، والتركيز المستمر على تطوير أعضاء فريق التدقيق الداخلي، مع زيادة التركيز على تحليلات البيانات والأمن السيبراني وخصوصية البيانات. آلان هو مدير تنفيذي متمرس في مجال التدقيق يتمتع بخبرة تزيد عن 22 عامًا في مجال التجارة الإلكترونية، والتكنولوجيا المالية، والتكنولوجيا، وشركات التصنيع، ولا يزال شغوفًا بالتعلم. قبل انضمامه إلى*Chewy* ، شغل مناصب قيادية تقدمية بدأ حياته المهنية في*Ernst & Young* ، و*LLC*، ثم تقدم إلى مناصب أخرى للتدقيق الداخلي في مؤسسات *Fortune 500* متعددة الجنسيات. حاصل على ماجستير في إدارة الأعمال. وماجستير في المالية من جامعة ولاية واشنطن. هو محقق الاحتيال المعتمد*(CFE)* ، وخبير معتمد في سلسلة الكتل*(Blockchain)* ، ومنتسب إلى الفروع المحلية لمعهد المدققين الداخليين.

سرينى سرينيفاسان **PMP, CBIP**

سرينى سرينيفاسان هو الرئيس التنفيذي لأمن المعلومات والبيانات في *Chewy Inc.* يعمل في الشركة منذ أكتوبر 2019، عندما انضم كرئيس لأنظمة الأمن والبيانات والشركات. في هذا المنصب، هو مسؤول عن الإشراف على أمن المعلومات وإدارة البيانات ومنصات التحليلات وأنظمة الشركات وحوكمة تكنولوجيا المعلومات والمخاطر والامتثال *(GRC)* عبر الشركة. هو مدير تنفيذي محنك في مجال التكنولوجيا يتمتع بخبرة تزيد عن 25 عامًا تشمل التجارة الإلكترونية والخدمات المصرفية والمالية وتجارة التجزئة والتسويق. قبل انضمامه إلى*Chewy* ، شغل مناصب قيادية في *Citizens Financial Group.* وهو حاصل على درجة الماجستير في علوم الكمبيوتر من جامعة بهاراتيداسان وماجستير إدارة الأعمال من جامعة بنتلي.

المقدمة

شراكات الأمن السيبراني ضرورة للنجاح

لا يزال الأمن السيبراني من بين أكبر المخاطر لجميع المؤسسات. تعكس الاستطلاعات باستمرار الجهود الدؤوبة والوقحة من قبل مجرمي الإنترنت لاختراق البيانات الحساسة أو إغراء غير المدربين وغير المرتابين في إفشاء معلومات حساسة أو السماح بالوصول إلى جهات سيئة.

على سبيل المثال، يعكس تقرير تحقيقات فيريزون لخرق البيانات لعام 2022 زيادة مذهلة بنسبة 13٪ في الانتهاكات المتعلقة ببرامج الفدية في عام 2021، وهي أكبر من السنوات الخمس الماضية مجتمعة. ومع ذلك، وجد التقرير أن أنجح الطرق لهجمات برامج الفدية لا تزال ثابتة - إساءة استخدام مشاركة المكتب وبرامج الوصول عن بُعد (40٪) والبريد الإلكتروني (35٪)، وفقًا لتقرير *Verizon* .

تم تصميم إرشادات جديدة من المعهد الدولي للمدققين الداخليين *(IIA)* ، تدقيق عمليات الأمن السيبراني: المنع والكشف *(GTAG)* ، لمساعدة المؤسسات على فحص عمليات الأمن الإلكتروني وتحديد أولوياتها. ويهدف إلى مساعدة المدققين الداخليين على تحديد عمليات الأمن السيبراني، وتحديد مكوناتها، والنظر في إرشادات الرقابة ذات الصلة في أطر التحكم في تكنولوجيا المعلومات، وفهم مناهج تدقيق عمليات الأمن السيبراني.

يتمثل أحد مفاتيح تحسين ضمان الأمن السيبراني الذي لا يشمله التوجيه في وجود علاقة صحية بين رؤساء التدقيق الداخلي وكبار مسؤولي أمن المعلومات *(CISOs)*. يمكن أن تساعد هذه العلاقة التكافلية المحتملة في مواءمة التدقيق الداخلي وأمن المعلومات في الأطر والمخاطر والضوابط مع دعم إدارة ملف تعريف مخاطر الأمن السيبراني الموسع.

يفحص "ملخص المعرفة العالمي" هذا فوائد العلاقة القوية بين رؤساء التدقيق الداخلي ونظرائهم في مجال أمن المعلومات، وينظر في المسارات لإنشاء ورعاية مثل هذه العلاقات مع ضمان استقلالية التدقيق الداخلي، ويقيم كيف يمكن لهذه الشراكات أن تضيف قيمة إلى المنظمة.

قضية الأمن السيبراني الجماعي

تتطلب المخاطر السيبرانية نهجًا على مستوى المؤسسة

لا يزال الأمن السيبراني يمثل مجالًا متزايدًا ومتطورًا للمخاطر حيث يشهد كل عام نمو مخططات مجرمي الإنترنت بشكل أكثر تعقيدًا ووفرة. لا يوجد نقص في الإحصاءات لإظهار أن المنظمات لا تزال عرضة للهجمات السيبرانية . في الوقت نفسه، يتزايد الضغط على المؤسسات عبر طيف الصناعة لتبني استراتيجيات الأعمال القائمة على البيانات التي تعتمد بشكل كبير على جمع البيانات وإدارتها وتحليلها واستخدامها مع الاستفادة من التكنولوجيا الجديدة لتحسين الأداء والنتيجة النهائية.

كما هو الحال مع مجالات المخاطر الكبيرة الأخرى، يجب فهم المخاطر السيبرانية وإدارتها عبر المؤسسة. ومع ذلك، هناك عدد قليل من المؤسسات التي تتبع نهجًا شاملاً لإدارة الأمن السيبراني، وفقًا لتقرير "حالة المرونة الإلكترونية" *17*، وهو تقرير من شركة *Microsoft* وشركة مارش لوساطة التأمين وإدارة المخاطر. استنادًا إلى دراسة استقصائية لأكثر من 600 من صانعي القرار بشأن المخاطر السيبرانية ، وجد التقرير أن حوالي 4 فقط من كل 10 مؤسسات تشارك الشؤون القانونية، أو التخطيط المؤسسي، أو المالية، أو العمليات، أو إدارة سلسلة التوريد في وضع خطط المخاطر السيبرانية *18* .

"أحد الأشياء التي تعيق الثقة هو أن معظم الشركات لم تعتمد نهجًا شاملاً للمخاطر السيبرانية ؛ واحدة تدور في جوهرها حول الاتصالات واسعة النطاق وتعزيز التعاون والمواءمة بين أصحاب المصلحة خلال لحظات الحقيقة الرئيسية لصنع القرار في رحلة المرونة الإلكترونية الخاصة بهم "، وفقًا للتقرير.

من بين اتجاهات المخاطر الرئيسية المحددة في التقرير:

"يجب مواءمة الأهداف الخاصة بالمخاطر السيبرانية - بما في ذلك تدابير الأمن السيبراني والتأمين والبيانات والتحليلات وخطط الاستجابة للحوادث - لبناء وسائل الدفاع الإلكترونية مقابل الاكتفاء بمنع الحوادث فقط، حيث يمكن لكل منظمة أن تتوقع هجومًا إلكترونيًا."

لدعم نهج مؤسسي فعال، يمكن لرؤساء التدقيق الداخلي المساهمة بشكل كبير من خلال إنشاء ورعاية العلاقات مع مدراء أمن المعلومات. يجب أن تستند هذه العلاقات على التفاهم المتبادل والأهداف والاحترام.

قال جيري بيرولو، مدير أمن المعلومات المخضرم ومؤسس شركة *Intercontinental Exchange* التابعة لبورصة نيويورك (*NYSE: ICE*)، إن الاتصالات الضعيفة أو الفهم غير الواضح لأمن المعلومات وأدوار التدقيق الداخلي يمكن أن يضر بالمواءمة في الأمن السيبراني. وعلى العكس من ذلك، فإن العلاقة الجيدة بين رؤساء التدقيق الداخلي وأمن المعلومات تفتح الباب أمام فهم أعمق للأهداف والاستراتيجيات والعمليات والسياسات التي يمكن أن تجعل التدقيق الداخلي - وبالتالي نتائجه وتوصياته - أكثر صلة بقادة المخاطر السيبرانية ، والإدارة التنفيذية ومجلس الإدارة. علاوة على ذلك، تعمل العلاقة القوية بين التدقيق الداخلي وفرق أمن المعلومات على توسيع المعرفة بالمهمة الحرجة لكل منطقة وكيفية دعمهما للأمن السيبراني بشكل عام.

قال بيرولو: "في نهاية المطاف، يريد التدقيق الداخلي التعرف على أمن المعلومات". "هناك العديد من الطرق للقيام بذلك، ولكن لا يوجد شيء مثل التعلم من فريق (أمن المعلومات) نفسه."

في عمله الاستشاري مع الشركات الناشئة، غالبًا ما يبدأ بيرولو بإعداد برامج حوكمة للأمن السيبراني. يتضمن ذلك عادةً إنشاء لجنة حوكمة للأمن السيبراني متعددة الوظائف يمكن أن تشمل الإدارة التنفيذية والتمويل والقانون وأمن المعلومات. وقال إنهم غالبًا ما يشملون أيضًا كبار المديرين التنفيذيين للتدقيق الداخلي كمراقبين.

17. "2022 Marsh and Microsoft Cyber Risk Survey"

18. «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.

خمسة مفاتيح أساسية للنجاح

فوائد العلاقة القوية بين التدقيق الداخلي وإدارة أمن المعلومات

يحدد التدقيق الداخلي و أمن المعلومات العديد من الفوائد للشراكة الجيدة التصميم. يمكن أن تختلف تفاصيل هذه الشراكات ومدى تطورها اعتمادًا على حجم المؤسسة، أو مستوى التنظيم في كل صناعة، أو ملف تعريف مخاطر الأمن السيبراني للمؤسسة. ومع ذلك، تظهر خمسة مجالات حيث يمكن للتعاون والتكامل أن يخلقوا فوائد واضحة بغض النظر عن حجم المنظمة أو الصناعة التي تعمل فيها.

فهم ومواءمة ملف تعريف المخاطر السيبرانية للمؤسسة

ملف تعريف المخاطر هو تحليل كمي لأنواع التهديدات التي تواجهها المؤسسة. من منظور الأمن السيبراني، يحدد هذا التحليل الأصول والمخاطر السيبرانية ، ويفحص السياسات والممارسات المصممة لإدارة تلك المخاطر، ويسعى جاهداً لفهم أي نقاط ضعف قد تكون موجودة. يوفر فهم التدقيق الداخلي لملف تعريف المخاطر السيبرانية أساسًا لبناء خطة تدقيق لا تدعم النهج العام للمؤسسة تجاه الأمن السيبراني فحسب، بل يمكنها أيضًا تحسين أهمية التدقيق الداخلي وقيمته في هذا المجال المهم.

طوَّر آلان ماران، رئيس قسم التدقيق الداخلي في شركة *Chewy Inc.* ،، علاقة قوية مع مدير أمن المعلومات في المنظمة، سريني سرينيفاسان، على مدار السنوات الثلاث التي انقضت منذ أن أصبح بيع أغذية الحيوانات الأليفة وغيرها من المنتجات المرتبطة بالحيوانات الأليفة متاحًا للجمهور. قال سرينيفاسان إن أمن المعلومات دخل في شراكة مع التدقيق الداخلي، وأصحاب المصلحة القانونيين وغيرهم من أصحاب المصلحة لتقييم وقياس ملف المخاطر السيبرانية للشركة بشكل شامل استنادًا إلى إطار عمل الأمن السيبراني.*NIST*

قال سرينيفاسان: "هذا هو خط الأساس لدينا". ثم وضعنا بعد ذلك خارطة طريق مدتها ثلاث سنوات للأمن السيبراني والحوكمة، وقمنا بتصميمها وتعزيزها بناءً على تقييم إطار عمل الأمن السيبراني الذي قمنا به. نقوم الآن بإجراء تقييم على أساس سنوي لمعرفة ما إذا كنا نجري تحسينات في مجالات الفرص هذه وتقييم كيفية قياس درجات المخاطر الإجمالية لدينا."

سمح هذا النهج التعاوني الذي يتضمن تدقيقًا داخليًا منذ البداية بوضع إستراتيجية متبادلة تتضمن ضمان التدقيق الداخلي والخدمات الاستشارية بهدف التحسين المستمر لموقف الشركة العام للأمن السيبراني.

قال ماران: "إن مفهومنا ليس أننا بحاجة دائمًا إلى تدقيق تكنولوجيا المعلومات والأمن. بل أننا، من جانب التدقيق الداخلي، نرى أننا شريك مع عقلية قوية لدعم سريني وفريقه في تطوير إستراتيجية كاملة".

ومن المزايا الإضافية لهذا التعاون أنه يتم دمج أمن المعلومات والضمان المستقل في المشاريع الجديدة في وقت مبكر. وبعبارة أخرى، فإن أمن المعلومات والتدقيق الداخلي وضوابط الحوكمة لم تعد تأتي بعد الانتهاء من المشروع، كما قال سرينيفاسان.

"ما نقوم به هو، مع بدء مبادرات المشروع، يشارك كلا الفريقين لدينا ويتشاركان مع فرق الهندسة وفرق الإنتاج وفرق العمل. . . ما هي اعتبارات الأمن؟ هل نتبع أفضل الممارسات؟ " قال سرينيفاسان.

قال سرينيفاسان إن هذا النهج يساعد في تحديد وتقليل، وإذا أمكن، القضاء على المخاطر السيبرانية من خلال بناء العمليات والضوابط المناسبة أثناء تطوير المشروع. "لذلك، عندما يبدأ المشروع، يصبح الأمر سهلاً للغاية لكلا (الفريقين) لأن لدينا فهمًا قويًا. عندما نتابع إما تقييمات رقابة التدقيق أو مراجعات الوصول أو ضوابط الحوكمة، يكون لدينا الكثير من الأفكار."

فهم الأدوار

تم دعم العلاقة التي أقامها ماران وسرينيفاسان بشكل كبير من خلال شركة *Chewy* كونها شركة جديدة نسبيًا يتم تداولها علنًا، مما وفر فرصة لتشكيل العلاقة من الألف إلى الياء. وضع هذا أيضًا توقعًا للتواصل المفتوح والمتكرر بين *Maran* و *Srinivasan* وفرقهما.

قال سرينيفاسان: "لقد كانت طريقة مثالية لتأسيس هذه الشفافية والثقة بين أصحاب المصلحة الرئيسيين، لذلك لم نكن نريد ترك هذه الفرصة تفوت."

هذا لا يعني أنه لا توجد خلافات أبدًا. وقال سرينيفاسان إنه عندما تنشأ الخلافات، فإن العلاقة تجعل من السهل مناقشتها والتوصل إلى حل يخدم كلا الجانبين.

قال "ليس هناك فائدة بالنسبة لي لإبعاد أي شيء عن التدقيق الداخلي". "كلما عرفوا أكثر عن ما نقوم به، كلماازداد مستوى تقديرهم لنا. وبنفس الطريقة من منظور التدقيق الداخلي، يمكنني أن أخبرك أنني أعتقد أنه لا توجد "مشاكل" هنا."

في نهاية المطاف، يسمح النهج التعاوني بالعمل بطريقة رشيقة حيث يكون التدقيق الداخلي جزءًا لا يتجزأ من عملية يمكن فيها اكتشاف أوجه القصور ومعالجتها في وقت مبكر، كما قال سرينيفاسان.

يضيف ماران أن التفاعل الصريح يؤكد ويعزز الفهم المتبادل للأدوار.

وقال "سريني لا يفترض أننا نعرف كل شيء، لكنه في نفس الوقت يحترم مخاوفنا ووجهة نظرنا."

وثاقة الصلة بالموضوع

يعد توفير رؤى ونتائج تأكيدية بشأن القضايا الهامة في الوقت المناسب أحد أكبر تحديات التدقيق الداخلي في أي مجال من مجالات المخاطر، ولكن بشكل خاص للأمن السيبراني. تتطلب هذه المخاطر دائمة التطور والسريعة أن يكون الضمان ذا صلة وفي الوقت المناسب.

حذر بيرولو من أن مشاركات التدقيق الداخلي والتوصيات ذات الصلة التي لا تتوافق مع مهمة الأمن السيبراني للمؤسسة يمكن أن تضر أكثر مما تنفع. يمكنهم خلق ارتباك داخل أمن المعلومات حول ما يريد التدقيق الداخلي رؤيته، خاصة إذا كان التدقيق الداخلي غير متأكد.

وقال: "قد لا يكون لدى التدقيق الداخلي في البداية فكرة جيدة عما يريد رؤيته". "من الأفضل التعاون في التدقيق المسبق ومراقبة عملية الحوكمة السيبرانية لضمان توافق عمليات التدقيق مع المهمة."

قال حسن خيال، مستشار التدقيق الداخلي ذو الخبرة في مجال الإنترنت، إن هذا مجال يكون التدقيق الداخلي فيه عرضة للنقد بشكل خاص. في كثير من الأحيان، يتجنب المدققون الداخليون التعرف على أعضاء فرق تكنولوجيا المعلومات أو أمن المعلومات ومعرفة المزيد عن الموضوع تحت ستار حماية استقلالية التدقيق الداخلي.

"ذهبت بلا خجل مع مهماتي الأولى وأقول لموظف تكنولوجيا المعلومات ،" اسمع، أنا هنا أكثر لأتعلم منك أكثر من أي شيء آخر. " أود أن آخذ الشخص الذي لديه فهم العملية أو الفهم التقني وإجراء محادثة غداء ودية حتى أعرف بالضبط الأجزاء الدقيقة لما يفعله."

وقال خيال إن هذه العملية التعليمية تساعد أيضًا المدقق الداخلي على فهم نضج الأمن السيبراني للمؤسسة، وهو أمر بالغ الأهمية لتقديم التوصيات ذات الصلة.

قال: "إذا كنت تتحدث عن مؤسسة صغيرة إلى متوسطة الحجم، أو حتى مؤسسة أكبر لا يتم تداولها علنًا، فهناك الكثير الذي يمكنك فعله أو ينبغي عليك فعله". "في مرحلة معينة، يمكن أن تكون التوصيات شديدة الجرأة، لذا فإن التوصيات التي تقدمها ليست واقعية."

إن بناء علاقة قوية بين فرق التدقيق الداخلي وأمن المعلومات يقلل من احتمالية وجود ارتباطات وتوصيات تدقيق غير ملائمة أو مضللة. تم تأكيد هذه الميزة في *Chewy*.

قال سرينيفاسان: "فريق آلان وآلان نفسه على دراية كبيرة بما هي إستراتيجيتنا الأمنية الشاملة، من منظور تكنولوجي، وما الذي نفعله حيال ذلك، وما هي بعض المخاطر الرئيسية لدينا". لذلك، ليس لدينا فجوة كبيرة بين تصنيفات المخاطر وقدراتنا الداخلية. سيستمر هذا في مساعدتنا على القيام بعمل أفضل من حيث تحسين المعرفة العامة لفريقنا أو أعضاء فريقنا في *Chewy* وكذلك فريق القيادة لدينا."

التواصل مع مجلس الإدارة والإدارة التنفيذية

توفر الثقافة التنظيمية لشركة *Chewy* عرضًا أكبر للمخاطر مدعومًا بالمحادثات المفتوحة. اضطلع ماران وسرينيفاسان بأدوار تثقيف أصحاب المصلحة - الإدارة التنفيذية ومجلس الإدارة - حول تعاونهم والفوائد التي حققها.

"في الكثير من المنظمات هناك، يتخذ الناس النهج المنعزل. مثل القول "إنه أمن تكنولوجيا المعلومات، لذلك سنتحدث مع رئيس قطاع تكنولوجيا المعلومات *CISO*، وسيتولى *CISO*." ولكن ضمن منظور إدارة المخاطر المتكاملة أو إدارة مخاطر المؤسسة، يمكن أن تأتي أي مخاطر نراها للشركة قال ماران: " "يمكن للهجوم الإلكتروني أن يؤثر على عملياتك وإنجازاتك وأمورك المالية. قام سرينى أيضًا بعمل جيد في تثقيف القيادة بشأن ما نقوم به والمخاطر التي نخففها. لذلك، من هذا المنظور، لقد كان تعاونًا."

ويترجم هذا أيضًا إلى استجابات سريعة وذكية لتغير المخاطر والمشهد السيبراني التنظيمي. على سبيل المثال، لدى ماران و سرينيفاسان ثقة متزايدة في أن المنظمة يمكن أن تستجيب لقواعد الإبلاغ عن الأمن السيبراني المقترحة من هيئة الأوراق المالية والبورصات الأمريكية والتي تم الكشف عنها في الربع الأول من عام 2022.

يتجاوز هذا التعاون أمن المعلومات والتدقيق الداخلي أيضًا. قال سرينيفاسان: "لا يقتصر الأمر على أمن المنظمة". "لدينا أصحاب مصلحة رئيسيون آخرون حيث لدينا شراكات مماثلة، بما في ذلك فريق المحاسبة والفريق القانوني. أعتقد أن إنشاء هذه العلاقات الشفافة يضعنا جيدًا عندما تظهر هذه اللوائح المتطورة والمتطلبات الإضافية في الصورة."

بينما تستفيد قيادة *Chewy* من الرسائل المتسقة والموحدة، يحذر خيال من مخاطر كبيرة عندما لا تكون القيادة على اطلاع على حالة واحتياجات الأمن السيبراني للمؤسسة. وقال إن تكنولوجيا المعلومات والأمن السيبراني يمكن أن يُنظر إليهما بسرعة على أنهما ببساطة مراكز تكلفة عندما لا يتم إعلام القادة وتثقيفهم حول هذا الموضوع. قال خيال إنه عندما يبتعد التدقيق الداخلي عن فهم أمن المعلومات، فمن غير المرجح أن يقدموا تأكيدات قيّمة وذات صلة في هذا المجال. يؤثر هذا على وجهات النظر حول الأمن السيبراني من منظور الإدارة التنفيذية ومجلس الإدارة.

حماية الاستقلالية واحترامها

قال خيال، الذي يعمل على أن يصبح مدققًا معتمدًا لنظم المعلومات*(CISA)* ، إن التزامه بالحصول على الشهادة قد عزز بالفعل مصداقيته بين محترفي تكنولوجيا المعلومات وأمن المعلومات. كما أنه سمح له بالتفاعل مع زملائه في العمل على مستواهم، مما يزيد من احتمالية تطوعهم بالمعلومات التي يمكن اعتبارها متقدمة جدًا أو معقدة بالنسبة للمدقق الذي يأتي فقط عند تنفيذ مهمة تدقيق. علاوة على ذلك، فهو لا يرى أن هذا التفاعل يمثل تهديدًا لقدرته على إجراء عملية تدقيق مستقلة وموضوعية.

قال: "في النهاية ، أنت في مكان العمل". "عندما نطلب من المراجعين أن يكونوا مستقلين، أنا شخصياً لا أعتقد أننا نقول لهم ،" لا يمكن أن يكون لديك أصدقاء في العمل ؛ يجب أن تذهب لتناول الغداء بمفردك."

قال خيال إنه يتبع هذا النهج في جميع ادارات المؤسسة. سيتحدث عن *Linux* مع موظفي الكمبيوتر أو وسائل التواصل الاجتماعي مع موظفي التسويق.

قال "إنها فرصة جيدة لتطوير نفسك مهنيا مع الحفاظ على العلاقات". "يشبه الأمر عندما نخبر عملاء التدقيق أو المدققين لدينا ،" نحن ننظر في العملية والمعاملات ؛ نحن لا نطارد الناس. "لذلك، عندما تأخذ الناس لتناول الغداء، فأنت لا تقوم بالعملية أو الصفقة."

قال ماران إن علاقة العمل الوثيقة بين ماران وسرينيفاسان في *Chewy* تدعم التفاهم المتبادل للحاجة إلى التحقق المستقل.

"طبيعة مهنتنا هي ثق أولا ولكن تحقق دائما. من وجهة نظر الموضوعية، من واجبي القيام بذلك. "لذا، نعم، نحن نثق بمستوى معين، خاصة الأشياء الإضافية التي اختبرناها. في معظم الحالات، نتحقق من أن الأمور لم تتغير. لكنني أواصل أيضًا اختبار سلامة المعلومات المقدمة من الإدارة. نحن لا ننظر إلى التقرير فقط في ظاهره ؛ نعود إلى المصدر للتأكد من حصولنا على نفس النتائج كما هي للتأكد من أنها كاملة ودقيقة."

قال ماران، في نهاية المطاف، أن فهم دور بعضنا البعض في المنظمة يجعل الأمر أسهل.

"هناك اتفاق هنا. هذا ما علي فعله. هذا هو التأكيد الذي أحتاج إلى تقديمه للقيادة العليا - مجلس الإدارة وأصحاب المصلحة ولجنة التدقيق. "نحن نقوم بمواءمة عمليات التدقيق التي سنقوم بها لهذا العام. نحن نتماشى مع النطاق. نعم، نجري أحيانًا محادثات حول وجهة نظرنا وكيف يراها بعضنا البعض، لكننا نادرًا ما نختلف في مجالات المخاطر التي نحتاج إلى توفير ضمان بشأنها."

يضيف سرينيفاسان أن التركيز على النهج القائم على البيانات للأمن السيبراني يفترض أنه سيكون هناك اتفاق على الحقائق بين أمن المعلومات والتدقيق الداخلي.

وقال: "إذا كان هناك أي خلاف، فنحن بحاجة إلى العمل والوصول إلى نفس مجموعة الحقائق". "ثم يمكنأن يكون لديك مستوى معين من النظرة الشخصيةللامور بحيث تقول بشكل فردي ،" حسنًا، أشعر أن هذا هو مهم بدرجة كبيرة أومتوسطة أو منخفضة ". أعتقد أن هذا يؤدي إلى مناقشة ونتائج صحية، بدلاً من توجيه الرؤوس دون وجود إطار مرجعي مشترك."

تعزيز مرونة الأمن السيبراني

قال سرينيفاسان إن نهجه منذ البداية كان الالتزام بمهمة *Chewy*. وهذا يعني تحقيق ثلاثة أشياء: ممارسة مبادئ التشغيل الداخلية للشركة، وضمان التوافق بين أمن المعلومات والتدقيق الداخلي، وبناء الثقة من خلال الشفافية.

وقال: "أعتقد أننا قطعنا شوطًا طويلاً، وهذا حقًا يؤتي ثماره كثيرًا فيما يتعلق بما يتطلبه الأمر من أعضاء الفريق والقيادة لإبقاء بعضنا البعض على اطلاع."

كما ذكرنا سابقًا، تدعم الدرجة العالية من التواصل والتعاون نهجًا رشيقًا يدمج التدقيق الداخلي في عملية الأمن السيبراني باستمرار. يلاحظ سرينيفاسان أن القوى الرئيسية، مثل التركيز المتزايد على الاستدامة، واعتبارات سلسلة التوريد، وظروف السوق، والتطورات الجيوسياسية، وغيرها تتطلب مناهج مرنة للأمن السيبراني والضمانات ذات الصلة.

قال: "أعتقد أن هذا يجبرنا على أن نكون يقظين و أذكياء وسريعي الاستجابة ووثيقي الصلة بالمواضيع". "إذا اتبعنا النهج الكلاسيكي مع فترات زمنية أطول، فسوف نتأخر عن اللحاق بالقطار. لذلك، أنا سعيد بمستوى المشاركة التي لدينا."

توسيع المعرفة

ومن الفوائد الجوهرية الأخرى للشراكة كيف تطور كلا الفريقين ونما فهمهما وتقديرهما لنهج بعضهما البعض لتحقيق نفس الهدف - الحفاظ على أمان الإنترنت للمؤسسة.

"نحن دائمًا نتحقق من المعرفة الفنية لبعضنا البعض من حيث ،" هل نظرنا إلى هذا؟ هل تفكر في ذلك؟ قال ماران: "ها هي وجهة نظري في تحليل المخاطر هذا - هل يتوافق مع وجهة نظرك أيضًا؟". "لذا، من البداية، نفكر بالفعل في المكان الذي سنبحث فيه، وسريني يشارك في اجتماعات البداية. إنه في المحادثة قبل أن نبدأ في التدقيق. لا توجد مفاجآت حقًا."

لكن القيمة المضافة الحقيقية تأتي من التعاون بمجرد تنفيذ ارتباطات التدقيق ويتعامل التدقيق الداخلي مباشرة مع موظفي تكنولوجيا المعلومات والأمن.

قال ماران: "من منظور التطوير الوظيفي، خاصةً مع عقلية تكنولوجيا المعلومات والأمن السيبراني، فإن الأمر مجزٍ حقًا لأنك ترى أكثر بكثير من مجرد تعبئة المربعات والقول ،" هل فعلت هذا؟ " "هناك الكثير. هناك تفسير. هناك خبرة فنية يجب القيام بها بشكل صحيح، لذلك أعتقد أن هذا هو المكان الذي يتعلم فيه فريقي الكثير."

الاستنتاج

توفر العلاقة السليمة بين التدقيق الداخلي وأمن المعلومات فوائد متعددة للمؤسسة، في المقام الأول في مواءمة وفهم ملف تعريف المخاطر السيبرانية للمؤسسة - من نقاط الضعف والفرص إلى اختبار النضج والاختراق.

علاوة على ذلك، يمكن للعلاقة السليمة أن تعزز المرونة وخفة الحركة إذا احتاجت المنظمة إلى الاستجابة للحوادث السيبرانية، أو التغييرات في العوامل التي تؤثر على الأمن السيبراني، أو المشهد التنظيمي المتطور. يساعد في توفير رسائل متسقة وموحدة إلى *C-suite* والمجلس حول مخاطر الأمن السيبراني، والاحتياجات، والأولويات، والصحة. يمكن حماية استقلالية التدقيق الداخلي بنجاح، بل وتعزيزها، عندما يطور كلا الجانبين فهمًا أعمق وتقديرًا للأدوار والأساليب والواجبات. في نهاية المطاف، يمكن لعلاقة قوية بين رؤساء التدقيق ومدراء أمن المعلومات أن تعزز أمن تكنولوجيا المعلومات من خلال دعم نهج على مستوى المؤسسة للأمن السيبراني.

"تتحول العقلية من مجرد التدقيق -" أحتاج إلى الحضور والتقييم وتقديم ملاحظات ذات مغزى "- إلى القول حقًا ،" هذه هي شركتي ؛ هذا ما أهتم به حقًا ؛ وهذه هي الطريقة التي سأساعد بها هذا الفريق ليكون ناجحًا "، قال ماران.

الاستجابة للحوادث السيبرانية والتعافي منها

عن الخبراء

Brian Tremblay

يقود *Brian Tremblay* ممارسة الامتثال في *Onapsis*، حيث كونه مسؤولاً عن مساعدة العملاء على فهم التحديات والفرص التي تنشأ عن التداخل المتزايد في الامتثال، الأمن السيبراني، واستمرارية الأعمال المتعلقة بالضوابط العامة لتكنولوجيا المعلومات والمسائل التنظيمية والامتثال مثل *Sarbanes- Oxley (SOX)* واللائحة العامة لحماية البيانات (*GDPR*). قبل انضمامه إلى *Onapsis*، شغل منصب رئيس التدقيق الداخلي لشركة *Acacia Communications* ذات التكنولوجيا العالية لأشباه الموصلات. بالإضافة إلى تأسيس وقيادة جميع أنشطة التدقيق الداخلي، فقد ساعد في إعداد الشركة للاكتتاب العام (بما في ذلك تطبيق *SOX*) وسهل تنفيذها لإدارة مخاطر المؤسسة (*ERM*). شغل *Tremblay* سابقًا منصب مدير التدقيق الداخلي في *Iron Mountain*، حيث أشرف على جميع عمليات التدقيق والمشاريع في أمريكا الشمالية بالإضافة إلى التنسيق مع مديري الجودة العالميين. قبل ذلك، بصفته مديرًا أول في *Houghton Mifflin Harcourt*، أنشأ قسمًا للتدقيق الداخلي ونفذ *SOX*. في وقت سابق من حياته المهنية، عمل في *Raytheon* و*Deloitte*.

DaMon Ross Sr.

في عام 2020، بدأ *Cyber Defense International DaMon Ross Sr.*، حيث يستفيد هو وفريقه من عمليات الأمن السيبراني وقدرات استخبارات التهديدات السيبرانية لتقديم حلول وخدمات الأمن السيبراني بأسعار معقولة للمنظمات التي تفتقر إلى الوسائل اللازمة لبناء القدرات بأنفسهم. قبل بدء *Cyber Defense International*، شغل *Ross* منصب نائب الرئيس الأول لعمليات الأمن السيبراني في *SunTrust Bank*. في هذا المنصب، تم تكليفه بإنشاء مركز عمليات الأمن السيبراني التابع لـ *SunTrust* على مدار الساعة *24/7/365*. عليه، أنشأ روس فرقًا متخصصة في الاستخبارات السيبرانية ، مراقبة التهديدات السيبرانية ، الاستجابة للحوادث السيبرانية ، والجرائم السيبرانية . والجدير بالذكر أنه نجح أيضًا في الشراكة مع الموارد البشرية، الشؤون القانونية، أمن الشركة، وشؤون أخلاقيات المؤسسة وشركاء المخاطر لإنشاء أول برنامج مراقبة التهديدات الداخلية للبنك. قام روس أيضًا بتيسير إنشاء العديد من شراكات تبادل المعلومات، بما في ذلك تلك الشراكات مع فرقة العمل المعنية بالجرائم السيبرانية التابعة للخدمة السرية للولايات المتحدة ووزارة الأمن الداخلي.

الرجوع إلى الأساسيات

لطالما كان الأمن السيبراني نقطة محورية بارزة للمنظمات وأقسام التدقيق الداخلي الخاصة بها، ومع تقديم مقترحات لجنة الأوراق المالية والبورصات الجديدة (*SEC*) بشأن إدارة مخاطر الأمن السيبراني، الاستراتيجية، الحوكمة، والكشف عن الحوادث، لم يكن عام 2022 استثناءً. هناك ما يبرر الزخم لهذه المقترحات التنظيمية وغيرها. وفقًا لتقرير صادر عن مركز موارد سرقة الهوية، تم تسجيل 1,862 انتهاكًا بارزًا للبيانات في عام 2021، وهو رقم تجاوز إجمالي عام 2020 بنسبة 68٪، كما الرقم القياسي المسجل في عام 2017. لم تنجو أي صناعة من الاتجاه[19] .

في هذه البيئة، ترغب المؤسسات، بل تتطلب، ضوابط وعمليات واضحة وقوية للأمن السيبراني مبنية على الأساسيات الجوهرية، بما في ذلك التعلم المستمر حول المخاطر واللوائح ذات الصلة، بالإضافة إلى الاتصال والمواءمة بين مجلس الإدارة، الإدارة، والتدقيق الداخلي. يركز الجزء الأول من سلسلة المعهد الدولي للتدقيق الداخلي المكونة من ثلاثة أجزاء، الأمن السيبراني في عام 2022، على التأثيرات التنظيمية المحتملة، بينما يبحث الجزء الثاني في فوائد العلاقة التكافلية بين كبار مسؤولي أمن المعلومات (*CISOs*) ونظرائهم في التدقيق الداخلي. يؤكد هذا الجزء الأخير على تطوير وتنفيذ استراتيجية الاستجابة للحوادث السيبرانية للمؤسسة، وبشكل أكثر تحديدًا، حيث يمكن للتدقيق الداخلي أن يوفر قيمة تنظيمية في تقييم الضوابط الحاسمة للتعافي بسرعة من خرق الأمن السيبراني.

[19] .مركز موارد سرقة الهوية، "تقرير خرق البيانات السنوي لعام 2021 الصادر عن مركز موارد سرقة الهوية يضع رقمًا قياسيًا جديدًا لعدد التسويات"، 24 يناير 2022
https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/.

الضوابط الرئيسية

إعطاء التدقيق الداخلي دورًا يلعبه في الاستجابة السيبرانية

مغالطة الاستجابة للحوادث

على الرغم من أن مصطلحي "الاستجابة للحوادث السيبرانية" و"الاستجابة والتعافي من الأمن السيبراني" هما تعريفان دقيقان ومفيدان، إلا أنهما يشيران أيضًا إلى وجهة نظر غير كاملة إلى حد ما لما تتطلبه هذه الخطط لتكون فعالة.

يوفر التدقيق الداخلي في أهم أدواره للمؤسسات ضمانًا مستقلًا بشأن إدارة المخاطر. وهذا لا يشمل فقط ضمان الاستجابة المناسبة للحوادث السيبرانية، ولكن أيضًا التقييم المناسب للضوابط لضمان التخفيف من المخاطر وآثارها أو، بشكل مثالي، منعها. لتحقيق مثل هذا المعيار النبيل على أي خطر معين، لا ينبغي أن يقتصر الاهتمام فقط على مجرد الاستجابة للمخاطر. بدلاً من ذلك، من الأكثر فاعلية النظر إلى الاستجابة للحوادث السيبرانية بطريقة شاملة ودورية تعطي الأولوية للضوابط الوقائية بالإضافة إلى تدابير الاستجابة النشطة.

قال *Brian Tremblay*، رئيس ممارسات الامتثال في شركة *Onapsis، Inc*: "إدارة المخاطر تشبه العجلة إلى حد ما". "في بداية العجلة، لدينا الضوابط الصحيحة، والعمليات هي ما نعتقد أنه يجب أن تكون عليه. وبعد ذلك، عندما يحدث شيء ما، تصبح المحادثة على الفور، 'هل كانت الضوابط تعمل كما هو متوقع، وهل حدث ما نعتقد أنه سيحدث؟' ثم، من هناك، نتعلم ما الذي يجب تغييره، وتبدأ الدورة مرة أخرى. إذا كانت المرة الوحيدة التي تستجيب فيها لحدث ما هو بعد الواقعة، فمن المحتمل أنك غير فعال فيما يتعلق بوقتك ومواردك. يجب منح الحاضر والمستقبل وزنًا متساويًا لأننا لا نبني أعمال اليوم فحسب، بل نبني أعمال المستقبل. نظرًا لأن المؤسسات غالبًا ما تعاني من هذا الأمر، يعد هذا مكانًا مهمًا حقًا للتدقيق الداخلي للتركيز عليه".

أساسيات ثابتة

نادرًا ما تصبح المخاطر أقل تعقيدًا، ولأن الأمن السيبراني بطبيعته ذو تقنية عالية، فإن منحنى التعلم لفهم كل من المخاطر نفسها والأنظمة اللازمة للتخفيف من حدته قد ازداد حدة مع كل تقدم تكنولوجي لاحق. ومع ذلك، لا يعني هذا بالضرورة أن الهيكلية الأساسي لخطة الاستجابة للحوادث السيبرانية والضوابط التي تتضمنها تتغير بشكل كبير.

تم توضيح هذه الضوابط في أحدث التوجيهات التكميلية من المعهد الدولي المدققين الداخليين، تدقيق الاستجابة للحوادث السيبرانية والتعافي منها، ويمكن تجميعها في أربعة أهداف عمل عالية المستوى:

- **تخطيط الاستجابة للحوادث**. يجب وضع السياسات والإجراءات لتوجيه تحديد ما إذا كان الحادث قد وقع وما العمل حيال ذلك. يجب أن يشمل التخطيط أصحاب المصلحة الرئيسيين، وتحديد الأدوار والمسؤوليات، واختبارها حسب الاقتضاء لتعزيز الوعي والتنفيذ.
- **تحديد الحوادث**. تؤدي عمليات تحليل البيانات من الضوابط الاستقصائية إلى تحديد وجود حادث سيبراني، والتي عادةً ما تكون الدافع لتنفيذ واحدة أو أكثر من خطط الاستجابة.
- **مجالات التواصل**. هناك العديد من أصحاب المصلحة المحتملين في الحوادث السيبرانية، لذلك يجب أن تتضمن كل خطة استجابة استراتيجية تواصل للإخطار المناسب وفي الوقت المناسب بالتأثيرات وجهود الحل.
- **الاستجابة الفنية والتعافي**. تحدد طبيعة الحادثة إلى حد كبير الضوابط اللازمة للإصلاح الفني والتعافي، وغالبًا ما تتضمن تنسيق الجهود داخليًا وخارجيًا[20].

[20] المعهد الدولي للتديق الداخلي، تدقيق الاستجابة للحوادث السيبرانية والتعافي منها، توجيهات تكميلية، دليل الممارسة، https://www.theiia.org/globalassets/documents/content/articles/guidance/gtag/2022/gtag_auditing_cyber_incident_response_and_recovery_final.pdf.

يتطلب تحقيق أهداف العمل هذه والالتزام بإطار عمل راسخ للاستجابة للحوادث السيبرانية مثل إطار عمل المعهد الوطني للمعايير والتكنولوجيا (NIST) لتحسين الأمن السيبراني للبنية التحتية الحرجة معرفة تقنية تتعلق بالتنفيذ، الصيانة، والتحسين التي يمكن لفرق أمن المعلومات وتكنولوجيا المعلومات توفيرها – المعرفة التي قد تمتلكها أو لا تمتلكها أقسام التدقيق الداخلي. ومع ذلك، هناك مساحة واسعة في نفس الوقت للآخرين الذين لديهم تخصصات أقل تقنية ولكن ذات قيمة متساوية لتقديم قيمة كبيرة. التدقيق الداخلي، مع إمكانية وصوله الفريد للمعلومات وفهمه للوظائف التنظيمية عبر جميع الإدارات، بالإضافة إلى منظوره المستقل الحاسم لتوفير ضمان موضوعي، هو مثال على هذا التخصص.

قال DaMon Ross Sr، مؤسس Cyber Defense International LLC، ونائب رئيس أول سابق، ورئيس عمليات الأمن السيبراني في SunTrust "من منظور التدقيق الداخلي، لا يختلف نهج الاستجابة للحوادث السيبرانية عن أي مخاطر أخرى من حيث التركيز على العملية الفعلية ونتائج تلك العملية". كما قال "حتى مع الطبيعة التقنية للمواد، فإن أي مدقق داخلي معتاد على العمل بشكل عملي سوف يلتقط الأمور المهمة بسرعة كبيرة."

تحمل مثل هذه العملية أكثر من تشابه عابر لما قد يراه التدقيق الداخلي في برامج الامتثال الخاصة بـ Sarbanes-Oxley (SOX)، أو خطط الاستجابة للأزمات، أو أي استراتيجية قائمة لإدارة المخاطر. وقال Ross "المؤسسات المختلفة لها مصطلحات مختلفة، ولكن خطة الحوادث السيبرانية هي في الأساس سياسة حاكمة تحدد وقت وقوع حادث سيبراني، وما هي أدوار ومسؤوليات جميع الأطراف المعنية، ومن يجب أن يكون على طاولة اتخاذ القرار".

أعرب Tremblay عن نفس المشاعر. وقال إن الضوابط ذات الصلة بالمخاطر السيبرانية هي أيضًا جزء من الأطر المستخدمة لإدارة مخاطر الامتثال المرتبطة بـ Sarbanes-Oxley.

على سبيل المثال، تتمثل إحدى الخطوات الأولى التي يتخذها المتسللون عند خرق أي تقنية في الوصول إلى الحقوق والامتيازات اللازمة لتحقيق هدفهم. في المخطط الكبير للمخاطر، يقع هذا تحت خطر الوصول غير المصرح به. قال Tremblay إنه لا يوجد فرق بين ما إذا كان ذلك ينطبق على SOX أو المخاطر السيبرانية. "المخاطر عند اختزالها في أبسط أشكالها، والضوابط للتخفيف من تلك المخاطر، متطابقة بشكل أساسي."

ضوابط التوثيق

كما ذكر Tremblay، إن الضوابط المضمنة في مثل هذه السياسة لها أيضًا تداخل كبير مع ما يمكن رؤيته مع المخاطر التنظيمية الأخرى. أحد الأمثلة هو وجود عملية توثيق فعالة. يوافق Ross. وقال إنه يجب على المؤسسات أن تفهم كيف يبدو سير العمل الذي يوثق الحوادث السيبرانية بشكل صحيح، وكيف تتحد جميع الأجزاء المتحركة التي تعمل بالتوازي.

"هذا ليس فقط للحوادث الكبيرة. يجب أن يكون لكل مؤسسة وظيفة تتعامل مع هذا بشكل يومي. لنفترض أن جهاز كمبيوتر تعرض لبرامج ضارة عليه. يمكن أن تتحول مثل هذه الحوادث الصغيرة إلى حوادث أكبر، وفي حالة حدوث الأسوأ، يساعد التوثيق المناسب في فهم كيفية تصعيدها. هذه الوظيفة هي من الضوابط في حد ذاتها".

ضوابط الكشف والبنية التحتية المادية

عنصر تحكم مهم آخر، والذي يقع تحت عنوان مخاطر الوصول غير المصرح به، هو البنية التحتية المادية. على الرغم من أن مثل هذه الضوابط قد لا تتبادر إلى الذهن على الفور عند مناقشة الأمن السيبراني، إلا أن الوصول غير المصرح به إلى محركات الأقراص الثابتة أو الخوادم حيث يتم تخزين المعلومات الحساسة كان مسؤولاً عن 10٪ من جميع الخروقات في عام 2020، مما كلف المؤسسات في المتوسط 4.36 مليون دولار لكل خرق، وفقًا للبحث من معهد *Ponemon* الذي نشرته شركة *IBM Security*.

يمكن أن تشمل هذه البنية التحتية غرف خادم آمنة ذات وصول مقيد، بالإضافة إلى المزيد من الإجراءات الأمنية الأساسية، مثل الأبواب المغلقة في جميع أنحاء المنشآت. في حين أن أمن البنية التحتية مهم، فإن وجود ضوابط للكشف عن الأنشطة المشبوهة وتوثيقها يمكن أن يكون أكثر أهمية.

قال *Tremblay* "عندما أتحدث عن البنية التحتية المادية، فأنا لا أتحدث عن الأبواب المغلقة بقدر ما أتحدث عن وجود إخطار وتوثيق للإجراء الذي يؤدي إلى حدوث مخاطر حقيقية. إنه مثل الطبق الرئيسي للوجبة مقارنة مع المقبلات."

وقال *Ross* إن تحديد مثل هذه الأنظمة وتقديم ضمانات لها يندرج بشكل مباشر ضمن مجموعة المهارات المحددة للتدقيق الداخلي، مضيفًا أن "التدقيق الداخلي لديه القدرة على تحديد الأنظمة الأكثر خطورة أو الأكثر أهمية لحياة المؤسسة. من المحتمل، في الواقع، أن التدقيق الداخلي قد أتم تحديد هذه الأنظمة بالفعل كجزء من توفير ضمان للامتثال للقوانين واللوائح الفيدرالية المتعلقة بالمخاطر الأخرى. كل ما هو مطلوب هو توسيع هذا التفكير ليشمل أنواع جديدة من التزويد التي يمكن أن توفر وصولاً أعلى."

مواءمة توقعات التعافي

يعد التوثيق الفعال في جميع مراحل خطة الاستجابة للحوادث السيبرانية أمرًا بالغ الأهمية. ومع ذلك، من المهم بنفس القدر نقل البيانات التي يوفرها مثل هذا التوثيق ومواءمة توقعات الكشف والتعافي للمؤسسة.

وفقًا لـ *Tremblay*، يعد هذا أحد أكبر الثغرات التي شاهدها في خطط الاستجابة السيبرانية للمؤسسات – وحيث يمكن للتدقيق الداخلي تقديم أكبر قيمة. وقال: "دور التدقيق الداخلي في التعافي من الكوارث السيبرانية ذو شقين. أولاً، التأكد من وجود الحادث، ويمكنك إثبات وجوده من خلال التوثيق أو أي تقنية أو عملية تستخدمها. الشيء الثاني، والشيء الذي لا أرى أنه يتم القيام به بشكل كافٍ، هو الجلوس مع جميع أصحاب المصلحة الرئيسيين [لتحديد] الجدول الزمني الواقعي للتعافي الذي سيعتمد على قابلية المؤسسة للمخاطر."

قال *Tremblay* إن الجدول الزمني سيحدده 'مالك' التطبيق المعني في المؤسسة، والذي يمكن أن يكون *CISO* أو رئيس سلسلة التوريد أو أي قائد آخر، اعتمادًا على مكان وقوع الحادث. من الأساسي أن يكون التدقيق الداخلي كحلقة وصل بين هذا الطرف وجميع الأطراف الأخرى المعتمدة على هذا التطبيق في المهام اليومية.

"على سبيل المثال، قد يقول *CISO* أن وقت التعافي المحدد بمدة 48 ساعة أمر مقبول، ولكن إذا لم تذهب إلى المدير المالي أو غيره من القادة أو الوظائف التي تعتمد على هذه التقنية قيد التشغيل والحصول على مدخلاتهم، فأنت بذلك تحضر نفسك لفوضى محتملة" قال *Tremblay*. "على سبيل المثال، قد يقول المدير المالي أن 48 ساعة جيدة، ولكن فقط إذا لم نكن نحضر البيانات المالية. ولكن إذا كنا نحضر البيانات المالية، فلن يُقبل أي توقف لأن المؤسسة ستضطر إلى تقديم تمديد، والذي سيبدو سيئًا حقًا في الأسواق العامة".

مثل هذه المحادثات لا تتطلب بالضرورة أن يتغلب أحد الطرفين على الآخر. بدلاً من ذلك، من خلال هذا التواصل، يمكن للتدقيق الداخلي أن يتوسط للإجماع بما يتماشى مع قابلية المؤسسة في المخاطرة. قال *Tremblay*: "في الحالات التي يوجد فيها تناقض، ما يمكن أن يطرحه [التدقيق] الداخلي هو، 'هل من الضروري حقًا حدوث ذلك؟' قد يقول الرئيس التنفيذي، 'نعم، إنه كذلك، لأنه سيكلف مليون دولار لحل هذه المشكلة'. ما نقوم به حقًا هو التأكد من أن الخطة قد تم تطويرها حقًا حول أصحاب المصلحة حول التكنولوجيا."

يتابع: "أعتقد أن هذا مجال لم نكن، كمهنة، جيدين فيه بشكل خاص. أعتقد أننا نحاول التأكد من القيام بالتحقق من صحة بعض الأشياء دون أن نقول حقًا، 'مرحبًا، كجزء من مراجعة الضوابط حول الاستجابة للحوادث، حددنا فجوة في المتطلبات بين أصحاب المصلحة لتقنيات معينة.' هذا صحيح للغاية. هذا هو تحديد مخاطر العمل غير المحددة سابقًا والتي يعتبر ذو قيمة للمؤسسة".

الوظائف المتداخلة

من المفاهيم الخاطئة الشائعة أن الملكية الأساسية لاستجابة الأمن السيبراني تقع على عاتق *CISO* وفريق الأمان. هذا صحيح جزئيا فقط. على الرغم من أن التجربة والخبرة اللازمتين لتنفيذ الجوانب الفنية للاستراتيجية السيبرانية ستوجد على الأرجح في هذا القسم، فمن الخطير الافتراض أن القسم سيكون لديه القدرة – أو الرغبة – لتحمل العبء بمفرده.

"يجب أن تكون الاستجابة للحوادث السيبرانية، على الأقل، عملية متعددة الوظائف" كما قال *Ross*. "السبب الأكبر للتأخر في أوقات استجابة المؤسسات التي أراها ليس قسم أمن المعلومات نفسه من حيث المعرفة، بل هو إنشاء الأدوار والمسؤوليات عبر الوظائف مع الإدارات التي لا يمثل الأمان مسؤوليتها الأساسية. لديهم أشياء أخرى ليفعلوها".

وفقًا لـ*Ross*، يجب أن يكون تصحيح هذا المفهوم الخاطئ وتعزيز فكرة المسؤولية المشتركة بين جميع أصحاب المصلحة مجالًا رئيسيًا لتركيز التدقيق الداخلي. "لا يلزم بالضرورة أن يكون التركيز على فريق الأمان وما يفعلونه، ولكن بدلاً من ذلك على كيفية دعم عملياتهم من قبل الأقسام الأخرى في المؤسسة التي لها مصلحة فيها. يعرف فريق الأمان ما يجب فعله، لكن لا يمكنهم إجبار فرق تقنية المعلومات والمطورين على المساعدة بطرق حرجة. هناك الكثير من السياسات المؤسساتية المتضمنة، وعندما كنت في هذا المنصب، وجدت شريكًا مهمًا في التدقيق الداخلي. لا تستطيع فرق الأمان خوض تلك المعارك بمفردها. إذا كان بإمكانك الحصول على طرف محايد إلى حد ما للمساعدة في تحديد المواضع التي توجد بها ثغرات في المؤسسة في العملية، فهذا يساعد الجميع".

قال *Ross* إن الاستراتيجية المفيدة لتسليط الضوء على هذه الثغرات وتوضيح الأدوار هي التدقيق الداخلي، عادة بالتعاون مع مستشار خارجي، لتسهيل عمليات المحاكاة على المستوى الإداري. "بمجرد أن تكون لديك خطة الاستجابة للحوادث السيبرانية في مكان يمكن اختباره فيه، تجمع المحاكاة على المستوى الإداري مدير المعلومات، مدير أمن المعلومات، قادة تكنولوجيا المعلومات، المدير التنفيذي، والتدقيق الداخلي – جميع أصحاب المصلحة المعنيين – معًا في

غرفة اجتماعات أو مكالمة *Zoom* لمتابعة سيناريو معقول. حتى بدون الخبرة الفنية، يمكن للتدقيق الداخلي تسهيل المناقشة عن طريق سؤال من يفعل ماذا وتقييم كيف تتوافق هذه المسؤوليات مع الواقع. يمكنهم أن يقولوا، 'في هذه المرحلة، يجب أن ينفذ فريقك *X* و*Y* وفقًا لخطتنا، ولكن في الواقع، يمكنك فعل *Z*'. هذا عندما تسمع الحقائق كما هي (*translating "the real dirt"*). يتعين على معظم المؤسسات القيام بها مرة واحدة على الأقل في السنة، ولكن يجب أن يتولى التدقيق الداخلي حقًا هذه المسؤولية".

الاستنتاج

التطور مع بيئة المخاطر

يستحق التدقيق الداخلي، من خلال مكانته الفريدة في المؤسسة، مقعدًا على الطاولة عندما يتعلق الأمر بخطط الاستجابة للحوادث السيبرانية للمؤسسة. لكن هذا النجاح لا يعفي التدقيق الداخلي من السعي وراء استكشاف وفهم أعمق للأمن السيبراني. في الواقع، في المستقبل الذي يتم فيه الاستغناء بسرعة عن البنية التحتية المادية لصالح التكنولوجيا القائمة على السحابة، ستصبح خبرة أكبر من التدقيق الداخلي ضرورية ومتوقعة حتمًا.

"عندما بدأت مسيرتي المهنية في التدقيق الداخلي، كانت إحدى أهم نقاط المثيرة للإهتمام أنه كان دورًا عامًا للغاية". كما قال *Tremblay*. "عليك أن ترى وتتعلم الكثير من الأشياء حول الكثير من الموضوعات التي لا تحتاج إلى أن تكون خبيرًا فيها. ولكن كان هناك مثل هذا التحول الهائل حول التكنولوجيا، لقد بدأت أتساءل عما إذا كانت أيام المدقق الداخلي العام باتت معدودة. بدلاً من ذلك، ربما يصبح التدقيق الداخلي يومًا ما من ذوي الخبرة (*SME-subject matter expert*) حول أشياء مهمة بطبيعتها للمؤسسات. لذلك، بدلاً من وجود فرق تدقيق تتألف من 8-10 مدققين للعمليات والامتثال والبيانات المالية، سيكون لدى المؤسسات مدقق للأمن السيبراني، ومراجع *ESG* واحد، وما إلى ذلك"

يوافق *Ross*. "في مرحلة معينة مع التكنولوجيا الناشئة، كيف تفهم حقًا الفجوات في عملية الاستجابة على مستوى عميق إذا لم تتمكن من التعمق في ذلك؟ لن تتمكن من ذلك حقًا"

هناك الكثير الذي يمكن تحقيقه بالمعرفة والموارد المتاحة، لكن مستقبل مثير وجذري جديد قادم. يجب أن يكون التدقيق الداخلي جزءًا منه.

الاعداد السابقة

للوصول إلى الإصدارات السابقة من Global Perspectives and Insights ، تفضل بزيارة www.theiia.org/GPI.

ملاحظات القارئ

لارسال ألاسئلة أو التعليقات إلى **globalperspectives@theiia.org**

عن المعهد الدولي للمدققين الداخليين

تأسس المعهد الدولي للمدققين الداخليين سنة 1941 وهو جمعية مهنية دولية و مقرها في بحيرة ماري، فلوريدا، الولايات المتحدة الأمريكية. وتخدم أكثر من 210,000 عضو منتسب من أكثر من 170 دولة وإقليم. يعتبر المعهد الدولي للمدققين الداخليين صوت مهنة التدقيق الداخلي، والمرجعية المعترف بها عالميا، والمصدرالرئيسي للمعايير والارشاد والشهادات المتعلقة بمهنة التدقيق الداخلي.

بالإضافة إلى برامج إصدار الشهادات العالمية، يتمتع أعضاء المعهد الدولي بمزايا مثل الوصول إلى الشبكات المهنية المحلية والوطنية والعالمية؛ والتدريب على مستوى عالمي؛ والمعايير والتوجيه؛ والبحث ؛ والتطوير التنفيذي؛ والفرص الوظيفية؛ والموارد مثل خدمات الجودة في المعهد الدولي. لمزيد من المعلومات، قم بزيارة theiia.org

إفصاح

ينشر المعهد الدولي للمدققين الداخليين (IIA) هذه الوثيقة لأغراض إعلامية وتعليمية. لا تهدف هذه المواد إلى تقديم إجابات نهائية لظروف فردية محددة وعلى هذا النحو يُقصد منها فقط استخدامها كدليل. ويوصي المعهد الدولي للمدققين الداخليين بالتماس مشورة الخبراء المستقلين فيما يتعلق مباشرة بأي حالة محددة. لا يتحمل المعهد الدولي للمدققين الداخليين (IIA) أي مسؤولية تجاه أي شخص يعتمد وحده على هذه المواد.

حقوق النشر

أغسطس 2022

قام بترجمة هذه الوثيقة الى اللغة العربية فريق عمل من جمعية المدققين الداخليين في لبنان برئاسة عضو مجلس الحكام ناجي فياض
مؤلف من: محمد شهاب، محمود غلاييني و داليا بوكروم

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