ترنيمة الإدارة العليا
TONE at the TOP®

تقدم للإدارة العليا ومجلس الإدارة ولجان التدقيق معلومات موجزة عن مواضيع تتعلق بالحوكمة.

العدد 113 | أكتوبر 2022

التخفيف من التهديدات السيبرانية

أصبح الأمن السيبراني عنصرًا ثابتًا دائمًا في مشهد المخاطر الحديث وتواجه المجالس ضغوطًا متزايدة لتوفير الإشراف المناسب على تهديد متعدد الجوانب ودائم التطور. إذ وصف ما مجموعه 70% من أعضاء مجلس الإدارة الأمن السيبراني بأنه "خطر استراتيجي مؤسسي" في استطلاع لمجالس الإدارة أجرته الرابطة الوطنية لأعضاء مجالس إدارة الشركات (NACD).[1] وتندرج مجموعة كبيرة من المسائل تحت مظلة الأمن السيبراني، كلها أمور بالغة الأهمية، منها على سبيل المثال لا الحصر حماية الخصوصية وبرامج الفدية والبرامج المؤذية وحجب الخدمة أو هجمات التصيد الاحتيالي وسياسات الأمن السيبراني غير الملائمة والاستجابة للحوادث وخطط التعافي.

تواجه المنشآت أيضًا قوانين جديدة تتطلب منها الإبلاغ عن الاختراقات التي تعرضت لها. فعلى سبيل المثال، يتطلب "قانون الإبلاغ عن الحوادث السيبرانية للبنية التحتية الحيوية" (Cyber Incident Reporting for Critical Infrastructure Act)[2] الإبلاغ الذي من شأنه أن يتيح للوكالة الفيدرالية للأمن السيبراني وأمن البنية التحتية (Cybersecurity and Infrastructure Security Agency) تقديم المساعدة للضحايا خلال الهجمات الإلكترونية وتحديد التوجهات، وإطلاع ضحايا محتملين آخرين على المعلومات. واقترحت هيئة الأوراق المالية والبورصات (SEC) أيضًا لوائح[3] من شأنها توحيد الإفصاحات المتعلقة بإدارة مخاطر الأمن السيبراني واستراتيجيتها وحوكمتها والإبلاغ عن الحوادث في الشركات العامة.

بإمكان التدقيق الداخلي، الذي يقدم للمنشآت توكيدًا مستقلًا وموضوعيًا ومشورة، أن يكون موردًا قويًا لمجالس الإدارة في معالجة المخاطر السيبرانية. فوفقًا لما ورد في تقرير برايس ووترهاوس كوبرز (PwC)[4]: «تستفيد العديد من الشركات من التدقيق الداخلي لمراجعة العمليات السيبرانية والضوابط الرقابية، ومنها القدرة على الصمود والاستجابة».

خطوات لتحسين الأمن

بينما تأخذ مجالس الإدارة في الحسبان تهديدات الأمن السيبراني التي تواجهها، من شأن التدقيق الداخلي إحداث أثر ملموس في عدة مجالات.

الاعتراف بوجود المخاطر. احتلت التهديدات السيبرانية صدارة تصنيفات المخاطر في الشركات. فوفقًا لما ورد في تقرير المخاطر 2022 (OnRisk 2022)[5] الصادر عن معهد المدققين الداخليين (IIA): «يستمر التطور والتنوع المتزايد للهجمات السيبرانية في إحداث أضرار واسعة في العلامات التجارية للمنشآت وسمعتها، مما يؤدي غالبًا إلى آثار مالية كارثية». وحدد التقرير، الذي يستند إلى مقابلات مع أعضاء مجالس الإدارة وكبار المسؤولين التنفيذيين ورؤساء تنفيذيين للتدقيق، الأمن السيبراني باعتباره الخطر الأكبر هذا العام.

للأسف، قد لا يدرك بعض قادة الشركات هذا التهديد تمامًا. ففي تقرير المخاطر (OnRisk)، أحد الأمور المثيرة القلق الواردة فيه على وجه التحديد هو الفارق بين أهمية مخاطر الأمن السيبراني التي صنفها كل من الرؤساء التنفيذيون وأعضاء مجلس الإدارة والإدارة التنفيذية. فعلى الرغم من أن 97% من الرؤساء التنفيذيين للتدقيق قد صنفوا الأمن السيبراني على أنه خطر ذو أهمية كبيرة بمنشآتهم (صنفوه بدرجة 6 أو 7 من مقياس مكون من 7 نقاط)، لم يصنفها كذلك إلا 87% فقط من أعضاء مجالس الإدارة و77% فقط من كبار المسؤولين التنفيذيين.

يشير تصنيف الأهمية القوي وسط الرؤساء التنفيذيين للتدقيق إلى ارتفاع مستوى وعيهم بمسائل الأمن السيبراني. وهذا ليس مفاجئًا، نظرًا للإلمام الشامل بالمنشأة الذي يتمتع به التدقيق الداخلي. وبما أن مجالس الإدارة تسعى إلى الاستفادة من توكيد المخاطر وتحسينه بما يتجاوز المخاطر المالية ومخاطر الامتثال، يمكنها اللجوء إلى التدقيق الداخلي للمساعدة في توضيح مصادر القلق المتعلقة بالأمن السيبراني وتقدير تأثيرها المحتمل. ويمكن أن يشمل ذلك تسليط الضوء على الإخفاقات في تغطية المخاطر ومراقبة المخاطر الناشئة والاستفادة المثلى من الأدوات التكنولوجية في الجهود المبذولة في سبيل الأمن السيبراني.

الاستفادة من القيمة التي يوفرها نموذج الخطوط الثلاثة. يمكّن نموذج الخطوط الثلاثة[6] الصادر عن معهد المدققين الداخليين المنشآت من تحديد هياكل وعمليات تساعد على أفضل وجه في تحقيق الأهداف وتسهل وجود حوكمة وإدارة مخاطر قويتين، بما في ذلك ما يخص الأمن السيبراني. ويحدد نموذج الخطوط الثلاثة الأدوار الرئيسية التي يؤديها كل من:

نبذة عن معهد المدققين الداخليين (IIA)

معهد المدققين الداخليين (IIA) جمعية مهنية عالمية تضم أكثر من 210,000 عضو في أكثر من 170 بلدًا وإقليمًا. ويعَد معهد المدققين الداخليين الجهة الرائدة الداعمة والتعليمية التي تضع المعايير الدولية وتجري الأبحاث في كل ما يخص مهنة التدقيق الداخلي.

The IIA

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

الاشتراك المجاني

تفضل بزيارة www.theiia.org/tone للتسجيل في الاشتراك المجاني.

آراء القرّاء

أرسلوا أسئلتكم وتعليقاتكم إلى البريد الإلكتروني: Tone@theiia.org

- الهيئة الإدارية، وهي مسؤولة أمام أصحاب المصلحة عن الإشراف التنظيمي.
- الإدارة التي تعمل على تحقيق الأهداف التنظيمية.
- التدقيق الداخلي، الذي يقدم توكيدًا مستقلًا وموضوعيًا بشأن تحقيق تلك الأهداف.

أظهرت الأبحاث أن للتعاون بين الخطوط الثلاثة تأثيرًا إيجابيًا على فاعلية إدارة مخاطر الأمن السيبراني. فوفقًا لمقال نُشر في "مجلة جمعية تدقيق ومراقبة نظم المعلومات" (ISACA Journal)[7]، بإمكان التدقيق الداخلي أن يقدم توكيدًا قيّمًا ويحدد التهديدات ومواطن الضعف. وقد يشمل ذلك تحديد توجهات الأمن السيبراني وتوقعات أصحاب المصلحة، وإجراء تقييم أولي للمخاطر السيبرانية، وتحديد معايير التدقيق المجدي. وبحسب ماورد في المقالة: «يمكن أن يساعد المدققون [مجلس الإدارة] إلى حد كبير في ممارسة الإشراف» بالإبلاغ وتقديم المشورة بشأن النتائج التي توصلوا إليها.

الحرص على الاستفادة من إسهامات التدقيق الداخلي. في العديد من المنشآت، تكون لجان التدقيق مسؤولة عن معالجة جميع أنواع المخاطر، ومنها التهديدات السيبرانية.[8] إلا أن البعض يسند الشؤون السيبرانية إلى لجان أخرى لعدة أسباب. وبحسب حجم المنشأة ومجال نشاطها والتهديدات التي تواجهها، قد تكون اللجنة المكلفة بالإشراف على المسائل السيبرانية لجنة منفصلة للأمن السيبراني أو لجنة مخاطر أو لجنة شؤون تقنية أو لجنة ترشيحات وحوكمة أو لجنة أخرى. فمن جملة أسباب أخرى، قد تجد مجالس الإدارة أن لجنة التدقيق مشغولة بالفعل بما يكفي من الأعمال أو أنها قد لا تتمتع بالخبرة اللازمة للإشراف على المسائل السيبرانية.

عادةً ما يكون التدقيق الداخلي تابعًا للجنة التدقيق، ولكن قد تقوّت المنشأة توصيات وتوكيدات قيّمة متعلقة بالمخاطر السيبرانية إذا كان التدقيق الداخلي أيضًا لا يقدم تقارير إلى أي لجنة منفصلة مسؤولة عن الأمن السيبراني. إذ إن وجود هذه العلاقة مع أي لجنة تشرف على الشؤون السيبرانية يضمن فهم رؤى التدقيق الداخلي والعمل على أساسها في الواقع.

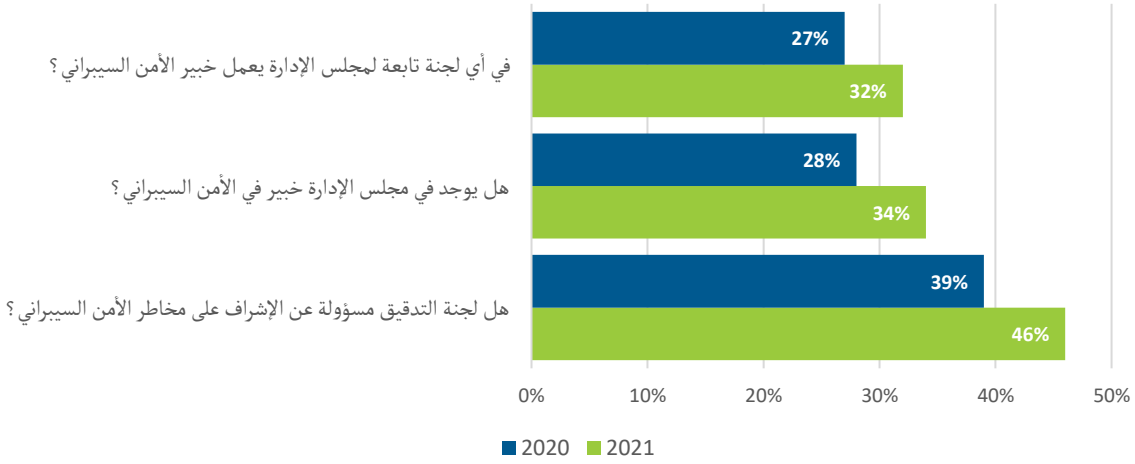
التعرف على التهديدات الخفية. قد تتفاجأ المجالس بعدد عمليات الإشراف التي تبدو صغيرة وبإمكانها أن تقوض جهود الأمن السيبراني وربما تؤدي إلى كارثة. وبإمكان التدقيق الداخلي تقديم رؤى متعمقة لمساعدة مجالس الإدارة على تحديد مدى قدرة خطة التدقيق بالمنشأة على تحديد التهديدات المهملة وتحديد المخاطر الناشئة. فوفقًا لما ورد في تقرير "ديلويت" (Deloitte)[9]، إن بضعة من التهديدات السيبرانية فقط التي عادةً ما تقلل الإدارة من شأنها ومنها:

- عدد الموظفين السابقين الذين لا يزال بإمكانهم تسجيل الدخول إلى النظام وعدد الموردين الخارجيين الذين يمكنهم الدخول إلى أنظمة الشركة. وفي كلتا الحالتين، ربما لا تكاد الشركات تعرف شيئًا عن عدد المستخدمين الخارجيين غير المعروفين وغير المصرح لهم الذين يمكنهم الدخول.

أسئلة لأعضاء مجلس الإدارة

- هل نستفيد الاستفادة القصوى من رؤية التدقيق الداخلي ومشورته في تخطيطنا الاستراتيجي فيما يتعلق بالأمن السيبراني؟
- هل دعمنا الجهود المبذولة في سبيل الأمن السيبراني بما يكفي من الموظفين والتمويل؟
- هل حددت المنشأة مستوى تحملها للمخاطر فيما يخص الأمن السيبراني من الناحية المالية؟
- هل أُسندت إلى لجنة خاصة مسؤولية الإشراف على الأمن السيبراني؟
- هل يُلم أعضاء مجلس الإدارة بالإجراءات التي تعتمدها الشركة في حال حدوث اختراق سيبراني ويعرفون ما هو دورهم عند حدوثه؟

ما عدد الشركات الواردة ضمن مؤشر ستاندارد آند بورز 500 (S&P 500) التي تفصح عن:



المصدر: 2021 Audit Committee Transparency Barometer, Center for Audit Quality, November 2021

- عدد الحسابات السحابية التي تستخدمها الشركة. إذ يمكن أن تخلّف كثرة الانخراط في الحسابات السحابية المزيد من الثغرات السانحة للهجمات السيبرانية. ويوصي تقرير "ديلويت" بأن تسأل المنشآت مقدمي الخدمات السحابية عن قدرة البنية التحتية على التحمل وعن تعطل الخدمة والأداء ومقاييس أخرى، بالإضافة إلى الامتثال التنظيمي وتقييمات الضوابط المستقلة.
- العدد الإجمالي الفعلي للاختراقات السيبرانية التي تعرضت لها المنشأة. فعلى عكس المتوقع، إذا تعرضت الشركة لعدد قليل من الهجمات السيبرانية، فربما يكون ذلك ببساطة علامة إنذار بأن ثمة حوادث لا يجري اكتشافها. وبإمكان فريق التدقيق الداخلي المساعدة في ضمان مراقبة هذه الأنواع من علامات الإنذار.

معالجة مصادر القلق في علاقات شركاء العمل. تتوقع شركة جارتنر (Gartner)[10] أنه بحلول عام 2025، ستأخذ 60% من المنشآت في الاعتبار مخاطر الأمن السيبراني عند الانخراط في معاملات وارتباطات عمل مع أطراف خارجية. واليوم، يرصد 23% فقط من قادة إدارة الأمن والمخاطر التعرض لمخاطر الأمن السيبراني المرتبطة بجهات خارجية في حينها، وقد يقتصر فحصهم على البائعين والموردين الفوريين بدلاً من سلسلة التوريد بأكملها.

وهنا أيضًا، ووفقًا لما ورد في تقرير المخاطر (OnRisk 2022)، لا تتوافق آراء قادة التدقيق وكبار المدراء التنفيذيين وأعضاء مجلس الإدارة. فعلى الرغم من أن الرؤساء التنفيذيين للتدقيق قيّموا القدرة التنظيمية في هذا المجال بنسبة 37%، يعتقد المدراء التنفيذيون أنها بلغت 53% وقيّمها أعضاء مجلس الإدارة بنسبة 57%. ومن المحتمل أن تدني الثقة لدى الرؤساء التنفيذين للتدقيق في هذا المجال ينبع إلى حد ما من إعطائهم هذا الخطر تقييم أهمية أعلى، إذ كان أعلى بـ 17 نقطة من تقييم أعضاء مجلس الإدارة (77% مقابل 60%).

وعلى أي حال، على مجالس الإدارة التأكد من أنها تستفيد الاستفادة القصوى من إسهامات وخبرات التدقيق الداخلي في هذا المجال. وبما أن التدقيق الداخلي يعمل مع فرق من جميع أقسام المنشأة، يمكنه تنبيه مجلس الإدارة إلى المخاطر السيبرانية المرتبطة أو المحددة لدى بائع معين أو في سلسلة التوريد بأكملها. وعندما يرغب شركاء العمل في المنشأة في الحصول على إعادة توكيد بشأن موثوقية الإجراءات الوقائية الخاصة بالأمن السيبراني، بإمكان التدقيق الداخلي تقديم أنواع البيانات والتأكيدات التي يريدون الحصول عليها.

تحسين الموارد

مع مواجهة المنشآت لمخاوف الأمن السيبراني المهولة، سيتعين عليها تحسين جميع مواردها الحالية. ويمكن أن تحسن مجالس الإدارة أمن شركاتها من خلال فهم والاستفادة من القيمة التي يمكن أن يقدمها المدققون الداخليون في جميع أقسام المنشأة من خلال تحديد الفرص السانحة لتعزيز الكفاءة والفاعلية.

سؤال الاستطلاع السريع

ما هي اللجنة التابعة لمجلس الإدارة المكلفة بالإشراف على إدارة مخاطر الأمن السيبراني بمنشأتك؟

- ○ لجنة التدقيق
- ○ لجنة الأمن السيبراني
- ○ لجنة الشؤون التقنية
- ○ لجنة الترشيحات والحوكمة
- ○ غير ذلك

تفضلوا بزيارة الصفحة www.theiia.org/tone للإجابة على السؤال والاطلاع على إجابات الآخرين.

الحواشي

[1] Principles for Board Governance of Cyber Risk, National Association of Corporate Directors, Internet Security Alliance, and World Economic Forum, In Collaboration with PwC, March 2021.

[2] https://www.cisa.gov/circia

[3] https://www.sec.gov/rules/proposed/2022/33-11038.pdf

[4] Overseeing Cyber Risk: The Board's Role, PwC, January 2022.

[5] OnRisk 2022: A Guide to Understanding, Aligning, and Optimizing Risk, The Institute of Internal Auditors, 2021.

[6] The IIA's Three Lines Model: An Update of the Three Lines of Defense, The Institute of Internal Auditors, July 2020.

[7] "How Effective Is Your Cybersecurity Audit?," Matej DraščEk, et al., ISACA Journal, June 1, 2022.

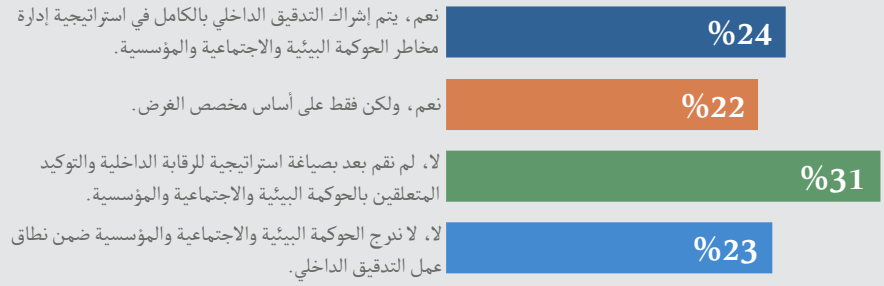
[8] "Cybersecurity: An Evolving Governance Challenge," Harvard Law School Forum on Corporate Governance, Phyllis Sumner, et al., March 15, 2020.

[9] Internal Audit: Risks and Opportunities for 2022, Deloitte, 2021.

[10] Predicts 2022: Cybersecurity Leaders Are Losing Control in a Distributed Ecosystem, Sam Olyaei, et al., Gartner, January 24, 2022.

نتائج الاستطلاع السريع

هل تستفيد منشأتك من التدقيق الداخلي للحصول على توكيد بشأن الحوكمة البيئية والاجتماعية والمؤسسية؟



المصدر: استطلاع "Tone at the Top" يونيو 2022.