ترنيمة الإدارة العليا
TONE at the TOP®

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

العدد 106 | أغسطس 2021

مواجهة وحش الأمن السيبراني

تؤثر المخاطر السيبرانية على المنشآت من جميع الأحجام وفي جميع الصناعات، ويبدو أنها وُجدت لتبقى ردحًا من الزمن. إذ صنفت إحدى الدراسات الاستقصائية، التي شملت مجالس إدارة ومدراء تنفيذيين على مستوى العالم، التهديدات السيبرانية على أنها من بين أكبر عشرة مخاطر في عام 2021، ويتوقع المستجيبون في الدراسة أن تشكل خطرًا رئيسيًا في عام 2030 أيضًا. ومن المتوقع أن ترتفع الجرائم السيبرانية على مستوى العالم بنسبة 15% سنويًا، مع توقع أن يصل تأثيرها السنوي إلى 10.5 تريليون دولار بحلول عام 2025، وفقًا لما أوردته شركة الأبحاث السيبرانية "Ventures Cybersecurity" إذ تصفها الشركة بأنها «أكبر تحول في الثروة الاقتصادية في التاريخ».

قد تكون حوادث الأمن السيبراني على شكل برامج فدية أو هجمات على موارد العمل عن بُعد أو هجمات سلاسل التوريد أو التصيد الاحتيالي أو أي مجموعة من الممارسات الإجرامية الأخرى. إذ يمكنها عرقلة الشركة، والقضاء على قيمة مؤسسية كبيرة بها، وإيقاعها تحت طائلة مساءلة قانونية أو ضجة إعلامية تضر بسمعتها. وتكاليف اختراق البيانات مرتفعة ومتزايدة، بمتوسط يبلغ 4.24 مليون دولار في عام 2021، بزيادة تصل إلى 10% تقريبًا في عام واحد، بناءً على بيانات شركة (IBM).

والأكثر من ذلك، أن جائحة فيروس كورونا لم تأتِ إلا بنقاط ضعف جديدة لم تُفهم تمام الفهم ولم تُعالج بعد.

إدارة الأخطار

إزاء هذا الوضع الحرج، تتخذ مجالس الإدارة عددًا من الخطوات لتعزيز إشرافها على المخاطر السيبرانية. وطوال هذه المسيرة يكون التدقيق الداخلي شريكًا رئيسيًا لها. ومن خلال العمل بالتعاون

مع خبراء الأمن السيبراني في المنشأة، بإمكان فريق التدقيق الداخلي تقديم تحقق موضوعي من أن خطط المنشأة يجري تنفيذها على النحو المنشود وأنها مناسبة للمهمة. إذ قالت ساندي بوندمان، مدققة داخلية معتمدة، وشريكة رئيسية متقاعدة في شركة ديلويت (Deloitte Risk and Financial Advisory): «يمكنه (فريق التدقيق الداخلي) إخبار مجلس الإدارة ما إن كان يوجد تعرض كبير للمخاطر أو شعور زائف بالأمان».

تتبع مجالس الإدارة العديد من الاستراتيجيات التي تساعد في معالجة المخاطر السيبرانية. وتوصي بوندمان وآخرون بأن تحرص مجالس الإدارة على استيعاب ملف المخاطر السيبرانية في منشآتها وأن تتبنى دورها الإشرافي وأن تمارس الشك المفيد لضمان أن يتشكل لديها فهم واضح لنقاط القوة والضعف والثغرات.

حدد الأدوار الإشرافية وحدد مواعيد الإحاطة المنتظمة بآخر المستجدات. مع أن أقل من 10% من المجالس اليوم لديها لجنة مخصصة للأمن السيبراني بقيادة عضو مجلس إدارة مؤهل، من المتوقع أن ترتفع هذه النسبة إلى 40% بحلول عام 2025، وفقًا لاستطلاع أجرته شركة جارتنر (Gartner). وهذا الارتفاع المتوقع قد يحفزه توسع الأعمال الرقمية أثناء الجائحة، وتبني العمل عن بُعد ومخاطره المحتملة الإضافية.

نبذة عن معهد المدققين الداخليين IIA

معهد المدققين الداخليين (IIA) جمعية مهنية عالمية تضم أكثر من 200,000 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 149
Lake Mary, FL 32746 USA

الاشتراك المجاني

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

آراء القرّاء

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

قالت بوندمان إنه قد يصعب تحديد المسؤولية عن الإشراف على الأمن السيبراني هذه الأيام لأنها غالبًا ما تكون متفرقة بين الإدارة ولجان متعددة. وأضافت أنه ينبغي تكليف لجنة واحدة بالمسؤولية ومناقشة الموضوع في كل اجتماع. هذا على أن يكون الأمن السيبراني أيضًا على جدول أعمال مجلس الإدارة بأكمله مرتين في السنة على الأقل.

تعرف على مستوى التهديد. الأمن السيبراني هو أكثر من مجرد مشكلة تتعلق بتكنولوجيا المعلومات. إذ قال جون نوبل، المدير الأسبق للمركز الوطني للأمن السيبراني في المملكة المتحدة، في نشرة صوتية لشركة الاستشارات الإدارية مكنزي (McKinsey): «سواء كان قبل أو أثناء حادثة ما، ينبغي ألا تُترك المهمة (الأمن السيبراني) على عاتق المدير التنفيذي لتقنية المعلومات والفريق التقني». وأضاف: «على القادة أن يقرروا كيفية إدارة التعارضات بين قابلية الاستخدام والأمن والتكلفة، وهذا أكثر مجال نحتاج فيه إلى أن يفند مجلس الإدارة العمليات ويختبرها».

تعمق في الموضوع. ينبغي أن تكون المجالس على دراية بما إن كانت منشآتها تعمل بانتظام على تقييم وتحسين تقييمات المخاطر السيبرانية. وغالبًا ما يُطلب من فريق التدقيق الداخلي إجراء تقييم أولي أو إنشاء مشروع، قد يكون تدقيق هجمة واختراق، إلا أن ذلك ليس سوى خطوة أولى، وذلك بحسب ما نبهت إليه بوندمان. وتحتاج الشركات إلى استراتيجية متعددة الأوجه لمنع الحوادث السيبرانية واكتشافها والاستجابة لها. وينبغي أن يشمل هذا الجهد تقييمًا للخطوات المتواصلة التي تتخذها الشركة لفهم الهجمات وفعالية التدابير التي يجري اتخاذها وكيفية مراقبة الحوادث والاستجابات وآليات استجابة الشركة ومدى نجاحها. فبحسب ما قالته بوندمان، إن تقييم الاستراتيجية كاملة يمكن أن يبدأ على مستوى اللجنة، ولكن ينبغي أن يناقشه مجلس الإدارة بأكمله.

بحسب ما أشارت إليه إحدى منشورات شركة ديلويت (Deloitte)، يتكون الخط الأول في مواجهة المخاطر السيبرانية من وحدات الشركة وتكنولوجيا المعلومات، التي تتناول المخاطر في قراراتها وعملياتها اليومية. والخط الثاني للمنشأة هو قيادة إدارة مخاطر المعلومات والتكنولوجيا، التي تتولى الحوكمة والمراقبة. ووظيفة التدقيق الداخلي هي الخط الثالث بصورة متزايدة، حيث تجري مراجعة مستقلة للتدابير الأمنية والأداء.

افهم ما يميز هذه المخاطر. المنشآت ومجالس إدارتها على دراية بالمخاطر، إلا أن مخاطر الأمن السيبراني تختلف عن غيرها لسببين. أولًا، أنها على درجة عالية من التخصص والتهديدات فيها تتغير باستمرار، مما يجعلها خارج نطاق خبرة العديد من أعضاء مجلس الإدارة. ثانيًا، يشيع استخدام الإنترنت في معظم المنشآت، وبالتالي فإن المخاطر وتأثيراتها متعددة الأوجه ومعقدة. إذ قال أحد المشاركين في حلقة نقاش "لشبكة مدير المخاطر السيبرانية" (CRDN): «إن استخدام المنشآت للإنترنت أمر ضروري لتحقيق منفعة، وجميع المعاملات التي تعتمد على استخدام الإنترنت غير آمنة بطبيعتها». وقال: «هذا لا ينطبق على أي جانب آخر من جوانب المخاطر التي تتعامل معها مجالس الإدارة».

أسئلة لأعضاء مجلس الإدارة

- كم مرة يتلقى مجلس الإدارة مستجدات عن تهديدات الأمن السيبراني على المنشأة والخطوات التي يجري اتخاذها لمعالجة وإدارة المخاطر السيبرانية؟
- هل تتعامل المنشأة مع الأمن السيبراني على أنه مشكلة تتعلق بمخاطر المؤسسة ككل وليس على أنه فقط أحد شؤون تكنولوجيا المعلومات؟
- هل يقوم مجلس الإدارة بدور استباقي في مراقبة المخاطر السيبرانية أم أنه يفترض أن كل شيء على ما يرام ما لم يتم إخباره بخلاف ذلك؟
- هل لدى مجلس الإدارة لجنة مخصصة للأمن السيبراني؟ إن لم يكن الأمر كذلك، فهل تتحمل لجنة أخرى، مثل لجنة التدقيق، مسؤولية مراقبة الأمن السيبراني؟

وفر مثالًا في الحياة الواقعية. في تمرين محاكاة، يمكن إجراؤه عن طريق التدقيق الداخلي أو إدارة أخرى أو طرف خارجي، يشرف مجلس الإدارة والإدارة على محاكاة هجمة لمعرفة كيفية استجابة المنشأة وكيفية إخطار المستثمرين وكيف يتأثر العملاء أو شركاء الأعمال. (حتى أن بوندمان عملت مع مجلس إدارة طلب أن يكون مدير تقنية المعلومات والمدير التنفيذي فقط على دراية بأن الوضع هو عبارة عن محاكاة، لجعل هذا التمرين واقعيًا قدر الإمكان). وبمجرد أن تقوم المنشأة بتقييم استجابتها، يمكن لمجلس الإدارة تلقي مستجدات عن التغييرات التي جرى تنفيذها أو قيد التنفيذ.

يمكن أن يضطلع التدقيق الداخلي أيضًا بدور محوري في تمرين قيّم آخر: تصوير نموذج نضج القدرة، والذي يقدم رؤية مؤسسية عالية المستوى للمخاطر السيبرانية ويقارن بين ما هي عليه المنشأة وما ينبغي أن تكون عليه، كل ذلك بلغة مبسطة. وبحسب ما قالته بوندمان، نظرًا لأنه من غير الممكن مراقبة جميع المخاطر ومعالجتها، يمكن أن تساعد هذه التمارين أيضًا في توضيح الأهداف الأهم حتى تتمكن المنشأة من تعزيز الوقاية والاكتشاف في هذه المجالات.

لا تدع المخاطر تفاجئك. مع التوسع في الاعتماد على التكنولوجيا، تزداد المخاطر المرتبطة بالتقنيات الناشئة غير المألوفة. وأشارت بوندمان إلى أنه يمكن حتى لنظام تخطيط موارد المؤسسات الجديد أن يشكل تحديات أمنية ينبغي عدم إغفالها. وتخطئ العديد من الشركات بالانتظار حتى حدوث مشكلة في النظام الجديد قبل التخطيط لكيفية التعامل مع المشكلات. وكما قالت بوندمان: «تأكد من أن لديك خطة أمنية من البداية للإستراتيجية السيبرانية والرقابية».

يمكن أن تواجه المنشآت المنخرطة في عمليات الدمج والاستحواذ أيضًا ثغرات جديدة. ونصحت بوندمان: «إن كنت ستستحوذ على شركة، اسأل عن المخاطر التي ستتعرض لها أثناء قيامك بربط أعمالك». وقد تتعرض الشركات التي تعمل مع سلاسل توريد أو أطراف خارجية أخرى أيضًا لمخاطر من تلك المصادر. بالإضافة إلى ذلك، في مجال الامتثال، ينبغي أن تكون المنشآت على دراية باللوائح ذات الصلة، مثل قوانين هيئة الأوراق المالية والبورصات (SEC) بشأن الإفصاحات المتعلقة بالأمن السيبراني.

الاستفادة من موارد التدقيق الداخلي

قد تكون التهديدات السيبرانية عسيرة، ولكن التدقيق الداخلي يمكن أن يقدم منظورًا فريدًا ومستقلًا عن مخاطر المنشأة وأفضل الطرق لمعالجتها. وينبغي أن تكون مجالس الإدارة، التي تكون استباقية في مراقبتها لمسائل الأمن السيبراني وتستفيد كامل الاستفادة من القيمة التي يمكن أن يقدمها التدقيق الداخلي، في وضع أفضل للتعامل مع مخاطر الأمن السيبراني بفعالية.

ما الذي ينقص مجلس الإدارة؟

60% من المنشآت لا يوجد بها رئيس للأمن السيبراني ضمن مجلس الإدارة أو على مستوى الإدارة التنفيذية.

59% من المنشآت تقول إن العلاقة بين الأمن السيبراني وخطوط العمل محايدة في أفضل الأحوال، أو غير موثوق بها أو غير موجودة.

20% من المجالس واثقة تمامًا من أن مخاطر الأمن السيبراني وإجراءات التخفيف المقدمة لها يمكن أن تحمي المنشأة من الهجمات السيبرانية الكبرى.

36% من المنشآت تقول إن الأمن السيبراني يتم تناوله منذ مرحلة التخطيط لمبادرة أعمال جديدة.

المصدر: *"The Risky Six: Key Questions to Expose Gaps in Board Understanding of Organizational Cyber Resiliency"* IIA Global and EY، March 30, 2021.

سؤال الاستطلاع السريع

هل يوجد في مجلس إدارتك عضو لديه خبرة في الأمن السيبراني؟

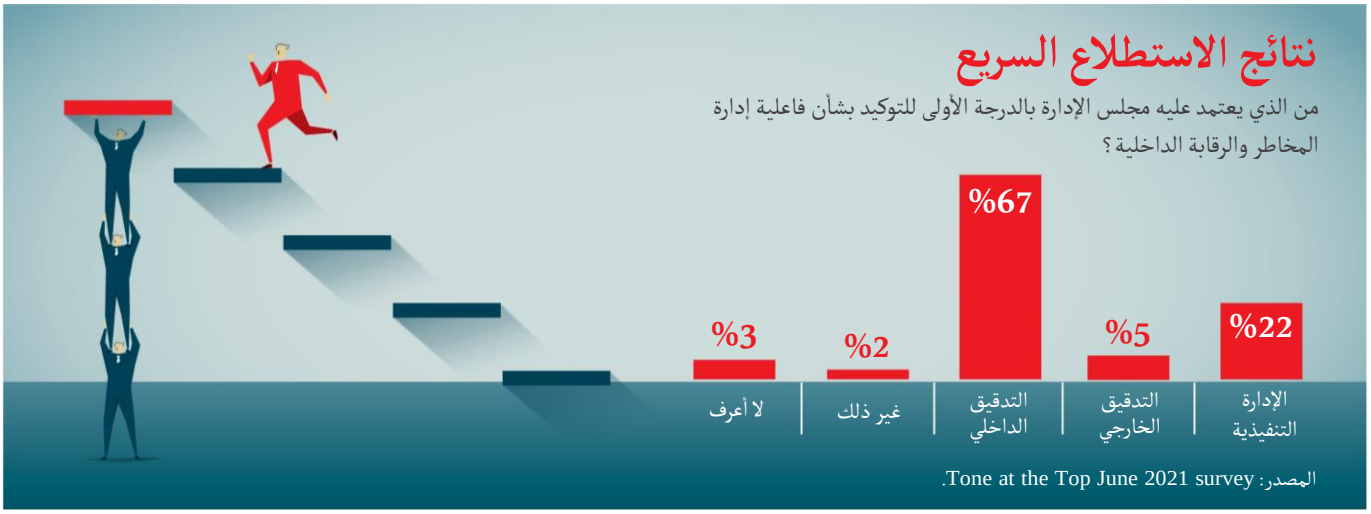
- ❑ نعم
- ❑ لا
- ❑ لا أعرف

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

[1] *Executive Perspectives on Top Risks for 2021 and 2030*, Protiviti and NC State University's ERM Initiative, 2021.
[2] *"Cybercrime to Cost the World $10.5 Trillion Annually by 2025,"* Steve Morgan, *Cybercrime Magazine*, November 13, 2020.
[3] *Cost of a Data Breach Report*, IBM, 2021.
[4] *"Gartner Predicts 40% of Boards Will Have a Dedicated Cybersecurity Committee by 2025,"* Gartner press release, January 28, 2021.
[5] *"Boards and Cybersecurity,"* McKinsey and Company podcast, February 2, 2021.
[6] *"Cybersecurity and the Role of Internal Audit: An Urgent Call to Action,"* Sandy Pundmann, Deloitte, 2017.
[7] *"Cybersecurity: An Evolving Governance Challenge,"* Harvard Law School Forum on Corporate Governance, March 15, 2020.
[8] *"Commission Statement and Guidance on Public Company Cybersecurity Disclosures,"* Release Nos. 33-10459; 34-82746, Securities and Exchange Commission, February 26, 2018.

نتائج الاستطلاع السريع

من الذي يعتمد عليه مجلس الإدارة بالدرجة الأولى للتوكيد بشأن فاعلية إدارة المخاطر والرقابة الداخلية؟



المصدر: Tone at the Top June 2021 survey.