ترنيمة الإدارة العليا
TONE at the TOP®

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

العدد 119 | أكتوبر 2023

قوانين إفصاح عن الأمن السيبراني جديدة صادرة عن هيئة الأوراق المالية والبورصات الأمريكية (SEC): ما يجب على مجالس الإدارة فعله لمواكبة المستجدات

تزيد قوانين الإفصاح الجديدة المتعلقة بالأمن السيبراني الصادرة عن هيئة الأوراق المالية والبورصات الأمريكية (SEC) من أهمية الحوكمة القوية في التعامل مع هذه المخاطر الواسعة الانتشار. ونظرًا للصياغة النهائية لهذه القوانين مؤخرًا، فإن «الشركات المطروحة أسهمها للتداول العام من كافة الأحجام تتسابق الآن للالتزام بها قبل المواعيد النهائية المحددة الوشيكة»، وذلك بحسب ما ورد في مقالة صادرة عن الرابطة الوطنية لأعضاء مجالس الشركات (NACD).[1] وينبغي أن يكون فهم تأثيرات القوانين الجديدة واتخاذ الخطوات اللازمة لضمان الالتزام بها من الأولويات القصوى للمنشآت. يتناول هذا العدد من "ترنيمة الإدارة العليا" التوجيهات الجديدة ويناقش أهم المساهمات التي يمكن أن يقدمها التدقيق الداخلي في الجهود المبذولة في مجال الأمن السيبراني في الشركة. كما أنه يسلط الضوء على المسؤوليات الجديدة والاعتبارات المهمة الأخرى لأعضاء مجلس الإدارة.

تهديد متزايد

يتعلق الأمن السيبراني بحماية موارد المعلومات لدى المنشأة، ومنها أجهزة الكمبيوتر وأجهزة الشبكة والبرمجيات والبيانات، من الوصول غير المصرح به أو التعطيل أو التدمير. إلا أن مع كل تقدم تكنولوجي، يجد المحتالون طرقًا جديدة لشن هجمات على الأمن السيبراني، مما يجعل المخاطر السيبرانية أحد الاعتبارات المهمة لأي منشأة.

قد تكون تكاليف الاختراقات السيبرانية فادحة: أفاد ما يقرب من 60% من الرواد في مجال الأمن السيبراني في القطاع الخاص الذين استجابوا لدراسة أجرتها شركة "سيسكو" (Cisco) أنهم تعرضوا لحادث أمن سيبراني خلال الاثني عشر شهرًا الماضية، وفيما يخص النسبة المتبقية 41% من المتضررين بلغت التكلفة 500,000 دولار على الأقل.[2] وبالإضافة إلى أي تكاليف مالية مباشرة، بإمكان الجرائم والهجمات السيبرانية أن تعرقل قدرة الشركة على القيام بنشاطها وتكشف البيانات السرية للشركة والعملاء وتضر بسمعتها.

ليس من المستغرب إذن أن تصدر هيئة الأوراق المالية والبورصات في الصيف الماضي قوانين جديدة بشأن كيف يجب أن تبلغ الشركات المطروحة أسهمها للتداول العام عن اختراقات الأمن السيبراني الجوهرية والإفصاح عن معلومات تتعلق بإدارة مخاطر الأمن السيبراني واستراتيجيته وممارسات الحوكمة المتعلقة به. ويأتي القانون بتحديث للمقترحات التي أُصدرت في عام 2022 والصياغة النهائية لها.

تأثير المخاطر السيبرانية

ما هي العواقب السلبية التي واجهتها المنشآت بسبب الحوادث والاختراقات السيبرانية ؟

الأثر	2021 الترتيب	2023 الترتيب	2023 النسبة
الاضطراب التشغيلي (بما في ذلك سلسلة التوريد/أو النظام البيئي الشريك)	1	1	%58
خسارة الإيرادات	9	2	%56
فقدان ثقة العملاء/التأثير السلبي على العلامة التجارية	4	3	%56
خسارة السمعة	5	4	%55
وقف تمويل مبادرة استراتيجية	غ/م	5	%55
فقدان الثقة في السلامة التكنولوجية	غ/م	6	%55
الأثر السلبي على توظيف المواهب والاحتفاظ بها	8	7	%54
سرقة الملكية الفكرية	2	8	%54
انخفاض في سعر الأسهم	2	9	%52
الغرامات التنظيمية	7	10	%52
التغيير في القيادة	5	غ/م	غ/م

نبذة عن معهد المدققين الداخليين (IIA)

معهد المدققين الداخليين (IIA) هو جمعية مهنية عالمية غير ربحية تخدم أكثر من 230,000 عضو في العالم ومنحت أكثر من 185,000 شهادة مدقق داخلي معتمد (CIA) في جميع أنحاء العالم. وتأسس معهد المدققين الداخليين (IIA) في عام 1941، وهو معروف في جميع أنحاء العالم باعتباره الجهة الرائدة التعليمية التي تضع المعايير وتمنح الشهادات وتجري الأبحاث وتقدم الإرشادات المختصة في مجال مهنة التدقيق الداخلي.. لمزيد من المعلومات، وتفضل بزيارة theiia.org.

The IIA

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

الاشتراك المجاني

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

التوسع في الإفصاح بشأن إدارة الأمن السيبراني وحوادثه

تهدف قوانين هيئة الأوراق المالية والبورصات الأمريكية (SEC) إلى رفع مستوى وتوحيد إفصاحات الأمن السيبراني من الشركات العامة الخاضعة لمتطلبات الإبلاغ المنصوص عليها في "قانون الأوراق المالية" (Exchange Act Securities). ووطدت القوانين الجديدة ما يجب على الشركات الإبلاغ عنه فيما يتعلق بإدارة المخاطر واستراتيجيتها وحوكمتها وحوادث الأمن السيبراني التي تعتبر جوهرية. وتتضمن القوانين الجديدة متطلبات على الشركات المسجلة للتداول:

- تبيان كيفية تقييمها وتحديدها وإدارتها لتهديدات الأمن السيبراني وهل أثرت أي مخاطر جوهريًا أو يوجد احتمال معقول بأنها ستؤثر جوهريًا على استراتيجية أعمالها أو نتائج العمليات أو الوضع المالي. ويجب على هذه الشركات أيضًا الإفصاح عن حوادث الأمن السيبراني الجوهرية ووصف الجوانب الجوهرية لطبيعة كل حادث ونطاقه وتوقيته.
- تقديم تفاصيل عن كيفية إشراف مجلس الإدارة على المخاطر السيبرانية ودور الإدارة في تقييم وإدارة المخاطر الجوهرية. إذ قررت هيئة الأوراق المالية والبورصات (SEC) عدم اعتماد متطلب مقترح بشأن الإفصاح عن خبرة مجلس الإدارة في مجال الأمن السيبراني.
- تخضع جهات الإصدار الخاصة الأجنبية للقوانين نفسها ويجب عليها أيضًا تقديم معلومات عن حوادث الأمن السيبراني الجوهرية التي تعلن عنها أو يُطلب منها الإعلان عنها أو الإفصاح عنها بطريقة أخرى في ولاية قضائية أجنبية أو لأي بورصة أو لحاملي الأوراق المالية.
- تقديم نموذج "K-8" عمومًا في غضون أربعة أيام عمل من تحديد المنشأة أن الحادث السيبراني جوهري. (قد يُسمح بالتأخير في الإفصاح إذا قرر المدعي العام الأمريكي أن الإفصاح الفوري من شأنه أن يشكل خطرًا كبيرًا على الأمن القومي أو السلامة العامة وأخطر لجنة الأوراق المالية والبورصات بذلك كتابيًا).

الاعتبارات الرئيسية لمجالس الإدارة

تُجري العديد من المؤسسات تقييمات للثغرات لمعرفة مدى نجاحها حاليًا في تحديد الأحداث السيبرانية وتحليلها وإدارتها والتعافي منها. فوفقًا لما قاله "جورج برهام"، مدقق داخل معتمد (CIA)، وحاصل على شهادة ضمان إدارة المخاطر المعتمدة (CRMA)، ومدقق نظم معلومات معتمد (CISA)، ومدير المعايير والتوجيه المهني في معهد المدققين الداخليين (IIA)، إنه على ضوء القوانين الجديدة، ينبغي أن تتأكد مجالس الإدارة من أن الإدارة تحدد ما إن كانت عملية التقييم الحالية ستدعم فترة تحول مدتها أربعة أيام. وعلى الرغم من أن فريق تكنولوجيا المعلومات سيحدد الحوادث، فإن تحديد الأهمية النسبية يجب أن يتضمن إسهامات من مجالات أخرى، مثل الفرق المالية والقانونية والتنظيمية، لاكتساب منظور واسع النطاق.

يجب أن يدرك أعضاء مجلس الإدارة أيضًا أن الأهمية النسبية تتضمن عناصر كمية ونوعية إذ قال برهام: «الأمر يتعلق بأمور أهم من مجرد تأثير الدولار». كما أنها تنطوي على اعتبارات قانونية وتنظيمية. فإذا كانت الشركة تعمل في الاتحاد الأوروبي، على سبيل المثال، قد يندرج حادث ما ضمن نطاق اللائحة العامة لحماية البيانات (GDPR). وقد تكون الاعتبارات الإستراتيجية أيضًا عاملًا ذا أهمية نسبية، على سبيل المثال، إذا كان الحادث ينطوي على الكشف عن أسرار تجارية أو معلومات أخرى تمنح المنشأة ميزة تنافسية. وقال برهام إن من المفترض أن يشمل تحديد الأهمية النسبية أي اعتبارات قد يكون لها تأثير على تحليل المستثمر للشركة.

ونظرًا لأن البند 106 من اللائحة يتناول أدوار مجلس الإدارة ومسؤولياته، فإن النموذج "K-10" السنوي هو المكان الذي ينبغي أن توثق فيه المنشآت حوكمتها للأمن السيبراني. فقد يقرر البند، على سبيل المثال، أن لجنة التدقيق التابعة لمجلس الإدارة مسؤولة عن مراجعة المخاطر السيبرانية، وهو ما يحدث غالبًا، ويمكن أن يشمل أيضًا كيف ترفع الإدارة تقاريرها إلى لجنة التدقيق أو مجلس الإدارة بشأن مسائل الأمن السيبراني. وكجزء من مسؤوليات أعضاء مجلس الإدارة، يُفترض أن يعرفوا مؤهلات من يتعامل مع مسائل الأمن السيبراني على مستوى الإدارة وكيفية إدارة التهديدات السيبرانية والتخفيف من حدتها.

مساهمة التدقيق الداخلي

غالبًا ما يكون المدققون الداخليون مسؤولين عن تحديد واختبار أهم الضوابط الداخلية التي تساعد في التخفيف من المخاطر المتعلقة بالأمن السيبراني، بما في ذلك الرجوع إلى أطر الرقابة المعتمدة على نطاق واسع. وعلى ضوء القوانين الجديدة، ستحتاج مجالس الإدارة والإدارة العليا في المنشآت إلى توكيد مستقل وموضوعي وواسع الاطلاع للتحقق من فاعلية وكفاءة ضوابط استجابة الأمن السيبراني وتعافيه. وبإمكان التدقيق الداخلي أن يقدم هذا التوكيد بما يتوافق مع معاييره المهنية الخاصة ومع أطر الرقابة المقبولة على نطاق واسع، لا سيما الأطر التي تستخدمها وظائف تكنولوجيا المعلومات وأمن المعلومات في المنشأة. وبإمكان المدققين الداخليين أيضًا تقديم خدمات استشارية حينما تحدد الشركات أفضل السبل للحماية من المخاطر السيبرانية.

وبينما تحدد المنشآت كيفية التعامل مع المتطلبات الجديدة، يمكن أن تشمل بعض الأدوار المحددة للرئيس التنفيذي للتدقيق الداخلي وفريق التدقيق الداخلي ما يلي:

- التشاور مع مجالس الإدارة والإدارة التنفيذية وقادة إدارة مخاطر الأمن السيبراني بشأن التأثير المتوقع للقوانين من منظور مالي ومنظور التخطيط الاستراتيجي ومنظور الامتثال ومنظور خطة التدقيق.
- تحديث تقييمات المخاطر فيما يتعلق بالالتزام باللوائح الجديدة ودعم استعدادات المنشأة لتلبية المتطلبات. وإذا لم يكن التدقيق الداخلي منخرطًا بالفعل في تقييمات مخاطر الأمن السيبراني، فيمكنه البدء في المساهمة في هذه العملية.
- الإبلاغ عما إن كانت ضوابط الأمن السيبراني الحالية مصممة التصميم المناسب وتعمل بفاعلية حتى تلتزم المنشأة بالقوانين الجديدة.

وأشار برهام إلى أن: «عادةً ما يُعتبر الأمن السيبراني من المجالات الأعلى خطورة التي يتعين على المنشآت إدارتها»، لذا فمن المؤكد أنه من الأساس من ضمن اهتمامات التدقيق الداخلي. وهذا يعني أن التدقيق الداخلي مدرك لما يتعلق به من مخاطر والضوابط الداخلية اللازمة للتخفيف من هذه المخاطر. وبإمكان التدقيق الداخلي أيضًا أن يوفر المعلومات والأفكار التي تحتاج إليها مجالس الإدارة للوفاء بمسؤولياتها المتعلقة بحوكمة الأمن السيبراني بموجب القوانين الجديدة. وبالإضافة إلى المنظور الذي تقدمه الإدارة، يمكن للتدقيق الداخلي أن يقدم وجهة نظر مستقلة وموضوعية بشأن كيفية إدارة المخاطر السيبرانية والإفصاح عنها. ويمكنه تقديم المشورة للجنة التدقيق بشأن إدراج مخاطر ولوائح الأمن السيبراني في خطة التدقيق وتقديم تقرير عن مدى استعداد المنشأة للالتزام بقوانين هيئة الأوراق المالية والبورصات ومدى تنفيذها في المستقبل.

الالتزام بالموعد النهائي

فيما يخص الإفصاح عن الحوادث، أو نماذج K-8، يبدأ سريان القوانين بعد 90 يومًا من نشرها في السجل الفيدرالي أو في 18 ديسمبر 2023 (أمام الشركات الصغيرة الملزمة بالإبلاغ ما يصل إلى 180 يومًا إضافيًا للالتزام). وسيكون موعد الإفصاحات في النموذج K-10 بدءًا بالتقارير السنوية للسنوات المالية المنتهية بتاريخ 15 ديسمبر 2023 أو بعده. وذكرت الرابطة الوطنية لأعضاء مجالس الشركات (NACD) أنه على الرغم من أن القوانين الجديدة لا تتناول مؤهلات أعضاء مجلس الإدارة، فإنها «ترتقي بدور جميع القيادات ومنها مجلس الإدارة والرؤساء التنفيذيون وكبار مسؤولي أمن المعلومات في إدارة المخاطر». وبينما يتولى أعضاء مجلس الإدارة مسؤولياتهم الجديدة، يمكنهم اللجوء إلى التدقيق الداخلي للحصول على التوكيدات القيّمة والرؤية المتعمقة التي سيحتاجون إليها لمعالجة شؤون الأمن السيبراني.

أسئلة لأعضاء مجلس الإدارة

- كيف تتأكد المنشأة من استعدادها للالتزام بالقوانين الجديدة الصادرة عن هيئة الأوراق المالية والبورصات (SEC)؟
- ما أنواع الضوابط الموجودة بالفعل لمنع الهجمات السيبرانية أو التخفيف منها؟ وما مدى نجاحها؟
- هل تُوضع ضوابط أو إجراءات جديدة للإبلاغ للتعامل مع القوانين الجديدة لهيئة الأوراق المالية والبورصات؟ إن كان الأمر كذلك، فما هي؟
- هل تعرضت المنشأة لأي حوادث سيبرانية جوهرية خلال العامين الماضيين؟ وكيف تمت معالجتها وما هي التحسينات التي يمكن إدخالها؟
- ما نوع التوكيد أو المشورة المقدمة من التدقيق الداخلي التي يمكن أن تساعد مجلس الإدارة على الوفاء بمسؤولياته المتعلقة بمراقبة المخاطر السيبرانية؟

"Time Is of the Essence with SEC's Approved Cybersecurity Disclosure Rules," James Turgal, NACD, September 12, 2023.
Cisco Cyber Security Readiness Index: Resilience in a Hybrid World Cisco, March 2023.