الأمن السيبراني للمؤسسات المالية الأصغر حجمًا

قائمة التدقيق الخاصة بمجلس الإدارة: قيادة الأمن السيبراني

أساسيات إدارة المخاطر السيبرانية

- ☐ كمجموعة، قوموا على أساس دوري بتقييم ما إذا كان مجلس الإدارة يمكن أن يجيب بشكل إيجابي عن الأسئلة التالية:
  - هل تلبي مؤسستك المتطلبات القانونية والتنظيمية ذات الصلة، مثال، النظام الأوروبي العام لحماية البيانات (GDPR)؟
  - هل حددت مؤسستك عدد الهجمات السيبرانية التي تعرضت لها واختبرت مرونتها المالية؟
  - هل تمتلك مؤسستك خطة تحسين لضمان أن الهجمات تقع ضمن معدل المخاطر المتفق عليه؟
  - هل يُناقش مجلس الإدارة بانتظام معلومات دقيقة وواضحة وقابلة للتنفيذ متعلقة بالمرونة السيبرانية للمؤسسة المدعومة من الإدارة؟
  - هل لدى مؤسستك خطط استجابة للحوادث خضعت مؤخرًا لاختبار تجريبي، بما في ذلك على مستوى مجلس الإدارة؟
  - هل أدوار الأشخاص الرئيسيين المسؤولين عن إدارة المخاطر السيبرانية واضحة ومتماشية مع خطوط الدفاع الثلاثة؟
  - هل أجريت تصديقًا وتأكيدًا مستقلين لوضع المخاطر السيبرانية لمؤسستك، على سبيل المثال، عبر الاختبار أو التصديق أو التأمين؟
- ☐ إذا لم تستطع الإجابة بشكل إيجابي عن واحد أو أكثر مما سبق، فتعاون مع المدير التنفيذي ومدير أمن المعلومات وموظفي المؤسسة المعنيين و/أو الجهات الخارجية لحل المشكلة.

الإشراف

- ☐ تأكد من أن مجلس الإدارة على دراية بدوره باعتباره صاحب المسؤولية النهائي للمخاطر والمرونة السيبرانية لمؤسستك.
  - ☐ فوض أمر الإشراف إلى لجنة مجلس إدارة معينة إذا لزم الأمر.
- ☐ قم بتعيين مسؤول شركة واحد، عادةً مدير أمن المعلومات (CISO) المعين، ليكون مسؤولاً عن الإبلاغ عن قدرة مؤسستك على إدارة المرونة السيبرانية والتقدم في تنفيذ أهداف المرونة السيبرانية.
  - ☐ تأكد من أن هذا المسؤول يتمتع بتواصل منتظم مع المجلس، وسلطة كافية، وإتقان للموضوع المعني، والخبرة والموارد اللازمة لتنفيذ هذه المهام.
- ☐ حدد مدى تحمل مؤسستك للمخاطر سنويًا؛ مع ضمان الاتساق مع استراتيجية شركتك ومعدل المخاطر.
- ☐ احرص على أن يتم إجراء مراجعة مستقلة للمرونة السيبرانية لمؤسستك سنويًا.
- ☐ اعمل على دمج المرونة السيبرانية وتقييم المخاطر في استراتيجية الأعمال الشاملة لمؤسستك، وإدارة المخاطر، ووضع الميزانية، وتخصيص الموارد.
- ☐ قم بالإشراف على ابتكار خطط المرونة السيبرانية وتنفيذها واختبارها وتحسينها بصورة مستمرة، لضمان توافقها في جميع أنحاء مؤسستك وأن مدير أمن المعلومات (CISO) أو الموظف الآخر المسؤول يقدم تقارير عنها بصفة منتظمة إلى مجلس الإدارة.
- ☐ راجع أدائك لما ورد أعلاه بشكل دوري وفكر في طلب مشورة مستقلة للتحسين المستمر.

البقاء على اطلاع

- ☐ عندما ينضم فرد جديد إلى مجلس الإدارة، تأكد من أنه يتمتع بمهارات ومعرفة مناسبة ومحدثة لفهم المخاطر التي تمثلها التهديدات السيبرانية وإدارتها.
- ☐ اطلب المشورة المنتظمة من الإدارة فيما يتعلق بتعرض مؤسستك للمخاطر الحالية والمستقبلية، والمتطلبات التنظيمية ذات الصلة، والمعايير الصناعية والاجتماعية لمعدل المخاطر الذي تتبناه. خطط للمشاركة في:
  - جلسات إحاطة منتظمة بشأن الواجبات التي تنشأ عن اللوائح والتشريعات الجديدة،
  - التخطيط المشترك لمجلس الإدارة واللجنة التنفيذية والزيارات إلى الأقران والقادة أصحاب أفضل الممارسات في مجال الأمن السيبراني،
  - جلسات الإحاطة الأمنية بشأن بيئة التهديد،
  - وتبادل المعلومات على مستوى مجلس الإدارة بشأن الإدارة والإبلاغ.
- ☐ أوضح للإدارة أنها مسؤولة عن الإبلاغ عن تقييم كمي ومفهوم للمخاطر والتهديدات والأحداث السيبرانية كعنصر دائم في جدول أعمال اجتماعات مجلس الإدارة.
- ☐ راجع بانتظام مع الإدارة والموظفين الآخرين المعنيين التطورات المتعلقة بالتحديات النظامية المستمرة مثل نقاط ضعف سلسلة التوريد، والتبعيات المشتركة، والفجوة في تبادل المعلومات بين مجالس الإدارة بشأن إدارة المخاطر السيبرانية.

تمهيد السبيل

- ☐ تأكد من أن الموظفين على جميع المستويات يدركون أن كلاً منهم لديه مسؤوليات مهمة لضمان المرونة السيبرانية لمؤسستك.
- ☐ قم بالإشراف على دور الإدارة في تعزيز ثقافة المخاطر لمؤسستك والحفاظ عليها. قيّم بانتظام فعالية ثقافة المخاطر لمؤسستك، مع الوضع في الاعتبار تأثير الثقافة على السلامة والقدرة وإجراء التغييرات عند الضرورة.
- ☐ وضح أنك تتوقع من جميع الموظفين التصرف بنزاهة والإبلاغ الفوري عن أية عملية عدم امتثال ملحوظة داخل مؤسستك أو خارجها.