دليل يستهدف مستوى مجلس الإدارة: قيادة الأمن السيبراني

أساسيات إدارة المخاطر السيبرانية

أكد قدرتك على الإجابة عن الأسئلة التالية بشكل إيجابي:

1. هل تلبي مؤسستك المتطلبات القانونية والتنظيمية ذات الصلة؟
2. هل حددت مؤسستك عدد الهجمات السيبرانية التي تعرضت لها واختبرت مرونتها المالية؟
3. هل تمتلك مؤسستك خطة تحسين لضمان أن الهجمات تقع ضمن معدل المخاطر المتفق عليه؟
4. هل يُناقش مجلس الإدارة بانتظام معلومات دقيقة وواضحة وقابلة للتنفيذ متعلقة بالمرونة السيبرانية للمؤسسة المدعومة من الإدارة؟
5. هل لدى مؤسستك خطط استجابة للحوادث خضعت مؤخرًا لاختبار تجريبي، بما في ذلك على مستوى مجلس الإدارة؟
6. هل أدوار الأشخاص الرئيسيين المسؤولين عن إدارة المخاطر السيبرانية واضحة ومتماشية مع خطوط الدفاع الثلاثة؟
7. هل أجريت تصديقًا وتأكيدًا مستقلين لوضع المخاطر السيبرانية لمؤسستك؟

الإشراف

باعتباره أعلى مستوى قيادي في مؤسستك، يتحمل المجلس المسؤولية الكاملة عن التحكم في المخاطر السيبرانية وبالتالي يجب أن يشرف على إستراتيجية المؤسسة وسياساتها والأنشطة في هذا المجال. تحديدًا، يجب على مجلس الإدارة:

- تحمل المسؤولية المطلقة عن الإشراف على المخاطر السيبرانية والمرونة، سواء كمجلس إدارة كامل أو من خلال تفويض لجنة مجلس إدارة معينة بالإشراف.
- تعيين مسؤول شركة واحد، عادةً مدير أمن المعلومات، ليكون مسؤولاً عن الإبلاغ عن قدرة مؤسستك على إدارة المرونة السيبرانية والتقدم في تنفيذ أهداف المرونة السيبرانية. التأكد من أن هذا المسؤول يتمتع بتواصل منتظم مع المجلس، وسلطة كافية، وإتقان للموضوع المعني، والخبرة والموارد اللازمة لتنفيذ هذه المهام.
- تحديد مدى تحمل مؤسستك للمخاطر سنويًا؛ ضمان الاتساق مع إستراتيجية شركتك ومعدل المخاطر.
- الحرص على إجراء مراجعة مستقلة للمرونة السيبرانية لمؤسستك سنويًا.
- الإشراف على ابتكار خطط المرونة السيبرانية وتنفيذها واختبارها وتحسينها بصورة مستمرة، لضمان التوافق في جميع أنحاء مؤسستك وأن مدير أمن المعلومات (CISO) أو الموظف الآخر المسؤول يقدم تقارير عنها بصفة منتظمة إلى مجلس الإدارة.
- قم بدمج المرونة السيبرانية وتقييم المخاطر في إستراتيجية الأعمال الشاملة لمؤسستك، وإدارة المخاطر، ووضع الميزانية، وتخصيص الموارد، بهدف دمج المخاطر السيبرانية بشكل كامل في المخاطر التشغيلية الشاملة. راجع مخاطر الجهة الخارجية بشكل منتظم.
- راجع دائمًا أداءك لما ورد أعلاه وفكر في الحصول على مشورة مستقلة لضمان التحسين المستمر.

البقاء على اطلاع

يعتمد الإشراف الفعال لمجلس الإدارة على المخاطر السيبرانية على مدى دراية الأعضاء بالموضوع والمعلومات الحديثة.

- تأكد من أن جميع الأفراد الذين ينضمون إلى مجلس الإدارة يتمتعون بمهارات ومعرفة مناسبة ومحدثة لفهم وإدارة المخاطر التي تمثلها التهديدات السيبرانية.
- اطلب المشورة المنتظمة من الإدارة فيما يتعلق بتعرض مؤسستك للمخاطر الحالية والمستقبلية، والمتطلبات التنظيمية ذات الصلة، والمعايير الصناعية والاجتماعية لمعدل المخاطر الذي تتبناه. علاوة على ذلك، شارك في جلسات إحاطة منتظمة بشأن أحدث التطورات فيما يتعلق ببيئة التهديدات والبيئة التنظيمية، والتخطيط المشترك والزيارات إلى الأقران والقادة الذين يطبقون أفضل الممارسات في مجال الأمن السيبراني، وتبادل الحوكمة والإبلاغ على مستوى مجلس الإدارة.
- حمل الإدارة مسؤولية تقديم تقييم كمّي ومفهوم للمخاطر والتهديدات والأحداث السيبرانية كعنصر دائم في جدول أعمال اجتماعات مجلس الإدارة.
- كن على وعي دائم بالتحديات التنظيمية المستمرة مثل نقاط الضعف في سلسلة التوريد، والتبعيات المشتركة، والفجوات في تبادل المعلومات.

تمهيد السبيل

بالتعاون مع الإدارة العليا، يجب أن يضع مجلس الإدارة القيم الأساسية لمؤسستك ويمثلها، ويحدد ثقافة المخاطر والتوقعات فيما يتعلق بالمرونة السيبرانية.

- تعزيز ثقافة يتعرف فيها الموظفون على جميع المستويات على مسؤولياتهم المهمة في ضمان المرونة السيبرانية لمؤسستك. القيادة بالقدوة.
- قم بالإشراف على دور الإدارة في تعزيز ثقافة المخاطر لمؤسستك والحفاظ عليها. عزز ثقافة المخاطر وقم بمراقبتها وتقييمها، مع مراعاة تأثير الثقافة على السلامة والصحة، وإجراء تغييرات عند الضرورة.
- وضح أنك تتوقع من جميع الموظفين التصرف بنزاهة والإبلاغ الفوري عن أية عملية عدم امتثال ملحوظة داخل مؤسستك أو خارجها.