छोटे संगठनों के लिएसाइबर सुरक्षा

बोर्ड चेकलिस्ट:साइबर सुरक्षा का नेतृत्व

साइबर जोखिम संचालन की मूल बातें

☐ **एक समूह के रूप में, आकलन करें कि क्या बोर्ड निम्नलिखित प्रश्नों का उत्तर हाँ में दे सकता है:**

- क्या आपके संगठन ने उपयुक्त वैधानिक और नियामक आवश्यकताओं को पूरा किया गया है, उदाहरण के लिए, GDPR?
- क्या आपके संगठन ने अपने साइबर जोखिमों को निर्धारित किया है और इसके वित्तीय लचीलेपन की जांच की है?
- क्या आपके संगठन के पास इस बात को सुनि श्चित करने के लिए सुधार योजना है कि जोखिम आपके सहमत-जोखिम इच्छा के अनुसार है?
- क्या बोर्ड नियमित रूप से प्रबंधन द्वारा प्रदान की गई संगठन के साइबर लचीलेपन के बारे में संक्षिप्त, स्पष्ट और कार्रवाई करने योग्य जानकारी पर चर्चा करता है?
- क्या आपके संगठन में घटना प्रतिक्रिया योजनाएं लागू की हैं जिसका हाल ही में बोर्ड स्तर सहित पूर्व परीक्षण किया गया है?
- क्या साइबर जोखिम के प्रबंधन के लिए प्रमुख लोगों की भूमिकाएं स्पष्ट और रक्षा की तीन लाइनों के साथ संरेखित हैं?
- क्या आपने अपने संगठन के साइबर जोखिम अवस्था का स्वतंत्र सत्यापन और आश्वासन प्राप्त किया है, उदाहरण के लिए, परीक्षण, प्रमाणीकरण, या बीमा के माध्यम से?

☐ **यदि आप उपरोक्त में से एक या एक से अधिक का हाँ में जवाब नहीं दे सकते हैं, तो समस्या को सही करने के लिए अपने सीईओ, सीआईएसओ, संगठन के उपयुक्त कर्मचारियों और/या बाहरी संसाधनों के साथ काम करें।**

निरीक्षण

☐ **सुनिश्चित करें कि बोर्ड आपके संगठन के साइबर जोखिम और लचीलेपन के लिए अंतिम जिम्मेदारी व्यक्ति के रूप में इसकी भूमिका से परिचित है।**

☐ **यदि आवश्यक समझा जाए तो निरीक्षण के लिए बोर्ड की एक विशेष समिति को दायित्व सौंपे।**

☐ **एक साइबर अधिकारी को असाइन करें, जिसे आमतौर पर मुख्य सूचना सुरक्षा अधिकारी (CISO) के रूप में नियुक्त किया जाता है, जो साइबर लचीलेपन को प्रबंधित करने की आपके संगठन की क्षमता और साइबर लचीलेपन लक्ष्यों को लागू करने में प्रगति की सूचना देने के लिए जिम्मेदार होगा।**

☐ **सुनिश्चित करें कि इस अधिकारी के पास इन जिम्मेदारियों को पूरा करने के लिए बोर्ड तक नियमित पहुंच, पर्याप्त अधिकार, विषय वस्तु का नियंत्रण, अनुभव और संसाधन हैं।**

☐ **अपने संगठन के जोखिम की सहनशीलता को वार्षिक रूप से परिभाषित करें, सुनिश्चित करें कि यह आपकी कार्पोरेट रणनीति और जोखिम इच्छा के अनुरूप है।**

☐ **सुनिश्चित करें कि प्रतिवर्ष आपके संगठन की एक औपचारिक, स्वतंत्र साइबर लचीलेपन की समीक्षा की जाती है।**

☐ **अपने संगठन की समग्र व्यावसायिक रणनीति, जोखिम प्रबंधन, बजट बनाने और संसाधन आवंटन में साइबर लचीलापन और जोखिम मूल्यांकन को एकीकृत करने के लिए काम करें।**

☐ **नियमित रूप से तीसरे पक्ष के जोखिमों की समीक्षा करें।**

☐ **साइबर लचीलेपन की योजना बनाने, कार्यान्वित करने, परीक्षण करने और चल रहे सुधार का निरीक्षण करें, ताकि सुनिश्चित किया जा सके कि वे आपके पूरे संगठन में समान है और कि आपके सीआईएसओ या अन्य जिम्मेदार अधिकारी नियमित रूप से बोर्ड को उनकी सूचना देते हैं।**

☐ **समय-समय पर उपरोक्त के अपने प्रदर्शन की समीक्षा करें और निरंतर सुधार के लिए स्वतंत्र सलाह लेने पर विचार करें।**

सूचित रहें

- ☐ जब कोई व्यक्ति बोर्ड में शामिल होता है, तो सुनिश्चित करें कि उनके पास साइबर खतरों से उत्पन्न जोखिमों को समझने और प्रबंधित करने के लिए उपयुक्त और अपडेटेड कौशल और ज्ञान है।
- ☐ अपने संगठन के वर्तमान और भविष्य के जोखिम प्रकट होने, उपयुक्त नियामक आवश्यकताओं, और जोखिम इच्छा के लिए उद्योग और सामाजिक मानदण्ड पर प्रबंधन से नियमित सलाह मांगें। शामिल होने के लिए योजना बनाएं:
  - नए नियमों और कानून द्वारा बनाई गई जिम्मेदारियों पर नियमित ब्रीफिंग करें,
  - बोर्ड और कार्यकारी समिति की संयुक्त योजना और साइबरसिटी में सबसे अच्छा व्यवहार करने वाले साथियों और प्रमुख का दौरा,
  - खतरे के माहौल पर सुरक्षा की ब्रीफिंग, और
  - संचालन और रिपोर्टिंग पर सूचना का बोर्ड स्तर का आदान-प्रदान।
- ☐ प्रबंधन को स्पष्ट करें कि वे बोर्ड बैठकों के दौरान एक स्थायी एजेंडा आइटम के रूप में साइबर जोखिमों, खतरों और घटनाओं की मात्रात्मक और समझने योग्य मूल्यांकन की सूचना देने के लिए जवाबदेह हैं।
- ☐ चल रही प्रणालीगत चुनौतियों से संबंधित घटनाक्रम के बारे में प्रबंधन और अन्य संबंधित कर्मचारियों के साथ नियमित रूप से जांच करें जैसे आपूर्ति श्रृंखला की कमजोरियां, सामान्य निर्भरताएं और सूचना साझा करने में फर्क।

लहजा सेट करना

- ☐ सुनिश्चित करें कि सभी स्तरों पर कर्मचारी यह स्वीकार करते हैं कि आपके संगठन की साइबर लचीलापन सुनिश्चित करने के लिए प्रत्येक की महत्वपूर्ण ज़िम्मेदारियाँ हैं।
- ☐ अपने संगठन की जोखिम संस्कृति को प्रोत्साहित करने और बनाए रखने में निगरानी प्रबंधन की भूमिका। सुरक्षा और सुदृढ़ता पर संस्कृति के प्रभाव को देखते हुए और आवश्यक होने पर परिवर्तन करने के लिए अपने संगठन की जोखिम संस्कृति की प्रभावशीलता का नियमित रूप से आकलन करें।
- ☐ स्पष्ट करें कि आप उम्मीद करते हैं कि सभी कर्मचारी ईमानदारी के साथ कार्य करेंगे और आपके संगठन के भीतर या बाहर गैर-अनुपालन को तुरंत सूचना देंगे।