छोटे संगठनों के लिएसाइबर सुरक्षा

सीईओ चेकलिस्ट: साइबर सुरक्षा का नेतृत्व

शासन

- ☐ यदि कोई मौजूद नहीं है, तो एक मुख्य सूचना सुरक्षा अधिकारी (सीआईएसओ) की नियुक्ति करें।
- ☐ एक संगठन की व्यापक साइबर सुरक्षा नीति को स्थापित करें और बनाए रखें जो जोखिम आधारित है और अंतर्राष्ट्रीय, राष्ट्रीय और उद्योग मानकों और दिशानिर्देशों द्वारा सूचित है।
- ☐ साइबर सुरक्षा में शामिल सभी कर्मचारियों के लिए भूमिकाओं और जिम्मेदारियों को परिभाषित करें। साइबर सुरक्षा की उचित भूमिकाओं की पहचान करने और सभी स्तर के कर्मचारियों के अधिकारों का मूल्यांकन करने के लिए अपने सीआईएसओ के साथ काम करें।
- ☐ किसी भी अलग-अलग इकाइयों या कर्मचारियों के बीच स्पष्ट संचार माध्यमों की स्थापना या पहचान करें जो साइबर सुरक्षा के विभिन्न पहलुओं के साथ कार्य करते हैं।
- ☐ सुनिश्चित करें कि आपके सीआईएसओ के पास संबंधित खतरों पर आपको और बोर्ड के साथ समय पर संचार करने के लिए स्पष्ट, संचार का सीधा माध्यम है।
- ☐ वरिष्ठ प्रबंधन को संक्षेप में बताने के लिए अपने सीआईएसओ या अन्य तकनीकी कर्मचारियों एक नियमित निमंत्रण बनाए रखें।
- ☐ जाँच करें कि साइबर सुरक्षा की नीतियां, मानक और तंत्र पूरे संगठन में एक समान हैं।

जोखिम का मूल्यांकन और प्रबंधन

- ☐ अपने सीआईएसओ या अन्य तकनीकी कर्मचारियों के सहयोग से एक साइबर सुरक्षा जोखिम मूल्यांकन करें, जिसमें निम्नलिखित शामिल होने चाहिए:
  - आपके संगठन की संपत्ति और उनके तकनीकी निर्भरता के विभिन्न स्तरों के बारे में वर्णन,
  - आपके संगठन की उसकी संपत्ति की तकनीकी निर्भरता से जुड़ी परिपक्वता और आंतरिक जोखिमों का आकलन करना,
  - आपके संगठन की परिपक्वता की वांछित स्थिति का निर्धारण,
  - इस बात को समझना कि साइबर सुरक्षा के खतरे आपके संगठन की जोखिम प्राथमिकता सूची में कहां पर रहते हैं,
  - साइबर सुरक्षा की आपकी मौजूदा स्थिति और इच्छित लक्षित स्थिति के अंतर को पहचानना,
  - परिपक्वता प्राप्त करने और बनाए रखने के लिए योजनाओं को लागू करना,
  - सुरक्षा और मौजूदा अंतर को दूर करने के लिए निवेश करने के लिए धन का मूल्यांकन और चिन्हित करना,
  - अपने संगठन की साइबर सुरक्षा की परिपक्वता, जोखिमों और लक्ष्यों का लगातार पुनर्मूल्यांकन करना, और
  - सुरक्षात्मक उपायों पर विचार करें जैसे साइबर बीमा खरीदना।
- ☐ विश्लेषण करें और प्रमुख हितधारकों और बोर्ड को परिणाम प्रस्तुत करें।
- ☐ साइबर तैयारियों और प्रगति की निगरानी को बढ़ाने के लिए किसी भी चरण का निरीक्षण करने की योजना बनाएं।

संगठनात्मक संस्कृति

- ☐ नेतृत्व स्तर पर साइबर जोखिम और सुरक्षा पर नियमित रूप से चर्चा करें।
- ☐ सुनिश्चित करें कि साइबर सुरक्षा प्रशिक्षण शामिल सभी कर्मचारियों का हिस्सा है और संगठन की साइबर सुरक्षा नीतियों का पालन करने की सहमति के लिए सभी कर्मचारी ने दस्तावेजों पर हस्ताक्षर किया है।
- ☐ सभी कर्मचारियों के लिए आवर्ती साइबर प्रशिक्षण स्थापित करें।
- ☐ जब संगठन संभावित वेंडर् का मूल्यांकन करता है और तीसरे पक्ष के साथ डेटा साझा करता है तो सुनिश्चित करें कि साइबर सुरक्षा पर हमेशा विचार किया जाता है।
- ☐ विलय और अधिग्रहण पर विचार करते समय संगठन की साइबर सुरक्षा का आकलन एकीकृत करें।
- ☐ संगठन की साइबर सुरक्षा नीतियों की वार्षिक समीक्षा करें।
- ☐ साइबर सुरक्षा खतरों और घटनाओं के बारे में स्वैच्छिक जानकारी साझा करने के लिए तकनीकी कर्मचारियों को प्रोत्साहित करें।