बोर्ड स्तर गाइड: साइबर सुरक्षा नेतृत्व

निगरानी

संगठन के सर्वोच्च स्तर के नेतृत्व के नाते बोर्ड साइबर खतरे के अधिशासित करने के लिए सर्वोच्च जिम्मेदारी धारण करता है, इस कारण वह इस क्षेत्र में संगठन की रणनीति, नीति और गतिविधियों पर नजर रखता है। विशिष्ट रूप से बोर्ड को चाहिए कि:

- वह साइबर खतरे और लचीलेपन की अनंतिम जवाबदेही ले, चाहे वह पूर्ण बोर्ड के माध्यम से हो या बोर्ड की किसी विशिष्ट कमेटी ओवरसाइट के प्रतिनिधिमंडल के माध्यम से हो।
- वह एक कॉरपोरेट अधिकारी सामान्यतया सीआईएसओ कार्य सौंपे जो साइबर पुनर्स्थापन और साइबर पुनर्स्थापन लक्ष्य की प्रगति और साइबर पुनर्स्थापन को लेकर संगठन की क्षमता की रिपोर्टिंग के लिए जवाबदेह हो। 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।
- खतरा को बर्दाश्त करने की आपकी संगठन की क्षमता को वार्षिक आधार पर परिभाषित करे; आपकी कॉरपोरेट रणनीति और जोखिम उठाने की क्षमता के साथ अनुरूपता को सुनिश्चित करें।
- यह सुनिश्चित करें कि आपके संगठन का एक औपचारिक, स्वतंत्र साइबर पुनर्स्थापन समीक्षा वार्षिक रूप संचालित किया गया है।
- वह साइबर पुनर्स्थापन योजना का निर्माण, क्रियान्वयन, जांच और जारी बेहतरी का निरीक्षण करे और संगठन में संरेखन को सुनिश्चित करे और यह कि आपका सीआईएसओ या अन्य जवाबदेह अधिकारी नियमित रूप इस सब की रिपोर्ट बोर्ड को उपलब्ध करे।
- वह साइबर लचीलेपन और जोखिम आकलन को आपके संगठन की संपूर्ण व्यापार रणनीति, जोखिम प्रबंधन, बजट उपबंधन और संसाधन आवंटन के साथ जोड़े जिसके साथ संपूर्ण ऑपरेशनल जोखिम के साथ साइबर जोखिम को पूर्ण रूपेण शामिल करने का लक्ष्य हो। नियमित रूप से तीसरे पक्ष के जोखिमों की समीक्षा करें।
- वह उपरोक्त के संबंध में आपके प्रदर्शन को आवर्ती रूप से समीक्षा करे और सतत बेहतरी के लिए स्वतंत्र सलाह पर विचार करे।

सूचना से लैस रहना

बोर्ड द्वारा प्रभावी साइबर जोखिम निरीक्षण का कार्य विषय पर सदस्यों के नियंत्रण और अद्यतन सूचना पर निर्भर करता है।

- यह सुनिश्चित करें कि बोर्ड से जुड़ने वाले सभी व्यक्ति को साइबर खतरे से उत्पन्न जोखिम को समझने और उसके प्रबंधन का सटीक अद्यतन कौशल और ज्ञान है।
- प्रबंधन से आपके संगठन के वर्तमान और भविष्यगत जोखिम एक्सपोजर, प्रासंगिक नियामक आवश्यक-ताएं और जोखिम उठाने की क्षमता के औद्योगिक एवं सामाजिक मानदंडों के संबंध में नियमित सलाह लेते रहना। आगे, खतरे की पृष्ठभूमि और नियामक माहौल के मद्देनजर नवीनतम प्रगति के बारे में नियमित ब्रीफिंग में शामिल होना और संयुक्त योजना बनाना और श्रेष्ठ अभ्यासकर्ता साथी और साइबर सुरक्षा के नेताओं से मिलना और अधिशासन एवं रिपोर्टिंग के विषय में उच्च स्तरीय विचार आदान-प्रदान करना।
- बोर्ड की बैठकों के दौरान कार्यशील एजेंडा विषय के तौर पर प्रबंधन को साइबर जोखिम, खतरे और इवेंट के मात्रात्मक और समझने योग्य आकलन के लिए तैयार रखना।
- प्रणालीगत चुनौतियां जैसे कि आपूर्ति शृंखला समस्याएं, आम निर्भरताएं और सूचना साझाकरण में अंतराल के प्रति जागरूकता कायम रखना।

टोन को सेट करना

वरिष्ठ प्रबंधन के साथ-साथ बोर्ड आपके संगठन के केंद्रीय मूल्यों, जोखिम संस्कृति और साइबर पुनर्स्थापन के संबंध उम्मीदों को जरूर निर्धारित और संवर्धित करे।

- ऐसी संस्कृति को बढ़ावा दें जिसमें आपके संगठन के साइबर पुनर्स्थापन के कार्य हेतु कर्मी सभी स्तर पर अपनी महत्वपूर्ण जिम्मेदारियों को पहचाने। उदाहरण प्रस्तुत कर नेतृत्व करना।
- प्रबंधन की भूमिका का निरीक्षण करें जो आपके संगठन की जोखिम संस्कृति को मजबूत और बरकरार रखे। सुरक्षा पर संस्कृति के प्रभाव, मजबूती पर विचार करते हुए जोखिम संस्कृति को बढ़ावा देना उसकी निगरानी और आकलन करना एवं जहां आवश्यक हो वहां परिवर्तन करना।
- यह स्पष्ट कर दें कि आप संगठन के बाहर अथवा भीतर सभी कर्मियों से ईमानदारीपूर्वक कार्य करने और अवलोकन किए गए गैर-अनुपालन को प्रमुखता के साथ दूर करने की अपेक्षा रखते हैं।

साइबर जोखिम प्रशासन के मूल तत्व

पुष्टि करें कि आप सकारात्मक रूप में निम्नलिखित प्रश्नों के उत्तर दे सकते/सकती हैं:

1. क्या आपके संगठन ने **वैधानिक और नियामक संबंधी आवश्यकताओं को पूरा कर लिया है**?
2. क्या आपके संगठन ने **अपने साइबर एक्सपोजर की मात्रा का आकलन और वित्तीय पुनर्स्थापन की जांच कर लिया है**?
3. क्या आपके बोर्ड के पास इस बात की **कोई बेहतरी की योजना** है जिससे यह सुनिश्चित हो कि एक्सपोजर सहमत जोखिम बर्दास्त करने की क्षमता के अंदर है?
4. **संगठन के साइबर पुनर्स्थापन के संबंध में प्रबंधन के द्वारा उपलब्ध कराए गए सघन, स्पष्ट और कार्रवाई करने योग्य सूचना के बारे में क्या बोर्ड नियमित रूप से चर्चा करता है**?
5. क्या आपके बोर्ड के पास **घटना आधारित प्रत्युत्तर योजना मौजूद है जिसे हाल में बोर्ड स्तर समेत ड्राई-रन अभ्यास के द्वारा परखी गई हो**?
6. क्या साइबर खतरे के प्रबंधन के लिए जिम्मेदार महत्वपूर्ण लोगों की **भूमिका सुरक्षा तीन पंक्तियों के संबंध में** स्पष्ट और संरेखित हैं?
7. क्या आपने अपने संगठन के साइबर खतरा संरचना का **स्वतंत्र मान्यकरण और आश्वासन** प्राप्त किया है?