सीईओ स्तरीय गाइड: साइबर सुरक्षा नेतृत्व

प्रशासन

आपके संगठन की साइबर सुरक्षा प्रबंधन के शीर्ष स्तर पर शुरू और समाप्त होती है। सीईओ बोर्ड के साथ मिलकर जोखिम की समझ को जरूर बरकरार रखें और संगठन की साइबर सुरक्षा से संबंधित गतिविधियां एवं कर्मियों के प्रति अनंतिम जवाबदेही और जिम्मेदारी धारण करें। आपको चाहिए कि:

- अगर पहले से मौजूद नहीं हो तो एक मुख्य सूचना सुरक्षा अधिकारी (सीआईएसओ) की नियुक्ति करें अथवा संसाधन काफी सीमित हो तो संगठन के अंदर से ही किसी को सीआईएसओ के कार्यों के लिए नियुक्त करें।
- सीआईएसओ अथवा अन्य तकनीकी कर्मी के साथ साइबर सुरक्षा रणनीति फ्रेमवर्क की स्थापना और रखरखाव के लिए कार्य करें जो अंतरराष्ट्रीय, राष्ट्रीय और उद्योग मानदंडों एवं दिशा-निर्देशों का उपयोग करते हुए संगठन के विशिष्ट साइबर सुरक्षा की जरूरत को मुहैया कराए।
- संगठन की साइबर सुरक्षा को क्रियान्वित एवं प्रबंधन करने वाले कर्मी के सामने उसकी भूमिका और जिम्मेदारियों को स्पष्ट करें।
    - उपयुक्त साइबर सुरक्षा की भूमिका एवं सभी स्तर के कर्मियों के अधिकार एक्सेस की पहचान के लिए सीआईएसओ के साथ कार्य करें।
    - संचार और सहयोग का निरीक्षण करें ताकि यह सुनिश्चित हो सके साइबर सुरक्षा का प्रबंधन संपूर्णतया में हो रहा है, खासकर तब जब संगठन के अंदर साइबर सुरक्षा की जिम्मेदारियां एक से अधिक कर्मियों या प्रभागों (जैसे कि पृथक सूचना सुरक्षा, जोखिम और तकनीकी वर्टिकल्स का होना) के बीच साझाकृत हो।
- यह सुनिश्चित करें कि समय पर खतरे को जोड़ने के लिए आईएसओ के पास आपसे और बोर्ड से संचार के लिए स्पष्ट और सीधी लाइन हो।
- सीआईएसओ अथवा अन्य तकनीकी कर्मियों को वरिष्ठ प्रबंधन के सामने रूटीन तौर जानकारी प्रदान करने के लिए आमंत्रित करें।
- सुनिश्चित करें कि संगठन की सुरक्षा नीतियां, मानदंड, प्रवर्तन की युक्ति और प्रक्रिया सभी टीम और व्यापार की रेखाओं के आर-पार एक समान है।

जोखिम का आकलन और प्रबंधन

मजबूत साइबर सुरक्षा जागरूकता और तैयारी की मौजूदगी सतत जोखिम आधारित विश्लेषण पर निर्भर करता है। अपने संगठन की साइबर सुरक्षा को बेहतर करने के लिए:

- अपने संगठन के व्यापक जोखिम प्रबंधन और अधिशासन प्रक्रियाओं के अंदर साइबर सुरक्षा जोखिम आकलन और प्रबंधन को प्राथमिकता के रूप में स्थापित करें। अपने सीआईएसओ अथवा अन्य तकनीकी कर्मी के साथ एक ऐसा जोखिम आकलन योजना का संचालन करें जिसमें निम्न शामिल हो:
    - 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 दुर 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
    - तीसरे पक्ष की पेनेट्रेशन-टेस्टिंग अथवा रेड-टीमिंग के उपयोग पर विचार करना,
    - सुरक्षात्मक उपायों पर विचार करें जैसे साइबर बीमा खरीदना।
- संस्थान भर से सामयिक प्रत्युत्तर प्राप्त हो इसकी व्यवस्थापना के लिए जोखिम आकलन प्रक्रिया के दौरान कर्मी के प्रयास का नेतृत्व करें।
- महत्वपूर्ण हितधारकों और बोर्ड समेत निरीक्षण एग्जिक्युटिव के लिए जोखिम आकलन का विश्लेषण करें और उनके सामने प्रस्तुत करें।
- आपके संगठन के इच्छित साइबर सुरक्षा तैयारी को बरकरार रखने या इसे बढ़ाने के लिए यथोचित बजट प्रबंध समेत अन्य किसी बदलाव का निरीक्षण करें जो इस बात को सुनिश्चित करता हो कि साइबर सुरक्षा के लिए उठाया गया कोई कदम जोखिम के मद्देनजर तर्कसंगत है या नहीं और आपके संगठन के लिए वहन करने योग्य है अथवा नहीं।
- उभरते साइबर जोखिम की समस्या से निपटने हेतु चल रहे निगरानी कार्य का प्रदर्शन तेज और स्फूर्त बना रहे इसका निरीक्षण करना।

सांगठनिक संस्कृति

आपके संगठन की साइबर सुरक्षा कोई एक बार की प्रक्रिया या कुछेक कर्मियों का कार्य नहीं है; यह हर व्यापार फैसले और ऑपरेशन का एक कारक है और एक अभ्यास है जिसका पालन हर कर्मी को आवश्यक रूप से करना होता है। आपके संगठन के अंदर सतत संपूर्ण साइबर सुरक्षा को प्रोत्साहन देने हेतु:

- टीम नेतृत्व के साथ साइबर सुरक्षा पर चर्चा आरंभ करें और नियमित रूप से साइबर जोखिम का प्रबंधन करने वाले कर्मी के साथ संचार करें।
- साइबर सुरक्षा प्रशिक्षण को सभी कर्मियों के लिए आनबोर्डिंग होने के एक हिस्सा के रूप शामिल करें जो इस बात को सुनिश्चित करे कि सभी कर्मी अद्यतन हैं और उन्होंने आपके संगठन की साइबर सुरक्षा नीतियों के समर्पित रहने के दस्तावेजों पर हस्ताक्षर कर दिया है और यह भी कि आपका आईटी विभाग या अन्य तकनीकी कर्मी ने उन्हें श्रेष्ठ कार्य अभ्यास के बारे में बता दिया है।
- संस्थान सभी कर्मियों को लघु और दीर्घकालीन सुरक्षा जिम्मेदारियों से अवगत कराने के लिए बारम्बार साइबर सुरक्षा प्रशिक्षण आयोजित करे।
- यह सुनिश्चित करें कि जब आपका संगठन संभावनाशील वेंडर का मूल्यांकन करता हो और तीसरे पक्ष के साथ डेटा साझा करता हो तो ऐसे मौकों पर हमेशा साइबर सुरक्षा पर विचार किया जाए।
- जब विलय या अधिग्रहण की बात हो तो संगठन की साइबर सुरक्षा के आकलन को इसमें शामिल करें।
- अपने संगठन की साइबर सुरक्षा नीतियों का वार्षिक रूप से समीक्षा करें।
- अपने संगठन के भीतर और भरोसामंद प्रतिस्पर्धी के साथ साइबर सुरक्षा के खतरे को लेकर स्वैच्छिक सूचना साझाकरण को बढ़ावा दें।
- सुरक्षा मसलों और आउटसेट से योजना निर्माण को शामिल करने वाले इनोवेशन को प्रोत्साहित करें।