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।

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।

छोटे संगठनों के लिएसाइबर सुरक्षा

सीआईएसओ चेकलिस्ट: अपने संगठन की सुरक्षा करना

जोखिम-आधारित सूचना सुरक्षा कार्यक्रम विकसित करना

- ☐ **सभी प्रकार की जानकारी को पहचानें और सूची बनाएं जिसे आपका व्यवसाय संग्रहित और उपयोग करता है (जैसे ग्राहक का नाम और ईमेल)।**
- ☐ **प्रत्येक प्रकार की जानकारी के लिए पूछें और उत्तर रिकॉर्ड करें:**
  - यदि यह जानकारी सार्वजनिक कर दी जाती तो क्या होगा?
  - यदि यह जानकारी गलत हो, तो मेरे व्यवसाय का क्या होगा?
  - यदि मैं/मेरे ग्राहक इस जानकारी तक नहीं पहुँच सकते तो मेरे व्यवसाय का क्या होगा?
- ☐ **रिकार्ड करें कि आपके द्वारा पहचानी गई जानकारी के संपर्क में कौन सी तकनीक आती है। इसमें हार्डवेयर (जैसे कंप्यूटर) और सॉफ़्टवेयर एप्लिकेशन (जैसे ब्राउज़र ईमेल) शामिल हो सकते हैं।**
  - जहां लागू हो, अपने व्यवसाय के बाहर की प्रद्योगिकियों (जैसे"क्लाउड") और किन्हीं लागू सुरक्षा तकनीकों, जैसे फायरवॉल को शामिल करें।
  - उन तकनीकों को शामिल करें, जिनका उपयोग घर से काम करने की स्थिति में उपयोग किया जा सकता है।
  - मेक, मॉडल, सीरियल नंबर और अन्य पहचानकर्ता शामिल करें।
  - निगरानी करें कि प्रत्येक उत्पाद कहां है। सॉफ़्टवेयर के लिए, पहचानें कि कौन सी मशीन(मशीनों) पर सॉफ़्टवेयर लोड किया गया है।
- ☐ **अपने राष्ट्रीय सीईआरटी, एफएस-आईएसएसी, आपके स्थानीय इंफ्रागार्ड चैप्टर और अन्य से नियमित रूप से जानकारी की समीक्षा करें कि वित्तीय क्षेत्र किन खतरों और कमजोरियों का सामना कर सकता है और इसका अनुमान लगाएं कि आप कितना प्रभावित हो सकते हैं।**
- ☐ **महीने में कम से कम एक बार अतिसंवेदनशीलता स्कैन या विश्लेषण करें।**
- ☐ **अपने संगठन के लिए एक साइबर सुरक्षा नीति बनाएं, जिसमें 'घर से काम करने' का प्रोटोकॉल शामिल हो।**
- ☐ **सभी कर्मचारियों को नीति के विवरण पर प्रशिक्षित करें और उनसे दस्तावेज़ों पर हस्ताक्षर कराएं जो नीति का पालन करके आपके संगठन की साइबर सुरक्षा को बनाए रखने में उनकी भूमिका को स्वीकार करता है।**
- ☐ **आंतरिक खतरों के विरूद्ध एक सुरक्षा योजना बनाएं, जिसमें उद्योग-जोखिम मूल्यांकन और अभिगम नियंत्रण प्रबंधन शामिल हो।**

मैलवेयर से नुकसान को रोकना

- ☐ **अपने फ़ायरवॉल को सक्रिय करें और एक्सेस कंट्रोल सूची (एलसीएलएस) सेट करें। व्हाइटलिस्टिंग सेटिंग का उपयोग करके पहुंच को प्रतिबंधित करें।**
- ☐ **सभी कंप्यूटर और लैपटॉप पर एंटीवायरस सॉफ़्टवेयर और एंटीस्पाइवेयर का उपयोग करें।**
  - ☐ सुनिश्चित करें कि सुरक्षा उपकरण "घर से काम करने' के वातावरण में प्रभावी ढंग से काम कर सकते हैं।
- ☐ **निर्माताओं और वेंडर्स द्वारा प्रदान किए गए नवीनतम सॉफ़्टवेयर अपडेट लागू करें। जहां उपलब्ध है वहां 'स्वतः अपडेट'।**
- ☐ **एडमिन अधिकारों के साथ आईटी कर्मचारियों के लिए नए प्रोग्रामों की स्थापना को प्रतिबंधित करें।**
- ☐ **सुरक्षा/पहचान हार्डवेयर या सॉफ्टवेयर द्वारा उत्पन्न गतिविधि लॉग को बनाए रखें और निगरानी करें। पासवर्ड सुरक्षा और एन्क्रिप्शन के साथ लॉग को सुरक्षित रखें।**
- ☐ **सुनिश्चित करें कि सभी होस्ट क्लॉक्स सिंक्रनाइज़ हैं।**
- ☐ **एसडी कार्ड और यूएसबी स्टिक जैसे रिमूवेबल मीडिया तक पहुंच को नियंत्रित करें। इसके बजाय कर्मचारियों को ईमेल या क्लाउड स्टोरेज के माध्यम से फ़ाइलों को स्थानांतरित करने के लिए प्रोत्साहित करें। बाहरी स्रोतों से यूएसबी का उपयोग करने या अपनी यूएसबी को दूसरों को देने के जोखिम पर कर्मचारियों को शिक्षित करें।**
- ☐ **अपनी ईमेल सेवाओं पर ईमेल सुरक्षा और स्पैम फ़िल्टर सेट अप करें।**

- ☐ **एन्क्रिप्शन और अन्य उपलब्ध उपकरणों के साथ अपनी सार्वजनिक उपयोग वाली वेबसाइटों पर सभी पेजों को सुरक्षित करें।**
- ☐ **अपने संगठन की संपत्ति और प्रणालियों का मूल्यांकन करने के लिए एक पेनीट्रेसन टेस्टिंग सेवा को हायर करने रखने पर विचार करें।**

कर्मचारियों का प्रशिक्षण

- ☐ **सभी नए कर्मचारियों को ऑनबोर्डिंग करने के दौरान और वर्तमान कर्मचारियों के लिए साल में कम से कम एक बार नियमित अंतराल पर अनिवार्य साइबर सुरक्षा प्रशिक्षण चलाने की योजना बनाएं। कर्मचारियों से आवश्यकता:**
  - सभी पेशेवर उपकरणों और खातों पर शक्तिशाली पासवर्ड का उपयोग करें और उन्हें व्यक्तिगत उपकरणों के लिए भी ऐसा करने और एक पासवर्ड मैनेजर का उपयोग करने के लिए प्रोत्साहित करें,
  - एट होम आईटी इन्फ्रास्ट्रक्चर सहित सभी उपकरणों पर ऑपरेटिंग सिस्टम, सॉफ्टवेयर और एप्लिकेशन अप टू डेट रखें,
  - सभी खातों पर दो-कारक वाला प्रमाणीकरण उपयोग करें,
  - खाते का विवरण और एक्सेस कार्ड्स को सुरक्षित रखें और उपयोग में ना होने पर उपकरणों को लॉक करें,
  - अनएन्क्रिप्टेड ईमेल या अन्य खुले संचार के माध्यम से खाते के विवरण या अन्य संवेदनशील डेटा को साझा करने से बचें,
  - अटैचमेंट को तुरंत खोलने या या अनापेक्षित या संदिग्ध ईमेल में लिंक को खोलने से बचें,
  - व्यक्तिगत जानकारी प्रदान करने से पहले एक संदिग्ध दिखने वाले ईमेल या एक पॉप-अप बॉक्स की वैधता की पुष्टि करें, और ईमेल अड्रेस पर पूरा ध्यान दें, और
  - अपने संगठन के तकनीकी कर्मियों और/या उच्च प्रबंधन को किसी भी संभावित आंतरिक या बाहरी सुरक्षा घटनाओं, खतरों, या डेटा या उपकरणों से छेड़छाड़ की सूचना दें।
- ☐ **नकली खातों से फ़िशिंग स्टाइल के ईमेल भेजने जैसे मिथ्याभास के माध्यम से कर्मचारी जागरूकता की नियमित परीक्षण करें। किसी भी कर्मचारी की असफलताओं का आकलन करें और उन्हें सीखने और सुधार के अवसरों के रूप में उपयोग करें।**

अपने डेटा की सुरक्षा करना

- ☐ **अपने महत्वपूर्ण डेटा (जैसे दस्तावेज़, ईमेल, कैलेंडर) का नियमित बैकअप लें और परीक्षण करें कि उन्हें पुनर्स्थापित किया जा सकता है। क्लाउड पर बैकिंग अप करने पर विचार करें।**
- ☐ **सुनिश्चित करें कि आपके बैकअप वाले डिवाइस को मूल प्रतिलिपि वाली डिवाइस से स्थायी रूप से कनेक्ट नहीं किया गया है, न तो भौतिक रूप से और न ही स्थानीय नेटवर्क पर।**
- ☐ **सर्ज प्रोटेक्टर इंस्टॉल करें, जनरेटर का उपयोग करें, और सुनिश्चित करें कि आपके सभी कंप्यूटर और महत्वपूर्ण नेटवर्क उपकरण निर्बाध विद्युत आपूर्ति में प्लग किए गए हैं।**
- ☐ **मोबाइल डिवाइस प्रबंधन (एमडीएम) समाधान का उपयोग करें।**

अपने उपकरण को सुरक्षित रखें

- ☐ **मोबाइल उपकरणों के लिए पिन या पासवर्ड सुरक्षा को चालू करें। उपकरणों को कॉन्फ़िगर करें ताकि खो जाने या चोरी होने पर उन्हें ट्रैक किया जा सके, दूर से मिटाया या बंद किया जा सके।**
- ☐ **यदि उपलब्ध हो तो 'स्वचालित अपडेट' का उपयोग करके, अपने उपकरणों (सभी इंस्टॉल्ड ऐप्स) को अप टू डेट रखें।**
- ☐ **संवेदनशील डेटा भेजते समय, सार्वजनिक वाई-फाई हॉटस्पॉट से कनेक्ट न करें - सेलुलर कनेक्शन (टेथरिंग और वायरलेस डोंगल सहित) का उपयोग करें या वीपीएन का उपयोग करें।**
- ☐ **उन उपकरणों को अप-टू-डेट विकल्पों से बदलें जो अब निर्माताओं द्वारा समर्थित नहीं हैं।**
- ☐ **खोए हुए या चोरी हुए उपकरणों के लिए रिपोर्टिंग प्रक्रियाएं सेट करें।**

पासवर्ड का उपयोग करते हुए

- ☐ **सुनिश्चित करें कि सभी कंप्यूटर एन्क्रिप्शन उत्पादों का उपयोग करते हैं जिन्हें बूट करने के लिए पासवर्ड की आवश्यकता होती है। मोबाइल उपकरणों के लिए पासवर्ड या पिन सुरक्षा पर स्विच करें।**
- ☐ **शक्तिशाली पासवर्ड का उपयोग करें, अनुमान लगाने योग्य पासवर्ड (जैसे passw0rd) और व्यक्तिगत पहचानकर्ता(जैसे परिवार और पालतू जानवर का नाम) से बचें। सभी कर्मचारियों को ऐसा करने का निर्देश दें।**

- ☐ जहाँ भी संभव हो दो-कारक वाले प्रमाणीकरण (2एफए) का उपयोग करें।
- ☐ स्टाफ को दिये जाने से पहले, नेटवर्क और आईओटी डिवाइस सहित सभी उपकरणों पर निर्माता द्वारा जारी किए गए डिफ़ॉल्ट पासवर्ड बदल दें।
- ☐ सुनिश्चित करें कि कर्मचारी अपने स्वयं के पासवर्ड को आसानी से रीसेट कर सकते हैं। यह यह भी चाह सकते हैं कि कर्मचारी नियमित अंतराल(जैसे तिमाही, छमाही, या सालाना) पर अपने पासवर्ड बदलें।
- ☐ पासवर्ड मैनेजर का उपयोग करने पर विचार करें। यदि आप एक का उपयोग करते हैं, तो सुनिश्चित करें कि मास्टर पासवर्ड (जो आपके सभी अन्य पासवर्ड तक पहुंच प्रदान करता है) शक्तिशाली है।

अनुमतियों को नियंत्रित करना

- ☐ सुनिश्चित करें कि सभी कर्मचारियों के पास विशिष्ट पहचान वाले खाते हैं जिनको हर बार प्रमाणित किया जाता है जब जो आपके सिस्टम का उपयोग करते हैं।
- ☐ केवल विश्वसनीय आईटी कर्मचारियों और प्रमुख कर्मचारियों को प्रशासनिक विशेषाधिकार दें और मानक उपयोगकर्ताओं के लिए कार्यस्थलों पर एडमिनिस्ट्रेटर विशेषाधिकार वापस लें।
- ☐ कर्मचारियों को केवल उन विशिष्ट डेटा प्रणालियों तक पहुंच प्रदान करें, जिनकी उन्हें अपनी नौकरियों के लिए आवश्यकता है और यह सुनिश्चित करें कि वे बिना अनुमति के कोई भी सॉफ़्टवेयर इंस्टॉल ना कर सकें।
- ☐ अपने संगठन के कंप्यूटर पर प्रत्येक कर्मचारी के लिए उपयोगकर्ता खाते बनाएं।
- ☐ दूरस्थ रूप से काम करने वाले कर्मचारियों और एडमिनिस्ट्रेटर्स के लिए स्पष्ट एक्सेस विकल्पों को परिभाषित करें।

अपने वाई-फाई को सुरक्षित करना

- ☐ सुनिश्चित करें कि आपका कार्यस्थल का वाई-फाई सुरक्षित है और डब्ल्यूपीए2 के साथ एन्क्रिप्टेड है। राउटर अक्सर एन्क्रिप्शन बंद होने के साथ आते हैं, इसलिए इसे ऑन करना सुनिश्चित करें। पासवर्ड राउटर के एक्सेस की सुरक्षा करता है, और सुनिश्चित करें कि पासवर्ड पूर्व-निर्धारित डिफ़ॉल्ट से अपडेट किया गया है। किसी भी "दूरस्थ प्रबंधन" विशेषता को बंद करें।
- ☐ केवल कुछ मीडिया एक्सेस कंट्रोल अड्रेस वाले उपकरणों की अनुमति देकर अपने वाई-फाई नेटवर्क के एक्सेस को सीमित करें। यदि ग्राहकों को वाई-फाई की आवश्यकता है, तो एक अलग सार्वजनिक नेटवर्क इंस्टॉल करें।
- ☐ अपने नेटवर्क पर मौजूद सभी उपकरणों की आसान ट्रैकिंग के लिए अपने नेटवर्किंग उपकरणों पर डायनामिक होस्ट कॉन्फ़िगरेशन प्रोटोकॉल (डीएचसीपी) लॉगिंग सक्षम करें।
- ☐ राउटर सेट करने के बाद एडमिनिस्ट्रेटर के रूप में लॉग आउट करें।
- ☐ अपने राउटर के सॉफ़्टवेयर को अपडेट रखें। निर्माता के साथ अपना राउटर पंजीकृत करें और अपडेट प्राप्त करने के लिए साइन अप करें।

फ़िशिंग हमले से बचें

- ☐ सुनिश्चित करें कि कर्मचारी वेब पर ब्राउज़ न नहीं करते हैं या सर्वर पर या एडमिनिस्ट्रेट विशेषाधिकारों के साथ ईमेल नहीं चेक करते हैं।
- ☐ वेब और ईमेल फ़िल्टर सेट करें। कर्मचारियों को आमतौर पर साइबर सुरक्षा खतरों से जुड़ी वेबसाइटों पर जाने से प्रतिबंधित करने पर विचार करें।
- ☐ कर्मचारियों को फ़िशिंग के स्पष्ट संकेतों की जाँच करना सिखाएं, जैसे खराब वर्तनी और व्याकरण, या पहचानने योग्य लोगो के निम्न-गुणवत्ता वाले संस्करण। क्या प्रेषक का ईमेल अड्रेस वैध लगता है?
- ☐ यदि आपको शंका होती है एक हमला हुआ है तो मैलवेयर के लिए स्कैन करें और जितनी जल्दी हो सके पासवर्ड बदलें। यदि स्टाफ फ़िशिंग हमले का शिकार हो जाता है तो कर्मचारी को दंडित ना करें (यह भविष्य में लोगों को रिपोर्टिंग से हतोत्साहित करता है)।

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE

CarnegieEndowment.org

THE WORLD BANK IBRD • IDA | WORLD BANK GROUP
SWIFT INSTITUTE
FS-ISAC
Standard Chartered
CYBER READINESS INSTITUTE
GLOBAL CYBER ALLIANCE
ICBA Independent Community Bankers of America

छोटे संगठनों के लिएसाइबर सुरक्षा

सीआईएसओ चेकलिस्ट: आपके ग्राहकों की सुरक्षा करना

व्यक्तिगत स्तर की डेटा की सुरक्षा पर ग्राहकों और कर्मचारियों को सुझाव देना

☐ **उनके डेटा की बेहतर सुरक्षा के लिए कर्मचारियों और ग्राहकों को पालन करने के लिए निम्नलिखित व्यक्तिगत दिशानिर्देशों प्रदान करें:**

- सभी व्यक्तिगत और व्यावसायिक उपकरणों पर शक्तिशाली पासवर्ड का उपयोग करें और पासवर्ड मैनेजर का उपयोग करने पर विचार करें।
- सभी कंप्यूटर और मोबाइल उपकरणों पर ऑपरेटिंग सिस्टम और अन्य सॉफ्टवेयर और एप्लिकेशन को अप टू डेट रखें।
- एंटी-वायरस, एंटी-मालवेयर और एंटी-रैंसमवेयर सॉफ़्टवेयर इंस्टॉल करें जो दुर्भावनापूर्ण प्रोग्राम को रोकता है, उनका पता लगाता है और हटाता है।
- अपने कंप्यूटर पर अनधिकृत पहुँच को रोकने के लिए फायरवॉल प्रोग्राम का उपयोग करें।
- केवल प्रतिष्ठित कंपनियों के सिक्योरिटी प्रोडक्ट का उपयोग करें। कंप्यूटर और उपभोक्ता प्रकाशनों से समीक्षाओं को पढ़ें और अपने कंप्यूटर या ऑपरेटिंग सिस्टम निर्माता के साथ परामर्श करने पर विचार करें।
- संवदेनशील जानकारी के प्रति सावधान रहें। अनएन्क्रिप्टेड ईमेल पर बैंक खाते का पासवर्ड या अन्य संवेदनशील वित्तीय अकाउंट डेटा न भेजें।
- इस बारे में स्मार्ट बनें कि संवेदनशील व्यक्तिगत जानकारी वाले बैंकिंग या अन्य संचार के लिए आप इंटरनेट से कहां और कैसे कनेक्ट होते हैं।
- ईमेल अटैचमेंट को तुरंत न खोलें या अनचाहे या संदिग्ध दिखने वाले ईमेल में लिंक पर क्लिक ना करें। रुकें। सोचें। क्लिक करें।
- यदि कोई व्यक्ति आपसे ऑनलाइन या टेलफोन से अनपेक्षित रूप से संपर्क करता है और आपकी व्यक्तिगत जानकारी मांगता है तो संदेह करें। यहां तक कि जब परिचित पतों के साथ संपर्क करते हैं, तो भी ईमेल के माध्यम से व्यक्तिगत जानकारी को कम से कम साझा करने का प्रयास करें।
- याद रखें कि कोई भी वित्तीय संस्थान आपको ईमेल या कॉल नहीं करेगा और गोपनीय जानकारी का अनुरोध नहीं करेगा जो आपके बारे में उसके पास पहले से मौजूद है।
- मान लें कि आपने जिस बैंक में कभी खाता नहीं खोला है, उससे जानकारी के लिए अनुरोध एक धोखाधड़ी है।
- व्यक्तिगत जानकारी प्रदान करने से पहले एक संदिग्ध दिखने वाले ईमेल या पॉप-अप बॉक्स की वैधता की पुष्टि करें। ईमेल पते पर सावधानी से ध्यान दें।

खातों का प्रबंध

☐ **यह आवश्यक है कि ग्राहक आपकी सेवाओं में लॉग इन करने के लिए शक्तिशाली आईडी और पासवर्ड का उपयोग करें। उन्हें सलाह दें कि वे उसी पासवर्ड का उपयोग न करें जिसका वे अन्य खातों के लिए उपयोग करते हैं।**

☐ **वास्तविक ग्राहकों को प्रमाणित करने और धोखाधड़ी के अवसर को कम करने के लिए तत्काल सत्यापन, वास्तविक समय के सत्यापन, परीक्षण जमा सत्यापन, पहचान सत्यापन, और/ या आउट ऑफ वॉलेट प्रश्नों का उपयोग करें।**

☐ **अपनी सेवाओं में लॉग इन करते समय ग्राहकों के लिए ऑफ़र या आदर्श रूप से, दो-कारक के प्रमाणीकरण की आवश्यकता होती है।**

☐ **धोखाधड़ी के संकेतों के लिए उपयोगकर्ता खातों की नियमित जांच करें।**

डेटा की सुरक्षा करना

☐ **इस बात पर विचार करें कि आपकी सेवाओं को करने के लिए आपके संगठन को कौन सा ग्राहक डेटा एकत्र करना चाहिए, और उससे आगे जाने वाले किसी भी ग्राहक डेटा को इकट्ठा करने से सावधान रहना चाहिए।**

☐ **डेटा बनाए रखने वाली नीतियों को स्थापित करें और वितरित करें। जब जरूरत ना हो तो ग्राहक के डेटा को नष्ट कर दें।**

☐ **पारगमन और स्थायी ग्राहक डेटा को एन्क्रिप्ट करें।**

☐ **यह स्पष्ट करने के लिए डेटा सुरक्षा नीतियों को लागू करें कि डेटा ट्रांसफर के कौन से तरीकों को मंजूर बनाम प्रतिबंधित किया गया है या उल्लेख करें कि जब ग्राहक डेटा से निपटने की बात आती है तो सभी कर्मचारियों के लिए क्या स्वीकार्य है। सुनिश्चित करें कि इन नीतियों को दस्तावेजीकृत किया गया है, सभी कर्मचारियों को बताया गया, लागू किया गया है, और समय-समय पर समीक्षा और अपडेट किया जाता है।**

सार्वजनिक वेब एप्लीकेशंस को सुरक्षित करना

- ☐ अपने संगठन के सार्वजनिक उपयोग वाले वेब एप्लिकेशन(एप्लिकेशनों) पर HTTPS लागू करें और सभी HTTP ट्रैफ़िक को HTTPS में पुनर्निर्देशित करें।
- ☐ अपनी वेबसाइट(वेबसाइटों) पर सामग्री सुरक्षा नीति का उपयोग करें।
- ☐ अपनी वेबसाइट(वेबसाइटों) पर पब्लिक की पिनिंग सक्षम करें।
- ☐ सुनिश्चित करें कि आपका सार्वजनिक उपोग वाला वेब एप्लिकेशन (एप्लिकेशंस) कभी भी ग्राहक की अत्यधिक संवेदनशील या महत्वपूर्ण जानकारी (जैसे पासवर्ड) को संग्रहीत करने के लिए कुकीज़ का उपयोग नहीं करता है और कि कुकीज़ के लिए उनकी सतर्क समाप्ति की तारीखें हैं (जितनी जल्दी हो सके)।
- ☐ उस जानकारी को एन्क्रिप्ट करने पर विचार करें जो आपके द्वारा उपयोग की जाने वाली कुकीज़ में संग्रहीत है।
- ☐ वर्ष में कम से कम एक बार अपने सार्वजनिक-उपयोग वाले वेब एप्लिकेशन (एप्लिकेशनों) की सुरक्षा का आकलन करने के लिए एक पेनीट्रेशन टेस्टिंग सर्विस को हायर करने पर विचार करें।

कर्मचारियों को प्रशिक्षित करना

- ☐ ऐसी मानवीय त्रुटि को कम करने के लिए अपने कर्मचारियों की जवाबदेही और रणनीति सिखाएं जो ग्राहक के डेटा को उजागर कर सकती है। इसका मतलब है कि उन्हें निम्नलिखित के लिए सुझाव दें:
  - ग्राहक डेटा तक उनकी पहुँच और संचार को वहां तक सीमित करें, जितना उनके कार्य को करने के लिए आवश्यक है,
  - शक्तिशाली पासवर्ड का उपयोग करके, दो कारकों वाले प्रमाणीकरण को सक्षम करके, सॉफ्टवेयर को अपडेट रखकर, और संदिग्ध लिंक पर क्लिक न करके उन सभी डिवाइसों और खातों पर शक्तिशाली सुरक्षा व्यवहार बनाए रखें जो ग्राहक के डेटा के साथ डील करते हैं, और
  - किसी भी संभावित आंतरिक या बाहरी सुरक्षा घटनाओं, खतरों या ग्राहक डेटा से छेड़छाड़ की सूचना अपने संगठन के तकनीकी कर्मचारियों और/ या उच्च प्रबंधन को दें।
- ☐ सुनिश्चित करें कि आपके कर्मचारी आपके संगठन के डेटा की सुरक्षा और अपने कर्मचारियों को समझते हैं और उसका पालन करने के लिए दस्तावेजों पर हस्ताक्षर किए हैं।

ग्राहकों को सूचित करना

- ☐ जब ग्राहक डेटा के उल्लंघनों को संभालने की बात आती है तो यह सुनिश्चित करने के लिए कि जब घटनाएं घटती हैं, तो आप उसका अनुपालन करने के लिए तैयार हैं, आप अपने संगठन के विनियामक वातावरण के बारे में जागरूकता का निर्माण करें।
- ☐ जब आपके संगठन को ग्राहक की संवेदनशील जानकारी तक अनधिकृत पहुंच की घटना के बारे में पता चलता है तो, तो इस संभावना की तुरंत जांच कर लें कि जानकारी का दुरुपयोग हुआ है या नहीं। अधिसूचना की सर्वोत्तम प्रथाओं का पालन करें और प्रभावित ग्राहक(ग्राहकों) को जल्द से जल्द सूचित करें:
  - घटना और जानकारी का सामान्य विवरण जिसका उल्लंघन हुआ था;
  - अधिक जानकारी और सहायता के लिए एक टेलीफोन नंबर;
  - अगले 12 से 24 महीनों में "सतर्क रहने के लिए" एक अनुस्मारक;
  - एक सिफारिश कि संदिग्ध पहचान की चोरी की घटनाओं को तुरंत सूचित किया जाए;
  - वित्तीय संस्था द्वारा जानकारी तक आगे अनधिकृत पहुंच या उपयोग से बचाने के लिए उठाए गए कदमों का एक सामान्य विवरण;
  - क्रेडिट रिपोर्टिंग एजेंसियों के लिए संपर्क जानकारी; और
  - आपके संगठन को जिन नियमों का पालन करना चाहिए, उनके लिए अन्य आवश्यक जानकारी।

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE

CarnegieEndowment.org

THE WORLD BANK IBRD • IDA | WORLD BANK GROUP
SWIFT INSTITUTE
FS-ISAC
Standard Chartered
CYBER READINESS INSTITUTE
GLOBAL CYBER ALLIANCE
ICBA Independent Community Bankers of America®

छोटे संगठनों के लिए साइबर सुरक्षा

सीआईएसओ चेकलिस्ट: तीसरे पक्ष से कनेक्शन की सुरक्षा करना

साइबर सुरक्षा को दिमाग में रखते हुए वेंडर चुनना

हर बार जब आप संभावित वेंडर का मूल्यांकन कर रहे हो तो निम्नलिखित प्रश्नों की जांच करें:

- ☐ उन्हें आपके संगठन की तरह ग्राहकों की सेवा करने का क्या अनुभव है?
- ☐ क्या उन्होंने ज्ञात साइबर सुरक्षा मानकों (जैसे NIST फ्रेमवर्क या आईएसओ 27001, या क्या वे एक एसओसी2 रिपोर्ट प्रदान कर सकते हैं) के साथ उनके अनुपालन का दस्तावेजीकरण किया है?
- ☐ उन्हें उनकी सेवाओं को देने के लिए आपके कौन से डेटा और/या परिसंपत्तियों के उपयोग करने की आवश्यकता होगी, और क्या वे किसी भी बिल्कुल अनावश्यक एक्सेस का अनुरोध कर रहे हैं?
- ☐ वे आपके संगठन की उन परिसंपत्तियों और डेटा की रक्षा करने की योजना कैसे बनाते हैं जो उनके अधिकार में हैं?
- ☐ वे अपने खुद के तीसरे पक्ष के साइबर जोखिम का प्रबंधन कैसे करते हैं, और क्या वे अपनी आपूर्ति श्रृंखला सुरक्षा के बारे में जानकारी प्रदान कर सकते हैं?
- ☐ यदि कोई घटना आपके संगठन को प्रभावित कर रही है तो आपदा से बहाली और व्यापार की निरंतरता के लिए उनकी क्या योजना है?
- ☐ वे आपके संगठन के भीतर के रुझानों, खतरों और परिवर्तनों का संचार करने के संदर्भ में आपके संगठन को कैसे अपडेट रखेंगे?

तीसरे पक्ष के द्वारा जोखिम को पहचानें

निम्नलिखित कदमों को शामिल करते हुए एक तीसरे पक्ष का साइबर जोखिम मूल्यांकन करें:

- ☐ सभी वेंडर संबंधों और परिसंपत्तियों और प्रत्येक में उजागर होने वाले डेटा की एक सूची बनाएं और लगातार अपडेट करें।
- ☐ उस डेटा की समीक्षा करें जिसकी प्रत्येक वेंडर या तीसरे पक्ष तक पहुंच है, ताकि सुनिश्चित किया जा सके कि पहुंच का प्रत्येक स्तर 'न्यूनतम विशेषाधिकार' के सिद्धांत का पालन करता है।
- ☐ उस प्रभाव के आधार पर अपने वेंडर्स और तीसरे पक्ष के संबंधों (निम्न, मध्यम, उच्च) को रैंक करें जो उनके सिस्टम के उल्लंघन के कारण आपके संगठन पर होगा।
- ☐ उच्चतम जोखिम वाले वेंडर्स के साथ शुरू करते हुए, प्रत्येक प्रदाता की साइबर सुरक्षा क्षमताओं और उपयुक्त मानकों के अनुपालन का मूल्यांकन करें।
- ☐ नियमित सुरक्षा मूल्यांकन के लिए एक योजना बनाएं, यह ध्यान में रखते हुए कि आप कभी-कभी सबसे अधिक जोखिम वाले और/या ग्राहक डेटा तक सबसे अधिक पहुंच वाले वेंडर्स के ऑन-साइट मूल्यांकन करना चाह सकते हैं।

तीसरे पक्ष की सुरक्षा को प्रबंधित करना

- ☐ सम्यक उद्यम के माध्यम से करें। वेंडरों के साथ प्रस्तावों, अनुबंधों, व्यापार निरंतरता, घटना की प्रतिक्रिया और सेवा स्तर के समझौतों के लिए सभी अनुरोधों में साइबर सुरक्षा की अपेक्षाएँ स्थापित करें। साइबर घटना के मामले में जिम्मेदारियों और उत्तरदायित्वों पर सहमति हों।
- ☐ वित्तीय संगठनों और अन्य संस्थाओं की साइबर सुरक्षा व्यवहार के बारे में पूछताछ करें, जिनके साथ आप लेनदेन करते हैं या डेटा साझा करते हैं, यह ध्यान में रखें कि आपके वेंडर और तीसरे पक्ष को किसी भी साइबर सुरक्षा आवश्यकताओं का पालन करना चाहिए जिसे आपके संगठन को पूरा करना चाहिए।

- ☐ साइबर सुरक्षा मानकों के साथ आपके वेंडर्स के अनुपालन की निगरानी करने के स्थापित और सहमत उपायों का उपयोग करें।
- ☐ यह देखने के लिए अपने वेंडर्स के साथ जांच करें जो संवेदनशील डेटा को संभालते हैं कि क्या वे आपके साथ उनके किसी भी खाते के लिए दो-कारक प्रमाणीकरण, एन्क्रिप्शन या अन्य सुरक्षा उपाय ऑफर करते हैं।
- ☐ सुनिश्चित करें कि आपके द्वारा इंस्टॉल किए गए सभी तीसरे पक्ष के सॉफ़्टवेयर और हार्डवेयर में एक सुरक्षा हैंडशेक है ताकि बूटिंग प्रक्रिया प्रमाणीकरण कोड के माध्यम से सुरक्षित हो और कोड मान्यता प्राप्त नहीं होने पर निष्पादित नहीं होगा।
- ☐ यदि आप ऐसे वेंडर उत्पादों का सामना करते हैं जो या तो नकली हैं या विनिर्देशों से मेल नहीं खाते हैं, तो एक प्रस्ताव पर बातचीत करने के लिए काम करें या एक बाहर निकलने की रणनीति बनाएं।
- ☐ वेंडर अनुबंधों का वार्षिक मूल्यांकन करें और सुनिश्चित करें कि वे आपके रणनीतिक दिशा-निर्देश और नियामक डेटा सुरक्षा आवश्यकताओं को निरंतर पूरा करते हैं। अनुबंध समाप्त होने पर, आपने परिसंपतियों या डेटा वापस पाने के बारे में नियम को शामिल करें और पुष्टि करें कि वेंडर के पक्ष पर परिसंपत्ति या डेटा पूरी तरह से मिट दिये गए हैं, और आपके सिस्टम या सर्वर तक किसी भी पहुंच को अक्षम कर दिया गया है।

जानकारी साझा करना

- ☐ सुनिश्चित करें कि आपके पास अपने संगठन के वेंडर और समकक्षों के साथ सुरक्षा कि मुद्दों के बारे में संचार करने के लिए स्पष्ट संचार चैनल और संपर्क के बिंदु हैं।
- ☐ जाँच करें कि आपने आंतरिक और बाह्य हितधारकों (वित्तीय क्षेत्र के भीतर और बाहर के संस्था और सार्वजनिक प्राधिकरण सहित) के साथ विश्वसनीय, कार्रवाई योग्य साइबर सुरक्षा जानकारी को समय पर साझा करने के लिए प्रक्रियाएं लागू की है।
- ☐ उसके बारे में उपयुक्त अपडेट्स को ट्रैक करें कि अन्य संगठन एफएस-आईएसएसी जैसी जानकारी को साझा करने वाले संगठनों और अन्य खतरों की जानकारी पाने वाले स्त्रोतों का हिस्सा बनकर खतरों, कमजोरियों, घटनाओं और प्रतिक्रियाओं के संदर्भ में उनके तीसरे पक्ष के साथ क्या अनुभव कर रहे हैं।

छोटे संगठनों के लिए साइबर सुरक्षा

घटना की प्रतिक्रिया चेकलिस्ट

तैयारियां

- ☐ आपके संगठन के साइबर जोखिम मूल्यांकन में पहचाने गए सबसे अधिक गंभीर जोखिमों के आधार पर एक घटना प्रतिक्रिया और व्यवसायिक निरंतरता योजना को विकसित करने के लिए अपने संगठन के वरिष्ठ नेतृत्व और अन्य संबंधित कर्मचारियों के साथ काम करें।
- ☐ आपके संगठन के सर्वोच्च-प्राथमिकता वाले साइबर जोखिमों से संबंधित घटनाओं के लिए खतरे के परिदृश्य विकसित करें। उन परिदृश्यों का जवाब देने के लिए क्षमता निर्माण पर ध्यान केंद्रित करें।
- ☐ आपके संगठन के भीतर घटना की प्रतिक्रिया के लिए संपर्क के बिंदुओं की सूची को पहचानें, रिकॉर्ड करें और उपलब्ध कराएं।
- ☐ उपयुक्त स्थानीय और संघीय कानून प्रवर्तन एजेंसियों और अधिकारियों के लिए संपर्क की जानकारी को पहचानें और रिकॉर्ड करें।
- ☐ किस प्रकार की घटनाओं को सूचित किया जाना चाहिए, उन्हें कब और किसे सूचित किया जाना चाहिए, यह निर्दिष्ट करते हुए प्रावधान बनाएं।
- ☐ लिखित दिशा-निर्देश बनाएं जो रूपरेखा बनाता है कि किसी घटना की प्रतिक्रिया कर्मियों को कितनी जल्दी देनी चाहिए और उपयुक्त कारकों के आधार पर कौन सी कार्यवाही की जानी चाहिए, जैसे घटना का कार्यात्मक और जानकारी का प्रभाव, और और घटना से वापस बहाली की संभावना।
- ☐ सभी कर्मचारियों को अपनी तकनीकी टीम से संपर्क करने के लिए सूचित करें - आमतौर पर यह आईटी के कर्मचारी और/या सीआईएसओ/सीआईओ/ अन्य समतुल्य प्रबंधक होगा - जब कोई घटना होती है।
- ☐ कर्मचारी की गतिविधियों पर नजर रखने और अंदरूनी खतरों और घटनाओं की पहचान को सक्षम करने के लिए समाधान लागू करें।
- ☐ यह समन्वय करने के लिए व्यवसायिक निरंतरता योजनाओं को शामिल करें कि आपकी संस्था व्यवसायिक आपातकाल के दौरान आपूर्तिकर्ताओं और प्राथमिक ग्राहकों के साथ कैसे काम करेगी, जिसमें शामिल है कि यदि आवश्यक हो तो आप मैनुअल और वैकल्पिक व्यवसायिक संचालन को कैसे करेंगे।
- ☐ इसमें आपातकालीन प्रणाली को बंद करने और दोबारा शुरू करने के लिए लिखित प्रक्रियाएं शामिल हैं।
- ☐ बैकअप डेटा को पुनः प्राप्त करने और पुनर्स्थापित करने; समय-समय पर इसकी वैधता को सत्यापित करने के लिए बैकअप डेटा का परीक्षण करने के लिए तरीकों का विकास और परीक्षण करें।
- ☐ एक वैकल्पिक सुविधा/साइट में व्यावसायिक संचालन करने के लिए समझौते और प्रक्रियाएं स्थापित की हुई है।
- ☐ सभी ग्राहकों के लिए एक स्पष्ट प्रसार चैनल स्थापित करें।
- ☐ बैकअप डेटा को पुनः प्राप्त करने और पुनर्स्थापित करने; समय-समय पर इसकी वैधता को सत्यापित करने के लिए बैकअप डेटा का परीक्षण करने के लिए तरीकों का विकास और परीक्षण करें।
- ☐ एक वैकल्पिक सुविधा/साइट में व्यावसायिक संचालन करने के लिए समझौते और प्रक्रियाएं स्थापित की हुई है।
- ☐ सभी ग्राहकों के लिए एक स्पष्ट प्रसार चैनल स्थापित करें।

अभ्यास

- ☐ सभी कर्मचारियों या कर्मचारियों के सभी स्तरों के प्रतिनिधियों के साथ छोटे टेबलटॉप अभ्यास आयोजित करें, जिसमें आपके संगठन के एक्सीक्यूटिव, पीआर/संचार कर्मचारी और कानूनी और अनुपालन टीमें शामिल हो।
- ☐ अपने संगठन के लिए प्रासंगिक उद्योग-व्यापी टेबलटॉप अभ्यास को पहचानें और आदर्श रूप से भाग लें।
- ☐ इस बात को सुनिश्चित करने के लिए एक प्रक्रिया स्थापित करें कि अभ्यास से सीखे गए पाठ को आपकी कंपनी की साइबर सुरक्षा रणनीति में शामिल और संबोधित किया गया है।

प्रतिक्रिया देना

- ☐ व्यवसाय संचालन पर प्रभाव को कम करने के लिए घटना प्रतिक्रिया योजना की कार्रवाइयों को लागू करें।
- ☐ प्रभावित हुई/ समझौता की गई प्रणालियों को पहचानें और नुकसान का आकलन करें।
- ☐ प्रभावित परिसंपत्तियों को हटाकर (डिस्कनेक्ट करके) नुकसान को कम करें।
- ☐ जैसे ही टीम को संदेह होता है कि कोई घटना हुई है, सभी सूचनाओं को रिकार्ड करना शुरू करें। प्रभावित चिन्हित संपत्तियों को पृथक/ अलग करते समय घटना के साक्ष्य को संरक्षित करने का प्रयास करें, जैसे प्रभावित परिसंपत्तियों से सिस्टम कॉन्फ़िगरेशन, नेटवर्क और घुसपैठ का पता लगाने वाले लॉग को एकत्र करें।
- ☐ उपयुक्त आंतरिक पक्षों, तीसरे पक्ष के वेंडर, और अधिकारियों को सूचित करें और यदि आवश्यक हो तो सहायता का अनुरोध करें।
- ☐ कानूनों, विनियमों और अंतर-एजेंसी मार्गदर्शन के अनुरूप ग्राहक को सूचित करने और सहायता की गतिविधियाँ शुरू करें।
- ☐ उद्योग को खतरे के बारे में सूचित करने के लिए एफएस-आईएसएसी या एमआईएसपी जैसे खतरों को साझा करने वाले प्लेटफार्मों का उपयोग करें।
- ☐ बाद में समीक्षा करने के लिए घटना के दौरान उठाए गए सभी चरणों को दस्तावेजीकृत करें।

समस्या से उबरना

- ☐ यदि उपलब्ध हो तो रिकवरी किये गए परिसंपत्तियों को समय-समय पर "रिकवरी पॉइंट" पर पुनर्स्थापित करें और सिस्टम को पिछली ज्ञात "अच्छी" स्थिति पर पुनर्स्थापित करने के लिए बैकअप डेटा का उपयोग करें।
- ☐ पुनर्स्थापित परिसंपत्तियों से अपडेट किया गया "नया" बैकअप बनाएं और सुनिश्चित करें कि सभी महत्वपूर्ण परिसंपत्तियों के बैकअप को भौतिक और पर्यावरणीय रूप से सुरक्षित स्थान पर संग्रहीत किये गए हैं।
- ☐ परीक्षण करें और सत्यापित करें कि संक्रमित सिस्टम पूरी तरह से बहाल हो गया हैं। पुष्टि करें कि प्रभावित सिस्टम सामान्य रूप से काम कर रहे हैं।

समीक्षा करना

- ☐ घटना घटित होने के बाद "सीखे गये सबक" चर्चा का आयोजन करें - संभावित कमजोरियों की समीक्षा करने या नए कदमों को लागू करने की सिफारिश करने के लिए वरिष्ठ कर्मचारियों, विश्वसनीय सलाहकारों और कंप्यूटर सपोर्ट वेंडर (वेंडर) से मिलें।
- ☐ संभव हो तो, उन कमजोरियों की पहचान करें (चाहे सॉफ्टवेयर, हार्डवेयर, व्यावसायिक संचालन, या कर्मचारियों के व्यवहार में) जिसके कारण घटना हुई और उनकी गंभीरता को कम करने की योजना बनाएं।
- ☐ पुष्टि करें कि प्रभावित सिस्टम सामान्य रूप से काम कर रहे हैं।
- ☐ पहचानी गई समस्याओं से संबंधित समान या आगे की घटनाओं का पता लगाने की निगरानी के लिए एक योजना बनाएं।
- ☐ खतरों को साझा करने वाले प्लेटफॉर्म जैसे एफएस-आईएसएसी पर सीखे गए सबक और घटना के बारे में जानकारी साझा करें।
- ☐ सीखे गए सबक को अपने संगठन की घटना प्रतिक्रिया प्रोटोकॉल में एकीकृत करें।

छोटे संगठनों के लिए साइबर सुरक्षा

रैंसमवेयर चेकलिस्ट

रैंसमवेयर की तैयारी

☐ **जब आप एक रैंसमवेयर की रोकथाम और संरक्षण योजना बनाते हैं, तो समय-समय पर निम्नलिखित का आकलन करें:**

- क्या आपके संगठन के पास नियमित रूप से निर्धारित बैकअप है?
- क्या आपके संगठन के नेटवर्क से कोई भी गैर-अनिवार्य उपकरण जुड़ा हुआ है?
- क्या आपका संगठन फिरौती देने से जुड़े विनियामक और कानूनी जोखिमों को समझता है?
- क्या आपका संगठन नियमित रूप से अपना सॉफ्टवेयर सिस्टम अपडेट करता है? क्या ये अपडेट स्वचालित हैं?
- क्या आपके संगठन के पास रैंसमवेयर के हमले और डेटा के नुकसान से निपटने की कोई योजना है?
- क्या आपके सिस्टम के पास साइबर बीमा पॉलिसी है? यदि है, तो यह योजना रैंसमवेयर हमलों को कैसे कवर करती है?

वास्तविक समय की सुरक्षा

☐ **उन एंटी-मैलवेयर सुरक्षा प्रणालियों में निवेश करें जो वास्तविक समय में नए खतरे की खुफिया जानकारी के अनुकूल हो।**

☐ **नेटवर्क से जुड़े सभी उपकरणों की सुरक्षा का मूल्यांकन करें जिसमें संवेदनशील या आवश्यक जानकारी रहती है।**

- ☐ सभी सभी गैर-अनिवार्य प्रणालियों को एक अलग नेटवर्क में कनेक्ट करें।
- ☐ रिपोट वर्क सेटअप की सुरक्षा पर विचार करें। सुनिश्चित करें कि सुरक्षा उपकरण सभी वेब ट्रैफ़िक की निगरानी के लिए ऑफ-नेटवर्क काम करते हैं।

☐ **फ़िशिंग हमलों और शक्तिशाली पासवर्ड सुरक्षाओं की आवश्यकता के बारे में कर्मचारी की शिक्षा को बढ़ावा देना।**

☐ **यदि संभव हो तो अपने संगठन में कई कारकों वाले प्रमाणीकरण को लागू करने पर विचार करें।**

☐ **सभी सॉफ्टवेयर और सिस्टम को नियमित रूप से अपडेट रखें।**

- ☐ यदि संभव हो तो स्वचालित अपडेट की अनुमति के लिए सेटिंग्स बदलें।

☐ **इसके लिए एक घटना की प्रतिक्रिया और संकट प्रबंधन योजना बनाएं कि रैंसमवेयर हमले और बहुमूल्य डेटा के नुकसान से कैसे निपटें।**

- ☐ रैंसमवेयर हमले की स्थिति में एक बाहरी संचार योजना तैयार करें।

डेटा बैकअप

☐ **सुरक्षित, नियमित रूप से अपडेटेड बैकअप सिस्टम में निवेश करें जो आपके डेटा को सुरक्षित रखे।**

- ☐ यदि यूएसपी या हार्ड ड्राइव का उपयोग करते हैं, तो बैकअप समाप्त होने के बाद नेटवर्क वाले कंप्यूटर से इन उपकरणों को भौतिक रूप से निकाल दें।
- ☐ यदि क्लाउड स्टोरेज का उपयोग कर रहे हैं, तो सर्वर्स को उच्च-स्तर के एन्क्रिप्शन और कई कारकों वाले प्रमाणीकरण से लैस करें।

☐ **सबसे खराब मामले में आपदा से उबरने के लिए सामान्य बही-खाता की केवल एक रीड-ओनली प्रतिलिपि बनाएं।**

☐ **ऐसी प्रणालियाँ बनाएं जो स्वचालित डेटा रिकवरी और सुधार करती हैं।**

☐ **महत्वपूर्ण डेटा और व्यावसायिक सेवाओं को पुनर्प्राप्त करने में कितना समय लगेगा, इसका आकलन करने के लिए परिदृश्य बनाएं।**

नियामक पर्यावरण

- ☐ **अपने संचालन वातावरण में रैंसमवेयर के लिए उपयुक्त विनियामक और कानूनी मार्गदर्शन का मूल्यांकन करें।**
  - ☐ देश-विशिष्ट मार्गदर्शन पर विचार करें।
  - ☐ वित्तीय-क्षेत्र के विशिष्ट मार्गदर्शन पर विचार करें
  - ☐ अंतरराष्ट्रीय कानूनी और नियामक आवश्यकताओं पर विचार करें।
  - ☐ बदलते मार्गदर्शन के आवधिक मूल्यांकन के लिए एक योजना बनाएं।
- ☐ फिरौती देने से जुड़े जोखिमों का आकलन करें।
- ☐ स्थानीय कानून प्रवर्तन के साथ संपर्क करें।
- ☐ हमले की स्थिति में त्वरित सूचना साझा करने के लिए संपर्क बनाएं।
- ☐ रैंसमवेयर के लिए साइबर बीमा पॉलिसियों के लाभों और कमियों का आकलन करें।

छोटे संगठनों के लिएसाइबर सुरक्षा

कार्यबल विकास

साइबर सुरक्षा कार्यबल विकास के लिए मूलभूत दृष्टिकोण

☐ **आपूर्ति पाइपलाइन का विस्तार करें।**

- क्या आपके संगठन के विश्वविद्यालयों और तकनीकी कॉलेजों के साथ संबंध हैं?
- क्या आप साइबरसिटी इंटर्नशिप और अप्रेंटिसशिप प्रदान करते हैं?

☐ **टैलेंट ओपनिंग के साथ मौजूदा आपूर्ति को पहचानें और मिलान करें।**

- क्या आपका मानव संसाधन विभाग आवश्यक कौशल को पोस्ट किए गए नौकरी विवरण में कुशलता से दिखला रहा है?

☐ **मौजूदा कर्मचारियों को साइबर कार्यबल का हिस्सा बनने के लिए पुनः प्रशिक्षित करें।**

- क्या आपका संगठन संसाधनों को अपने साइबर कार्यबल में स्थानांतरित करके मौजूदा प्रतिभा का लाभ उठा रहा है?

☐ **तकनीकी नवीनता के माध्यम से अपने साइबर कर्मचारियों की मांग को कम करें।**

- क्या आपकी क्षमता में वृद्धि करने के लिए तीसरे पक्ष के सेवा प्रदाताओं के साथ समझौते हैं?

☐ **वर्तमान कार्यबल को बनाए रखने की शक्ति में सुधार करें।**

- क्या आपका संगठन टीम के प्रतिभाशाली सदस्यों में निवेश कर रहा है?
- क्या आपका संगठन इच्छुक व्यक्तियों को साइबर सुरक्षा में करियर तलाशने की अनुमति देता है?

आवश्यकताओं को पहचानना

☐ **अपने कार्यबल की आवश्यकताओं को पहचानें।**

- ☐ अपने संचालन की जटिलता और उस गति का मूल्यांकन करें जिसके साथ कार्यों को निष्पादित करने की आवश्यकता है।
- ☐ बढ़ती क्षमता की आवश्यकताओं पर विचार करें और विचार करें कि क्या उन्नत तकनीकियां हमले की सतह को कम करने में मदद कर सकती हैं।

☐ **अपने कार्यबल की आवश्यकताओं को पहचानें।**

- ☐ अपने संगठन में साइबर सुरक्षा कार्यबल की योग्यता, लचीलेपन और दक्षता पर विचार करें।
- ☐ आदर्श रिपोर्टिंग संरचनाओं को पहचानें और उसे हाइलाइट करें जहां बहु-कार्यक्षमता बेहतर है।

☐ **उनके द्वारा समर्थित व्यावसायिक कार्यों के आधार पर साइबर सुरक्षा कार्यबल के आवश्यक ज्ञान, कौशल, क्षमताओं और योग्यता को परिभाषित करें।**

☐ **अपने संगठन के मौजूदा साइबर सुरक्षा कार्यबल में महत्वपूर्ण कमी को पहचानें।**

- ☐ भूमिकाओं और जिम्मेदारियों के आंतरिक आकलन के दिशा-निर्देश के लिए एनआईसीई फ्रेमवर्क जैसे मौजूदा उपकरणों को लगाएं।

बाहरी भर्ती में सुधार

- ☐ **स्पष्ट, आंतरिक रूप से सुसंगत नौकरी के विवरण लिखकर जॉब पोस्टिंग को मजबूत करें।**
  - ☐ उपयुक्त कौशल सेट को उजागर करने के लिए एनआइसीई फ्रेमवर्क जैसे मौजूदा उपकरणों का उपयोग करें।
- ☐ **आवेदन प्रक्रिया के माध्यम से भर्ती के लिए डेटा इकट्ठा करें।**
  - ☐ डेटा इकट्ठा करने को व्यवस्थित करें और सिलो बनने को रोकने और प्रतिभा उद्गम और विकास का समर्थन करने के लिए कंपनी भर में साझा करें।
  - ☐ पहुँच में कमी की पहचान करने के लिए समय-समय पर भर्ती डेटा का मूल्यांकन करें
- ☐ **उम्मीदवार की क्षमता का आकलन करने के लिए कई संकेतकों पर भरोसा करें।**
  - ☐ व्यवस्थित हायरिंग के आकलन को कार्यान्वित करने पर विचार करें।
  - ☐ उपयुक्त डिग्री, प्रमाणपत्र और कार्य अनुभव का मूल्यांकन करें।
  - ☐ हायरिंग का निर्णय लेते समय एक विशिष्ट मीट्रिक पर निर्भर होने से बचें।

आंतरिक प्रशिक्षण और विकास को आगे बढ़ाना

- ☐ **कैरियर मैप बनाएं जो आपके साइबर सुरक्षा कार्यबल के लिए उन्नति ट्रैक को प्रदर्शित करता है।**
- ☐ **स्टाफ को साइबर सुरक्षा की भूमिका में बनाए रखने और पुनः स्थिति निर्धारण करने करने के लिए अपने संगठन के भीतर रास्ते की पहचान करें।**
  - ☐ रूचि और क्षमता के आधार पर साइबर सुरक्षा में गैर-पारंपरिक प्रवेश-बिंदुओं पर विचार करें।
  - ☐ अपने संगठन के भीतर अपस्किलिंग और पुनः- प्रशिक्षण कार्यक्रमों का विस्तार करें और पारगमन को प्रोत्साहित करें।
- ☐ **आंतरिक प्रशिक्षण और स्वतंत्र रूप से सीखने को प्रोत्साहित करें।**
  - ☐ निरंतर शिक्षा और कौशल प्रमाणन के लिए अवसर खोलें।
- ☐ **कार्यबल को बनाए रखने पर डेटा की निगरानी करें।**
  - ☐ यह पहचानने के लिए समय-समय पर अवधारित डेटा का मूल्यांकन करें कि क्या कार्यक्रम कर्मचारी की जरूरतों को पूरा कर रहे हैं।