लोक सभा सचिवालय

शोध और सूचना प्रभाग

सूचना बुलेटिन

सं. लार्डिस (ई एंड एफ) 2017/आईबी-2 अगस्त 2017

वित्तीय क्षेत्र में साइबर-सुरक्षा

परिचय

वित्तीय क्षेत्र को सुदृढ़ बनाने के लिए लेन-देन और संचार के डिजिटल माध्यमों का महत्व तेजी से बढ़ता जा रहा है, जिससे समाज और अर्थव्यवस्था का सशक्तिकरण हो रहा है। डिजिटल परिचालनों के लाभों को मान्यता प्रदान करते हुए, विश्व भर की सरकारें अपनी वित्तीय संस्थाओं के दैनिक कार्यकरण में डिजिटीकरण को बढ़ावा दे रही हैं। तथापि, इलेक्ट्रॉनिक लेन-देनों में हुई अभूतपूर्व वृद्धि और तेजी से विकसित होती डिजिटल अर्थव्यवस्था के चलते साइबर हमले गंभीर चिंता का विषय बन गए हैं। इस प्रकार, डिजिटीकरण ने न केवल अवसर उपलब्ध कराए हैं; अपितु इसने अर्थव्यवस्थाओं को ऐसे जोखिमों के समक्ष ला खड़ा किया है जिनमें बैंकिंग और अन्य वित्तीय संस्थाओं के परिचालनों में गंभीर व्यवधान उत्पन्न करने की क्षमता है।

उच्च कनेक्टिविटी के डिजिटल निर्भरता वाले किसी भी तंत्र के साथ साइबर हमलों का सतत खतरा बना रहता है, जो कि आज, विशेषकर वित्तीय क्षेत्र हेतु, गंभीर चिंता का विषय बन गया है। वित्तीय सेवाएं उपलब्ध कराने के लिए सूचना प्रौद्योगिकी (आईटी) का उपयोग तेजी से बढ़ा है और वर्तमान में यह सभी बैंकों और वित्तीय संस्थानों की परिचालन रणनीति का एक अभिन्न अंग है। इंटरनेट बैंकिंग और नवीनतम तकनीकयुक्त वित्तीय सेवाओं के बढ़ते उपयोग के साथ ही साइबर जोखिमों में वृद्धि हुई है और साइबर अपराधों में भी अत्याधुनिक प्रौद्योगिकी का उपयोग बढ़ रहा है। ऐसे हमले करने वालों में ''हैक्टिविस्ट्स'', साइबर अपराधी और आतंकवादी शामिल हैं जो राजनीतिक और वित्तीय अस्थिरता पैदा करने तथा वित्तीय अवसंरचना को ठप्प करने के लिए वित्तीय प्रलोभनों से प्रेरित होते हैं।

साइबर सुरक्षा, अथवा साइबर स्पेस की सुरक्षा, राष्ट्रीय हित के पहलू से भी स्वाभाविक रूप से अन्तर्राष्ट्रीय चिंता का मुद्दा है। राष्ट्रीय सीमाओं की तरह, साइबर स्पेस की सीमाएं सुपरिभाषित नहीं हैं। इसकी भौगोलिकीय अथवा संस्थागत सीमाएं नहीं हैं। यह एक ऐसा स्वतंत्र परिवेश है जिसमें लोगों और सॉफ्टवेयर सेवाओं का आपसी संपर्क शामिल है जिनके द्वारा सूचना और संचार का विश्वव्यापी वितरण संभव होता है। इंटरनेट की बढ़ती पहुंच से साइबर स्पेस का विस्तार हो रहा है क्योंकि इसका आकार इसके माध्यम से किए जाने वाले कार्यकलापों से समानुपातिक होता है। ऐसे परिदृश्य में प्रौद्योगिकी को सावधानीपूर्वक अपनाने की आवश्यकता है ताकि साइबर जोखिमों की संभावनाओं को कम से कम किया जा सके।

बॉक्स-1
डिजिटल अर्थव्यवस्था क्या है

1995 की सर्वाधिक बिकने वाली पुस्तक ''दि डिजिटल इकोनोमी: प्रॉमिस एंड पेरिल इन दि ऐज ऑफ नेटवर्कड् इंटेलीजेंस'' (डिजिटल अर्थव्यवस्था: प्रसार तंत्र से जुड़ी आसूचना के युग में संभावनाएं और खतरे) के लेखक डॉन टैप्स्कॉट द्वारा गढ़े गए शब्द ''डिजिटल अर्थव्यवस्था'', सूचना और संचार प्रौद्योगिकियों (आईसीटी) द्वारा समर्थित आर्थिक कार्यकलापों का विश्वव्यापी नेटवर्क है। इसे अधिक सरल शब्दों में डिजिटल प्रौद्योगिकियों पर आधारित एक अर्थव्यवस्था के रूप में भी परिभाषित किया जा सकता है।

डिजिटल अर्थव्यवस्था का अर्थ मात्र व्यावसायिक लेन-देन को व्यक्तिगत लेन-देन से ऑनलाइन लेन-देन में बदलने से ही नहीं है; अपितु इसका अर्थ व्यावसायिक संपर्कों और लेन-देन करने के तरीकों को बदलने और साथ ही आर्थिक-नवोन्मेषों को सक्षम बनाने से भी है। डिजिटल अर्थव्यवस्था के कई महत्वपूर्ण घटक हैं। इनमें प्रौद्योगिकीय अवसंरचना जिसमें, हार्डवेयर, सॉफ्टवेयर और नेटवर्क्स शामिल हैं; डिजिटल प्रक्रियायें जिनके माध्यम से व्यावसायिक कार्यकलाप सम्पन्न होते हैं और साथ ही ऐसे डिजिटल लेन-देन भी शामिल हैं जिनके माध्यम से उपभोक्ता संगठनों से उत्पाद और सेवाएं खरीदते और प्राप्त करते हैं।

डिजिटल अर्थव्यवस्था लगातार विकसित हो रही है। व्यक्तिगत कम्प्यूटिंग उपकरणों, उद्यम कम्प्यूटिंग क्षमताओं और सुलभ इंटरनेट के बढ़ते उपयोग के द्वारा गति प्राप्त करके अब यह अधिक उन्नत डिजिटल प्रौद्योगिकियों, उल्लेखनीय रूप से वायरलेस नेटवर्क्स, मोबाइल उपकरणों, भूस्तैथिकी प्रौद्योगिकियों [अर्थात् भूस्तैथिकी प्रणाली (अर्थात् जीपीएस)], एम्बेडेड सेंसर और तत्समय वैश्लेषिकी द्वारा संचालित हो रही है।

साइबर अपराध अथवा साइबर हमले में कम्प्यूटर नेटवर्क पर हमला करना भी शामिल हो सकता है जिसमें इंटरनेट के माध्यम से एक कम्प्यूटर द्वारा दूसरे कम्प्यूटर पर हमला किया जाता है। इन अपराधों में व्यक्तिगत/संगठन अथवा देश की बौद्धिक संपदा को चुराना, ऑनलाइन बैंक खातों पर कब्जा करना और किसी देश की महत्वपूर्ण अवसंरचना को भी बाधित करना शामिल हैं। अभी हाल ही में, रैनसमवेयर हमले के द्वारा सौ से भी अधिक देशों में एक लाख से अधिक कम्प्यूटरों को लॉक किए जाने का अनुमान है जो कम्प्यूटर और इंटरनेट संचालित (आभासी) दुनिया में साइबर खतरों के वास्तविक जोखिम को दर्शाता है। आज, साइबर हमलों की बारम्बारिता और प्रभाव कई गुणा बढ़ गया है और प्रमुख रूप से ऐसा ही वित्तीय क्षेत्र में भी हुआ है जो बैंकों और वित्तीय संस्थानों द्वारा सतत आधार पर पर्याप्त साइबर सुरक्षा तैयारी सुनिश्चित करने की अत्यंत आवश्यकता को रेखांकित करता है। इस मुद्दे ने पूरी दुनिया का ध्यान आकर्षित किया है और इसे विश्व भर में सभी सरकारों और वित्तीय क्षेत्र के लगभग प्रत्येक संगठन के भी एजेंडे में सबसे ऊपर स्थान दिया गया है।

वित्तीय क्षेत्र हेतु साइबर सुरक्षा के मूलभूत तत्व

अधिक खतरनाक तरीके से बढ़ रहे साइबर जोखिम और वैश्विक वित्तीय तंत्रों के समक्ष इसके खतरे को ध्यान में रखकर जी-7 देशों[1] के एक विशेषज्ञ समूह ने वित्तीय क्षेत्र में साइबर सुरक्षा के संबंध में 2016 में एक रिपोर्ट तैयार की है जिसमें ऐसे मूलभूत तत्व शामिल किए गए हैं जिनका उद्देश्य वित्तीय क्षेत्र के किसी निकाय को अपनी साइबर सुरक्षा रणनीति और संचालन ढांचे के डिजाइन और कार्यान्वयन के साथ-साथ अपनी नीतियों के विकास के लिए सार्वजनिक प्राधिकरणों को निर्देशित करने के लिए सहायता करना है।

(i) साइबर सुरक्षा रणनीति और ढांचा: किसी साइबर सुरक्षा रणनीति और ढांचे का उद्देश्य यह निर्दिष्ट करना है कि एक एकीकृत और व्यापक तरीके से साइबर जोखिम को कैसे पहचानें, उसका प्रबंधन करें और उसे कम करें। वित्तीय क्षेत्र के निकायों को उनकी प्रकृति, आकार, जटिलता, जोखिम प्रोफाइल और संस्कृति के अनुरूप साइबर सुरक्षा रणनीतियों और ढांचों को तैयार करना चाहिए। साइबर खतरे और अतिसंवेदनशील परिदृश्य से अवगत कोई न्यायाधिकार क्षेत्र क्षेत्रव्यापी साइबर सुरक्षा रणनीतियां और रूपरेखाएं भी तैयार कर सकता है जो यह रेखांकित करता है कि वित्तीय क्षेत्र में निकायों और लोक प्राधिकरणों के बीच तथा उन क्षेत्रों के साथ, जिन पर वित्तीय क्षेत्र निर्भर करता है और अन्य प्रासंगिक न्यायाधिकार क्षेत्रों के साथ, किस प्रकार सहयोग किया जाना चाहिए।

(ii) शासन: प्रभावी शासन संरचनाएं स्पष्ट उत्तरदायित्वों और सूचना की पद्धतियों को स्पष्ट कर जवाबदेही को मजबूती प्रदान करती हैं। प्रभावी शासन प्रतिस्पर्धात्मक उद्देश्यों में मध्यस्थता भी करता है और परिचालन इकाइयों, सूचना प्रौद्योगिकी, जोखिम और नियंत्रण संबंधी कार्यकलापों के बीच संचार को भी बढ़ावा देता है। अपने मिशनों और रणनीतियों के अनुरूप, बोर्ड के निदेशकों (अथवा सार्वजनिक निकायों अथवा प्राधिकरणों हेतु इसी तरह के निगरानी निकायों) को उनके निकायों के लिए साइबर जोखिम सहनशीलता स्थापित करनी चाहिए और संबंधित साइबर सुरक्षा कार्यक्रमों के डिजाइन, कार्यान्वयन और प्रभावकारिता की निगरानी करनी चाहिए।

(iii) जोखिम और नियंत्रण आकलन: आदर्श रूप से, उद्यम जोखिम प्रबंधन कार्यक्रम के एक भाग के रूप में, निकायों को कहीं से भी उपस्थित होने वाले अंतर्निहित साइबर जोखिम का आकलन करना चाहिए। इसके बाद, निकायों को शेष साइबर जोखिम का पता लगाने के लिए चिह्नित जोखिमों के विरुद्ध सुरक्षा के लिए नियंत्रकों की उपस्थिति और प्रभावकारिता का पता लगाना चाहिए और उसका आकलन करना चाहिए। सुरक्षातंत्रों में किसी चिह्नित गतिविधि में शामिल न होकर जोखिम से बचने या उसे समाप्त करने को शामिल किया जा सकता है। उनमें जोखिम को नियंत्रित, साझा या अंतरित करके जोखिम की गंभीरता को कम करना भी शामिल किया जा सकता है। सार्वजनिक प्राधिकरणों को विफलता और जोखिम की अधिकता वाली एकल स्थितियों की पहचान करने के लिए अपने जोखिम और नियंत्रण आकलनों के एक भाग के रूप में अपनी वित्तीय प्रणालियों में महत्वपूर्ण वित्तीय कार्यकलापों की रूपरेखा तैयार करनी चाहिए।

(iv) निगरानी: प्रभावी निगरानी से निकायों को स्थापित जोखिम वहनीयता का पालन करने और मौजूदा नियंत्रण प्रणाली में खामियों को समय रहते दूर करने में सहायता मिलती है। किसी निकाय के स्वरूप, उसके साइबर जोखिम प्रोफाइल और नियंत्रण परिवेश के आधार पर जांच और परीक्षण कार्यकलापों को समुचित रूप से साइबर-सुरक्षा कार्यक्रम प्रबंधन के समरूप बनाया जाना चाहिए।

(v) प्रतिक्रिया: निकायों को अपने जोखिम और नियंत्रण आकलनों के एक भाग के रूप में प्रभावी अप्रत्याशित घटना प्रतिक्रिया को सुगम बनाने के लिए अप्रत्याशित घटना प्रतिक्रियाशील नीतियों और अन्य नियंत्रण प्रणाली को कार्यान्वित करना चाहिए। अन्य बातों के अतिरिक्त, इन नियंत्रण प्रणालियों के माध्यम से निकायों में निर्णय लेने के उत्तरदायित्वों पर स्पष्ट रूप से ध्यान दिया जाना चाहिए।

(vi) पुन: बहाली (रिकवरी): प्रचालनात्मक स्थिरता और समेकता सुनिश्चित होने पर प्रचालनों की त्वरित और प्रभावी बहाली, महत्वपूर्ण आर्थिक और अन्य कार्यकलापों की प्राथमिकता पर आधारित और संबंधित सार्वजनिक प्राधिकरणों द्वारा निर्धारित लक्ष्यों के अनुरूप होनी चाहिए। निकायों और सार्वजनिक प्राधिकरणों के पास महत्वपूर्ण कार्यकलापों, प्रक्रियाओं और गतिविधियों को फिर से शुरू और बहाल करने में एक दूसरे की सहायता करने की क्षमता होने पर वित्तीय क्षेत्र में विश्वास और भरोसा बनाए रखने में काफी सुधार होता है। अत:, कोई अप्रत्याशित घटना होने से पहले वित्तपोषण जैसी आवश्यक गतिविधियों और महत्वपूर्ण प्रक्रियाओं हेतु आकस्मिकता योजनाएं बनाने और उनकी जांच करने से एक त्वरित और अधिक प्रभावी बहाली (रिकवरी) में सहायता मिल सकती है।

(vii) सूचना साझा करना: सुभेद्यता (वलनेरेबिलिटी) का किस प्रकार अनुचित लाभ उठाया गया, इससे संबंधित आशंका सूचकों अथवा ब्यौरों जैसी तकनीकी जानकारी को साझा करने से निकायों को अपनी सुरक्षा में अद्यतन बने रहने तथा हमला करने वाले (अटैकर्स) द्वारा अपनाई जाने वाली नवीन पद्धतियों के बारे में सीखने में सहायता मिलती है। निकायों और सार्वजनिक प्राधिकरणों के बीच व्यापक आंतरिक जानकारी को साझा करने से यह सामूहिक समझ बढ़ती है कि हमला करने वाले (अटैकर्स) क्षेत्र व्यापी सुभेद्यताओं (सेक्टर-वाइड वलनेरेबिलिटिस) का किस प्रकार अनुचित लाभ उठा सकते हैं जिससे महत्वपूर्ण आर्थिक कार्यकलापों में व्यवधान पैदा हो सकता है तथा वित्तीय स्थिरता के लिए खतरा पैदा हो सकता है। इसके महत्व को देखते हुए, निकायों और सार्वजनिक प्राधिकरणों को सूचना साझा करने में आने वाली बाधाओं की पहचान और उनका समाधान करना चाहिए।

[1] सात देशों का समूह (जी-7) जिसमें कनाडा, फ्रांस, जर्मनी, जापान, इटली, यूनाइटेड किंगडम और संयुक्त राज्य अमेरिका शामिल हैं।

(viii) **लगातार सीखना:** साइबर खतरे और सुभेद्यता तेजी से बढ़ते जाते हैं जैसे-जैसे उनका समाधान करने हेतु उत्कृष्ट पद्धतियां और तकनीकी मानक विकसित होते जाते हैं। जैसे-जैसे नए निकाय, उत्पाद और सेवाएं विकसित होती हैं उसी प्रकार समय के साथ-साथ वित्तीय क्षेत्र की संरचना में भी परिवर्तन होता है। खतरे और नियंत्रण परिवेश में बदलाव के प्रति अनुकूल बनाने, उपयोगकर्त्ता जागरूकता बढ़ाने तथा प्रभावशाली तरीके से संसाधनों का उपयोग करने के लिए निकाय विशेष और क्षेत्र-व्यापी साइबर सुरक्षा रणनीतियों और रूपरेखाओं की समय-समय पर समीक्षा किए जाने और उन्हें अद्यतन बनाए जाने की आवश्यकता है। ऊर्जा और दूरसंचार जैसे अन्य क्षेत्र बाहरी क्षेत्रों पर निर्भर होते हैं और इसलिए निकायों और सार्वजनिक प्राधिकरणों को किसी समीक्षा प्रक्रिया के भाग के रूप में इन क्षेत्रों में हुए विकास पर विचार करना चाहिए।

डिजिटल इंडिया और साइबर सुरक्षा

देश को एक डिजिटल रूप से सशक्त समाज और ज्ञान आधारित अर्थव्यवस्था के रूप में परिवर्तित करने के दृष्टिकोण से डिजिटल इंडिया भारत सरकार का एक अग्रणी कार्यक्रम है। नकदी रहित लेन-देन को बढ़ावा देने और भारत को एक कम नकदी का प्रयोग करने वाले (लेस कैश) समाज के रूप में परिवर्तित करने के भाग के रूप में डिजिटल भुगतान के ई-वालेट, काड्र्स (प्रीपेड, डेबिट, क्रेडिट), प्वाइंट ऑफ सेल (पीओएस), यूनीफाइड पेमेंट इंटरफेस (यूपीआई), अनस्ट्रक्चर्ड सप्लीमेंटरी सर्विस डाटा (यूएसएसडी) चैनल आदि जैसे विभिन्न तरीके उपलब्ध हैं।

तथापि, भारत में डिजिटल भुगतान में अत्यधिक वृद्धि तथा कम नकदी वाली अर्थव्यवस्था की दिशा में अग्रसर होने से देश की वित्तीय साइबर सुरक्षा अवसंरचना और तैयारी को सुदृढ़ बनाने की आवश्यकता पर नए सिरे से ध्यान दिया जा रहा है। बैंक और वित्तीय संस्थान विभिन्न प्रकार के साइबर हमलों और ऑनलाइन धोखाधड़ी हेतु अत्यधिक सुभेद्य है। कोर बैंकिंग के अतिरिक्त, ई-बैंकिंग, एटीएम और खुदरा बैंकिंग जैसी सेवाएं, साइबर अपराध हेतु और अधिक सुभेद्य बनती जा रही हैं। इंडियन कम्प्यूटर इमरजेंसी रेसपांस टीम (सीईआरटी-इन)[2] ने केवल जून, 2015 में ही चालीस हजार से अधिक साइबर अप्रत्याशित घटनाओं की जानकारी दी, जिनमें अन्य के अतिरिक्त वेब अतिक्रमण, मैलवेयर प्रसार, फिशिंग, ''डिस्ट्रीब्यूटिड डिनायल ऑफ सर्विसेस अटैक्स और वेब विरूपण'' आदि शामिल हैं। यद्यपि, यह संख्या वास्तविक खतरे के स्तर को नहीं दर्शाती है क्योंकि, कंपनियां और व्यक्ति प्राय: सुरक्षा को लेकर लापरवाह होते हैं और साइबर हमलों की रिपोर्ट दर्ज कराने के प्रति अनिच्छुक होते हैं। अलग-अलग रूप से ऐसे हमले बैंकिंग प्रणाली को बड़े पैमाने पर क्षति नहीं पहुंचा सकते परंतु, बहु हमला रणनीतियों (मल्टीपल अटैक टैक्टिस) सहित एक समन्वित दृष्टिकोण (कोआर्डिनेटेड एप्रोच), जिसमें सूचना की चोरी और इसी प्रकार के अन्य उद्देश्यों हेतु मैलवेयर की सहायता से प्रणालियों में सेंध लगाना और संक्रमित (इंफेक्टिंग) करना शामिल है एक वास्तविक खतरा पैदा करता है।

वित्त वर्ष 2016-17 के दौरान भारत में साइबर सेंधमारी के गंभीर मामले सामने आए। ऐसी एक घटना में हैकरो ने हितैची के नेटवर्क में सेंध लगाई थी, जिसे कुछ बैंकों ने अपने एटीएम लेन-देन की प्रक्रिया आउटसोर्स की थी। इन बैंकों के लगभग 32,00,000 डेबिट कार्ड धारकों को यह आशंका थी कि इसके परिणामस्वरूप उनके खाते की जानकारी को खतरा पैदा हो गया है। एक पेमेंट सिक्युरिटी फार्म, हितैची ने जिसकी सेवाएं ली थीं, के माध्यम से फारेंसिक जांच किए जाने पर यह पता चला कि हैकरों ने हितैची के सिस्टम में एक ''डमी कोड बुक'' तैयार की थी, जिसमें, जब कभी ग्राहक अपने एटीएम कार्ड का इस्तेमाल करते थे, तब उनकी व्यक्तिगत पहचान संख्या को चुराने के प्रयास में वह ''कोड बुक'' 0000 से 9999 तक सभी 4-अंकों की संभावित संख्या को पकड़ लेता था। एक अन्य घटना में एक साइबर हैकिंग ऑपरेशन में यूनियन बैंक ऑफ इंडिया के खाते से बिना अनुमति (विदाउट ऑथोराइजेशन) के 171 मिलियन अमरीकी डालर की निकासी की गई। 2017 के पहले दो माह के दौरान भारत में विभिन्न बैंकों ने रैनसमवेयर हमले के मामलों की भी जानकारी दी।

बॉक्स-2
हाल ही में विश्व स्तर पर हुए साइबर हमले

- **फिलिपींस:** केसिनोस को धन शोधन रोधी अधिनियम के दायरे से बाहर रखने से हैकरों को जांच के दायरे में आए बिना धनराशि का लेन-देन करने के लिए बचाव का एक रास्ता (लूपहोल) मिल गया। हैकरों ने 4 और 5 फरवरी, 2016 को जब बंगलादेश बैंक कार्यालय बंद थे, फैडरल रिजर्व बैंक ऑफ न्यूयार्क में बंगलादेश सेंट्रल बैंक के खातों से 951,000,000 अमरीकी डालरों की चोरी करने के लिए स्विफ्ट (सोसाइटी फार वर्ल्डवाइड इंटरबैंक फाइनेंशियल टेलीकम्युनिकेशन) नेटवर्क के माध्यम से अनुदेश जारी किए। वे लोग 101,000,000 अमरीकी डालरों की चोरी करने में सफल रहे। इनमें से 81,000,000 अमरीकी डालर फिलीपींस में पाए गए (रिजल कमर्शियल बैंकिंग कारपोरेशन के पास पांच अलग-अलग खातों में) और शेष 20,000,000 अमरीकी डालर श्रीलंका (शलीका फाउंडेशन, श्रीलंका में स्थित एक कंपनी) में पाए गए।
- **यूनाइटेड किंग्डम:** हैकरों ने जनवरी, 2016 में एचएसबीसी यूनाइटेड किंग्डम की वेबसाइट को हैक कर लिया। इसके बाद कई घंटों के लिए इंटरनेट बैंकिंग सेवा को बंद (ब्लॉक) कर दिया गया। यद्यपि, इस घटना से ग्राहकों से संबंधित किसी ब्यौरे (डाटा) को कोई नुकसान नहीं हुआ।
- **ग्रीस:** जनवरी, 2016 में ''अज्ञात'' एक्टिविस्ट हैकर ग्रुप ने बैंक ऑफ ग्रीस को कई मिनटों के लिए ऑफलाइन कर दिया था। तथापि, बैंक के सुरक्षा दस्ते ने इस पर तुरंत कार्यवाही की और डाटा को किसी प्रकार का नुकसान नहीं हुआ।
- **कतर:** अप्रैल, 2016 में कतर नेशनल बैंक पर एक अज्ञात साइबर हमला हुआ जिसके परिणामस्वरूप ग्राहकों के लगभग 1.4 जीबी तक के डाटा की हानि हुई। चोरी हुए डाटा में अल जजीरा के कर्मचारियों, कतर पर शासन करने वाले अल-थानी परिवार के सदस्यों और आसूचना तथा रक्षा विभाग के अधिकारियों से संबंधित फाइलें शामिल थीं।
- **वियतनाम:** मई, 2016 में हैकरों ने वियतनाम के ताइन फोंग बैंक से 1,100,000 मिलियन अमरीकी डॉलर चुराने की कोशिश की। इस हमले में स्विफ्ट नेटवर्क के माध्यम से अनुदेशों का प्रयोग किया गया था। तथापि, बैंक के साइबर सुरक्षा दस्ते ने इस पर तुरंत कार्यवाही की और कोई हानि नहीं हुई।
- मई, 2017 में रैनसमवेयर ने रूस और यूनाइटेड किंगडम सहित 100 से अधिक देशों के XP के पुराने वर्जन पर चल रहे कम्प्यूटरों को संक्रमित करके; फाइलों तक पहुंच पर रोक लगाकर वहां के सिस्टम को प्रभावित किया।

[2] इंडियन कम्प्यूटर इमरजेंसी रेसपांस टीम (सीईआरटी-इन) इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय के अंतर्गत एक संगठन है। सूचना प्रौद्योगिकी (संशोधन) अधिनियम, 2008 की धारा 70ख के अंतर्गत सीईआरटी-इन को साइबर सुरक्षा के क्षेत्र में निम्नलिखित कार्य करने के लिए एक राष्ट्रीय एजेंसी के रूप में नियुक्त किया गया है:—(एक) साइबर अपराध संबंधी घटनाओं का संग्रहण, उनका विश्लेषण और जानकारी का प्रचार-प्रसार; (दो) साइबर सुरक्षा घटनाओं का पूर्वानुमान और चेतावनी; (तीन) साइबर सुरक्षा घटनाओं के प्रबंधन हेतु आपातकालीन उपाय; (चार) साइबर घटना प्रतिक्रिया कार्यकलापों का समन्वय; और (पांच) सूचना सुरक्षा पद्धतियों, प्रक्रियाओं, निवारण, प्रतिक्रिया और साइबर घटनाओं की रिपोर्टिंग के संबंध में दिशानिर्देश, परामर्श, सुभेद्यता टिप्पण और श्वेत पत्र जारी करना।

भारत में बैंकिंग और वित्तीय क्षेत्र में साइबर खतरों के प्रकार

भारतीय कम्प्यूटर आपातकालीन प्रतिक्रिया दल (सीईआरटी-इन) को सूचित की गई बैंकिंग और वित्तीय क्षेत्र की अप्रत्याशित घटनाओं में यह देखा गया कि ट्रेडिशनल फिशिंग अटैक्स, डिस्ट्रीब्यूटेड डिनायल ऑफ सर्विस (डीडीओएस) अटैक्स, वैब विरूपण आदि की अपेक्षा खतरा उत्पन्न करने वालों द्वारा एटीएम, प्वाइंट ऑफ सेल, टर्मिनल्स और इलेक्ट्रॉनिक वैलेट्स जैसे वैकल्पिक चैनलों में सुभेदयताओं और जटिलताओं का अधिकाधिक अनुचित लाभ उठाने का प्रयास किया गया। भारत में मोटे तौर पर निम्न प्रकार के साइबर खतरे हैं:—

एटीएम पर हमले

(क) **एटीएम जैकपॉटिंग/स्पिटिंग मालवेयर अटैक्स:** मालवेयर ग्रीन डिसपेंसर पुराने सॉफ्टवेयर से संचालित एटीएम (ओ) की श्रृंखला की लोकलाइस्ड हैकिंग को सुगम बनाता है। यह हमलावरों को किसी व्यापक नेटवर्क संक्रमण को शामिल किए बिना एटीएम तक पहुंचने, वहां से आसानी से नकदी निकालने की सुविधा प्रदान करता है। यह हैक ''भौतिक'' (फिज़िकल) मालवेयर हमला होता है जिसमें डिस्पेंसर के यूएसबी पोर्ट में लैपटॉप, फोन अथवा पेनड्राइव जैसा कोई भी यंत्र लगाकर उसमें कोई संक्रमित फाइल अथवा वायरस डाला जाता है जिससे मशीन अनियमित ढंग से कार्य करने लगती है। जब इन्हें लगाया जाता है तब ग्रीन डिस्पेंसर एटीएम पर ''सेवा में नहीं'' (आउट ऑफ सर्विस) संदेश प्रदर्शित कर सकता है परंतु मशीन को वर्चुअल की-बोर्ड द्वारा दूर से नियंत्रित किया जा सकता है तथा उसे नकदी बाहर निकालने का अनुदेश दिया जा सकता है। तत्पश्चात् मालवेयर इस रिकार्ड को मिटा देता है ताकि न्यायिक जांच से बचा जा सके।

(ख) **एटीएम स्कीमिंग और प्वाइंट ऑफ सेल क्राइम:** इसमें एटीएम मशीन अथवा पीओएस सिस्टम की सुरक्षा में सेंध लगाई जाती है और मशीन के कीपैड के ऊपर एक स्किमिंग यंत्र लगाया जाता है ताकि वह असली कीपैड जैसा प्रतीत हो अथवा कार्ड रीडर से एक यंत्र लगाया जाता है ताकि वह मशीन का ही एक हिस्सा दिखे। इसके अलावा, क्रेडिट कार्ड के डाटा को चुराने वाले मालवेयर को सीधे इन यंत्रों पर लगाया जा सकता है। स्किमरस के सफल कार्यान्वयन से एटीएम मशीन से कार्ड नंबर और निजी पहचान संख्या कोड (पीआईएन) एकत्रित करके कपटपूर्ण लेन-देन करने के लिए इनका बाद में फिर से उपयोग किया जाता है।

फिशिंग घोटाले

फिशिंग सामाजिक इंजीनियरी का एक ऐसा रूप है जिसमें ई-मेल अथवा इंस्टंट मैसेज जैसे ऊपरी तौर पर अधिकृत प्रतीत होते इलेक्ट्रॉनिक संप्रेषण में एक विश्वस्त व्यक्ति अथवा व्यापार का छद्म वेश धारण करके धोखे से पासवर्ड, यूसरनेम, लॉगिन आईडी, एटीएम पिन और क्रेडिट कार्ड के ब्यौरे जैसी संवेदनशील जानकारी प्राप्त कर ली जाती है। फिशिंग हमलावर संदेश प्राप्तकर्ता को एक वेब पेज (प्रतिरूप वेब पेज) की ओर निदेशित करता है जिसे पूर्णत: इस ढंग से तैयार किया जाता है कि वह किसी संगठन (अक्सर बैंक और वित्तीय संस्थान) की अपनी वेबसाइट की तरह दिखता है और तत्पश्चात् वे चालाकी से उपभोक्ता की निजी सूचना एकत्र कर लेते हैं और पीड़ित व्यक्ति को अक्सर इस हमले के बारे में पता भी नहीं होता है। यह हमला सामान्यत: नि:शुल्क अथवा सशुल्क फिशिंग किट का प्रयोग करके किया जाता है इस किट में स्क्रिप्ट, इमेजिस, वेब सरवर कोड और वेब पेज होते हैं। सशुल्क किट अपने विक्रेताओं को गुप्तद्वार (बैकडोर) से चोरी किए गए डाटा की फाइलें प्राप्त करने की अनुमति देती है। जहां इसे होस्ट किया जाता है वहां यह सरवर में भी हेरफेर कर सकती है। स्कैमर्स फिशिंग वेबसाइट की लिंकों के वितरण के लिए सोशल मीडिया वेबसाइट्स, स्पैम ई-मेल, इन्स्टैंट मैसिजिंग सर्विसेज, ब्लॉग्स और टैक्स्ट मैसिजिस का प्रयोग करते हैं।

भारत के बाहर अन्तर्राष्ट्रीय पीओएस टर्मिनलों पर छलपूर्ण वित्तीय लेन-देन

ऐसी अनेक घटनाएं हुई हैं जिनमें धोखेबाजों ने भारतीय बैंकों के उपभोक्ताओं के चोरी किए गए ऐसे कार्डों, ट्रैक 2 डाटा, जिनमें कार्ड धारक का नाम, खाता संख्या और अन्य विवेकाधीन डाटा होता है और पिन आधारित प्रमाणीकरण की आवश्यकता नहीं होती है, का प्रयोग करके सफलतापूर्वक लेन-देन किया है।

मोबाइल बैंकिंग का अनुचित लाभ उठाना

मोबाइल बैंकिंग एप्स ने उपभोक्ताओं को मोबाइल फोन अथवा टैबलेट जैसे मोबाइल यंत्रों का प्रयोग करते हुए दूर से ही (रिमोटली) वित्तीय लेन-देन करने में सक्षम बनाया है इन एप्लीकेशन बग्स का निजी पहचान योग्य सूचना को चुराने और छलपूर्वक वित्तीय लेन-देन को करने के लिए भी लगातार प्रयोग किया जा रहा है।

बैंक नेटवर्क प्रणाली और सेवाओं तक पहुंच को निशाना बनाकर व्यवधान उत्पन्न करना

(क) **बिटक्वाइन[3] जबरन वसूली करने वाले (इक्स्टॉर्शनिस्ट) साइबर अपराधी गिरोहों द्वारा डिस्ट्रीब्यूटेड डिनायल ऑफ सर्विस का प्रयोग:** ये हमलावर बड़ी मात्रा में व्यर्थ ट्रैफिक को एक लक्षित नेटवर्क की ओर भेजने के लिए बोटनेट्स[4] का प्रयोग करते हैं ताकि वह उस नेटवर्क को नियंत्रित कर सकें। लक्ष्यों से धन की जबरन वसूली करने का प्रयास करने वाले गिरोह के सदस्य हमला करने से पहले पीड़ितों को यह ई-मेल भेजते हैं कि उन्हें भुगतान कहां और कैसे करना है तथा साथ ही यह भी वादा करते हैं कि यदि वे उनकी बात मानेंगे तो उन्हें फिर से निशाना नहीं बनाया जाएगा। हैकर्स अपनी इन गतिविधियों के संचालन के लिए क्लोज सर्किट टेलीविजन कैमरे (सीसीटीवी) और मोबाइल फोन जैसे यंत्रों का प्रयोग करते हैं।

(ख) **साइबर जबरन वसूली के लिए रैनसमवेयर ट्रोजन्स का प्रयोग:** इसमें हैकर सभी फाइलों को कूट रूप देने (इन्क्रंप्ट) के लिए रैनसमवेयर का प्रयोग करके बैंक के कम्प्यूटरों के नियंत्रण पर कब्जा कर रहे हैं और उनसे नियंत्रण हटाने (अनफ्रीज) के लिए विकोडन (डिक्रिप्शन कीस) हेतु बिटक्वाइन में फिरौती की मांग कर रहे हैं।

एडवान्सड परसिसटेंट थ्रैट (एपीटी) अटैक्स

इसमें बैंक के डाटा में सीधे परिवर्तन करने, मिटाने और/अथवा उन्हें चोरी करने के लिए बैंक की प्रणालियों को सीधे निशाना बनाया जाता है। इसकी विशेषता यह है कि इसे सम्मिश्र, गुप्त और चल रही कम्प्यूटर हैंकिंग प्रक्रियाओं के सेट के रूप में किया जाता है, जिसमें एक विशिष्ट समयावधि में बेइमानी से संवेदनशील लक्षित सूचना निकालने के लिए पहचान से बचने

[3] बिटक्वाइन ऐसी डिजिटल मुद्रा है जिसमें किसी केन्द्रीय बैंक से पृथक रूप से संचालित मुद्रा इकाई के सृजन को विनियमित करने, निधियों के अंतरण की जांच करने के लिए गूढ़लेखन (इनक्रिप्शन) तकनीकों का प्रयोग किया जाता है।

[4] बोटनेट द्वेषपूर्ण (मैलिसियस) सॉफ्टवेयर से संक्रमित और स्पैम भेजने के लिए मालिक की जानकारी के बिना एक समूह के रूप में नियंत्रित निजी कम्प्यूटरों का एक नेटवर्क होता है।

के लिए नेटवर्क में प्रवेश के लिए किसी विशिष्ट निकाय को लक्ष्य बनाया जाता है। एटीपी में विशिष्ट रूप से अनेक चरण शामिल हैं:—

- ऐसे संगठन का चयन करने के लिए व्यापक रिसर्च करना जो ऐसी सूचना प्रौद्योगिकी का इस्तेमाल करते हैं जिसका अनुचित लाभ उठाया जा सकता है।
- निशाना बनाए गए संगठन की सूचना प्रौद्योगिकी की अवसंरचना की रूपरेखा बनाने के लिए फुटप्रिंटिंग करना ताकि उसकी साइट्स, नेटवर्क टोपोलॉजी, डोमेन, इंटरनल डोमेन नेम सिस्टम (डीएनएस) और डायनैमिक होस्ट कॉनफिगरेशन प्रोटोकॉल (डीएचसीपी) सर्वरस, इंटरनल इंटरनेट प्रोटोकॉल ऐड्रेस (आईपी) रेंजेस तथा किन्हीं और पोर्ट्स जिनका अनुचित लाभ उठाया जा सकता है अथवा उन सेवाओं जिन्हें अधिकार में किया जा सकता है का अध्ययन किया जाता है।
- मालवेयर इंजीनियरिंग जिसमें हमलावर अपनी लक्षित संगठन की सूचना प्रौद्योगिकी प्रणालियों और अनुचित लाभ उठाए जा सकने वाली सुभेद्यताओं की पहचान करने के बाद हमले की योजना बनाता है। वे हमला करने के लिए अपेक्षित मुख्य अथवा अनुपूरक मालवेयर को बनाते (इंजीनियर) हैं अथवा अधिप्राप्ति करते हैं।
- आरंभिक भेदन जब हमलावर अपनी लक्षित कंपनी के कर्मचारियों को मालवेयर डाउनलोड करने के लिए मना लेते हैं अथवा न्यायसंगत साधनों से लक्षित नेटवर्क तक पहुंचने के लिए किसी प्रकार की सामाजिक इंजीनियरी का प्रयोग करते हैं। वैकल्पिक तौर पर वे कर्मचारियों द्वारा उपयोग में लाए गए सॉप्टवेयर की कोई जीरो डे वलनरेबिलिटी का उपयोग भी कर सकते हैं।
- लगभग सभी प्रकार के हमलों में एडमिनिस्ट्रेटिव प्रिविलेजों पर कब्जा कर हैकर्स पीड़ित व्यक्ति के कम्प्यूटर के लोकल एडमिनिस्ट्रेटर क्रिडेन्शियल्स को चुराने का प्रयास करते हैं और फलस्वरूप डोमेन-लेवल एडमिनिस्ट्रेटिव क्रिडेन्शियल्स को चुरा लेते हैं।
- प्रिविलेज्ड क्रिडेन्शियल की चोरी और चोरी किए गए डाटा के इच्छित प्रवाह के लिए गुप्त व्यवस्था तथा और अधिक संख्या में सिस्टम्स को संकट में डालने हेतु अधिक मालवेयर डालना।
- हैक, अनधिकार प्रवेश, संकट में डालने और चोरी के डिजिटल प्रमाण को मिटाने के लिए ट्रैकों को कवर करना।

इनसाइडर साइबर अपराध

इनसाइडर साइबर अपराध विभिन्न संगठनात्मक नेटवर्क संसाधनों के एक्सेस के अधिकारों का दुरुपयोग, सामग्रियों की चोरी और भौतिक उपकरणों को गलत ढंग से चलाकर किया जाता है। जानबूझकर तोड़-फोड़, चोरी, जासूसी, छल-कपट और प्रतिस्पर्द्धात्मक लाभ सहित इनसाइडर जोखिमों के कारण बैंकों में कई घटनाएं घटित होती हैं।

साइबर सुरक्षा समस्या का समाधान करने हेतु भारत सरकार द्वारा की गई पहलें

सुरक्षित ऑनलाइन भुगतान प्रणालियों के लिए भारत सरकार ने कई कदम उठाए हैं। वर्ष 2016 में साइबर नियमों के उल्लंघन की घटना के बाद भारतीय रिजर्व बैंक (आरबीआई) ने भी बैंकों को क्या करें और क्या न करें की एक सूची जारी की है। तथापि, साथ ही, यह भी वृहद रूप से स्वीकार किया गया है कि किसी अनिष्ट को रोकने और एक त्रुटि रहित साइबर सुरक्षा सुनिश्चित करने की प्राथमिक जिम्मेदारी ऑनलाइन लेन-देन की सुविधा प्रदान करने वाले अभिकरणों की है।

राष्ट्रीय साइबर सुरक्षा नीति-2013

राष्ट्रीय सुरक्षा सुरक्षा नीति-2013 की मुख्य विशेषताएं इस प्रकार हैं:—

- सूचना पर निगरानी रखने और उसके संरक्षण तथा साइबर हमलों से सुरक्षा तंत्र को मजबूत करने के उद्देश्य से 2 जुलाई, 2013 को भारत सरकार द्वारा राष्ट्रीय साइबर सुरक्षा नीति, 2013 जारी की गई थी। इस प्रारूप दस्तावेज का उद्देश्य नागरिकों, व्यवसायों और सरकार के लिए एक सुरक्षित और लचीला साइबरस्पेस सुनिश्चित करना है।
- साइबर सुरक्षा नीति का उद्देश्य संस्थागत संरचनाओं, लोगों, प्रक्रिया, प्रौद्योगिकी और सहयोग के संयोजन के माध्यम से साइबरस्पेस में सूचना अवसंरचना की रक्षा करना, वलनरेबिलिटी को कम करना, साइबर जोखिमों को रोकने और उस पर कार्यवाही करने हेतु क्षमता निर्माण तथा साइबर घटनाओं से नुकसान को न्यूनतम करना है।
- व्यापक अर्थों में इस नीति का उद्देश्य एक सुरक्षित साइबरस्पेस इकोसिस्टम का सृजन करना तथा नियामक ढांचे को मजबूत करना है। राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केन्द्र [नेशनल क्रिटिकल इंफार्मेशन इंफ्रास्ट्रक्चर प्रोटेक्शन सेंटर] (एनसीआईआईपीसी) के माध्यम से साइबर जोखिमों का सामना करने के लिए एक राष्ट्रीय और क्षेत्रीय चौबीस घंटे (24×7) वाले तंत्र पर बल दिया गया है।
- संकट प्रबंधन प्रयासों के समन्वय हेतु एक नोडल अभिकरण के रूप में कार्य करने के लिए भारतीय कम्प्यूटर आपातकालीन प्रतिक्रिया दल (सीईआरटी-इन) का गठन किया गया है। सीईआरटी-इन क्षेत्रीय सीईआरटी-इन के समन्वय और संचालन के लिए मुख्य संगठन के रूप में भी कार्य करेगा।
- प्रभावी, भविष्यसूचन, निरोधक, प्रतिक्रियाशील और बहाली संबंधी कार्यवाही का परिदृश्य सृजित करके सूचना और संचार प्रौद्योगिकी (आईसीटी) अवसंरचना के प्रति संकट के संबंध में रणनीतिक जानकारी प्राप्त करने हेतु एक तंत्र गठित किए जाने का प्रस्ताव है।
- इस नीति में तकनीकी और संचालन संबंधी सहयोग के माध्यम से प्रभावी सरकारी-निजी साझेदारी और सहयोगपूर्ण कार्य की अपेक्षा की गई है।
- इस नीति में शिक्षण और प्रशिक्षण कार्यक्रमों के माध्यम से मानव संसाधन विकसित करने, सरकारी-निजी साझेदारी के माध्यम से साइबर सुरक्षा प्रशिक्षण अवसंरचना की स्थापना करने और कानून प्रवर्तन अभिकरणों के लिए क्षमता निर्माण हेतु संस्थागत तंत्र की स्थापना करने की अपेक्षा की गई है।
- संगठनों को अपनी कार्य योजनाओं से उचित मेल खाने वाली सूचना सुरक्षा नीतियों को सुचारू रूप से विकसित करने और उन नीतियों को अन्तर्राष्ट्रीय स्तर के संव्यवहारों के अनुसार लागू करने की आवश्यकता है।
- इस नीति दस्तावेज का उद्देश्य सभी संगठनों, चाहे वे सरकारी हो या निजी, को मुख्य सूचना सुरक्षा अधिकारी (सीआईएसओ) के रूप में कार्य करने के लिए एक व्यक्ति को पदनामित करने को बढ़ावा देना है। यह व्यक्ति साइबर सुरक्षा पहलों के लिए उत्तरदायी होगा।

- यह नीति साइबर सुरक्षा के क्षेत्र में शोध और विकास को बढ़ावा देने पर भी बल देती है।

डिजिटल भुगतान के प्रति सुरक्षा चिंताओं का समाधान करने के लिए सरकार द्वारा हाल ही में निम्नलिखित प्रमुख पहलें की गई हैं:—

- सचिव, इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी की अध्यक्षता में तथा सचिव, दूरसंचार विभाग की सहअध्यक्षता में डिजिटल भुगतान सुरक्षा समिति की स्थापना की गई है। इस समिति की प्रथम बैठक 31 मार्च, 2017 को आयोजित की गई थी।
- इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय ने सूचना प्रौद्योगिकी अधिनियम, 2000[5] के अंतर्गत प्रीपेड पेमेंट इंस्ट्रूमेंट्स की सुरक्षा संबंधी नियमों का प्रारूप तैयार किया है। इस प्रारूप नियम में इलेक्ट्रॉनिक प्रीपेड पेमेंट इंस्ट्रूमेंटों के लिए शिकायत समाधान तंत्र हेतु प्रावधान है। इस प्रारूप नियम को इलेक्ट्रॉनिक और सूचना प्रौद्योगिकी मंत्रालय की वेबसाइट पर प्रकाशित किया गया है और जनता एवं सभी पक्षकारों से टिप्पणियां मांगी गई हैं।
- चुनौतियों का सामना करने और डिजिटल पेमेंट इकोसिस्टम की साइबर सुरक्षा स्थिति के सुधार हेतु मंत्रालय में डिजिटल भुगतान प्रभाग की स्थापना की गई है।

भारत में साइबर सुरक्षा हेतु संस्थागत ढांचा

भारतीय कम्प्यूटर आपातकालीन प्रतिक्रिया दल (सीईआरटी-इन)

भारतीय कम्प्यूटर आपातकालीन प्रतिक्रिया दल (सीईआरटी-इन) इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय के तहत एक कार्यरत संगठन है, जिसका उद्देश्य भारतीय साइबर स्पेस की सुरक्षा को सुनिश्चित करना है। सीईआरटी-इन घटना रोधक और प्रतिसंवेदी सेवाओं के साथ-साथ सुरक्षा गुणवत्ता प्रबंधन सेवाएं भी प्रदान करता है। सीईआरटी-इन नियमित आधार पर अद्यतन साइबर जोखिमों और उनके बचाव के संबंध में चेतावनी और परामर्श जारी करता है। इस संगठन ने निम्नलिखित पहलें की हैं:—

- सीईआरटी-इन ने केन्द्र सरकार के सभी मंत्रालयों/विभागों, राज्य सरकारों और उनके संगठनों तथा अन्य महत्वपूर्ण क्षेत्रों द्वारा कार्यान्वयन हेतु साइबर हमलों और साइबर आतंकवाद का सामना करने के लिए एक साइबर संकट प्रबंधन योजना (साइबर क्राइसिज़ मैनेजमेंट प्लान) (सीसीएमपी) तैयार की है। सीईआरटी-इन नियमित रूप से सीसीएमपी के कार्यान्वयन हेतु भारतीय रिजर्व बैंक (आरबीआई) बैंकिंग तकनीकी में विकास और शोध हेतु संस्थान [इंस्टीट्यूट फॉर डेवलपमेंट एंड रिसर्च इन बैंकिंग टेक्नोलॉजी (आईडीआरबीटी)] एवं बैंकों से चर्चा करता रहता है।
- साइबर सुरक्षा अभ्यास अनुरूपी और अनुमानित साइबर सुरक्षा की घटना की स्थितियों के आधार पर विश्वास निर्माण और सीखने का अभ्यास है। अभ्यास का इरादा मुख्य क्षेत्रों में सीईआरटी-इन और संगठनों के बीच इंटरफेस में सहयोगी और समन्वयक बनना है। सरकारी और महत्वपूर्ण क्षेत्रों में साइबर सुरक्षा की स्थिति के मूल्यांकन और संगठनों की तैयारी के लिए सीईआरटी-इन द्वारा नियमित रूप से साइबर सुरक्षा अभ्यास आयोजित किए जाते हैं। वर्ष 2016 में सीईआरटी-इन द्वारा दो वित्त क्षेत्र विशिष्ट साइबर सुरक्षा अभ्यास आयोजित किए थे।
- सूचना प्रौद्योगिकी संबंधी अवसंरचना को सुरक्षित रखने के लिए सीईआरटी-इन ने कुछ दिशा-निर्देशों का प्रकाशन किया है, जो इसकी वेबसाइट (www.certin.org.in) पर उपलब्ध हैं। देश के बाहर से होने वाले विभिन्न प्रकार के साइबर हमलों और खतरों का पता लगाने के लिए समय-समय पर साइबर स्पेस की बारीकी से जांच की जाती है।
- साइबर स्वच्छता केन्द्र (बोटनेट क्लीनिंग एंड मैलवेयर एनालिसिस सेंटर) की स्थापना सीईआरटी-इन द्वारा फरवरी 2017 में की गई थी, जिसका उद्देश्य भारत में संकटकारी प्रणालियों का पता लगाना तथा मैलवेयर संक्रमण को बढ़ने से रोकना है। यह केन्द्र इंटरनेट सेवा प्रदाताओं, शिक्षाविदों और उद्योग जगत के साथ घनिष्ठ समन्वय और सहयोग से कार्य करता है। केन्द्र आम उपयोगकर्ताओं के लिए उनके सिस्टम में संक्रमित कार्यक्रमों का पता लगाकर उन्हें हटाने के लिए उपकरण प्रदान करता है। यह केन्द्र बैंकों के साथ मिलकर उनके नेटवर्क में मैलवेयर संक्रमण का पता लगाने और सुधारात्मक कदम उठाने का कार्य भी कर रहा है।
- सीईआरटी-इन भारतीय रिजर्व बैंक, नेशनल पेमेंट कार्पोरेशन ऑफ इंडिया (एनपीसीआई) और पेमेंट कार्ड इंडस्ट्री ऑरगनाइजेशन जैसी संस्थाओं को नियमित रूप से बैंकिंग और एटीएम प्रणालियों पर लक्षित खतरों के संबंध में परामर्श जारी करता है। परामर्श में आईसीटी प्रणालियों की सुरक्षा सुदृढ़ करने के लिए सर्वोत्तम प्रथाओं को कवर किया जाता है। वित्तीय क्षेत्र के लिए, सीईआरटी-इन ने पॉइंट ऑफ सेल (पीओएस), माइक्रो, एटीएमस, इलेक्ट्रॉनिक वैलेटस, ऑन लाइन बैंकिंग, स्मार्ट फोन, यूनिफाइड पेमेंट इंटरफेस, अनस्ट्रक्चर्ड सप्लीमेंटरी सर्विस डाटा (यूएसएसडी), रूपे, सिम कार्ड, वायरलेस एक्सेस पॉइंटस/राउटरस, मोबाइल बैंकिंग, क्लाउड और आधार अनेबल्ड पेमेंट सिस्टम (एईपीएस) को कवर करते हुए सुरक्षा की दृष्टि से सुरक्षापायों संबंधी 23 परामर्श जारी किये हैं।
- सीईआरटी-इन सूचना प्रौद्योगिकी अवसंरचना की सुरक्षा और साइबर हमलों को कम करने के संबंध में नेटवर्क और सिस्टम एडमिनिस्ट्रेटर को जानकारी देने के लिए नियमित रूप से प्रशिक्षण कार्यक्रम आयोजित करता है। वर्ष 2016 के दौरान 580 प्रतिभागियों के लिए इस प्रकार के 18 प्रशिक्षण कार्यक्रम आयोजित किये गये।
- सीईआरटी-इन साइबर सुरक्षा संबंधी इंटर-डिसिप्लिनरी स्थायी समिति के सदस्य के रूप में विभिन्न सुरक्षा मानदंडों/प्रोटोकॉल अपनाने संबंधी अध्ययनों द्वारा वर्तमान/उभरती हुई प्रौद्योगिकी में आने वाले खतरों की समीक्षा करने में योगदान देता है; सभी हितधारकों के साथ इंटरफेस द्वारा जुड़ता है तथा साइबर सुरक्षा को सुदृढ़ करने और वित्तीय क्षेत्र में लचीलापन लाने के लिए उचित नीति बनाने के संबंध में सुझाव भी देता है।

[5] संसद का एक अधिनियम जिसका उद्देश्य हर ऐसे लेन-देन को कानूनी मान्यता देने का प्रावधान करना है, जिन्हें इलेक्ट्रॉनिक आंकड़ों के आदान-प्रदान और सूचना तकनीक के अन्य माध्यमों से किया गया है और जिसे आमतौर पर ''इलेक्ट्रॉनिक कॉमर्स'' के नाम से जाना जाता है। इलेक्ट्रॉनिक कॉमर्स सूचना के आदान-प्रदान और उसके संग्रहण के लिए कागज आधारित माध्यमों के विकल्प के रूप में इलेक्ट्रॉनिक माध्यम का इस्तेमाल करता है। इससे सरकारी संस्थानों में भी इलेक्ट्रॉनिक माध्यम से दस्तावेजों का आदान-प्रदान संभव हो सकता है और इंडियन पेनल कोड, इंडियन एविडेंस एक्ट, 1872, बैंकर्स बुक्स एविडेंस एक्ट, 1891 और रिजर्व बैंक ऑफ इंडिया एक्ट 1934 अथवा इससे प्रत्यक्ष या परोक्ष रूप से जुड़े किसी भी कानून में संशोधन में भी इन दस्तावेजों का उपयोग हो सकता है। इस अधिनियम को बाद में सूचना तकनीक (संशोधन) अधिनियम, 2008 के रूप में संशोधित किया गया।

- साइबर सुरक्षा के संबंध में आईडीआरबीटी के साथ मिलकर बैंकों, आरबीआई, भारतीय प्रतिभूति एवं विनिमय बोर्ड (सेबी) के लिए नियमित रूप से कार्यशालाएं आयोजित की जाती हैं। आईडीआरबीटी में सीईआरटी-इन के अधिकारियों को प्रशिक्षकों के रूप में नियुक्त किया जाता है।

फाइनेंशियल कम्प्यूटर इमरजेंसी रिस्पांस टीम (सीईआरटी-फिन)

वर्ष 2017 में भारत के वित्त मंत्री द्वारा वित्तीय क्षेत्र में कम्प्यूटर इमरजेंसी रिस्पांस टीम (सीईआरटी-फिन) के गठन की घोषणा यह दर्शाती है कि भारत सरकार वित्तीय क्षेत्र में साइबर सुरक्षा को बहुत महत्व देती है। प्रस्तावित सीईआरटी-फिन योजना का उद्देश्य एक एकीकृत साइबर सुरक्षा ढांचे की स्थापना कर देश के प्रमुख वित्तीय विनियामकों, संस्थानों और हितधारकों को सुरक्षा रिस्पांस इकाई के साथ जोड़ना है। इससे भारत के वित्तीय क्षेत्र को प्रभावित कर सकने वाले साइबर अपराधों और खतरों से जुड़ी किसी वारदात और घटना के प्रति बेहतर समन्वय, नियंत्रण और प्रतिक्रिया करने में सहायता मिलेगी।

सीईआरटी-फिन के लागू होने से आधुनिक डिजिटल सुरक्षा, सामर्थ्य और नियंत्रण का विकास होगा जिससे डाटा सुरक्षा और गोपनीयता के क्षेत्र में भारत पूरे विश्व में अग्रणी और अनुकरणीय बनेगा। यह पूरे देश में सामान्य सुरक्षा संबंधी जागरूकता बढ़ाने मे भी सहायक होगा तथा भारत में वित्तीय क्षेत्र में मुख्य सूचना अधिकारियों (सीआईओस) और मुख्य सूचना सुरक्षा अधिकारियों (सीआईएसओस) को तथा सुरक्षा विशेषज्ञों को एकजुट करने में भी महत्वपूर्ण भूमिका निभाएगा ताकि एक प्रभावशाली साइबर सुरक्षा फ्रेमवर्क के लिए एक सहयोगपूर्ण मंच तैयार किया जा सके। सबसे अधिक महत्वपूर्ण यह है कि सीईआरटी-फिन मजबूत डाटा संरक्षण नीतियों और सुरक्षा ढांचे के कार्यान्वयन और अनिवार्य सुरक्षा प्रथाओं या नीतियों को लागू करने में भी सहायक होगा, जिनका वित्तीय संस्थानों को पालन करना आवश्यक होगा।

विनियामकों द्वारा की गयी पहलें

1. भारतीय रिजर्व बैंक (आरबीआई)

भारत में बैंकों पर साइबर हमलों की घटनाओं में हुई वृद्धि को देखते हुए, आरबीआई ने बैंकों में साइबर सुरक्षा की तैयारियों को सुदृढ़ करने के लिए अनेक मुख्य पहलें की हैं और महत्वपूर्ण कदम उठाए हैं। आरबीआई ने 2 जून 2016 को साइबर सुरक्षा फ्रेमवर्क संबंधी एक व्यापक परिपत्र जारी किया था, जिसमें साइबर सुरक्षा के विभिन्न पक्षों से संबंधित सर्वोत्तम प्रथाओं को कवर किया गया था। साइबर सुरक्षा फ्रेमवर्क की कुछ महत्वपूर्ण विशेषताएं निम्नवत् हैं:

- बैंकों के जोखिम को चार श्रेणियों-कम, माध्यम, उच्च और बहुत अधिक के रूप में वर्गीकृत करना होगा तथा अपने सर्वर/नेटवर्क में किसी असामान्य व्यवहार की सूचना अनिवार्य रूप से तुरंत आरबीआई को देनी होगी।
- निरंतर निगरानी और साइबर खतरों से संबंधित नवीनतम जानकारी हेतु बैंकों को सुरक्षा संचालन केन्द्र (एसओसी) की स्थापना करनी होगी।
- आईटी वास्तुकला, जिसे इस प्रकार की नीति के सुचारू कार्यकरण में सहायक होना चाहिये, की निरंतर समीक्षा होनी चाहिये।
- बैंकों को साइबर संकट प्रबंधन योजना (सीसीएमपी) लागू करनी होगी। सीसीएमपी में चार घटक अनिवार्य हैं- (1) डिटेक्शन (पता लगाना) (2) रिस्पांस (प्रतिक्रिया) (3) रिकवरी (बहाली) और (4) कंटेनमेंट (नियंत्रण)। साइबर ढांचे के लचीलेपन की समुचित जांच करते समय कुछ संकेतक विकसित किये जाने चाहिये और यह जांच स्वतंत्र एवं योग्य पेशेवरों द्वारा कराई जानी चाहिये। इसके अतिरिक्त बैंकों को सभी हितधारकों के बीच साइबर सुरक्षा संबंधी जागरूकता बढ़ाने के निर्देश भी दिये गये हैं।
- न्यूनतम साइबर सुरक्षा और आवश्यक लचीलेपन तथा सुरक्षा संचालन केन्द्र के गठन और संचालन हेतु दिशा-निर्देश स्पष्ट कर दिये गये हैं।

इसके अतिरिक्त आरबीआई सीईआरटी-इन के सहयोग से समय-समय पर साइबर ड्रिल का भी आयोजन कराता है। जैसा कि वर्ष 2016-17 के लिए बैंक की छठी द्विमासिक मॉनीटरी पॉलिसी स्टेटमेंट में घोषणा की गयी है, वर्तमान/उभरती हुई प्रौद्योगिकी में आने वाले खतरों की समीक्षा हेतु; विभिन्न सुरक्षा मानदंडों/प्रोटोकाल अपनाने संबंधी अध्ययन हेतु; सभी हितधारकों के साथ हस्तक्षेप करके तथा साइबर सुरक्षा और लचीलेपन को सुदृढ़ करने के लिये उचित नीतिगत सुझाव देने हेतु साइबर सुरक्षा संबंधी इंटर-डिसिप्लिनरी स्थायी समिति का गठन किया गया है। समिति की नियमित बैठकें होती हैं और इसकी सिफारिशों के अनुरूप गहराई से जांच हेतु कुछ प्रमुख क्षेत्रों के लिये उप-समूह बनाये जाते हैं। आरबीआई ने रिजर्व बैंक सूचना प्रौद्योगिकी प्रा. लि. नामक एक आनुषंगिक आईटी निकाय भी स्थापित किया है जो अन्य बातों के साथ-साथ आरबीआई और अन्य विनियमित संस्थाओं में साइबर सुरक्षा पर ध्यान केन्द्रित करता है। आरबीआई ने प्रमुख बैंकों की साइबर जोखिम संबंधी लचीलेपन और प्रतिक्रिया का आकलन करने के लिए इनकी विस्तृत आईटी जांच भी की है। आरबीआई बैंकों द्वारा की गयी सुधारात्मक कार्यवाही की निगरानी भी करता है।

2. भारतीय प्रतिभूति एवं विनिमय बोर्ड (सेबी): सेबी द्वारा साइबर सुरक्षा संबंधी एक उच्च स्तरीय निगरानी समिति का गठन किया गया है। समिति के प्रमुख कार्य इस प्रकार हैं:—

- सेबी और सम्पूर्ण पूंजी बाजार की साइबर सुरक्षा पहलों की निगरानी और सम्पूर्ण मार्गदर्शन प्रदान करना;
- सेबी को भारतीय पूंजी बाजार संरचना की आवश्यकता के अनुसार वैश्विक सर्वोत्तम प्रथाओं और औद्योगिक मानदंडों के साथ साइबर सुरक्षा और आवश्यक साइबर लचीलेपन के विकास और इसे बनाए रखने हेतु सलाह देना;
- साइबर लचीलेपन और संबंधित कार्यों तथा भारतीय प्रतिभूति बाजार में डिसास्टर रिकवरी प्रक्रिया में सुधार हेतु उपाय खोजना;
- भारतीय प्रतिभूति बाजार में साइबर सुरक्षा और लचीले साइबर ढांचे की जांच के लिए प्रक्रियाओं को सुदृढ़ करने हेतु सिफारिशें करना;
- समय-समय पर एसओसी (सुरक्षा संचालन केन्द्र) के अधिदेश और कार्यकरण की समीक्षा करना और प्रतिभूति बाजार हेतु साइबर प्रयोगशाला/साइबर उत्कृष्टता केन्द्र की स्थापना करने में सेबी का मार्गदर्शन करना;
- घरेलू और वैश्विक बाजारों में वित्तीय बाजारों से संबंधित बड़े साइबर हमले की घटनाओं का अध्ययन करना और मौजूदा साइबर सुरक्षा और लचीले साइबर ढांचे में खामियों की पहचान करना;

- साइबर सुरक्षा और साइबर लचीलेपन को और सुदृढ़ बनाने के लिए बाह्य एजेंसियों जैसे सीईआरटी-इन (इंडियन कम्प्यूटर इमरजेंसी रेस्पान्स टीम), राष्ट्रीय साइबर समन्वय केन्द्र (एनसीएससी)/राष्ट्रीय सुरक्षा परिषद सचिवालय (एनएससीएस), दूरसंचार विभाग (डीओटी) इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय (एमईआईटीवाई), प्रमुख शैक्षिक संस्थानों और संगठनों आदि से निरंतर संवाद करना।

साइबर सुरक्षा और बीमा कंपनियां

बीमाकर्ताओं के लिए साइबर सुरक्षा जोखिम, एक गंभीर चिंता के रूप में उभरे हैं क्योंकि साइबर सुरक्षा संबंधी घटनाएं उनके व्यवसाय संचालन की क्षमता को हानि पहुंचा सकती हैं; निजी और स्वामित्व संबंधी ब्यौरे की सुरक्षा के लिए खतरा पैदा कर सकती है और बीमा क्षेत्र में विश्वास में कमी ला सकती हैं। अत:, यह सुनिश्चित करना आवश्यक है कि बीमाकर्ताओं हेतु सूचना और साइबर सुरक्षा के लिए एक समान तंत्र लागू किया जाए और समय-समय पर ऐसे सुरक्षा संबंधी मुद्दों का समाधान करने के लिए विनियमित निकायों के भीतर एक अंतर्निहित शासन तंत्र विकसित किया जाए।

भारतीय बीमा विनियामक और विकास प्राधिकरण (आईआरडीएआई) ने बीमा क्षेत्र में साइबर सुरक्षा स्थिति की समीक्षा के संबंध में राष्ट्रीय सुरक्षा परिषद सचिवालय (एनएससीएस) और अनेक साधारण बीमा तथा जीवन बीमा कंपनियों के साथ अनेक बैठकें करने के पश्चात् सूचना और साइबर सुरक्षा के संबंध में 7 अप्रैल, 2017 को सभी बीमा कंपनियों को दिशा-निर्देश जारी किए हैं। ये दिशा-निर्देश सभी बीमाकर्ताओं पर लागू हैं और मध्यस्थों तथा अन्य विनियमित निकायों, जिनके साथ बीमाधारकों की जानकारी साझा की जा रही है, के मामले में सूचना और साइबर सुरक्षा संबंधी मुद्दों पर ध्यान देने के लिए सक्षम तंत्रों की स्थापना करने की जिम्मेदारी बीमाकर्ताओं की होगी। दिशा-निर्देशों की मुख्य विशेषताएं इस प्रकार हैं:—

- मुख्य सुरक्षा अधिकारी की नियुक्ति करना, जो उनकी सूचनाओं की सुरक्षा करने के लिए नीतियां बनाने और लागू करने तथा सूचना सुरक्षा समिति (आईएससी) के गठन के लिए जिम्मेदार होगा।
- कमियों के विश्लेषण संबंधी रिपोर्ट तैयार करने के अतिरिक्त साइबर संकट प्रबंधन योजना तैयार करना।
- बोर्ड द्वारा अनुमोदित सूचना और साइबर सुरक्षा नीति को अंतिम रूप देना।
- बोर्ड द्वारा अनुमोदित सूचना और साइबर सुरक्षा नीति के अनुरूप सूचना और साइबर सुरक्षा आश्वासन कार्यक्रम (कार्यान्वयन योजना/दिशा-निर्देश) तैयार करना।
- प्रथम व्यापक सूचना और साइबर सुरक्षा आश्वासन जांच को पूरा करना।

निष्कर्ष

एक व्यापक साइबर सुरक्षा संदर्भ में, वित्तीय क्षेत्र में साइबर सुरक्षा सुनिश्चित करना वित्तीय और बैंकिंग क्षेत्र, जो हमारे जैसी विकासशील और बदलती हुई अर्थव्यवस्था के महत्वपूर्ण स्तम्भ हैं, में सुरक्षा व्यवस्था को बढ़ाने और मजबूत करने की दिशा में एक निर्णायक कदम है। जैसाकि पूरे विश्व में हुई विभिन्न घटनाओं से पता चलता है, साइबर खतरों की कोई भौगोलिक अथवा संस्थागत सीमाएं नहीं होती। वित्तीय क्षेत्र में विभिन्न बाजार भागीदार बड़े पैमाने पर एक दूसरे पर निर्भर होते हैं। ऐसी स्थिति में, साइबर जोखिमों के संकट से निपटने और यह सुनिश्चित करने के लिए कि आर्थिक व्यवधानों से वित्तीय स्थिरता के लिए कोई खतरा पैदा न हो, एक समन्वित दृष्टिकोण होना आवश्यक है। इसके अतिरिक्त, लोगों को पासवर्ड प्रबंधन और साइबर सुरक्षा संबंधी जानकारी के बारे में जागरूक करना आवश्यक है। विशेषज्ञों ने भारत के नाभिकीय निवारण सिद्धान्त के अनुसार एक साइबर निवारण सिद्धान्त तैयार करने का सुझाव दिया है।

संदर्भ

- भारत सरकार, वित्त मंत्रालय, मंत्रालय द्वारा उपलब्ध कराई गई टिप्पणियां/जानकारी।
- भारत सरकार, इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय द्वारा उपलब्ध कराई गई टिप्पणियां/जानकारी।
- भारत सरकार, इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय, राष्ट्रीय साइबर सुरक्षा नीति-2013
- अंकित सिन्हा और हर्षित दुसाद, साइबर सिक्यूरिटी इन इंडिया: नीड फॉर एन एडवांस्ड फ्रेमवर्क, बार एंड बेंच, 21 मार्च 2017
- अकीलस ए. अलमांसी, फाइनेंशियल सैक्टर साइबर सिक्यूरिटी: हु इज इनचार्ज, वर्ल्ड बैंक
- सीसीजी एनएलयू दिल्ली, साइबर सिक्यूरिटी इन द फाइनेंशियल सैक्टर: एन ओवरव्यू (http://www.legallyindia.com), 8 फरवरी, 2017
- कान्फ्रेंस ऑफ स्टेट बैंक सुपरवाइजर्स (सीएसबीएस), साइबर सिक्यूरिटी 101: ए रिसार्स गाइड फॉर बैंक एक्जीक्यूटिव्स, एक्जीक्यूटिव लीडरशिप ऑफ साइबर सिक्यूरिटी।
- साइबर सिक्यूरिटी फॉर द फाइनेंशियल सैक्टर, (http://www.nccgroup.trust/uk)
- यूरोपियन फाइनेंशियल सर्विसेज राउंड टेबल, ईएफआर पेपर ऑन साइबर सिक्यूरिटी
- जी-7 फंडामेंटल एलीमेंट्स ऑफ साइबर सिक्यूरिटी फार द फाइनेंशियल सैक्टर (http://www.ecb.europa.eu)
- मो. उजले, साइबर सिक्यूरिटी फर्मस् लाउड गवर्नमेंट मूव टू सेट अप सीईआरटी फॉर फाइनेंशियल सैक्टर, (http://computer.expressbpd.com) 3 फरवरी, 2017
- पंकज मारु, व्हाट सॉफ्टवेयर सिक्यूरिटी इंडस्ट्री थिंक ऑफ इंडियास सीईआरटी प्लान फॉर फाइनेंस सैक्टर? (http://cio.economictimes.indiatimes.com), 2 फरवरी, 2017
- पुरुषोत्तम नायडु, ड्रीम डिजिटल इंडिया? लेट अस सिक्यूर ऑवर बैंकिंग फ्रोम साइबर अटैक्स फर्स्ट (http://factordaily.com) 22 दिसम्बर, 2016
- संजीव तोमर, नेशनल साइबर सिक्यूरिटी पालिसी, 2013: एन एसेसमेंट, (http://www.idsa.in), 26 अगस्त, 2013

संसद सदस्यों के उपयोग के लिए इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी तथा वित्त मंत्रालय और अन्य प्रकाशित स्रोतों से प्राप्त जानकारी के आधार पर लोक सभा सचिवालय के शोध और सूचना प्रभाग के आर्थिक और वित्तीय कार्य स्कंध द्वारा तैयार किया गया है। इस बुलेटिन का हिन्दी संस्करण अनुवाद (प्रकाशन) शाखा द्वारा तैयार किया गया है।