*निरापद वित्तीय प्रणाली के लिए साइबर सुरक्षा**

एम के जैन

कंप्यूटर इमरजेंसी रिस्पांस टीम – आईएन (सीईआरटी-आईएन) के महानिदेशक डॉ. संजय बहल, आईएमएफ, बीआईएस के विशिष्ट अतिथि, अन्य केंद्रीय बैंकों और सीईआरटी के प्रतिनिधि, भारतीय बैंकों के एमडी/सीईओ और उनकी टीम के सदस्य, वैश्विक विदेशी बैंकों के सीआईएसओ और सीटीओ, आरबीआई के मेरे सहयोगी, देवियो और सज्जनो। आप सबको नमस्कार!

मैं, साइबर सुरक्षा के महत्वपूर्ण क्षेत्र, जो इस त्वरित डिजिटल युग में ज्यादा प्रासंगिक हो गया है, पर विचार-विमर्श करने हेतु इस महत्वपूर्ण कार्यक्रम में शामिल होने के लिए आप सभी को धन्यवाद देता हूं। जैसे-जैसे वित्तीय लेनदेन डिजिटल प्लेटफ़ॉर्म पर स्थानांतरित होते हैं, सूचना प्रौद्योगिकी अवसंरचना पर निर्भरता तेजी से बढ़ती है। जहां यह बदलाव सुविधा और दक्षता लाता है, वहीं इससे जोखिमों का खतरा भी बढ़ता है। पैसों की ठगी के लिए साइबर अपराधी डिजिटल सिस्टम की कमजोरियों का लगातार फायदा उठाते हैं, सुरक्षा में सेंध लगाने और मूल्यवान डेटा तक अनधिकृत पहुंच हासिल करने की कोशिश करते हैं।

इस परस्पर जुड़ी हुई दुनिया में, जहां वित्तीय लेनदेन कुछ ही सेकेंड में महाद्वीपों को पार कर जाते हैं, साइबर खतरों से निपटने में अंतरराष्ट्रीय सहयोग की आवश्यकता आवश्यक हो गई है। बैंकों को निशाना बनाने वाले साइबर हमले न केवल व्यक्तिगत संस्थानों की स्थिरता को खतरे में डालते हैं, बल्कि वित्तीय प्रणालियों को भी बाधित करने की क्षमता रखते हैं। इसलिए राष्ट्रों को एक साथ मिलकर इस गंभीर चुनौती का समाधान करना जरूरी है। भारत द्वारा जी20 की अध्यक्षता में यह आयोजन बैंकिंग क्षेत्र में साइबर सुरक्षा के मुद्दों के समाधान के लिए विभिन्न अंतरराष्ट्रीय निकायों के प्रयासों का पूरक प्रयास होगा।

प्रौद्योगिकी का महत्व

प्रौद्योगिकी वित्तीय क्षेत्र को आकार देने, अधिक दक्षता, पहुंच और सामर्थ्य को सक्षम करने में एक प्रेरक शक्ति रही है। हालाँकि, वर्तमान फिनटेक क्रांति कई मायनों में अद्वितीय है, जिसे बढ़ी हुई कंप्यूटिंग शक्ति और नई प्रौद्योगिकियों के अनुप्रयोग से तैयार किया गया है। इसके अलावा, नए प्रवेशकर्ता और नवीन व्यवसाय मॉडल का उदय हो रहा है।

पहले, वित्तीय सेवाओं के डिजिटलीकरण ने बैंकों और वित्तीय संस्थानों को अपने उपभोक्ताओं से संबंधित व्यवस्थित डेटा रखना सुलभ बनाया था, जिसका उपयोग ग्राहक की जोखिम प्रोफ़ाइल को समझने के लिए किया जाता था। हालाँकि, बिग डेटा एनालिटिक्स के उद्भव के साथ, वैकल्पिक अर्ध-व्यवस्थित और अव्यवस्थित डेटा का उपयोग करके ग्राहकों की प्राथमिकताओं और व्यवहार के बारे में और भी बेहतर जानकारी प्राप्त की जा सकती है।

डेटा को अक्सर उसकी मूल्यवत्ता, आर्थिक संवृद्धि और नवोन्मेष को प्रेरित करने की क्षमता और जिम्मेदारी से उपयोग किए जाने पर सकारात्मक प्रभाव के कारण "नया तेल" कहा जाता है। हालाँकि, जब यह लापरवाह तरीके से उपयोग किया जाता है, तो कई नकारात्मक परिणाम सामने आते हैं, जैसे- गोपनीयता का उल्लंघन, पहचान की चोरी और धोखाधड़ी, लक्षित विज्ञापनों का उपयोग करके हेर-फेर, आदि। वास्तव में, डेटा का लापरवाह उपयोग न केवल व्यक्तियों के लिए जोखिम पैदा करता है, बल्कि डिजिटल परितंत्र में विश्वास को भी कमजोर करता है और यहां तक कि इससे वित्तीय स्थिरता और राष्ट्रीय सुरक्षा भी प्रभावित हो सकते हैं।

वित्तीय स्थिरता की दुर्बलताओं को समझना

साइबर परिप्रेक्ष्य में उभरने वाली वित्तीय स्थिरता की दुर्बलताओं को समझना महत्वपूर्ण है क्योंकि मौजूदा पूंजी और चलनिधि प्रविधियां किसी साइबर घटना के प्रभाव को उसी तरह कम नहीं कर सकते हैं जिस तरह वे वित्तीय घाटे को कम करते हैं। उदाहरण के लिए, पूंजी और चलनिधि, साइबर घटना का मुकाबला करने के लिए वित्तीय संसाधन प्रदान कर सकते हैं लेकिन सिस्टम या डेटा को पुनर्प्राप्त करने की प्रक्रिया को गति नहीं दे सकते।

साइबर हमले बैंकों के भीतर महत्वपूर्ण वित्तीय कार्यों को बाधित कर सकते हैं, जिससे वे लेनदेन संसाधित करने, ग्राहक

* श्री एम के जैन, उप गवर्नर, भारतीय रिज़र्व बैंक का मुख्य भाषण - मुंबई में भारत के जी20 की अध्यक्षता के तहत एक अंतरराष्ट्रीय कार्यक्रम - 'बैंकिंग क्षेत्र के लिए साइबर सुरक्षा अभ्यास' - 5 जून 2023।

खातों तक पहुंचने या आवश्यक कार्यों को निष्पादित करने में असमर्थ हो सकते हैं। इस व्यवधान के परिणामस्वरूप बैंकिंग प्रणाली में जनता का भरोसा कम हो सकता है, क्योंकि ग्राहकों और कारोबारियों को धन प्राप्त करने या सामान्य वित्तीय गतिविधियां निपटाने में कठिनाइयों का सामना करना पड़ सकता है। इस तरह के व्यवधान वित्तीय अस्थिरता का कारण बन सकते हैं - खासकर यदि वे कई बैंकों को प्रभावित करते हैं या लंबे समय तक चलते हैं।

पेशकश की जाने वाली सेवाओं में बढ़ोतरी, जैसे कि भुगतान प्रणालियों के लंबे परिचालन घंटे और छोटी समाशोधन और निपटान विंडो, वित्तीय प्रणाली में ऐसे कम सेवा अवकाश छोड़ते हैं, जिनमें साइबर घटना के बाद परिचालन को बहाल की जा सके। किसी घटना की प्रकृति और सीमा के बारे में अनिश्चितता प्रतिपक्षियों, प्रतिस्पर्धियों, या वित्तीय इकाई के संचालन से अप्रभावित क्षेत्रों पर भी असर डाल सकती है।

दरअसल, कॉलेनियल पाइपलाइन पर 2021 के रैंसमवेयर हमले ने, हालांकि यह एक वित्तीय इकाई नहीं है, महत्वपूर्ण बुनियादी ढांचा प्रणालियों के अंतर्संबंध और बैंकिंग सहित विभिन्न क्षेत्रों पर संभावित व्यापक प्रभावों पर प्रकाश डाला। इसमें दर्शाया गया है कि कैसे एक साइबर हमला, इस मामले में, चालू गैस स्टेशनों के लिए खतरा उत्पन्न कर सकता है, जो मूल आघात से कहीं व्यापक दुष्प्रभाव है।

हालाँकि इकाई-स्तरीय साइबर सुदृढ़ता पर लगातार बृहत् पर्यवेक्षी ध्यान दिया जा रहा है, फिर भी डेटा विसंगतियां बनी हुई हैं। साइबर घटनाओं के संबंध में नियमित इकाई स्तरीय डेटा की आवश्यकता है। सिस्टम स्तर पर, डिजिटल अंतर-निर्भरता के प्रासंगिक डेटा माप और गति जिससे बैकअप सिस्टम को जल्द सक्षम किया जा सकता है, आवश्यक है।

साइबर सुरक्षा और डिजिटल वित्तीय समावेशन

साइबर जोखिम, वित्तीय समावेशन प्रयासों पर भी महत्वपूर्ण प्रभाव डाल सकते हैं। वित्तीय समावेशन का उद्देश्य वंचित और हाशिए पर मौजूद आबादी के लिए वित्तीय सेवाओं तक पहुंच प्रदान करना है, और डिजिटल सार्वजनिक बुनियादी ढांचे द्वारा इस क्षेत्र में तेजी से प्रगति हुई है। हालाँकि, साइबर सुरक्षा के बारे में जागरूकता की कमी के कारण इस आबादी को साइबर जोखिमों से खतरा है।

यदि व्यक्तियों को वित्तीय समावेशन के नाम पर ऑनलाइन लाया जाता है तो वे साइबर खतरे के संपर्क में आ सकते हैं, जिससे वे उबर नहीं सकते। डिजिटल वित्तीय समावेशन को सफल बनाने के लिए, लोगों को डिजिटल अर्थव्यवस्था में लाना ही पर्याप्त नहीं है। सभी हितधारकों को यह भी सुनिश्चित करना चाहिए कि लोग उन जोखिमों से प्रतिरक्षित हों, जो सामने आ सकतीं हैं।

भारतीय परिप्रेक्ष्य

मैं इस अवसर का उपयोग भारतीय परिप्रेक्ष्य को साझा करने के लिए करना चाहूंगा। वित्तीय उत्पादों और सेवाओं के नवोन्मेष और डिजिटलीकरण को प्रोत्साहित करते हुए, आरबीआई का दृष्टिकोण यह सुनिश्चित करना रहा है कि वित्तीय प्रणाली में नवोन्मेष को सहज तरीके से आत्मसात किया जाना चाहिए और डिजिटलीकरण के दौरान हर कदम पर ग्राहक की सुरक्षा सुनिश्चित होनी चाहिए।

भारत उन कुछ देशों में से एक है जो डिजिटल भुगतान लेनदेन के लिए द्वि-स्तरीय प्रमाणीकरण के माध्यम से उपयोगकर्ताओं की सुरक्षा करता है। हालाँकि अब इसे एक नवोन्मेषी विनियमन के रूप में मान्यता प्राप्त है, लेकिन जब आरबीआई ने लगभग एक दशक पहले इसे पेश किया था, तो इसका विरोध और आलोचना हुई थी। इसी तरह, कार्ड के उपयोग पर बेहतर ग्राहक नियंत्रण, लेनदेन विफलताओं के लिए अल्प निपटान अवधि (टीएटी), टोकेनीकरण (टोनाइजेशन), आदि जैसे हालिया उपाय ग्राहक की सुरक्षा के लिए की गई पहल हैं।

भुगतान क्षेत्र में, रियल टाइम ग्रॉस सेटलमेंट (आरटीजीएस) और नेशनल इलेक्ट्रॉनिक फंड ट्रांसफर (एनईएफटी) को 24x7 कर दिया गया है। इसके अलावा, आरबीआई ने 1996 में इंस्टीट्यूट फॉर डेवलपमेंट एंड रिसर्च इन बैंकिंग टेक्नोलॉजी (आईडीआरबीटी) और 2008 में नेशनल पेमेंट कॉरपोरेशन ऑफ इंडिया जैसे उपयुक्त संस्थानों की स्थापना को प्रेरित किया, जो विभिन्न भुगतान प्रणाली प्रौद्योगिकियों और समाधानों को आगे बढ़ाने में सहायक रहे हैं।

समुचित विनियामक ढांचे के माध्यम से, आरबीआई ने डिजिटल ऋण, मुक्त बैंकिंग और पी2पी ऋण प्लेटफार्मों में

नवोन्मेषों को प्रोत्साहित किया है। 2019 में एक विनियामक सैंडबॉक्स ढांचा बनाया गया था, जिसने नवीन वित्तीय उत्पादों और सेवाओं को अपनाने हेतु प्रोत्साहित करने के लिए कई समूह चलाए हैं। वित्तीय नवोन्मेषों से संबंधित विचारों के आदान-प्रदान और प्रोटोटाइप के विकास के लिए वित्तीय क्षेत्र के संस्थानों, प्रौद्योगिकी उद्योग और शैक्षणिक संस्थानों के साथ सहयोग करने के लिए रिज़र्व बैंक नवोन्मेष केंद्र (आरबीआईएच) की स्थापना की गई है। हैकथॉन जैसे प्रतिस्पर्धी कार्यक्रम फिनटेक और स्टार्ट-अप क्षेत्र को, नवोन्मेषों को प्रदर्शित करने के लिए, एक मंच प्रदान करने हेतु आयोजित किए जाते हैं।

सुरक्षा, गति और स्केलेबिलिटी पर ध्यान केंद्रित करने वाले सहायक विनियामक वातावरण ने भारत को भुगतान प्रणाली नवोन्मेष में अग्रणी के रूप में स्थापित किया है। उदाहरण के तौर पर, 2016 में शुरु की गई भारत की त्वरित भुगतान प्रणाली यूपीआई ने मई 2023 के दौरान 300 मिलियन से अधिक मात्रा और ₹480 बिलियन मूल्य के औसत दैनिक लेनदेन के साथ भारत में उल्लेखनीय वृद्धि देखी है। हाल ही में, भारत और सिंगापुर ने अपने यूपीआई और पे-नाउ के साथ समझौता किया है, जिससे दोनों देशों के बीच वास्तविक समय पर सीमा-पार धन अंतरण सहज हो गया है। दरअसल, अन्य देशों के साथ साझेदारी और सहयोग के माध्यम से वैश्विक स्तर पर यूपीआई के उपयोग की अपार संभावनाएं हैं।

आरबीआई लगातार साइबर जोखिमों पर अपनी पर्यवेक्षी निगरानी को मजबूत करने की कोशिश कर रहा है। नकली फ़िशिंग, साइबर पूर्व-परीक्षण और अन्य साइबर अभ्यास प्रचलित साइबर जोखिमों पर एक प्रणालीगत दृष्टिकोण प्राप्त करने में पर्यवेक्षी प्रक्रियाओं के पूरक हैं। आरबीआई ने सेक्टोरल सिक्योरिटी ऑपरेशंस सेंटर (एस-एसओसी), जैसे नवीन उपकरणों के विकास को भी प्रोत्साहित किया है जो बैंकिंग और वित्तीय क्षेत्र के साइबर जोखिम को बड़े पैमाने पर कम करने में मदद कर सकता है।

हालाँकि कहा जाता है कि साइबर जोखिम नियमों से आगे निकल जाते हैं, भारतीय रिज़र्व बैंक अपनी विनियमित संस्थाओं में आईटी और साइबर जोखिम प्रबंधन को मजबूत करने के लिए सक्रिय रूप से उपाय कर रहा है। 2011 की शुरुआत में, आईटी जोखिमों के प्रबंधन के लिए बैंकों को विस्तृत दिशानिर्देश जारी किए गए थे, जिसके बाद 2016 में एक सिद्धांत-आधारित साइबर सुरक्षा ढांचा जारी किया गया था। डिजिटल भुगतान सुरक्षा नियंत्रण और आईटी सेवाओं की आउटसोर्सिंग पर भी नियम जारी किए गए हैं। आरबीआई ने आईटी गवर्नेंस पर मसौदा दिशानिर्देश भी प्रकाशित किए हैं जिन्हें शीघ्र ही अंतिम रूप दिया जाएगा और जारी किया जाएगा।

सामूहिक प्रयास की जरूरत

साइबर खतरों की वैश्विक प्रकृति को ध्यान में रखते हुए, सरकारों, वित्तीय संस्थाओं और तकनीकी कंपनियों के प्रयास उनसे बचाव के लिए अपर्याप्त हैं। साइबर खतरे भौगोलिक सीमाओं को पार कर जाते हैं, जिससे देशों और वित्तीय संस्थानों के लिए उनसे निपटने हेतु मिलकर काम करना आवश्यक हो जाता है।

मैं छ: रणनीतियों की रूपरेखा बनाना चाहूंगा जो वैश्विक साइबर सुरक्षा वातावरण को बेहतर बनाने में मदद करेंगी :

i. पहला, वैश्विक वित्तीय प्रणाली की अन्योन्याश्रितताओं को, महत्वपूर्ण अवसंरचना के साथ-साथ प्रमुख परिचालन और तकनीकी अंतर्संबंधों को मैप करके, बेहतर ढंग से समझने की आवश्यकता है। वित्तीय स्थिरता विश्लेषण में साइबर जोखिम के अधिक समावेश से, सिस्टम-व्यापी जोखिम को समझने और कम करने की क्षमता में सुधार होगा।

ii. दूसरा, साइबर सुरक्षा के लिए एक न्यूनतम सामान्य ढांचा तैयार करने की आवश्यकता है जो वित्तीय संस्थानों के पालन के लिए सर्वोत्तम प्रथाओं और मानकों की रूपरेखा तैयार करे। इससे यह सुनिश्चित करने में मदद मिल सकती है कि सभी संस्थान साइबर खतरों से खुद को बचाने के लिए आवश्यक कदम उठा रहे हैं।

iii. तीसरा, घरेलू कानूनों के अनुसार जहां तक संभव हो, विभिन्न देश साइबर खतरों और हमलों के बारे में जानकारी और आसूचना साझा कर सकते हैं। इससे उभरते खतरों और कमजोरियों की पहचान करने में मदद मिल सकती है और हमलों को रोकने के लिए सक्रिय उपाय करने में वित्तीय संस्थानों को सक्षम बनाया जा सकता है।

iv. चौथा, विभिन्न देश, घटना प्रतिक्रिया योजनाओं को विकसित करने और लागू करने के लिए साथ मिलकर काम कर सकते हैं। इससे यह सुनिश्चित करने में मदद मिल सकती है कि साइबर हमले की स्थिति में, एक समन्वित और प्रभावी प्रतिक्रिया योजना हो जो वित्तीय क्षेत्र पर दुष्प्रभाव को कम कर सके।

v. पांचवां, अपराध की आय को जब्त करने और अपराधियों पर मुकदमा चलाने के प्रभावी उपायों किए जाएं ताकि अपराधियों के लिए साइबर हमले अधिक महंगे और जोखिम भरे हो जाएं। हमलावरों को रोकने और बाधित करने के अंतरराष्ट्रीय प्रयास बढ़ा कर इस खतरे की जड़ पर चोट की जा सकती है।

vi. अंत में, विभिन्न देश यह सुनिश्चित करने के लिए क्षमता निर्माण और प्रशिक्षण कार्यक्रमों में सहयोग कर सकते हैं कि वित्तीय संस्थानों के पास साइबर जोखिमों का प्रभावी प्रबंधन करने के लिए आवश्यक कौशल और संसाधन हों। इसमें साइबर सुरक्षा की सर्वोत्तम प्रथाओं पर प्रशिक्षण, घटना प्रतिक्रिया योजना और साइबर हमलों का पता लगाने और रोकने के लिए उन्नत प्रौद्योगिकियों का उपयोग किया जा सकता है।

निष्कर्ष

अब, मैं निष्कर्ष पर आता हूँ। दुनिया भर में बढ़ते संपर्क के साथ-साथ, साइबर जोखिम पर अंकुश लगाने के लिए अंतरराष्ट्रीय प्रयास की आवश्यकता है। उम्मीद है कि जी20 मंच, अंतरराष्ट्रीय मानकों और सर्वोत्तम प्रथाओं को प्राथमिकता देते हुए उन्हें डिजाइन और कार्यान्वित कर, वित्तीय क्षेत्र की मदद के लिए एक दृष्टिकोण बनाने की दिशा में विभिन्न अंतरराष्ट्रीय निकायों के प्रयासों का पूरक होगा।

मैं सभी से, आज होने वाले आगामी साइबर सुरक्षा अभ्यास में, सक्रिय रूप से भाग लेने का अनुरोध करता हूं। हम मिलकर वित्तीय क्षेत्र को अधिक सुरक्षित और भरोसेमंद बना सकते हैं।

धन्यवाद !