*सूचना प्रौद्योगिकी और बैंकिंग क्षेत्र में साइबर जोखिम - चिंता की उभरती लकीरें**

एस. एस. मूंदड़ा

सुप्रभात !

मैं सबसे पहले कैफरल को बधाई देना चाहता हूं कि उन्होंने बैंकों और वित्तीय संस्थाओं के लिए साइबर जोखिम और उसकी रोकथाम विषय पर सेमिनार का आयोजन किया, यह एक ऐसा विषय है जो न केवल भारत में बल्कि पूरे विश्व में केंद्रीय मुद्दा बन चुका है। मैं अपनी बात की शुरुआत जॉन चैंबर्स के कथन से करना चाहूंगा, जो सिसको के भूतपूर्व सीईओ रह चुके हैं, उन्होंने उद्यमों में साइबर जोखिम के महत्व को रेखांकित करते हुए कहा है; **'केवल दो प्रकार के संगठन हैं, एक वे जो हैक कर लिए गए हैं और दूसरे वे जो यह नहीं जानते कि उन्हें हैक कर लिया गया है।'** मैं यह देख रहा हूं कि सेमिनार का कार्यक्रम काफी व्यापक है और सहभागी इससे दो तरह से लाभान्वित होंगे- एक तो प्रेजेंटेशंनों से और परस्पर चर्चाओं से तथा इस विषय पर अपने-अपने विशेष अनुभवों के माध्यम से। मैं आज के अपने भाषण में बैंकों में साइबर सुरक्षा के दो प्रमुख आयामों के बारे में बताना चाहूंगा: ए) आंतरिक सूचना प्रौद्योगिकी सुरक्षा और बी) नेटवर्क की कमज़ोरियां।

भारतीय बैंकों में आईटी का आविर्भाव

2. मैं संक्षेप में यह बताना चाहूंगा कि भारत में सूचना प्रौद्योगिकी की शुरुआत कब हुई और उसे कब अंगीकार किया गया। देश की बैंकिंग प्रणाली के विनियामक के रूप में रिज़र्व बैंक ने बैंकों में प्रौद्योगिकी के अपनाए जाने में महत्वपूर्ण भूमिका अदा की है। बैंकों में मशीनीकरण से संबंधित रंगराजन समिति (1984) को भारतीय बैंकों में प्रौद्योगिकी के अग्रदूत के रूप में माना जा सकता है। उसके बाद विभिन्न समितियों/कार्यदलों ने इस क्षेत्र में प्रौद्योगिकी को अपनाने तथा उससे जुड़े सुरक्षात्मक उपाय किए जाने की आवश्यकता की अनुशंसा की। यह यात्रा आमतौर पर लेजर पोस्टिंग मशीन के आने से प्रारंभ हुई थी, उसके बाद संपूर्ण शाखा का आटोमेशन किया गया और अब कोर बैंकिंग साल्यूशन (सीबीएस) तक पहुंच गई है। 1990 के दशक में, निजी क्षेत्र के नई पीढ़ी के बैंकों को यह अधिदेश दिया गया था कि वे अपने कार्य पूरी तरह से कंप्यूटरीकृत परिवेश में करें। जैसाकि गार्डेन मूर ने भविष्यवाणी की थी कि कंप्यूटर की समग्र प्रोसेसिंग शक्ति प्रत्येक दो वर्ष में दुगुना हो जाएगी, उनका कथन सत्य सिद्ध हो रहा है, कंप्यूटरीकृत वातावरण में बैंकिंग क्षेत्र में अधिक से अधिक एप्लीकेशन लगाए जा रहे हैं।

3. भारतीय रिज़र्व बैंक ने भी भुगतान बाज़ार की बुनियादी सुविधाओं के विकास के लिए तथा बैंकिंग क्षेत्र में प्रौद्योगिकी के इस्तेमाल को आसान बनाने के लिए आईडीआरबीटी, एनपीसीआई, सीसीआईएल आदि जैसी संस्थाओं की स्थापना करके बहुत महत्वपूर्ण भूमिका अदा की है। इस समय ये संस्थाएं भुगतान-मिशन के लिए महत्वपूर्ण एवं भुगतान प्रणाली एप्लीकेशन जैसे आरटीजीएस, सुरक्षित वित्तीय संदेशन प्रणाली, तयशुदा लेनदेन निपटान प्रणाली आदि के संचालन के लिए प्लेटफार्म उपलब्ध करवा रही हैं।

4. वर्ष 2000 में सूचना प्रौद्योगिकी अधिनियम पारित होने से कंप्यूटरीकृत परिवेश में लेनदेन को संचालित करने को अत्यधिक बढ़ावा मिला जिसमें उसे कानूनी सहारा मिल गया। इंटरनेट का इस्तेमाल धीर-धीरे बढ़ता गया और बैंकिंग उत्पादों एवं सेवाओं की डिलेवरी के लिए इंटरनेट का चैनल के रूप में उपयोग बढ़ गया। देश में मोबाइल फोन के उपयोग करने वालों की अत्यधिक वृद्धि से यह चैनल डिलेवरी का फस्ट-ट्रैक बन गया। बैंकिंग प्रौद्योगिकी में हुए नवोन्मेष की लंबी श्रृंखला में सबसे आधुनिक है यूनिफाइड भुगतान इंटरफेस (यूपीआई), जिसने विप्रेषण की सीमाओं को बढ़ा दिया है। इस लंबी कहानी को यदि संक्षेप में कहें तो प्रौद्योगिकी का इस्तेमाल कई गुना बढ़ गया है, और आज कोई भी बैंक तीव्र प्रौद्योगिकी, ग्राहक-मैत्रीय डिजिटल उत्पाद, बाधारहित उपयोक्ता अनुभव तथा सतत नवीनीकरण के बिना जीवित नहीं रह सकता है।

फिनटेक क्रांति

5. पूरे विश्व में फिनटेक संबंधी क्रांति आने से एक बार फिर बैंकों के लिए स्थिति चुनौतीपूर्ण बन गई है। आज अधिकांश

---

* श्री एस.एस.मूंदड़ा, उप गवर्नर, भारतीय रिज़र्व बैंक द्वारा कैफरल द्वारा 7 सितंबर 2016 को 'साइबर जोखिम और बैंकों में उसे दूर करने से संबंधित अंतरराष्ट्रीय सेमिनार' विषय पर दिए गए भाषण का मुख्य अंश। श्री आर रविकुमार द्वारा दिए गए सहयोग के लिए आभार।

बैंकिंग आवश्यकताओं को मोबाइल के माध्यम से पूरा किया जा सकता है। कार्ड-आधारित भुगतान भी, प्रीपेड कार्ड, टैप एंड गो, वर्चुअल कार्ड, बहु-करेंसी कार्ड, क्यूआर कोड धारित भुगतान आदि के आ जाने से, काफी परिपक्व हो गया है। प्रौद्योगिकी अब सुविधाजनक बनती जा रही है तथा उससे यह अंतर महसूस किया जा सकता है कि वह आखिरकार आवश्यकता एवं जीवन जीने का तरीका बन गई है। इस वर्ष के अंत तक भारत में थोड़े-बहुत भुगतान बैंक अपने कार्य प्रारंभ कर देंगे जो बैंकों को प्रौद्योगिकी की दौड़ में खींचेंगे। वित्तीय क्षेत्र में कुछेक प्रौद्योगिकीय तरक्की, जो धीरे-धीरे वित्तीय क्षेत्र पर धावा बोल रही है, उसमें **बिग डाटा, आर्टिफिशियल इंटेलिजेंस, ब्लॉक-चेन प्रौद्योगिकी तथा इंटरनेट जैसी चीजें** शामिल हैं। मैं कुछ उदाहरण देकर अपनी बात रखना चाहूंगा।

6. बैंकों ने यह इरादा ज़ाहिर किया है कि वह अपने बैंकिंग एप के माध्यम से आवाज़ की पहचान करते हुए सुरक्षित लेनदेन उपलब्ध कराएंगे। आरबीएस ने 'लुवो' का ट्रायल लिया है, जो ए1 ग्राहक सेवा सहायता देता है जिसके माध्यम से स्टाफ से संपर्क किया जाता है और यह निकट भविष्य में अत्यधिक सुरक्षित तरीके से ग्राहकों को सेवा प्रदान करेगा। जापान के साफ्टबैंक ने पेरिस के रोबोटिक एक्सपर्ट अलडेबरन के साथ मिलकर पेप्पर तैयार किया है जो विश्व का पहला मानव रोबोट है। पेप्पर का इस्तेमाल पहले से ही ग्राहक सेवा उद्योगों में किया जा रहा है जिसने सूचान बूथ तथा स्वागत कक्ष को प्रतिस्थापित कर दिया है। बताया जाता है कि मिजूहो फाइनेंशियल ग्रुप इन्कार्पो. बैंक ने 2015 में टोकियो में अपनी प्रमुख शाखा में पेप्पर का इस्तेमाल शुरू कर दिया है जो ग्राहक की पूछताछ संबंधी जरूरतों को पूरा करेगा, जबकि मितसुबिशी यूएफजे फाइनेंशियल ग्रुप ने 'नावो' का परीक्षण किया है, जो मानव रोबोट है और ग्राहकों से बातचीत करेगा। मैं समझता हूं कि एचडीएफसी भी अपने जापानी साथी से संकेत ग्रहण करते हुए भारत में रोबोटिक्स के माध्यम से इसी प्रकार के आटोमेशन की शुरुआत करने का इरादा रखता है।

7. बैंकिंग क्षेत्र में प्रौद्योगिकी पर बढ़ती निर्भरता के केंद्र-बिंदु को और पुष्ट करने के लिए मैं कुछ आंकड़ों का इस्तेमाल करना चाहूंगा। भारतीय रिज़र्व बैंक की वर्तमान वार्षिक रिपोर्ट के अनुसार मात्रा के हिसाब से कुल लेनदेन में इलेक्ट्रॉनिक लेनदेन का हिस्सा पिछले साल 74.6 प्रतिशत था जो बढ़कर 84.4 प्रतिशत हो गया है। इसी प्रकार यदि मूल्य के हिसाब से देखें तो इसका हिस्सा 94.6 प्रतिशत से बढ़कर 95.2 प्रतिशत हो गया है। मार्च 2016 के अंत में 172 बैंकों की 130,013 शाखाओं में राष्ट्रीय इलेक्ट्रॉनिक निधि अंतरण(एनईएफटी) सेवाएं उपलब्ध थीं, साथ ही कारोबारी प्रतिनिधि आउटलेट भी उपलब्ध थे। एनईएफटी द्वारा 1.2 बिलियन लेनदेन का संचालन किया गया जिसका कुल मूल्य 83 ट्रिलियन रुपए (लगभग 1.3 ट्रिलियन अमरीकी डालर) था जिसकी तुलना में यह लेनदेन पिछले वर्ष 928 मिलियन था जिसका कुल मूल्य 60 ट्रिलियन रुपए(लगभग 0.9 ट्रिलियन अमरीकी डालर) था। मार्च 2016 के महीने में एनईएफटी से सबसे अधिक 129 मिलियन लेनदेन किए गए थे। इसी प्रकार इंटरनेट बैंकिंग एवं मोबाइल बैंकिंग आधारित भुगतान बड़ी तेजी से बढ़ रहे हैं। मैंने यूपीआई का उल्लेख पूर्व में किया था। इस संदर्भ में यह भी उल्लेख करना समीचीन होगा कि आधार (देश में रहने वालों की एक विशिष्ट पहचान) में लोगों ने काफी बड़ी संख्या में स्वयं को सूचीबद्ध किया है जिसे प्रत्येक व्यक्ति के खाते से जोड़ा गया है, जिसको यूपीआई से जोड़कर अंतर्निहित क्षमता सृजित करके आगे चलकर **खाता संख्या की सुवाह्यता (पोर्टेबिलिटी) संभव हो सकती है**। यह बैंकिंग क्षेत्र में ऐसा बदलाव लाएगा जिसकी कल्पना अभी से नहीं की जा सकती है।

8. जहां हर कोई इस बात की सराहना कर रहा है कि तीव्र एवं कुशल तरीके से 24x7 बैंकिंग लेनदेन सेवाएं उपलब्ध हैं, वहीं इस प्रकार की उन्नत प्रौद्योगिकी युक्त सुविधा मुहैया कराने का मेरुदंड बैंकों की आईटी संरचना द्वारा उपलब्ध कराया जा रहा है। इसलिए आदर्श रूप से नए डिजिटल उत्पाद मुहैया कराने के लिए नई प्रौद्योगिकी का सहारा लेने हेतु बैंकों में आईटी सिस्टम तेज़ होना चाहिए, लेनदेन की बढ़ती हुई मात्रा को सुरक्षित तरीके से संचालित करने में, बैंक की कोर बैंकिंग साल्यूशन में एक्सेस करने के लिए विभिन्न एप्लीकेशन में सुरक्षित ढंग से कनेक्टिविटी उपलब्ध कराने में सक्षम होना चाहिए और वहीं पर ग्राहकों की सूचनाओं की गोपनीयता बनाए रखनी चाहिए। इन चुनौतियों को ध्यान में रखते हुए भारतीय रिज़र्व बैंक प्रौद्योगिकी को अपनाने के संबंध में बैंकों को मार्दर्शन देता रहा है। इस प्रयोजन से रिज़र्व बैंक ने एक बड़ी पहल यह की है कि सूचना सुरक्षा, इलेक्ट्रॉनिक बैंकिंग के संबंध में प्रौद्योगिकी जोखिम प्रबंधन और साइबर धोखाधड़ी (श्री गोपालकृष्ण के अधीन) विषय पर एक कार्य समूह का गठन किया है। इस समूह ने नौ बड़े क्षेत्रों के बारे में सिफारिशें की

है जैसे आईटी अभिशासन, सूचना सुरक्षा, आईएस आडिट, आईटी परिचालन, आईटी सेवाओं की आउटसोर्सिंग, साइबर धोखाधड़ी, कारोबार निरंतरता योजना, ग्राहक जागरूकता कार्यक्रम और क़ानूनी पहलू। भारतीय रिज़र्व बैंक द्वारा इस संबंध में दिशानिर्देश अभी-अभी जारी किए गए हैं जिसमें यह रेखांकित किया गया है कि इन सिफारिशों का कार्यान्वयन जोखिम आधारित हो और प्रत्येक बैंक की गतिविधियों के स्वरूप एवं दायरे तथा प्रौद्योगिकी पर उनकी कारोबार प्रक्रिया की निर्भरता के अनुरूप हो। बैंकों में बोर्ड स्तरीय समितियों को यह अधिदेश दिया गया है कि वे संबंधित बैंकों में इन दिशानिर्देशों को लागू करने की स्थिति पर निगरानी रखें। पिछले कुछ वर्षों में इस दिशा में जहां काफी प्रगति हुई है वहीं मुझे यकीन है कि बैंकों को अभी भी समस्त आवश्यकताओं का पूरी तरह से पालन कर लिए जाने से पूर्व काफी लंबी यात्रा तय करनी है। आज बैंकों में जिस प्रकार से प्रौद्योगिकी ने अपना प्रमुख स्थान बना लिया है, उसे देखते हुए इसे मात्र अनुपालन का मामला नहीं समझा जाना चाहिए बल्कि इसे अपने कारोबार का प्रमुख अंग मानना चाहिए।

पर्यवेक्षी सरोकार

9. बैंक के भीतर विभिन्न गतिविधियों को कंप्यूटरीकृत कर दिए जाने से एक विनियामक एवं पर्यवेक्षक के रूप में बैंकों से हमारी अपेक्षा है कि वे निर्णय लेने के उद्देश्य से संबंधित प्रबंधन सूचना को सृजित करने के लिए और अधिक क्षमताएं पैदा करें। लेकिन हर कोई जानता है कि वादा करने और निभाने में काफी अंतर होता है, इसलिए मैं कुछ खास क्षेत्रों पर प्रकाश डालना चाहूंगा।

10. वित्तीय जगत के लिए सबसे पहली चिंता का विषय यह सुनिश्चित करना है कि बैंकिंग प्रणाली का दुरुपयोग अवांछित तत्वों द्वारा धन-शोधन के लिए न किया जाए। समस्त क्षेत्रों में अपने ग्राहक को जानिए/धन-शोधन निरोधी विनियमों को सभी क्षेत्राधिकारों के अंतर्गत मजबूत बना दिया गया है। लेकिन हमने अक्सर यह पाया है कि बैंकों में इन विनियमों का पालन करने के लिए तीव्र प्रणाली नहीं है। ग्राहकों से जानकारी लेते समय बैंकों को चाहिए कि वे अपने ग्राहकों का मूल्यांकन करें, उनके कारोबार और उनके खाते में अंदाज़न कितने का लेनदेन होगा, लेनदेन किससे होगा आदि के बारे में पता करें। हाल के समय में हमने बैंकों में ऐसे अनेक मामले देखें हैं जिनमें ग्राहकों के खातों में लेनदेन की अनुमति दे दी गई है और उनके घोषित कारोबारी प्रोफाइल का उचित ध्यान नहीं रखा गया है। इन खातों में आरटीजीएस/एनईएफटी के माध्यम से अनेक विप्रेषण आए हैं और भेजे भी गए हैं। अनेक खातों का दुरुपयोग विदेश में आयात अग्रिम का धन भेजने के लिए किया गया है। इन खातों में अलग-अलग तरह के कार्यकलाप होने के बावजूद बैंकों की निगरानी प्रणाली हमारी अपेक्षाओं पर खरी नहीं उतरी है। मुझे आश्चर्य है कि **बैंकों ने ऐसे गलत लेनदेन का पता लगाने के लिए फुलप्रूफ प्रौद्योगिकी आधारित समाधान क्यों नहीं तैयार किया है।** जैसाकि आप जानते होंगे कि भारतीय रिज़र्व बैंक ने वर्तमान केवायसी/एएमएल अनुदेशों का पालन न करने के लिए तथा बैंकों द्वारा उनके जोखिम प्रोफाइल के अनुसार ग्राहकों को वर्गीकृत न कर पाने के लिए 13 बैंकों पर जुर्माना भी लगाया है।

11. एक अन्य क्षेत्र जो मेरे दिमाग में आ रहा है वह है **एनपीए की सिस्टम-आधारित पहचान करना।** हम यह महसूस करते हैं कि इस क्षेत्र में सुधार की काफी गुंजाइश है। जहां हम यह जानते हैं कि बैंक मल्टिपल प्रणाली का उपयोग कर रहे हैं, उनके नियम विस्तृत हैं तथा गुणवत्तापूर्ण भी हैं, फिर भी कंप्यूटर सिस्टम में पैरामीटर को कैप्चर करने के प्रति चुनौती पेश कर हे हैं; लेकिन प्रौद्योगिकी क्षेत्र में हुई प्रगति को देखते हुए इस समस्या को काफी पहले हल कर लिया जाना चाहिए था। हम यह चाहते हैं कि एनपीए की पहचान के लिए एक सिस्टम धारित तीव्र प्रणाली हो, जो न केवल रेगुलेटर के उपयोग के लिए हो बल्कि बैंक के आंतरिक उपयोग के लिए भी हो ताकि समय पर बहाली हो सके/समाधान हो सके।

12. तीसरा क्षेत्र जिसके बारे में मैं बताना चाहूंगा वह है स्वत: डाटा फ्लो चार्ट, जिसमें यह निहित है कि रेगुलेटरी रिपोर्टिंग के उद्देश्य से उनके सिस्टम द्वारा डाटा स्वत: निकलकर आएगा। मेरा यह मानना है कि एडीएफ प्रणाली को अपेक्षित स्तर तक नहीं लागू किया गया है और प्रौद्योगिकी के मोर्चे पर अत्यधिक प्रगति हो जाने के बावजूद डाटा प्रस्तुतीकरण की गुणवत्ता, एकरूपता एवं समयबद्धता का मुद्दा अभी भी बना हुआ है।

13. मैं इसी प्रकार से बहुत से उदाहरण दे सकता हूं। लेकिन इन सब मामलों में एक बात कामन है, वह है **बोर्ड के स्तर पर निगरानी तथा कार्यपालक प्रबंधन की प्रतिबद्धता का अभाव।** प्रौद्योगिकी सेवा प्रदाता, खासतौर से उत्पाद वेंडर्स की भी

काफी भूमिका है। यह महत्वपूर्ण है कि वे जो प्रौद्योगिकी उपलब्ध करा रहे हैं वह विनियामकीय अपेक्षा को सतत आधार पर पूरा करने में सक्षम होनी चाहिए और यदि कोई अंतर आता है तो उसे कम से कम समय में पूरा किया जाना चाहिए तथा इस प्रकार से अपग्रेड किया जाना ऐसा हो जो बाधारहित हो तथा उनके समस्त ग्राहकों के लिए किफायती हो।

हाल की साइबर घटनाएं

14. अब मैं हाल में हुई साइबर घटनाओं का उल्लेख करना चाहूंगा जिनका संबंध वित्तीय जगत से है।

- 2 अगस्त 2016 को, डिजिटल करेंसी की ट्रेडिंग के लिए हांगकांग एक्सचेंज बिटफिनेक्स ने घोषणा की कि उसके कुछ ग्राहकों के खाते हैक कर लिए गए हैं और बिटक्वाइन चोरी कर लिए गए हैं। चोरी किए गए बिटक्वाइन का मूल्य तकरीबन 65 मिलियन अमरीकी डालर या उससे अधिक था। फलस्वरूप बिटक्वाइन का मूल्य गिर गया और डिजिटल करेंसी से भरोसा हिल गया।

- वर्ष के प्रारंभ में, बांगलादेश बैंक को निशाना बनाया गया और 1 मिलियन अमरीकी डालर चोरी करने का प्रयास किया गया और अंतत: चोर 81 मिलियन अमरीकी डालर की चोरी करने में सफल रहे । हाल में भारत में भी एक कमर्शियल बैंक में इसी प्रकार का प्रयास किया गया था जिसमें नोस्त्रो खाते में धोखे से भुगतान अनुदेश जारी किए गए और उसे स्विफ्ट संदेश प्रणाली पर डाला जा रहा था। यद्यपि संबंधित भुगतानकर्ता/मध्यस्थता करने वाले बैंक के साथ सक्रिय अनुवर्तन किए जाने से मौद्रिक नुकसान बचा लिया गया लेकिन इस घटना से यह ज्ञात हुआ कि अभी भी अनेक स्टेकहोल्डरों ने इन घटनाओं से सबक नहीं लिया है। हमें भी ऐसी घटनाएं देखने में आई हैं जिनमें स्विफ्ट की सुविधा का उपयोग करते हुए दस्तावेजी क्रेडिट की पुष्टि का कपटपूर्ण संदेश भेजा जा रहा था। हालांकि बाद की जो घटनाएं हुई हैं वे मुख्यत: आंतरिक नियंत्रण प्रणाली की असफलता तथा 'चार आंख के सिद्धांत' का पालन न करने से हुई हैं। यह घटना इसलिए भी हुई कि एक ऐसी प्रणाली पर निर्भरता है जिसमें स्विफ्ट लेनदेन को सीबीएस में उसी प्रकार के लेनदेन के लिए अंजाम दिया जा सकता है।

  एक अन्य घटना में बैंक के मोबाइल वैलेट को साझा किया गया था, इसमें कमजोरी एप्लीकेशन में ही पाई गई जिसका दुरुपयोग चोर द्वारा किया गया था। अंतरण करने वाला बड़ी मात्रा में लेनदेन में उस राशि को राशि पाने वाले के खाते में बिना तदनुरूपी डेबिट करके वापस पा सकता था (इसमें निहित कुल राशि लगभग 12 करोड़ रुपए थी)। बैंक किसी प्रकार वास्तविक समय का समायोजन कार्य नहीं कर रहा था और यह बात तब पता चली जब लेनदेन में कुछ गड़बड़ी महसूस हुई जिसे समायोजन के दौरान पाया गया। इस घटना में सिस्टम के प्रति संवेदनशीलता के दुरुपयोग को टाला जा सकता था, बशर्ते कि उत्पाद की शुरुआत उसके माध्यम से न की जाती।

- एक अन्य घटना में एक बड़े बैंक की ई-पेमेंट वेबसाइट को हैक कर लिया गया। आश्चर्य की बात तो यह है कि उस बैंक ने उसे तब तक नोटिस नहीं किया जब तक कि एक विधि प्रवर्तन एजेंसी ने नोटिस करके नहीं बताया। पड़ोसी देश से फेसबुक पर एक पोस्ट डाली गई थी जिसमें उसके परिचालन का दावा किया गया था। हालांकि हैकिंग घटना से किसी प्रकार का माली नुकसान नहीं हुआ क्योंकि साइट में केवल अंतिम उपयोक्ता द्वारा किए गए इनपुट की वैधता का प्रमाणन कार्य किया जाता था, तो भी इससे यह पता चलता है कि सुरक्षा का गंभीर अतिक्रमण किया गया है।

15. जैसा कि ऊपर दिए गए उदाहरणों से देखा जा सकता है कि साइबर चुनौतियां बढ़ती जा रही हैं। ऐसा होना स्वाभाविक भी है क्योंकि पैसा अब न केवल मूर्त रूप में बल्कि ज्यादातर इलेक्ट्रॉनिक माध्यम से इधर से उधर हो रहा है। इससे गलत तत्वों को शह मिलती है कि वे उसे चुराने के लिए गलत तरीकों का इस्तेमाल करें। आक्रमणकारियों का सबसे बड़ा लक्ष्य ग्राहक के विवरण जानने का होता है, क्योंकि उससे उन्हें 'ख़ज़ाना' की चाबी प्राप्त हो जाती है। हाल के अनुभवों से पता चलता है कि इनमें संगठित गिरोह और राष्ट्र-राज्य के एक्टर्स शामिल होते

हैं जिनको बड़ी मात्रा में वित्तीय मदद हासिल होती है। दूसरी ओर, इस प्रकार के आक्रमण को निष्पादित करने में लागत कम होती जा रही है। अनेक रिपोर्टों से पता चलता है कि इस डार्क वेब में बहुत से ग्राहकों के ब्योरे बिक्री के लिए उपलब्ध हैं, यह स्थिति वास्तव में भयावह है।

साइबर की समुत्थानशक्ति में सुधार

16. पूरे विश्व में अब फोकस साइबर सुरक्षा पर है। साइबर सुरक्षा अब किसी भी तरह से पृथक घटना नहीं है जो केवल एक उद्योग/देश को प्रभावित कर रही है। हाल के समय में अनेक साइबर आक्रमण की योजना बनाई गई है ताकि राजनैतिक/धार्मिक उद्देश्य पूरे किए जा सकें तथा आतंकवाद को बढ़ावा देने के लिए धन प्राप्त किया जा सके। इसके बड़े भयावह आयाम हैं क्योकि इससे वित्तीय स्थिरता पर प्रभाव पड़ेगा। इस मुद्दे के महत्व का अंदाज़ा इस बात से लगाया जा सकता है कि विश्व के मानक निर्धारक निकाय तथा प्रतिष्ठित केंद्रीय बैंक इस तबाही को दूर करने के लिए बहुत बड़े संसाधनों को लगा रहे हैं।

17. अनेक देशों ने साइबर से लड़ने की अपनी शक्ति बढ़ाने के लिए उपाय किए हैं। भुगतान और बाज़ार इन्फ्रास्ट्रक्चर से संबंधित समिति और अंतरराष्ट्रीय प्रतिभूति आयोग संगठन (आईओएससीओ) ने जून 2016 में स्टेकहोल्डरों से परामर्श करके वित्तीय बाज़ार की साइबर समुत्थानशाक्ति के संबंध में मार्गदर्शी निर्देश जारी किए हैं। बैंक आफ इंग्लैंड की वित्तीय नीति समिति (एफपीसी) ने सीबीईएसटी नामक पहल की है - यह एक प्रभावकारिता परीक्षण संरचना है। जून 2013 में उनकी बैठक के बाद एफपीसी ने सिफारिश की थी कि महारानी की ट्रेजरी एवं रेगुलेटर्स मिलकर यूके के प्रमुख वित्तीय सिस्टम एवं उसके इंफ्रास्ट्रक्चर को एक कार्यक्रम लागू करने के कार्य में लगाएंगे तथा साइबर-आक्रमण से निपटने की शक्ति का परीक्षण करेंगे। समिति ने यह भी नोट किया था कि वित्तीय फर्मों के बोर्ड तथा इन्फ्रास्ट्रक्चर प्रदाता यह मानें कि इस प्रकार के आक्रमणों का जवाब देने की उनकी जिम्मेदारी है। हाल ही में, मई 2016 में हांगकांग मौद्रिक प्राधिकारी ने एक साइबर सुरक्षा फोर्टिफिकेशन पहल (सीएफआई) प्रारंभ की है। सीएफआई मुख्यत: तीन स्तंभों पर आधारित है :

ए. साइबर समुत्थानशक्ति मूल्यांकन संरचना

बी. प्रोफेशनल विकास कार्यक्रम और

सी. साइबर आसूचना साझा करने का प्लेटफार्म

18. भारत में हम भी साइबर अपराध से रक्षा को सुदृढ़ बनाने के लिए कार्य कर रहे हैं। भारत सरकार ने साइबर-आक्रमण के खतरे को दूर करने के लिए अनेक कदम उठाए हैं और महत्वपूर्ण संस्थागत व्यवस्थाएं की गई हैं। भारतीय कंप्यूटर एमरजेंस रेस्पांस टीम (सीईआरटी-इन) की स्थापना की गई है जो भारतीय साइबर स्पेस की निगरानी करती है और बड़े खतरों के प्रति सजग एवं सतर्क करने में समन्वय का कार्य करती है तथा देश में सरकारी एवं निजी उपयोक्ताओं तथा संगठनों के बीच होने वाले हानिकर आक्रमणों का पता लगाती है। बैंक/वित्तीय संस्थाओं के इन्फ्रास्ट्रक्चर को इस प्रयोजन से महत्वपूर्ण पाया गया है। एक राष्ट्रीय साइबर समन्यवयन केंद्र की भी स्थापना की गई है।

19. भारतीय रिज़र्व बैंक ने 2 जून 2016 को बैंकों में साइबर सुरक्षा संरचना के संबंध में अनुदेश जारी किए हैं। मुझे उम्मीद है कि आप में से कई लोगों ने उन अनुदेशों को देखा होगा। अन्य बातों के साथ-साथ परिपत्र में यह अपेक्षा की गई है कि बैंक अपने बोर्ड द्वारा अनुमोदित साइबर सुरक्षा नीति लागू करें ताकि साइबर-संकट प्रबंध योजना बनाई जा सके, निरंतर चौकसी की व्यवस्था की जा सके, हार्डवेयर, साफ्टवेयर, नेटवर्क डिवाइसेस आदि खरीदते समय/कनेक्ट करते समय सुरक्षा पहलुओं का आकलन किया जा सके, उपभोक्ता सूचना की रक्षा सुनिश्चित की जा सके, असामान्य सुरक्षा घटनाओं को भारतीय रिज़र्व बैंक के साथ साझा किया जा सके, परिपत्र में दी गई बेसलाइन अपेक्षाओं के अनुरूप साइबर सुरक्षा कि तैयारी में कमी का मूल्यांकन किया जा सके तथा साइबर सुरक्षा परिचालन केंद्र स्थापित किया जा सके। भारतीय रिज़र्व बैंक ने **आईटी परीक्षण और साइबर सुरक्षा से संबंधित एक विशेषज्ञ पैनल** (अध्यक्ष: श्रीमती मीना हेमचंद्रा) गठित किया है जिसमें आईटी जगत से प्रतिनिधि सदस्य शामिल किए गए हैं। यह पैनल बैंकों में आईटी परीक्षण/साइबर सुरक्षा पहल में मदद करता है, परीक्षण रिपोर्टों की समीक्षा करता है तथा कार्रवाई योग्य सुझाव प्रदान करता है। भारतीय रिज़र्व बैंक ने अक्तूबर 2015 में विस्तृत आईटी परीक्षण का कार्यक्रम प्रारंभ किया है। यह प्रस्ताव है कि यह परीक्षण 2016-17 के दौरान 30 से अधिक प्रमुख बैंकों में किया जाए तथा 2017-18 तक सभी बैंकों में यह परीक्षण कर लिया जाए। रिज़र्व बैंक ने साइबर सुरक्षा लैब

की भी स्थापना का प्रस्ताव किया है, जो आईटी परीक्षकों को बैंक में साइबर सुरक्षा के विश्लेषण में सहायता प्रदान करेगा। भारतीय रिज़र्व बैंक अपनी आईटी सहयोगी संस्था {द रिज़र्व बैंक सूचना प्रौद्योगिकी (रिबीट) प्रा.लिमि.} को भी कार्यशील करने की प्रक्रिया में है। रिबीट का अधिदेश अन्य बातों के साथ-साथ यह भी है कि वह आईटी सिस्टम एवं वित्तीय क्षेत्र की साइबर सुरक्षा (संबंधित अनुसंधान सहित) से जुड़े मुद्दों पर फोकस करेगा और रिज़र्व बैंक द्वारा विनियमित संस्थाओं की लेखापरीक्षा एवं मूल्यांकन में सहायता प्रदान करेगा।

20. मुझे यह देखकर प्रसन्नता हो रही है कि आईडीआरबीटी ने जुलाई 2016 में साइबर सुरक्षा पर तैयार की गई व्यापक जांच-सूची जारी की है जो विशेषज्ञों के पैनल द्वारा तैयार की गई है जिसमें उद्योग एवं अकादमिक क्षेत्र से विशेषज्ञ शामिल हैं। मैंने देखा है कि जांच-सूची में साइबर सुरक्षा के व्यापक पहलुओं को समाहित किया गया है जैसे उद्यम नियंत्रण, आईटी इन्फ्रास्ट्रक्चर सुरक्षा, अंतिम सुरक्षा, सुरक्षा निगरानी तथा आउटसोर्सिंग सुरक्षा। मुझे भरोसा है कि बैंक/वित्तीय संस्थाएं जब अपनी संस्था में ऐसी प्रथाओं को लाएंगे तब इस जांचसूची में उल्लिखित सर्वोत्तम प्रथाओं को इसके मुकाबले में बहुत उपयोगी पाएंगे।

बैंकों से अपेक्षाएं

21. अब मैं बैंकों से की गई कुछ अपेक्षाओं को साझा करना चाहूंगा। सबसे पहली बात यह है कि निदेशक मंडल प्रौद्योगिकी संबंधी मामलों में सक्रिय रूप से शामिल हो जाए। आईटी रणनीति को कारोबार की कार्यनीति से बिलकुल समरूप बनाना है। प्रौद्योगिकी में किए जा रहे प्रयासों को देखते हुए बोर्डों के लिए प्रभावी तरीके से प्रौद्योगिकी को अपनाना मुश्किल होगा यदि उनके पास प्रौद्योगिकी संबंधी क्षेत्रों के विशेषज्ञ नहीं होंगे। **साइबर जोखिम सहित प्रौद्योगिकी जोखिम को उसी तरह से माना जाना चाहिए जिस प्रकार से बैंक कोई अन्य निहित जोखिम का सामना कर रहे हैं जैसे क्रेडिट जोखिम, बाज़ार, परिचालनगत जोखिम** तथा बोर्ड को यह तय करना होगा कि उनकी वहन क्षमता कितनी है, वे कौन से अवशिष्ट जोखिम उठाना चाहेंगे तथा निराकरण की कौन सी रणनीति अपनाना पसंद करेंगे। प्रौद्योगिकी अपनाने के नाम पर जहां बैंक विभिन्न प्रकार के गैजेट्स खरीदने में सक्रिय हैं, हमें अनेक संस्थाओं में यह देखने को मिला है कि इन डिवाइसेस के कॉन्फिगुरेशन को बहुत महत्व दिया गया है और वह कार्य वेंडर पर छोड दिया गया है। प्रभावशीलता हार्डवेयर, मिडिलवेयर, साफ्टवेयर, आपरेटिंग सिस्टम, एप्लीकेशंस, नेटवर्क डिवाइसेस, कम्यूनिकेशन डिवाइसेस आदि में मौजूद हैं। अत: कोई भी नया डिवाइस खरीदते समय/लागू करते समय तथा साल्यूशन लेते समय बहुत अधिक ध्यान दिए जाने की ज़रूरत है। **साइबर अपराधी भी बढ़चढ़कर स्मार्ट फोन साफ्टवेयर से होने वाली प्रभावशीलता का दुरुपयोग कर रहे हैं जो मालवेयर से आपरेटिंग सिस्टम को रुग्ण बना रहे हैं।** जो बैंक मोबाइल बैंकिंग के माध्यम से बड़े पैमाने पर सेवाएं दे रहे हैं उन्हें इस उभरते हुए जोखिम के प्रति सुरक्षा की ओर ध्यान अवश्य देना चाहिए।

22. चिंता का एक अन्य क्षेत्र **पैच प्रबंधन है।** ओआएमएस द्वारा पैच जारी किए जाते हैं जब उन्हें ज्ञात प्रभावशीलता को प्रेषित कर दिया जाता है और यदि पैच को समय पर रोलआउट नहीं किया जाता है तो हम व्यावहारिक रूप से दुरुपयोग के लिए दरवाज़ा खोल देते हैं। उपयोक्ता प्रबंधन काफी हद तक साझा-पासवर्ड की अपेक्षित प्रथा, कोई पासवर्ड न होना, एडमिनिस्ट्रेटर स्तर पर स्वतंत्र उपलब्धता दिनांकित प्राधिकृत उपयोक्ता सूची को सामान्य स्थान पर छोड़ देने में लापरवाही बरतते हैं। प्राय: नये उपयोक्ता के सृजन की तथा उयोक्ताओं की सूची की समीक्षा करने एवं निष्क्रिय उपयोक्ता को सूची से हटाने की कोई तेज प्रक्रिया मौजूद नहीं होती है। उसके बाद प्रत्यक्ष सुरक्षा को लागू करने का मुद्दा सामने आता है। मैंने देखा कि प्रत्यक्ष रूप से एक्सेस नियंत्रण प्रणाली मौजूद है लेकिन उसके इस्तेमाल के लिए आग्रह नहीं किया जाता है। इसके अलावा, वेंडर पर निर्भरता बढ़ती जा रही है, और कई बार केवल वेंडर को मालूम होता है कि सिस्टम को कैसे आपरेट किया जाए। वेंडर की सुविधा के हिसाब से ग्राहक की सूचनाएं भंडारित की जाती हैं, वह भी पर्याप्त सुरक्षा व्यवस्था किए बिना। एक अन्य चकित कर देने वाली बात मैंने नोट की है कि जहां बैंक यह दावा करते हैं कि उनके पास कुशल संसाधन नहीं हैं, वहीं एक ही वेंडर अनेक बैंकों को महत्वपूर्ण सेवाएं प्रदान कर रहा होता है। इससे यह सवाल पैदा होता है कि क्या बैंक को पता है कि उन्हें आउटसोर्स वेंडर से प्राप्त हो रहा है, साथ ही उसकी डिलीवरी की क्वालिटी क्या है? समय पर यह निर्णय लेना कि क्षमता को बढ़ाया जाना, जरूरी है ताकि यह सुनिश्चित हो सके कि सेवाएं लगातार उपलब्ध हों और कारोबार में वृद्धि हो रही है। लोग और प्रक्रिया को पर्याप्त महत्व देने की आवश्यकता है, क्योंकि अच्छे कार्मिकों के बिना अच्छे से अच्छा सिस्टम भी फेल हो सकता है। निगरानी रखना सबसे महत्वपूर्ण है - जो पोर्ट विशेष कार्य के लिए खोला गया था क्या उसे कार्य समाप्त हो जाने के बाद समय पर बंद कर दिया

गया था, वह कौन है जो उन लाग्स का विश्लेषण करता है जिन्हें अनिवार्य रूप से सृजित किया गया था, घटनाओं को किस प्रकार से लिया जाता है, क्या विभिन्न सिस्टम में किए जा रहे इनपुट सुरक्षा आपरेशन केंद्र (एसओसी) से जुड़े हुए हैं, क्या जो अपवाद बताए जाते हैं उन्हें उचित स्तर तक पहुंचाया जाता है आदि।

23. **बैंकों में सुरक्षा संस्कृति में बेहतर बदलाव लाने की आवश्यकता है।** एक पक्के मकान में शाखा के होने पर यदि तिजोरी के लिए अच्छा ताला लगाने का सिस्टम नहीं है, या दीवारों में दरारें पड़ी हुई हैं, छत टपक रही है, क्या बैंकों ने इस पर ध्यान दिया है। डिजिटल संसार में क्या यह ज़रूरी नहीं है कि इस प्रकार से छत के टपकने, दरारों को तथा प्रभावित होने की संभावना के लिए उचित कार्रवाई की जाए? ग्राहकों पर फिशिंग के आक्रमण बढ़ रहे हैं। क्या यह बैंकों की जिम्मेदारी नहीं है कि वे अपने ग्राहकों को शिक्षित करें और आसपास कुछ ऐसे कार्य करें कि धोखेबाज़ इतनी आसानी से न निकलने पाएं? यह देखते हुए कि ग्राहक इतने ज्यादा संगठित इलेक्ट्रॉनिक अपराध के सामने नहीं टिक पाएगा, **भारतीय रिज़र्व बैंक ने एक ऐसी संरचना लागू की है जिसमें ग्राहक के सुरक्षा उपाय की दृष्टि से अनधिकृत इलेक्ट्रॉनिक बैंकिंग लेनदेन में ग्राहक की देयता को सीमित किया गया है।** इसी प्रकार, चाहे प्रौद्योगिकी सेवा देने वाला हो या स्विफ्ट जैसा इन्फ्रास्ट्रक्चर उपलब्ध कराने वाला हो, क्या यह वेंडर की जिम्मेदारी नहीं है कि वह यह सुनिश्चित करे कि उनके एजेंट हर समय समस्त प्रकार की इलेक्ट्रॉनिक सुरक्षा अपेक्षाओं को पूरा करें और उनका संपूर्ण परिदृश्य उल्लिखित कारोबार करने के लिए पर्याप्त रूप से सुरक्षित है? मेरा मानना है कि समाज को यह देखना होगा कि इस उभरते डिजिटल परिदृश्य को पहचानें तथा अपने-अपने स्तर पर छोटे छोटे प्रयास करें ताकि हमारा डिजिटल संसार जो हमारे लिए सुविधा मुहैया कराता है तथा उपभोक्ताओं को आराम उपलब्ध कराता है, उसकी सुरक्षा से किसी प्रकार का समझौता न करे।

समापन

24. अपनी बात समाप्त करते हुए मैं पुन: कुछ बिंदुओं को बताना चाहूंगा:

- साइबर सुरक्षा पूरे विश्व में, खासतौर से वित्तीय क्षेत्र में एक महत्वपूर्ण क्षेत्र के रूप में उभरा है जिसपर ध्यान देने की आवश्यकता है,
- **साइबर की घटनाएं अधिकांशत: अंतिम उपयोक्ता को निशाना बनाने के बजाए वित्तीय संस्थाओं को लक्ष्य करने की ओर बढ़ती जा रही हैं।** इस प्रवृत्ति की जीता जागता उदाहरण कारबनाक से सिद्ध है, जो एक बहुत बड़ी उन्नत किस्म की बनी रहने वाली चुनौती (एपीटी) स्वरूप का आक्रमण है जो पूरे विश्व में वित्तीय संस्थाओं के खिलाफ किया जा रहा है। इस एपीटी आक्रमण में हैरान करने वाली बात यह है कि वे अपने रास्ते बदल लेते हैं तथा उनकी योजना बहुत सावधानीपूर्वक होती है, जिसमें उपभोक्ता के ब्योरे चुराने के साइबर अपराधी तरीके अपनाने या मालवेयर से प्रत्येक आनलाइन बैंकिंग सेशन के साथ काम्प्रोमाइज करने के बजाय कारबनाक गिरोह ने बैंक की आंतरिक प्रणाली और परिचालनों को लक्ष्य किया था, फलस्वरूप इसमें अनेक चैनलों में डकैती डाली गई और लगभग 1 बिलियन अमरीकी डालर की चोरी की गई।
- साइबर जोखिम को शून्य तक नहीं लाया जा सकता है। इसलिए तुरंत बहाली लाने की योजना तैयार रहना महत्वपूर्ण है ताकि बाद में होने वाला नुकसान कम से कम हो। **ऐसी स्थितियों में वित्तीय संस्थाओं तथा सार्वजनिक प्राधिकारियों के बीच समन्वय की एक रूपरेखा बनाए जाने की आवश्यकता है।**

25. डिजिटल संसार बड़ी तेजी से बढ़ रहा है और इसलिए प्रौद्योगिकी को सावधानीपूर्वक अपनाया जाना चाहिए, प्रयोजनपरक होना चाहिए तथा वैल्यू बढ़ाने वाली होनी चाहिए। आईटी सुरक्षा को बेहतर बनाने के लिए बैंको को चाहिए कि वे इसके बारे में स्टाफ/ग्राहकों में अधिक जागरूकता पैदा करें तथा प्रशिक्षण दें। इस प्रयास के पहले कदम के रूप में स्टाफ तथा ग्राहकों को इस बात से सावधान किया जाना चाहिए कि वे संदेह परक ईमेल न खोलें, अज्ञात व्यक्तियों के ईमेल न खोलें, जाली वेबसाइट, विशिंग पर अपने व्यक्तिगत खाते के ब्योरे आदि न डालें।

26. जहां वित्तीय क्षेत्र दशकों से लगातार इस बात के लिए कार्य कर रहा है कि धोखाधड़ी की रोकथाम की जाए तथा धोखाधड़ी को पहचानने एवं उससे बचाव की प्रणाली को सुदृढ़ बनाया जाए, वहीं उनके आंतरिक परिचालन नेटवर्क के प्रति

चुनौती थोड़ी कम आंकी जाती रही है जब तक कारबनाक जैसी घटनाएं नहीं घट जाती हैं। इन उभरती परिस्थितियों में बैंकों को सावधान रहना है कि बैंक की आंतरिक कोर प्रणाली से ही आक्रमण हो सकता है और इस प्रकार के आक्रमण से प्रभावित होने से बचें। बैंकों को 'साइबर हायजीन' की प्रैक्टिस करनी चाहिए और मुझे उम्मीद है कि बोर्ड एवं शीर्ष प्रबंधतंत्र इस महत्वपूर्ण कार्य के लिए जितनी जल्दी हो सके संवेदनशीलता पैदा कर लेंगे। इस पहल में सीआइएसओ की भी बहुत ही महत्वपूर्ण भूमिका है कि वे बोर्ड तथा वरिष्ठ तंत्र की सहायता करें जिसमें आईटी पर, सूचना सुरक्षा आडिट, ग्राहक संप्रेषण, धोखाधड़ी प्रबंधन तथा क़ानूनी पहलुओं पर फोकस किया जाए। **हमारा विचार है कि सीएसआईओ की भूमिका परिचालन स्तर से बढ़ा कर रणनीति के स्तर पर कर दी जानी चाहिए।**

27. मैं सेमिनार की सफलता की कामना करता हूं और उम्मीद करता हूं कि इसमें होने वाली चर्चाएं सभी के लिए फायदेमंद होंगी और आगे चलकर बैंकिंग क्षेत्र को अधिक सुरक्षित, कुशल एवं पारदर्शी बनाने के लिए उपाय तलाशने में मददगार साबित होंगी।

धन्यवाद !