*लक्ष्यित आक्रमण: देश की महत्वपूर्ण मूलभूत सुविधाओं का संरक्षण और क्षमता निर्माण**

आर. गांधी

यह मेरे लिए प्रसन्नता का विषय है कि आज मैं यहां सायबर सुरक्षा तथा सायबर की चुनौतियों से महत्वपूर्ण मूलभूत सुविधाओं की रक्षा करने के संबंध में हुई चर्चाओं जिसके साथ इस महत्वपूर्ण क्षेत्र में क्षमता निर्माण की बात जुड़ी हुई है, के समापन पर उपस्थित हूं। मैं व्यवस्थापकों को यह थीम रखने के लिए बधाई देता हूं कि जिसमें सायबर सुरक्षा से संबंधित घटनाओं पर चिंताएं प्रकट की जा रही हैं।

2. आज हम एक ऐसे संसार के महत्वपूर्ण दोराहे पर खड़े हैं जिसमें सूचना एवं संचार प्रौद्योगिकी(आईसीटी) का तेजी से उन्नत उपयोग किया जा रहा है तथा जहां इन सुविधाओं के दुरुपयोग से न केवल वित्तीय नुकसान हो रहा है और सामान्य गतिविधियां बाधित हो रही हैं, अपितु लोगों का विश्वास भी समाप्त हो रहा है। आज के विश्व में जीवन के प्रत्येक क्षेत्र में हर चीज में आईटी का इस्तेमाल निहित है; चाहे वह कारोबार हो या वित्तीय क्षेत्र हो, आईसीटी का उपयोग व्यापक होता जा रहा है; यहां तक कि एक साधारण सी चीज जैसे बत्ती जलाने का कार्य भी आईसीटी के उपयोग से किया जा रहा है, इसके अलावा, नेटवर्क डिवाइसेस अब इसका मानदंड बन गई हैं। नई संकल्पनाएं जैसे केंद्रीकृत प्रोसेसिंग प्रणाली, इंटरनेट जैसी चीजें और मोबाइल कंप्यूटिंग ने जीवन को आसान सा बना दिया है; लेकिन इसमें जोखिम भी मौजूद हैं, जिसमें सबसे बड़ा जोखिम सायबर सुरक्षा का है। वित्तीय प्रणाली जो आर्थिक गतिविधियों का शक्तिशाली केंद्र मानी जाती है, इसका आसानी से शिकार हो सकती है क्योंकि न सिर्फ इसलिए कि इसमें सूचना और संचार प्रौद्योगिकी का सर्वाधिक इस्तेमाल होता है बल्कि वित्तीय अपराध धन के मामले में आसानी से कर लिए जाते हैं; इससे सायबर सुरक्षा और भी महत्वपूर्ण हो जाती है।

3. बैंकिंग क्षेत्र में हाल में हुई प्रगति तथा भुगतान और निपटान प्रणाली ने ग्राहकों की सुविधा बढ़ा दी है तथा समय, स्थान एवं चैनल के चयन को लेकर काफी लचीलापन आ गया है। लेकिन इससे ग्राहकों तथा बैंकों को सायबर आक्रमण के जोखिम का खतरा भी पैदा हो गया है। जहां बैंकों की संरचना ऐसी है कि वे जोखिम को सहन करने की शक्ति रखते हैं तथा नुकसान एवं खर्च को वहन कर सकते हैं वहीं ग्राहक इसे सहन करने की स्थिति में नहीं हो सकते हैं। अपेक्षाकृत छोटी रकम कुछ हज़ार रुपए का जोखिम बुनियादी ज़रूरतों की चीजें खरीदन में परेशानी पैदा कर सकती हैं और अधिकांश ग्राहकों को यह जानकारी बहुत कम होती है कि वे सेवाओं के साथ दी गई सुरक्षा व्यवस्था का इस्तेमाल कैसे करें। हमने तो यह भी सुना है कि विश्व में अन्य स्थान पर एक प्रति लेनदेन एक पैसे की चोरी हुई है, आईसीटी क्षमताओं का दुरुपयोग किया गया है, जिससे बहुत बड़ी राशि का नुकसान हुआ था। यह माना जाता है कि ग्राहक को संवेदनशील पासवर्ड, पिन आदि नहीं बताना चाहिए और उसकी रक्षा स्वयं करनी चाहिए, क्योंकि वे यह अच्छी तरह अंतर नहीं कर पाएंगे कि ग्राहक सेवा से संबंधित जो कॉल आई है वह वास्तविक है या धोखेबाज़ परिचालकों से आई है।

सायबर अपराध का स्वरूप

4. सायबर अपराधी और आक्रमण वित्तीय क्षेत्र पर होते हैं और इसके उपयोगकर्ता कई चेहरे अपनाते हुए यह कार्य करते हैं। बहुत ही संगठित अपराधी हैं जो वित्तीय संस्थाओं पर आक्रमण करते हैं, जिनका मकसद गैर-क़नूनी तरीक से धन उड़ा ले जाना होता है। इसके अलावा ऐसे लोग हैं जो वित्तीय संस्थाओं से गोपनीय डाटा चुरा लेते हैं जिनमें ग्राहकों से संबंधित जानकारी भी होती है। बाद वाली चोरी में वे डाटा को फिल्डर करते हें, हालांकि उसमें तत्काल कोई नुकसान नहीं होता है। इसके बाद ये डाटा छोटे-छोटे अपराधियों के हाथों में जाते हैं, जो बैंक में सीधे-सीधे धोखाधड़ी करते हैं या ग्राहकों को अधिक जानकारी देने के लिए उकसाते हैं जैसे पासवर्ड या पिन नंबर देने के लिए और उसके बाद वास्तविक घटना घटित होती है।

* श्री आर. गांधी, उप गवर्नर, द्वारा सायबर और नेटवर्क सुरक्षा विषय पर सोचैम एवं यूरोप, स्ट्रासबोर्ग, फ्रांस द्वारा 29 जुलाई 2016 को होटल हयात, भीकाजी कामा प्लेस, नई दिल्ली में आयोजित नौवें वार्षिक सम्मेलन में समापन सत्र में दिया गया भाषण। श्री एस गणेश कुमार, मुमप्र द्वारा दी गई सहायताके प्रति आभार।

5. इस प्रकार के आक्रमणों में वे बैंक अधिकारियों के रूप में स्वांग रचते हैं तथा ग्राहकों से जानकारी प्राप्त करते हैं, इसके लिए वे इसे-उसे फोन करते हैं, फोन नंबर उन्हें विभिन्न स्त्रोतों से प्राप्त हो जाते हैं, या फिर आंख बंद करके कोई भी नंबर डायल कर लेते हैं और कई बार ऐसा करते रहने से सफलता मिल ही जाती है।

6. अन्य प्रकार के सायबर अपराध भी हैं जो धोखाधड़ी से लेनदेन करके धन की चोरी करते हैं या फिर विवरण बदल देते हैं ताकि वे भारी रकम निकाल कर भाग जाएं। ऐसे मामलों में ग्राहकों से सीधे संपर्क नहीं किया जाता है, लेकिन इनमें ब्योरे मालवेयर से या अन्य माध्यमों से प्राप्त किए जाते हैं। हाल ही में हुई इस प्रकार की घटना ने होश उड़ा दिए हैं। मैं आपका ध्यान उस घटना की ओर आकर्षित करना चाहूंगा जिसे हमारे एक बैंक ने रिपोर्ट किया था, जिसे संभवतः आप सभी जानते होंगे, खासतौर से जब इसी प्रकार की घटना हमारे पड़ोसी देश के केंद्रीय बैंक में घटित हुई हो और जो हमारे ज़ेहन में अभी ताज़ा बनी हुई है।

7. इसके अतिरिक्त अन्य सायबर-आक्रमण होते हैं जिसे हम सायबर-संघर्ष कहते हें। यह एक संगठित आक्रमण होता है; कभी-कभी यह बड़े आतंकवादी संगठनों की मदद किया जाता है और कभी शासन प्रायोजित की आड़ में किया जाता है, जो दुश्मन राष्ट्र के विरुद्ध सूचना संबंधी आस्तियां प्राप्त करने के लिए किया जाता है।

8. विभिन्न प्रकार के सायबर अपराध के लिए स्वाभाविक है कि अलग-अलग प्रतिक्रियाएं होंगी और उन चुनौतियों से लड़ने के लिए अलग- अलग तरीके बनाए गए हैं जिसके टूल्स एवं इस्तेमाल के तरीके अलग स्वरूप के हैं। मैं यह समझता हूं कि दिन में होने वाली चर्चाओं के दौरान इनपर विस्तार से चर्चा की जाएगी इसलिए मुझे इनपर विस्तार से बताने की आवश्यकता नहीं है। लेकिन मैं इस संबंध में बनाए गए पांच प्रकार के हुक्मनामों के बारे में बताना चाहूंगा जो पूरी तरह से सायबर संबंधी जोखिमों के प्रभाव को दूर करने केलिए बने हुए हैं।

रक्षा संबंधी रणनीतियां - पछताने से बेहतर है सुरक्षा करना

9. रोकथाम करने एवं पता लगाने को रोकने से संबंधित रणनीतियां विशिष्ट लिंक पर आधारित होती हैं जिसकी सुरक्षा की जाती है। वित्तीय लेनदेन के लिए ईकोसिस्टम में केवल बैंक एवं उनके ग्राहक ही शामिल नहीं हैं बल्कि नेटवर्क सेवा देने वाले, आईटी इंफ्रास्ट्रक्चर प्रदाता, नियंत्रण सेवा प्रदाता जैसे डाटा सेंटर, साफ्टवेयर डेवलपर्स, सुरक्षा समाधान प्रदाता तथा एंड-प्वाइंट डिवाइस प्रदाता जिनका इस्तेमाल वित्तीय सेवा के उपयोग के लिए किया जाता है, साथ ही एटीएम भी शामिल हैं जो हो सकता है कि बैंक के स्वयं के न हों/इन डिवाइसों की व्यवस्था की गई हो।

10. समस्त ईकोसिस्टम के लिए जिन डिवाइसों का प्रयोग किया जाता है उनसे बड़ी मात्रा में सूचनाएं एवं गतिविधियों का अंबार प्राप्त होता है, जिनमें महत्वपूर्ण जानकारियां होती हैं जो संभावित आक्रमण, यहां तक आक्रमण होने से पूर्व की गतिविधियों का पर्दाफाश कर सकती हैं। लेकिन, जिस प्रकार से भारी भरकम लाग-डाटा जनरेट किया जाता है उसमें परंपरागत तकनीक के माध्यम से यह पता कर पाना संभव नहीं हो पाता है कि बाहर का कोई इसे ले रहा है। पारंपरिक तकनीकों से कई बार गलत अलार्म बजते हैं तथा वास्तविक गतिविधि में अड़चन पैदा करती है, जिससे असुविधा उत्पन्न होती है और उसके उपयोगकर्ताओं में उस उत्पाद की सुरक्षा एवं तकनीक के प्रति अविश्वास पैदा होता है।

11. अतः अब लोगों का ध्यान ऐसी तकनीक की ओर मुड़ रहा है जो नियम-आधारित न हों, लेकिन उनमें समान्य गतिविधियों के पैटर्न एवं त्रुटिपूर्ण तथा नुकसान पहुंचाने वाली गतिविधियों को पता लगाने की क्षमता हो। कहना गलत नहीं होगा कि इसके लिए मशीन की जानकारी एवं साफ्ट कंप्यूटिंग तकनीक की जनाकरी होना ज़रूरी है। ऐसी तकनीकों के प्रयोग से बिना झूठे अलार्म के चुनौतियों का सटीक पता लगाया जा सकता है। चूंकि प्रत्येक अलार्म के प्रति प्रतिक्रिया होती है और उसके लिए समय, धन एवं श्रमशक्ति लगती है, इसलिए एकसपर्ट सिस्टम की क्षमता का निर्धारण इस बात से होगा कि सामान्य गतिविधि पैटर्न से आकस्मिक विचलन कैसे हुआ और उसमें दुर्भावपूर्ण व्यवहार कहां है तथा इन उपकरणों की अहमियत सुरक्षा इंफ्रास्ट्रक्चर में कितनी है।

12. टूल्स के अलावा, महत्वपूर्ण इंफ्रास्ट्रक्चर के घटक जैसे कौशल, अनुभव एवं उस गतिविधि में लगाई गई श्रमशक्ति के प्रति सचेत रहना एवं उनकी सुरक्षा करना है। सुरक्षा के लिए अपेक्षित कौशल ज्ञान पारंपरिक आईटी कौशल से हटकर आपराधिक खोज के खोजी-

कौशल की ओर मुड़ रहा है, ऐसे डाटा वैज्ञानिक जो भारी मात्रा में डाटा की आवश्यकता को संचालित करते हैं उन्हें नये-नये तरीकों के साथ सायबर- अपराध से एक कदम आगे चलना होगा।

13. चूंकि समस्त सुरक्षा की ताकत उतनी ही है जितनी कि प्रत्येक कंपोनेंट की होती है इसलिए सभी हिताधारकों को चाहिए कि वे सूचना प्रणाली के प्रति चुनौतियों का मिलकर समाधान करें। इस तरह का मंच यह अवसर उपलब्ध कराता है कि हम आपसे में बात कर सकें तथा यह समझ सकें कि हममें से प्रत्येक की क्या भूमिका है हमें यह सुनिश्चित करना होगा कि हम जो कार्रवाई करें वह एक-दूसरे की सहायता के लिए हो न कि एक दूसरे के विपरीत हो।

सायबर सुरक्षा के लिए तैयारी - बैंकिंग में सुरक्षा के लिए पांच फरमान

14. मैं बहुत ही सामान्य अपेक्षा से अपनी बात शुरू कर रहा हूं - **अपने ग्राहक को जानिए** - यह मेरा पहला फरमान है। आप सभी अपने ग्राहक को जानिए या केवायसी से भलीभांति परिचित हैं। केवायसी के बारे में बहुत कुछ कहा जा चुका है, चर्चा की जा चुकी है और बहुत से ब्योरे दिए जा चुके हैं, इसलिए मैं उन्हें दुबारा नहीं बताना चाहूंगा; बस इतना कहना पर्याप्त होगा कि हमें अपने ग्राहक को जानना अनिवार्य है, यदि नहीं जानेंगे तो उसके परिणाम भुगतने के लिए तैयार रहें जो हमारे कार्य के उद्देश्य के प्रतिकूल हो सकता है।

15. मेरा दूसरा फरमान यह है कि **अपने कर्मचारियों को जानिये -** अधिकांश सायबर अपराध भीतर के लोगों की मिलीभगत से कहीं न कहीं घटित हुए हैं, जिनमें सामान्य रूप से संगठन के कर्मचारी शामिल होते हैं जिसे सायबर सुरक्षा आक्रमण का लक्ष्य बनाया जाता है। इसलिए किसी भी संगठन के लिए यह जरूरी है कि भर्ती के समय वह न केवल कर्मचारी के पूर्व-इतिहास के बारे में सत्यापन करे, बल्कि कर्मचारी के आचरण पर लगातार निगरानी रखे, संगठन के संसाधनों के परिचालनात्मक उपयोग की उसकी प्रवृत्ति कैसी है, अपने साथियों के साथ एवं अधीनस्थों के साथ उसका व्यवहार कैसा है और इसी प्रकार की अन्य कई बातें। आईटी टूल्स कर्मचारियों के व्यवहार एवं व्यवाहरगत प्रवृत्तियों के बारे में बहुत सी जानकारी प्रदान करते हैं, इसलिए संगठनों के लिए आवश्यक है कि इन पहलुओं को काफी महत्व दें।

16. तीसरा फरमान यह है - **आप अपनी आईटी प्रणाली अद्यतन रखें और सभी प्रकार के जोखिमपूर्ण घटकों से मुक्त रखें** जैसे वायरस, स्पैम, मालवेयर, स्पूफिंग साफ्टवेयर आदि-आदि। आजकल केंद्रीकृत आईटी प्रणाली की सुविधा उपलब्ध है जिसमें प्रणाली को अद्यतन बनाने एवं उसपर निगरानी रखने का कार्य केंद्रीकृत रूप से सुनिश्चित किया जाता है।

17. चौथा फरमान यह है कि **आप आईटी गवर्नेंस का अधिकतम प्रावधान रखें।** इस क्षेत्र में जो मुख्य आवश्यकता है अच्छी आईटी परंपरा जैसे वित्तीय लेनदेन के लिए मेकर एंड चेकर, आईटी आधारित परिचालनों के लिए बहु-दृष्टि सिद्धांत, सिस्टम एवं आपरेशनल लॉग की नियमित निगरानी, आईटी प्रणाली की निरंतर, आवधिक रूप से तथा सुपरिभाषित तरीके से लेखापरीक्षा करना तथा उसके बाद जहां आवश्यक हो सुधारात्मक कार्रवाई करना, और एक अलग सीआईएसओ(मुख्य सूचना सुरक्षा अधिकारी) रखना जो संगठन में आईटी की गुणवत्ता, स्थायित्व एवं आईएस सुरक्षा पर सतत रूप से निगरानी रखे।

18. मेरा आखिरी फरमान यह है कि श्रृंखला से जुड़े समस्त खिलाड़ियों के बीच **आप सायबर सुरक्षा जागरूकता सतत रूप से बनाए रखें।** सायबर संबंधी चुनौतियां विश्व में तेजी से बदल रही हैं और आज की चुनौती कल पुरानी बन जाती है। यदि सतत रूप से सायबर सतर्कता सुनिश्चित कर ली जाती है तो उसके बाद जागरूकता पैदा करने, शिक्षा देने, लागू करने, जांच करने ट्रायल करने तथा उन्नयन करने की सतत प्रक्रिया बनी रहनी चाहिए। यह वही क्षेत्र हैं जिनमें हम प्रायः ढिलाई बरतते हैं और जिनका दुरुपयोग सायबर-प्रलोभियों द्वारा किया जाता है।

19. अब मैं यह बताना चाहूंगा कि हमारे देश का केंद्रीय बैंक इस संबंध में क्या कर रहा है। आईटी के कार्यान्वयन का एक व्यापक ढांचा उपलब्ध कराने की दृष्टि से रिज़र्व बैंक अति सक्रिय रहा है और सुरक्षा ढांचे के मामले में परामर्शी एवं समरूपता का दृष्टिकोण अपनाता रहा है। उस दिन से जब भारतीय रिज़र्व बैंक ने सबसे पहले कंप्यूटरीकरण के बारे में मार्गदर्शन दिया था, तभी से हम ग्राहकों की उभरती आवश्यकताओं को पूरा करने में आईटी की भूमिका तथा सायबर

संबंधी पहलुओं सहित इसके अवसर एवं प्रौद्योगिकी के उपयोग की चुनौतियोंके प्रति सजग रहे हैं। मैं आपका ध्यान कुछ ऐसी पहल की ओर आकर्षित करना चाहता हूं जो भारतीय रिज़र्व बैंक ने इस संबंध में हाल में की हैं।

20. रिज़र्व बैंक ने हाल ही में 2 जून 2016 को बैंकों में सायबर सुरक्षा ढांचे से संबंधित व्यापक दिशानिर्देश जारी किए हैं। ये दिशानिर्देश पूर्व में किए गए कार्यों के आधार तैयार किए गए हैं जिसमें सायबर की चुनौतियों एवं चुनौतियों को दूर करने के ढांचे तथा सूचना आस्तियों की सुरक्षा पर फोकस किया गया है। मैं आपका ध्यान पुनः हाल की एक सायबर चुनौती की ओर दिलाना चाहूंगा जो हमारे एक बैंक में घटित हुई है। लेकिन इस घटना में कोई मौद्रिक नुकसान नहीं हुआ था। हालांकि अभी इस नतीजे पर नहीं पहुंचा जा सका है कि यह घटना किस प्रकार और कैसे हुई है। लेकिन संवेदनशील प्रणाली जैसे धन-प्रेषण पर सतर्कता बरतने की आवश्यकता है क्योंकि एक बार फिर इसी में यह घटना हुई है, खासतौर से इस घटना में सिस्टम कन्फिगुरेशन एवं प्रणाली को नियंत्रित करने में मानव पहलू शामिल हैं। बैंकों को रोकथाम की प्रणाली लगाने की ज़रूरत है जैसे सिस्टम के आसपास उपयुक्त नियंत्रण ढांचा रखना, लेनदेन का वास्तविक/लगभग वास्तविक समय आधार पर समाधान करना, संदेश सृजन एवं प्रेषण पर नियंत्रण रखना, इंटरफेसेस को समय पर सुरक्षा पैचेस लगाना, यदि कोई हो; लेनदेन पर कड़ी नज़र रखना तथा यूएसबी को बंद कर देना, तथा जुड़े हुए नोड्स पर इंटरनेट एक्सेस करने पर निगाह रखना। इसी प्रकार समान रूप से समय पर पता लगानेवाले उपाय रखना भी महत्वपूर्ण हैं। बेहतर होगा कि इस प्रकार की घटना का सामना करने के लिए हम स्वयं को तैयार रखें और एक तीव्र संकटकालीन प्रबंधन योजना लागू रखें। मुझे उम्मीद है कि बैंक परिपत्र के प्रावधानों का पालन करने केलिए यथाशीघ्र कदम उठाएंगे। अब समय आ गया है कि उभरती हुई चुनौतियों का सामना करने के लिए सायबर सुरक्षा तैयारी को और बेहतर बनाया जाए।

21. सायबर संबंधी घटनाओं के खतरे को रोकने के लिए सूचनाओं का प्रसारण करना महत्वपूर्ण है। जहां रिज़र्व बैंक, बैंकों से सायबर घटनाओं के बारे में सूचनाएं प्राप्त करता है, वहीं उन घटनाओं के बारे में भी हासिल करता है जिनमें धन या सूचनाओं का नुकसान नहीं हुआ था, इन सूचनाओं को समस्त बैंकों के साथ साझा किया जाता है और सर्वोत्तम प्रथाओं के अनुरूप सुझाव भी दिए जाते हैं। आईडीआरबीटी के पास भी इस प्रकार की सूचनाओं को साझा करने की व्यवस्था है और वे बैंकों के सीआईएसओ के साथ जेनरिक पहलुओं को साझा करते हैं। मुझे आशा है कि ये सब मिलकर बैंकों में सायबर सुरक्षा से संबंधित उनकी क्षमताओं को बेहतर बनाने में मदद करेंगे।

22. मैं बड़ी सकारात्मकता के साथ अपनी बात समाप्त करना चाहूँगा। अर्थव्यवस्था के अन्य क्षेत्रों के समान बैंकिंग क्षेत्र भी बदलाव लाने के प्रति अत्यधिक जिम्मेदारीपूर्ण भूमिका निभा रहा है और स्वयं को तेजी से उभरती चुनौतियों से सामना करने के लिए तैयार करता रहा है। इसने यह भी सिद्ध कर दिया है कि न केवल अच्छी तरह स्वयं को तैयार कर लिया है बल्कि तेजी से तैयार किया है ताकि किसी भी प्रकार की नकारात्मक घटना के होने पर उससे कहीं तेजी से वह उसपर प्रतिक्रिया दे सके। मुझे उम्मीद है कि यही स्थिति सायबर सुरक्षा के क्षेत्र में भी दिखाई देगी तथा बैंकों के ग्राहकों के दिमाग पर विश्वास की छाप अंकित करेंगे। इससे यह सुनिश्चित हो सकेगा कि बैंक सुरक्षित एवं संरक्षित प्रोसेसिंग वातावरण प्रदान कर रहे हैं जहां जमाकर्ता की राशि सुरक्षित है तथा जहां अन्य ग्राहक भी बैंकिंग लेनदेन सुरक्षित एवं संरक्षित तरीके से कर सकते हैं।

23. मुझे विश्वास है की आज के इस सम्मेलन से कई सबक हासिल हुए होंगे। मुझे यह भी यक़ीन है कि जब आप अपनी संस्थाओं में वापस जाएंगे तब इन्हें परिचालनों में इस्तेमाल करेंगे। मुझे आमंत्रित करने के लिए और मेरे विचारों को सुनने के लिए आप सभी का आभार और आपके लिए सुरक्षित एवं संरक्षित आईटी आधारित परिचालनों के लिए शुभकामनाएं।

24. धन्यवाद!