भारतीय बैंकों में आईटी सुरक्षा के नये प्रतिमान*

के. सी. चक्रवर्ती

श्री एम. वी. नायर, अध्यक्ष, आईबीए और अध्यक्ष एवं प्रबंध निदेशक, यूनियन बैंक ऑफ इंडिया, श्री बी. सम्बामूर्ति, निदेशक, आईडीआरबीटी, श्री श्यामलाल घोष, अध्यक्ष, डीएससीआई, डॉ. के. रामकृष्णन, सीईओ,आईबीए, गणमान्य वक्तागण एवं पैनलिस्ट, आईटी एवं आईटी सुरक्षा प्रोफेशनल्स, गणमान्य अतिथिगण, देवियो एवं सज्जनो।

2. सूचना आज के व्यवसाय के मूल में है और सूचना के विपुल भंडार को उपयोग में लाने, उसे मिलाने और संसाधित करने में सूचना प्रौद्योगिकी का सर्वव्यापी प्रभाव निश्चायक है। इस परिदृश्य में यह सुनिश्चित करना अधिक महत्वपूर्ण हो जाता है कि निजता के स्वीकृत मानदंडों का पालन करते हुए सूचना को गोपनीय रखा जाए और प्रयोक्ताओं को उसे उपयुक्त समय पर उपलब्ध कराया जाए। यह बैंकिंग क्षेत्र के मामले में विशेष रूप से तर्कसंगत है जहां दैनंदिन परिचालन सूचना और सूचना संसाधन पर केंद्रित हैं जो बदले में प्रौद्योगिकी पर अत्यधिक निर्भर है। ज्ञान भागीदार के रूप में बैंकिंग प्रौद्योगिकी में विकास एवं अनुसंधान संस्थान के सहयोग से भारतीय बैंक संघ और भारतीय आंकड़ा सुरक्षा परिषद् (डीएससीआर) द्वारा ठ भारतीय बैंकों में सुरक्षा ढांचेठ विषय पर संयुक्त रूप से आयोजित यह सम्मेलन इस प्रकार न केवल उपयुक्त है, बल्कि बैंकों के लिए प्रासंगिक भी है। इस विषय पर संयुक्त प्रयास अत्यंत प्रशंसनीय है और आज के इस सम्मेलन के विषय पर गणमान्य श्रोताओं के समक्ष अपना विचार प्रस्तुत करना मेरे लिए बड़े गौरव की बात है।

3. एक व्यवसाय के रूप में बैंकिंग में ग्राहकों द्वारा जताये गये विश्वास के आधार पर जोखिमों का प्रबंधन शामिल है। यदि इस लक्ष्य को हासिल किया जाना है तो यह आवश्यक हो जाता है कि सुरक्षा संबंधी सभी चिंताओं, विशेषकर ग्राहक संवेदनशील आंकड़ों को प्रभावी ढ़ंग

* 26 अप्रैल 2010 को मुंबई में आयोजित भारतीय बैंकों में सुरक्षा ढांचे पर आईबीए-डीसीएसआई सम्मेलन में भारतीय रिजर्व बैंक के उप-गवर्नर डॉ. के. सी. चक्रवर्ती द्वारा दिया गया उद्घाटन भाषण। श्री जी. पद्मनाभन, श्री एस. गणेश कुमार और श्री ए. माधवन से मिले सहयोग की भूरि-भूरि सराहना की जाती है।

से समाधान किया जाए ताकि यह सुनिश्चित किया जा सके कि विश्वास के स्तर को अच्छी तरह से बनाये रखा जाए और सूचना आस्तियां अपेक्षित भूमिका अदा करें। जबकि हरेक बैंकर वित्तीय जोखिमों के निहितार्थ को समझता है, प्रौद्योगिकी तथा सूचना प्रौद्योगिकी के बड़े पैमाने पर कार्यान्वयन से उत्पन्न जोखिम उतनी अच्छी तरह से परिभाषित नहीं है। इस प्रकार बैंकों में सुरक्षा काफी महत्वपूर्ण हो जाता है जिसमें सूचना तथा सूचना प्रणालियों की सुरक्षा से संबंधित विभिन्न कारकों के अलावा प्रत्यक्ष सुरक्षा शामिल है। इन सभी का प्रभाव बैंक की प्रतिष्ठा जोखिम पर पड़ता है।

4. प्रौद्योगिकी ने महत्वपूर्ण नेटवर्किंग और विभिन्न प्रकार के वितरण माध्यमों के माध्यम से बैंकिंग के कार्यक्षेत्र, पहुंच और व्याप्ति को इस कदर बढ़ा दिया है कि अब दूरियां सिमट गयी हैं। इसके अलावा, बैंकिंग 'कहीं भी और कभी भी बैंकिंग', एटीएम नेटवर्कों के माध्यम से प्रदान की जाने वाली सेवाओं के प्रचुरोद्भवन, बैंकों में सूचना प्रौद्योगिकी आधारित तत्काल विप्रेषण, ग्राहक भुगतान, मोबाइल भुगतान जैसी सुविधाओं और इसी तरह की कई अन्य सुविधाओं के माध्यम से सर्वव्यापी हो रही है। आईसीटी समर्थित वित्तीय समावेशन की विशाल परियोजना बैंकिंग सेवाओं को पूर्णतः समावेशी बनाकर भारतीय बैंकिंग के समूचे परिदृश्य को बदलने के लिए पूरी तरह से तत्पर है।

5. प्रौद्योगिकी के कार्यान्वयन और साथ ही भारतीय रिजर्व बैंक द्वारा इसके सुगमीकरण से बैंकों को परिचालनात्मक तथा विधिक दोनों परिप्रेक्ष्यों में फायदा पहुंचा है। इसके अलावा, भारतीय रिजर्व बैंक ने कई नवोन्मेषी प्रौद्योगिकी आधारित प्रणालियों के व्यापक ढांचा प्रदान किया है। इंटरनेट बैंकिंग संबंधी दिशानिर्देश और 2001 में सूचना प्रणाली सुरक्षा / लेखा परीक्षा के लिए दिशानिर्देश बैंकों द्वारा सुरक्षित प्रौद्योगिकी आधारित परिचालन सुनिश्चित करने की दिशा में प्रारंभिक पहलें थीं। समय के साथ तालमेल बिठाते हुए और अंतर्राष्ट्रीय पद्धतियों को क्रमबद्ध करते हुए भारतीय रिजर्व बैंक ने मोबाइल बैंकिंग और प्रीपेड (स्टोर्ड) मूल्य कार्डों के संबंध में विस्तृत दिशानिर्देश जारी किये हैं। तत्काल सकल भुगतान (आरटीजीएस) जैसी सुव्यवस्थित रूप से महत्वपूर्ण भुगतान तथा निपटान प्रणालियों और इलेक्ट्रॉनिक समाशोधन प्रणाली (जमा तथा नामे समाशोधन), राष्ट्रीय इलेक्ट्रॉनिक निधि अंतरण (एनईएफटी) प्रणाली, राष्ट्रीय इलेक्ट्रॉनिक समाशोधन प्रणाली (एनईसीएस), क्षेत्रीय इलेक्ट्रॉनिक समाशोधन प्रणाली (आरईसीएस) जैसी अन्य खुदरा भुगतान प्रणालियों की स्थापना के साथ इसने बैंकिंग के तौर-तरीके बदल दिये हैं और आज के ग्राहकों के पास चुनने के लिए नाना विकल्प हैं। इन सभी में संबंधित प्रणालियों के केंद्र में सुरक्षा तथा संरक्षा की भावना होती है।

6. एक प्रमुख क्षेत्र जहां आईटी सुरक्षा महत्वपूर्ण हो जाती है वह संप्रेषण के माध्यम के रूप में आईटी का प्रयोग करते हुए सूचना के पारेषण से संबंधित है। पारंपरिक रूप से, कागज आधारित प्रणालियां कुछ नियंत्रणों के अधीन रही हैं ताकि यह सुनिश्चित किया जा सके कि वास्तविकता, प्रामाणिकता आदि से संबंधित आधारभूत अपेक्षाओं को पूरा किया जा सके। इनमें हस्ताक्षर का सत्यापन करने के साथ यह सुनिश्चित करना शामिल है कि उनमें कोई संशोधन नहीं है या यदि कोई संशोधन हैं तो उसे उपयुक्त रूप से अभिप्रमाणित किया गया है तथा इसी प्रकार अन्य कार्य। सूचना प्रौद्योगिकी आधारित परिदृश्य में ये पहलू न केवल आईटी आधारित सूचना के प्रवाह की गति के कारण, बल्कि गलत अनुदेशों के चलते उत्पन्न होने वाले संभावित नुकसान के कारण भी अधिक महत्वपूर्ण हो जाते हैं।

7. पिछले दशक के दौरान ग्राहकों को उपलब्ध करायी जाने वाली बैंकिंग सेवाओं के तौर-तरीके में आमूल-

चूल परिवर्तन हुआ है। कोर बैंकिंग प्रणालियों का कार्यान्वयन बैंकिंग सेवाओं तक कहीं से भी पहुंच प्रदान करने में और ग्राहक के साथ बैंक के एक ग्राहक के रूप में, न कि किसी खास शाखा के ग्राहक के रूप में व्यवहार करने में महत्वपूर्ण वरदान साबित हुआ है। एटीएमों के अंतर-संयोजन से ग्राहक को पुनः एक बैंक के बजाय वित्तीय क्षेत्र के एक ग्राहक के रूप में रूपांतरित कर दिया है। साथ ही, बैंकिंग क्षेत्र में सूचना प्रौद्योगिकी आधारित परिदृश्य में सुरक्षा खामियों की पहचान करने की दिशा में महत्वपूर्ण प्रयास किये हैं और उनका प्रभावी ढंग से समाधान किया है। बैंकों द्वारा किये गये उपायों की पर्याप्तता की समीक्षा का अब उपयुक्त समय आ गया है। हालांकि बैंक और आईटी उद्योग ने अपनी प्रणालियों की सुरक्षा के लिए कई संस्तर तैयार किये हैं, तथापि धोखेबाजों, हैकरों और विभिन्न प्रकार की ऐसी विस्मयकारी संस्थाओं ने सुरक्षा के विभिन्न संस्तरों को तोड़ने के प्रयास किये हैं। जब अनुप्रयोग संस्तर को मजबूत बनाया गया तब नेटवर्क संचार को तोड़ने पर ध्यान दिया गया। जब नेटवर्क उपकरण निर्माताओं ने सुरक्षा प्रोटोकॉल सर्वर को तोड़ना अत्यंत कठिन बनाते हुए उसे मजबूत बनाया तब इंटरनेट सर्वरों पर आक्रमण शुरू कर दिया गया। फिशिंग जैसे कार्य ग्राहकों तथा बैंकरों दोनों से उच्चस्तरीय सुरक्षा अपनाने की अपेक्षा करते हैं। हालांकि ये उदाहरण इंटरनेट बैंकिंग से संबंधित हैं, अद्यतन आयाम मोबाइल बैंकिंग की सुरक्षा से संबंधित हैं। चूंकि आईसीटी का दायरा व्यापक होता जा रहा है, सुरक्षा खामियां भी बढ़ रहीं हैं जिसमें बैंक तथा ग्राहक पिछड़ रहे हैं। अतः यह आवश्यक हो जाता है कि बैंकर, विनियामक आईसीटी विनिर्माता, सॉफ्टवेयर प्रोफेशनल और लेखा-परीक्षक सभी कपटपूर्ण प्रयासों के सफल होने से पहले एक नियमित कार्यकलाप के रूप में सुरक्षा खामियों की तत्परतापूर्वक पहचान करने, उनकी प्रत्याशा करने और उन पर रोक लगाने की दिशा में निरंतर मिलकर काम करें। यह बात ध्यान में रखी जाए कि सूचना सुरक्षा के दो महत्वपूर्ण आयाम हैं, अर्थात्

i. सुरक्षा आस्तियों में निवेश और उस पर वास्तविक सूचना का संरक्षण।

ii. जब भी और जहां भी आवश्यक हो, उपयोग के लिए आस्तियों की उपलब्धता।

8. धोखाधड़ी या प्रयतित धोखाधड़ी का प्रबंध प्रतिक्रिया दिखाने में प्रत्युत्तर काल की चुनौती प्रस्तुत करता है जो आगे की धोखाधड़ियों और ग्राहक से संबंधित महत्वपूर्ण सूचना की हानि को टालने के लिए काफी महत्वपूर्ण है। यदि साइबर अपराधों का तत्काल प्रत्युत्तर नहीं दिया जाता है, तो उन्नति, भूमंडलीकरण और सीमापार बैंकिंग के चलते विशिष्ट भौगोलिक क्षेत्रों से साइबर अपराध गहरी पैठ कर लेंगे। त्वरित कार्रवाई और एक सामान्य अम्ब्रेला के नीचे रिपोर्ट करने की प्रणाली से संपूर्ण उद्योग लाभान्वित होगा जिसके लिए त्द्वह समय में शुरू की जाने वाली कार्रवाई निर्दिष्ट करते हुए निश्चित मानक स्पष्टतः सूचित किये गये हैं। यद्यपि सर्ट (सीईआरटी अर्थात् कंप्यूटर आपदा प्रत्युत्तर टीम) की अपेक्षाओं का अनुपालन इस मुद्दे का कुछ सीमा तक एक समाधान करेगा, अतएव सुरक्षा-भंग की रिपोर्ट करने, बड़े भंग के लिए त्वरित प्रत्युत्तर टीम, अनुपालन की निगरानी और विनियामकों को रिपोर्ट करने के लिए वित्तीय क्षेत्र के लिए एक समर्पित संस्थागत ढांचा रखना उचित होगा। मुझे विश्वास है कि आईडीबीआरटी ऐसे ढांचे के निर्माण की दिशा में केंद्रीय भूमिका अदा कर सकता है। धोखाधड़ी की संभावना का पूर्वानुमान लगाना और उन्हें टालने के लिए प्रणाली लागू करना एक बड़ी चुनौती होगी। सूचना तथा संचार प्रौद्योगिकी आस्तियों की सुरक्षा तथा संरक्षा और समग्र रूप से बैंक और विशेष रूप से ग्राहक से संबंधित आंकड़े तथा सूचना की सुरक्षा से संबंधित मूलभूत चिंताओं का समाधान करना आवश्यक है।

9. इस पृष्ठभूमि में मैंने सोचा कि ऐसी उत्कृष्ट पद्धतियों का एक सेट सुनिश्चित करना उचित होगा जिनसे आईटी सुरक्षा का मूल्य बढ़े। मैं ''बैंकों में आईटी की सुरक्षा / प्रबंध के दस आदेशक'' के रूप में उनका नामकरण करना पसन्द करता हूं। अब मैं इनमें से हरेक की संक्षेप में चर्चा करना चाहूंगा।

i. यह सूचना प्रौद्योगिकी (आईटी) के कार्यान्वयन में मानव कारक का पर्याप्त ध्यान रखेगा। आईटी सुरक्षा तकनीकी मुद्दों की अपेक्षा व्यक्ति सापेक्ष पहलू अधिक है। यह बैंकों के आंतरिक व्यक्तियों और ग्राहकों दोनों के लिए लागू होता है। ऐसे आंतरिक व्यक्ति के प्रति अधिक सजग रहने की आवश्यकता है जिसे जरूरत से ज्यादा जानकारी हो और जब उसे उन्मुक्त पहुंच मिलेगी तो वह संबंधित बैंक पर कहन बरपा सकता है। उतना ही महत्वपूर्ण वह ग्राहक है जो कदाशयी इरादों से प्रौद्योगिकी की खामियों का लाभ उठाता है। इस प्रकार यह आवश्यक है कि आईटी सुरक्षा मानदंड लक्ष्यित श्रोतागण के अलावा प्रणाली से सीधे जुड़े लोगों पर पर्याप्त फोकस करें। इस संबंध में, इन अंशधारकों द्वारा समझी जाने वाली भाषा में सम्प्रेषण अत्यधिक महत्वपूर्ण हो जाता है।

ii. यह समूचे संगठन में आईटी सुरक्षा की व्याप्ति सुनिश्चित करेगा। पूरी दुनिया में यह माना तथा स्वीकार किया गया है कि यदि कार्यान्वयन ऊपर से संचालित हो तो आईटी सुरक्षा इष्टतम है। इसमें यह संकेत निहित है कि बैंकों के शीर्ष प्रबंधन वर्ग को आईटी सुरक्षा का कार्यान्वयन सुनिश्चित करने के लिए एक मिशनरी उत्साह प्रदान करना चाहिए। उनके प्रयास यह सुनिश्चित करेंगे कि आईटी सुरक्षा से संबंधित प्रक्रियाएं बैंक के सभी स्तरों पर प्रभावी ढंग से कार्यान्वित की जाएं।

iii. इसमें आईटी सुरक्षा संबंधी स्पष्ट नीतियां और प्रक्रियाएं होंगी। भारत में बैंकिंग की एक मुख्य विशेषता इसके परिचालन क्षेत्रों से संबंधित है। तथापि आईटी सुरक्षा डॉमेन उसी प्रकार के अनुपालन स्तर की डींग नहीं मार सकता है। निर्धारित पद्धतियां तथा प्रक्रियाएं न केवल कर्मचारियों की कार्यकुशलता बढ़ाती हैं, बल्कि यह सुनिश्चित करने में काफी सहायक भी होती हैं कि सुरक्षित तथा संरक्षित तरीके से परिचालनों के संचालन के लिए एक सच्चे मार्गदर्शक के रूप में कार्य करने के अलावा इसमें उद्देश्यों की स्पष्टता हो। यह भी आवश्यक है कि ये प्रक्रियात्मक अपेक्षाएं स्टाफ के सभी वर्गों में प्रसारित की जाएं ताकि उनका हमेशा पूर्ण रूप से अनुपालन हो सके।

iv. यह उपयुक्त समय पर कार्रवाई करेगा। किसी भी संगठन में पूर्ण आईटी सुरक्षा प्राप्त करना लगभग असंभव है। इस प्रकार, आईटी सुरक्षा से संबंधित चिंताओं और उल्लंघनों का समाधान करना महत्वपूर्ण हो जाता है। सतर्कता शब्द यहां समयनिष्ठता है, केवल वे ही बैंक सुरक्षा उल्लंघनों की जबरदस्त मार से बच सकते हैं जो त्वरित सुधारात्मक कार्रवाई करते हैं। ऐसी त्वरित कार्रवाई तभी संभव है जब बैंकों द्वारा सुपरिभाषित प्रणालियों और प्रक्रियाओं को पहले से ही लागू किया गया हो। सुरक्षा का उल्लंघन करने के लिए किये गये प्रयासों पर विशेष ध्यान देने की जरूरत है क्योंकि ये स्वयं एक उत्कृष्ट प्रारंभिक चेतावनी संकेत देते हैं। यदि इन पर ध्यान नहीं दिया जाता है तो इससे भारी हानि हो सकती है और एक छोटी-सी चूक सही समय पर सही दिशा के अभाव के कारण अक्सर एक बड़ी घटना में तब्दील हो जाती है।

v. यह सुनिश्चित करेगा कि पर्याप्त संसाधन क्षमता का प्रावधान किया जाता है। एक प्रभावी आईटी सुरक्षा ढांचे को एकाकीपन में कार्यान्वित नहीं किया जा सकता है। यह आवश्यक है कि उन सभी संसाधनों का पर्याप्त

रूप से प्रावधान किया जाए जो इस उद्देश्य को पूरा करने में सहायक हों। इसमें पर्याप्त कार्मिक, प्रभावी तथा कार्यकुशल आईटी प्रणालियां, अच्छी वेंडर प्रबंधन नीतियां और सुदृढ़ आईटी / एआरई लेखा-परीक्षा व्यवस्था शामिल है। इनसे लागतें निश्चित रूप से जुड़ी हुई हैं किंतु आईटी सुरक्षा उल्लंघनों के घटे हुए प्रभाव से होने वाला लाभ इस संबंध में उपगत होने वाली लागत की क्षतिपूर्ति से अधिक होता है।

vi. यह इष्टतम व्यवसाय प्रक्रिया पुनर्विन्यास का प्रावधान करेगा। भारतीय बैंकिंग परिदृश्य में अधिकांश आईटी कार्यान्वयन मैनुअल कार्य प्रक्रियाओं की प्रतिकृति है जिन्हें सूचना प्रौद्योगिकी आधारित वातावरण में कार्य करने के लिए सिर्फ मोड़ा गया है। इसका परिणाम अनावश्यक प्रक्रियाओं की विद्यमानता और कार्यकुशलता की हानि है। व्यवसाय प्रक्रिया पुनर्विन्यास से लागत की बचत होती है, कार्य का प्रवाह बेहतर होता है, कार्यकुशलता में सुधार आता है और ग्राहक सेवा का स्तर बेहतर होता है क्योंकि व्यवसाय प्रक्रिया प्रणालियां परस्पर कार्यमूलक होती हैं अर्थात् प्रणाली की सीमा एकल कार्य के भीतर नहीं है बल्कि वस्तुतः सीमा-रेखाओं के पार जाती है।

vii. यह आईटी सुरक्षा के लिए अप्रचलन संबंधी मुद्दों का भी ध्यान रखेगा। शायद आईटी उद्योग आज के विश्व में एकमात्र ऐसा उद्योग है जहां उन्नति बहुत तीव्र है और हरेक उन्नति अपने पीछे अंगीकरण के लिए घटी हुई लागतें लाती है। जहां तक लागत का संबंध है, नेटवर्क आधारित संचार निम्नतम स्तर पर पहुंच गया है जबकि आईटी प्रणालियों की कीमतें घातांकीय रूप से कम हुई हैं। आईटी उद्योग में उत्पाद तथा रूपक (फीचर) के अप्रचलन की तीव्र मात्रा बैंकों के लिए एक कठिन चुनौती है। ऐसे अप्रचलन का मुकाबला बैंकों तथा उनके ग्राहकों के पारस्परिक लाभ के लिए सुव्यवस्थित तथा सक्रिय रूप से किया जाना चाहिए। इस ढंग से सावधानी बरती जानी चाहिए कि प्रौद्योगिकी अप्रचलन का ध्यान रखने के लिए उन्नयन वैज्ञानिक तरीके से और उन्नयन की आवश्यकता के आधार पर किया जाए। इससे बैंकों को प्रौद्योगिकी अप्रचलन की जाल में फंसने से बचने में सहायता मिलेगी क्योंकि इस जाल से निकलने के लिए भारी राशि की जरूरत पड़ती है।

viii. यह घटना प्रबंधन के लिए एक ढांचा प्रदान करेगा। सुरक्षा संबंधी घटनाओं की अनदेखी नहीं की जा सकती है। एक प्रभावी आईटी सुरक्षा ढांचे की दिशा में सर्वोत्तम साधन इस प्रकार वह होगा जो ऐसे सुरक्षा दृष्टांतों को स्वीकार करता है और संगठन के भीतर तथा विनियामकों को घटना की उपयुक्त रिपोर्टिंग के लिए एक ढांचा प्रदान करता है। ऐसी व्यवस्था सुरक्षा उल्लंघनों तथा ऐसे अन्य प्रयासों की पूरी जानकारी देगी किन्तु एकल सबसे बड़ा लाभकारी कारक ज्ञान-कार्मिकों के एक सेट का विकास होगा जिनके पास देश में बैंकों द्वारा किसी भी आईटी आधारित पहल की सफलता की कुंजी है जो यह डींग मार सकते हैं कि कुछ उत्कृष्ट आईटी कंपनियां प्रभावी आईजीआर द्वारा संचालित हैं।

ix. यह डाटा की गुणवत्ता और अखंडता का ध्यान रखेगा। आईटी सुरक्षा का सबसे महत्वपूर्ण घटक डाटा है जो सूचना प्रौद्योगिकी आधारित व्यवसाय प्रसंस्करण प्रणाली का भाग हो। डाटा पाना या सृजित करना कठिन है, इसका दुरुपयोग करना आसान है और किसी सार्थक विश्लेषण के लिए लाभकारी व्याख्या की दिशा में प्रेषित करना कठिन है। इसे लक्ष्य में रखते हुए बैंकों को डाटा की गुणवत्ता तथा अखंडता के उच्च स्तरों को लक्ष्यित करते हुए प्रभावी मानदंड तैयार करने चाहिए। इस अवसर पर मुझे सिमसन गारफिंकेल द्वारा लिखी गई

''डाटाबेस नेशन'' शीर्षक एक पुस्तक की याद आती है जो इक्वीसवीं शताब्दी में निजता के खत्म होने की रूपरेखा प्रस्तुत करती है। लेखक डाटा पॉयरेसी को नियंत्रित करने वाले विभिन्न पहलुओं को कुशलतापूर्वक स्पष्ट करता है और अंत में यह निष्कर्ष निकालता है कि अपने स्वयं की निजी सूचना का स्वामी व्यक्ति स्वयं नहीं होता है। बैंक इस श्रेणी में आना सहन नहीं कर सकते हैं और आंकड़े का परिष्करण एक ऐसा दृष्टिकोण है जो संरक्षी सुरक्षाओं के पर्याप्त स्तरों के साथ आंकड़ों का अच्छा प्रबंधन सुगम बनाता है।

x. यह एक जीवन शैली के रूप में आईटी सुरक्षा के लिए प्रावधान करेगा। अंतिम आदेशक रूपरेखा की तरह अधिक है, किंतु आईटी सुरक्षा संबंधी सभी पहलों के केंद्र-बिंदु में है। आईटी सुरक्षा को अकेले में नहीं देखा जा सकता है और न ही इसे मनमौजी ढंग से कार्यान्वित किया जा सकता है। आईटी सुरक्षा के अच्छे कार्यान्वयन के उदाहरणों से पता चलता है कि अच्छी आईटी सुरक्षा विशेषताएं सामान्य जीवन-चर्या में अनिवार्य अपेक्षाओं के रूप में अनुप्राणित हैं। बैंकों की तरह हमें अपने सामान्य दैनंदिन कार्यकलापों में सुरक्षा संस्कृति को अंतर्ग्रहण करना है। यह एक चुनौतीपूर्ण और दुष्कर कार्य है क्योंकि सामान्य मानव मस्तिष्क घटी हुई सुरक्षा की ओर एक सरल, अहस्तक्षेपपूर्ण दृष्टिकोण के प्रति अधिक अनुकूल है जिससे सुविधाएं बढ़ सकें। आईटी सुरक्षा से असुविधा नहीं बढ़ती है क्योंकि यह बढ़ी हुई लागतों के प्रति होता है, किंतु यह दीर्घावधि में किफायती होता है।

10. आदेशक निर्दिष्ट करने के बाद, आइए अब हम बैंकों के लिए तात्कालिक परिचालनात्मक प्रासंगिकता रखने वाले कुछ विचारों की चर्चा करें। हमने देखा है कि सुरक्षा मानक कई वर्षों से विकसित हो रहे हैं और हॉर्डवेयर तथा सॉफ्टवेयर अनुप्रयोगों की उन्नति के साथ परिपक्व हो रहे हैं। वित्तीय क्षेत्र भी वैश्विक मानकों के साथ सही तालमेल बिठा रहा है। सभी विनियंत्रित संस्थाओं के पास उनके बोर्ड द्वारा संचालित आईटी नीति है और इस नीति में सूचना सुरक्षा नीति जैसी कई उप-नीतियां हैं। मोबाइल बैंकिंग के लिए सुरक्षा मानक नवीनतम नीति है। बैंकों ने सूचना प्रणाली लेखा-परीक्षा के लिए भी व्यवस्था-तंत्र लागू किया है और बैंकों के बोर्ड की लेखा-परीक्षा समिति द्वारा इनकी गहन समीक्षा की जाती है। हालांकि ये विनियामक तथा विनियमित संस्थाओं की ओर से सचेतन प्रयास किये गये हैं। मुझे अब भी ऐसा लगता है कि सभी वित्तीय संस्थाओं में परिचालनगत जोखिमों, खासकर सूचना सुरक्षा जोखिमों के लिए एकसमान रूप से स्वीकृत मानक तथा प्रणालियां रखने की दिशा में कार्य करने के लिए पर्याप्त गुंजाइश है, यह इसी संदर्भ में है कि मैंने आईटी सुरक्षा के लिए मानक निर्धारित करने के प्रयास किये हैं। ये सामान्य परिचालनात्मक स्तरों में बैंकों के समक्ष मौजूदा जटिलताओं को और बढ़ाने के लिए आशयित नहीं हैं। दूसरी ओर, इनका अनुसरण करने वाले बैंक आईटी सुरक्षा से संबंधित अप्रचलनों से उत्पन्न होने वाले भावी आघातों के विरुद्ध अच्छी तरह से सुरक्षित होंगे। मुझे विश्वास है कि आज के विश्व में जहां सिर्फ योग्यतम के टिके रहने के अवसर हैं, हमारे बैंक न केवल टिके रहेंगे, बल्कि उत्कृष्ट सूचना तथा प्रौद्योगिकी का प्रयोग करते हुए उन्नति भी करेंगे और परिपक्व भी होंगे। सम्मेलन के दौरान विचार-विमर्श से श्रोतागण लाभान्वित होंगे और मुझे विश्वास है कि आप सभी अधिक प्रबुद्ध होंगे और कल के बेहतर ज्ञान कार्मिक होंगे। यही लक्ष्य है जिसे हमें हासिल करना है और इस दिशा में आप में से हरेक को सफलता की ढेर सारी शुभकामनाएं देता हूं। मुझे विश्वास है कि यह सम्मेलन आप सभी के लिए विचार उत्प्रेरक, उच्च ऊर्जा तत्वों से भरपूर और लाभप्रद होगा। सम्मेलन की सफलता के लिए ढेर सारी शुभकामनाएं।