*बैंकों में धोखाधड़ी का नियंत्रण : क्या करें और क्या न करें**

एस.एस. मूंदड़ा

श्री गोपालकृष्णन, उन्नत वित्तीय अनुसंधान एवं शिक्षण केंद्र (कैफ़ल) के निदेशक; बैंक एवं वित्तीय अपराध नियंत्रण कार्यक्रम के साथी सहभागीगण । सबसे पहले यह कहना चाहूंगा कि पिछले तीन महीनों में यह तीसरी बार है जब मैं धोखाधड़ी के बारे में बोल रहा हूं । मैंने नवंबर 2016 में 'बैंकों में धोखाधड़ी का नियंत्रण - प्रमुख चिंताएं एवं बैंकरों के लिए 12 सूत्र' विषय पर भाषण किया और पिछले महीने 'धोखाधड़ी जोखिम नियंत्रण - सरकारी और निजी बैंकों के बीच साझेदारी बढ़ाना' विषय पर अपनी बात कही, जिसमें मैंने 'समसामयिक परिदृश्यों', 'चुनौतियों' तथा धोखाधड़ी के खिलाफ सुरक्षा को मजबूत बनाने के लिए हम सामूहिक रूप से 'और क्या कर सकते हैं' विषयों पर ध्यान केंद्रित किया । यह महज एक संयोग नहीं हो सकता कि मैं इस विषय पर इतनी बार बोल रहा हूं । संभवत: इसका संबंध बैंकिंग क्षेत्र में धोखाधड़ी की घटनाओं में तेजी से हुई वृद्धि के साथ ही प्रणाली में धोखाधड़ी के जोखिम के काफी बढ़ जाने -दोनों से है । इन संगोष्ठियों/कार्यशालाओं में मेरे शामिल होने से बैंकिंग पर्यवेक्षक के रूप में भारतीय रिज़र्व बैंक द्वारा प्रणाली में धोखाधड़ी के जोखिम को नियंत्रित करने को दिया जाने वाला महत्व भी रेखांकित होता है । मैं इस मुद्दे पर हर बार इस उम्मीद से बोलता हूं कि इन संगोष्ठियों के प्रत्येक प्रतिभागी अपने संबंधित संगठनों में धोखाधड़ी के जोखिम को कम करने और नियंत्रित करने के लिए अधिक प्रतिबद्धता और संवेदनशीलता विकसित करेंगे । मैं, आज धोखाधड़ी प्रबंध की व्यापक थीम के कुछ अन्य आयामों को तलाशने की कोशिश करूंगा । किंतु, अपनी बात प्रारंभ करने के पहले मैं इस आयोजन और बेहद महत्वपूर्ण मामले पर बैंकों के वरिष्ठ पधाधिकारियों को एकत्र करने और मंथन करने के लिए मंच उपलब्ध कराने के लिए कैफ़ल की सराहना करना चाहूंगा ।

मैं अपने आज के भाषण के प्रथम हिस्से में साइबर सुरक्षा और साइबर धोखाधड़ी पर ध्यान केंद्रित करूंगा, और दूसरे हिस्से में साइबरस्पेस से बाहर की कुछ चिंताओं पर प्रकाश डालूंगा ।

साइबर सुरक्षा एवं धोखाधड़ी

2. हाल के समय में, हम लोगों ने भारत में और वैश्विक स्तर पर भी हाईप्रोफाइल साइबर घटनाएं देखा है । आपको बांगलादेश बैंक की घटना स्मरण होगी, जिसने बैंकों/केंद्रीय बैंकों को हिला के रख दिया और हमें साइबर सुरक्षा जोखिमों पर और बारीकी से नजर रखने को मजबूर किया । वैयक्तिक सूचनाओं की चोरी होने, ओटोमेटेड टेल्लर मशीनों (एटीएम) के दुरुपयोग होने और विभिन्न बैंकों पर डिस्ट्रीब्यूटेड डिनायल ऑफ सर्विसेस (डीडीओएस) के हमलों की घटनाओं में वृद्धि का रुझान दिखाई दे रहा है । हम स्विफ्ट संदेश प्रणाली का दुरुपयोग करते हुए धोखाधड़ी की एक घटना पहले ही देख चुके हैं, जिसे शुक्र है कि घटना के बाद बिना किसी मौद्रिक नुकसान के बचाया जा सका । हमें बहुत सी अन्य साइबर घटनाओं की भी सूचनाएं प्राप्त हो रही हैं, जैसे - रैन्समवेयर अटैक, एटीएम/डेबिट कार्ड की घटना और बैंक के सर्वर में अनधिकृत सेंध मारी। फिशिंग / विशिंग के हमले अधिक गूढ़ (सॉफिस्टिकेटेड) होते जाने से भी बैंकों के ग्राहक डरे हुए हैं ।

3. हाल के वर्षों में बैंकों और अन्य वित्तीय संस्थानों द्वारा प्रौद्योगिकी को अपनाए जाने में बहुत वृद्धि हुई है और अगर आज कोई बैंक डिजिटल संसार में उपलब्ध नहीं हो तो बाजार में प्रतिस्पर्धा करना उसके लिए लगभग असंभव हो जाएगा । प्रौद्योगिकी का उद्भव बैंकों के परिचालनों को संभव बनाने और उनमें अंतर करने वाले प्रमुख कारक के रूप में हुआ है, इसलिए सुरक्षा से संबंधित मामलों पर भली-भांति ध्यान दिए जाने की जरूरत है ।

4. ₹500 एवं ₹1000 के बैंक नोटों का वैधानिक दर्जा वापस लिए जाने के बाद देश भर में डिजिटल मोड में भुगतान को बहुत अधिक बढ़ावा मिला है । आधार समर्थित भुगतान

---

* सीएएफआरएल द्वारा 30 जनवरी 2017 को मुंबई में वित्तीय अपराध प्रबंध विषय पर आयोजित सेमीनार में दिया गया श्री एस.एस. मूंदड़ा, उप गवर्नर, भारतीय रिज़र्व बैंक का मुख्य भाषण । श्री मनोज शर्मा, श्री आर. रवि कुमार एवं डॉ. के. बालु से प्राप्त सहायता के प्रति आभार ।

प्रणालियां लोकप्रिय हो रही हैं और भुगतान की सुविधा प्रदान करने वाला हाल ही में प्रारंभ किया गया 'भीम' एप्प एक अन्य स्वागत योग्य कदम है । डिजिटल भुगतान प्रौद्योगिकी को तेजी से अपनाए जाने से अर्थव्यवस्था को बहुत से लाभ होंगे, किंतु हमें सुरक्षा संबंधी पहलुओं के बारे में जागरुक रहने की जरूरत है । इस पृष्ठभूमि के साथ, हमें कुछ अंतरराष्ट्रीय गतिविधियों पर नजर डाल लेनी चाहिए।

5. अक्तूबर 2016 में जी-7 के सदस्य देशों ने 'वित्तीय क्षेत्र के लिए साइबर सुरक्षा के मूलभूत तत्वों' की बात प्रारंभ की जिसके अंतर्गत साइबर सुरक्षा कार्यनीति और ढांचा, अभिशासन, जोखिम एवं नियंत्रण आकलन, निगरानी, प्रतिक्रिया, बहाली, सूचना साझा करने और निरंतर सीखने को मुख्य तत्वों के रूप में शामिल किया गया । वित्तीय बाजार आधारभूत संरचनाओं (एफएमआई) के लिए भुगतान एवं बाजार की आधारभूत संरचना समिति (सीपीएमआई), बीआईएस एवं अंतरराष्ट्रीय प्रतिभूति आयोग संगठन (आईओएससीओ) ने साइबर लचीलेपन से संबंधित दिशानिर्देश जारी किए हैं, जिनमें व्यापक वित्तीय स्थिरता के लक्ष्यों को सहारा देने के लिए प्राधिकारियों के आपस में सहयोग करने पर भी जोर दिया गया है । बैंक ऑफ इंग्लैंड (बीओई) ने "सीबीईएसटी" लागू कर दिया है, जो साइबर सुरक्षा की कमजोरियों, विशेषरूप से वित्तीय क्षेत्र की मुख्य संस्थाओं की, जांच करने के लिए एक नई संरचना है । हांगकांग के मौद्रिक प्राधिकार ने "साइबर सुरक्षा किलाबंदी की पहल" (सीएफआई) करने की घोषणा की है, जो बैंकों की साइबर सुरक्षा के स्तर को बढ़ाने के लिए समग्र पहल है ।

6. अपनी बात करें, भारतीय रिज़र्व बैंक ने बैंकों में साइबर सुरक्षा संरचना के संबंध में 2 जून 2016 को परिपत्र जारी किया है, जिसके तहत साइबर सुरक्षा की तैयारी को अनिवार्य बनाया गया है । बैंकों की साइबर सुरक्षा तैयारी की विस्तृत आईटी संबंधी जांच करने, कमियों की पहचान करने और उपचारात्मक उपायों की प्रगति की निगरानी करने के लिए भारतीय रिज़र्व बैंक के पर्यवेक्षण विभाग में विशेष प्रकोष्ठ (सी-एसआईटीई) का गठन किया गया है । 2016-17 के दौरान 30 से अधिक प्रमुख बैंकों को विस्तृत आईटी जांच के दायरे में लाने की योजना है । 2017-18 तक सभी बैंक इसके दायरे में होंगे । भारतीय रिज़र्व बैंक की सूचना प्रौद्योगिकी (आईटी) संबंधी अनुषंगी, द रिज़र्व बैंक इन्फर्मेशन टेक्नोलॉजी (आरईबीआईटी) प्रा. लिमिटेड कार्यशील हो चुकी है जिसको आईटी प्रणालियों के मुद्दों और वित्तीय क्षेत्र की साइबर सुरक्षा (संबंधित अनुसंधान सहित) के साथ ही रिज़र्व द्वारा विनियमित संस्थाओं के लेखापरीक्षण में सहयोग प्रदान करने का अधिदेश दिया गया है ।

7. 2 जून 2016 के परिपत्र के माध्यम से बैंकों को उनकी तैयारी में कमी के साथ ही साथ भारतीय रिज़र्व बैंक द्वारा निर्धारित आधारभूत अपेक्षाओं का आकलन करने और कमियों को पूरा करने के लिए समयबद्ध योजना तैयार करने को कहा गया था । आकलन से पता चलता है कि कुछ बैंकों को छोड़कर अन्य बैंकों में महत्वपूर्ण कमियां हैं । सार्वजनिक क्षेत्र के बैंकों में कमियां अधिक पाई गई हैं । इसके कारण बैंकों के बोर्ड और वरिष्ठ प्रबंध तंत्र भी इसकी ओर तत्काल एवं सतत् ध्यान दिए जाना आवश्यक हो जाता है । इस बदल चुके संसार में यदि बैंक के बोर्डों के पास इस संबंध में विशेषज्ञता नहीं होगी, तो यह बात बैंकों के सुचारू संचालन को मुश्किल बना देगी । दूसरी बात, सूचना प्रौद्योगिकी संबंधी सेवाओं और विशेषरूप से साइबर सुरक्षा के बजट आबंटन के पारंपरिक तरीकों में बड़े परिवर्तनों की आवश्यकता है ताकि जरूरत के अनुसार आकलन किया जा सके और मितव्ययी समाधान ढूंढ़े जा सकें । हाल के समय में एटीएम/डेबिट कार्ड की घटनाओं से उत्पन्न चिंताओं से स्पष्ट संदेश मिलता है कि साइबर सुरक्षा के मामले में बोर्ड को पहले ध्यान देने की जरूरत है । कुछ दिन पहले, Risk.net ने 2017 के शीर्ष 10 परिचालनगत जोखिमों के संबंध में लेख प्रकाशित किया और मुख्य जोखिम अधिकारियों के दिमाग में सबसे बड़ा जोखिम साइबर जोखिम होने का संकेत दिया ।

8. इस पृष्ठभूमि के साथ, मुख्य सूचना सुरक्षा अधिकारी (सीआईएसओ) की नियुक्ति में बोर्ड/वरिष्ठ प्रबंध तंत्र के जुड़ने का महत्व बढ़ता जा रहा है । यह आवश्यक है कि **पदानुक्रम में मुख्य सूचना सुरक्षा अधिकारी (सीआईएसओ) को पर्याप्त उच्च स्थान दिया जाना चाहिए**; जिसे प्रौद्योगिकी की बेहतर समझ हो, जो बैंक द्वारा अपनाई जाने वाली प्रौद्योगिकियों के सुरक्षा संबंधी पहलुओं को जाने, जो प्रतिक्रिया दे और जब कभी जरूरी हो तब **असुरक्षित उत्पादों को जारी करने से रोकने के**

लिए पर्याप्त शक्तियां धारण करता हो । हालांकि जमीनी हकीकत में अपेक्षित आराम की स्थिति नहीं होती । मैं इस मंच का प्रयोग करते हुए पुन: कहना चाहूंगा कि मुख्य सूचना सुरक्षा अधिकारी (सीआईएसओ) की भूमिका को स्पष्ट करने और तत्काल लागू करने की जरूरत है ।

9. 2 जून 2016 के हमारे परिपत्र में अलग से साइबर सुरक्षा नीति एवं साइबर संकट प्रबंध योजना के होने को भी अनिवार्य बनाया गया है । हम लोगों ने देखा है कि बहुत से मामलों में साइबर घटनाएं होने पर बैंक बिना सोचे अनौपचारिक रूप से प्रतिक्रिया देते हैं, जिसके कारण भावी जांच-पड़ताल भी खतरे में पड़ जाती है । वर्तमान परिस्थितियों में कोई साइबर घटना होने पर स्पष्ट रूप से निर्धारित भूमिका और जिम्मेदारियों के साथ पुख्ता कार्य-योजना का होना अत्यावश्यक है ।

10. उपचार से सावधानी भली, की पुरानी कहावत साइबर सुरक्षा पर भी लागू होती है । बैंकों के पास साइबर घटनाओं के प्रति मजबूत सुरक्षा प्रणाली का हमेशा उपलब्ध होने की जरूरत है । तथापि, हम लोगों ने देखा है कि बहुत बार, यंत्र के कॉन्फ्युगरेशन, पैच मैनेजमेंट, ओईएम समर्थित सॉफ्टवेयर, पासवर्ड प्रबंध या पोर्ट प्रबंध जैसे विशिष्ट छोटे विवरणों पर ध्यान नहीं दिया जाता या उन्हें पूर्णत: वेंडरों पर छोड़े जाने से अनपेक्षित प्रभाव पड़ता है । आंकड़े कहते हैं कि बाहरी लोगों द्वारा साइबर हमलों का पता लगाने में औसतन लगभग 6 महीने लगते हैं और भीतरी व्यक्तियों द्वारा हमलों के मामलों का पता लगाने में इससे भी अधिक समय लगता है । इसलिए, इस तरह की घटनाओं का जल्दी पता लगाने तथा प्रतिक्रिया का महत्व और बढ़ जाता है । साइबर हमलों का जल्दी पता लगाने और उन पर त्वरित कार्रवाई करने के लिए बैंकों को अपनी क्षमताएं बढ़ाने की जरूरत है । ऐसी किसी घटना के बाद वसूली किया जाना एक अन्य पहलू है, जिस पर अच्छी तरह विचार करने की आवश्यकता है ।

11. दुनिया भर ने यह सीख ली है कि साइबर हमलों से निपटने के लिए जागरुकता एवं जानकारी को साझा करने की भूमिका महत्वपूर्ण है । साइबर के विभिन्न पहलुओं की जानकारी बोर्ड के सदस्यों सहित सभी हितधारकों को होना जरूरी है । हम अक्सर देखते हैं कि इस आधार बिंदु को नजरंदाज किया जाता है।

12. भारतीय रिज़र्व बैंक ने सभी असामान्य साइबर-घटनाओं को 2 से 6 घंटे के भीतर रिपोर्ट करना अनिवार्य कर दिया है। हम लोगों ने पाया है कि घटनाओं की रिपोर्ट करने में बैंक काफी अधिक समय लेते हैं । एक बार रिपोर्ट किए जाने के बाद कारणों के विश्लेषण के परिणामों के साथ ही अन्वेषी (फॉरेंसिक) लेखापरीक्षा के परिणामों को भी तुरंत साझा किया जाना चाहिए । आप यह बात समझते ही हैं कि अन्य बैंकों को उचित चेतावनी जारी किए जाने के लिए साइबर-घटनाओं की समय में रिपोर्ट किया जाना बहुत महत्वपूर्ण है ।

13. संक्षेप में, साइबर चुनौती की समस्या से निपटने के लिए सभी हितधारकों को सम्मिलित रूप से काम करना होगा । हमारे प्रधानमंत्री का कहना है, 'मैं ऐसे भारत का स्वप्न देखता हूं, जहां पर साइबर सुरक्षा हमारी राष्ट्रीय सुरक्षा का अभिन्न अंग हो जाती है'[2]। जी हां, जब ऐसे संदेश देश के सर्वोच्च प्राधिकार की ओर से आते हैं, तब हमें कार्रवाई करने के लिए किसी और प्रोत्साहन की जरूरत नहीं होती है । मैं आश्वस्त हूं कि इस कार्यक्रम से आप बहुत कुछ सीखकर जाएंगे जो आपको अपने-अपने संबंधित संस्थानों में आईटी की आधारभूत संरचना में परिवर्तन के कारक बनने के साथ ही साथ ग्राहकों को धोखाधड़ी का शिकार होने से बचने के संबंध में शिक्षित करने के लिए समर्थ बनाएंगी ।

14. मैं, साइबर जगत से इतर अन्य प्रकार की धोखाधड़ी के बारे में बातें करने से पहले साइबर सुरक्षा से जुड़े उन तीन मुद्दों का जिक्र करना चाहूंगा जिनके बारे में मेरी इच्छा है कि इस सेमीनार के दौरान प्रतिभागी विचार-विमर्श करें । एक विषय, नीति निर्माताओं के विचार-विमर्श के लिए भी है -

क. प्रौद्योगिकी में जबर्दस्त तेजी से परिवर्तन हो रहा है । इसके विपरीत, मनुष्य धीमी गति से सीखने वाले होते हैं और परिवर्तन को स्वीकार करने में उससे भी अधिक धीमे होते हैं । ऐसा विशेषरूप से तब अधिक होता है जब मामला नई प्रौद्योगिकी का हो । इस पृष्ठभूमि के साथ, हमें स्वयं से यह प्रश्न करना चाहिए कि क्या हमें प्रौद्योगिकी समर्थित नए-नए उत्पादों को तीव्र गति से इस्तेमाल करने की जरूरत है या हम ऐसा सिर्फ प्रतियोगिता के कारण कर रहे हैं ? क्या आप मान चुके हैं कि नए उत्पादों से दक्षता में काफी वृद्धि होने वाली है और ग्राहकों के लिए यह बेहतर अनुभव होने वाला है ?

मैं यह बात कहना चाहता हूं कि बारंबार नई प्रौद्योगिकी को व्यवहार में लाने का परिणाम सिर्फ मानव संसाधनों को उनकी क्षमताओं से अधिक प्रयोग करने के रूप में आ सकता है और संभवत: इसका विपरीत प्रभाव पड़ सकता है ।

ख. साइबर धोखाधड़ी की ताजा घटनाओं में धोखेबाजी करने वालों द्वारा कंप्यूटरों में मालवेयर के प्रयोग की प्रवृत्ति बढ़ती हुई देखी जा रही है । ये मालवेयर धोखेबाजी किए जाने से कई दिनों एवं महीनों पहले कंप्यूटरों पर मौजूद रहता है । ये मालवेयर इनके अपेक्षित परिणाम प्राप्त करने के बाद स्वयं को समाप्त करने के लिए भी जाने जाते हैं । यह सचमुच चिंता की बात है, इसलिए हमें न सिर्फ हमारे कंप्यूटरों में मौजूद कमजोरियों की पहचान करने के लिए निरंतर रक्षात्मक होने और उन्हें नियंत्रित करने की जरूरत है बल्कि अहानिकर प्रतीत होने वाले अज्ञात प्रोग्रामों/मालवेयर का समय-समय पर पता लगाने की भी आवश्यकता है ।

ग. मैं, अगले जिस पहलू पर जोर देना चाहता हूं वह मानवीय व्यव्हार से संबंधित है । हमने बैंकिंग को हमेशा से भरोसे पर आधारित संबंधों के रूप में देखा है । हालांकि, जब हम साइबर सुरक्षा के बारे में बात करते हैं तब मैं यह मानने लगता हूं कि इसके समाधान की दृष्टि हमें 'किसी पर भी भरोसा' नहीं करना चाहिए । मैं यह इशारा कर रहा हूं कि फिजिकल और लॉजिकल एक्सेस कंट्रोल को अनिवार्य रूप से डिज़ाइन किए अनुसार कार्य करना चाहिए और इनकी एक्सेस सिर्फ उन कर्मचारियों को होना चाहिए जिनको एपलीकेशन सॉफ्टवेयर/प्रोग्रामों की गूढ़ताओं की 'जानने की आवश्यकता' हो ।

15. अंतत:, मैं नीति निर्माताओं के विचार-विमर्श हेतु साइबर जागरुकता (साइबर लिटरेसी) का मुद्दा उठाना चाहता हूं । जैसे ही हम डिजिटल संसार में पूर्णत: प्रवेश करते हैं, कर्मचारियों के साथ ही साथ ग्राहकों का साइबर जागरुक होना आवश्यक हो जाता है । मुझे ज्ञात है कि इज़राइल जैसे कुछ देशों ने साइबर जागरुकता को उनके स्कूली पाठ्यक्रम में शामिल कर दिया है । शायद, हमें भी इस दिशा में सोचने की जरूरत है । हमारे देश में सामान्य साक्षरता के मध्यम स्तर के मद्देनजर यह विशाल कदम हो सकता है, फिर भी यह उद्देश्य निरंतर प्रयासों के माध्यम से हासिल करने के काबिल है ।

मैं, अब साइबर जगत से निकलकर वास्तविक धरातल का रुख करना चाहूंगा ।

अग्रिमों से संबंधित धोखाधड़ी

16. वित्तीय वर्ष 2016 के दौरान सभी बैंकों द्वारा रिपोर्ट की गई धोखाधड़ी की घटनाओं में से 92 प्रतिशत हिस्सा अग्रिमों से संबंधित घटनाओं का था । ऐसा सार्वजनिक क्षेत्र के उपक्रम बैंकों में अधिक देखा गया और निजी तथा विदेशी बैंकों में कम। लगभग सभी मामलों में, हमने पाया कि उधारकर्ता के धोखापूर्ण घोषित किए जाने के 3 से 4 वर्ष पहले एक्सपोजर अनर्जक आस्ति के रूप में कालानुसार वर्गीकृत किया गया था। परिणामस्वरूप, ऐसा होने की तारीख और इसकी पहचान किए जाने की तारीख का अंतर बढ़ता जा रहा है । इसके अलावा, भारतीय रिज़र्व बैंक को उधार संबंधी खाते के धोखाधड़ीपूर्ण होने की रिपोर्ट किए जाने में प्रथम और अंतिम बैंक के बीच अंतराल भी बहुत अधिक है । यहां पर चिंता की कौन सी बात है ? जैसा कि आप जानते हैं, 'धोखाधड़ी' आपराधिक जुर्म है और किसी एक्सपोजर को प्रारंभ में चिह्नित (रेड फ्लेगिंग) करने में और बाद में इसे धोखाधड़ी घोषित करने में बैंकर की ओर से होने वाले किसी भी प्रकार के विलंब का कर्मचारी के आचरण और आंतरिक अभिशासन मानकों पर दूरगामी परिणाम होगा । बैंकों और बैंकरों पर आपराधिक जुर्म को सहयोग करने का आरोप लगाया जा सकता है । इसलिए, मेरा आपसे यह कहना है कि धोखापूर्ण खाते की पहचान करने और उसके इस प्रकार का होने की घोषणा बिना समय गंवाए करें । सर्वोत्तम कार्यपद्धति यह होगी कि अनुदेशों का अनुपालन सच्ची भावना के अनुरूप किया जाए और कंसोर्टियम की बैठकों में भाग लेते वक्त जिम्मेदारीपूर्ण तथा अग्रसक्रिय रुख अपनाएं।

17. खाते में धोखाधड़ी करनेवाले उधारकर्ताओं को बैंकों/ वित्तीय संस्थानों (एफआई)/एनबीएफसी इत्यादि के माध्यम से वित्तपोषण प्राप्त करने पर, दाण्डिक उपाय के रूप में, धोखाधड़ीपूर्ण राशि का पूर्ण भुगतान किए जाने की तारीख से, 05 वर्षों के लिए रोक लगा दी जाती है । इस अवधि के बाद, इस तरह के उधारकर्ता को ऋण देने के संबंध में विशिष्ट बैंक निर्णय ले सकता है । उपाख्यानात्मक साक्ष्यों और लेनदेन की की हमारी वास्तविक जांच से पता चला कि इस अनुदेश का हमेशा पालन नहीं किया जा रहा है । हाल ही में, हमारे समक्ष

एक मामला आया जिसमें किसी बैंक ने बहुत बड़े धोखाधड़ी पूर्ण खाते के मामले में 'हैंड होल्डिंग ऑपरेशन' की सुविधा प्रदान की ।

18. चेक का प्रतिरूपण (क्लोनिंग) किए जाने से संबंधित धोखाधड़ी हमारे लिए चिंता का विषय बनी हुई है । हमारे सामने ऐसे मामले आए हैं, जिनमें चेक की मूल प्रति ग्राहक के पास रहने के बावजूद धोखाधड़ी कर्ताओं द्वारा उसी श्रृंखला के चेक प्रस्तुत किए गए और उन्हें भुनाया गया । भारतीय रिज़र्व बैंक ने इस मामले में बैंकों को दिशानिर्देश नवंबर 2014 में जारी कर दिया है । धोखाधड़ी की घटनाओं को रोकने के लिए यह आवश्यक है कि इन दिशानिर्देशों का पालन किया जाए ।

लागों (मानव संसाधन) का जोखिम

19. अधिकांश पीएसयू बैंकों में कर्मचारियों की जनांकिकीय संरचना बहुत अनुकूल है और प्रारंभिक स्तर पर बड़े पैमाने में भर्ती की जा रही है । बैंक मानव संसाधन के भंडार में वृद्धि तो कर रहे हैं किंतु बैंकों के पास उन्हें प्रशिक्षित करने, तैयार करने और उनकी सेवाओं का प्रयोग करने की क्षमता नहीं है । इस प्रक्रिया में बैंकों पर लोगों के महत्वपूर्ण जोखिम में वृद्धि हो रही है ।

20. दो प्रकार के कर्मचारी समूहों, जिन्हें बोलचाल की भाषा में "डिजिटल इमिग्रेंट्स" (पुरानी पीढ़ी) और "डिजिटल नेटिव्स" (नई पीढ़ी) कहा जाता है, के बीच प्रौद्योगिकी की समझ में अंतर के कारण भी लोगों का जोखिम एक अन्य स्वरूप में प्रकट हो सकता है । विशेषरूप से, सरकारी क्षेत्र के बैंकों में; जो "मिसिंग मिडल" की समस्या से जूझ रहे हैं, पर्यवेक्षकों और पर्यवेक्षणाधीन लोगों के बीच अंतराल बहुत अधिक हो सकता है । यह नियंत्रण में कमजोरी के रूप में परिणत हो सकता है । इसलिए, बैंकों के बोर्ड और शीर्ष प्रबंध-तंत्र के लिए यह महत्वपूर्ण हो जाता है है कि धोखाधड़ी जोखिम प्रबंध ढांचे के समग्र हिस्से के रूप में वे लोगों के जोखिम को कम करने के उपाय करें ।

समापन

21. मेरा यह मानना है कि सिर्फ निरंतर सतर्कता बरतते हुए ही धोखाधड़ी-मुक्त ईको-सिस्टम को हासिल किया जा सकता है । दोहराव कहे जाने की आशंका के बावजूद, मैं बैंकरों के लिए 12 महत्वपूर्ण संदेशों/सूत्रों का जोर देकर उल्लेख करना चाहूंगा, जो मेरे हिसाब से धोखाधड़ी के जोखिम के बेहतर प्रबंध के लिए महत्वपूर्ण हैं । मैं इनका जिक्र एक अन्य सम्मेलन में कर चुका हूं । संक्षिप्त सारगर्भित अनुदेशात्मक कहावतों के रूप में सूत्रों की तरह, ये संदेश सहज एवं स्पष्ट हैं ।

सूत्र 1 : धोखाधड़ी के जोखिम की पहचान करने, घटना की रिपोर्टिंग करने, नियंत्रण, वितरण और कम करने की मजबूत व्यवस्था होनी चाहिए । सभी संवेदनशील क्षेत्रों में 'चार आंखों वाले सिद्धांत' का पालन, बिना किसी ढील के, अनिवार्य रूप से किया जाना चाहिए ।

सूत्र 2 : ऋण (क्रेडिट) संबंधी 5 'सी' - कैपेसिटी, कैपिटल, कोलेटरल, कंडीशन और कैरेक्टर का पालन करें ।

सूत्र 3 : निरंतर सतर्कता, मजबूत आंतरिक नियंत्रण एवं अनुपालन की संस्कृति को अपनाएं । कृपया यह ध्यान में रखें कि धोखाधड़ी आपराधिक जुर्म है ।

सूत्र 4 : स्मरण रहे कि प्रौद्योगिकीय चुनौतियों का समाधान हमेशा और जटिल प्रौद्योगिकी नहीं होती है ।

सूत्र 5 : लोगों के जोखिम को नियंत्रित करने के लिए जांच-परख को संस्थागत रूप प्रदान करें । संघर्ष की अधिकता नए प्रकार की सामान्य बात है, जिसका हमें सामना करना ही है । इन परिस्थितियों में, यह महत्वपूर्ण है कि नए भर्ती किए गए स्टॉफ को अपने संबंधित डैस्क में कार्य करने का समुचित प्रशिक्षण दिया जाए । मैं महसूस करता हूं कि कुछ तरह के अक्सर पूछे जाने वाले प्रश्नों (एफएक्यू) की मदद के साथ ही विधिवत दस्तावेजीकृत प्रणालियों का होना नए भर्ती किए गए स्टॉफ के लिए भी उपयोगी होगा ।

सूत्र 6 : धोखाधड़ी के जोखिम के प्रबंधक को समुचित शक्तियां प्रदान करें ।

सूत्र 7 : 3 सी - सीएफआर (सेंट्रल फ्रॉड रजिस्ट्री), सीआररआईएलसी एवं क्रेडिट ब्यूरो का व्यापक प्रयोग करें ।

सूत्र 8 : बाजार आसूचना (मार्केट इंटेलिजेंस) पर भरोसा करें ।

सूत्र 9 : कारोबारी विश्लेषण के टूल विकसित करें ।

सूत्र 10 : घाटा कम करें और वक्त की मांग होने पर इसे समाप्त करें।

सूत्र 11 : धोखाधड़ी के मामलों में बैड मनी की खातिर गुड मनी का अपव्यय न करें ।

सूत्र 12 : भारतीय रिज़र्व बैंक के विनियमों का सच्ची भावना के साथ अक्षरस: अनुपालन करें ।

22. मैं, अपनी बात समाप्त करते हुए कहूंगा कि इस तरह के कार्यक्रम अपेक्षित हुनर हासिल करने के लिए बहुत उपयोगी होते हैं। इनमें सहभागी अपने साथी प्रतिभागियों के व्यावहारिक अनुभवों से भी सीखते हैं । मैं, आज की सुबह यहां आमंत्रित किए जाने के लिए, श्री गोपालकृष्णन के प्रति एक बार फिर से आभार व्यक्त करता हूं और सम्मेलन की सफलता की कामना करता हूं ।