ભારિબેં/2015-2016/418 જેઠ 12, 1938 (શક)

બેંપવિ.કેકા.સીએસઆઈટીઈ/બીસી.11/33.01.001/2015-16 02 જુન 2016

અધ્યક્ષ / પ્રબંધક નિર્દેશક / મુખ્ય કાર્યપાલક અધિકારી

[બધી જ અનુસૂચિત વાણિજ્યિક બેંકો (ક્ષેત્રીય ગ્રામીણ બેંકોને બાકાત રાખતા)**]**

મહોદયા / પ્રિય મહોદય,

બેંકોમાં સાઇબર સિક્યૂરિટીની રુપરેખા

પ્રસ્તાવના

બેંકો અને તેમના સંઘટકો દ્વારા સૂચના પ્રૌદ્યોગિકી (information technology) નો ઉપયોગ ઝડપથી વધી રહ્યો છે અને આ હવે બેંકોની પરિચાલનીય કાર્યનીતિનુ એક મહત્વપૂર્ણ અંગ છે. ભારતીય રિઝર્વ બેંકે તારીખ 29 એપ્રિલ 2011ના એક પરિપત્ર ડીબીએસ.સીઓ.આઈટીસી.બીસી.સં.6/31.02.008/2010-11 ના માધ્યમથી માહિતી સુરક્ષા (information security), ઇલેકટ્રોનિક બેંકિંગ, તકનીકી જોખમ પ્રબંધન (Technology Risk Management) અને સાઈબર ઠગાઈ (જી. ગોપાલ કૃષ્ણ સમિતિ) ના સંબંધમાં માર્ગદર્શીકાઓ જાહેર કરી હતી જેમાં એમ દર્શાવવામાં આવ્યું હતું કે અમલ માટે બતાવવામાં આવેલા ઉપાયો સ્થાયી રહી શકે નહીં અને નવીન વિકાસ અને તે કારણે ઉત્તપન્ન થતી કઠીનાઈઓના આધાર પર બેંકોએ તેમની નીતિઓ, પ્રણાલિઓ અને ટેકનોલોજીને સક્રિય રૂપથી તૈયાર કરે / ઠીક કરે અને સંશોધિત કરતી રહે.

2. ત્યારથી, બેંકો દ્વારા ટેકનોલોજી ના ઉપયોગમાં આગળ વધારે વૃદ્ધિ થઈ છે. બીજી બાજુ, તાજેતરના ભૂતકાળમાં સાઈબર ઘટનાઓ/આક્રમણોની સંખ્યા, અંતરાલ અને પ્રભાવમાં પણ અનેકગણી વૃદ્ધિ થઈ છે, ખાસ કરીને બેંકો સહિત નાણાકીય ક્ષેત્રમાં વધુ પ્રમાણમાં વૃદ્ધિ થઈ છે જેનાથી એમ સંકેત પ્રાપ્ત થાય છે કે બેંકોમાં સુદૃઢ સાઇબર સુરક્ષા / આઘાત સહનીય (resilience) ઢાંચાને લાગૂ કરવાની તત્કાળ આવશ્યકતા છે અને બેંકો પર્યાપ્ત સાઇબર

સુરક્ષા માટે સતત તૈયાર રહે તે બાબત સુનિશ્ચિત કરવી આવશ્યક છે. બેંકિંગ પ્રણાલીમાં ખાસ પ્રતિબંધ વગર મળતા પ્રવેશ, તેમાં વિકસી રહેલા સાયબર ખતરાનું સ્વરૂપ, તેના સ્તર / વેગમાં વૃદ્ધિ, તેને મળતી પ્રેરણા અને હિકમતના બળ વિગેરેને ધ્યાનમાં રાખતા, એ આવશ્યક છે કે સાઇબર જોખમોથી નિપટવા માટે વર્તમાન સુરક્ષામાં સુધાર દ્વારા બેંકિંગ પ્રણાલીની આઘાત-સહનીયતામાં વૃદ્ધિ કરવામાં આવે. જ્યારે પણ આવી પ્રતિકૂળ ઘટનાઓ / અડચણો બને, ત્યારે તેને પહોંચી વળવા માટે યોગ્ય પ્રકારના "ઘટના પ્રતિક્રિયા પ્રબંધ અને પુન:પ્રાપ્તિ (Incident Response Management and Recovery)" માળખાને કાર્યરત કરવામાં આવશે પણ ઉપાયો આટલા પૂરતા સિમિત નહીં હોય.

બોર્ડ દ્વારા અનુમોદિત સાઇબર સુરક્ષા નીતિની આવશ્યકતા

3. બેંકોએ તેમના બોર્ડ દ્વારા વિધિવત્ અનુમોદિત સાઇબર સુરક્ષા નીતિને **તત્કાળ** લાગૂ કરવી જોઈએ જેમાં સાઇબર ખતરાઓથી લડવા માટે ઉચિત ઉપાયોની રણનીતિ તથા કારોબારની જટિલતાઓના સ્તર અને જોખમના સ્વીકાર્ય સ્તરની સ્પષ્ટતા કરેલી હોય. આ બાબતમાં બેંકોએ તેમની પુષ્ટિ (confirmation) જલ્દીમાં જલ્દી સાઇબર સુરક્ષા અને સૂચના પ્રૌદ્યોગિકી જાંચ કક્ષ (Cyber Security and Information Technology Examination Cell), બેંકિંગ પર્યવેક્ષણ વિભાગ, ભારતીય રિઝર્વ બેંક, કેન્દ્રીય કાર્યાલય, વર્લ્ડ ટ્રેડ સેન્ટર-1, ચોથે માળ, કફ પરેડ, મુંબઈ 400 005 ને જણાવવી અને કોઈ પણ પરિસ્થિતિમાં 30 સપ્ટેમ્બર 2016 કરતા મોડુ તો નહીં જ.

એ સુનિશ્ચિત કરવામાં આવે કે કાર્યનીતિમાં નીચે જણાવેલી બાબતો શામેલ હોય.

સાઇબર સુરક્ષા નીતિ, બેકની વિસ્તૃત આઈટી નીતિ / આઈએસ સુરક્ષા નીતિથી અલગ હો.
(Cyber Security Policy to be distinct from IT Policy / IS Security Policy of a bank)

4. સાઇબર-સુરક્ષિત માહોલમાં સંપૂર્ણ બેંકના યોગદાનની આવશ્યકતા પર ધ્યાન આપવા માટે સાઇબર સુરક્ષા નીતિ, વિસ્તૃત આઈટી નીતિ / આઈએસ સુરક્ષા નીતિથી ભિન્ન અને

અલગ હોવી જોઈએ જેથી સાઇબર ખતરાના જોખમો અને આ જોખમોથી નિપટવા અને તેને ઘટાડવા માટેના ઉપાયો પર તે પ્રકાશ ફેંકી શકે.

5. કદ, પ્રણાલી, ટેકનીકલ કઠિનાઈઓ, ડિજિટલ ઉત્પાદનો, હિતધારકો (stakeholders) અને ખતરાની સંભાવનાઓ બેંકે બેંકે બદલાતી રહે છે અને આથી જ, એ મહત્વપૂર્ણ છે કે અંતર્નિહિત જોખમોની ઓળખાણ કરવામાં આવે અને યોગ્ય સાઇબર સુરક્ષા માળખાને અપનાવવા માટે નિયંત્રણો સ્થાપિત કરવામાં આવે. અંતર્નિહિત જોખમોની ઓળખાણ તથા તેના મૂલ્યાંકન કરવા માટે બેંકો પાસેથી એ અપેક્ષિત છે કે અપનાવવામાં આવેલી ટેકનોલોજી, કારોબાર અને નિયમનકારી આવશ્યકતાઓ વચ્ચે સામંજસ્ય, સ્થાપિત કનેક્શનો, આપૂર્તિ ચેનલો, ઑનલાઇન/મોબાઈલ ઉત્પાદનો, ટેકનોલોજીકલ સેવાઓ, સંગઠનાત્મક પરિવેશ અને આંતરિક તેમજ બાહ્ય ખતરાઓને ગણતરીમાં લે. અંતર્નિહિત જોખમોના સ્તરના આધાર પર બેંકોએ તેમના જોખમોને નિમ્ન, સામાન્ય, ઉચ્ચ અને અતિ ઉચ્ચના રૂપમાં ઓળખી કાઢવા જોઈએ અથવા આ પ્રકારના કોઈ અન્ય વર્ગીકરણને પણ તેઓ અપનાવી શકે છે. અંતર્નિહિત જોખમોનું મૂલ્યાંકન કરતી વખતે કારોબાર ઘટકોના જોખમો પણ ધ્યાનમાં લેવા જોઈએ. નિયંત્રણોના મૂલ્યાંકનના સમયે બોર્ડની ચૂક, નીતિઓ, પ્રક્રિયા, અનુભવી અને યોગ્ય સ્ત્રોત સહિત સાઇબર જોખમ પ્રબંધન આર્કિટેક્ચર, પ્રશિક્ષણ અને પરિવેશ, ખતરા આસૂચનાને એકત્રિત કરવાની વ્યવસ્થા (threat intelligence gathering arrangements), બેંકોની પાસેથી ખતરા આસૂચનાની સ્થિતિઓની તુલનામાં પ્રાપ્ત સ્થિતિઓની દેખરેખ એવં વિશ્લેષણ, માહિતી આદાન-પ્રદાન કરવાની વ્યવસ્થા (સહયોગી બેંકોની વચ્ચે, આઇડીઆરબીટી/આરબીઆઇ/સીઇઆરટી- આની સાથે), પ્રતિરોધક, જાસૂસી અને સુધારાત્મક સાઇબર સુરક્ષા નિયંત્રણો, વિક્રેતા પ્રબંધન અને ઘટના પ્રબંધન તથા પ્રતિક્રિયા દર્શાવવામાં આવે.

નિયમિત દેખરેખની વ્યવસ્થા (Arrangement for continuous surveillance)

6. સમયના યોગ્ય અંતરાલ પર સંવેદનશીલતાઓ (vulnerabilities) ની તપાસ કરવાની બાબત બહુ જ મહત્વપૂર્ણ છે. સાઇબર-આક્રમણનું સ્વરૂપ એવા પ્રકારનું છે કે તે ક્યારેય પણ

થઈ શકે છે અને કરેલા અનુમાનથી પર પણ હોઈ શકે છે. આથી, એમ આદેશ કરવામાં આવે છે કે એસઓસી (સિક્યૂરિટી ઑપરેશન સેન્ટર) ની સ્થાપના શક્ય એટલી ઝડપથી કરવામાં આવે, જો પહેલા ન કરી હોય તો. એ પણ આવશ્યક છે કે આ કેન્દ્ર સતત દેખરેખ રાખવાની બાબતને સુનિશ્ચિત કરે અને હવે પછી આવવાવાળા સાયબર ખતરાના હાલના સ્વરૂપનો અભ્યાસ કરીને પોતાની જાતને માહિતગાર રાખે.

આઈટી આર્કિટેક્ચર સુરક્ષા માટે હિતકારી હો (IT Architecture should be conducive to security)

7. આઈટી આર્કિટેક્ચર એવી રીતે બનાવવામાં આવે કે તે કાયમ માટે લાગૂ કરવામાં આવનાર સુરક્ષા ઉપાયોને અનુરૂપ થઈ તેનો સમાવેશ કરી શકે. બોર્ડની આઈટી ઉપ સમિતિ દ્વારા તેની સમીક્ષા કરવામાં આવે અને જો આવશ્યક હોય તો, તેના જોખમ મૂલ્યાંન મુજબ તેને તબક્કાવાર મુજબ અદ્યતન બનાવવામાં આવે. બેંક દ્વારા લેવામાં આવનાર જોખમ લાગત / સંભવિત લાગત ટ્રેડ-ઑફ ને સંબંધિત નિર્ણયોને લેખિતમાં નોંધવા જોઈએ જેથી પાછળથી તેનું યોગ્ય પર્યવેક્ષી મૂલ્યાંકન કરી શકાય.

8. અનુબંધ 1 માં આપવામાં આવેલા ન્યૂનતમ મૂળભૂત સાઇબર સુરક્ષા રેસિલિયન્સ ફ્રેમવર્ક બેંકો દ્વારા કાર્યાન્વિત કરવામાં આવશે જે ઉદાહરણ રૂપે આપેલ છે, સંપૂર્ણ નથી. બેંકોએ એક સિક્યૂરિટી ઑપરેશન સેન્ટર (એસઓસી) ની સ્થાપના કરવાની તથા તેનો પ્રારંભ કરવાની પ્રક્રિયાને પૂરી સક્રિયતાની સાથે શરૂ કરવી પડશે, જેથી રિયલ ટાઈમમાં સાઇબર જોખમોની દેખરેખ તથા પ્રબંધન કરી શકાય. એસઓસીનું એક નિર્દેશાત્મક કન્ફીગ્યુરેશન અનુબંધ 2 માં આપવામાં આવેલ છે.

9. હાલમાં બનેલી ઘટનાઓને કારણે પ્રત્યેક બેંકમાં નેટવર્ક સુરક્ષાની વધુ સારી રીતે સમીક્ષા કરવાની જરૂરિયાત ઊભી થઈ છે. તદ્ઉપરાંત, એમ જોવામાં આવેલ છે કેટલીક વ્યવસાયિક અથવા પરિચાલનીય અપેક્ષાઓ પૂરી કરવા માટે એક વિશિષ્ટ સમયાવધિ માટે નેટવર્ક/ડેટાબેસમાં કેટલીકવાર કનેકશનની અનુમતિ આપવામાં આવે છે. તેમ છતાં, તેને ભૂલથી બંધ કરવામાં આવતું નથી જેના ફળસ્વરૂપે નેટવર્ક/ડેટાબેસ સાઇબર-હુમલાની

ઝપટમાં આવી શકે છે. એ જરૂરી છે કે નેટવર્કો તથા ડેટાબેસ માં અનધિકૃત રૂપથી એક્સેસ કરવાની અનુમતિ નહીં આપવી જોઈએ તથા જ્યારે પણ અનુમતિ આપવામાં આવે, તો તે માટે નિર્ધારિત પ્રક્રિયાઓનું અનિવાર્ય રૂપથી પાલન કરવામાં આવે. આ પ્રકારના નેટવર્કો તથા ડેટાબેસોની જવાબદારી સ્પષ્ટરૂપથી દર્શાવવી જોઈએ તથા અનિવાર્ય રૂપથી બેંકોના અધિકારીઓને સોંપવામાં આવવી જોઈએ.

ગ્રાહક માહિતીની સુરક્ષા સુનિશ્ચિત કરવી (Ensuring Protection of customer information)

10. બેંક ફક્ત તેના સુચારુ કામકાજ માટે જ નહીં પણ તેના ગ્રાહકોને અદ્યતન ડિજિટલ ઉત્પાદનો (cutting-edge digital products) આપવા માટે ટેકનોલોજી પર સંપૂર્ણ રીતે નિર્ભર હોય છે તથા આ પ્રક્રિયામાં તે વિવિધ વ્યક્તિગત તથા સંવેદનશીલ માહિતી એકત્ર કરે છે. બેંકોએ, આવા ડેટાના માલિકના રૂપમાં, તેની ગોપનિયતા, સત્યનિષ્ઠા તથા ઉપલબ્ધતાનું સંરક્ષણ કરવા માટે ઉચિત ઉપાય કરવા જોઈએ, ભલે પછી તે ડેટા તેની પાસે હોય / ટ્રાન્સીટમાં હોય યા ગ્રાહકો કે પછી તૃતીયપક્ષ વેંડરની પાસે હોય, આ પ્રકારની સંગ્રહિત માહિતીની ગોપનીયતા સાથે કોઈ પણ સંજોગોમાં કોઈ પ્રકારની ખિલવાડ ન થવી જોઈએ તથા તે પ્રયોજન માટે, બેંકો દ્વારા ડેટા/માહિતીના સમગ્ર જીવનકાળમાં ઉચિત પ્રણાલીઓ અને પ્રક્રિયાઓને લાગૂ કરવાની આવશ્યકતા છે.

સાઇબર સંકટ પ્રબંધન યોજના (Cyber Crisis Management Plan - CCMP)

11. સાઇબર સંકટ પ્રબંધન યોજના (સીસીએમપી) તુરંત શરૂ કરવી જોઈએ તથા તે બોર્ડની અનુમોદિત સમગ્ર કાર્યનીતિનો એક હિસ્સો હોવી જોઈએ. સાઇબર-જોખમ એ અન્ય જોખમો કરતા અલગ છે તે બાબતને ગણતરીમાં લેતા, પરંપરાગત બીસીપી / ડીઆર વ્યવસ્થાઓ પૂરતી નથી તથા સાઇબર-જોખમોની માત્રાને ધ્યાનમાં રાખતા તેની પર ફરીથી ધ્યાન આપવાની આવશ્યકતા છે. જેમ કે આપ જાણો છો, ભારતમાં કોમ્પ્યુટર આપાત કાર્યવાહી ટીમ, ભારત, એક સરકારી સંસ્થા (Computer Emergency Response Team - India, a Government entity - CERT - સીઈઆરટી-ઇન) સક્રિય તથા પ્રતિક્રિયાત્મક સેવાઓની સાથે સાથે માર્ગદર્શિકા પ્રદાન કરીને તેમજ ખતરાની આસૂચના અને નાણાકીય ક્ષેત્રો સહિત બધા

જ ક્ષેત્રોમાં વિભિન્ન એજન્સીઓની તૈયારીનું મૂલ્યાંકન કરીને, સાઇબર-સુરક્ષાને દુરસ્ત કરવામાં મહત્વપૂર્ણ કદમ ઉઠાવી રહી છે. સીઈઆરટી-આઈએને રાષ્ટ્રીય સાઇબર સંકટ પ્રબંધન યોજના તથા સાઇબર સુરક્ષા મૂલ્યાંકન ફ્રેમવર્ક પણ તૈયાર કરેલ છે. સીસીએમપી બનાવતી વખતે સીઈઆરટી-આઈએન / એનસીઆઈઆઈપીસી / આરબીઆઈ / આઈડીઆરબીટીની માર્ગદર્શિકાઓનો સંદર્ભ લેવામાં આવે.

12. સીસીએમપીએ નીચે જણાવેલી ચાર બાબતો ધ્યાનમાં લેવી જોઈએ: (i) શોધી કાઢવુ (detection)((ii) જવાબી કાર્યવાહી (Response) (iii) પુન:પ્રાપ્તિ (Recovery) અને (iv) નિયંત્રણ (Containment). બેંકોએ સાઇબર હુમલાને રોકવા માટે પ્રભાવી ઉપાયોની સાથે સાથે કોઈપણ સાઇબર-ઘૂસપેઠની તુરંત ખબર મેળવવી પણ આવશ્યક છે જેથી કોઈ પણ અનહોની પર જવાબી કાર્યવાહી / સુધારાત્મક કાર્યવાહી / નિયંત્રણાત્મક કાર્યવાહી તુરંત કરી શકાય. બેંકો પાસેથી એ અપેક્ષિત છે કે ઉભરાતા સાઇબર હુમલાઓ જેવા કે 'ઝીરો-ડે હુમલા', રિમોટ એક્સેસ ખતરા અને ઇરાદતન હુમલાઓનો સામનો કરવા માટે સંપૂર્ણ રીતે તૈયાર રહે. બીજી બાબતોની સાથે સાથે, બેંકોએ વિવિધ પ્રકારના સાઇબર ખતરા, જેવાકે સેવાથી નકાર, ડ્રિસ્ટ્રીબ્યૂટેડ ડિનાયલ ઑફ સર્વિસીસ (ડીડીઓએસ), રેનસમ-વેર / ક્રિપ્ટોવેર (ransome-ware / crypto ware), ઘાતક માલવેર (destructive malware), વ્યવસાય ઈમેલ ઠગાઈ (business email frauds) જેવા કે સ્પામ, ઈમેલ ફિશિંગ, સ્પિયર ફિશિંગ, વ્હેલિંગ, વિશિંગ ઠગાઈ, ડ્રાઇવ-બાય ડાઉનલોડ, બ્રાઉઝર ગેટવે ઠગાઈ, ઘોસ્ટ એડમિનિસ્ટ્રેટર એક્સપ્લોઈટ્સ, ઓળખાણ સંબંધી ઠગાઈ, મેમરી અપડેટ ઠગાઈ, પાસવર્ડ સંબંધી ઠગાઈ વિગેરેથી નિપટવા માટે આવશ્યક નિષેધાત્મક તેમજ સુધારાત્મક ઉપાય કરવા જોઈએ.

સાઇબર સુરક્ષા તૈયારીના સંકેતકો (Cyber security preparedness indicators)

13. સાઇબર રેસિલિઅન્સ ફ્રેમવર્કની પર્યાપ્તતા તથા તેના પાલનનું મૂલ્યાંકન કરવામાં આવવું જોઈએ તથા જોખમ / તૈયારીના સ્તરનું મૂલ્યાંકન કરવા માટે સંકેતકો વિકસાવવા જોઈએ. આ સંકેતકોને સ્વતંત્ર અનુપાલન ચેક્સ (independent compliance checks) તથા યોગ્ય તેમજ સક્ષમ પ્રોફેસનલ્સ દ્વારા કરવામાં આવેલી ઓડિટ પરીક્ષાઓ દ્વારા વ્યાપક જાંચ

માટે ઉપયોગમાં લેવા જોઈએ. કર્મચારીઓની સહિત હિતધારકોની જાગૃતિને પણ આ મૂલ્યાંકનનો હિસ્સો બનાવવી જોઈએ.

આરબીઆઈની સાથે સાઇબર-સુરક્ષા ઘટનાઓથી સંબંધિત માહિતીને શેર કરવી (Sharing of information on cyber-security incidents with RBI)

14. એમ જોવામાં આવ્યું છે કે બેંકો તેમના દ્વારા જાણવામાં આવેલી સાઇબર ઘટનાઓને બીજા સાથે વહેંચવામાં સંકોચ અનુભવે છે. તેમ છતાં, વૈશ્વિક રૂપથી પ્રાપ્ત થયેલ અનુભવ એમ દર્શાવે છે કે સાઇબર ઘટનાઓને શેર કરવામાં સંસ્થાઓની વચ્ચે સહયોગ તથા નિર્ધારિત પ્રક્રિયાઓથી સાઇબર-જોખમોને રોકવા માટે સમય પર ઉપાય લાગૂ કરી શકાય છે. આની ઉપર ફરી વખત વિચારવામાં આવે કે બેંકોએ પણ બધા અસામાન્ય સાઇબર-સુરક્ષાના કિસ્સાઓ રિઝર્વ બેંકને રિપોર્ટ કરવા પડશે (ભલે તે કિસ્સા સફળ થયા હોય કે પછી નિષ્ફળ પ્રયાસના સ્વરૂપમાં હોય). બેંકોને પ્રોત્સાહિત કરવામાં આવે છે કે તેઓ આઈડીઆરબીટી દ્વારા સમન્વયિત તેમના સીઆઈએસસીઓ ફોરમની ગતિવિધિઓમાં સક્રિયતાની સાથે ભાગ લે તથા આવી ઘટનાઓ / કિસ્સાઓને આઈડીઆરબીટી દ્વારા સ્થાપિત ભારતીય બેંક - જોખમ તથા ખતરા વિશ્લેષણ કેન્દ્ર (Indian Banks – Centre for Analysis of Risks and Threats – IB – CART - આઈબી - સીએઆરટી) ને તુરંત રિપોર્ટ કરે. આ પ્રકારના સમન્વયિત પ્રયાસોથી સામૂહિક ખતરાની આસૂચના, સમય પર એલર્ટ્સ તથા સક્રિય સાઇબર સુરક્ષા ઉપાયો અપનાવવામાં બેંકોને મદદ મળશે.

પર્યવેક્ષી રિપોર્ટિંગ ફ્રેમવર્ક (Supervisory Reporting Framework)

15. એમ નિર્ણય લેવામાં આવ્યો છે કે સાઇબર-ઘટનાઓ સહિત માહિતી સુરક્ષા ઘટના સંબંધી સારાંશ સ્તરીય માહિતી તેમજ વિગતવાર માહિતી, એમ બંને એકત્ર કરવામાં આવે. બેંકો પાસેથી એમ અપેક્ષા રાખવામાં આવે છે કે ઘટનાઓની સૂચના અનુબંધ-૩ માં આપેલ ફોર્મેટમાં તુરંત આપવામાં આવે.

આરબીઆઈને રિપોર્ટ કરવા માટેની તૈયારીમાં ચૂકનું શીઘ્ર મૂલ્યાંકન (An immediate assessment of gaps in preparedness to be reported to RBI)

16. નિયંત્રણોમાં મહત્વપૂર્ણ ખામીઓની શીઘ્ર ઓળખી કાઢવામાં આવે તથા બોર્ડની સાથે-સાથે બોર્ડની આઈટી ઉપ સમિતિના સક્રિય માર્ગદર્શન તથા પર્યવેક્ષણની અંતર્ગત ઉચિત ઉપચારાત્મક કાર્યવાહી તુરંત શરૂ કરવામાં આવે. ઓળખી કાઢવામાં આવેલી ખામીઓ, પ્રસ્તાવિત ઉપાયો / નિયંત્રણો તથા તેમની અપેક્ષિત પ્રભાવશીલતા, પ્રસ્તાવિત નિયંત્રણો / ઉપાયોને કાર્યાન્વિત કરવા માટે સમયમર્યાદાની સાથે માઇલસ્ટોન તથા બેંક દ્વારા અનુપાલિત / પ્રસ્તાવિત જોખમ મૂલ્યાંકન તથા જોખમ પ્રબંધન પ્રક્રિયા સહિત તેમની પ્રભાવક્ષમતાનું મૂલ્યાંકન કરવા માટે માપદંડને મુખ્ય માહિતી સુરક્ષા અધિકારી દ્વારા 31 જુલાઈ 2016 સુધી સાઇબર સુરક્ષા તથા માહિતી પ્રૌદ્યોગિકિ જાંચ કક્ષ (Cyber Security and Information Technology Examination (CSITE) Cell), બેંકિંગ પર્યવેક્ષણ વિભાગ, કેન્દ્રીય કાર્યાલયને પ્રસ્તુત કરવામાં આવે.

સંગઠનાત્મક વ્યવસ્થાઓ (Organisational Arrangements)

17. બેંકોએ સંગઠનાત્મક વ્યવસ્થાઓની સમીક્ષા કરવી જોઈએ જેથી સુરક્ષા સમસ્યાઓનું મૂલ્યાંકન કરી શકાય, પર્યાપ્ત ધ્યાન આપી શકાય અને તુરંત કાર્યવાહી કરવા માટે પદક્રમના ઉચિત સ્તર સુધી લઈ જવામાં આવે.

હિતધારકો / ઉચ્ચ પ્રબંધન / બોર્ડની વચ્ચે સાઇબર-સુરક્ષા જાગૃતિ (Cyber-security awareness among stakeholders / top management / Board)

18. એમ જોવામાં આવેલ છે કે સાઇબર જોખમનું પ્રબંધન કરવા માટે સાઇબર-સુરક્ષિત માહોલ બનાવવા માટે પૂરા સંગઠનની પ્રતિબદ્ધતા આવશ્યક છે. તે માટે બધા જ સ્તરો પર રહેલા સ્ટાફ વચ્ચે એક ઉચ્ચ સ્તરની જાગૃતિની આવશ્યકતા રહેશે. ઉચ્ચ પ્રબંધન તથા બોર્ડની પાસે ખતરાની સૂક્ષ્મતમ જાણકારી હોવી જરૂરી છે તથા તેને યોગ્ય પ્રકારે ફેમિલિયરાઇજેશન પ્રદાન કરવામાં આવવું જોઈએ. બેંક પૂરી સક્રિયતાથી તેના ગ્રાહકો, વિક્રેતા, સેવા પ્રદાતાઓ તથા અન્ય સંબંધિત હિતધારકો વચ્ચે બેંકની સાઇબર રેસિલિયન્સ ઉદ્દેશોની સમજણ પેદા કરે તથા તેના એકલયબદ્ધ કાર્યાન્વયન તથા જાંચ માટે ઉચિત કાર્યવાહીની અપેક્ષાને સુનિશ્ચિત કરે. એ બાબત પ્રસ્થાપિત છે કે હિતધારકો (ગ્રાહકો,

કર્મચારીઓ, ભાગીદારો તથા વિક્રેતાને શામેલ કરતા) ને સાઇબર-હુમલાથી થવાવાળી સંભવિત અસરો અંગેની જાગૃતિ, બેંકોની સાઇબર સુરક્ષાની તૈયારીમાં મદદરૂપ થશે. બેંકો આ બાબતમાં યોગ્ય પગલા લે. સાથે ને સાથે, નિર્દેશક મંડળ તથા ઉચ્ચ પ્રબંધન સાઇબર-સુરક્ષા સંબંધી બાબતો અંગે, જ્યાં જરૂર હોય ત્યાં, ઝડપી કાર્યવાહી કરે અને તેથી બેંકોને આ દિશામાં તુરંત પગલા લેવા માટે સૂચિત કરવામાં આવે છે.

આ પરિપત્રની એક નકલ નિર્દેશક મંડળની આગામી બેઠકમાં તેમની સમક્ષ રાખવામાં આવે.

ભવદીય

(આર. રવિકુમાર)
મુખ્ય મહાપ્રબંધક
સંલગ્ન – ઉપર મુજબ