

Cyber Security Framework for UCBs-A Graded Approach

Level III – Basic Controls

આ વિભાગ UCB Level III માં પ્રવેશ કરે છે, જ્યાં RBI નું ધ્યાન માત્ર સુરક્ષા (Security) પર નહીં પરંતુ સાયબર રિઝિલિયન્સ (Cyber Resilience) અને Proactive Defence પર છે.

Level III – 1. Network Management and Security

1.1 Unusual Activity Detection- Put in place mechanism to detect and remedy any unusual activities in systems, servers, network devices and endpoints.

RBI Requirement

બેંકે એવી વ્યવસ્થા સ્થાપિત કરવી જોઈએ કે જે સિસ્ટમ, સર્વર, નેટવર્ક ઉપકરણો અને Endpoints પર થતી અસામાન્ય (Unusual) પ્રવૃત્તિઓને શોધી શકે અને તરત યોગ્ય કાર્યવાહી કરી શકે.

બેંકમાં એવી ટેકનોલોજી હોવી જોઈએ કે જે કોઈપણ અસામાન્ય અથવા શંકાસ્પદ પ્રવૃત્તિને તરત ઓળખી શકે.

આ પ્રવૃત્તિઓમાં સામેલ હોઈ શકે: મધરાત્રે Login, હજારો ફાઇલો Copy થવી, એક જ User દ્વારા અસામાન્ય Transaction, Server નો CPU અચાનક 100% થઈ જવો (100% CPU → CPU સંપૂર્ણ ક્ષમતાથી કામ કરી રહ્યું છે.), Means DDoS Attack Cryptomining Malware, Ransomware, અજાણ્ય IP Address પરથી Login

RBI આ શા માટે કહે છે?

સાયબર હુમલો એક જ ક્ષણે થતો નથી. તે પહેલાં ઘણી શંકાસ્પદ પ્રવૃત્તિઓ થાય છે. જો તે સમયસર શોધાઈ જાય તો મોટો હુમલો અટકાવી શકાય.

UCB Example

એક Branch નો User દરરોજ સવારે 10 થી સાંજે 6 વાગ્યા સુધી Login કરે છે. એક દિવસ રાત્રે 2:30 વાગ્યે Login થાય છે.

System તરત Alert આપે. IT Team તપાસ કરે. ખબર પડે કે Password ચોરાઈ ગયો હતો. હુમલો અટકી જાય.

"સાયબર હુમલો શરૂ થાય તે પહેલાં તેની અસર દેખાવા લાગે છે. બુદ્ધિશાળી બેંક હુમલો થયા પછી નહીં, પરંતુ હુમલાના સંકેતો દેખાતા જ કાર્યવાહી કરે છે."

"Cyber Security માં Monitoring એટલે CCTV જેવી વ્યવસ્થા છે."

1.2 Firewall Rules

Firewall rules shall be defined to block unidentified outbound connections, reverse TCP shells and other potential backdoor connections.

RBI Requirement

Firewall એવી રીતે Configure કરવું કે Unidentified Outbound Connections i) Reverse TCP Shell ii) Backdoor Connections Block થઈ જાય. Firewall માત્ર બહારથી આવતા હુમલાને રોકે એટલું પૂરતું નથી. જો કોઈ Malware અંદર આવી જાય, તો તે બહાર Hacker સાથે સંપર્ક ન કરી શકે, તેની પણ વ્યવસ્થા હોવી જોઈએ.

RBI આ શા માટે કહે છે?

ધણ Malware બહારના Hacker સાથે સંપર્ક કરીને Data ચોરે છે, Command લે છે, Ransomware Download કરે છે, Firewall એ બધું અટકાવે.

Reverse TCP Shell શું છે? સામાન્ય રીતે User→ Server→સાથે જોડાય છે. પણ Reverse TCP Shell માં Infected Computer→ Hacker → સાથે જોડાય છે. હવે Hacker અંદર બેઠો હોય તેમ Computer ચલાવી શકે.

UCB Example

એક Branch Computer માં Malware આવી ગયો. Malware Hacker ના Server સાથે જોડાવાનો પ્રયત્ન કરે છે. Firewall Rule તેને Block કરી દે છે. Data Leak અટકી જાય છે.

"Firewall માત્ર દરવાજો બંધ કરતું નથી; તે અંદર રહેલા ચોરને બહારના સાથીદાર સાથે વાત પણ કરવા દેતું નથી."

2. Secure Configuration

2.1 Remote Connection Disable

Disable remote connections from outside machines to the network hosting critical payment infrastructure (Ex: RTGS/NEFT, ATM Switch, SWIFT Interface). Disable Remote Desktop Protocol (RDP) on all critical systems.

RBI Requirement: RTGS, NEFT, ATM Switch, SWIFT Interface, જેવી Critical Systems માટે બહારથી Remote Connection બંધ રાખવું. અને Remote Desktop Protocol (RDP) Disable કરવું.

Critical Payment Systems પર Internet દ્વારા Remote Login કરવાની મંજૂરી ન હોવી જોઈએ.

RBI આ શા માટે કહે છે? ધણ Ransomware Attack, Remote Desktop દ્વારા થયા છે. જો RDP ખુલ્લું હોય તો Hacker સીધો Server માં Login કરવાનો પ્રયાસ કરે.

UCB Example

IT Vendor ઘરે બેઠા RDP દ્વારા CBS Server માં Login કરે છે. જો Password Leak થાય તો Hacker પણ Login કરી શકે. RBI કહે છે. RDP Disable રાખો.

"જે દરવાજાનો ઉપયોગ જ થતો નથી તે ખુલ્લો કેમ રાખવો? RDP પણ એવો જ દરવાજો છે."

2.2 IP Table Restriction: Enable IP table to restrict access to the clients and servers in SWIFT and ATM Switch environment only to authorised systems.

RBI Requirement

SWIFT અને ATM Switch માં માત્ર Authorised Systems જ જોડાઈ શકે. ફક્ત મંજૂર થયેલા Computer અને Server જ SWIFT અથવા ATM Switch સુધી પહોંચી શકે. બીજા કોઈ Computer ને પ્રવેશ ન મળે.

UCB Example

CBS Room માં 20 Computers છે. પરંતુ ATM Switch સુધી માત્ર 2 Computers જ જઈ શકે.

"બધાને બધે પ્રવેશ ન આપવો. Critical Systems સુધી માત્ર અધિકૃત Computer જ પહોંચે."

2.3 Software Integrity: Ensure the software integrity of the ATM Switch/SWIFT related applications.

RBI Requirement: ATM Switch અને SWIFT Software માં કોઈ અનધિકૃત ફેરફાર થયો નથી તેની ખાતરી કરવી.

Software સાથે કોઈએ ચેડાં કર્યા નથી તેની નિયમિત તપાસ કરવી. **RBI આ શા માટે કહે છે?** Malware ઘણી વખત Original Software માં ફેરફાર કરે છે. તે બહારથી દેખાતું નથી. પણ અંદરથી Data ચોરી શકે.

"સાચું Software પણ જો કોઈએ ચેડાં કરીને બદલી દીધું હોય તો તે સૌથી મોટું જોખમ બની શકે છે."

2.4 Disable PowerShell: Disable PowerShell in servers where not required and disable PowerShell in Desktop systems.

RBI Requirement જ્યાં જરૂર ન હોય ત્યાં PowerShell Disable કરવું. **PowerShell શું છે?** PowerShell Windows નું ખૂબ શક્તિશાળી Administration Tool છે. System Admin તેનો ઉપયોગ કરે છે. પણ Hackers પણ તેનો ઉપયોગ કરે છે.

RBI આ શા માટે કહે છે? ઘણા Malware PowerShell દ્વારા Virus Download કરે છે, Command ચલાવે છે, Data ચોરી કરે છે. સામાન્ય User Mouse થી કામ કરે છે. જેમ કે: Folder ખોલવો, File Copy કરવી, Printer Install કરવું, પરંતુ System Administrator PowerShell માં માત્ર એક Command લખીને:

- 500 Computers પર Software Install કરી શકે. બધા Users ના Password Reset કરી શકે. Windows Update ચલાવી શકે. Server Restart કરી શકે. Backup શરૂ કરી શકે. એટલે PowerShell એ IT Administrator માટે ખૂબ ઉપયોગી સાધન છે.

PowerShell નો ઉપયોગ ક્યાં થાય છે?

- Windows Server Management
- Active Directory Management
- User Account બનાવવું
- Password Reset
- Software Installation
- Patch Management
- Backup
- Office 365 / Microsoft 365 Administration
- Azure Cloud Management

RBI આ શા માટે કહે છે કે "જ્યાં જરૂર ન હોય ત્યાં PowerShell Disable કરો"?

કારણ કે જે PowerShell Administrator માટે ઉપયોગી છે, તે જ Hacker માટે પણ ખૂબ શક્તિશાળી હથિયાર બની શકે છે.

ઘણા Cyber Attack માં Hacker PowerShell નો ઉપયોગ કરીને:

- Virus Download કરે છે.
- Malware Install કરે છે.
- Ransomware ચલાવે છે.

- Data ચોરી કરે છે.
- બીજા Computers પર હુમલો ફેલાવે છે.

"જે સાધન Administrator માટે ઉપયોગી છે, તે જ Hacker માટે પણ હથિયાર બની શકે છે."

2.5 Restrict Default Shares (IPC\$)

RBI Requirement- Default Windows Shares જેમ કે IPC\$, ADMIN\$, C\$, વગેરે Restrict કરવી.

IPC\$ શું છે?

Windows માં રહેલું એક Hidden Administrative Share. તે Computer વચ્ચે Communication માટે ઉપયોગી છે. પરંતુ Hackers પણ તેનો ઉપયોગ કરે છે.

RBI આ શા માટે કહે છે?

ઘણા Malware IPC\$ દ્વારા એક Computer માંથી બીજા Computer માં ફેલાય છે.

એક Branch નો Computer Virus થી Infected થયો. IPC\$ ખુલ્લું હોવાથી Virus બીજા 25 Computers માં પણ પહોંચી ગયો. જો IPC\$ Restrict કરેલું હોત તો Virus ત્યાં જ અટકી જાત. "Virus દરવાજેથી નહીં, ઘણી વખત Windows ના Hidden રસ્તાઓથી અંદર આવે છે. IPC\$ એવો જ એક Hidden રસ્તો છે."

Level III નો મુખ્ય સંદેશ

"Level I આપણને સુરક્ષિત બનાવે છે. Level II આપણને મજબૂત બનાવે છે. પરંતુ Level III આપણને બુદ્ધિશાળી બનાવે છે, જ્યાં બેંક માત્ર હુમલાથી બચતી નથી, પરંતુ હુમલાના પ્રારંભિક સંકેતો ઓળખીને સમયસર પ્રતિસાદ પણ આપે છે."

Level III – Application Security Life Cycle (ASLC) નો સૌથી ટેકનિકલ અને સૌથી મહત્વપૂર્ણ વિભાગ છે. RBI અહીં માત્ર Software Development વિશે નથી કહેતી, પરંતુ "Secure Software Development" અને "Security by Design" ના સિદ્ધાંતો ફરજિયાત બનાવે છે.

Application Security Life Cycle (ASLC)

ASLC શું છે?

ASLC (Application Security Life Cycle) એટલે કોઈપણ Software અથવા Application નું આયોજન, વિકાસ, પરીક્ષણ, અમલીકરણ અને જાળવણી – આ તમામ તબક્કામાં શરૂઆતથી જ સુરક્ષાને (Security) સામેલ કરવી.

"Software તૈયાર થયા પછી તેમાં Security ઉમેરવાની નહીં, પરંતુ Software બનાવવાની પ્રથમ લાઇનથી જ Security શરૂ થવી જોઈએ."

3.1 Source Code Audit

RBI Requirement

મહત્વપૂર્ણ (Critical) Applications માટે UCB એ

- Professional Experts દ્વારા Source Code Audit કરાવવું

અથવા

- Software Vendor/OEM પાસેથી ખાતરી મેળવવી કે Software માં કોઈ Malware, Backdoor અથવા Fraudulent Code નથી.

બેંકના CBS, Mobile Banking, Internet Banking અથવા ATM Switch જેવા મહત્વપૂર્ણ Software નો મૂળ Program (Source Code) સુરક્ષિત છે કે નહીં તેની તપાસ કરાવવી.

Source Code શું છે?

Source Code એટલે Software બનાવતો મૂળ Program. જેમ કોઈ મકાનનો નકશો હોય છે, એમ Software નો Source Code હોય છે.

Source Code Audit શું છે?

નિષ્ણાતો Source Code વાંચે છે અને તપાસે છે કે તેમાં:

- ✓ Backdoor નથી
- ✓ Hidden Password નથી
- ✓ Malware નથી
- ✓ Fraud કરવા માટે કોઈ Secret Code નથી
- ✓ Coding Errors નથી

RBI આ શા માટે કહે છે?

ક્યારેક Software બહારથી બરાબર ચાલતું હોય છે, પણ અંદરથી તેમાં Trojan, Backdoor, Malicious Code છુપાયેલું હોઈ શકે. Source Code Audit આ જોખમ શોધી કાઢે છે.

"સુંદર દેખાતું Software હંમેશા સુરક્ષિત હોય એવું જરૂરી નથી. Software નો સાચો ચહેરો તેના Source Code માં છુપાયેલો હોય છે."

"Source Code Audit એ Software નું X-Ray છે."

3.2 Security Requirements from Beginning

RBI Requirement Software બનાવતી વખતે માત્ર Business Requirements નહીં, પરંતુ નીચેની Security Requirements પણ શરૂઆતથી જ નક્કી કરવી.

તેમાં શું આવે? Access Control, Authentication, Transaction Authorization, Data Integrity, Audit Logs, Session Management, Security Event Tracking, Exception Handling

Software બનાવતી વખતે શરૂઆતથી જ નક્કી કરવું જોઈએ:

કોણ Login કરશે? કોણ Transaction કરશે? કોણ Approval આપશે? કોણ Log જોઈ શકશે? ભૂલ થાય તો શું કરવું?

મુખ્ય Security Requirements- Access Control-યોગ્ય વ્યક્તિને જ યોગ્ય Access.

Authentication-User સાચો છે તેની ખાતરી.

Transaction Authorization-મોટા Transaction માટે Approval. Data Integrity- Data માં કોઈ ચેડાં ન થાય.

Session Management: User લાંબા સમય સુધી નિષ્ક્રિય હોય તો Automatic Logout.

Audit Trail- કોણે શું કર્યું? ક્યારે કર્યું? તેનો Record.

Exception Handling: Software Error આવેતો Sensitive Information બહાર ન જાય.

"Software માત્ર કામ કરતું હોવું પૂરતું નથી; તે સુરક્ષિત રીતે કામ કરતું હોવું વધુ મહત્વનું છે."

3.3 Defence in Depth

RBI Requirement: Software Development દરમિયાન Defence in Depth અપનાવવું.

Defence in Depth શું છે?

એક Security Control નિષ્ફળ જાય તો બીજું Control, ત્રીજું Control, ચોથું Control, હુમલો અટકાવે.

ઉદાહરણ Internet Banking, Password, OTP, Transaction Password, Risk Monitoring, Fraud Detection આ બધું Layered Security છે.

RBI આ શા માટે કહે છે? એક Password Leak થઈ જાય તો OTP બચાવે. OTP Leak થાય તો Fraud Detection બચાવે.

Defence in Depth.

"એક તાળા પર વિશ્વાસ ન કરો. બેંકમાં પણ અને Cyber Security માં પણ અનેક તાળાં હોવા જોઈએ."

3.4 Adoption of New Technology

RBI Requirement: નવી Technology જેમ કે AI, Cloud, API Banking, UPI, Open Banking, Blockchain, અપનાવતા પહેલાં તેના Cyber Risks નું મૂલ્યાંકન કરવું.

નવી Technology સારી હોય એટલે તરત જ તેનો ઉપયોગ શરૂ ન કરવો. પહેલાં તપાસવું: ✓ સુરક્ષિત છે? ✓ Risks શું છે? ✓ IT Team ને તેનો અનુભવ છે? નવી Technology સાથે નવી Vulnerabilities પણ આવે છે

"નવી Technology ઝડપથી અપનાવવી સારી વાત છે, પરંતુ સમજ્યા વગર અપનાવવી જોખમી છે."

"Technology પહેલા આવે કે Security? RBI નો જવાબ છે – બંને સાથે."

Auditor શું તપાસશે?

IS Auditor સામાન્ય રીતે પૂછશે:

✓ Source Code Audit Report છે?

✓ Vendor નું Security Assurance છે?

- ✓ Secure SDLC Policy છે?
- ✓ Access Control Design Document છે?
- ✓ Threat Modelling થયું છે?
- ✓ Secure Coding Guidelines છે?
- ✓ New Technology Risk Assessment છે?
- ✓ Penetration Testing પછી Software Live થયું?

Level III ASLC નો સાર

Business Requirement, Security Requirement, Secure Coding Source Code Audit Security Testing Risk Assessment Production Deployment Continuous Monitoring

Directors અને CEOs માટે એક મિનિટનો સંદેશ

"આજના સમયમાં બેંકની સૌથી મોટી સંપત્તિ માત્ર Core Banking System નથી, પરંતુ તેનું સુરક્ષિત Software છે. જો Software ની ડિઝાઇનમાં સુરક્ષા ન હોય તો પછી કેટલા પણ Firewall, Antivirus કે SOC લગાવો, જોખમ સંપૂર્ણપણે દૂર થતું નથી. તેથી RBI Level III માં ભાર મૂકે છે કે Security અંતે ઉમેરવાની વસ્તુ નથી; Security તો Software ની પ્રથમ લાઇનથી જ શરૂ થવી જોઈએ."

User Access Control નો સૌથી મહત્વપૂર્ણ ભાગ છે. આજના મોટાભાગના Cyber Frauds Weak Access Control ના કારણે થાય છે, Hacking ના કારણે નહીં. RBI હવે માત્ર Password પર નહીં પરંતુ Identity & Access Management (IAM) પર ભાર મૂકે છે.

4. User Access Control

4.1 RBI Requirement

Critical Applications, Operating Systems, Databases, Network Devices અને Security Systems માટે Identity & Access Management (IAM) દ્વારા Centralised Authentication અને Authorisation System અમલમાં મૂકવો. તેમાં Strong Password Policy, Two-factor/Multi-factor Authentication (2FA/MFA), Least Privilege Principle અને Separation of Duties નો અમલ કરવો.

1 બેંકમાં તમામ મહત્વપૂર્ણ IT સિસ્ટમો (CBS, ATM Switch, Database, Firewall, Server વગેરે) માટે એવી કેન્દ્રિય (Centralised) વ્યવસ્થા હોવી જોઈએ કે:

- કોણ Login કરી શકે?
- કોણ શું જોઈ શકે?
- કોણ શું ફેરફાર કરી શકે?

- કોણ Approval આપી શકે?

આ બધું એક જ સુરક્ષિત વ્યવસ્થા દ્વારા નિયંત્રિત થાય.

Identity & Access Management (IAM) શું છે?

IAM એટલે: "યોગ્ય વ્યક્તિને, યોગ્ય સમયે, યોગ્ય સિસ્ટમમાં, યોગ્ય અધિકાર સાથે પ્રવેશ આપવાની વ્યવસ્થા."

IAM ચાર પ્રશ્નોના જવાબ આપે છે: તમે કોણ છો? (Identity) તમારી ઓળખ સાચી છે? (Authentication) તમને શું કરવાની મંજૂરી છે? (Authorization) તમે શું કર્યું? (Audit Trail)

RBI આ શા માટે કહે છે? જો દરેક સિસ્ટમ માટે અલગ User ID અને Password હોય, તો:

- Password Management મુશ્કેલ બને. કર્મચારી નોકરી છોડે પછી Access બંધ કરવાનું રહી જાય. Audit કરવું મુશ્કેલ બને. તેથી RBI કહે છે: એક કેન્દ્રિય વ્યવસ્થા (IAM) બનાવો.

Authentication એટલે શું?

Authentication એટલે: "User ખરેખર તે જ વ્યક્તિ છે કે નહીં તેની ખાતરી."

Authorization એટલે શું?

Authorization એટલે: "Login થયા પછી User શું કરી શકે?" ઉદાહરણ: Cashier: ✓ Cash Entry

Strong Password Policy

- લાંબા Password
- Complex Password
- નિયમિત બદલવા
- Default Password નહીં
- Password Share નહીં કરવો

Multi-Factor Authentication (MFA)

એક Password પૂરતો નથી. Password, OTP, Biometric

Privileged Access શું છે? Privileged Access એટલે Administrator, Database Admin, Network Admin, CBS Super User, આ User પાસે ખૂબ અધિકાર હોય છે. તેમની વિશેષ દેખરેખ જરૂરી છે. આ Cyber Security નો Golden Rule છે. તેનો અર્થ:

"જેટલી જરૂર હોય એટલો જ અધિકાર આપવો."

Separation of Duties (SOD)

એક જ વ્યક્તિ પાસે સંપૂર્ણ સત્તા ન હોવી જોઈએ.

ઉદાહરણ

એક જ વ્યક્તિ Loan બનાવે અને Loan Approve પણ કરે તો Fraud નો જોખમ વધે.

RBI આ શા માટે કહે છે? ઘણા Fraud બહારના Hacker કરતા અંદરના કર્મચારીઓ દ્વારા થાય છે. Separation of Duties તે અટકાવે છે.

Auditor શું તપાસશે?

- ✓ User Matrix
- ✓ Role Based Access
- ✓ Privileged User List
- ✓ Password Policy
- ✓ MFA Enabled?
- ✓ Dormant IDs
- ✓ Employee Exit પછી Access બંધ?
- ✓ Access Review થાય છે?

"બેંકની ચાવી દરેકને આપી શકાતી નથી. તેવી જ રીતે CBS ની ચાવી પણ દરેક User ને આપી શકાતી નથી."

"Cyber Security માં વિશ્વાસ કરતાં નિયંત્રણ વધુ મહત્વનું છે."

"Least Privilege એટલે કર્મચારીને કામ કરવા જેટલો જ અધિકાર આપવો, વધારે નહીં."

4.2 Active Directory / Endpoint Management

RBI Requirement: Active Directory અથવા Endpoint Management System દ્વારા Centralised Policies અમલમાં મૂકવી.

અને USB External Hard Disk Pen Drive CD/DVD જેમ Removable Media ને Whitelist Blacklist અથવા Restrict કરવું.

બેંકમાં તમામ Computers માટે એક કેન્દ્રિય નિયંત્રણ હોવું જોઈએ. કયો USB ચાલશે? કયો નહીં? કઈ Website ખુલશે?

કઈ નહીં? કયું Software Install થશે? કયું નહીં? આ બધું Active Directory અથવા Endpoint Management દ્વારા નિયંત્રિત કરવું.

Active Directory શું છે?

Microsoft નું Central User Management System. તે દ્વારા ✓ Login ✓ Password ✓ User Rights ✓ Group Policy ✓ Printer ✓ Shared Folder બધું નિયંત્રિત થાય છે.

Endpoint Management શું છે? બેંકના Desktop Laptop Mobile Tablet ATM PC બધાનું Central Management.

Whitelist શું છે? ફક્ત મંજૂર વસ્તુઓ ચાલે.

Blacklist શું છે? જોખમી વસ્તુઓ સંપૂર્ણ Block.

Restrict એટલે? ખાસ Permission પછી જ ઉપયોગ.

Auditor શું પૂછશે?

✓ Active Directory છે?

✓ Endpoint Management છે?

✓ USB Policy છે?

✓ Group Policy છે?

✓ Unauthorized Software Install થાય છે?

✓ Device Control છે?

"દરેક Computer અલગ રીતે ચલાવવાને બદલે સમગ્ર બેંકના Computers એક જ જગ્યાએથી નિયંત્રિત થવા જોઈએ."

Pen Drive નાનો હોય છે, પરંતુ તેની અંદર રહેલો Virus આખી બેંકને બંધ કરી શકે છે."

"Access Control નો અર્થ માત્ર Login નથી; તે એ પણ નક્કી કરે છે કે User શું કરી શકે અને શું નહીં."

"બેંકમાં જેમ Strong Room ની ચાવી દરેક કર્મચારીને આપવામાં આવતી નથી, તેવી જ રીતે CBS, Database, Server અને Firewall જેવા Critical Systems નો અધિકાર પણ માત્ર અધિકૃત વ્યક્તિઓને જ મળવો જોઈએ. RBI Level III નો મુખ્ય સિદ્ધાંત એ છે કે દરેક User ને તેના કામ માટે જરૂરી એટલો જ અધિકાર આપવામાં આવે, અને સમગ્ર Access કેન્દ્રિય રીતે નિયંત્રિત અને સતત મોનિટર કરવામાં આવે."

5.1 Robust Defence Against Malicious Code

RBI Requirement

Build a robust defence against the installation, spread, and execution of malicious code at multiple points in the enterprise.

1. બેંકમાં એવી મજબૂત અને બહુસ્તરીય (Multi-layered) સુરક્ષા વ્યવસ્થા હોવી જોઈએ કે:

- Malware (Virus) Install ન થઈ શકે.
- Install થઈ જાય તો અન્ય Computers માં ફેલાઈ ન શકે.
- Malware ચાલવાનું (Execute) શરૂ કરે તે પહેલાં જ તેને અટકાવી શકાય.

Malicious Code એટલે શું?

Malicious Code એટલે બેંકને નુકસાન પહોંચાડવા માટે બનાવવામાં આવેલ Software.

જેમ કે: Virus Worm Trojan Horse Ransomware Spyware Keylogger Rootkit

આધુનિક Malware માત્ર એક Computer સુધી મર્યાદિત રહેતું નથી. તે થોડા જ મિનિટોમાં આખા Network માં ફેલાઈ શકે છે.

તેથી RBI કહે છે: "માત્ર Antivirus પૂરતું નથી; દરેક સ્તરે સુરક્ષા જરૂરી છે."

Multi-layer Defence કેવી રીતે કામ કરે?

પ્રથમ સ્તર Email Security- Phishing Email Block, બીજો સ્તર, Firewall- Malware Download Block, ત્રીજો સ્તર, Endpoint Security-Virus Detect, ચોથો સ્તર, Application Control-Unknown Program Execute ન થાય, પાંચમો સ્તર, Network Monitoring. Malware બીજા Computer માં ફેલાય તો Alert

"Cyber Security નો હેતુ માત્ર Virus પકડવાનો નથી; Virus ને Install પણ ન થવા દેવાનો અને ફેલાતો પણ અટકાવવાનો છે."

"એક Antivirus આખી બેંકને સુરક્ષિત રાખી શકતું નથી. અનેક સુરક્ષા સ્તરો સાથે મળીને જ સુરક્ષા શક્ય બને છે."

5.2 Website Whitelisting

RBI Requirement

Implement Whitelisting of Internet Websites/Systems.

બેંકના Computers પર માત્ર મંજૂર કરેલી Websites જ ખુલવી જોઈએ. બાકીની Websites Block કરવી.

Whitelisting શું છે? Whitelist એટલે: માત્ર મંજૂર Websites. ઉદાહરણ, મંજૂર ✓ RBI ✓ NPCI

RBI આ શા માટે કહે છે? ઘણા Malware, Fake Websites થી Download થાય છે.

"દરેક Website ખોલવાની સ્વતંત્રતા Cyber Security નું જોખમ બની શકે છે."

6. Maintenance, Monitoring and Analysis of Audit Logs

Audit Log શું છે? Audit Log એટલે Computer અથવા Software ની Digital Diary અથવા ઇલેક્ટ્રોનિક નોંધપોથી.

તેમાં લખાય છે કોણ Login થયું? ક્યારે Login થયું? શું કર્યું? ક્યારે Logout થયું? કોણે Password બદલ્યો?

6.1 RBI Requirement Stakeholders સાથે ચર્ચા કરીને નક્કી કરવું: કયા Logs રાખવાના? કેટલા સમય સુધી રાખવાના? ક્યાં Store કરવાના? "જે રીતે બેંક Cash Book રાખે છે, તેવી જ રીતે IT System Audit Log રાખે છે."

6.2 Audit Log Analysis

RBI Requirement

Logs માત્ર રાખવાના નહીં પણ તેનું નિયમિત Analysis કરવું.

RBI આ શા માટે કહે છે? Log માત્ર Record નથી. તે Early Warning System છે.

"Audit Log વાંચવામાં આવે ત્યારે જ તેની કિંમત છે; નહીં તો તે માત્ર Computer ની ડાયરી છે."

6.3 Appropriate Logs

RBI Requirement દરેક Device, Operating System Application, Database ની Logs રાખવા. Log માં ઓછામાં ઓછું Date, Time Stamp, Source Address, Destination Address હોવું જોઈએ.

Auditor શું તપાસશે?

✓ બધા Server Logs ચાલુ છે?

✓ Firewall Logs છે?

✓ CBS Logs છે?

✓ ATM Logs છે?

✓ Log Retention Policy છે?

✓ Logs સાથે ચેડાં થઈ શકે?

✓ Log Review થાય છે?

✓ SIEM માં Logs જાય છે?

Directors માટે મહત્વનો સંદેશ

"બેંકમાં CCTV Camera જેટલો મહત્વનો છે, IT System માં Audit Log એટલો જ મહત્વનો છે. CCTV ચિત્ર બતાવે છે, જ્યારે Audit Log ડિજિટલ પુરાવો આપે છે."

"Cyber Attack પછી સૌથી પહેલો સાક્ષી Audit Log હોય છે."

"Log વગર Investigation કરવી એટલે FIR વગર પોલીસ તપાસ કરવા જેવી વાત છે."

"Malware ને રોકવું મહત્વનું છે, પરંતુ જો તે અંદર આવી જાય તો તેને શોધવામાં Audit Logs સૌથી મોટું હથિયાર છે."

એક મિનિટનો સમાપન સંદેશ

***"Level III નો આ વિભાગ બેંકને 'પ્રતિક્રિયા આપતી સંસ્થા'માંથી 'સજાગ અને બુદ્ધિશાળી સંસ્થા' બનાવે છે. Malware સામે બહુસ્તરીય સુરક્ષા, માત્ર મંજૂર Websites નો ઉપયોગ અને દરેક ડિજિટલ પ્રવૃત્તિનો વિશ્વસનીય Audit Trail – આ ત્રણેય મળીને બેંકને સાયબર હુમલા સામે વધુ સક્ષમ બનાવે છે."

આ વિભાગ Level III માં સૌથી મહત્વપૂર્ણ વિભાગોમાંનો એક છે. RBI હવે માત્ર Cyber Attack અટકાવવા વિશે નથી કહેતી, પરંતુ હુમલો થયા પછી બેંક કેટલી ઝડપથી અને કેટલી સુરક્ષિત રીતે ફરી કાર્યરત થાય છે (Cyber Resilience) તેના પર ભાર મૂકે છે.

મારી દૃષ્ટિએ, Directors અને CEOs ને આ વિભાગ સમજાવતી વખતે એક વાત જરૂર કહેવી જોઈએ:

"Cyber Security નો અર્થ માત્ર હુમલો અટકાવવો નથી; પરંતુ હુમલો થાય તો પણ બેંકનું કામ અટકવું ન જોઈએ."

આ જ Cyber Resilience નો મૂળ સિદ્ધાંત છે.

7. Incident Response and Management

Incident Response એટલે શું?

Incident Response એટલે કોઈપણ Cyber Security Incident (જેમ કે Ransomware, Phishing, Data Breach, Malware Attack, CBS Failure વગેરે) બને ત્યારે બેંકે પૂર્વનિર્ધારિત યોજના મુજબ તરત અને યોગ્ય કાર્યવાહી કરવી.

Incident Management એટલે શું?

Incident Management એટલે:

- ઘટનાની ઓળખ (Detection)
- ઘટનાની જાણ (Reporting)
- હુમલો રોકવો (Containment)
- નુકસાનનું મૂલ્યાંકન (Assessment)
- સિસ્ટમ પુનઃસ્થાપિત કરવી (Recovery)
- ભવિષ્યમાં ફરી ન બને તે માટે સુધારા (Lessons Learnt)

7.1 BCP/DR અને Cyber Resilience

RBI Requirement

BCP/DR એવી રીતે તૈયાર કરવું કે Cyber Attack પછી બેંક ઝડપથી Recovery કરી શકે અને Recovery Time Objective (RTO) અનુસાર Critical Services ફરી શરૂ કરી શકે. Recovery દરમિયાન Data અને Security પણ સુરક્ષિત રહેવી જોઈએ.

બેંક પાસે એવી Business Continuity Plan (BCP) અને Disaster Recovery (DR) યોજના હોવી જોઈએ કે જો Cyber Attack થાય તો:

- ગ્રાહકોને ઓછી અસર થાય.
- બેંકનું કામ ઝડપથી ફરી શરૂ થાય.
- Customer Data સુરક્ષિત રહે.
- CBS, ATM, UPI જેવી મહત્વપૂર્ણ સેવાઓ ચાલુ થઈ જાય.

BCP શું છે?

Business Continuity Plan (BCP)

"બેંકનું કામ કોઈપણ પરિસ્થિતિમાં બંધ ન થાય તેની યોજના."

DR શું છે?

Disaster Recovery (DR)

"મૂળ સિસ્ટમ નિષ્ફળ જાય તો Backup Site પરથી સેવા ફરી શરૂ કરવાની વ્યવસ્થા."

Cyber Resilience શું છે?

Cyber Security = હુમલો અટકાવવો

Cyber Resilience = હુમલા પછી પણ ઝડપથી ઉભા થવું

Recovery Time Objective (RTO)

RTO એટલે: "સિસ્ટમ કેટલા સમયમાં ફરી ચાલુ થવી જોઈએ?"

Recovery Point Objective (RPO)

RPO એટલે: "વધુમાં વધુ કેટલો Data ગુમાવી શકાય?"

"BCP એ કાગળ પરની યોજના નથી; તે બેંકને જીવંત રાખવાની યોજના છે."

"Cyber Attack પછી બેંક કેટલા સમયમાં ફરી ઉભી થાય છે, તે જ તેની Cyber Resilience બતાવે છે."

7.2 Third Party Vendor Coordination

RBI Requirement

જો બેંકની IT Services Vendor સંભાળે છે, તો Incident સમયે Vendor સાથે લેખિત પ્રક્રિયા હોવી જોઈએ. Vendor તરત બેંકને જાણ કરે.

જો CBS, ATM Switch, Cloud અથવા Data Centre Vendor પાસે હોય, તો Cyber Attack થાય ત્યારે Vendor શું કરશે, Bank શું કરશે, કોણ કોને જાણ કરશે, તે બધું પહેલેથી લખેલું હોવું જોઈએ.

RBI આ શા માટે કહે છે? ઘણી UCB Outsourcing કરે છે. પણ Incident થાય ત્યારે Vendor અને Bank વચ્ચે ગૂંચવણ થાય છે.

કોણ જવાબદાર? કોણ RBI ને જાણ કરશે? કોણ Customer ને જાણ કરશે? આ બધું પહેલેથી નક્કી હોવું જોઈએ.

"Outsourcing કરવાથી જવાબદારી બહાર જતી નથી. જવાબદારી હંમેશા બેંકની જ રહે છે."

7.3 Lessons Learnt

RBI Requirement દરેક Incident પછી તેમાંથી શું શીખ્યા? તેના આધારે Policy સુધારવી. દરેક Cyber Incident પછી

માત્ર Recovery કરવી પૂરતી નથી. પછી બેઠક કરીને જાણવું: આ કેમ થયું? આગળ શું સુધારવું? ફરી ન બને તે માટે શું કરવું? **Incident Review Meeting**

Stakeholder Communication Incident સમયે યોગ્ય સંકલન હોવું જોઈએ. કોને જાણ કરવી? Board-CEO-CISO-IT Team-Vendor-CERT-In-RBI-Customer

"દરેક Cyber Incident એક ખર્ચાળ ભૂલ નહીં, પરંતુ એક મોંઘો પાઠ છે. જો આપણે તેમાંથી શીખીએ તો ભવિષ્યમાં મોટા નુકસાનથી બચી શકીએ."

"Incident પછી સૌથી મોટો પ્રશ્ન 'કોણ જવાબદાર?' નહીં, પરંતુ 'આગળ ફરી ન બને તે માટે શું કરવું?' હોવો જોઈએ."

સારી બેંક એ નથી કે જ્યાં Incident ક્યારેય ન થાય; સારી બેંક એ છે જે Incident પછી ઝડપથી Recovery કરે અને તેમાંથી શીખે."

Auditor શું તપાસશે?

IS Auditor સામાન્ય રીતે નીચેની બાબતો ચકાસશે:

- ✓ Incident Response Policy
- ✓ Cyber Crisis Management Plan
- ✓ BCP Document

- ✓ DR Policy
- ✓ RTO અને RPO નિર્ધારિત છે?
- ✓ DR Drill થાય છે?
- ✓ Vendor Incident Reporting Clause
- ✓ CERT-In/RBI Reporting Procedure
- ✓ Incident Register
- ✓ Root Cause Analysis (RCA)
- ✓ Lessons Learnt Report
- ✓ Corrective Action Taken Report

"RBI Level III નો આ વિભાગ આપણને એક મહત્વપૂર્ણ સંદેશ આપે છે - Cyber Security નું અંતિમ લક્ષ્ય હુમલો અટકાવવું જ નથી, પરંતુ બેંકને એવી રીતે તૈયાર કરવી છે કે જો હુમલો થાય તો પણ ગ્રાહકોનો વિશ્વાસ ન તૂટે, બેંકની સેવાઓ ઝડપથી ફરી શરૂ થાય અને દરેક ઘટનામાંથી શીખીને ભવિષ્ય માટે વધુ મજબૂત વ્યવસ્થા ઊભી થાય. આ જ સાચા અર્થમાં Cyber Resilience છે."

8. User / Employee / Management Awareness

RBI નો મુખ્ય હેતુ

"Cyber Security માત્ર IT Department ની જવાબદારી નથી. બેંકના દરેક કર્મચારી, દરેક અધિકારી, દરેક મેનેજર અને દરેક Director એ Cyber Security નો સક્રિય ભાગીદાર હોવો જોઈએ."

8.1 Encourage Reporting of Suspicious Behaviour

RBI Requirement

Encourage them to report suspicious behaviour incidents to the incident management team.

બેંકે એવી સંસ્કૃતિ (Cyber Security Culture) વિકસાવવી જોઈએ કે જેમાં કોઈપણ કર્મચારીને જો કોઈ શંકાસ્પદ ઘટના દેખાય તો તે ડર્યા વગર તરત જ Incident Management Team અથવા IT Security Team ને જાણ કરે.

"Suspicious Behaviour" એટલે શું?

એવી કોઈપણ ઘટના જે સામાન્ય ન લાગે.

ઉદાહરણો

- અજાણી Email આવવી.
- અજાણી Link પર Click કરવાની વિનંતી.
- CBS માં અજાણ્યું Login.
- Password પોતે બદલાઈ જવો.

- Computer અચાનક ધીમો થઈ જવો.
- Antivirus બંધ થઈ જવો.
- અજાણી USB મળી આવવી.
- ગ્રાહકના ખાતામાં અસામાન્ય Transaction.
- ATM માં અસામાન્ય પ્રવૃત્તિ.
- Server માં અજાણી File બનવી.

RBI આ શા માટે કહે છે?

ઘણી Cyber ઘટનાઓ શરૂઆતમાં નાની લાગે છે. જો કર્મચારી તરત જાણ કરે, તો મોટું નુકસાન અટકી શકે. જો ડરે, અથવા વિચારે કે "આ તો સામાન્ય બાબત હશે" તો હુમલો ફેલાઈ શકે.

"સાયબર સુરક્ષામાં શંકા કરવી એ ખરાબ બાબત નથી; યોગ્ય સમયે શંકા કરવી એ જ સારી સુરક્ષા છે."

"જો તમને કંઈક અસામાન્ય લાગે, તો મૌન ન રહો - તરત જાણ કરો."

"ઘણી વખત એક કર્મચારીની સમયસર આપેલી માહિતી આખી બેંકને બચાવી શકે છે."

8.2 Mandatory Cyber Security Awareness Programme

RBI Requirement

Make cyber security awareness programs mandatory for new recruits and web-based quiz and training for lower, middle and upper management every year.

દરેક નવા કર્મચારી માટે Cyber Security Training ફરજિયાત હોવી જોઈએ.

તે ઉપરાંત દર વર્ષે કર્મચારી માટે માટે Cyber Security Training અને Online Quiz યોજાવી.

RBI આ શા માટે કહે છે? Technology સતત બદલાય છે. Cyber Fraud ની નવી પદ્ધતિઓ દર વર્ષે આવે છે. પાંચ વર્ષ જૂની Training આજે પૂરતી નથી.

નવા કર્મચારીઓને શું શીખવવું?

- Password Policy
- Email Security
- Phishing
- USB નો ઉપયોગ
- Data Privacy
- Social Engineering
- Customer Information Protection
- Incident Reporting

Senior Management માટે શું?

- Cyber Risk
- RBI Guidelines
- Governance
- Business Continuity
- Vendor Risk
- Board Reporting

Cyber Security Week Online Quiz

- Phishing Simulation
- Poster Competition
- Cyber Awareness Session

આથી કર્મચારીઓ વધુ સતર્ક બને.

"Cyber Security એક વખત શીખવાની બાબત નથી; તે સતત શીખવાની પ્રક્રિયા છે."

"નવી ટેકનોલોજી જેટલી ઝડપથી બદલાય છે, એટલી જ ઝડપથી આપણી જાણકારી પણ અપડેટ થવી જોઈએ."

8.3 Board Awareness

RBI Requirement

Board members may be sensitised on various technological developments and cyber security related developments periodically.

બોર્ડ ઓફ ડિરેક્ટર્સને સમયાંતરે નવી ટેકનોલોજી અને Cyber Security ના નવા જોખમો વિશે માહિતી અને તાલીમ આપવી.

RBI આ શા માટે કહે છે? આજે Cyber Security માત્ર IT નો વિષય નથી. તે Governance નો વિષય છે. Board પાસે યોગ્ય સમજણ ન હોય, તો યોગ્ય નિર્ણયો લઈ શકાશે નહીં.

Directors ને શું જાણવું જોઈએ?

- Cyber Risk Landscape
- RBI Circulars
- Digital Banking Risks
- Ransomware
- Phishing
- Business Email Compromise (BEC)
- Third Party Risk
- Cloud Computing

- Artificial Intelligence Risks
- Cyber Insurance
- BCP / DR

દર ત્રણ મહિને Board Meeting પહેલાં 30 મિનિટનું Cyber Risk Update પ્રસ્તુત કરવામાં આવે છે. છેલ્લા ત્રણ મહિનાના Cyber Incidents નવલ RBI Circulars Pending Compliance, Top Risks

"Board પાસે IT નું Technical Knowledge હોવું જરૂરી નથી, પરંતુ Cyber Risk સમજવાની ક્ષમતા હોવી અત્યંત જરૂરી છે."

"આજના સમયમાં Cyber Security એ માત્ર IT Investment નથી; તે Business Survival માં કરાવેલું રોકાણ છે."

Auditor શું તપાસશે?

Information System Auditor સામાન્ય રીતે પૂછશે:

- ✓ Cyber Security Awareness Policy છે?
- ✓ નવલ કર્મચારીઓની Training નો Record છે?
- ✓ Annual Training Calendar છે?
- ✓ Phishing Simulation થાય છે?
- ✓ Online Quiz થાય છે?
- ✓ Attendance Record છે?
- ✓ Board ને Cyber Risk Presentation આપવામાં આવે છે?
- ✓ Board Minutes માં Cyber Security ચર્ચાનો ઉલ્લેખ છે?
- ✓ Awareness Posters / Emails મોકલાય છે?

UCB માટે વાર્ષિક Cyber Security Awareness Calendar

સમય પ્રવૃત્તિ

જાન્યુઆરી તમામ કર્મચારીઓ માટે Cyber Security Refresher Training

માર્ચ Phishing Simulation Exercise

જૂન Cyber Security Quiz

સપ્ટેમ્બર Branch-wise Awareness Programme

ડિસેમ્બર Board & Senior Management Cyber Risk Session

"Firewalls, Antivirus અને SOC કરોડો રૂપિયાનું રોકાણ હોઈ શકે છે, પરંતુ એક અજાણ કર્મચારી એક ખોટી Link પર Click કરીને તે તમામ સુરક્ષા વ્યવસ્થાને નિષ્ફળ બનાવી શકે છે. તેથી RBI Level III નો અંતિમ અને સૌથી મહત્વપૂર્ણ સંદેશ એ છે કે સાયબર સુરક્ષા માત્ર ટેકનોલોજીથી નહીં, પરંતુ જાગૃત કર્મચારીઓ, સતર્ક મેનેજમેન્ટ અને માહિતગાર Board દ્વારા જ મજબૂત બને છે."

GUARDED