Securing Infrastructure for DFS

Narendra Nath Gangavarapu
Department of Telecommunications
India

- Single-layer risk mitigation strategies such as a cyber insurance cover might shield an organization's financial exposure, but may erode public trust in the system and cause systemic risks.
- Lay down a comprehensive approach
  - Balance between cost of fraud and firms' incentives towards putting adequate level of controls.
-

- Number and sophistication of cyber-attacks is increasing
- Data on cyber frauds in the financial sector as per RBI incident reporting indicate amount involved in cyber frauds past three years averaged about Rs.75 crore per annum.
- Cost incurred on account of frauds is perceived to be less than cost of security required to prevent such frauds
- Undermine confidence in digital payment system
- Opportunity cost in terms of delay in adoption of digital payments.

- The Committee of Chief Ministers on Digital Payment had advised to set up a Digital Payment Security Committee (DPSC).
- Process Sub-Committee headed by RBI member of the Committee for providing guidance on processes associated with digital payment security
- Technical Sub-committee to be headed by DoT member of the Committee for providing guidance on technological issues relating to ensuring digital payment security.

- Action Items consisting of set of recommendations leading to strengthening of Digital Financial Systems have been grouped as:
  - Strengthening the device security
  - Strengthening the network security
  - Strengthening the SIM security
  - Strengthening the Mobile OS, App based security
  - Updation, Monitoring and Evaluation of security guidelines
  - Effective collaboration between the DFS ecosystem players
  - Consumer Guidelines
  - Policy Framework

- Standards based
  - Security as per ITU-T 805 framework
    - Across Infrastructure, Services and Applications layer
    - Over Management, Control, and End-user planes
    - Covering Access control, Authentication, Non-repudiation, Data confidentiality, Communication security, Data integrity, Availability and Privacy.
  - ITU-T Focus Group Digital Financial Services: *Security Aspects of Digital Financial Services (DFS)*"
  - ITU Y.2740, ITU Y.2741
  - ISO 12812: Technical Specifications addressing interoperable and secure systems for the provision, operation and management of Mobile Financial Services (MFS)
- Further, the guidance provided has generally been at a higher level without getting into minute and specific details

- Cyber Security Framework in Banks issued by RBI June, 2016
- Committee headed by former Chief Justice to “identify key data protection issues in India and recommend methods to addressing them”.
- Proposal to set up a Computer Emergency Response Team – Financial Sector (CERT-FIN) was mooted in the Budget 2017-18

- Incorrect linking of Aadhaar number with the bank account, embezzled more than Rs 11 lakh in 30 days.
  - Operational lapses
  - Absence of specific alert mechanism if any sensitive customer data is tampered with.
- Phone Fraud
  - Reporting mechanism
  - KYC, Device tracking
  - Multi agency SoP
  - CLI spoofing
- Replacement SIMs
- POS skimming - Mechanism to verify the authenticity of the devices before the card credentials are provided by the customers

- Security Guidelines
  - ADSL guidelines
  - WIFi guidelines
- DNSSEC implementation
- Security Policy Guidelines
- Security Audits
- Security Testing and Certification
- Mobile device – OTA updates
- SIM; Personalisation, Use of SIM Application Toolkit
- Securing USSD
- CEIR impementation

- Thank you