Cyber Security for Banking

Following are the modules covered in the course:

Module 1 – Insights into Cyber Security while building Banking Solutions

This is a comprehensive thought process about aspects that need consideration in the face of threats and potential cyber issues, how can any banking solution be built? What are the various use cases where newer technologies are likely to be implemented and how can we foolproof our systems to cover the cyber-crime prevention ground.

- Cyber Risk Assessment and Mitigation Techniques
- Assessing Vulnerabilities in Banking Solutions (Deriving Insights while building solutions)
- What to look out for when you are
    - Moving to Cloud
    - Implementing Blockchain Technologies
    - Implementing Big Data Management
    - Analyzing Data Patterns
    - Integrating various new technologies

- Cyber Vulnerabilities in **Use Cases**
    - KYC
    - Cross Border Payments
    - Asset Transfers
    - Peer to Peer Payments
    - Reduced complexity of Correspondent and partner banks
    - Deposits & Lending
    - Decentralized Finance
    - Contactless Payments

        - QR Code
        - E-Wallets
        - Google Pay
        - Apple Pay
        - Wearables using NFC Ring
        - Voice enabled payments

Current Trending Examples of Fraud and Breaches in Cyber Security

Module 2 – Fundamentals of Cyber Security

This module is focused on understanding certain technical terminology and how it impacts our Cyber Security systems, it is explained in a way that a layman can easily understand the terms. The topics will be covered with a functional understanding of how a cyber attack takes place and how we can mitigate it.

Topics covered

- Security Essentials
- Cryptography
- Computer Networks and Security
- Application Security
- Data and End Point Security
- Identity & Access Management
- Cloud Security
- Phases of a Cyber Attack
- Security Processes in Practice in Banking

Module 3 – Cyber Security in the Banking Ecosystem

This Module explains the importance of Cyber Security in banking, what types of attacks can a bank be subjected to? What should banks look out for in terms of compliance to ensure safety.

Topics covered

Cyber Security Threats faced by Banks

- Third Party Applications posing threats (E-Commerce Applications, E-Shopping Customers)
- Risks from Mobile Applications
- Continuous Threats to Data
- Phishing Attacks
- Ransomware Attacks
- Denial of Service Attacks

Importance of Cyber Security in Banking

- Safeguarding Bank's reputation
- Safeguarding customer's money
- Safeguarding customer data
- Adherence to compliance

Module 4 - Cyber Security Management Essentials

This is the most important subject which is not well covered by most training institutions that rely mostly on technical training. Understanding your Reserve Bank's policy and framework in terms of cyber security. How can your bank align your own policy framework and be compliant with the RBI. Manage risk, improvement in quality of service etc.

- Cyber Security Policy & Strategy
- Reserve Bank of India policy and framework on Cyber Security for Banks
- Board and Senior Management Accountability
- Penetration Testing & Vulnerability Assessment
- Information Sharing with other banks and financial institutions
- Ethical Hacking for Vulnerability testing
- Risk Management & Quality of Service Improvement
- Prevention Steps in circumventing and preventing Cyber Crime