GLOBAL TRENDS

With the increase in the development of technologies the banking industry is evolving at an extraordinary rate. Unmanned aerial systems, the Internet of Things, Near Field of Communication (NFCs), and nearable devices are some of the technological advancements that banks will need to consider in the near future.

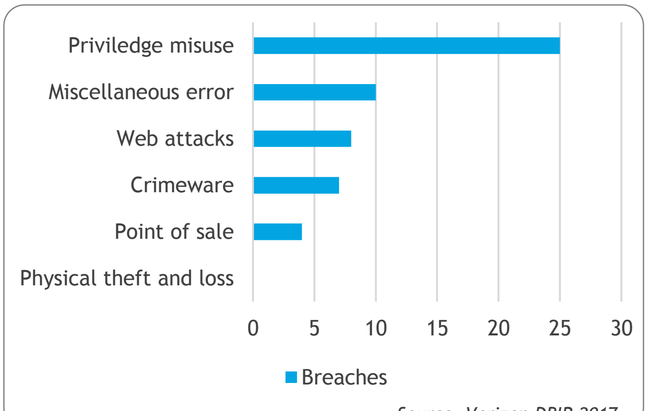
Few of the top upcoming priorities for banks could be cloud based platforms, robotic process automation and cognitive technologies. Automation will drive new efficiencies across the security lifecycle, but require the creation of control mechanisms and strong governance.

The above trends however pose their own set of challenges which are discussed in the next section.

CHALLENGES

The exponential growth of digital payments platform in India and the push towards a cashless economy has renewed focus on the need to strengthen cybersecurity posture. Few of the major challenges faced by banks include:

- **Strict compliance regulations**: Managing regulatory compliances has become enormously challenging for the banks. Over the past few years the volume of regulations has increased dramatically. Along with the larger banks, smaller ones too are required to fulfil the regulatory obligations
- **The struggle to secure customer data**: There are number of ways in which violation of privacy can take place in banking sector like stolen or loss card data, unauthorised sharing of data with third parties and loss of client's personal data due to improper security measures
- **Third party risk**: Banks need to conduct due diligence on third parties they are associated with. As per Payments card industry data security standard, third parties need to report any critical issues associated the card data environment to the bank .
- **Evolving cyber threat landscape**: The development in technologies is leading to the latest cyber threats like next generation ransomwares, web attacks etc.
- **Transaction frauds**: Fraud detection technologies should be in place with proper consideration of risks based on the business factors.
- **Secure SDLC**: Banks need to incorporate SDLC security for banking products and applications.



Source: Verizon DBIR 2017

REGULATORY PERSPECTIVE

To ensure security in banking industries, the Reserve Bank of India removed a **Circular DBS.CO.ITC.BC.No.6/31.02.008/ 2010-11** dated **April 29 2011**, where all banking institutions have to comply for. Some of the key features of the regulations are:

- Cyber Security Policy to be distinct from the broader IT policy / IS Security Policy of a bank
- Arrangement for continuous surveillance
- Comprehensive network and database security
- Protection of customer information
- Cyber security preparedness indicators
- Cyber Crisis Management Plan
- IT architecture should be conducive to security
- An immediate assessment of gaps in preparedness to be reported to RBI
- Cyber security awareness among stakeholders/ Top Management/ Board

Source: www.rbi.org.in

SECURITY CONSIDERATIONS

While each bank thinks distinctively on adopting various considerations it is imperative to assume that the theme remains the same for various banking channels:

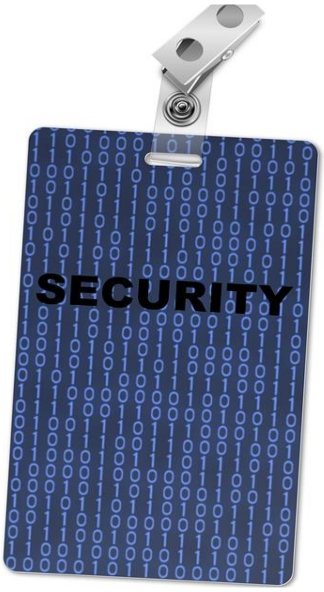
Internet Banking: Security controls like multi factor authentication, creation of strong passwords, adaptive authentication, image authentication, etc. can be considered.

Mobile Banking: It should be ensured that mobile applications are up to date and should be tested. Latest hardening standards could be implemented.

Wallet Transactions: Awareness material on Phishing, Malware attacks, vishing and social engineering, Password security etc. should be incorporated.

ATM Security: Biometrics like eye-retina, voice scan or fingerprint scan should be introduced by Banks.

UPI (Unified Payment Interface) : Banks and PSPs need to think through their security strategies, governance models and predictive controls to build a secure UPI environment that ensures a seamless user experience and at the same time balances security risks.



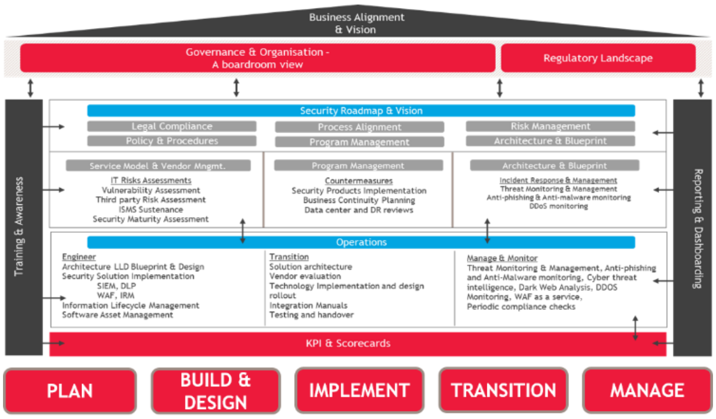
Banks must conduct regular drills, awareness programs and simulation exercises to keep their infrastructure secured.

APPROACH TO SECURITY

At BDO India, we endeavour to provide expertise driven solutions to help and assist our clients business needs are met, through a well defined risk based approach

Approach to adoption can have the following phases:

- **Plan**: Discussing the scope of work, making a roadmap for the approach, formalising leadership & project SPOC and to understand the policy and procedures all can be a part of the planning phase.
- **Build & Design**: The build phase consists of requirements as a part of a systems engineering process. The main milestone of design phase would be matching the system specifications and the disposition of risk from the organisation as shown in the framework.
- **Implementation**: Gaps identified during the plan phase are implemented. Integration elements should be carefully planned.
- **Transition**: A seamless transition and handover to the operations team should be taken into consideration.
- **Manage**: This phase includes management, monitoring, and periodic reviews against security threats and frauds.


Business Alignment & Vision
Governance & Organisation - A boardroom view
Regulatory Landscape
Training & Awareness
Reporting & Dashboarding
Security Roadmap & Vision
Legal Compliance
Policy & Procedures
Process Alignment
Program Management
Risk Management
Architecture & Blueprint
Service Model & Vendor Mngmt.
IT Risks Assessments
Vulnerability Assessment
Third party Risk Assessment
ISMS Sustenance
Security Maturity Assessment
Program Management
Countermeasures
Security Products Implementation
Business Continuity Planning
Data center and DR reviews
Architecture & Blueprint
Incident Response & Management
Threat Monitoring & Management
Anti-phishing & Anti-malware monitoring
DDoS monitoring
Operations
Engineer
Architecture LLD Blueprint & Design
Security Solution Implementation
SIEM, DLP
WAF, IRM
Information Lifecycle Management
Software Asset Management
Transition
Solution architecture
Vendor evaluation
Technology Implementation and design rollout
Integration Manuals
Testing and handover
Manage & Monitor
Threat Monitoring & Management, Anti-phishing and Anti-Malware monitoring, Cyber threat intelligence, Dark Web Analysis, DDOS Monitoring, WAF as a service,
Periodic compliance checks
KPI & Scorecards
PLAN
BUILD & DESIGN
IMPLEMENT
TRANSITION
MANAGE

Detailed cyber security framework is shown on the next page