Contents

2 Executive Summary
4 Disruptive Innovations in Financial Services Industry
5 The Evolving Cyber Threat Landscape
7 Increased Regulatory Requirements
8 Multi-pronged Approach to Managing Cyber Risks
9 India Contacts
Technology trends and a shift to digital business, accompanied with the revolution in the smart systems, have caused a massive re-positioning of the financial services market from a fundamentally labor-based model to an automated process-driven business model. We see an emergence of new, agile, and hitherto largely unregulated players who are dis-intermediating the traditional incumbents. Regulation is making it harder to innovate and to grow, while legacy strategy, infrastructure, and thinking are preventing the existing players from responding aggressively to these threats.

As consumer behavior evolves, traditional players are facing new competitors in direct and mobile banking. In the payment market, cash and credit cards are giving way to digital alternatives. Cyber-attacks on financial services companies are increasingly diverse — and therefore unpredictable — and are also here to stay. When the attack severity increases, it may be likely that only a resilient and flexible cybersecurity model can prepare financial services companies to survive the inevitable cyber risks. As such, financial services firms should consider raising their level of preparedness and evolve into a new cyber risk management paradigm that strives to achieve three fundamental qualities:

1. **Being secure** against known threats through risk-driven investment in foundational, preventive controls, and policies
2. **Being vigilant** by improving the ability to detect emerging threats and anomalous patterns amid the highly complex and data-saturated environment; and
3. **Being resilient** to enable the organization to recover from attacks as quickly as possible and minimize both direct and indirect damages.

Actionable threat intelligence – derived from a wide range of sources and well-defined governance processes, which instill cyber risk awareness, accountability, and effective continuous adaptation can be critical fuel in driving this paradigm shift. For many firms, what are currently called IT risk management programs can evolve into executive-driven cyber risk management programs that are an integral part of strategic business planning.
Disruptive Innovations in Financial Services Industry

Disruptive innovation is an innovation that creates a new market and value network, and eventually disrupts an existing market and value network, displacing established market leaders and alliances. We are seeing an increasing number of disruptive innovations, with products and services offered by increasingly powerful alternative financial services providers seeking to dis-intermediate large incumbents’ stronghold on areas such as payments, financing, and deposits.

Disruptive innovations emerge as both an opportunity and a threat to banks. Digitization is a threat to traditional banking models but can also be an opportunity for banks that respond. The following sections illustrate how disruptive innovations are affecting financial businesses around the world.

Manage Consumer Interactions across Multiple Channels – Omni-channel Banking

Adoption of technology has resulted in higher penetration of mobile, internet, and smartphones cutting across consumer segments and geographies. This is changing consumer behavior, including buying behavior; with social networking, peer reviewing of products, and online research becoming the norm. Digital payments are becoming significant in India, and the evidence of the digital disruption is mounting in Financial Industry.

Channel preferences in banking have shifted significantly among younger and wealthier segments towards non-branch channels. About 40 percent of Asian mass-affluent customers now prefer online or mobile banking. Among those under 40 years of age, around 50% prefer digital banking. The internet is making headway in the generally older, affluent and mass-affluent segments, where ATM usage is the norm; for younger generations of Asians, on the other hand, the internet has become a preferred channel.

Banks must integrate across channels: this entails generating digital demand with smart tools, choosing intuitive products, and using direct channels for customer self-services. Digital banking is about more than enabling digital channels. Banks that successfully manage multichannel by creating a seamless customer experience, rethinking branch formats, and using data strategically, will be able to withstand competition and pressure from new technology players. They will also be better positioned to capture the loyalty of emerging and new customer segments.

Transacting and functioning on smartphones – Mobility

Popularity and increase in usage of mobile devices has made it imperative for the banks to develop mobile-based applications. Banks sourced to respond to the rapid adoption of the mobile platforms by providing basic services – however, these were quickly superseded by fully-functional mobile applications for performing banking transactions such as mobile peer-to-peer money transfer, bill payments, as well as wallet applications.

Process Externalization – The Cloud

The next generation of process externalization has created ripples across the financial services industry. Traditionally, organizations were required to buy packages – hardware, software, solutions – from several vendors, look for system integrators who would design and implement them and lastly onboard a partner who would assist in management and operations of all of these components in the information technology world. The organization was also expected to manage the compliance and mandates from regulations within their industry, ensuring they are audited regularly. Essentially, the organization was expected to perform all these activities, as well as the security of their business, to keep up with the cyber-crimes.

This was not only time-consuming and expensive, but it limited the organization to the vision of the services provided by their vendors and service providers. The software and the hardware had to be compatible with the accounting software implemented at the financial services provider. Cloud computing came up with a practical solution – while they could “own” the technology they opted for, the management of vendors and service providers as well as the housekeeping of the implemented technology was taken care of by the cloud service providers.

The Evolving Cyber Threat Landscape

The business and technology innovations that financial services companies are adopting in their quest for growth, innovation, and cost optimization, are in turn presenting heightened levels of cyber risks. These innovations have most likely introduced new vulnerabilities and complexities into the financial services technology ecosystem. For example, the continued adoption of alternate channels such as ATMs, kiosks, internet, mobile, cloud, and social media technologies have probably increased opportunities for attackers. Similarly, the waves of outsourcing, offshoring, and third-party contracting, driven by a cost reduction objective, may have further diluted institutional control over IT systems and access points. These trends have resulted in the development of an increasingly boundary-less ecosystems from which financial services companies operate, and thus has offered a much broader “attack surface” to the threat actors to exploit.

Account Takeovers: Cyber criminals have demonstrated their ability to exploit online financial and market systems that interface with Internet, such as the Automated Clearing House (ACH) systems, card payments, and market trades.

Payment Systems: Fraudulent monetary transfers and counterfeiting of stored value cards are the most common result of exploits against financial institutions, payment processors, and merchants.

ATM Skimming: ATM skimming is also a prevalent global cyber-crime. A criminal affixes a skimmer to the outside or inside of an ATM to collect card numbers and personal identification number (PIN) codes.

Point of sale terminals: Point of Sale (POS) terminals have been a primary target for cyber criminals engaging in credit card fraud and have resulted in the compromise of millions of credit and debit cards the US.

Mobile Banking Exploitation: As more mobile devices have been introduced into personal, business, or government networks, they have been increasingly targeted for stealing PII. Cyber criminals have successfully demonstrated man-in-the-middle attacks against mobile phones using malwares.
Banking in India is governed through various legal and regulatory requirements issued by the Government of India and the banking regulator – Reserve Bank of India (RBI). Periodically, RBI issues various circulars and guidelines on various aspects of Banking. The regulations may also vary depending on the type of bank e.g., Scheduled Commercial Bank, NBFC, Regional Rural Bank, Authorized Dealer Banks, etc.

RBI Guidelines on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds, issued in April 2011, define the fundamental information security requirements which all Banks need to follow. In addition to the above guidelines, there are multiple regulatory requirements related to Internet Banking, Payment Systems, Mobile Banking, IT Outsourcing, etc., which may be applicable to a particular bank depending on the context of the organization and the nature of its operations in India.

Some of the key RBI requirements are highlighted below:

- **June 2001**
  - Guidelines on Internet Banking in India

- **December 2007**
  - The Payment and Settlement Systems Act, 2007

- **December 2009**
  - System Audit of the Payment Systems operated under the PSS Act, 2007
  - Minimum Check to be followed for the Payment Systems operated under the PSS Act, 2007

- **February 2013**
  - Security and Risk Mitigation Measures for Electronic Payment Transactions

- **April 2011**
  - Guidelines on Information security, Electronic Banking, Technology risk management and cyber frauds

- **May 2015**
  - Security and Risk Mitigation Measures for Card Present and Electronic Payment Transactions

- **July 2014**
  - Master Circular on Credit Card, Debit Card and Rupee Denominated Collected Prepaid Card operations of banks

- **July 2015**
  - Guidelines on issue of ATM-cum-debit cards
  - Mobile Banking transactions in India – Operative Guidelines for Banks

- **July 2015**
  - Master Circular – Mobile Banking transactions in India – Operative Guidelines for Banks

- **July 2015**
  - Security and Risk Mitigation Measures for Card Present and Electronic Payments Transactions

- **November 2010**
  - Minimum Check to be followed for the Payment Systems operated under the PSS Act, 2007

- **July 2014**
  - Minimum Check to be followed for the Payment Systems operated under the PSS Act, 2007

De-risking India’s Banking Industry
Multi-pronged Approach to Managing Cyber Risks

Financial services firms have traditionally focused their investments on becoming secure. However, this approach is no longer adequate in the face of the rapidly changing threat landscape. Put simply, financial services companies should consider building cyber risk management programs to achieve three essential capabilities: the ability to be secure, vigilant and resilient.

Enhancing Security through a “defense-in-depth” Strategy

A good understanding of known threats and controls, industry standards and regulations can guide financial services firms to secure their systems through the design and implementation of preventative, risk-intelligent controls.

Based on leading practices, financial services firms can build a “defense-in-depth” approach to address known and emerging threats. This involves a number of mutually-reinforcing security layers both to provide redundancy and potentially slow down the progression of attacks-in-progress, if not prevent them. Such slowing down can work in the defendant's favor by providing adequate time to secure their digital assets and mount effective counter-strategies.

Enhancing Vigilance through Effective Early Detection and Signaling Systems

Early detection, through the enhancement of programs to detect both the emerging threats and the attacker’s moves, can be an essential step towards containing and mitigating losses. Incident detection that incorporates sophisticated and adaptive signaling and reporting systems, can automate the correlation and analysis of large amounts of IT and business data, as well as various threat indicators, on an enterprise-wide basis.

Financial services companies’ monitoring systems should work 24/7, with adequate support for efficient incident handling and remediation processes.

Enhancing Resilience through Simulated Testing and Crisis Management Processes

Resilience may be more critical as destructive attack capabilities gain steam. Financial services firms have traditionally planned for resilience against physical attacks and natural disasters; cyber resilience can be treated in much the same way. Financial services companies should consider their overall cyber resilience capabilities across several dimensions:

First, systems and processes can be designed and tested to withstand stresses for extended periods. This can include assessing critical online applications for their level of dependencies on the cyber ecosystem so as to determine vulnerabilities.

Second, financial services firms can implement good playbooks to help triage attacks and rapidly restore operations with minimal service disruption.

Finally, robust crisis management processes can be built with participation from various functions including business, IT, communications, public affairs and other areas within the organization.

India Contacts

Amry Junaideen  
President  
Enterprise Risk Services  
amjunaideen@deloitte.com

Abhay Gupte  
Partner  
National Leader - Governance Risk and Regulatory  
agupte@deloitte.com

A.K. Viswanathan  
Leader - Financial Services and Insurance, Enterprise Risk Services  
akviswanathan@deloitte.com

Shree Parthasarathy  
Partner  
National Leader - Cyber Risk Services  
sparthasarathy@deloitte.com