

# Creating Value Through Security

To manage information security across FT group, a dedicated IT Security Team has been formed who is responsible for managing and maintaining information security. IT Security team ensures that guidelines provided in Risk assessment process to manage Risk are implemented and maintained.

**F**inancial Technologies (India) Limited, the flagship company of the Financial Technologies Group, is among global leaders in offering technology IP (Intellectual Property) and domain expertise to create and trade on next generation financial markets, that are transparent, efficient and liquid, across all asset class including - equities, commodities, currency and bonds.

Financial Technologies product suite includes flagship products like Exchange Technology, back-office and front-office solution for Brokerage houses, and Messaging solutions for various entities involved in financial domain.

Financial Technologies has envisioned to build a brand-centric technology company that leverages strong technological platforms to promote a transaction-intensive and multi-billion dollar business.

The technology IP and domain expertise forms an integral part of business model of Financial Technologies. FTIL has developed a business model which includes software solutions, exchange and ecosystem ventures. This business model has enabled accelerated economic expansion of the ecosystem in which FTIL operates and has made it virtually self-fuelling.

## INFORMATION SECURITY – THE PRESSING PRIORITY

In view of the above protection of Intellectual Property takes utmost importance in FTIL. With the advancement of technology and increased human capital, security is increasingly becoming management's concern. Further, being a listed company, FTIL is bound by the corporate governance requirements at one end and interacts with these bodies for technological developments, at the other. Therefore, compliance is the "Way of Life" at Financial Technologies.

Therefore, the management has institutionalized an Internal Program which is aligned with the corporate objectives, harmonizes with the organization's value system and creates an information security assurance.

FTIL has gone beyond the traditional mould of having an isolated information security function and has taken a step towards achieving the governance in information security.

The information security strategy at FTIL revolves around its six core drivers:

- Strategic Alignment
- Risk Management
- Data Architecture
- Security Models and Standards
- Incident Response & Containment
- Monitoring & Improvements

The CISO alongwith the other IS Steering Committee Members ensures ongoing upkeep of the program with the changing business dynamics.

## SECURITY ORGANIZATION – IT'S NOT A PROJECT; IT'S THE CULTURE

There has been prominent studies that reveal the importance of "Awareness and Culture" in the success of the Information Security Program. The IS Steering Committee has ensured to spread "Information Security AIR – Awareness, Inculcate, Reinstate" all around.....within and outside the organization. This has played a major role in the sustenance of the Information Security Program.

Each and every member of the organization is given the security specific responsibilities alongwith their work objectives. This has helped largely in integrating security organization structure with the business organization. Further, FTIL has extended the security enterprise to its vendors and customers.



**Paras Ajmera,**  
Director Operations , Financial  
Technologies (India) Limited

Vendors and Customers of Financial Technologies are further spontaneously integrated into the security culture during their interactions with the organization.

With the check on the existing threats through audits, the CISO also keeps radar on the emerging risks. For this, Financial Technologies interfaces with the industry experts, SMEs and authorities which form a knowledge pool for the organization.

#### **DATA CENTRIC INITIATIVES – KNOW WHAT YOU OWN**

Information Security Program at FTIL includes risk management, information security policies, procedures, standards, information classification, security organization, and security education. These core components serve as the foundation of a FTIL's security program. As a part of our robust security program, FTIL has built data centric approach in all security initiatives by understanding the criticality of data. At FTIL, data owners and process owners are involved in determining the sensitivity of data based the level of damage that could be caused if the data were disclosed, modified, corrupted or not available. This allows a balanced approach towards protection of data whereby trivial information assets are not overprotected and critical data is not left out.

This forms the basis for information security architecture at FTIL which is based on "Defense-in-Depth" approach. Multi-tier

security controls are in place with state-of-the-art technology that enforces approved policies with least manual interruption. All the users of the FTIL, have a responsibility to protect FTIL data and information from unauthorized generation, access, modification, disclosure, transmission or destruction, and are expected to be familiar with and comply with this policy.

#### **OPERATIONALIZATION OF THE FRAMEWORK – GET THE HOUSE "IN-ORDER"**

FTIL has taken a "Defense-in-depth" approach for operationalization of security strategy. The following diagram depicts the security operationalization at FTIL:

To manage information security across FT group, a dedicated IT Security Team has been formed who is responsible for managing and maintaining information security. IT Security team ensures that guidelines provided in Risk assessment process to manage Risk are implemented and maintained. This is achieved through deployment of

- Industry standard Stateful Inspection Firewall to prevent unauthorized access to/from FT network
- Network Intrusion Prevention System to monitor and prevent any intrusion and attacks
- Network Segregation techniques distributing the network in various zones and logical separation through VLANs
- End point network security by tagging Individual network ports to MAC addresses of equipment
- DLP Solution to prevent data pilferage through use of USB/ portable devices
- Renowned Antivirus software to protect the business

<b>DATA</b>	ACL, Encryption, Database Hardening, End Point Security
<b>APPLICATION</b>	Application Hardening, Role Based Access
<b>HOST</b>	OS Hardening, Patch Management
<b>INTERNAL NETWORK</b>	VLAN, MAC Security, CA Unicenter NMS
<b>PERIMETER</b>	Firewall (Stateful) VPN, Gateway Anti Virus
<b>PHYSICAL SECURITY</b>	Guards, CCTV, Biometric
<b>POLICIES, PROCEDURES &amp; AWARENESS</b>	Management Framework, Training

- environment from malicious codes
  - RD-WEB (Remote desktop web access) To prevent data leakage and any attacks from Internet
  - Web Filtering Solution to ensure internet usage as per FTIL Internet Policy
  - Outbox solution (Email Moderator) to scan and send every mail that goes out of FTIL domain to the cyber world
  - Mail Security Gateway to ensure all incoming mails are scanned for any spam, virus or malware content
  - Remote access through Citrix remote access solution to protect data leakage from remote access
  - Enterprise Policy for all Blackberry devices to prevent data loss through handheld devices.
- This is supported by the implementation of various processes that compliments the technology deployments.
- Some Risk Management Process
  - User access Management Process
  - Password Management Process
  - Change Management Process
  - Incident Management Process
  - Monitoring & Analysis Internal Audit & Assessments
  - Backup & Media handling
  - Information Security Awareness Program
    - Disciplinary Action
    - Physical & Environmental Security

**Aligning technology for enabling the aggressive business vision and coupling security controls with it requires correct foresight and tireless efforts at all levels.**

**Paras Ajmera,**  
Director Operations,  
Financial Technologies  
(India) Limited.

#### **SECURITY INVESTMENTS – IT'S NOT A "BLACK BOX"**

The security Investment culture of the organization revolves around protecting our assets with controls that are effective and reasonable in costs. Where costs exceed the value of the asset other measures such as insurance or acceptance of the risk are adopted.

A process has been laid down that helps the security personnel to select the right products which is what ensures that the investment optimization in security is achieved. This process includes a thorough examination of the products / services, running a round of POC, evaluation of multiple solutions, partners / principal companies, to name a few.

The ROI is calculated based on the costs that we would have incurred without the product versus the

costs and savings made with the product. This is calculated over a three year period as a minimum. This includes man power costs, costs of recovery and qualitative costs such as loss of credibility.

#### **SECURITY IN CUSTOMER OFFERINGS – VALUE CREATION**

Security is very much considered to be a business enabler at FTIL. Security is de-facto at Financial Technologies as its products and services (including SAAS and the cloud) mainly cater to the financial markets. Our products and services enable our clients to conduct their critical trading operations. The entire suite of our software takes care of all the clients' needs and extends from mobile trading solutions to back end software to settlement platforms supporting real-time data. Security is therefore a mandatory feature that gives Financial Technologies an edge over its competition.

Therefore, security becomes utmost important when it comes to designing and providing high transaction density exchange applications. With such domain expertise noted, FTIL has ensured to integrate the following "domain-specific" security features in all solutions:

- AAA – Authentication, Authorization and Auditability in all product suites to ensure confidentiality and integrity of the information
- Contingency Planning for mission-replication features to ensure Zero data loss
- System & Information Integrity – employing suitable encryption techniques over and above authentication mechanism to ensure information integrity
- Interface / integration controls – interfacing with other applications and information exchange based on online authorization
- Data Center Security – Facility that hosts mission-critical infrastructure

Our solutions and services, besides providing performance advantages, also ensure maximum security for our clients. All our solutions and services are built with security in mind and support the standards, such as encryption and dual factor authentication. Security testing forms are mandatory part of the release management and the ready features enable the necessary compliance for clients with regards to governing bodies.

FTIL is empanelled with CERT-IN, CCA and RBI for security audits and testing. This therefore gives FTIL an additional feather in its cap with regard to client confidence.