ENTERSOFT

CASE STUDY

Securing A Non-Banking Financial Company

www.entersoftsecurity.com

THE CLIENT

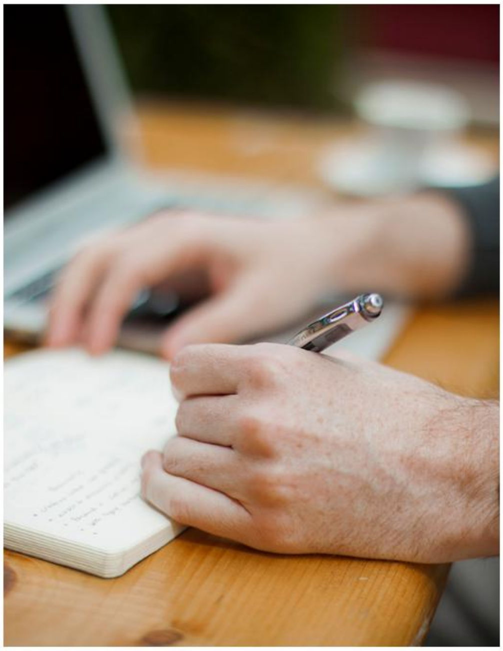
Helping a leading NBFC achieve secure digitization and adherence to RBI security guidelines.

1. A leading NBFC company that provides easy & quick business loans in India. Among the Top 100 FinTechs across the globe and their product stands out in B2B Lending.

2. With over 400 employees across the globe and 50+ tech talent, client is proactive about Cyber security.

3. Client has a 10+ member team that manages operations and security internally. They also have 30+ member developer team.

BACKGROUND



Important for the client to make sure all their products are secure, at the same time achieve required compliances.

Like other NBFCs in India, client has assessed the numerous benefits of digital and transformed themselves into a digital company with heavy focus in technology. But the management is concerned that security can ruin their digital transformation efforts.

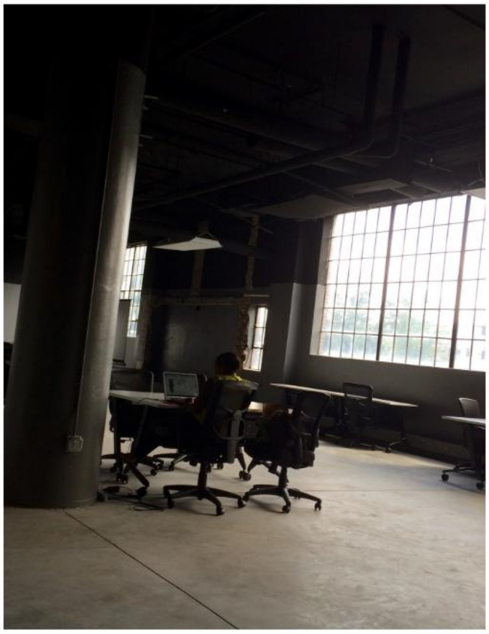
Prior to engaging with Entersoft, Client has earlier engaged with one of the Big four audit firms and burnt its hands in implementing a pragmatic cyber security plan. Management decided to have a sound security strategy and policy in place and should change their approach to security.

The need of the hour is to be proactive, not reactive and they would require a partner who understands Fintech and more hands-on.

While the new threats sound scary, it should not be a deterrent to digitalisation. Countering these cyberthreats is not difficult with the right technology and implementation partner.

Entersoft has earlier helped the client evade a massive ransomware attack.

EVALUATION



Client approached Entersoft to evaluate their Cyber security posture and help them improve it.

1. Entersoft identified the gaps and measured their Cyber security maturity, in addition to evaluating their existing processes and assessing the required compliances.

2. Since the client is an NBFC in India, they also have to adhere to security guidelines issued by RBI in 2017.

3. The management was keen to attain a security certification that would help them in manage their operational security.

ENGAGEMENT

Complexities of the engagement.

All of Client's products are deployed and managed on cloud, with **Microsoft Azure** and **Amazon AWS** as cloud providers. Client had approached one of the big four audit companies in India and were provided with an **IT Security audit report**.

The results were alarming and the suggestions provided by the audit company were extremely **complex** to implement on the cloud. Also, the **cost of security implementation** was an adherence as per the suggestions.

Many key internal applications are managed in house as well. Hence, the need for security brought in many perimeter security tools like **Firewalls, VPNs, Load balancers, Data back ups** and so on. Implementing a **Business Continuity Process** was key for the client for their operations.

Also, managing in-house security operations and cloud security operations is a challenge for the customer.

NBFC security guidelines issued by RBI are relatively new and client had to achieve them with in a year. They were confused between choosing **PCI-DSS and ISO 27001** compliances for their operational security compliance.

ANALYSIS

A comprehensive Gap analysis was performed and the following road map was created for the client.

#1 Setting up Audit committees & defining CISO responsibilities

#2 Gap Analysis

#3 Risk assessments & Penetration tests on entire operations and applications

#4 Policy and Process definitions (For RBI guidelines and ISO 27001)

#5 Process and Policy implementation and monitoring

#6 Vulnerability management program and DevSecOps implementation

#7 Security training and Internal audits

#8 External audits and Certification

#9 Ongoing Security review and audit management

ASSESSMENTS

Phase	Deliverables	Details
1 - Project Assessment	• Gap Analysis Report • Action plan document	Entersoft performed a detailed Gap analysis of the QMS/existing/process documents to check for compliance with ISO 27001 & RBI's Master Direction "Information Technology Framework for the NBFC Sector". Existing application security practices in the organization were also evaluated. A gap analysis report was created and an action plan document covering a year was made for the customer. Additional support was provided to implement the action plan to address gap analysis.
2 - Risk Assessment	Client did not have a risk register and had never had a risk assessment performed. We identified the need to create and draft the following : • Statement of Applicability • Quality Policy • ISMS Policy • Asset Register • Risk Register	A Risk Assessment Methodology was defined & documented as per ISMS. One round of risk assessment was performed and all the risks were identified.

Phase	Deliverables	Details
3 - Process & Policies Definition	• Base-lined ISMS & Processes Definitions. • Vendor Management Process. • Asset Management Process. • Change Management Process. • Disciplinary Process. • Internal Audit Process. • Access Control Process. • Business Continuity Policy. • Capacity Management Process. • Vendor Management Policy. • Access Control Policy. • Antivirus Policy. • Asset Management Policy. • Backup Policy. • Recovery Policy. • Business Continuity and Disaster Recovery Policy. • Incident Management Policy. • Internet Usage Policy. • Malicious Code control policy. • Media Disposal Policy. • Password Management Policy. • Patch Management Policy. • Supplier Security Policy.	The processes for the organization were defined & implemented as per ISO 27001 parameters and RBI's Master Direction "Information Technology Framework for the NBFC Sector". Processes and policies to manage both cloud products and internal operations were balanced.
4. Internal Quality Audit & Management Review	Internal Quality Audit & Management Review Report	Helped the client form an Internal Quality Audit Committee and perform Management Reviews. The committee reports directly to the board of directors.

Phase	Deliverables	Details
5 - IT Security Audit	Security Audit Report	The following security audits were performed : • IT Interface controls assessment • Contract management review • IT SOP review • VAPT of Internal IPs • Network Architecture review • Product security assessments • Application security assessment • Cloud security assessments
6 - IT Policies & structures as per RBI's Master Direction – "Information Technology Framework for the NBFC Sector" - RBI/DNBS/2016-17/53	• Identified a need to hand hold the customer for 1 year and support them with required compliances. • Provided the client with an audited report to submit to regulatory authorities and RBI.	Helped customer in defining and maintaining RBI/DNBS/2016-17/53 - Master Direction DNBS.PPD.No.04/66.15.001/2016-17 compliance requirements.
7 - ISO 27001:2013 certification Audit	• Audit report • Corrective actions	Provided the following to the client: • Lead Auditor. • Auditing support. • The final audit report.
8 - ISO 27001 Certification	ISO 27001 Certificate	Helped the customer achieve ISO 27001 certification.
9 - CISO role	Virtual CISO for a year	Client required a virtual or a full time CISO to manage the security posture.

HIGHLIGHTS OF THE ENGAGEMENT

Audited and Secured by Entersoft.

ISO 27001 certification
achieved.

34 Applications
audited and secured.

80+ cloud instances
reviewed and secured.

450 desktops
audited and secured.

5 internal networks
reviewed and secured.

50+ policies and processes
defined and implemented.

300000 lines of code
reviewed.

OWASP top 10, SANS security standards
achieved for products.

ENTERSOFT

www.entersoftsecurity.com