Analysis of Key Digital Technology Infrastructure and Cyber Security Consideration Factors for Fintech Companies

J A R C Jayalath[a], S. C. Premaratne[b]

[a] *vl.ravinduj@icbtcampus.edu.lk* , [b] *samindap@uom.lk*

[a]*Department of Information Technology, International College of Business & Technology, Sri Lanka*
[b]*Department of Information Technology, University of Moratuwa , Sri Lanka*

Abstract

Fintech companies have disrupted the financial industry by means of the way customers are served with their financial needs with the usage of immerging technologies such as Artificial Intelligence, Robotic Process Automation, Natural Language Processing, Facial Recognition, Data Analytics etc. and the development of the supporting digital technology infrastructure by using the benefit of the enhanced digital literacy of new generation customers by providing a great deal of customer convenience by delivering easily accessible and fast service to customers. In addition to this, when more and more customers are using the digital channels, several customer insights get collected in fintech platforms that can be effectively used for cross-selling and generating customer-centric products and services.
As a result of the digital disruption that happened due to this Fintech initiative and the demand of especially the new generation customers, established financial companies such as banks also followed with Fintech initiatives either with the collaboration of startup Fintech companies or by developing the Fintech initiative internally. As a result of this more and more financial channels have been opened to the public internet providing access to larger-scale customer base via online channels and in the form of open APIs. As a result of these factors digital financial platforms have become highly critical hence Fintech companies had to look at implementing reliable digital infrastructure and when financial platforms were more opened to the public internet, more and more cyber threats to the systems also increased rapidly. Therefore, it had become a high necessity for the Fintech companies and the Banks and Finance companies who provides digital solutions to build a structured Digital Technology Infrastructure considering resilience, performance and security to thrive in the highly competitive Digital Financial landscape.

Keywords: Cyber Security, Digital Technology, Fintech, Banking, Finance, Digital Disruption

1. Introduction

Digital Disruption is one of the key topics in the financial industry today which mainly comes to the picture with the startup Fintech initiatives to provide alternative financial services via digital platforms developed by using emerging technological innovations. The key cutting edge technological developments such us Industry 4.0, Internet of Things (IoT), Artificial Intelligence (AI), Facial Recognitions, Data Analytics, Data Mining, Robotic Process Automation (RPA), Natural Language Processing (NLP) and many more helped fintech

companies to provide attractive user-friendly solutions to the customers with the use of these state of art technological innovation which enhanced the efficiency, fast accessibility from any time and any where which provides higher convenience to the customers. As a result of these convenient services more and more customer especially the young generation were attracted by these innovative fintech products and services to cater their financial demands conveniently and fast. This trend has impacted the traditional business models of the established banks and finance companies based on manual processes. Further, it has slowed down the revenue and market share growth of them. To overcome these challenges, many established banks and financial companies started following fintech initiatives either by entering into partnerships with startup fintech or by developing the fintech capabilities internally. These fintech initiatives developed by the banks resulted in delivering several products and services to the market such as open banking APIs, Digital Wallets, CryptoCurrency which became the supporting factors for the industry to be pushed towards a cashless society. Based on these fintech initiatives, the dependency of these digital platforms on the financial companies' business models has been highly increased. Hence it has become a high necessity to maintain reliable digital technology infrastructure considering the high performance, high availability to achieve fault tolerance, geographical redundancy to achieve disaster recovery, which help businesses to provide uninterrupted service to the customers. In addition to this, financial systems have been more opened to the public internet and to the other external parties which has opened more rooms for the risk of intrusions and unauthorized access to the financial platforms. This type of security breach could lead the organization towards loss of revenue, loss of data, reputation damages, loss of customer trust, malfunctions of critical financial systems, etc. which need to be carefully analysed and implement necessary systems and control to avoid such failures. Therefore, fintech companies must define a comprehensive framework and a procedure to manage Digital Technology Infrastructure and Cyber Security aspects to address the above stated issues by taking the business requirements also in to consideration. This study is mainly focusing on analysing key areas related to effectively manging Digital Infrastructure and Cyber Security aspects for fintech companies to achieve business continuity, customer convenience, protection of customer’s privacy and confidential data, compliance to the industry standard frameworks and regulations, etc to ensure a smooth operation to achieve the defined outcomes of digital initiatives. It is expected to categorize this study in to multiple areas as follows.

In terms of Digital Infrastructure, it is expected to discuss the requirements by focusing on the following areas.

- How to align the technology to cater business demands
- How to ensure business continuity to cater un interrupting business

In terms of Cyber Security, it is expected to discuss the requirements by focusing on the following areas.

- Ensuring of Information Security
- Compliance to the industry standards and regulations with governance

It is necessary to align the above factors in to the organization's technology roadmap with key considerations such as clear top management leadership, delivery timelines at the critical phases of the digital solution delivery, budgeting for the successful execution to achieve the final outcomes.

2. Digital Infrastructure Consideration Factors

As briefly discussed in the Introduction chapter, maintaining a reliable Digital Technology infrastructure with adequate capacity while maintaining a higher uptime helps Fintech deliver effective digital products and services to the customers to achieve the specified business outcomes. These factors can be used selectively based on the type of technology infrastructure used in the organization, such as private cloud, public cloud, or hybrid cloud, based on the requirements. Proper policies and procedures have to be defined covering these aspects in designing, building, and maintaining the digital technology infrastructure to consider these factors effectively.

2.1. Aligning the Digital Technology Infrastructure with Business Requirements

When the digital technology infrastructure is designed, built and maintained one of the most essential aspect to consider is the business requirements where the entire technology life cycle needs to be aligned with the business requirements as end of the day if the business is not catered the final outcome of digital will not be served. When the digital technology infrastructure is aligned to the business there are multiple aspects to be considered. The first area to consider is the compatibility of the digital technology infrastructure to cater to the required business applications. The second area to consider is the adequate capacity of digital technology infrastructure to cater to the business demand, including future business growth.

When digital technology infrastructure compatibility with digital application is concerned, it is necessary to identify the key applications and the technologies that are going to be used on top of the infrastructure and design the infrastructure to facilitate these requirements. The digital technology infrastructure can be mainly categorized in to three pillars known as computing, storage and network resources. Compute is responsible of proving the necessary processing power and the memory for the applications to function. It is important to analyze and identify the required processing power, cache memory, bus speed, etc. when designing the compute depending on the application types. As an example, higher processing power will be required for an application using an advanced AI-based algorithm than a general application. Storage is responsible of

providing the required storing capacity for the data generated by the applications. When it comes to the storage read and write speed is one of the main factors impacting application performance apart from the storage capacity hence it is important to identify the application requirement to have the required input/output operations per second (iops) including the required data capacity with a future forecast. When designing the storage, it is necessary consider above factors to identify the exact storage infrastructure needs to be built such as Fiber Channel based Storage Area Network with Flash or SAS disk arrays depending on the requirement. Then the network component is responsible for the transmission of data end to end. When network infrastructure is designed it is necessary to identify the relevant throughput required by the application with future forecast to supply adequate capacity from the network layer such as Gibic (10 Gbps) fiber network or higher. One of the most important factors in designing, deploying, and maintaining the compute, storage, and network power required to build the digital technology infrastructure is identifying the correct requirement to run the business application considering cost factors. Higher the performance the cost of building such infrastructure also will be higher. Hence, it is necessary to build the infrastructure into multiple layers such as high, medium, and low to manage the cost and provide the resources for the necessary applications from the relevant layer according to their resource requirements, which balance the cost and the performance. As an example, an application which is handling a scheduled job such as sending statements via email might not require high performance resources than an application which is processing AI based algorithm so the former can be given resources via the medium or low performance layer while later can be given resources via the high-performance layer.

2.2. Business Continuity

One of the significant factors to consider when design, build and maintain digital infrastructure is the assurance of business continuity by providing an uninterrupted service to the customers. The key aspects in providing uninterrupted service are ability to withstand against failures in digital infrastructure components by designing them with resilience and consider geographic redundancy to withstand against a major disaster. These two aspects are known as high availability and disaster recovery in digital technology infrastructure design.

As explained in section 2.1 high availability should be considered in compute, storage and network layers considering the business requirements as well. Clustering, redundant nodes, Redundant Array of Independent Disks (RAID), offline backups, network component stacks, network link aggregation, network port binding, software defined networking, virtualization are some of the key technology points that are supporting high availability implementation in multiple modes such as active /active or active/ passive. Regular monitoring

and testing should be in place to ensure the functionality of them to avoid failures.

Disaster Recovery is highly important for the business to continue in major disaster situations like natural disaster or total system failure. The replica of the digital infrastructure should be implemented in different geographic locations to cater to the business. Two major terminologies used in designing, building and maintaining Disaster Recovery System are Recovery Point of Objective (RPO) and Recovery Time of Objective (RTO) which define how fast system will be available from DR site and the data availability when system switch over to the DR site. Factors like real time data replication and Global Server Load Balancing (GSLB) are some of the key factors to achieve lower RPO and RTO which enhance business continuity.

Business continuity should be widely discussed and considered in the top management level with board approved policies and procedures ensuring a proper Business Continuity Plan (BCP). There should be a separate unit in the organization responsible in executing the BCP for effective management. Defined RPO and RTO for each system, emergency call tree, conduct regular drills executed to ensure DR functionalities are some of the key functions. The process should be regularly reviewed and updated with solutions to the identified loop holes.

3. Cyber Security Consideration Factors

As explained in the introduction, consideration of cyber security is very important due to the financial systems are now more exposed to the external environments due to fintech initiatives. Security aspects need to be considered in the information security side and compliance aspects with the governance to ensure proper polices and procedures are in place with continuous improvement. All the policies and procedures should be approved in the board level and continuous revision is required based on the changes in the threat landscape.

3.1. Information Security

Information security implementation, operation, incident response, etc. are some of the key components ensuring the security of digital technology infrastructure. Key cyber security technological factors such as maintaining strict perimeter and internal level security through firewalling, Intrusion Prevision and Intrusion Detection Solutions (IPS/IDS), Web Application Firewall (WAF), log collection and correlation with Security Incident and Event Management (SIEM), Digital Data Classification, Data Leakage Prevention (DLP), end user identity management, Network Access Control (NAC), Security Operation Centre (SOC), Privilege Access Management (PAM), two factor authentication , etc. support Fintech companies to manage their information security landscape effectively. It is important to maintain network level segregation, detection and monitoring of security incidents , control of access to the financial systems by provisioning only required

access for the business needs, control and monitoring of privilege user access to the systems , control of network access to the Fintech network infrastructure, threat intelligence, frequent vulnerability assessments , penetration testing, application code review, digital technology architecture review, ensure confidential customer data and other internal data is appropriately classified and used reasonably within the organization based on business requirements with proper controls in place to prevent loss of such data which would result the company in facing business losses, legal issues and reputation damages, data encryption methodologies at data in rest and data in transit, endpoint malware protection and endpoint encryption, comprehensive patch update mechanism, etc. are some of the key requirements in maintaining the information security in digital technology architecture. Once again there is a cost factor to consider when implementing such solutions hence it is not practical for the Fintech companies to implement all these technologies at day one hence it is important for them to formulate a cyber security strategy in alignment with the technology and business strategy with a clear understanding of the potential risks posed and align the required solutions to the technology road map.

3.2. Information Security Compliance and Governance

Information Security Compliance and Governance play a major role in controlling the information security landscape by ensuring the above-mentioned technologies deliver the expected outcomes with frequent review and enforcement of necessary polices and procedures for the relevant stakeholders to follow to achieve them. Information security awareness Chief Information Security Officer (CISO) role is a very important role representing the top management commitment in developing, managing and operationalizing in information security strategy. Board approved polices are procedures should be in place for acceptable usage of information systems, document control procedure, access control procedure, data classification, physical and environmental security procedure, change management procedure, vulnerability assessment and management, backup and recovery, information security incident management, log management, availability and capacity management, malware protection, password policy, patch update process, etc. to ensure proper management of information security aspects are taking place. In addition to these, some other important factors to consider are establishing a comprehensive risk management framework to manage technology risks in terms of risk identification, risk assessment, risk treatment, risk monitoring, risk review, and risk reporting. Board Information Risk Management Committee (BIRMC), Operational Risk Management Committee (ORMC), Information Security Steering Committee (ISSC), Information Technology Steering Committee (ITSC), etc are some of the key bodies within the organization to be appointed in regulating these information security requirements.

In addition to these, compliance requirements such as IS0 27001:2013, PCI-DSS, GDPR, etc. based on industry standards, regulatory requirements and business requirements will also be helpful and required in executing and governing a proper information security frame work for Fintech companies which ensures continuity and the success of their business outcomes.

Conclusion

Fintech companies often leverage on the Digital Technology Infrastructure to run their business applications hence it is a key requirement of them to formulate Technology and Cyber Security strategy in alignment with the business strategy and to understand the potential risks posed by technology clearly. Based on the above facts discussed in terms of analyzing of Key Digital Technology Infrastructure and Cyber Security Consideration Factors for Fintech Companies, it is high important for them to identify the requirements in aligning the digital technology infrastructure with key business requirements, ensuring business continuity by providing an un interrupted service, information security technology frame work with governance and compliance which facilitates business applications which use emerging technologies to function smoothly, error freely with adequate performance ensuring the customer satisfaction and the expected business results are delivered. These factors should be appropriately regularized in top management level with proper review process in place to ensure the requirements are fulfilled with expected business outcomes ensuring the performance of digital platforms and the security of confidential data with the development of required people, process and technology to cater the requirements. There can be services provided by third parties including cloud service providers, system integrators, etc., while deploying technology providing improved customer service and such engagement with third parties needs to be carefully evaluated in view of the potential cyber risks they pose to the Fintech and hence it is necessary for them to articulate strategy including the limits to mitigate risk tolerance for such activities. Technology and Cyber Security strategy shall be supported by top management approved policies including a well written information security policy, sound and robust risk management framework with appropriate management oversight, adequate technical resources, institutional arrangement for building awareness on the subject and an independent audit.

References

Badr Machkour, Ahmed Abriane, 2020. Industry 4.0 and its Implications for the Financial Sector, Procedia Computer Science. p 496-502.

Bernardo Nicoletti, 2017. The Future of FinTech,Integrating Finance and Technology in Financial Services.

Camillo, Mark, 2017. Cybersecurity: Risks and management of risks for global banks and financial institutions,Journal of Risk Management in Financial Institutions, p. 196-200.

Carmen Cuesta, Macarena Ruesta, David Tuesta, Pablo Urbiola, 2015. The digital transformation of the banking industry, Digital Economy Watch.

Derek Mohammed, 2015. Cybersecurity Compliance in the Financial Sector, Journal of Internet Banking and Commerce.

E Wheeler, 2011. Security risk management: Building an information security risk management program from the Ground Up.

Henri Arslanian, Fabrice Fischer, 2019. The Future of Finance: The Impact of FinTech, AI, and Crypto on Financial Services.

Ian Pollari,2016. The rise of Fintech opportunities and challenges, The Journal of the Securities Institute of Australia, p. 15-21.

Klaus Schmidt,2006. High Availability and Disaster Recovery: Concepts, Design, Implementation.

Mercurius Broto Legowo, Steph Subanidja, Fangky Antoneus Sorongan, 2020. FinTech and Bank: Past, Present, and Future, Jurnal Teknik Komputer AMIK BSI, p. 1-6.

Paul Schulte, Gavin Liu, 2017. FinTech Is Merging with IoT and AI to Challenge Banks: How Entrenched Interests Can Prepare, The Journal of Alternative Investments Winter 2018, p 41-57.

Robert Grandl, Yizheng Chen, Junaid Khali, Suli Yang, Ashok Anand, Theophilus Benson, Aditya Akella, 2013.Harmony: coordinating network, compute, and storage in software-defined clouds.

Robert L. Grossman, Yunhong GU, Michael Sabala, Wanzhi Zhang,2009. Compute and storage clouds using wide area high performance networks, Future Generation Computer Systems,p.179-183.

Simon Pamplin, 2021. SD-WAN revolutionises IoT and edge security, Network Security, p. 14-15.

Zahoor Ahmed Soomro, Mahmood Hussain Shah, Javed Ahmed, 2016. Information security management needs more holistic approach: A literature review, International Journal of Information Management, p. 215-225.