<u>**Final Report**</u>

RISE OF FINTECH AND ITS CHALLENGES: A STUDY ON CYBER SECURITY THREATS TO FINTECH INDUSTRY

Submitted in the partial fulfilment for the award of degree in

Master of Business Administration

AT

INDIAN INSTITUTE OF FOREIGN TRADE, DELHI

Under the esteemed guidance of

DR. JITENDRA KUMAR VERMA

PREPARED BY

Pranavi Gosha

31A

MBA IB 20-22

ACKNOWLEDGEMENT

I, **Pranavi Gosha,** have put all my efforts in the completion of the project titled,
"Rise of fintech and its challenges: A study on cyber security threats to fintech industry".

It would not have been possible without the great help of my fellow batchmates and my college, **IIFT Delhi**, which provided me with useful resources for the fruitful completion of the project. I would like to take this as an opportunity to thank all of them.

I am, from the bottom of my heart, thankful to **Dr. Jitendra Kumar Verma,** for his constant guidance and help at every step of the project. Sir made this project journey a very great learning experience for me personally. Sir made himself available to us at any point of time, to clarify our doubts and help us in moving forward and supported us and guided

I would also "like to express my gratitude" towards my **batch mates**, **friends** and **parents** who helped me and encouraged me at every step of the project duration.

INDIAN INSTITUTE OF FOREIGN TRADE

MBA IB: 2020-22
RESEARCH PROJECT

DECLARATION

This is to certify that **Pranavi Gosha** Roll Number 31A student of MBA (IB) batch of 2020-22 Indian Institute of Foreign Trade, New Delhi have submitted this research project "**Rise of fintech and its challenges: A study on cyber security threats to fintech industry**" to IIFT in partial fulfilments of requirements for MBA IB degree. This is original work. It is neither copied (partially/fully) from any other scholastic work nor it is submitted to any other institution for any degree or diploma.

PRANAVI GOSHA
ROLL NO- 31A
MBA(IB) :2020-2022
IIFT Delhi

PROJECT GUIDE CERTIFICATION

This is to inform that **Pranavi Gosha** Roll Number 31A student of MBA (IB) batch of 2020-22 Indian Institute of Foreign Trade, New Delhi has completed this Research work as her final dissertation project for domain **IT** under my guidance. The topic of research is "**Rise of fintech and its challenges: A study on cyber security threats to fintech industry".** She has completed all the requirements of the successful completion of the project and her performance has been satisfactory

DR. JITENDRA KUMAR VERMA

Date:

Contents

List of Tables

Abstract

In current days for any organization to grow and sustain, it is highly dependent on data. Data plays a vital role in determining a firm's strategies and results. With huge data comes huge threat to it. Especially due to rising disruptive technologies, there is a trend in increase of cyber-attacks. This rising trend is very significant in financial industry especially in fintech space. With rapid growth of economies of world, fintech industry is changing the way a bank works and making them switch to digitization to sustain and dominate current markets. This report provides a detailed analysis about financial technology industry, current challenges the industry is facing, understanding of relevance of cybersecurity to fintech firms by understanding the concept of threat intelligence and advantages it can bring to establish secure cybersecurity. This report also provides analysis of various cybersecurity threats, fintech firms are exposed to and understand them. This research report identifies the factors contributing to implementing cybersecurity and aims to determine their level of significance towards successful establishment of cybersecurity in fintech firms. Using Interpretive Structural Modelling (ISM) model, significantly contributing factors to implement an efficient cybersecurity system especially in fintech firms are identified. Based on such findings, consequent measures can be taken to setup a robust cybersecurity system that is resistant to attacks especially due to disruptive technologies. This report also tests the association between device getting diagnosed with malware and enabled with safety modes like Firewall, Secure boot mode and Admin approval mode using Chi-square statistic on data from past trends.

Introduction to Fintech:

Financial Technology widely known as Fintech refers to new financial industry procedures, applications, business models, or products. It widely includes five essential areas, including banking industry, lending and insurance industries, e-commerce, and management of personal finance.

- Financing, payments, cross-product assistance, investments, financial information, and advising on financial decisions are all processes in the insurance industry.
- Banking is used for all forms of payments in our daily transactions. Private, retail, and corporate banking transactions are all included.
- E-commerce includes business-to-customer(B2C), customer-to-customer(C2C) and business-to-business(B2B) activities.
- Lending services including peer-to peer lending are provided by financial institutions and banks.
- Personal finance management involves assets, investment details, personal income, and expenses.

FinTech began as a back-end application in the institutions of finance and trade, but it has now expanded to include literacy of finance, education, investment, cryptocurrency, and retail banking. The internet and mobile technologies are responsible for its tremendous rise as a combination of technological breakthroughs in business and personal finance.

The following elements have spurred FinTech innovation:

- Innovation in Fintech has been boosted rapidly due to developments in emerging technologies like artificial intelligence and cybersecurity.
- As a result of the devastation created by the financial crisis happened in 2008, investors are flocking to FinTech.
- Fluctuations in economies of Europe and United Kingdom have hampered startup investment.

According to the security research report from 2017 on fintech, global cybercrime damages would climb by USD 3 trillion by the end of 2021, reaching 6 trillion USD, rising from 3 trillion USD in 2015. Financial institutions have become a prominent target for cyber-attacks since their incorporation into the Internet. 60 percent of financial organizations, according to the same survey, use services like cloud, the majority of which are private.

Fintech refers to technological developments that allow for the creation of novel banking systems and the more efficient delivery of financial products to provide better value to clients. As a result of economic globalization, there is a growing need for various and complicated financial services. Fintech addresses the diversity and complexity of consumer services, banking, and financial back-end activities, and delivers a wide range of advantages to the economy. Fintech can help global banks and financial services companies enhance efficiency, reduce operating costs, and provide a larger choice of goods and services.(Arashhhabibiilashkari, n.d.)

Challenges in Fintech:

Consumers have benefited from collaborations between conventional financial institutions and modern enterprises, which have helped them receive better goods at lower costs and enhanced access to current products and services—seamless data exchange is at the heart of such partnerships. In order to prevent data from being misused or exploited in the grey market, organizations will need to impose stricter methods for obtaining customer consent for data sharing and reuse, as well as develop technology and processes for life cycle management of data. Furthermore, the problem of determining data ownership must be solved through a mix of technical and legal approaches. Enforcing processes that securely dispose of client data whenever he or she de-subscribes from fintech services is one approach for enterprises to overcome the possible threat of lawsuit (over data leaks or abuse).

Digital identity management of individuals and businesses is a big difficulty for fintech firms as they strive to give customers with a seamless omnichannel experience by providing a variety of payment services, wealth management, and banking. Devices equipped with biometric sensors (for example fingerprint scanners) are increasingly being utilized to provide authorization and authentication services. The usage of biometrics, one-time passwords (OTPs), and code-generating applications (for example Google Authenticator) on mobile phones as authentication devices has decreased reliance on traditional authentication techniques such as passwords and PINs. While digital identities have gotten safer on one level, given their pervasiveness in the growing finance sector, copying these identities might result in increased hazards.

Interfacing systems via APIs (Application Programming Interfaces) that connect with numerous corporate programs has enabled smooth data sharing, but it has also opened opportunities for malware to spread. With the rising integration of technologies in the financial industry, cross-platform malware infection is a growing issue. It is conceivable to construct malware that may infect and spread from one platform to another, as real evidence viruses have shown in the past. Combating such a danger necessitates not just the use of cutting-edge technology, but also a rethinking of traditional security structures.

Adopting insecure coding practices to develop fintech applications especially during its start-up phase may bring serious threat as it would be easier to impact the foundation of the applications and cause serious data breach by malware and other frauds.(*Cybercrime and Cybersecurity: FinTech's Greatest Challenges 1*, n.d.)

Cybersecurity and its relevance in Fintech:

With the proliferation of digital wallet techniques, denial of service attacks, credit card fraud, extortion and financial transactions and other cyber risks in the industry of finance became more common. These cyber-attacks have the potential to put the financial system at danger. Critical economic infrastructures have been hit by well-known cyber-attacks in the industry of banking and finance till date. These assaults can harm technology and compromise key company data, causing services to be disrupted.

Breaches in data, malware, service denial, phishing and cyber fraud are just some of the cyber risks that FinTech has seen. Distributed denial of service (DDoS) and breaches of data are common cyber security attacks identified in the chronology of threats in fintech industry.

Banks and financial companies from many parts of the world have been victims to cyber-attacks. Hacking prominent bitcoin (US) twitter account, GoldenSpy virus in tax software (China), Scotiabank data breach (Canada), DDoS attacks (Europe), dForce cryptocurrency (China), ransomware attacks (US) and DDoS extortion are just a few recent cyber threat initiatives (Australia).

Unauthorized persons or groups who undertake cyber-attacks on any company are known as threat actors. Although the purported individuals are the same for all organizations, financial institutions have a distinct group of attackers. Based on the past trends of cyber-attacks against the industry of finance, few of the most prominent threat actors have been identified as Malicious Insiders, Hactivists, Cyber criminals, Cyber terrorists and script kiddies

Threat Intelligence:

- Technical information: Gathered through the use of technology and tools is referred to as tactical information. Compromise indicators like as IP addresses, file names, and hashes are included in tactical data. This information aids in the identification of threat actors.
- Operational Information: Operational data identifies the adversary's tools, techniques, and procedures in order to gain a better understanding of it. It also assists in determining the motivations for a cyberattack.
- Strategic Information: It creates a high-level organizational plan by mapping the risks linked with cyber threats. The strategy defines the organization's risks and plans to avoid, accept, prevent, identify, or deny each one.

Advantages of Threat Intelligence:

- Improvement in Management of Risk: Management of risk is now a part of the process of planning for most businesses. It allows individuals to recognize and anticipate potential dangers in the future, as well as how to mitigate such dangers.
- Better judgments: Being aware of the dangers aids in making more informed decisions. Institutions can avoid cybersecurity threats and invasions this way.
- Posture of proactive cybersecurity: Threat intelligence enables firms to take proactive cybersecurity measures, such as deploying threat detection using advanced techniques and prevention solutions which learns from historical and current data to prepare enterprises for potential threats.

- Improved threat detection: Gathering meaningful threat information ahead of time is tremendously helpful in detecting attacks before they can take advantage of vulnerabilities and create significant loss.
- Know your adversary: It gathers data on operations that indicates attackers' intentions for launching assaults. The defense can alter his strategy and protect critical assets by understanding the adversary and his maneuvers in a war. Same holds true for cybersecurity warfare.

Threat Modeling Methodology for Fintech:

STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege), Trike (risk-centric approach), VAST (Visual Agile and Simple Threat), PASTA (Process for Attack simulation and Threat Analysis) is popularly used threat modeling methodologies in fintech companies.

FinTech has progressed significantly recently, and this success growth can be linked to the advancement of technology. However, it is impossible to ignore the reality that these cutting-edge technologies also raise the risk of exposing a number of vulnerabilities that can be exploited at no additional expense. URL redirection, crafted URL redirection, remote code execution, information disclosure, DLL hijacking, Ransomware, Command injection etc. are some of the general weaknesses in FinTech technologies, platforms, frameworks, and associated solutions

Specific Fintech vulnerabilities:

- Technology Vulnerabilities: Outdated security controls, susceptible to smartphone application, websites
- Human Vulnerabilities: Password handling habits, Cyber awareness, handling habits of computer
- Vulnerabilities in Transactions: Transactions that are based on cloud, exchanges related to cryptocurrency and Compliance

Strategies to handle fintech cyber security vulnerabilities:

- Identifying Assets crucial to business that are exposed to cyber threats
- Aligning proper communication between business and its IT strategies
- Identifying inherent risks to business or fintech industry
- Monitor risk tolerance level and setup a program for monitoring continuously

(Arashhhabibiilashkari, n.d.)

Research Objectives

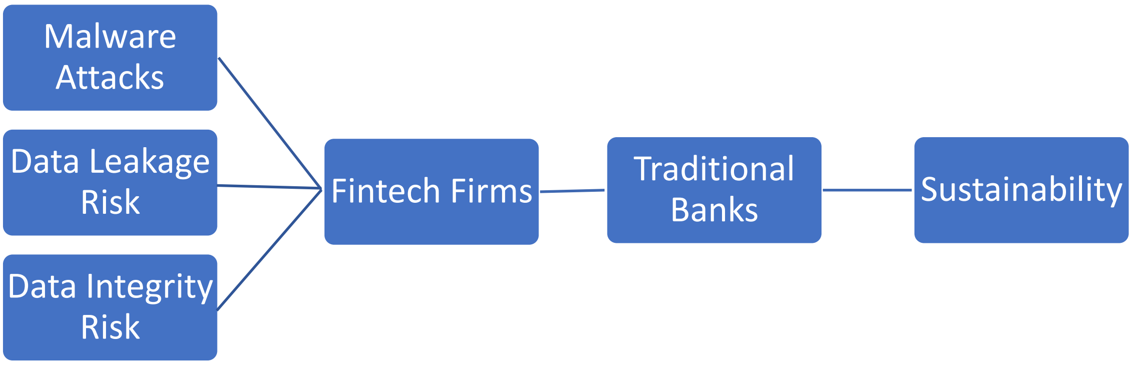
Through this project I aim to study about financial technology industry and its services, detailed study on cyber security and its relevance to fintech products and services

The objectives of the project would be

- To study about financial technology industry and applications that are exposed to cybersecurity vulnerabilities
- Study the challenges for cybersecurity for fintech applications
- Understand the impact of cybersecurity threats for banking and fintech industries.
- To identify potential cybersecurity risks and suggest preventive measures
- Study various threat modelling methodologies for fintech
- Study the risk that fintech brings to the traditional banks on collaborations and by adopting innovating technologies to drive and meet the customer demand.
- To gather interdependent factors contributing to successful implementation of robust cybersecurity in fintech firms and adopt econometric model to understand their significance for the same
- To also determine how likely a device is exposed to malware attacks when firewall, secure boot mode and administrator approval mode are enabled in devices through statistical study on SPSS

Review of Literature

- **NAJAF, Khakan, SCHINCKUS, Christophe, MOSTAFIZ, Md Imtiaz and NAJAF, Rabia** in their paper on **Conceptualising cybersecurity risk of fintech firms and banks sustainability** has identified that traditional banks have become more exposed to cybersecurity risk after collaborating with fintech firms due to risk of data leakage, risk of data integrity and malware risk and provides theoretical evidence for it.

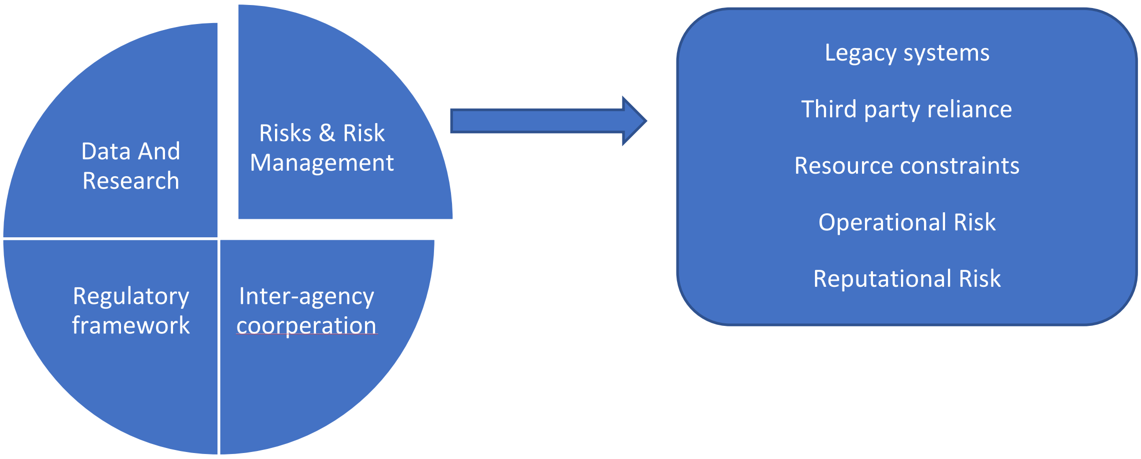


This paper implies the revision of fintech sandbox system by regulatory authorities based on its findings that all fintech and bank integrated firms face the risk of cybersecurity breach. Cyber-attacks are reported immediately after the bank-fintech collaboration. One of the main reasons for such incidents to happen might be because of lack of compatibility of fintech firms and size of operations by banks and other financial institutions are beyond the capacity to handle by fintech organizations.(Imtiaz, n.d.)

- **Vishakha Bhattacharjee** in her research paper on **Predicting Infection of Organization Endpoints by Cybersecurity Threats using Ensemble Machine Learning Techniques** discussed about the machine learning techniques like multiple imputation for missing data analysis and imputation, ensemble learning algorithm og Bagging and Boosting to predict the type of devices that are susceptible to ransomware, malware, and other similar attacks.
  50,000 row data with a mixture of numerical and categorical data for this study was collected from Microsoft Malware Classification Challenge 2015.
  This study proved the hypothesis that by proper knowledge of the hardware and software specifications in an organization, there is a possibility of prediction of the endpoint that is likely to be attacked by malware and also get impacted by other cyber security threats.(*Predicting Infection of Organization Endpoints by Cybersecurity Threats Using Ensemble Machine Learning Techniques*, n.d.)
- **Venkatesh Jaganathan, Priyesh Cherurveettil, and Premapriya Muthu Sivashanmugam** in their research paper **Using a Prediction Model to Manage Cyber Security Threats** has discussed the use of CVSS (Common Vulnerability Scoring System) framework for predicting the occurrence of cyber-attacks quantitatively.
  Regression equation:
  Dependent factor Y: CVSS Score(overall)

Independent factor X1: Vulnerabilities in total detected by dynamic and static target application's vulnerability detection technologies
Independent factor X2: Network traffic input average detected by the application during the week in which attack took place
Null Hypothesis: X1 and X2 has no impact on Y
Predicted CVSS Score = −0.2893 + (0.07174 ∗ Number of vulnerabilities on the IT application reported by tools) + (0.0025 ∗ Proposed input network traffic average for the application for a week(kbps)).
From the result it was proved that CVSS score (overall) gets impacted by the network vulnerabilities and network traffic vulnerabilities. This model helped in prioritizing the vulnerabilities that need to be tackled based on severity to technical analyst of the company. It also helps technical analysts in planning preventing actions to cyber security vulnerabilities.
This paper also states that predictive models should be continuously run and monitored and do not make it one-time activity. (Jaganathan et al., 2015)

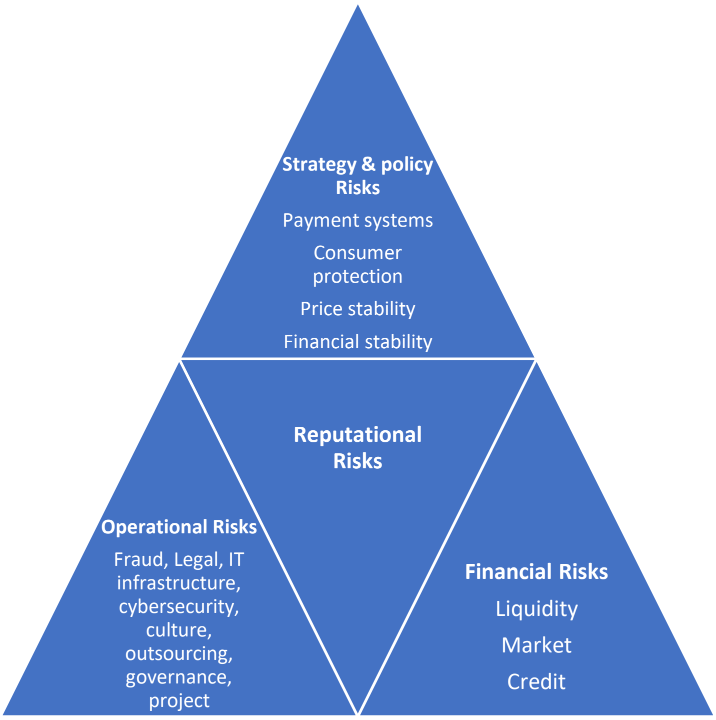
- **IMF Report on Central Bank Risk Management, Fintech and Cyber security by Ashraf Khan and Majid Malaika:**
  This report presents an analysis with central banks of Singapore, Canada and Korea. It states that legacy systems of traditional banks along with their slower, outdated with less agility contributes to the main factor of increasing the risk profile of the bank when collaborated with fintech firms. It also highlighted the fact that there is an increase in dependence on third party systems in banking sector which makes this sector more attractive to cyber-security attacks. Operating a sandbox related to fintech possess a risk to central bank thereby emerging the need for continuous monitoring for reputational risks



This report also discusses a detail overview of risks faced by central banks such as

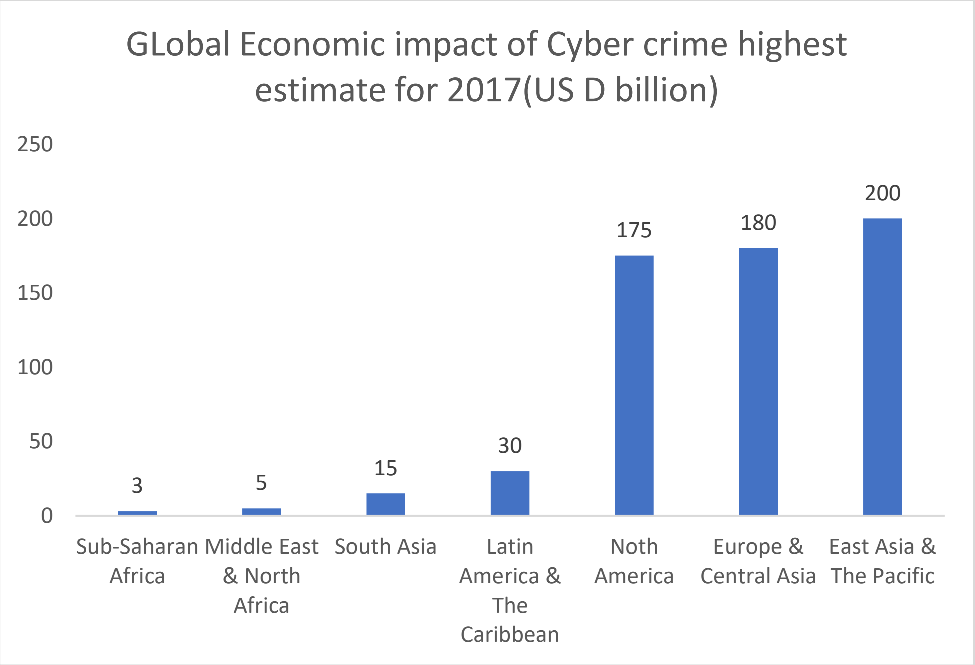
- Strategic and Policy Risk: This risk arises mainly because of Central Bank's strategies and regulatory policies and loopholes in it. Robust strategy and policies can help in reducing this risk.
- Operational Risk: This risk arises from a wide range of categories like governance, cybersecurity, outsourcing, IT infrastructure and other processes.

- Reputational Risk: This arises from materializing one or more risks



(Khan & Malaika, 2021)

- **Fintech Cyber Security – An ASEAN Outlook 2021 by Paypal** states that with rise in pandemic there is rise in cybercrime with social media scams and phishing attacks. Cybercrime is predicted to cost the world economy some USD 608 billion each year, or roughly 1% of global GDP. The Asia-Pacific area alone accounts for over a third of that (32.9 percent). Cyberattacks may cost Southeast Asia's top 1,000 corporations up to USD 750 billion in market value.



This paper also identifies 6 major threats for cybersecurity for which an increasing trend has been identified in individuals and businesses for ASEAN region. These threats are mentioned below:

  - **Phishing**: It is a cyberthreat in which hostile actors send users fake communications in order to trick them into divulging sensitive personal information. Email has become the most popular method of phishing attack distribution. In the region, phishing assaults are becoming more complex and involve advanced social engineering tactics. According to Kaspersky's 2019 phishing report, 17% phishing victims in Philippines, 16% phishing victims in Malaysia, and 14% phishing victims in Indonesia. These countries have the largest number of scam targets in the Southeast area.
  - **Ransomware**: Ransomware is a sort of virus that infects a system and encrypts particular data, preventing the user from viewing them unless payment of ransom is done. Ransomware attacks have apparently hit a number of big businesses across the world. Cerber, a more advanced ransomware technique, has surpassed the number of ransomwares found in the ASEAN area.
  - **Botnet**: Botnets are cybercriminal-controlled networks of hacked computers and devices that may be used to attack financial firms and their consumers. Andromeda and Conficker is one of the most well-known botnet threats in the ASEAN area.
  - **Crptojacking**: A new threat has emerged: the unauthorized use of a victim's computer to covertly mine bitcoin. As per Interpol, hijacked routers in Southeast Asia are responsible for 18% of all cryptojacking infections worldwide. Cryptojacking is a rising issue that puts both organizations and individual consumers at risk. It is driven by bitcoin rewards.
  - **Malware**: Malware is any harmful piece of software that is disguised as genuine and causes damage to the user once deployed on the user's computing device. Malware is always changing. Emotet, for example, has shifted its goal from stealing banking information to distributing other malware. Other financial malware has been discovered targeting the ASEAN area, such as Xloader and LokiBot.
  - **Web and Mobile Application Attack**: Cybercriminals might use configuration flaws or vulnerabilities in online and mobile applications to steal data and carry out other illicit operations. The range of vulnerabilities that must be controlled grows as firms utilize more diverse technology stacks. As a result, online and mobile application assaults are becoming more prevalent as the digital revolution of the area and the world unfolds.(*Executive Summary Introduction*, n.d.)

- **Cybersecurity and Fintech At Crossroads By Vimal Mani, CISA, CISM, Six Sigma Black Belt** suggests various solutions and proactive measure for addressing risks like Third party Security risks, Malware Risks, Data Leakage, Data Integrity Risks, Cloud environment Security Risks, Application Security Risk, Digital Identity Risk that are emerging in fintech space.

  The following are some suggestions for protecting a company from the risk of using fintech:

  - Avoid utilizing public clouds since they are prone to data leaking.

- Refresh the IT infrastructure and fundamental banking systems that have been in place for a long time.
- Improve the fintech venture's cybersecurity posture by utilizing machine learning.
- Protect your digital identity by implementing digital identity theft protection solutions.
- Put in place well-defined third-party security controls.
- Examine the acquisition of new technological solutions from a security standpoint.
- Access control techniques should be strengthened.
- Implement data privacy policies that are well-defined.
- Consider using security orchestration technologies like as Security Operations and Analytics Platform Architecture (SOAPA), Security Orchestration and Automated Response (SOAR), and User and Entity Behavior Analytics (UEBA), which aid in proactive incident response.

(*Cybersecurity-and-Fintech-at-a-Crossroads_joa_Eng_0219*, n.d.)

Research Methodology:

Understanding the industry of fintech and cybersecurity and its relevance through primary and secondary research.

Primary Research:

- Gather insights from industry professionals on financial technology and factors contributing for cybersecurity in their firms. This data will help me to develop Interpretive Structural Modelling (ISM) to determine their significance in contributing towards robust system of cybersecurity and make it resistant to various threats.

Secondary Research:

- Study various research papers published and available online to understand the various aspects of cybersecurity risk.
- Study research articles, technology blogs to understand the root cause of cybersecurity threat.
- Study literature and books written on cybersecurity and fintech industry to understand various threat modelling methodologies to predict cybersecurity threats and suggest measures to prevent and control them.
- Study statistical approaches to identify the endpoints that are likely to be attacked by cybersecurity threats.
- Study case studies on incidents of cybersecurity breaches and measures taken to tackle them.

This will provide a detailed understanding on extent of cyber security threats and damage it causes to financial firms. This also helps to understand various predictive techniques to identify the threats and suggest measures to prevent them.

Study 1: Identification of key drivers for cybersecurity implementation in financial technology firms:

Interviews were conducted for 10 employees working in fintech firms about the factors that influence the establishment of cybersecurity in fintech firms. Below mentioned factors were identified as key drivers for successful implementation of cybersecurity in fintech firms.

1. **Feasibility:** Extent of resilience to cyberattacks for a fintech organization depends upon feasibility of establishing a robust and anti-cyberattack system. Costs the firm is incurring and its ability to meet them determines the quality of infrastructure and employee skills to protect the firm from various threats. Firm should also check feasibility of outsourcing and licensing costs of cybersecurity software and systems.
2. **Awareness:** Every person working in any organization especially in fintech firm needs to be fully aware of cybersecurity threats he/she is exposed to. Employees should be aware of company policies such as encrypting email attachments, not posting company's confidential data on public sites, not responding to phishing e-mails, not sharing their passwords with anyone including their fellow colleagues, Monitoring the grant of access to systems based on various protocols etc.… to protect the firm from potential cyberattacks.
3. **Expertise:** Employee's skill on handling security incidents and in place infrastructure to support and facilitate cybersecurity for protecting organization from various cyber threats plays a vital role in any financial technology firm. This gives the fintech firms a robust shield against cyberattacks when they build and adopt different technologies to meet market demand effectively. However continuous monitoring needs to be done to ensure infrastructure is functioning effectively and report any discrepancies immediately to concerned authorities to avoid further damage.
4. **Stricter industry and company policies:** Policies such as encryption of emails, restrictions to employees on leakage of confidential data, blocking access to social media and other sites on company systems help in making cybersecurity robust to various threats. As data breaches and cyberattacks cost a lot to the firm, establishing robust security policies, and effectively implementing them will help the firm to reduce its costs as well.
5. **Internet security policies:** As Cybersecurity includes extensive range of governance, technical and organizational issues, internet policies guide the firms to protect networked systems against the threat which could be either by accident or deliberate.
6. **Employee training:** By facilitating training of employees as part of their on-boarding process itself on cybersecurity and its threats, make the organization resistant to threats to some extent. For example, employees will be able to identify phishing mails and not fall for such threats jeopardizing the confidential data of the firm.
7. **Increasing competition in industry:** As barriers to entry to fintech industry are falling due to disruptive technologies, there are many emerging fintech firms leading to a highly competitive environment. As new technologies are being adopted rapidly, chance of cybersecurity threats is increasing. Firms that do not posses' full knowledge of new technologies are exposed to cybersecurity threats as they have no cybersecurity implementation to counter them.

However, above mentioned factors are interdependent on each other and has different level of importance in determining cybersecurity of fintech firms. Interpretive Structural Modelling

(ISM) enabled model is used below to determine the primary and key drivers among these factors to gauge their importance comparatively for establishing cybersecurity in financial technology firms.

Determining significance of drivers for Cybersecurity implementation in financial technology firms through Interpretive Structural Modeling (ISM) enabled mapping

John N. Warfield (1974) presented Interpretive Structural Modelling (ISM), a computer-based technique for assisting importing organizations in developing visualizations using graphs and charts of complex systems in order to map the ladder of decision logically based on the discovered decision factors matrix. Interpretive Structural Modelling (ISM) is a well-competent tool for determining the significance of important drivers for a business problem, which describes an issue or a problem, or the molding of a decision, based on relational mathematical models. ISM Modelling is an efficient research methodology to comprehend the intrinsic intricacies of any complicated topic, such as what are the primary drivers determining the factors affecting cybersecurity implementation and facilitation in fintech firms, based on expert comments, and officially evaluated by ISM. By adding in the input of Industry Professionals in fintech organizations, ISM modelling allows us to examine those complex difficulties. ISM Modelling aids in the establishment of direct and indirect linkages between the components, allowing the situation to be described much more accurately than if the individual factors were considered separately. As a result, ISM gains insight into how people perceive these interactions collectively. ISM was discovered to offer users a systematic and thorough way for incorporating group judgments into the building of "first-cut" structural models.

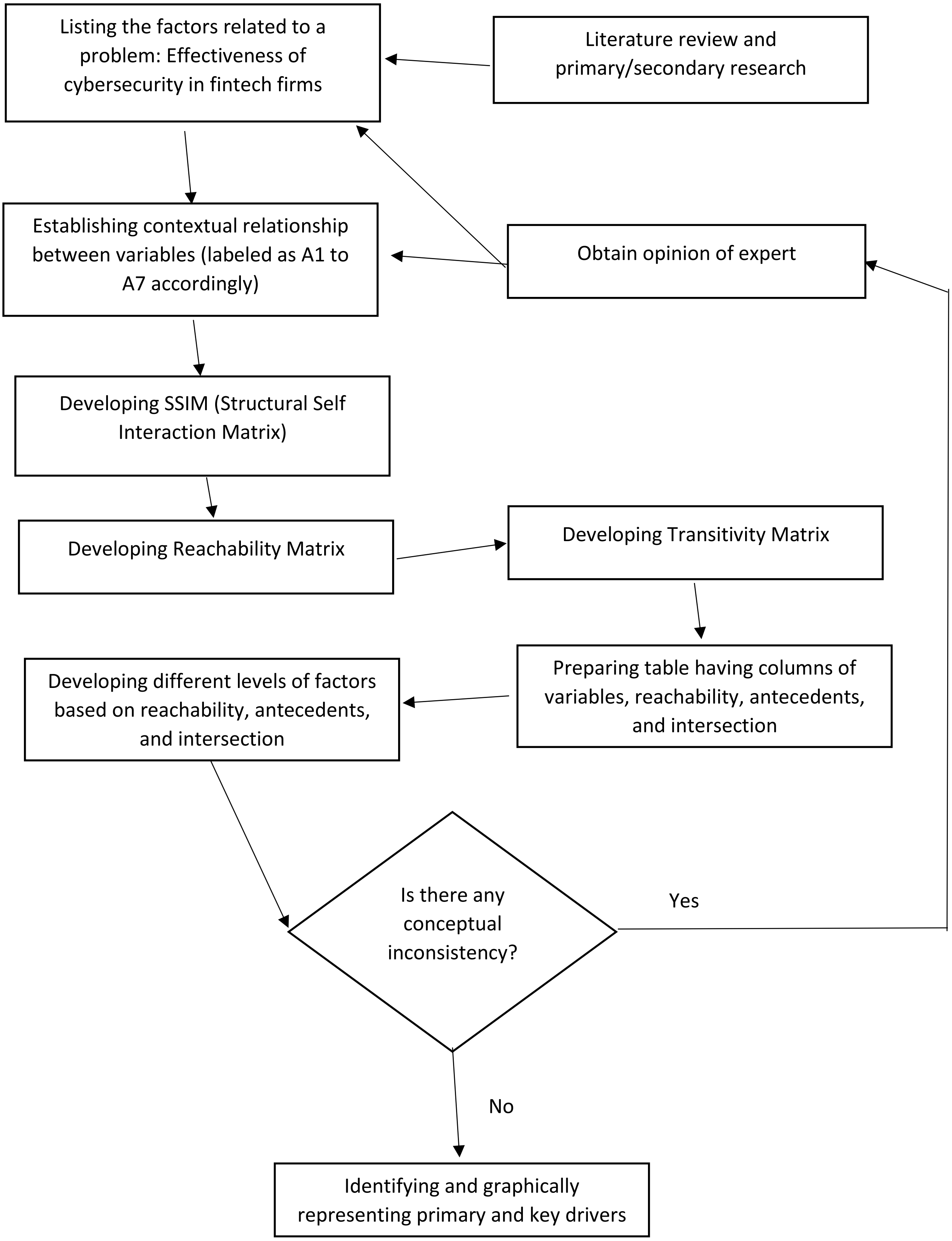
Interpretive structural modelling (ISM) is a well-established approach for finding out linkages between distinct factors that describe an issue or problem. A variety of aspects may be associated to an issue or difficulty in any complicated topic under examination. The active and passive linkages between the elements, on the other hand, characterize the situation significantly more precisely than any single factor. As a result, ISM elucidates community understandings of these linkages.

Characteristics of ISM:

This technique is interpretative, since the group's judgement determines if and how the various aspects are connected. It is structural because of the mutual interaction between the parts; a core architecture is taken from the complicated set of elements. Because the exact relationships and general structure are depicted in a digraph model, it is a modelling tool. It aids in the imposition of order and purpose on the intricacy of interactions between diverse system elements3, 6. It is designed primarily for group learning, although it may also be used by individuals.

ISM begins with the determination of important factors to the issue or problem, and then proceed to a collaborative problem-solving approach. Then a connection that is subordinate in nature and that is meaningful contextually is selected. After deciding on the contextual relationship and element set, a structural self-interaction matrix (SSIM) is created by comparing variables pairwise. The SSIM is then converted into a reachability matrix (RM) and the transitivity of the Reachability Matrix is tested. A matrix model is created when embedding of transitivity is completed. The splitting of the components is next performed, followed by the derivation of the structural model known as ISM.(Attri et al., 2013)

Steps involved in preparing ISM Model:


Listing the factors related to a problem: Effectiveness of cybersecurity in fintech firms
Literature review and primary/secondary research
Establishing contextual relationship between variables (labeled as A1 to A7 accordingly)
Obtain opinion of expert
Developing SSIM (Structural Self Interaction Matrix)
Developing Reachability Matrix
Developing Transitivity Matrix
Developing different levels of factors based on reachability, antecedents, and intersection
Preparing table having columns of variables, reachability, antecedents, and intersection
Is there any conceptual inconsistency?
Yes
No
Identifying and graphically representing primary and key drivers

Structural Self Interaction Matrix (SSIM):

Feedback from fintech is collected, collated, and comprehended to understand various drivers that influence cybersecurity in fintech industry. Pairs of variables are compared to gauge the dependence of these factors on each other. 7 factors were identified (Feasibility, Awareness, Expertise, Stricter industry and company policies, Internet policies, Employee training, increasing competition in fintech industry) which are labeled from A1 to A7 respectively.

Below mentioned conditions (labeled as V, A, X, O) arise when a pair of factors are compared against each other in SSIM Matrix:

- **V:** When variable mentioned in row (Ai) influences variable mentioned in column (Aj) but converse doesn't hold true i.e. Aj bear no influence over Ai
- **A:** When variable mentioned in column (Aj) influences variable mentioned in row (Ai) but converse doesn't hold true i.e. Ai bears no influence over Aj
- **X:** When variable mentioned in row (Ai) influences variable mentioned in column (Aj) but converse is also true i.e. Aj influences Ai
- **O:** When variable mentioned in row (Ai) doesn't influence variable mentioned in column (Aj) but converse is also true i.e. Aj bear no influence over Ai

		A1	**A2**	**A3**	**A4**	**A5**	**A6**	**A7**
	SSIM	**Feasibility**	**Awareness**	**Expertise**	**Stricter policies**	**Internet security policies**	**Training**	**Increasing competition in fintech**
A1	**Feasibility**	X	O	A	A	A	A	X
A2	**Awareness**		X	X	O	O	A	V
A3	**Expertise**			X	A	A	X	V
A4	**Stricter policies**				X	X	V	X
A5	**Internet security policies**					X	V	X
A6	**Training**						X	V
A7	**Increasing competition in fintech**							X

Table1: Structural Self Interaction Matrix (SSIM)

Reachability Matrix and Transitivity Matrix:

Reachability matrix is derived from SSIM where V, A, X, O are replaced with Boolean values 0s and 1s according to their dependency on each other by following below mentioned steps:

- **V**: Entry in cell a_{ij} is set as 1 and entry in cell a_{ji} is set as 0
- **A**: Entry in cell a_{ij} is set as 0 and entry in cell a_{ji} is set as 1
- **X**: Entry in cell a_{ij} is set as 1 and entry in cell a_{ji} is set as 1
- **O**: Entry in cell a_{ij} is set as 0 and entry in cell a_{ji} is set as 0

		A1	A2	A3	A4	A5	A6	A7
	Reachability	Feasibility	Awareness	Expertise	Stricter policies	Internet security policies	Training	Increasing competition in fintech
A1	Feasibility	1	0	0	0	0	0	1
A2	Awareness	0	1	1	0	0	0	1
A3	Expertise	1	1	1	1	1	1	1
A4	Stricter policies	1	0	0	1	1	1	1
A5	Internet security policies	1	0	0	1	1	1	1
A6	Training	1	1	1	0	0	1	1
A7	Increasing competition in fintech	1	0	0	1	1	0	1

Table 2: Reachability matrix for key drivers for cybersecurity in fintech firms

Transitive links are identified based on reachability by following below mentioned process.

- If the variable A1 has influence over variable A2, A1 doesn't have any direct influence on A3 and variable A2 has influence over A3 then variable A1 will have influence over A3 and transitive link is established between them.
- Mathematically it can be interpreted from initial reachability matrix as if entry in a_{ij} is 1 and entry in a_{jk} is 1 then entry in a_{ik} is also 1(represented as 1*)
- If variable A1 has influence over variable A2, A1 doesn't have any direct influence on A3 and variable A2 doesn't hold any influence over A3 then A1 will also not have any influence on A3 transitively.
- Mathematically it can be interpreted from initial reachability matrix as if entry in a_{ij} is 1 and entry in a_{jk} is 0 then entry in a_{ik} is also 0.

Transitivity matrix is developed for 7 factors identified for establishing cybersecurity in fintech firms following the mentioned procedure accordingly.

		A1	A2	A3	A4	A5	A6	A7
	Transitivity	Feasibility	Awareness	Expertise	Stricter policies	Internet security policies	Training	Increasing competition in fintech
A1	Feasibility	1	0	0	1*	1*	0	1
A2	Awareness	0	1	1	1*	1*	1*	1
A3	Expertise	1	1	1	1	1	1	1
A4	Stricter policies	1	1*	1*	1	1	1	1
A5	Internet security policies	1	1*	1*	1	1	1	1
A6	Training	1	1	1	1*	1*	1	1
A7	Increasing competition in fintech	1	0	0	1	1	0	1

Table 3: Transitivity matrix for key drivers for cybersecurity in fintech firms

After developing transitivity matrix, Iteration matrix is prepared by portioning the variables into different levels. Iteration matrix has 5 columns namely **Variables, Reachability, Antecedents, Intersection and Levels.**

A. **Variables:** The column1 consists of labels of factors identified at the beginning of the study that impact the implementation of cybersecurity in fintech firms. Feasibility, Awareness, Expertise, Stricter industry and company policies, Internet policies, Employee training, increasing competition in fintech industry which are labeled from A1 to A7 are entered in first column of Iteration Matrix
B. **Reachability:** This column contains all the variables a particular variable from column1 is influencing either directly or indirectly. This is evaluated by considering all 1s and 1*s from transitivity matrix and listing them in this column.
C. **Antecedents:** The column3, Antecedents, lists all of the factors that have the potential to affect or reach out to the variable under study. All 1s and 1*s in the column carrying the variable under consideration in the Final Reachability Matrix can be used to assess this.

D. **Intersection:** This column4 depicts all the variables that are common in column 2 and column 3. This column collects the intersection set of Reachability and Antecedents.

E. **Levels:** Variables with equal reachability set and intersection set are marked as level 1 and are removed from the variables (from columns of Reachability, Antecedents, and Intersection) for which any level is not assigned yet. Multiple variables can be assigned to same level depending upon the model. This indicates that variables of same level have similar influence in structure of hierarchy of problem at hand i.e., implementing cybersecurity in fintech firms.

   The same process is repeated until all the variables are assigned to corresponding levels. Considering the similarity between Intersection set and Reachability set, variables are assigned to level 2, level 3, level4 etc.… However, it is highly important to remove variables from these sets once a level is assigned to them.

By following above mentioned procedure under different iteration final iteration matrix is developed as below:

	Reachability	**Antecedent**	**Intersection**	**Level**
A1	A1, A4, A5, A7	A1, A3, A4, A5, A6, A7	A1, A4, A5, A7	Level 1
A2	A2, A3, A4, A5, A6, A7	A2, A3, A4, A5, A6	A2, A3, A4, A5, A6	Level 2
A3	A1, A2, A3, A4, A5, A6, A7	A2, A3, A4, A5, A6	A2, A3, A4, A5, A6	Level 2
A4	A1, A2, A3, A4, A5, A6, A7	A1, A2, A3, A4, A5, A6, A7	A1, A2, A3, A4, A5, A6, A7	Level 1
A5	A1, A2, A3, A4, A5, A6, A7	A1, A2, A3, A4, A5, A6, A7	A1, A2, A3, A4, A5, A6, A7	Level 1
A6	A1, A2, A3, A4, A5, A6, A7	A2, A3, A4, A5, A6	A2, A3, A4, A5, A6	Level 2
A7	A1, A4, A5, A7	A1, A2, A3, A4, A5, A6, A7	A1, A4, A5, A7	Level 1

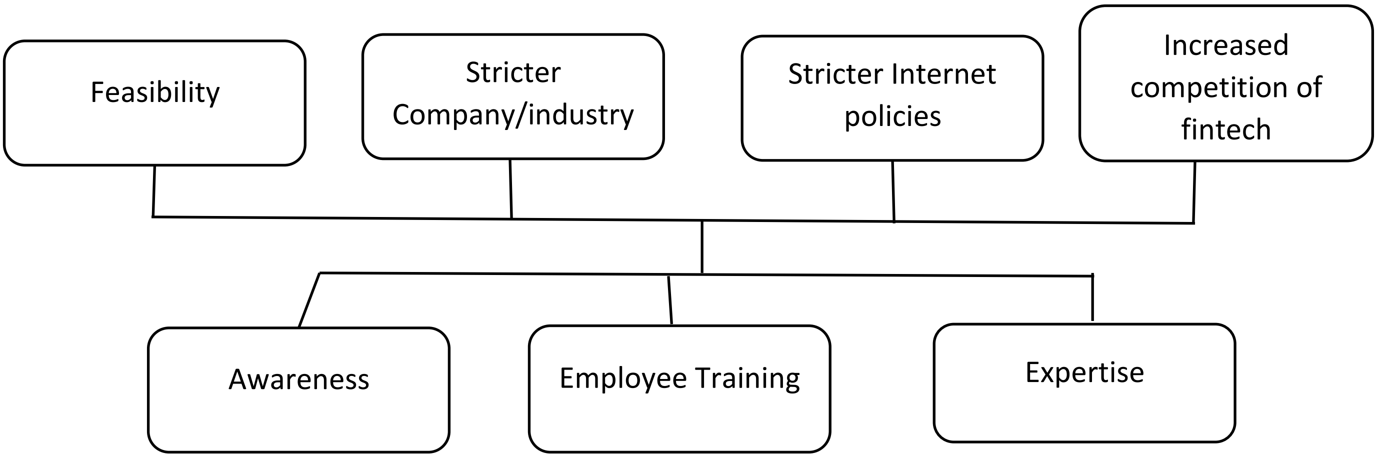
Table 4: Final Iteration matrix for drivers for cybersecurity in fintech firms

Variables	**Levels**
Awareness	Level 2
Expertise	Level 2
Employee Training	Level 2
Feasibility	Level 1
Stricter company/industry policies	Level 1
Stricter internet policies	Level 1
Increasing competition in Fintech industry	Level 1

Table 5: Identification of key and primary drivers for cybersecurity in fintech firms

After levels are identified, ISM model is developed in the form of diagraph in a hierarchical structure. Variables belonging to same level are mentioned together and finally, it leads to the creation of the final ISM Model for the complicated issue statement in question, which clearly divides the variables into tiers based on their capacity to impact other factors and hierarchical influence. Primary drivers are place above key drivers in diagraph as shown below:

Level 1: Primary Drivers


Feasibility
Stricter Company/industry
Stricter Internet policies
Increased competition of fintech
Awareness
Employee Training
Expertise

Level 2: Key Drivers

Feasibility of fintech firms in establishing cybersecurity, stricter company and industry policies guiding cybersecurity, internet policies supporting the implementation of cybersecurity and rapidly growing competition in fintech industry variables are identified as primary drivers for implementing cybersecurity in fintech firms as derived from ISM model

Awareness regarding cybersecurity in fintech firms, training of employees on cybersecurity in fintech firms and expertise of fintech with respect to infrastructure and management in establishing efficient cybersecurity in fintech firms are identified as key drivers from ISM model.

These 3 key drivers are more impactful and significant comparatively with 4 primary drivers in cybersecurity implementation in fintech industry. However primary drivers also play a major role in developing cybersecurity in fintech space but less influential than key drivers.

Study 2: Chi Square Test to determine the dependency of malware attack on parameters like Firewall, admin mode and Secure boot mode that are enabled for devices (organization endpoints) under study

Chi-square test is Pearson’s most significant contribution to contemporary statistics. Chi-square distribution, often known as the test of independence and test for goodness of fit. The significance of Pearson’s Chi-square distribution was that users could interpret the data statistically and do not have to rely on the normal distribution.

Chi-square test is considered to be non-parametric in nature that is used for mainly two purposes as mentioned below:

1. Testing hypothesis stating association/no-association among two or more populations, groups or criteria.
2. To examine how the observed data fits with the data distribution that is expected. This is done basically to examine goodness of fit

Data under analysis using Chi-square test should be categorial. Under no circumstances this test is used to measure parametric or continuous data.

Assumptions for Chi-square Test

- Sample size should be large. For small sample data, it is highly likely to accept null hypothesis which would be false scenario when Chi-square test is applied. However, there is minimum cut-off for data size, but 20 to 50 samples are generally considered.
- Variables on which Chi-square test is applied should be mutually exclusive in nature. This indicates that every variable is counted only once in specific category and cannot be repeated in other category

Formula used to calculate Chi-square statistic is

$$\chi^2 = \sum_{i=1}^{n} \frac{(O_i - E_i)^2}{E_i}$$

Where E indicates frequency that is expected

O indicates frequency that is observed

(Singhal & Rana, 2015)

Data Analysis:

Source of Data is secondary from Microsoft Malware Classification Challenge. 50,000 rows of data are considered for the study

Categorical data under study:

- IsInfected: Determines whether the device is detected with malware or not (Yes/No)
- Firewall: Determines whether the firewall is enabled for the device or not (Yes/No)
- IsSecureBootEnabled: Determines whether the secure boot mode is enabled or not for the device under study (Yes/No)

- AdminApprovalMode: Determines whether the administrator approval mode (Admin Mode user type) is enabled or not (Yes/No)

Chi-square Test using SPSS tool is applied on the data and following results are obtained with confidence interval of 95% which denotes Alpha = 0.05

Hypothesis considered to test using Chi-square statistic are mentioned below:

Hypothesis 1:

Null Hypothesis(H0): No association found between variables IsInfected and Firewall

Alternate Hypothesis(H1): Association found between variables IsInfected and Firewall

Hypothesis 2:

Null Hypothesis(H0): No association found between variables IsInfected and IsSecureBootEnabled

Alternate Hypothesis(H1): Association found between variables IsInfected and IsSecureBootEnabled

Hypothesis 3:

Null Hypothesis(H0): No association found between variables IsInfected and AdminApprovalMode

Alternate Hypothesis(H1): Association found between variables IsInfected and AdminApprovalMode

Test results:

Result 1:

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	.005[a]	1	.944		
Continuity Correction[b]	.002	1	.968		
Likelihood Ratio	.005	1	.944		
Fisher’s Exact Test				.952	.484
Linear-by-Linear Association	.005	1	.944		
N of Valid Cases	49447				

a. 0 cells (0.0%) have expected count less than 5. The minimum expected count is 561.17.

b. Computed only for a 2x2 table

Table 6: Chi-Square test results of hypothesis 1

P-value from Pearson Chi-square is 0.944

Result 2:

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	.354[a]	1	.552		
Continuity Correction[b]	.343	1	.558		
Likelihood Ratio	.354	1	.552		
Fisher's Exact Test				.555	.279
Linear-by-Linear Association	.354	1	.552		
N of Valid Cases	46951				

a. 0 cells (0.0%) have expected count less than 5. The minimum expected count is 11551.23.

b. Computed only for a 2x2 table

Table 7: Chi-Square test results of hypothesis 2

P-value from Pearson Chi-square is 0.552

Result 3:

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	.190[a]	1	.663		
Continuity Correction[b]	.144	1	.704		
Likelihood Ratio	.190	1	.663		
Fisher's Exact Test				.694	.352
Linear-by-Linear Association	.190	1	.663		

N of Valid Cases	49942				

a. 0 cells (0.0%) have expected count less than 5. The minimum expected count is 159.12.

b. Computed only for a 2x2 table

Table 8: Chi-Square test results of hypothesis 3

P-value from Pearson Chi-square is 0.663

Alpha considered was 0.05

In all the three cases, p-value < alpha

This indicates that Null hypothesis is accepted, and alternate hypothesis is accepted.

Hence it was found from Chi-square test on 50,000 rows of sample data that:

- These is no association between the device is infected with malware and firewall in the device is enabled.
- These is no association between the device is infected with malware and Secure boot mode in the device is enabled.
- These is no association between the device is infected with malware and Admin approval mode in the device is enabled.

Therefore, from both study 1 and study 2 it is found that the threat of cyberattack like malware doesn't only dependent on safety mode enabled at organization's endpoints but highly dependent on employee's awareness. Hence it is highly essentials for employees in firms especially fintech need to be properly trained on cyber threats due to disruptive technologies and build a strong expertise.

Conclusion

Cybersecurity breaches are experiencing an increasing trend especially in the field of financial technology. This trend has become steeper due to pandemic of Covid-19. As the economies of the world are progressing rapidly, there is huge growth in banking and financial technology space. Fintech firms are adopting advanced technologies to establish their dominance in current markets. When such firms collaborate with traditional banks by extending their services, threat of cybersecurity is increasing due to traditional IT infrastructure that are vulnerable to cybersecurity attacks like ransomware, crypto jacking, botnet, malware etc.…

As per the study 1 conducted by identifying factors that influence successful implementation of cybersecurity in fintech firms(Feasibility, Employee Awareness, Firm's expertise, Employee training on cybersecurity, Company and industry policies, internet polices and increasing competition in fintech space) which were interdependent on each other, It was evident from Interpretive Structural Modelling(ISM) that Employee Awareness on cybersecurity threats and its preventive measures, Employee training on cybersecurity threats and its preventive measures and Fintech firm's expertise to establish cybersecurity act as key drivers and slightly more significant in contributing towards a robust system of cybersecurity. Slightly less significant factors denoted by primary drivers as per ISM model were identified as Stricter Internet policies, Stricter internet and company polices, Feasibility and increasing competition in fintech industry. However primary drivers also play a vital role towards identifying, solving and preventing cybersecurity threats but they are slightly less significant than the key drivers in this purpose.

To further build on study 1, study 2 was conducted to understand the influence of safety factors like firewall, secure boot mode and admin approval mode on the likeliness of the device getting infected with malware. Chi-square statistic was applied on the huge data of 50000 rows collected from Microsoft Malware Classification Challenge to understand the dependence of these factors. It was evident from the results even though devices were enabled with firewall, secure boot mode and Administrator approval mode (user profile) or not, they were diagnosed with Malware. There was no association found between firewall, secure boot mode and administrator approval mode with the devices getting affected with malware. Hence, proving that simply adopting safety protocols and policies on organization's endpoints will not solve the problem of cybersecurity attacks. Management and employees need to stay updated and aware of new technology trends, different kinds of threats it brings to data. Proper training should be setup to management and employees in the firm and build expertise in this area to make it more resilient to cyber-attacks.

Future Scope

As the world is moving towards digitization, organizations become highly dependent on data to meet the growing demands of the markets. With huge data that is highly essential and confidential to the firms, it is very much necessary to establish a robust cybersecurity for their firms to safeguard their sensitive data. As the hybrid mode (online + offline mode of working) is taking the work culture as a storm because of covid-19 pandemic, it is highly essential for fintech firms to have resilient cybersecurity infrastructure in place.

As the threats to data are increasing due to growing competition because of adopting disruptive and advanced technologies, cybersecurity is highly essential and very huge scope in current days and in future to safeguard not only confidential data but also protect the firm's integrity by establishing a sense of trust with its customers. Ecosystem of fintech brings technical complexities and dependencies along with advanced technologies. When they collaborate with traditional banks, breaches in data security is increasing. Hence it is highly relevant to have efficient cybersecurity system in place to drive the economy towards digitization.

By complete understanding of cyber threats, identifying the loopholes, significant factors that can help in setting up an efficient system, cyber threats can be tackled and prevented which can add huge value to the firm. Machine learning techniques can be implemented to predict cyber-threats beforehand based on previous trends. Once they are predicted, necessary measures like stricter industry polices, stricter company polices, management and employee training and increasing their awareness so that they can prevent cyberattacks can be adopted and safeguard the firm's data and integrity and continue to strive and achieve dominance in the financial markets.

References:

Arashhhabibiilashkari, G. Z. (n.d.). *Future of Business and Finance Understanding Cybersecurity Management in FinTech Challenges, Strategies, and Trends*. http://www.springer.com/series/16360

Attri, R., Dev, N., & Sharma, V. (2013). Interpretive Structural Modelling (ISM) approach: An Overview. In *Research Journal of Management Sciences* (Vol. 2, Issue 2). www.isca.in

Cybercrime and Cybersecurity: FinTech's Greatest Challenges 1. (n.d.). https://www.paloaltonetworks.com/cyberpedia/what-is-cyber-security

Cybersecurity-and-Fintech-at-a-Crossroads_joa_Eng_0219. (n.d.).

Executive Summary Introduction. (n.d.). https://www.ibm.com/sg-en/security/data-breach

Fintech by the numbers Incumbents, startups, investors adapt to maturing ecosystem Contents. (n.d.).

Fintech in India. (n.d.).

Imtiaz, M. (n.d.). *Conceptualising cybersecurity risk of fintech firms and banks sustainability*. http://shura.shu.ac.uk/27504/

Jaganathan, V., Cherurveettil, P., & Muthu Sivashanmugam, P. (2015). Using a prediction model to manage cyber security threats. *Scientific World Journal*, *2015*. https://doi.org/10.1155/2015/703713

Khan, A., & Malaika, M. (2021). *Central Bank Risk Management, Fintech, and Cybersecurity, WP/21/105, April 2021*.

Predicting Infection of Organization Endpoints by Cybersecurity Threats using Ensemble Machine Learning Techniques. (n.d.).

Singhal, R., & Rana, R. (2015). Chi-square test and its application in hypothesis testing. *Journal of the Practice of Cardiovascular Sciences*, *1*(1), 69. https://doi.org/10.4103/2395-5414.157577

Dissertation_updated

ORIGINALITY REPORT

9%	6%	6%	6%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to VIT University Student Paper	1%
2	Submitted to Indian Institute of Foreign Trade Student Paper	1%
3	eprints.uanl.mx Internet Source	1%
4	core.ac.uk Internet Source	1%
5	uniassignment.com Internet Source	1%
6	Gurdip Kaur, Ziba Habibi Lashkari, Arash Habibi Lashkari. "Understanding Cybersecurity Management in FinTech", Springer Science and Business Media LLC, 2021 Publication	<1%
7	downloads.hindawi.com Internet Source	<1%
8	Submitted to Universitas Diponegoro Student Paper	

		<1%
9	Agarwal, A.. "Modeling agility of supply chain", Industrial Marketing Management, 200705 Publication	<1%
10	etd.aau.edu.et Internet Source	<1%
11	Submitted to Asia Pacific University College of Technology and Innovation (UCTI) Student Paper	<1%
12	www.bis.org Internet Source	<1%
13	shura.shu.ac.uk Internet Source	<1%
14	Submitted to Coventry University Student Paper	<1%
15	Submitted to Oklahoma State University Student Paper	<1%
16	www.isaca.org Internet Source	<1%
17	International Journal of Productivity and Performance Management, Volume 62, Issue 3 (2013-03-09) Publication	<1%
18	blog.isc2.org	

	Internet Source	<1 %
19	cadinc.com Internet Source	<1 %
20	staging.fuw.ch Internet Source	<1 %
21	Naveen Kumar, K. Mathiyazhagan, Deepak Mathivathanan. "Modelling the interrelationship between factors for adoption of sustainable lean manufacturing: a business case from the Indian automobile industry", International Journal of Sustainable Engineering, 2020 Publication	<1 %
22	Sarbjeet Singh, Rupesh Kumar, Uday Kumar. "Modelling factors affecting human operator failure probability in railway maintenance tasks: an ISM-based analysis", International Journal of System Assurance Engineering and Management, 2014 Publication	<1 %
23	Submitted to University of Bristol Student Paper	<1 %
24	hdl.handle.net Internet Source	<1 %

25	Journal of Modelling in Management, Volume 9, Issue 2 (2014-09-16) Publication	<1 %
26	J S Sudarsan, Kakuru Jyothi Priyanka Reddy, Haseeb.A.H. Biyabani, Purnima Kumari, Swati Sinha. "Impact of Fragile Water Management Strategies and Mitigation-A Case Study of Pune City, India", IOP Conference Series: Materials Science and Engineering, 2021 Publication	<1 %
27	Submitted to University of Lancaster Student Paper	<1 %
28	rimag.ricest.ac.ir Internet Source	<1 %

Exclude quotes	On	Exclude matches	< 5 words
Exclude bibliography	On		