A Resilient Cybersecurity Framework for Mobile Financial Services (MFS)

Stephen Ambore,Christopher Richardson, Huseyin Dogan, Edward Apeh, David Osselton
Cybersecurity Unit, Bournemouth University,
Dorset, UK
{S. Ambore, C.J. Richardson, H. Dogan, E. Apeh, D. Osselton}@bournemouth.ac.uk

***Abstract*—Cybercrime has astronomically risen with technological advancements alongside the business opportunities in cyberspace. So much so that cybercrime is now viewed as one of the top ten global risks. In recognition of the threat posed by cybercrime, organisations are investing in controls and countermeasures that would combat the threat of cybercrime and its impact. However, incidences of successful cyber-attacks are still on the rise. The advent of mobile devices has created a means of providing financial services to over 2 billion people globally that hitherto had no access to formal banking services. Also, banks and other financial institutions use mobile platforms as an alternative delivery channel for financial services. However, the dark side of using mobile devices to bridge the banking gap is that mobile devices are now an added vector for cybersecurity threats. This has affected trust in the use of the system and consequently slowed down the uptake of Mobile Financial Services (MFS). This paper presents an in-depth analysis of the opportunities mobile platforms provide for the unbanked and how cybersecurity is hampering the uptake of MFS. Furthermore, the paper proposes an approach for mitigating cybercrime in the complex MFS ecosystem, and presents preliminary results from the research conducted so far.**

Keywords—cybersecurity; Mobile Financial Services; human factors; countermeasures; framework

I. INTRODUCTION

Projected to reach an estimated cost of about $2.1 trillion by 2019, on fraud related to data breaches alone [1], cybercrime is not abating. Recent events have shown how pervasive and disruptive cybercrime has become. Repetitiveness and frequency of cybercrime is also on the rise. For instance, the Society for Worldwide Interbank Financial Telecommunication (SWIFT), an interbank message carrier, recently reported attacks on 3 banks. This is in addition to recent attacks on SWIFT bank customers in Vietnam, Ecuador and Bangladesh [2].

The main motivation for cybercrime is financial gains [17]. Attackers use malware to obtain money from customer bank accounts. Ransomewares have also been deployed to extort money from their victims. Other motivations for cybercrime may include sabotage or curiosity. Cyber-attacks can also occur due to insider abuse. For instance, a staff of an organisation can fraudulently obtain elevated privileges on systems if the right controls are not put in place. These privileges may be used to commit fraudulent acts. Insider abuse may also occur as a result of genuine mistakes or lack of knowledge.

While some organisations have invested in implementing technological controls to mitigate the risks posed by cybercrime, others have invested in more comprehensive information security programs for the same purpose. These efforts notwithstanding, news of successful cyber-attacks on organisations are still frequently in the news.

The top cybersecurity threats for 2015 according to European Union Agency for Network and Information Security (ENISA) [18] include:

- Malware;
- Web based attacks;
- Web application attacks;
- Botnets;
- Denial of service;
- Physical damage/theft/loss; and
- Insider abuse.

Worthy of note is the role of the human element in these attacks. None of the attacks can be successfully executed without the participation of the human element, either as the originator, the medium or the actual executor of the attack. Therefore, any effective countermeasure must be very robust enough to address the risk(s) posed by the human element in the perpetuation of cybercrime.

With the introduction of new technologies like mobile devices, more people are becoming connected to the cyberspace and the risks of cybercrime is becoming more widespread. This has been made worse by poor mobile device users' security practices. The expectation on end-users to be ultimately responsible for the security of their mobile devices has made the mobile device a likely attack vector.

While most organisations can acquire the skills and have the financial capability to put some controls in place, end-user technologies like mobile devices depends very much on the user's awareness of cybersecurity and technology as a key control. This further buttresses the need to consider the unique characteristics of the human element in coming up with an effective cybersecurity solution for MFS.

Strong technical infrastructure base for secure electronic financial transactions exists. For instance, strong encryption, multiple levels of authentication using biometric, steganography and a combination of biometry based authentication and tokenization have been implemented [3,4,5].

Furthermore, standards and frameworks for mitigating the risk of cybercrime and to serve as guidelines for the appropriate use of the technical security solutions have been published. For instance, a guideline for mobile platform applications developers and merchants [6], meant to serve as a control for cybercrime, was published by the Payment Card Industry Data Security Standard (PCI DSS), a proprietary information security standard organisation for the card payment industry.

The US based National Institute of Standards and Technology (NIST) has over 900 publications addressing various aspects of cybersecurity [19]. Furthermore, in recognition of the impact of cybersecurity to national security, countries like the UK have established a cybersecurity centre, to facilitate intelligence sharing [32].

In spite of the existence of these countermeasures, the threat of cybercrime is not abating. The 2016 Global Risk report, an annual report published by the World Economic Forum has identified data fraud as 1 of top 10 likely global risks of 2016 [7].

Over 2 billion people in the world currently do not have access to formal banking services [8]. This group comprises of the “Unbanked” and the “Under-banked”. While the unbanked do not have access at all, the under-banked do not have sufficient access. We will refer to both groups as the unbanked in the rest of this paper.

Advancement in mobile technologies had made mobile platforms and their devices accessible to over 7 billion people worldwide, reaching a global penetration rate of 97% [9]. In order to take advantage of the opportunities provided by mobile platforms, companies have developed various financial products to serve the unbanked. For instance, Mobile Money is a mobile device based technological innovation that has been used as a channel to provide financial services to the unbanked and to overcome barriers to financial inclusion. Since debuting in Kenya in 2007, the Mobile Money company M-PESA now has over 40 million customers. 20 million of these customers recorded over $500 million in funds transfers alone in a certain month [14].

The unbanked are not the only benefactors of the advancement in mobile technologies and platforms. Mobile platform based financial products now exit that serve other segments of the world population. For instance, MFS has gained prominence as a replacement for cash purchases and as a countermeasure against credit card fraud through the implementation of mobile wallets [10]. Since Starbucks; an American coffee company lunched a mobile payment application in 2011 for its American customers, acceptance of MFS has grown largely due to its convenience and value add services [20].

Also, given the opportunity presented for cutting down cost and increasing operational efficiency, banks now use mobile devices as an alternative banking delivery channel to its customers [11]. Mobile banking is now a hygiene factor for the technology savvy banking population and other customers who prefer to bank anywhere at their own convenience. Furthermore, access to insurance products is available via mobile devices.

Cybercrime is the dark side of progress of mobile device based financial products. With the advent of mobility, the paradigm of cyberspace has shifted. The high penetration rate, personalised and affordable nature of mobile devices mean more people are now connected to the cyberspace than ever before. Consequently, the risks inherent in the cyberspace has now moved closer to the door steps of a larger segment of the world population and has made the attainment of cybersecurity a moving target. A recent report showed that over 5 billion downloaded mobile applications are vulnerable to remote attacks [33]. Furthermore, over 173% increase in mobile fraud was recorded between 2013 and 2015. With estimated revenue from MFS projected to reach $516 billion by 2017, MFS is the new cash cow for cybercrime [34]. Therefore, along with the opportunities presented by MFS to provide financial services, it has also created a new vector for cybercrime, threatening to erode the gains. This has led to a lack of trust in MFS, which has slowed down the adoption of MFS, despite the obvious benefits [12].

The existence of strong technical security countermeasures for electronic transactions, framework and standards while providing a mechanism for mitigating against the threat of cybercrime, have not provided a workable solution specifically for MFS. In a recent global survey conducted by ISACA, respondents expected an 87% increase in data breach on MFS in the next 12 months. MFS was also adjudged the least preferred method of payment compared to instruments like payment cards and cheques [10].

Research has been conducted on strengthening MFS technical security countermeasures [3, 4 and 5], and improving MFS security [10]. Approaches for implementing cybersecurity countermeasures for complex systems have also been researched [13]. The solutions proffered in previous works advocated strengthening technical controls, and have not been circumspect in providing a workable solution for cybersecurity. Available standards tend to be generic and not specifically built to address the unique context of MFS.

Furthermore, improved information security practices now exist. For instance, concepts like defense in depth; where layered security mechanisms are used to improve system security and security by design; where software are design from scratch with security in mind, have both been successfully implemented to improve the security posture of technological landscapes [35].

However, highly resilient countermeasures for cybersecurity go beyond providing technological controls and generic standards to putting in place measures that would consider the unique characteristics of the ecosystem and social context of the system, in this case, the complex MFS ecosystem.

The MFS ecosystem is a socio-technical system because it involves complex social and technical interaction within trusted and untrusted elements, within and outside systems, organisational and national boundaries [36].

Existing countermeasures work well for predefined environments but are not well suited for socio-technical interactions within a complex socio-technical system like the MFS Socio-Technical System (MFS STS). For instance, one of the controls for MFS fraud is setting a maximum limit for allowable transaction. While this countermeasure limits the impact of fraud, it also limits trusted entities within the system from enjoying the full benefit of MFS. Furthermore, some end-users who are granted elevated privileges on systems in an organisation, also retain same privileges even when they attempt to logon from untrusted environments, compromising the countermeasures put in place. In a complex environment like the MFS ecosystem where information flows within trusted and untrusted elements, these types of controls might not be effective in tackling cybercrime. The ideal control for the complex MFS STS must be dynamic enough to address various information flow scenarios within the STS and redundant enough to compensate for failing controls.

No known study has been conducted on developing a resilient cybersecurity framework for the complex MFS ecosystem considering its unique characteristics and social context with the aim of mitigating the risks of cybercrime and consequently boosting adoption.

The purpose of this paper is to introduce the research into developing a resilient framework for information assurance aimed at providing a methodology for mitigating the risks posed by cybercrime to the uptake of MFS. The proposed framework aims to be dynamic enough to cater for the complex social interaction within trusted and untrusted components of the system and redundant enough to ensure sufficient compensating controls are put in place to further improve trust in the ecosystem. The resilient framework will break the trust barrier and improve adoption and usability within the MFS ecosystem.

This paper presents an in-depth analysis of the opportunities mobile platforms provide to access financial services, and how cybersecurity is hampering the uptake of MFS. It then describes the approach adopted for mitigating the threat posed by cybercrime to MFS. Preliminary results and understanding obtained in analysing cybersecurity issues affecting the complex MFS ecosystem are also discussed.

The next section presents a background overview of mobile financial services including a description of stakeholders and underpinning technology. Existing cybersecurity threats to MFS and current countermeasures are also discussed in Section II. Section III describes the approach adopted in developing the solution. Preliminary results of the work done to date are discussed in section IV. The paper concludes with a summary and direction for future work in Section V.

II. BACKGROUND OVERVIEW OF MOBILE FINANCIAL SERVICES

To facilitate better understanding of cybersecurity issues in MFS, we shall provide an understanding of MFS and the ecosystem.

A. MOBILE FINANCIAL SERVICES TAXONOMY

The benefits of using Mobile devices as a means of carrying out financial transaction include; effectiveness, security and convenience of transactions by end-users, cost reduction and improved operational efficiency by banks and attainment of financial inclusion objectives by government and institutions amongst others. What is lacking is a generally accepted taxonomy for describing mobile devices based financial products. Terms like Mobile Wallets, Mobile Money, and Mobile Payment have been used interchangeably to describe the same products [14, 15, and 16].

Mobile Banking stands out in this regards, as it has been generally accepted as an alternative channel of delivery for banking services. Furthermore, the advent of Financial Technology (Fintech) 2.0 [1] has thrown products like Mobile Insurance into the fray. With the exception of insurance products, all other products can be used for payments.

Mobile Money users do not require a bank account. Mobile Payment as part of Mobile Wallets requires users to own credit cards. The scope of this research covers Mobile Wallets, Mobile Money and Mobile Banking. We henceforth refer to them broadly as MFS. We further describe these 3 MFS products.

(i) Mobile Wallets: One important innovation of e-commerce was the e-wallet. E-wallets enable customers to store monetary value online, which they could use to make payments for procurements done from merchants who accept them. Examples of popular e-wallet services include google wallet and Paypal. The advent of mobile devices led to the implementation on a Mobile device based e-wallets. Mobile wallets sometimes referred to as M-wallets provide the same kind of services offered previously by e-wallets. M-wallets have the added capability of mobility that enables proximity payments. Examples of mobile wallets include Apple pay, Samsung pay and Android pay. Near Field Communication (NFC), a contactless communication technology is the underpinning technology used by mobile wallets for proximity payments. Biometric authentication capability of smart phones provides an added layer of security for mobile wallet based payments products.

(ii) Mobile Money: Cash is still the preferred means of payments in most developing countries. Cash transactions however are fraught with many risks which include theft and loss. Availability of banking

services is also a major concern. Mobile money provides banking services that replaces the use of cash with "electronic" money. Mobile Money agents act on behalf of banks to collect cash from their customers in exchange for e-float. Customers can perform a person-to-person money transfer or payments of goods without the need for physical cash. Cash-in and cash-out operations can also be conducted with the agents. Mobile money implementation is more predominant in developing countries. The predominant technologies used in Mobile Money are Unstructured Supplementary Service Data (USSD) and Short Message Services (SMS). These are cellular communication technologies that are used to send messages between end-user phones and applications programs in communication networks. Lack of end-to-end encryption for both technologies however, makes them vulnerable to attacks [21].

(iii) Mobile Banking: Mobile Banking is an extension of banking services provided by banks through mobile platforms. Customers remotely connect to their bank via mobile applications to conduct normal banking operations. Customers can also access the bank by connecting to a secure bank Uniform Resource Locator (URL), popularly referred to as web address via mobile platform browsers.

Fig 1 shows the taxonomy of MFS.

B. TECHNOLOGY UNDERPINING MFS

To further provide an understanding of how mobile platforms are used to provide financial services, we analysed the basic technologies underpinning mobile platforms, their characteristics and impact on the uptake of MFS

The end-user tool used to access MFS products is the mobile phone. Mobile phones are of 2 types; Smartphones and feature phones (non-smart phones). While both phone types can be used to access MFS, the capability of the phones either enables or restricts certain services. For instance, the graphic user interface of smartphones and its underlying Operating System (OS) can facilitate contactless payment using the biometric capability for authentication, in addition to token and personal identification number (PIN). Feature phones largely depend on USSD and SMS for payment operations. Regardless of the phone types, mobile phones can only establish connection through two primary means; the internet or Mobile Network Operator (MNO) access.

The phone features and means of connection to financial services have implications on security. For instance, biometric authentication in combination with tokens and PINs has provided an improved level of security for payments using smartphones. On the other hand, vulnerabilities in USSD and the lack of end-to-end encryption on SMS coupled with the basic nature of feature phones make them more prone to cyber-attacks. The use of public WI-FI to provide internet connection for mobile platforms makes it vulnerable to mobile malware attacks.

A typical MFS transaction using the mobile platform traverses through various stakeholders and technologies before it is consummated. For instance, a mobile payment request goes through the internet or MNO to the wallet manager, then to the card issues, then to the payment network, and then finally to the merchant via a contactless operation using the NFC technology. Each service provider in the value chain has its own technologies and processes. Some of these transactions traverse organizational and geographic boundaries.

Hence, the MFS ecosystem is a complex one. These types of systems are Socio-Technical Systems (STS). They are a combination of social and technical interaction to achieve a certain objective [31].

An understanding of the technological base that underpins mobile platforms and their characteristics together with an understanding of the complex ecosystem in which MFS operates provides a better insight to the cybersecurity threats facing MFS and how to mitigate them. The next section further describes the complex MFS ecosystem.

C. THE COMPLEX MOBILE FINANCIAL SERVICES SOCIO-TECHNICAL SYSTEMS (STS)

Initial investigations in [36] revealed that the MFS STS consist of the end-user who uses mobile device to access financial services. While the banked use mobile to access MFS services directly by connecting remotely using their mobile devices, the unbanked depend on agents who act in capacity of banks. Service providers also exist to provide direct and in direct services in the MFS STS. The periphery of the complex MFS STS spans beyond institutional and nations.

The major influencers in the STS are the service providers, who provide services either directly to the end-users or as secondary service providers to other service providers within the STS.

The path of information flow in the STS is not clear thereby raising concerns about data privacy. The coordination in the STS is not central as several regulators responsible for different aspects exist within the STS. Stakeholder analysis conducted revealed the following stakeholders:

(iv) End-User: This can be the initiator or beneficiary of a financial service initiated by the use of mobile devices.

(v) Mobile Network Operator (MNO): The MNO provides a means of connectivity; in some instances, it participates in providing MFS.

(vi) Mobile Money Operators (MMO): These are agents that act on behalf of the bank to provide banking services via mobile devices to end-user. They also

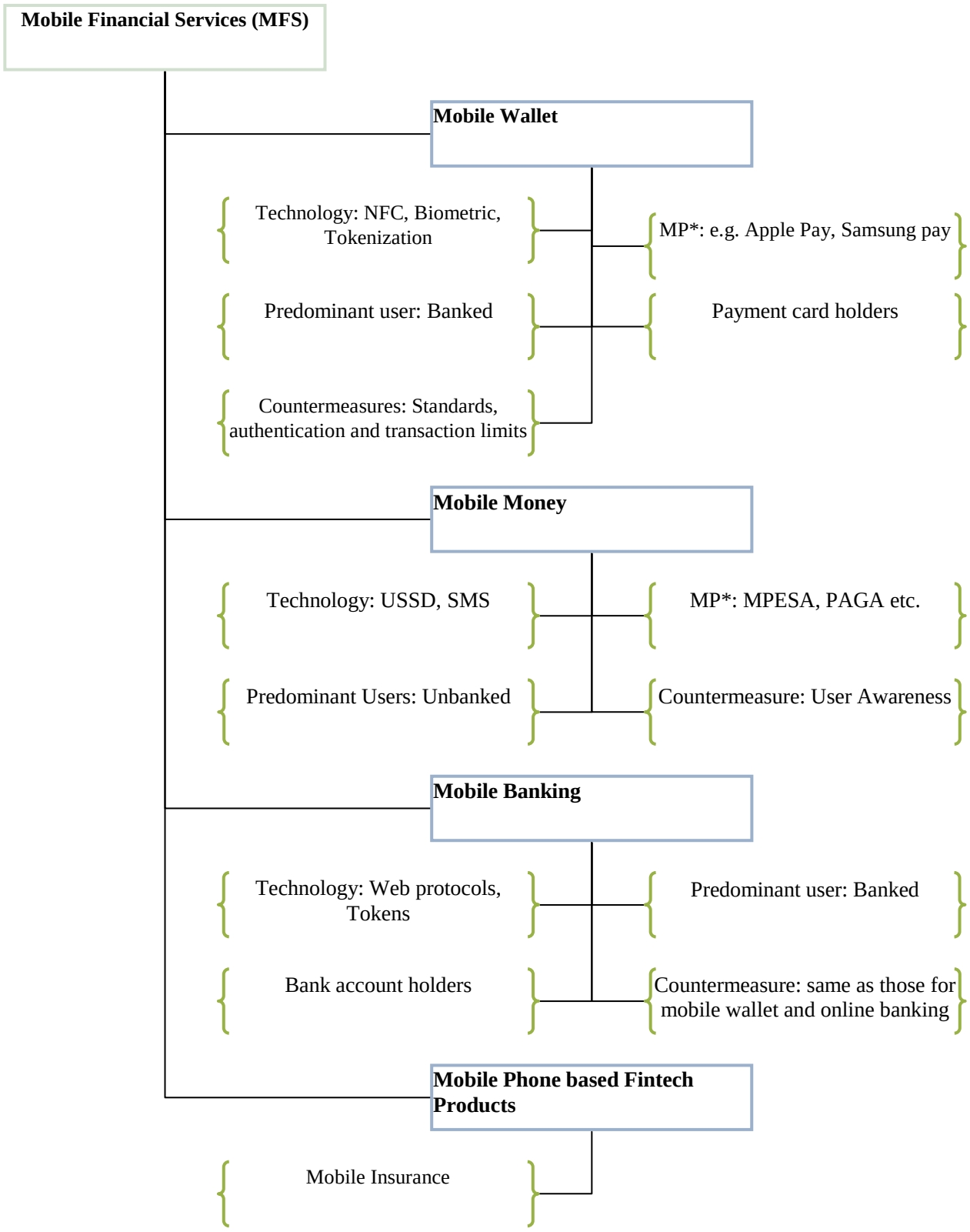

Fig. 1. Mobile Financial Services Taxonomy

perform cash-in and cash-out operations. They operate in the value chain for Mobile Money only.

(vii) Deposit Money Banks (DMB): Banks provide settlement services to MMOs; they and banking services delivery channel through Mobile Banking.

(viii) Merchants: They provide terminals for Mobile Payments.

(ix) Card Issuers: They issue cards that are coded in smartphones and used for Mobile Payments.

(x) Regulators: Include; financial services and telecommunications regulators. They regulate the activities in the ecosystem.

(xi) Service Providers: These include mobile applications developers, phone manufacturers, utility services providers and all third party stakeholders that provide services to enhance MFS.

(xii) Law Enforcement and Security Agency: These are not direct stakeholders but require information from the STS to enable a secure wider ecosystem.

Understanding the role of each stakeholder and the mode of interaction between components within the STS is important in understanding the issues impacting cybersecurity in complex MFS. The findings obtained in examining the STS are presented in Section IV of this paper.

D. CYBERSECURITY IN MFS STS AND COUNTERMEASURES

While, loss/theft of mobile devices, misconfiguration of mobile applications and mobile malwares are the better known cybersecurity threats with mobile applications [18]. There are vulnerabilities inherent in the technologies and processes that drive the use of the product.

Cybersecurity vulnerabilities in the MFS can generally be classified into the follow:

(i) End-User Device Technology: The primary tool to access MFS is the mobile phone. On a basic level, the smartphone architecture consists of 4 areas [10] namely:

a. Normal Operating System (OS) and Application Environment. It hosts third party software and generally has low security.

b. Secure Elements (SE). A more secure hardware environment than the OS environment. It hosts multiple sensitive applications and data.

c. Trusted Execution Environment (TEE). A secure area of the main processor that protects sensitive data and authorises software applications.

d. Client Apps. A specific area for housing client application on the devices.

Understanding of this architecture has facilitated the development of fairly strong technology countermeasure for MFS. However, this same knowledge has been exploited to commit fraud in the system.

(ii) Communication Channels: Users must establish network communication before they can perform any MFS transaction. This could be through Mobile Network Operator (MNO) access, the internet or proximity payment using contactless technologies like NFC or Bluetooth. These technologies are vulnerable to cyber-attacks

(iii) Services Provider Backend: Services providers invest in backend technology infrastructure including databases, software applications and network platforms. If these backend technology bases for the service providers are not regularly updated and patched it leaves a gap that could be exploited for cybercrime.

(iv) Process: Human actors interact with technology through defined processes; these processes need to be optimised and robust enough to encourage behaviours that would mitigate the threat of cybercrime.

(v) Human Element: This vulnerability relates to the action or inaction of the human element along the value chain of providing MFS. These include mistakes in design of technology leaving gaps that could be exploited. It also involves other malicious acts by humans or genuine mistakes by users and system administrators in the MFS STS. Stringent security measure can also lead to end-user actions that could compromise security.

Technologies like biometry have been implemented in conjunction with tokenization to “harden” the security for MFS. However, end- users are expected to perform complex tasks to enable certain countermeasures. For instance, end-users are expected to enable certain functions on their smart phones to enable remote wipe in the event of loss of phones [10].

Privacy of user data cannot be vouched for when using MFS [22]. Most service providers along the value chain wants a piece of user data to enable them analyse current use and improve future products. To mitigate the risk of data privacy, Apple implemented mobile device encryption and in its recent operation system (OS) versions, users do not have the option to turn it off [23]. However, this countermeasure does not exist in all mobile devices.

In addition, privacy agreement is still complex for an average end-user to comprehend [24]. The timing of updates and patches are inconsistent in some mobile OS because of the wireless carrier that controls the update schedule, making

some of the mobile applications prone to mobile malware attacks [23].

The rush to release mobile applications also makes some MFS applications not properly tested and vulnerable to cyber-attacks [25]. The presence of rogue mobile applications and the ability of phone users to sideload; install mobile application from unauthorized sources, has also presented security challenge for MFS. Though standards exist in countries like the US and the UK, some countries do not have explicit legislation on data privacy [26]. The standards in some other jurisdictions have not been updated regularly. This poses a risk for cross border transactions using MFS.

The means of connection for MFS transaction and some technologies used are susceptible to cyber-attacks. Connection via public WI-FI can provide a window for cyber-attack [27]. Mobile Money still uses vulnerable technologies like USSD and SMS as the primary technologies to perform transactions, and these can be exploited for cybercrime.

In the MFS STS, several regulators exist. The overlapping roles they play have caused a gap in regulation in the ecosystem. For instance, the issues of ownership of customer data between the Banks and the MNO have made the management of privacy in the STS more challenging. The anonymous nature of mobile device users and the ability for more than one person to use a particular mobile device makes it difficult to ascertain the actual initiator of a financial transaction, except in devices where biometric authentication has been deployed.

When Mobile devices of end-users that initiate a transactions are patched and up-to-date on security fixes, the threat of cybercrime would still exist in the value chain where any or part of the technical infrastructure of one or more of the service providers is not updated or patched . No authority in the MFS STS is responsible for providing an assurance that the technical infrastructure of all service providers in the STS is up-to-date on security fixes and patches.

Countermeasures exist to mitigate cybersecurity threat in the use of MFS products and in the complex MF STS. Technological advancement in threat monitoring and threat intelligence has also been implemented as controls against cybercrime [18].

Research has been conducted on how to strengthen cybersecurity controls in the use of MFS. (Public Key Infrastructure) PKI [3, 5] and biometry based authentication [4] have all been proposed to improve the strength of technical security controls for MFS products. Also, some work has been conducted on developing cybersecurity framework for complex systems. For instance, Carin, et al., [28] proposed an approach that was used to determine strategies and investment levels required for protecting intellectual property in complex systems.

In spite of the existence of these countermeasures, cybersecurity threats in the MFS STS have not abated. Existing countermeasures do not fully address these areas:

- Privacy of user data;
- Understanding the impact of human elements in cybersecurity of MFS STS;
- Balance between usability and security in MFS;
- Regulatory concerns in the complex MFS STS including cross border regulation;
- Mobile forensic;
- Information assurance within the complex MFS STS;
- Understanding of requirement for building a resilient framework for cybersecurity for MFS STS; and
- Enforcement of standards in the STS etc.

Consequently, there is a need for a resilient framework for tackling cyber-crime in the complex MFS STS.

A Cybersecurity framework for Mobile Financial Services would help:

- Put controls in place that would by dynamic and redundant to improve resilience;
- Provide understanding of the Mobile Financial Services STS;
- Provide understanding of information flow within the system;
- Identify key stakeholders in the ecosystem and facilitate common understanding of challenges in the ecosystem; and
- Developed a cross-functional approach that would help mitigate the risk of cybercrime in the ecosystem.

Such an artifact will:

- Provide countermeasures with compensating controls that would facilitate high availability within the MFS STS;
- Break the trust barrier within the ecosystem and improve trust in MFS;
- Provide information assurance framework for MFS STS; and
- Provide best practice case studies for adopting the information assurance framework.

In developing the framework, the unique characteristics of the human element and the social context of mobile device communication would be examined.

E. OVERVIEW OF THE PROPOSED MFS-STS FRAMEWORK

Existing countermeasures for mitigating cybercrime in complex systems work well in predefined environments. However, the element of social interaction and the existence of trusted and untrusted elements in complex STS make existing countermeasures unsuited for MFS STS. The framework seeks to close the existing gap by taking into cognisance the dynamic social interactions within the STS and the existence of trusted and untrusted elements, to build controls that while mitigating undesirable actions by untrusted elements, is flexible enough to encourage desirable actions by trusted elements.

The framework will analyse and provide an understanding of the risk(s) inherent in the process flows and components within the STS. It will then provide guidelines for putting in place appropriate control(s) to mitigate the risk(s). Furthermore, due to the dynamic nature of the risk(s) envisaged, guidelines for the adequate compensating controls to be deployed will be included in the framework. The controls will be flexible enough to adapt to changes in information flow and social interactions.

The resilient nature of the framework is derived from the availability of compensating controls that can adapt to changes in the environment.

The next section describes the approach for developing the framework.

III. APPROACH ADOPTED FOR DEVELOPING SOLUTION

The MFS STS is an ill-defined problem space. Therefore, in coming up with an approach to develop a resilient framework for cybersecurity it was imperative to identify key stakeholders, analyse trusted and untrusted entities in the STS, understand flow of information and develop requirement for a resilient solution.

To achieve these, a 5 prong systematic approach was adopted that focused on defining the problem space before attempting to proffer solution. We describe the phases of the approach below.

A. AS-IS ANALYSIS.

In this phase best practices and literatures would be examined with a view to understanding the current state of play as it regards MFS. Due to the importance of the human element in building resilient controls, literature on human factors approaches and how they can improve cybersecurity would also be investigated. Best practices in capability maturity would be investigated with a view to understanding the most effective approach to gathering requirements for developing a robust framework. Lastly, the nature of information flow within the system would be investigated; this would help in building controls that would improve information assurance within the system. The major outcome of this phase would be a better understanding of the state of play in MFS, cybersecurity issues in MFS, human factors approaches, capability maturity approaches and best practices in information assurance.

B. REQUIREMENT

Requirement for building the cybersecurity framework would be developed in this phase based on the understanding of the MFS. Requirement management techniques like Use Case and MosCow would be used alongside human factor approaches like Soft System Methodology (SSM) and Interactive Management (IM) techniques to elicit requirement for developing the framework. Other methods for analysing complex systems as identified from the “As-Is” phase would also be applied to build the requirements as the need arises.

C. FRAMEWORK DEVELOPMENT

Solution architecture and technology governance frameworks like The Open Group Architecture Framework (TOGAF) and Control OBjectives for Information and related Technology (COBIT) alongside proprietary information assurance frameworks would be used to build an integrated framework, based on the requirement gathered in the previous phase.

D. TESTING

The developed framework would then be tested via focused group workshops and peer reviews. The workshops would seek to validate the framework. The framework would then be refined to reflect improvements.

E. APPLICATION

The tested framework would be applied to the unbanked. Policies procedures and guidelines would be applied to address specific requirements for cybersecurity that would facilitate the uptake of MFS by the unbanked.

Fig 2 shows the flow of activities for developing the framework.

The proposed approach was derived from best practices and review of relevant literatures. The approach would be refined as the need arises during the course of the research.

IV. Research Design and Preliminary Results of Work Undertaken

This section highlights some preliminary findings based on the work done so far.

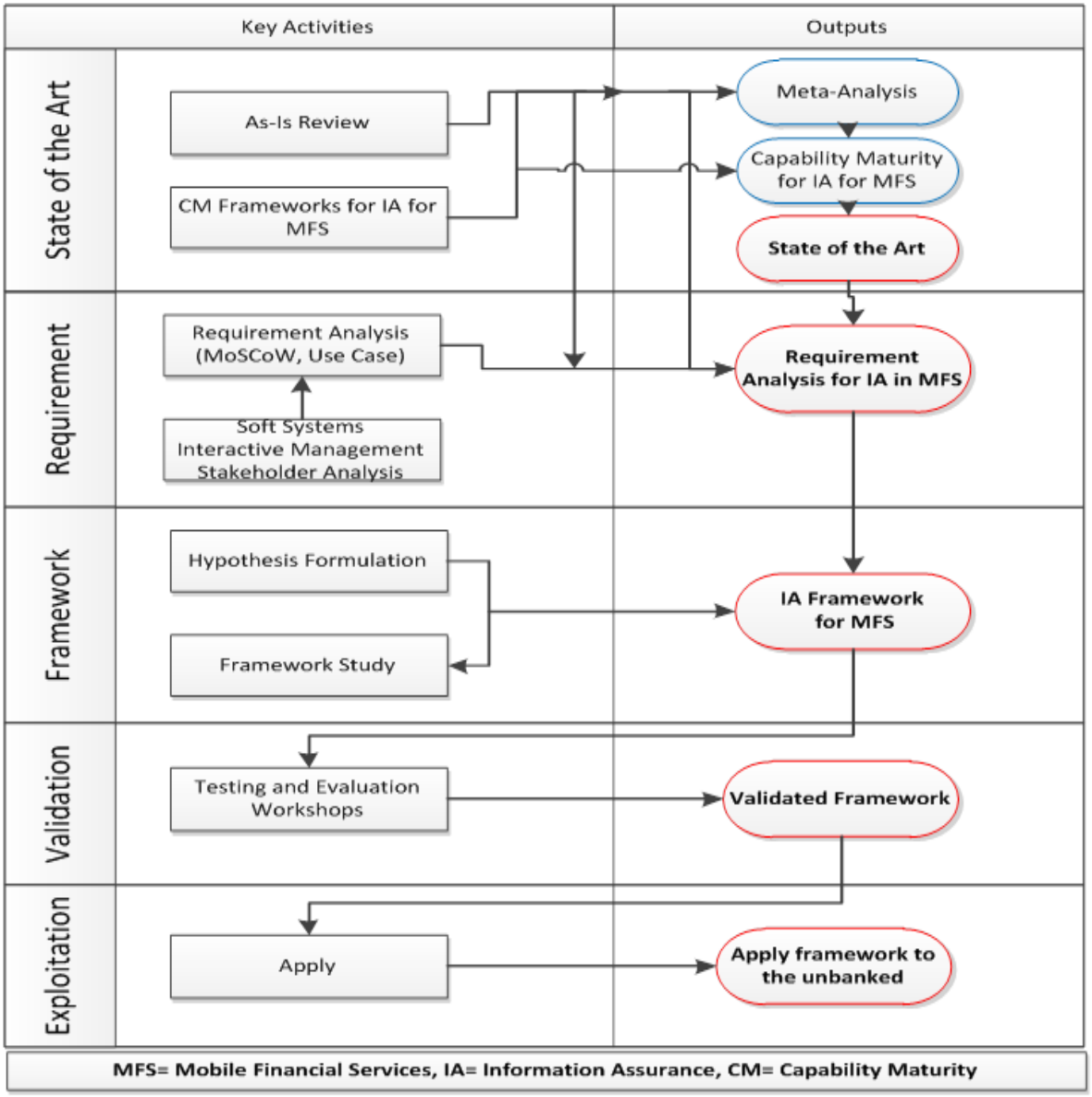

Fig. 2. Flow of activities

One of the key findings of the literature review conducted was the importance of the human element in building a robust solution. Some of the existing technical countermeasures have not been effective due to the neglect of this important factor. Consequently, we investigated human elements and cybersecurity issues in the MFS STS.

A. RESEARCH DESIGN FOR HUMAN ELEMENTS AND CYBERSECURITY ISSUES IN MFS STS

The objective of this task was to analyse the human element and cybersecurity issues in the MFS STS from the perspective of the stakeholders in the STS, so as to gain better understanding of what it entails to develop controls and countermeasures that would be all-encompassing and easily applicable by the stakeholders.

6 workshops were conducted for a total of 30 stakeholders; with each group consisting of 5 stakeholders. The 5 stakeholder groups comprised of the following:

(i) Financial Services Regulators: This group was comprised of Deposit Money Banks and MFS regulators.
(ii) Bank: Participants that made up this group were drawn from e-business units of Deposit Money Banks.
(iii) Unbanked: All participants in this group had no form of bank account.
(iv) Banked: All participants had formal bank accounts; some were user of MFS products.
(v) Service Provider: The group consisted of technology service providers.
(vi) CERT: This group was comprised of cybersecurity experts.

TABLE I. JUSTIFICATION FOR HUMAN FACTOR APPROACHES USED.

SN	Approach	Technique	Justification
1	Soft Systems	Rich Picture	Provided understanding of ill-defined problem space from stakeholder view point
2		Root Definition and Conceptual Model	Provided understand in on various stakeholder world views and key requirements for security concerns in the ecosystem
3	Interactive Management	Idea Writing	Used to generate ideas by brain storming on human factor related cyber security challenges in the problem space. The technique helped in avoiding a situation where early focus would be on the solution before a proper understanding of the problems
4		Nominal Group Technique	Provided an understanding of key objectives of mitigating challenges identified.
5		Interpretive Structural Modelling (ISM)	Linked objectives to determine relationships and influences

We adopted human factors approaches to achieve this objective. Human factors techniques have been known to help in defining ill-defined complex problem spaces similar to the MFS STS. For instance, Dogan et al., [37] used Human factors approaches to capture requirements for Knowledge Management research within the aerospace and defense industry.

Human factors techniques have also be used to guide the analyses of problems without early focus on solution. In a research conducted to understand the use of Human factors techniques in practice, it was discovered that most people use Human factors techniques to gain an understanding of a problem environment and to ease the understanding of problems [38].

The objective of the workshops was to gain understanding of the human elements and cybersecurity issues from stakeholder perspective and how to mitigate them.

To ensure effective participation, each workshop session started by a clarification of workshop objectives and a presentation on human factors approach and MFS. The procedure for the workshop was also described to participants. The tasks commenced by asking each group to come up with a rich picture depicting their understanding of the STS. Rich pictures are free sketches show interaction within the components of the system, including information flow [29]. They then built conceptual models representing their understanding of requirements for building cybersecurity in the STS. Rich picture and conceptual models are Soft System Methodology techniques.

Soft Systems Methodology (SSM) developed by Peter Checkland is an action oriented approach for analysing ill-defined problem spaces of complex systems [29]. Interactive Management (IM) techniques; Idea Writing (IW), Nominal Group Techniques (NGT) and Interpretive Structural Modelling (ISM), were used to generate issues and objectives for mitigating them, and how they influenced each other. Interactive Management techqnues are group decision making techniques suited for analysing complex environments [30].

Table 1 provides justification for the approaches used.

Semi-structured interviews were conducted to validate the outcome of the research. Experts in the workshop had an average of 18 years in Information Technology and related disciplines, and had also participated in implementing information security programs for organisations.

B. PRELIMINARY RESULTS

The understanding of the STS depends on the world view of the stakeholders. While the Bank is the ultimate regulator from the view point of the unbanked, the CERT group views international security enforcement agencies as stakeholders in the STS. Unknown stakeholders whose characteristics need to be understood exist in the ecosystem. To analyse the environment, we built the MFS STS. *Fig 3* below shows the consolidated SSM from all stakeholder groups depicting the STS.

The principal in the ecosystem that serves in the capacity of bank agents is responsible for user registration for MFS products. Special care needs to be taken by the principal when registering users as mistakes in user registrations can be exploited to perpetuate fraud. Agents might also have float; availability of physical or electronic money issues. They may not have enough money when customers need to cash-out. The proximity of agents to banks could also delay the restocking of cash, creating a gap for e-float supply.

Banks do not operate beyond normal business hours, so do the principals. Hence, some functionality of MFS that requires input from the Bank, e.g. cash-in can only be accessed during normal banking hours. Other functionalities like money transfers and online payments can be achieved at any time of the day.

Poor network connectivity in the use of MFS leads to poor customer experience which has further affected trust in the use of MFS products. The 2 key regulators in the ecosystem are the Financial Services (FS) regulator and the telecommunications (telco) regulators.

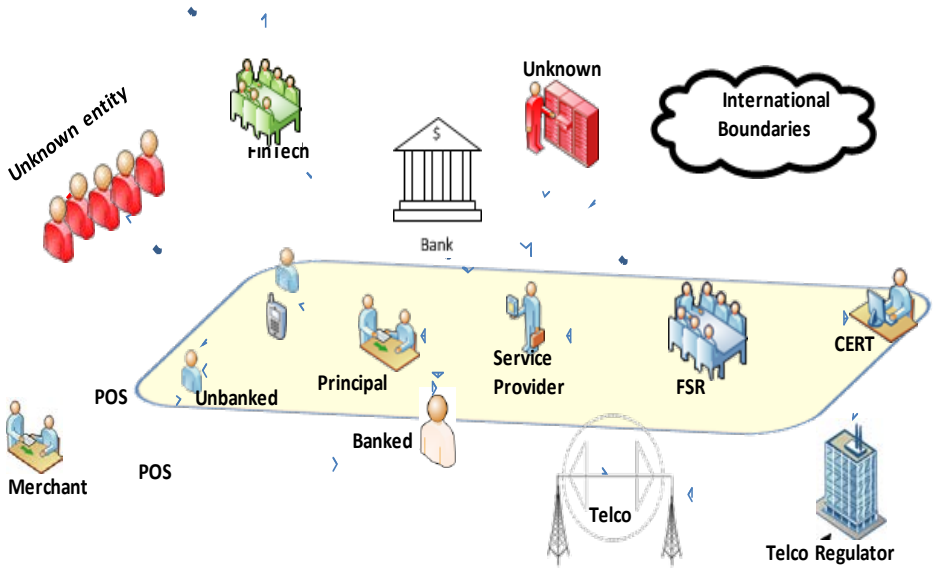

Fig. 3. MFS STS (*Banked: Bank accounts owners, Unbanked: No bank account, Principal: Mobile Money Operator, FS R= Financial Services Regulator CERT: Authorities responsible for cyber-incident management, POS: Point of Sale)*

The objectives of the regulators differ. While the FS regulator is concerned with the delivery of financial services, the telco regulator is primarily concerned with the quality of communication services. Collaboration between these regulators is essential, in order to effectively manage performance and ensure compliance within the STS.

TABLE II. TOP OBJECTIVES FOR MITIGATING CYBERSECURITY.

SN	Objectives
1	Setup an industry wide cybersecurity operations centre (O1)
2	Mitigate risks associated with poor infrastructure (e.g. power, internet, technology) (O2)
3	Implement robust awareness program on social engineering for users (O3)
4	Enforce segregation of duty in Banks to minimize possibility of insider abuse(O4)
5	Improve awareness on technology and information security(O5)
6	Understand familiar phone hackers' mode of operation(O6)
7	Understand the security put in place for MFS to improve trust in the process(O7)
8	Be open to change (O8)
9	Revise current cybersecurity act with input from all key stakeholders(O9)
10	Develop capacity building program on cybersecurity for all key players (O10)
11	Ensure adequate investment in cybersecurity is imbedded in the strategy of service providers (O11)
12	Ensure every service provider has a Business Continuity strategy (O12)

The method of implementation of MFS varies. For instance, telcos are in the forefront of implementation of MFS in Kenya. FS regulator leads the implementation in some jurisdictions e.g. Nigeria. Payment services providers are also in the lead in some markets. The method of implementation of MFS in any jurisdiction has consequences for regulation and cybersecurity in the STS.

38 out of the 269 issues generated were by the Deposit Money Bank (DMB) participants. The group viewed all issues impacting cybersecurity in the ecosystem in 4 broad categories that included awareness, infrastructure, process and others. Issues raised under others include, the rise in mobile malware and the threat of insider abuse. Trade-off between user experience and mobile application security was also identified as a threat impacting the STS. To encourage adoption, Mobile Money operators have implemented very minimal Know Your Customer (KYC) requirement. The regulator group fears this could be exploited for fraudulent purposes. The regulator group also expressed concern on the lack of skills of the regulators to develop and enforce standards for cybersecurity within the MFS STS.

Due to legal and regulatory differences between jurisdictions, it was noted that international money transfer capability using MFS might be an avenue for money laundering and terrorism financing.

User awareness, either on technology, security or consumer protection process was an objective that recurred amongst all groups. However, responsibility for user awareness was not clearly understood within the ecosystem. While some participants expect users to educate themselves, others expect the bank and service providers to be responsible for end-user education on cybersecurity.

Participants also observed that most providers of MFS products do not have dedicated help desk for cybersecurity. Cybersecurity concerns were treated like every other customer concerns. Furthermore, participants also observed that even when successfully reported incidences of cybercrime take a long time to be completely investigated, if they are ever concluded at all. Customers also noted that most of the investigations conducted end up with advicing users to be more security conscious in the use of the products. The lack of urgency in treating customer concerns relating to cyber fraud and the inability to satisfactorily close issues raised have further affected trust in the use of MFS.

To address the issues raised, participants came up with a prioritised list of objectives. These objectives when applied in the opinion of the participants would mitigate the threat of cybercrime in the complex MFS STS. Table 2 shows the top 12 objectives generated by all 6 groups.

While the regulators saw implementing a cybersecurity operations centre as the most important objective for mitigating cybersecurity in the MFS STS, the banks view user awareness as the most important. The unbanked believed an improved understanding of the basic use of technology and cybersecurity threats would help mitigate against the threat of cybercrime. According to the unbanked, clarity of the process for escalating fraud issues was an important countermeasure cybercrime.

The output of the ISM from the workshops showed that objective O1 was the most influential objective. Subject Matter Experts (SMEs) were concerns about how to balance the need for implementing countermeasures and the availability of financial and material resources.

Similar to when generating issues that affected cybersecurity in the complex MFS STS, perspectives of stakeholders and their understanding of cybersecurity requirements in the ecosystem also came into to play when ranking objectives for mitigating cybersecurity.

In addition to an industry wide security operations centre, the regulators gave equal importance to ensuring that banks provide appropriate oversight to MFS agents and mitigating

the risk associated with poor infrastructure, which included sustainable energy supply and internet infrastructure.

Providing a robust awareness program on social engineering along with segregation of duty to mitigate the risks of cybercrime and improving service availability were the main preoccupation of banks and their agents.

The CERT group which was more interested in how to obtain and share intelligence was concerned about ensuring that legal frameworks for managing cybersecurity in the MFS were regularly updated to reflect changes in the ecosystem and the legal and regulatory environment as a whole.

The CERT group recognised that there was no one-size-fit-all solution to cybersecurity awareness and were interested in developing a cybersecurity awareness program specifically tailored to the needs of key stakeholders in the space.

Generating and ranking objectives by participants in each group was based on NGT which had a voting process. However, consolidating all objectives from the groups was more challenging. By consensus, the participants agreed to consider the top 2 objectives in each group as the most important, after which the objectives were linked.

The *fig 4* shows the ISM result showing how the 12 listed top objectives for mitigating cybercrime in the MFS STS influence each other.

It was observed that some objectives might impact on one or more of the other objectives. For instance, implementing a robust awareness program would facilitate improved security awareness for all key stakeholders. Updating cybersecurity regulations might require service providers to improve their Business Continuity capability.

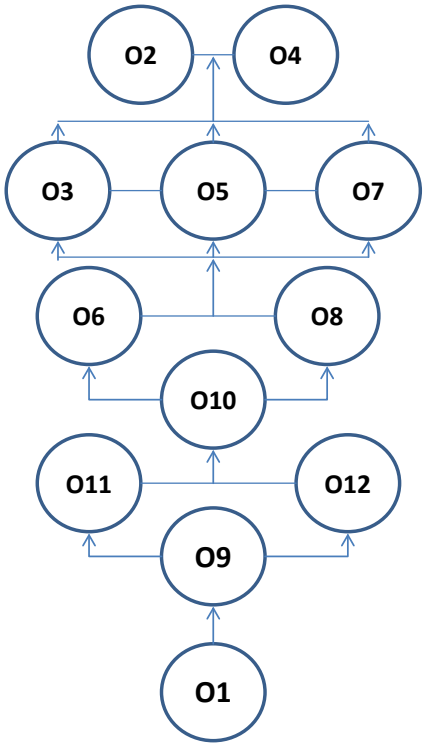

Fig. 4 ISM model showing relationship between objectives

Feedback obtained from the semi-structured interviews with SMEs included the following:

(i) Financial intermediaries and settlement companies should be treated as separate stakeholders and not lumped under service providers as they play critical roles in MFS.

(ii) To mitigate the risks affecting information flow within the ecosystem, it was suggested that technologies that manage partial commits due to infrastructure (Internet, power) failure should be implemented.

(iii) To improve forensic investigation, implementation of software interfaces with forensic capabilities was recommended.

(iv) Hardening of the user interface without compromising usability was also suggested.

(v) In view of the huge cost consideration for implementing countermeasures. A shared services approach was recommended.

(vi) To mitigate the risk of vulnerabilities with WI-FI, it was suggested that mobile applications with the capability to identify malicious WI-FI accesses should be deployed.

(vii) It was also suggested that mobile applications should have the capability to disconnect automatically if the device is not appropriately patched and updated.

(viii) Due to the vulnerability associated with human elements, it was suggested that banks should have a 24/7 customer care centre to respond to cybercrime incidences.

(ix) It was suggested that socio-cultural issues like myth and belief should be considered in coming up with a solution to mitigate the threat of cybercrime.

(x) It was recommended that a legal framework which supports the unique operation of the MFS STS should be developed.

Most of the feedback received from experts advocated strengthening of technical controls, improving user awareness and consideration for human factors and process workflow as a precursor for building a resilient cybersecurity countermeasure for the MFS STS.

The feedback from the experts generally aligns with the issues raised in the IM workshops and the objectives recommended for mitigating cybersecurity issues in the complex MFS STS.

V. SUMMARY AND NEXT STEPS

Lack of trust has slowed down the adoption of MFS products in spite of its inherent benefits. Cybercrime was a major issue responsible for lack of trust in MFS. Existing countermeasures for mitigating the threat of cybersecurity have not succeeded in reducing incidences of cybercrime and improving trust in the MFS.

To have a better understanding of the benefits of MFS and the threat posed by cybercrime on its adoption, an in-depth analysis of MFS and the ecosystem it operates was conducted. The MFS STS is a complex ecosystem. In building a resilient framework for cybersecurity in the complex MFS STS, the complex nature of the STS and the nature of social interaction within the system, should be considered.

The technology underpinning MFS facilitates the attainment of objectives of stakeholders in the MFS STS. However, vulnerabilities in the technology are exploited by untrusted elements in the STS to commit cybercrime. An analysis of the technological landscape provided more insight into these vulnerabilities and how they could be addressed.

Existing countermeasures for mitigating the threat of cybercrime in MFS was examined. Though these countermeasures have enhanced the security of MFS, issues around data privacy, mobile forensic, information assurance and human elements still exist.

A resilient cybersecurity framework as a control against cybersecurity threat in the MFS STS was proposed. The solution will be developed through a 5-pronged approach focusing on analysing the ill-defined problem space, understanding trusted and untrusted elements in the MFS STS, developing the requirement for building the framework and developing a framework based on solution architecture, IT governance and information assurance frameworks.

Based on preliminary work conducted, an understanding of the stakeholders and components of the MFS STS and how components interact within the system were presented. We also identified unknown stakeholders that interact within the STS. Service providers were crucial as they could become a single point of failure within the STS.

We generated 269 cybersecurity issues in the MFS STS using human factors approaches. We also identified 30 objectives of how to mitigate these issues. We used the ISM technique to provide an understanding of the relationship and influences within identified objectives.

Most of the feedbacks obtained from experts during the semi-structured interviews conducted, advocated strengthening of technical controls, improving user awareness and consideration for the human element and process workflow as a precursor to building a resilient cybersecurity countermeasure for the MFS STS.

The need to further analyse the MFS STS with a view to understanding the trusted and untrusted elements was identified. Also, the need to identify mobile applications with high level of uptake with the view to determining the usability patterns and usability aesthetics that facilitated their uptake was also identified.

Future work would aim to investigate issues affecting trust in MFS in Mobile Social Networks (MSN) and how a trust model for the MFS STS would be applied to improve trust in the MSN. Usability and security characteristics of mobile applications with high uptake would also be examined, with a view to understanding characteristics and aesthetics of mobile applications that could be applied to MFS application to improve their uptake.

REFERENCES

[1] InnoVentures, S. and Wyman, O., the Anthemis Group.2015, The Fintech 2.0 Paper: Rebooting financial services

[2] The World Street Journal, 2016. Swift Reports Summer Cyber Attacks on Three Banks. Retrieved October 9, 2016 from http://www.wsj.com/articles/swift-reports-summer-cyber-attacks-on-three-banks-1474924036

[3] Albasheer, M.O. and Bashier, E.B., 2013, August. Enhanced model for PKI certificate validation in the mobile banking. In Computing, Electrical and Electronics Engineering (ICCEEE), 2013 International Conference on (pp. 470-476). IEEE

[4] Ahamad, S.S., Sastry, V.N. and Nair, M., 2013, September. A Biometric based Secure Mobile Payment Framework. In Computer and Communication Technology (ICCCT), 2013 4th International Conference on (pp. 239-246). IEEE.

[5] Narendiran, C., Rabara, S.A. and Rajendran, N., 2009, October. Public key infrastructure for mobile banking security. In Global Mobile Congress 2009 (pp. 1-6). IEEE

[6] Emerging Technologies, PCI Security Standards Council, 2014. PCI Mobile Payment Acceptance Security Guidelines for Merchants as End-Users

[7] The World Economic Forum 2016. The Global Risk Report 2016, 11th Edition. Retrieved October 4, 2016. https://www.weforum.org/reports/the-global-risks-report-2016/

[8] World Bank 2015. Global Findex, 2014, Financial Inclusion. Retrieved September 3, 2016,from http://datatopics.worldbank.org/financialinclusion/Infographics

[9] ITU 2015. The world in 2015: ICT facts and figures , Retrieved September 19, 2016, from https://www.itu.int/en/ITU D/Statistics/Documents/facts/ICTFactsFigures2015.pdf

[10] ISACA 2015. Mobile Payment Security Study Global Results. Retrieved August 25, 2016.from www.isaca.org/mobile-payment-security-study.

[11] Valcke, J. 2016. Best practices in mobile security, Biometric Technology Today, Volume 2016, Issue 3, March 2016, Pages 9–11

[12] Malaquias, R.F. and Hwang, Y., 2016. An empirical study on trust in mobile banking: A developing country perspective. *Computers in Human Behavior*, *54*, pp.453-461.

[13] Carin, L., Cybenko, G. and Hughes, J., 2008. Cybersecurity strategies: The queries methodology. Computer, 41(8), pp.20-26

[14] Donovan, K., 2012. Mobile money for financial inclusion. Information and Communications for Development, 61, pp.61-73

[15] Donner, J., 2007, May. M-banking and m-payments services in the developing world: complements or substitutes for trust and social capital. In Preconference on Mobile Communication at the 57th Annual Conference of the Int. Communication Association

[16] Shin, D.H., 2009. Towards an understanding of the consumer acceptance of mobile wallet. *Computers in Human Behavior*, *25*(6), pp.1343-1354.

[17] Security Intelligence, 2016. Know your enemy, understand the motivation behind cyber-attacks. Retrieved October 11, 2016 from,https://securityintelligence.com/know-your-enemy-understanding-the-motivation-behind-cyberattacks/

[18] ENISA ,2016. ENISA Threat Landscape 2015. European Union Agency For Network And Information Security.

[19] NIST, 2016. National Institute of Standards and Technology, Retrieved October 11, 2016 from, https://www.nist.gov/publications

[20] Hayashi, F., 2012. Mobile payments: what's in it for consumers?. *Economic Review-Federal Reserve Bank of Kansas City*, p.35.

[21] Nyamtiga, B.W., Sam, A. and Laizer, L.S., 2013. Security Perspectives for USSD versus SMS in conducting mobile transactions: A case study of Tanzania. *international journal of technology enhancements and emerging engineering research*, *1*(3), pp.38-43.

[22] Jain, A.K. and Shanbhag, D., 2012. Addressing Security and Privacy Risks in Mobile Applications. *IT Professional*, *14*(5), pp.28-33.

[23] Techtarget, 2016. Overcoming Common Mobile Data Security Hurdles

[24] Boyles, J.L., Smith, A. and Madden, M., 2012. Privacy and data management on mobile devices. *Pew Internet & American Life Project*, *4*.

[25] Ponemon Institute Research, 2015. Report on The State of Mobile Application Insecurity., Sponsored by IBM Independently conducted by Ponemon Institute LLC Publication Date: February 2015

[26] Gov. UK, 2016. Data Protection Act 1998, Retrieved October 11, 2016 from http://www.legislation.gov.uk/ukpga/1998/29/contents

[27] Brad Casey , 2015. Top 3 Wi-Fi Security Vulnerabilities. Retrieved June 5 2016, from https://www.techopedia.com/2/28536/networks/wireless/top-3-wi-fi-security-vulnerabilities

[28] Carin, L., Cybenko, G. and Hughes, J., 2008. Cybersecurity strategies: The queries methodology. Computer, 41(8), pp.20-26

[29] Checkland, P. 1981. Systems thinking, systems practice.

[30] Broome, B. J., & Keever, D. B. 1986. Facilitating Group Communication: The Interactive Management Approach.

[31] Whitworth, B. 2006. Socio-technical systems. Encyclopaedia of human computer interaction, 533-541.

[32] Gov.uk., 2016. Cabinet Office, Government Communications Headquarters , New National Cyber Security Centre set to bring UK expertise together, Retrieved 15 October, 2016 from https://www.gov.uk/government/news/new-national-cyber-security-centre-set-to-bring-uk-expertise-together

[33] Fireeye, 2015, Special Report Out of Pocket: A Comprehensive Mobile Threat Assessment of 7 Million iOS and Android Apps. Retrieved October, 15 2016, from https://www2.fireeye.com/rs/fireye/images/rpt-mobile-threat-assessment.pdf

[34] RSA, 2016: Current State of Cybercrime, Retrieved October, 15 2016, from https://www.rsa.com/content/dam/rsa/PDF/2016/05/2016-current-state-of-cybercrime.pdf

[35] Smith, C.L., 2003, October. Understanding concepts in the defence in depth strategy. In *Security Technology, 2003. Proceedings. IEEE 37th Annual 2003 International Carnahan Conference on* (pp. 8-16). IEEE.

[36] Ambore, S. Richardson, C. Dogan,H, Apeh,E. Osselton, D. 2016. A “Soft” Approach to Analysing Mobile Financial Services Socio-Technical Systems. Proceedings of British HCI 2016.

[37] Dogan, H., Henshaw, M. and Urwin, E., 2009. A ‘Soft’Approach to Requirements Capture to Support Through-Life Management.

[38] Mingers, J. and Taylor, S., 1992. The use of soft systems methodology in practice. *Journal of the Operational Research Society*, *43*(4), pp.321-332.