Development of Human Factors and Cybersecurity Objectives for Mobile Financial Service (MFS)

Stephen AMBORE, Edward APEH, Huseyin DOGAN, Christopher RICHARDSON, and David OSSELTON

Bournemouth University, UK

Abstract. Cybercrime is slowing down the adoption of Mobile Financial Service (MFS). Despite the existence of a strong technical infrastructure base for security and the benefits inherent in MFS, adoption has been slow. Highly resilient countermeasures for cybersecurity go beyond just providing technological controls to put in place measures to cater for the human element. This paper presents the findings of an analysis of the human factors issues in complex MFS Socio-Technical System (STS) and the objectives for mitigating these.

Keywords. Cybersecurity, Human Factors, Trust, Socio-Technical Systems.

1. Introduction

Cybercrime has increased over the years with profound financial and economic impacts on countries, organizations and individuals. It is estimated that the cost of data breaches due to cybercrime will reach $2.1 trillion by 2019 (Juniper, 2016). Recent events have demonstrated how widespread and disruptive cybercrime has become, with financial gain as the highest motivation (ISACA, 2015). Advances in mobile and network technologies have however presented unprecedented opportunities to develop and provide services. For instance, with over 97% penetration rate (ITU, 2015), mobile phones have the capability to provide financial services to about 2 billion of the world's population that hitherto had no access to formal financial services (World Bank, 2015). However, this advance has provided another vector for cybercrime which is threatening to erode these gains.

Despite this risk, most banks have adopted mobile platform based financial products to drive down costs and improve competitive advantage (Valcke, 2016). Due to the benefit gained from mobile and network services, banks are now more incentivised to move their key operations from conventional "brick and mortar" to the cyber space. This move has been further strengthened by the development of a strong technical infrastructure base for secure electronic financial transactions. These include: strong key encryption and tokenization technologies, high speed internet, and improved threat intelligence capability (ENISA, 2016).

Despite the existence of this strong technical infrastructure base for secure electronic financial transactions, adoption of MFS products by consumers has been low, due to lack of trust (Malaquias, 2016). For instance, in recent research conducted on Mobile Payment adoption, 87% of the respondents expected there could be a data breach to Mobile Payment. Also, Mobile Payment was judged by respondents to be the least secure method of payment compared to other payment methods like cash, cheques, credit cards and money order (ISACA, 2015).

The human element has been described as the "weakest" link in information security (Sasse et al., 2001, West et al., 2008). The action, inaction, experience and perception of the human element in the use of MFS products has created a lack of trust which has slowed down the adoption of MFS (Kraemer et al., 2009). The lack of balance between usability and security (Adams and Sasse, 1999), concerns around privacy of customer data, information assurance

and poor mobile forensic capability have all contributed to this.

In cybersecurity, the human element is also a potential target for attacks and can unwittingly participate in a cyber-attack (VonSolms and VanNiekerk, 2013). So highly resilient countermeasures for cybersecurity now go beyond providing technological controls to also putting in place measures to cater for the human element. However, the complex interactions between the human element and technology in an STS make the design of such countermeasures very challenging. While a lot of work has been conducted on analysing the human element in STS (Cooper et al., 1996, Kraemer et al., 2003, Barfield, 2014), no known research has analysed cybersecurity issues from the perspective of the human element in the MFS STS.

This paper presents results obtained from analysing the complex MFS STS using human factors approaches such as Soft System Methodology (SSM) and Interactive Management (IM). The objective of this paper is to gain an understanding of the human element issues that affect cybersecurity in the MFS STS and to develop objectives for how to mitigate them.

The next section presents a background overview of MFS STS along with a literature review. Section 2 describes the methods used in conducting the research. Section 3 provides a summary of key findings of the research. The paper concludes in section 4 by further discussing the research and providing direction for further studies.

1.1 Mobile Financial Services Socio-Technical Systems (MFS STS)

STS are a combination of social and technical systems (Cooper, et al., 1996, Whitworth, 2006). They depict complex interactions that cut across organisations and at times, national boundaries. Using examples from healthcare (Cucciniello et al., 2015) and traditional computer and information security and system design (Carayon, 2006), it has been argued that working across these boundaries increases complexity of interaction within the system.

Complex systems can be identified by how components interact within the system and how they may or may not be analysed. Examples include ecosystems and the web etc. (Ottino, 2004). MFS STS is a complex system which consists of, among others: bank account holders, people without access to formal financial services, unbanked, Mobile Money operators, Mobile Payment service providers, financial services and telecommunications regulators, financial settlement and other utilities companies. Unknown entities also exist within the STS (Ambore et al., 2016) so the MFS ecosystem is an ill-defined problem space comprising trusted and untrusted entities. The right approach to analyse the MFS STS must be both suited to analysing the ill-defined problem space and be simple enough to enable the participation of STS stakeholders in the analysis.

A framework for analyzing complex systems based on linguistic variables and fuzzy algorithm has been developed (Zadeh, 1973). Though the framework can be applied to ill-defined problem space, the reliance on human elements for the execution of fuzzy algorithms makes it poorly suited for analysing MFS STS. Other methods such as Cognitive Work Analysis (Naikar et al., 2006) and Human Factors Analysis and Classification Framework (Jennings, 2008) have been proposed for analysing complex systems. However, none of them can successfully analyse an ill-defined problem space like the MFS STS from the perspective of its stakeholders.

Soft Systems Methodology (SSM) developed by Peter Checkland is an action-oriented approach to analysing ill-defined problem spaces of complex systems (Checkland, 1981,

Checkland and Poulter, 2010). Interactive Management (IM) includes a technique called Interpretive Structural Model (ISM). These are group decision-making techniques suited for analysing complex environments (Broome and Keever, 1986). Combining Human Factor approaches like SSM, IM and ISM to analyse the complex MFS STS closes the gaps presented by other approaches as they include techniques that can be used to analyse the system from the STS stakeholders' perspectives.

2. Methods

Techniques from SSM and IM were applied in a systematic way to analyse the human element and cybersecurity issues in the MFS STS. Six workshops were conducted. The workshops were preferred to questionnaires because they provided a face-to-face opportunity for the clarification of workshop objectives and to educate participants on key concepts in human factors and STS in an interactive manner. The procedure used to analyse the MFS STS is detailed in the next subsection.

2.1 Procedure

The procedure adopted in analysing the MFS STS consisted of 5 key actions applied in 5 phases using appropriate human factors' techniques, as described below:

I. Phase 1

The objective of this phase was to provide an understanding of the elements of the MFS STS and their interactions. This provided consensus on the definition of the problem space without an early focus on solutions. Rich Picture and Conceptual Model techniques from SSM were used (Checkland et al., 2010). These were preferred to others like Persona and Interviews due to the strength of their approach in providing insight into ill-defined problem spaces from a stakeholder perspective.

Each of the 6 workshop groups sketched a Rich Picture and developed a conceptual model based on their own understanding of the MFS STS. The major output of this phase was the consolidated SSM view of the environment.

II. Phase 2

The IM approach was used to generate the issues impacting cybersecurity in the MFS STS. IM was preferred because it has techniques like Idea Writing (IW) and Nominal Group Technique (NGT) which can generate and rank ideas, and facilitate stakeholder participation. IW was the specific technique used in this phase. The output of this phase was a categorised list of issues from stakeholders in the MF STS.

III. Phase 3

Stakeholders generated objectives for mitigating the concerns raised through brainstorming. These objectives were refined to make them Simple, Measurable, Achievable, Realistic and Time Bound (SMART). Stakeholders then used NGT to prioritise the objectives and produce alist.

IV. Phase 4

In this phase, relationships and influences between the objectives were identified. ISM was used in preference to mind maps because it provides a systematic way of identifying interdependences and influences between objectives. The final output of this phase was an influence diagram of objectives depicted in an ISM model.

In summary, the IM workshops conducted followed the steps below:

A. Human element related issues impacting cybersecurity in the MFS STS were generated in a round-robin way using IW. These issues were then grouped based on similarities. A trigger question was used to kick-start the process.

B. Objectives for mitigating the issues raised were then generated using NGT. The process for NGT was similar to that of IW, except that NGT included a voting process to facilitate prioritisation.

C. Lastly, influences and interdependences between objectives were then determined using ISM.

V. Phase 5

The final phase involved an independent validation of the output by Subject Matter Experts (SME). Although semi-structured interviews were used, focus group workshops can also achieve the same objective and these would be used in future work. SMEs selected to participate in the interviews had an average work experience of 18 years in IT and related roles, and all had experience in deploying Information Security programs in organisations. Five experts were interviewed in the validation phase. The figure below shows flow of activities of the work undertaken.

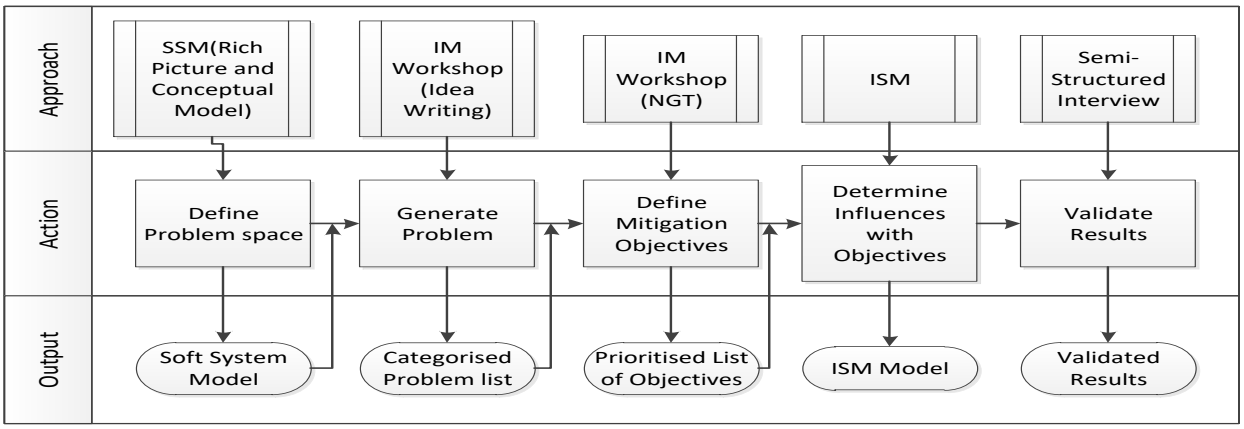

Figure 1.0 Flow of activities.

3. Results

3.1 System Systems Model (SSM) Result

The perspective of each stakeholder group affects their understanding of the MFS STS and the human and cybersecurity issues in the STS. This was reflected in the SSM. While the regulator is primarily concerned with how to develop and implement a strategy to mitigate cybercrime, Deposit Money Banks were more focused on delivering effective user awareness on cybersecurity. The figure below is the Rich Picture produced by the "Banked" group which shows interactions within components of the MFS STS from the perspective of bank customers. The red lines show suspicious interaction while dotted lines depict communication outside the boundaries of the system.

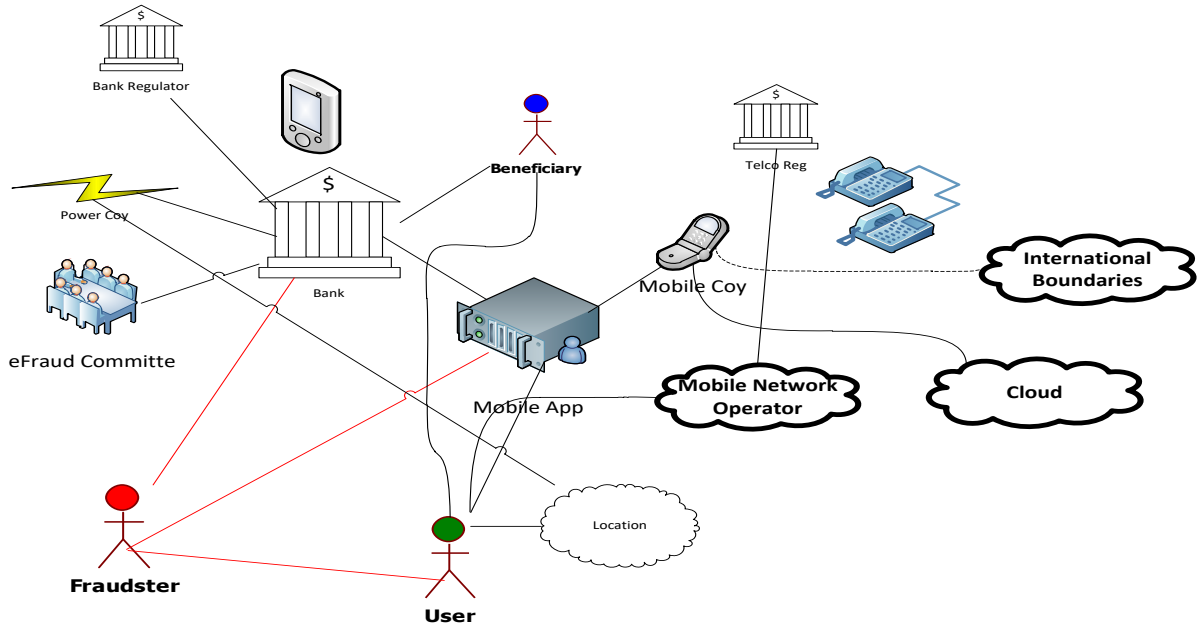

Figure 2.0 Rich Picture result for "Banked" group.

3.2 Interactive Management (IM) Workshop Result

Roles and responsibilities in the MFS STS were not well understood by stakeholders in the MFS STS. While the "Unbanked" group considered banks responsible for security awareness, the "Banked" group saw it as the responsibility of regulators. For instance, the most important objective for mitigating cybercrime in the MFS STS according to the "Financial Services Regulator" group was the development of an industry-wide cybersecurity operations center. The Service Providers on the other hand, viewed having a business continuity plan in place as the most important objective. The figure below shows the output of NGT from the "Service Providers" group. Objective 3 with the highest vote of 17 was the most important objective according to the group.

SN	Objectives	P1	P2	P3	P4	P5	Total
1	Ensure every service provider has a business continuity strategy	3	4	2	3	4	16
2	Define minimum performance and availability level for all service providers	1	3	3	5	3	15
3	Ensure adequate investment in cybersecurity is imbedded in the strategy of service providers	2	5	1	4	5	17
4	Develop end-to-end process on complaint management	4	1	5	2	1	13
5	Educate client on cybersecurity	5	2	4	1	2	14

Table 1.0 NGT result from the "Service Provider" group.

3.3 Interpretive Structural Modelling (ISM) Result

The output of the ISM shows that the most pivotal objective for mitigating cybersecurity is setting up a cybersecurity operation center. The figure below shows the output of the ISM depicting how the top objectives from all groups relate to each other.

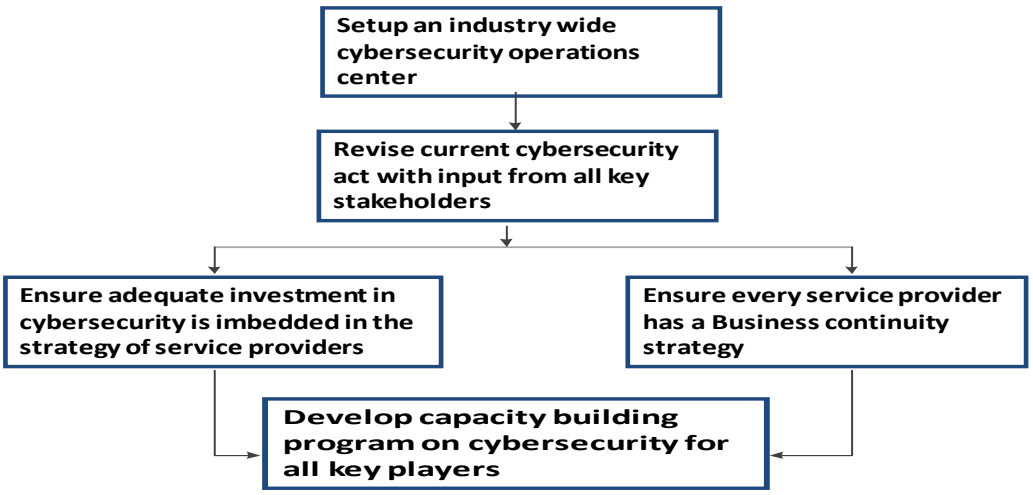

Figure 3.0 ISM workshop result, showing most influential objectives.

Stakeholders in MFS STS were grouped into 6 based on functions. The groups were:

I. Financial Services Regulators: This group was comprised of Deposit Money Banks and Mobile Payment regulators.
II. Banks: 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.

During the semi-structured interviews conducted to validate the result obtained, most experts that participated in the interviews believed the strengthening of technical countermeasures and proactive consideration for the human element in developing controls for cybersecurity, will go a long way to boosting cybersecurity for MFS STS.

4. Discussion and Conclusion

The paper presented findings of the analysis of human-related cybersecurity issues in MFS STS by using human factors' approaches. This has helped in the development of key objectives for mitigating cybersecurity concerns in the interactions between the complex infrastructures and human factors in the ecosystem for MFS STS. While users have different understandings of the requirements for improving security in the MFS STS, the approach used extracted and consolidated user requirements in a systematic way.

Furthermore, during one of the semi-structured interview sessions, it was suggested that understanding of the human factor issues will drive the right approach to designing countermeasures for mitigating cybersecurity. For instance, one of the issues identified by the users was the expectation on them to perform complex security tasks to ensure the security of their own transactions. Another issue identified was the lack of a purpose-built help desk for addressing cybersecurity issues for MFS users, especially given the urgency arising from the speed at which fraud can be committed. An objective proposed to address this amongst others was the setting up a cybersecurity operations center. It would provide a central authority that will immediately act to mitigate or minimize the impact of financial loss due to fraud. It would also provide intelligence on impending threats. One major feedback from the semi-

structured interviews was the need to prioritise the implementation of these objectives so as to focus on addressing the most pressing ones. This was to meet the challenge of limited financial resources to implement recommended changes.

To strengthen the capability of the existing technical countermeasures and procedures for mitigating cybercrime, we have shown that the human element should be analysed with a view to developing objectives for mitigating cybercrime. This was corroborated by SMEs participating in the semi-structured interviews to validate the results obtained. Human factors' approaches provided a way to analyse human elements that affect cybersecurity in the MFS STS and to develop objectives for mitigating them. Future work will focus on examining existing trust models to analyse trusted and untrusted elements in the complex MFS STS.

References

Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM*, *42*(12), 40-46.

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.

Barfield, W., & Dingus, T. A. (2014). *Human factors in intelligent transportation systems*. Psychology Press.

Broome, B. J., & Keever, D. B. (1986). Facilitating Group Communication: The Interactive Management Approach.

Carayon, P. (2006). Human factors of complex Socio-technical systems. Applied ergonomics, 37(4), 525-535.

Checkland, P. & Poulter, J. (2010). Soft Systems Methodology. In Systems approaches to managing change: A practical guide (pp. 191- 242). Springer London.

Checkland, P. (1981). Systems thinking, systems practice.

Cooper, J., Gencturk, N., & Lindley, R. A. (1996). A sociotechnical approach to smart card systems design: an Australian case study. Behaviour & Information Technology, 15(1), 3-13

Cucciniello, M., Lapsley, I., Nasi, G., & Pagliari, C. (2015). Understanding key factors affecting electronic medical record implementation: a sociotechnical approach. BMC health services research, 15(1), 1.

ENISA (2016). ENISA Threat Landscape 2015. European Union Agency For Network And Information Security. Page 11.

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

ISACA (2015). State of Cybersecurity: Implications for 2015, An ISACA and RSA Conference Survey. Retrieved October 3, 2016 from http://www.isaca.org/cyber/Documents.

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

Jennings, J. (2008). Human Factors Analysis & Classification Applying the Department of Defense System During Combat Operations In Iraq. *Professional Safety*, *53*(06).

Juniper Research (2016), Cybercrime will Cost Businesses Over $2 Trillion by 2019. Retrieved October 3, 2016 from http://www.juniperresearch.com/press/press-releases/

Kraemer,S., Carayon, P., & Clem, J. (2009). Human and organizational factors in computer and information security: Pathways to vulnerabilities. Computers & Security, 28(7), 509-520.

Malaquias, R. F., & Hwang, Y. (2016). An empirical study on trust in mobile banking: A developing country perspective. *Computers in Human Behavior*, *54*, 453-461.

Naikar, N., Moylan, A., & Pearce, B. (2006). Analysing activity in complex systems with

cognitive work analysis: concepts, guidelines and case study for control task analysis. *Theoretical Issues in Ergonomics Science*, *7*(4), 371-394.

Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security. BT technology journal, 19(3), 122-131.

Ottino, J. M. (2004). Engineering complex systems. *Nature*, *427*(6973), 399-399.

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

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. computers & security, 38, 97-102.

West, R., Mayhorn, C., Hardee, J., & Mendel, J. (2008). The Weakest Link: A Psychological Perspective on Why. Social and Human Elements of Information Security: Emerging Trends and Countermeasures: Emerging Trends and Countermeasures.

Whitworth, B. (2006). Socio-technical systems. Encyclopaedia of human computer interaction, 533-541.

Whitworth, B. (2009). The social requirements of technical systems. Handbook of research on socio-technical design and social networking systems, 3.

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

Zadeh, L. A. (1973). Outline of a new approach to the analysis of complex systems and decision processes. *IEEE Transactions on systems, Man, and Cybernetics*, (1), 28-44.