ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 8, Issue 3, pp: (284-290), Month: July - September 2020, Available at: www.researchpublish.com

ANALYSING THE CURRENT STATE OF INFORMATION SECURITY USING HUMANISTIC SECURITY CEREMONIES: A CASE OF SAUDI ARABIA

Norah Alyousif

Saudi Aramco, Dhahran, Saudi Arabia

Abstract: **Security Ceremonies enrich the concept of computer security by involving humans, as well as those individuals involved in creating security threats, and thus consider humanistic behaviours. Most of the current studies covers technical factors with the absence of human behaviour factor. Therefore, there is a need to better understand security ceremonies from a human perspective. This paper analysed the sociocultural aspects of security ceremonies in order to understand the interactions between humans and technology in regard to security protocols. A qualitative case study with the support of semi-structured interviews with twenty security professionals operating in Saudi Arabia was conducted. The aim is to explore the phenomenon owing to their cultural differences, stances on censorship and lack of knowledge in many aspects of security using different aspects including Human computer interaction (HCI), Informational concerns (IC), Mutual considerations (MC), Operational concerns (OC), and Personal interaction (PI). The findings from this paper has highlighted the importance of additional aspects such as functionality, awareness, human error and the relationship between protocols, technology and human. These aspects of security ceremonies can contribute towards assist Saudi Arabia in understanding the interactions between humans and technology in terms of security protocols.**

Keywords: **Security, Ceremonies, Human, Behaviour, Security Protocols.**

I. INTRODUCTION

Information security is an area of research that has received significant attention within the past decade [1]. In particular, studies pertaining to security ceremonies are on the rise [2]. Security ceremonies go beyond the technicalities of security by involving users, as well as those individuals involved in creating security threats. Internet security software, for example, offers protection against potential online threats, such as malware and spyware. However, a security ceremony would go beyond its technical bounds and consider the human perspective as well, where the human would essentially be the users of the security software and configure it to maximise the protection for their computer or mobile device [3]. However, many existing studies fail to explicitly explore the human aspects of information security, and thus there is a need to better understand security ceremonies from a human perspective [2],[4].

Saudi Arabia is a developing country that is currently facing a host of information security issues [5]. While western countries are starting to become more aware of various information threats, the current state of information security awareness in Saudi Arabia is poor. This owes to the high levels of censorship in the country and its tribal culture, which are potential indicators of a poor information security rating [6]. For the above reasons, the aim of this paper is to understand how security ceremonies can help to understand and examine the current state of information security from the intersection of technical and human perspectives. The main contribution is to develop a model to demonstrate the existing information security problems occurring in Saudi Arabia where information security technologies are emerging, but problematic. This was achieved by conducting an empirical study that aims to gather information regarding security ceremonies from a human perspective, as well as developing a model to help address the existing information security problems in Saudi Arabia by gaining an understanding of existing cultural and human security issues.

II. SECURITY CEREMONIES BACKGROUND

Within the last decade, there has been some research emphasizes that information security is not about technical characteristics only, it can be associated with a multidisciplinary approach including social sciences. It has branched out into the social realm, namely the involvement of human perspective in information security [8].This sociotechnical phenomenon has helped to understand the relationship between humans and technology. However, achieving the security goal on a practical level calls for heterogeneous and joint efforts from the likes of human computer interface designers to information security experts. More recently, there has been some research focus on the social aspects of security as opposed to the technical side [3], which has been influenced by a concept known as "ceremonies". This concept was first established by Ellison (2007). A ceremony is essentially a security protocol that understands the human perspective of information security. It also involves capturing imperfect data and real-life behaviours and interactions.

It has become known that humans are not always able to make decisions regarding technology design e.g. remembering a password without making a mistake as the authentication system expects this. Thus, there are always clear limitations where traditional security protocols are concerned owing to flaws in human behaviour. Karlof et al. (2009) studied the challenges of establishing the need of security ceremonies. Later studies by Radke et al. (2011) had recognised a number of areas that existing ceremony analyses had to address in order to consider the humanistic perspective of security technologies. A more recent study by Johansen and Jøsang (2015) proposed a model to include more information pertaining to the user interaction. The limited number of researches has highlighted the importance to investigate on this matter and to expand the existing publications that discuss ceremonies and protocols to consider the humanistic perspective. Therefore, there is a clear need for a model that integrate sociocultural aspects of security ceremonies to ultimately understand the interactions between humans and technology.

III. CONCEPTUAL MODEL

With security ceremonies, the consideration is based on two important nodes which are protocols and humans. The problem is that with human node it is hard to predict human's behaviour, as it's hard to program it [9]. The significant lack of guidance available on how to integrate both nodes presents further challenge. In an attempt to fill the gap, the following section propose a model by the sociotechnical aspects of security analysis. The model identifies several concepts that reflect the various aspects of security with direct impacts on users. These concepts are inspired after reviewing related works, particularly Whitworth (2011) who identified the significance of interfaces between humans and machines, as well as humans' engagement with technology [21]. The key aspects of this model are Human computer interaction (HCI), Informational concerns (IC), Mutual considerations (MC), Operational concerns (OC), Personal interaction (PI). (see Fig.1).

A. Human computer interaction (HCI):

This reflects the sociotechnical protocol. Here, the user is presented with a graphical user interface (GUI), which they interact with and often comes in the form of online forms that users have to complete. Although this aspect may involve some social protocols reflecting users' perceptions of social competencies like giving advice and placing trust into someone, it is explicitly technical owing to the interaction with technology. In other words, the user has no direct involvement with this process, but rather through their human characteristics.

B. Informational concerns (IC):

This reflects the information aspects associated with the security protocol of a system in order to secure communications within an insecure network e.g. data encryption and authentication.

C. Mutual considerations (MC):

This reflects the communal impact of society over people. For instance, advertising that aims to convince users to be safer on the Internet by being more careful when visiting malicious websites.

D. Operational concerns (OC):

This reflects the operating system that handles the communication between the processes that support the functionality of the security protocol in the best interest for the user as well as the process that handles the GUI that is displayed to the user.

E. Personal interaction (PI):

This reflects users' expressing their human characteristics as a means to interact with technology. This involves users of designs and their realistic descriptions, while taking into account their specific goals, perceptions and attitudes. Therefore, the main goal of this aspect is to establish the human perception or side of security protocols. Fig.1 illustrates the proposed model for the current study.

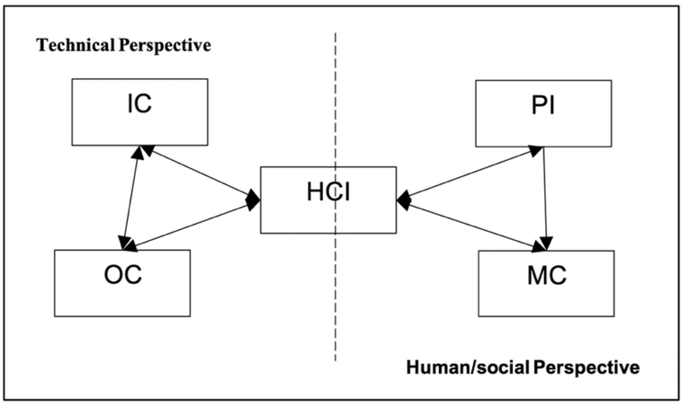

Fig.1: Model of Sociotechnical Considerations of Security Ceremonies.

IV. METHODOLOGY

In order to meet the paper aim, several potential research methods were explored with the most suitable being chosen. There are three key research methods: quantitative, qualitative and mixed method approaches [13]. Since the current study places much emphasis on the human perspective of information security issues, a qualitative approach is adopted. This helped to capture the wider sociotechnical issues associated with security ceremonies that involve peoples' behaviours and perceptions of security protocols. Therefore, a qualitative approach helped to capture these individual behaviours, views and opinions.

A. Data Collection

Based on the qualitative inductive nature of this paper, there are several possible data collection methods, including interviews, observations and focus groups. for this paper face-to-face conversations were conducted in person, while external conversations took place over a particular medium or technology e.g. video conferencing via Skype. This research chose Saudi Arabia as the case study to explore and examine the aspects identified earlier. As for a research sample, the population of participants are Saudi professionals who work in the information security field. The sample size is twenty Saudi professionals. The rationale for this sample size stems from Creswell and Creswell's recommendation of 20-30 participants in qualitative inquiry [13].

B. Method of Analysis

Owing to the qualitative nature of the current study, thematic analysis is the most suitable method of analysis. This involved transcribing the data and then inputting this data into a software package that facilitates qualitative analysis. This helped to identify themes in the paper findings, which in turn helped to understand the sociotechnical aspects of security ceremonies [18]. Moreover, the software package Nvivo was used to code, interpret and write the paper findings into a readable format.

V. DISCUSSION

After analysing the data, three categories of security ceremony have been identified: human, attack and vulnerabilities. Here, a number of key themes were also deduced from the findings.

A. Human Ceremonies

This category is made up of the **HCI**, **IC** and **MC** aspects of security ceremonies as these closely look at human, as well as sociocultural issues that affect these types of ceremonies. For the HCI aspect of security ceremonies, the key theme identified was the **relationship between the protocols and technology and the humans** that interact with it. Here, the interviews highlighted the importance of human interface and the roles humans play in handling computing devices via interaction, and this interaction must come with a degree of security knowledge. The security professionals also talked out the human computer interface issues and how they can help to define the relationship between the creators of protocols and the designers who play a major role in ensuring that the ceremony is secured, all of which requires a degree of security knowledge. Other security professionals argued that the human computer interface is a technology layer but is affected by other non-technology related factors that shape users' responses, such as cultural values, belief systems and demographic factors.

For the IC aspect of security ceremonies, the key theme identified was the **communications** aspect of security ceremonies. The security professionals stated that IC is a way of protecting the communication between two parties. For instance, encryption methodologies and authentication methods were given as a means to demonstrate effective security in their systems to ensure communication is exercised to the fullest. Cryptographic methods were the chosen security method at their respected companies and satisfies both encryption and authentication needs. However, the relationship between user communication and security providers was also deliberated by the security professionals. The security professionals go on to mention that informational is the first layer of a security ceremony and looks at the communication between users and how they establish secure channels. Data encryption and user trust were identified as key issues in the protection of information over a network [4],[7].

For the MC aspect of security ceremonies, the key theme identified was the **awareness** aspect of security ceremonies. Here, the security professionals emphasised that competitors aim to mislead people into believing that their rival's computers are no good. A good example was given by the interviewees: competitors do this is when the importance of data confidentiality is the main topic of discussion. It was also pointed out by the security professionals that humans are driven to interact with computers and design technologies in different ways and expand out to backgrounds in terms of knowledge and security perspectives. The security professionals identified that people are affected by culture and competitive companies. This identified semantic gap that exists between human and computer's understandings towards mutual behaviours, mitigated through sharing knowledge and developing awareness campaigns for people from different perspectives to address this gap among various parties. Moreover, campaigns appear to affect peoples' opinion, and thus change their perception towards security. As a countermeasure, the interviews results highlighted that it is essential to any nation to raise the awareness in their respected societies in order to better understand and recognise the security threats that are based on social engineering, e.g. phishing campaigns [11].

B. Attack/Vulnerabilities Ceremonies

This category is for the **OC** and **PI** aspects of security ceremonies as these closely look at the more technical and wider security vulnerabilities of systems. For the OC aspect of security ceremonies, the key themes identified were the **functionality** and **communication** aspect of security ceremonies. Here, the security professionals talked about the functionality of security systems in terms of being free from security breaches under particular conditions of operation, including system attacks. The security professionals stated that their systems are not vulnerable, and that a reliable, operational, and attack free system is only achieved by enabling trustworthy people to manage them. System reliability was identified as the most significant operation concern to maintain the security measures confidentiality, integrity, and availability of a given system. The security professionals also stated that securing any IT environment requires an inter-process communication between the process that executes the security protocol and the process that runs the graphical interface, and this has to be managed in a secure way. This was identified as a key function of a security system [9].

For the PI aspect of security ceremonies, the key theme identified was the **communication** and **design** aspect of security ceremonies. The security professionals emphasised that it is the designers' goal to design a system that is functioning and operating smoothly with zero attacks, and free of vulnerability. Also having a good design layout is good to reflect society and their needs. Several other security professionals talked about the design issues of protocols, namely human interaction where most human system errors occur. The security professionals pointed out that human's unpredictable behaviour is the reason why systems are left vulnerable and security free. Therefore, human interaction is central and should be considered when designing security protocols as a means to circumvent security weakness and minimize any impacts caused by human interaction [4], [7].

C. Comparison of Themes

Our contribution to this paper is the categorisation and identification of various themes and aspects pertaining to humanistic security ceremonies. Whilst the existing literatures looks at security ceremonies from a technical or social perspective, our paper aimed to look at both together. The concepts are defined and categorised based on their social or technical nature. The literature found that both **PI** and **MC** are the human or social aspects since they involve the users' role in the technological or security process e.g. users' specific system goals and convincing users to use technology in the safest way possible via advertising. Our findings found that **functionality** and **communication** aspects of security ceremonies are relevant to aforementioned categories as they look at the wider communication and functional issues associated with attacks and vulnerabilities in key security systems.

The literature found that **IC** and **OC** are technical as these aspects consider the system functionality e.g. information security and the operating systems and GUIs that help users control such security. Our findings found **communication** and **awareness** as well as **human error** aspects of security ceremonies are relevant to aforementioned categories as they not only look at the wider communication and issues associated with attacks and vulnerabilities in key security systems, but also the role of humans and how they contribute to the impacts of security systems, as well as the degree of knowledge humans have to circumvent or prevent such problems from occurring.

Although the literature found that **HCI** is a crossover between social and technical perspectives [4], [7], [19], the sociotechnical nature of the concept points more to the human category. This because despite being technical to some extent owing to the computer interaction part of the aspect, more emphasis is placed on the human here. Our findings show that the HCI aspect deals more with the **relationship between the protocols and technology and humans** that interact with it. Therefore, the importance of human interface and the roles humans play in handling computing devices via interaction points to more humanistic considerations as opposed to technical ones.

The above findings facilitated the importance of remap these concepts on the revised model for exploring the perspectives of security ceremonies. This acts as roadmap that spans from the technical or systems aspects through to the human and societal aspects of security ceremonies. Moreover, the model looks at security ceremonies from an aspectual view and can help to analyse security ceremonies from a human perspective. Moreover, this model demonstrates a broad range of perspectives in order to understand the human involvement of security ceremonies. Fig.2 illustrates the revised model based on our empirical findings.

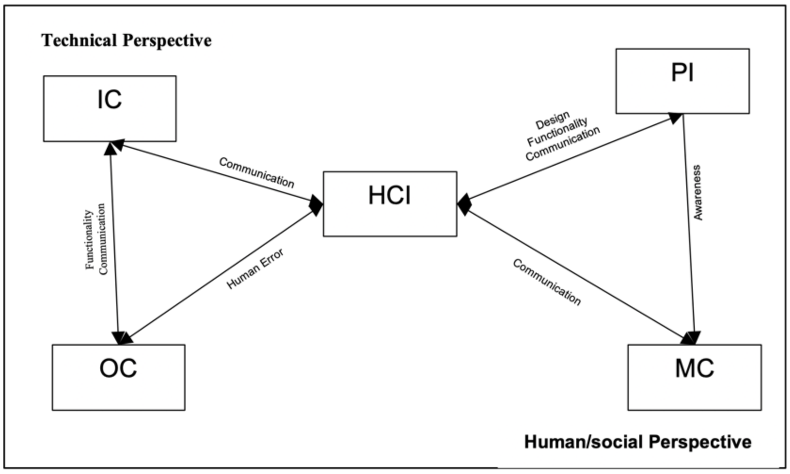

Fig 2: Revised Model of Sociotechnical Considerations of Security Ceremonies.

The findings covered some general issues about security ceremonies, as well as several concepts that reflect the various aspects of security that directly impacts users. Functionality and communication aspects were found to consider the wider communication and functional issues associated with attacks and vulnerabilities in key security systems. Communication and awareness aspects in addition to human error aspects look at the role of humans and how they contribute to the impacts of security systems, which in turn helps to establish a clear relationship between protocols, technology and humans.

VI. CONCLUSION

This paper has analysed the current state of information security via the use of humanistic security ceremonies in developing countries such as Saudi Arabia. It is common knowledge that western countries are well aware of threats, whilst Saudi Arabia lag behind owing to its tribal culture and high censorship in the country. Security ceremonies in particular were found to be a system of including not only the technical side of security threats, but also the human side of security, namely those individuals involved in creating security threats.

This paper found a lack of research into the human considerations of security ceremonies. One research gap that emerged were the lack of informational and social aspects of security ceremonies in the existing literatures, particularly in Saudi Arabia where security awareness is poor. Therefore, this paper aimed to fill this gap by analysing the wider sociotechnical aspects of security ceremonies in Saudi Arabia.

By adopting a qualitative case study, there are various aspects were deduced from the findings as a result of data collection and dedicated analysis with support of the research model (see Fig.1). In addition to the aspects assessed in our model (HCI, IC, MC, OC and PI), new aspects were deduced such as functionality, awareness, human error and the relationship between protocols, technology and humans. These aspects were added to our revised model (see Fig.2). Therefore, the aforementioned aspects of security ceremonies could help Saudi Arabia to better understand the interactions between humans and technology in terms of the security protocols. For example, awareness and determining human errors helps to shed light on the current state of security knowledge in Saudi Arabia and where it can be improved.

The paper limitations hinge mostly on the limited sampled population (Saudi Professionals). This could have been expanded to include other populations that work in the security field, which in turn could have offered a more inclusive and holistic perspective of security ceremonies as our findings are based on a single population’s perspective.

REFERENCES

[1] L. Hadlington, "Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours," *Heliyon,* vol. 3, *(7),* pp. e00346, 2017.

[2] Johansen and A. Jøsang, "Probabilistic modelling of humans in security ceremonies," in *Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance*Anonymous Springer, 2015, pp. 277-292.

[3] T. Martimiano *et al*, "Modelling user devices in security ceremonies," in *Socio-Technical Aspects in Security and Trust (STAST), 2014 Workshop On,* 2014, pp. 16-23.

[4] Bella and L. Coles-Kemp, "Layered analysis of security ceremonies," in *IFIP International Information Security Conference,* 2012, pp. 273-286.

[5] Hathaway, M., Spidalieri, F., Alsowailm, F. & Studies, P. I. F. P., "*Kingdom of Saudi Arabia Cyber Readiness at a Glance*, Potomac Institute for Policy Studies," 2017.

[6] A. Alarifi, H. Tootell and P. Hyland, "A study of information security awareness and practices in saudi arabia," in *Communications and Information Technology (ICCIT), 2012 International Conference On,* 2012, pp. 6-12.

[7] Bella *et al*, "A socio-technical methodology for the security and privacy analysis of services," in *Computer Software and Applications Conference Workshops (COMPSACW), 2014 IEEE 38th International,* 2014, pp. 401-406.

[8] H. Alqahtani, "Developing an Information Security Policy: A Case Study Approach," *Procedia Computer Science,* vol. 124, pp. 691-697, 2017.

[9] C. M. Ellison, "Ceremony Design and Analysis." *IACR Cryptology ePrint Archive,* vol. 2007, pp. 399, 2007.

[10] B. Whitworth, "The social requirements of technical systems," in *Virtual Communities: Concepts, Methodologies, Tools and Applications* Anonymous IGI Global, 2011, pp. 1461-1481.

[11] C. Karlof, J. D. Tygar and D. Wagner, "Conditioned-safe ceremonies and a user study of an application to web authentication." in *Ndss,* 2009.

[12] Bella and L. Coles-Kemp, "Seeing the full picture: the case for extending security ceremony analysis," 2011.

[13] J. W. Creswell, "Research Design: Qualitative, Quantitative, and Mixed Methods Approaches," 2018.

[14] J. Bell, Doing Your Research Project: A Guide for First-Time Researchers. McGraw-Hill Education (UK), 2014.

[15] M. D. Myers, Qualitative Research in Business and Management. Sage, 2013.

[16] S. Mcleod, "The Interview Method [Online]. ," Accessed 6th July 2018, 2014.

[17] S. Sullivan-Bolyai, C. Bova and M. D. Singh, "Data-Collection Methods," *Nursing Research in Canada-E-Book: Methods, Critical Appraisal, and Utilization,* pp. 287, 2014.

[18] M. B. Miles, A. M. Huberman and J. Saldana, *Qualitative Data Analysis.* Sage, 2013.

[19] B. Whitworth, Handbook of Research on Socio-Technical Design and Social Networking Systems. IGI Global, 2009.

[20] K. Radke et al, "Ceremony analysis: Strengths and weaknesses," in IFIP International Information Security Conference, 2011, pp. 104-115.

[21] B. Whitworth, "The social requirements of technical systems," in Virtual Communities: Concepts, Methodologies, Tools and Applications Anonymous IGI Global, 2011, pp. 1461- 1481.

APPENDIX - A

Appendix 1: Interview questions

1. What is your current position at your respected company?

2. What are your personal views on security ceremonies? Please explain

3. From your point of view, how users can use secured systems insecurely?

4. From your professional experience, how important are human computer interface issues to help better understand security ceremonies? E.g. security protocols and graphical user interface (GUI)

5. From your professional experience, how important are informational concerns to help better understand security ceremonies? E.g. data encryption and authentication

6. From your professional experience, how important are mutual considerations to help better understand security ceremonies? E.g. creating awareness of security issues to society

7. From your professional experience, how important are operational concerns to help better understand security ceremonies? E.g. functionality of security systems

8. From your professional experience, how important are personal interaction to help better understand security ceremonies? E.g. defining personal goals, perceptions and attitudes.

9. Are there any other issues you wish to comment about based on our discussion?

10. How you can explain/identify Security Ceremonies?