A Socio-Technical Approach to Information Security

Completed Research Full Paper

Mathias Mujinga
School of Computing, University of South Africa
mujinm@unisa.ac.za

Mariki M. Eloff
ICC, CEMS, University of South Africa
eloffmm@unisa.ac.za

Jan H. Kroeze
School of Computing, University of South Africa
kroezjh@unisa.ac.za

Abstract

The main objective of this paper is to present a preliminary socio-technical information security (STInfoSec) framework for the development of online information security applications that addresses both social and technical aspects of information security design. The paper looks at theoretical aspects related to a view of information security as a socio-technical system in the context of online banking. The STInfoSec framework investigates usability and security requirements for an improved online banking system that seeks to improve the adoption and continued use of the service. The STInfoSec framework proposes 12 usable security design principles that assist in addressing security and usability requirements in online applications such as online banking. The framework seeks to influence the behaviour of designers of online information security applications by incorporating principles that consider the end user behaviour of such applications. The validation of the framework is beyond the scope of this paper.

Keywords

Socio-technical approach, information security, social theory, STInfoSec.

Introduction

Information security in this digital age is increasingly becoming more of a social than a technical problem. This is highlighted by the prevalence of information security attacks that utilise social engineering and other tactics aimed at human weaknesses in the security chain. Therefore, technical solutions used in isolation are inadequate to protect information security assets for individuals and organisations. The main objective of the socio-technical information security (STInfoSec) framework is to highlight both security and usability requirements in the design and development of online information systems (IS) applications. There is a need for design strategies that can address both social and technical aspects of IS design. One such strategy is the socio-technical systems (STS) approach (Paja et al. 2015). The STS approach views any IS as one that consists of two subsystems, namely, a social subsystem and a technical subsystem. This study is motivated by the argument that current online information security threats such as social engineering attacks that target individual users' sensitive and confidential information utilise a combination of social and technical methods (Krombholz et al. 2015). The need to address this security problem is more significant in the context of online banking service, as security breaches potentially lead to financial losses for individual users, organisations, and financial institutions. Therefore, it is imperative that both technical and social aspects be addressed in developing such applications, especially with many people conducting most aspects of their daily lives online such as work and entertainment.

The STS approach is used to achieve the research objective, which is to develop a framework that addresses both technical and social aspects of online IS development. The framework has been developed specifically for online banking services as case study. The case study is used throughout the research to investigate the issues of security culture, usability analysis, security requirements, and security internal controls. This paper proposes a conceptual socio-technical view of information security that will assist in the design of usable security, specifically aimed at online information security applications. The study identifies design principles that aid in the development of usable and secure online applications. The security of online applications can significantly be improved through such design principles, given the increased online activity from users with diverse backgrounds and computer literacy, coupled with limited information security awareness and training.

The paper is organised as follows: firstly, we discuss information security as a social problem that requires a multidisciplinary approach and the relevance of social theory in tackling current information security issues; secondly, a brief discussion of the STS theory and how it applies to information systems and information security is provided. A brief outline of the methodology followed in the development of the framework is then given, followed by a presentation of the STInfoSec framework.

Information Security as a Social Problem

Information security is currently receiving more attention, given all the high-profile security breaches involving numerous organisations that deal with citizens' personal information such as the Emory Healthcare data breach (McGee 2017) and Yahoo's 2013 data breach, dubbed *"the largest data breach in history"* (Leary 2016). In most cases, adversaries take advantage of generous human kindness; hence, it is apparent that information security problems cannot be solved through technical solutions in isolation. Given the additional complex dimension of the pervasive nature of online activity by both individuals and organisations, information security threats are ever-present. Individuals and organisations are increasingly storing confidential and sensitive information on a plethora of connected devices and transmitting this information over the public global and open network: the internet. Technical solutions to protect critical information assets that include devices, transmission media, and data might be impenetrable, but without addressing other aspects such as the human element, these solutions are insufficient. This gives rise to a holistic view of information security that addresses a combination of technical and social problems. At the heart of this argument is the unpredictable element of human (or user) behaviour that cannot be accurately conceptualised, as many factors such as computer proficiency and information security mental models describe it as highly dynamic (Yee 2004). This has resulted in information security being treated – rightly so – as a multidisciplinary field (Sveen et al. 2009), bringing together expertise from computer science, engineering, social sciences, and many other disciplines.

Humans as 'Weakest Link'

Information security attacks increasingly target human behaviour, as users are universally regarded as the *"weakest link in the security chain"* (Sasse et al. 2001). As noted by Schneier (2000), the biggest security risk is the interaction between a computer system and the user. As such, the multidisciplinary approach to information security mainly strives to understand and predict human behaviour. The objective of understanding user behaviour is to assist in the design and development of an IS that takes human behaviour into account. Understanding human behaviour is even more important in information security systems that usually rely on user intervention to create a secure environment and protect information assets from adversaries. This is because a computer system can be expected to behave in a certain way, but users' behaviour is unpredictable. Furnell (2005) argues that the design of systems and the nature of security tasks make it difficult for users to adhere to security requirements.

It has been found that most users cannot correctly interpret SSL security error/warning messages generated by the web browser during the authentication process for a secure connection (Tarazan and Bostan 2016). Regardless, security is often complex, making it difficult to understand, but easy to misconfigure and misuse. Serious design flaws still exist in IS, such as those identified by Falk et al. (2008) in high-security websites, that designers overlook, including requesting login options on insecure pages and emailing sensitive information in plain text. These issues leave novice users of online information security applications vulnerable to increasingly sophisticated online information security attacks. Therefore, before designers expect users to comply with information security requirements, the applications need to at least comply with basic requirements. Only then can a secure environment be created because a system with design flaws creates an insecure environment, regardless of the level of compliance of its users.

Usable Security

Usable security is essentially concerned with information security issues around the intersection of usability and information security. Usable security strives to give equal importance to both areas in the design and development process of information systems. Information security inevitably involves human users for the successful achievement of its intended goals, making its success or failure dependent on how users use the information security mechanisms designed to protect information security assets (Crossler et al. 2013). The involvement of humans suggests the need to address social aspects of information security, since technical solutions, on their own, are insufficient. Given the above assertions, an IS that addresses both information security and usability aspects is essentially a socio-technical system, which must account not only for the technical functionalities of the system, but also for social user behaviour.

One of the earliest landmark studies on usable security is the work of Whitten and Tygar (1999), which evaluates the usability of PGP 5.0 in email encryption. The authors define usable security based on a set of four priorities:

> *"Security software is usable if the people who are expected to use it: (1) are reliably made aware of the security tasks they need to perform; (2) are able to figure out how to successfully perform those tasks; (3) don't make dangerous errors; and (4) are sufficiently comfortable with the interface to continue using it."*

Generally, computer users expect computers to protect their information without much effort from the user. Therefore, it is essential that security and usability be seamless and, instead of contradictory goals, be complementary in protecting information systems.

Socio-Technical System

The socio-technical systems (STS) theory can be traced back to the work of Eric Trist and other social scientists (Trist and Bamforth 1951) at the Tavistock Institute of Human Relations in London soon after World War II (Mumford 1995). The theory was originally developed to address the work system in an organisational context, but has since been applied in a variety of scenarios. In the context of IS, the theory implementation involves two stages, namely, (1) technical capabilities of the system without regard for user behaviour and (2) technical capabilities with user behaviour properties in consideration (Ferreira et al. 2014). This view highlights the importance of the technical aspects of the socio-technical approach, as the main goal of the approach is to create a system that meets technical goals and allows users to utilise the system effectively. An STS is comprised of two subsystems: the technical subsystem and the social subsystem.

Technical Subsystem

The technical subsystem of a work system consists of the tools, techniques, devices, artefacts, methods, configurations, procedures, and knowledge used by system users to convert system inputs into system outputs (Pasmore 1988). The technical subsystem components are divided into two categories, namely, technology and tasks. The technical subsystem can also be viewed as including technologies, policies, and practices that describe the modes of production and users' actions when performing tasks (Bélanger et al. 2013). In the context of this research, we view the technical subsystem as comprised of tools, devices, methods, configurations, and procedures that make up an online application such as an online banking system. The technology and tasks involved in an online banking system enable people (users and developers) to achieve their business and individual goals.

Social Subsystem

Traditionally, the social subsystem of a work system is comprised of the individuals and organisations that interact with the system, including their unique social attributes (Paja et al. 2013). Rather than regarding it as an aggregate of individual attributes, the social subsystem in an organisation may be viewed as the context in which the organisational work system operates and is characterised by its attributes as a whole rather than as an aggregate of individual attributes.

Socio-Technical System in Information Security

The need to address socio-technical aspects is even more important in information security systems. Information systems can be technically secure through the use of advanced encryption mechanisms, but all of those can fail if users misuse or bypass them. Social attacks such as social engineering render technical protections useless. Given these varying aspects, achieving effective security becomes a complex and complicated goal and highlights the need for a socio-technical approach that is largely dependent on human factors. Online information security systems fit perfectly into this socio-technical definition; hence, their design can be improved by applying this approach. This prompts designers to find a balance between information security and usability goals to allow IS, especially information security systems, to be effectively and efficiently used by end-users. The socio-technical design approach strives for the equal importance of social and technical aspects of system design. The STS approach is suitable for addressing information security and usability aspects of online applications, thereby fostering applications that are both usable and secure.

Kirlappos and Sasse (2014) argue for the creation of a secure organisational environment by developing security mechanisms that recognise the trust relationship between individuals and their organisation in providing usable and effective security implementations. The authors also argue that current approaches that ‘require’ certain user behaviour and making security tools ‘easy to use’ are ineffective. This trust approach is insufficient on an online environment that is used by individual users such as social media, online shopping, and online banking where the employee-organisation relationship does not exist. Hence the need to align information security and usability goals to avoid sacrificing one of these aspects has been a challenge and a focus of research studies in both the information security and human-computer interaction (HCI) communities. However, while there are several gaps in the knowledge of designing usable security applications, there is extensive research in the separate fields. Currently, there is no agreement on exactly how to design usable online applications while providing effective security. Effective security is the main goal of most information security design. Ferreira et al. (2014) define an effective security system as one that is secure, even when used by humans. The literature reveals that such systems are becoming increasingly difficult to design, especially given diverse user groups and an increasing reliance on social attacks by cyber attackers. The human element neutralises state-of-the-art technical security mechanisms, mainly because information security is not perceived as a primary goal by users of the system. We argue that an STS approach can bring the two often contradictory fields of information security and usability together. Although technical solutions in information security are necessary, it is widely accepted that they are not adequate in solving information security challenges in complex and ever-changing socio-technical environments (Holgate et al. 2012).

Preliminary Framework Development

This section outlines the proposed socio-technical information security (STInfoSec) framework that draws from the literature on usable security design principles and best practices. The end result is a set of critically informed design guidelines for online information security applications such as online banking. In the final framework, the design principles are validated through a heuristic evaluation method. We first explain the four STS components in the context of online banking, describing what constitutes each component. The framework proposed in this research integrates the unified theory of acceptance and use of technology (UTAUT2) (Venkatesh et al. 2012), usability, and security in a socio-technical system in the design and development of online applications.

STInfoSec Components

The STInfoSec framework looks at improving the development of online applications that rely on effective information security to provide services to the user. The idea is to make these applications meet both usability and security requirements, thereby creating an environment that fosters adoption and continued use of the applications by a diverse set of users. The framework specifically applies to online banking systems, but can still be applied to any other online security IS applications. Figure 1 illustrates the framework components, including external elements that contribute to the framework. Firstly, we present usability and security requirements that are necessary for secure and usable information security applications. These are design principles that developers need to address in developing applications that meet usable security properties. Secondly, using UTAUT2, we investigate users’ perceptions of the current online banking service; this evaluation highlights areas that need attention to improve the service based on users' feedback.

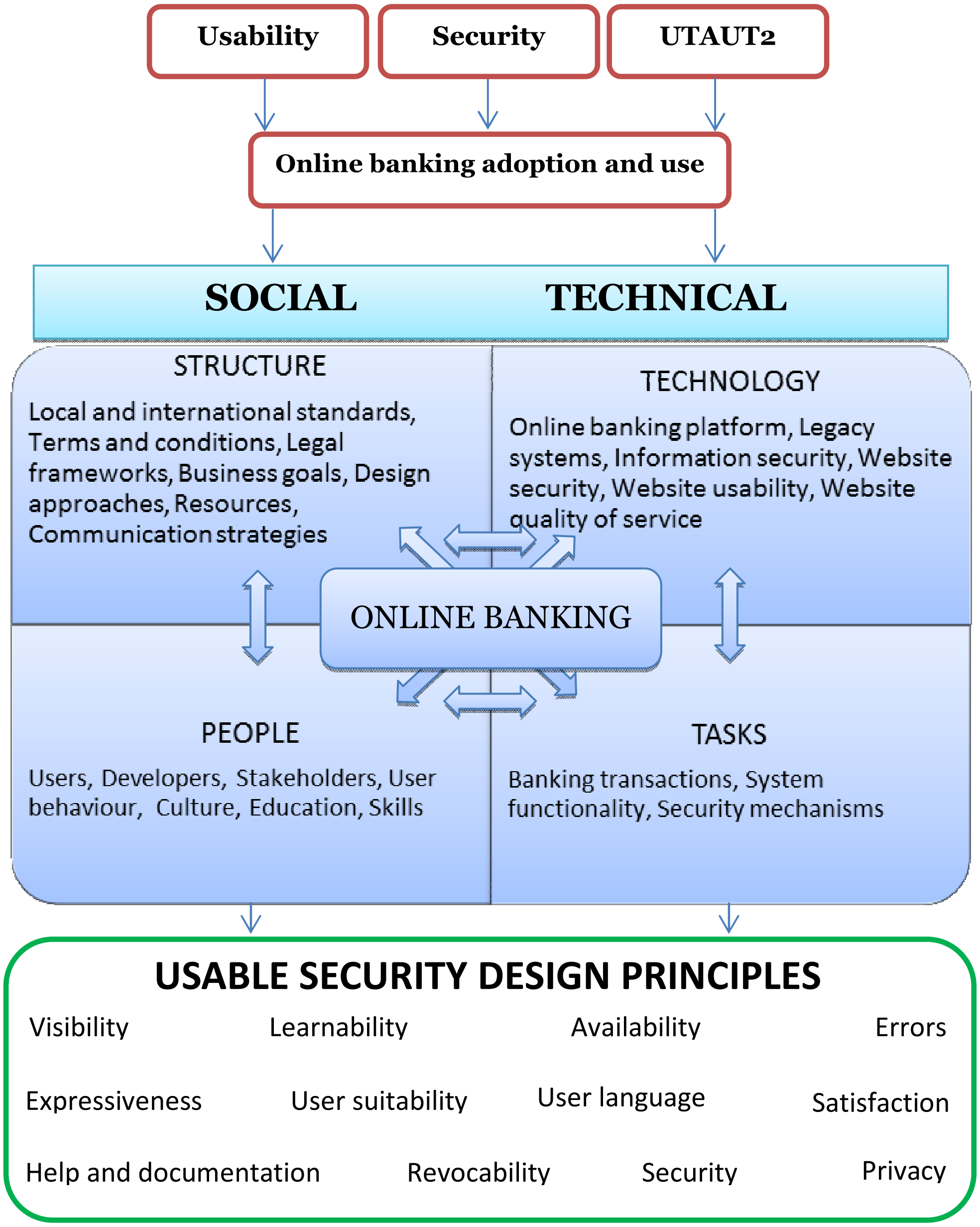
Usability
Security
UTAUT2
Online banking adoption and use
SOCIAL
TECHNICAL
STRUCTURE
Local and international standards, Terms and conditions, Legal frameworks, Business goals, Design approaches, Resources, Communication strategies
TECHNOLOGY
Online banking platform, Legacy systems, Information security, Website security, Website usability, Website quality of service
ONLINE BANKING
PEOPLE
Users, Developers, Stakeholders, User behaviour, Culture, Education, Skills
TASKS
Banking transactions, System functionality, Security mechanisms
USABLE SECURITY DESIGN PRINCIPLES
Visibility
Learnability
Availability
Errors
Expressiveness
User suitability
User language
Satisfaction
Help and documentation
Revocability
Security
Privacy

Figure 1. STInfoSec Framework Components

Usability

Usability plays a huge role in facilitating effective and efficient use of the system, and it has a significant impact on potential users' adoption and use of the system. Therefore, it is essential that information systems implement usability principles from the outset when design decisions are made, as usability cannot be an add-on component at a later stage. There is significant research on the usability principles that need to be addressed in developing IS applications. Table 1, presented later in this paper, highlights these research studies. Some of these are general guidelines, while others have been developed for specific types of applications. In this study, the interest is in usability principles intended for information security applications.

Security

Information systems applications need to protect confidential and sensitive information provided by the users for the system to be trusted. This requirement is particularly important when the risk includes potential financial loss and leaking of privacy information that can lead to identity theft. One such system is the online banking system. The security or perceived security of an online banking system, as viewed by users, needs to be trustworthy for them to adopt or continue using the service. Hence, the design of the system needs to address security mechanisms to protect the users' personal information. There are several design principles for the development of secure IS found in the literature.

UTAUT2 Model

Sensitive online applications such as online banking need more than just usefulness and ease of use to encourage potential users to adopt them. Usability, security, privacy, and trust, be these perceived or real, need to be addressed for users to be comfortable with adopting and continuing to use the systems. With the advent of more pervasive mobile and portable devices, the emphasis has moved to addressing user experience when users interact with these devices. In this research, it was found that users and developers of online banking applications raised both social and technical issues regarding information security. Therefore, the design of such applications needs to address both aspects as well.

Socio-Technical Components

Studies of the socio-technical approach to information security are mainly based on technical and organisational aspects of system design, which are the main foundation of the socio-technical model. This research looks at the socio-technical aspects based on individual context, not necessarily organisational context. The main objective of the STInfoSec framework is to gain a better understanding of how socio-technical aspects that affect information security usage can assist in the development of online applications in the context of online banking. The specific technical and social dynamics at play in users' interaction with information security mechanisms have been widely researched separately. This research intends to bring these dynamics together in the context of usable security.

Theoretically, information system security elements belong to three views, namely, social, technical, and socio-technical (Iivari and Hirschheim 1996). While both the social and technical views place the emphasis on either social or technical aspects, respectively, a socio-technical view appreciates social and technical aspects of information system development equally. STS as a system strives to encourage a systems approach, with a holistic approach to IS development that addresses information security problems brought about by the interrelationship between users and technology. Rather than approaching the two aspects separately, the emphasis is on approaching the social and technical components of the system simultaneously. Ropohl (1999) argues that a socio-technical systems model is useful in explaining the impact of technology on society, making technical development equivalent to social change. The following subsections discuss the four components of an STS in the context of online banking.

Structure

The structural component deals with policy and legal elements that ensure a code of conduct among different groups of people involved in the system. Financial institutions are governed by the country's rules and regulations regarding providing financial services to its citizens, usually through the country's central bank and other financial regulatory bodies. The banks, in turn, create banking and online banking terms and conditions that set up recommended behaviour for users, including responsibilities and liabilities that accompany enrolment and continued use of the provided services. These terms and conditions include dispute resolution procedures in case of security breaches or other related disputes, which are usually referred to the banking ombudsman when the parties (the user and the bank) fail to resolve the issue. Structure also includes design approaches used in developing the system, including local and international standards and best practices that are compulsory or recommended in application (or product) design and development. Such standards might include those prescribed by international bodies such as the International Organisation for Standardisation (ISO) and national bodies such as the South African Bureau of Standards (SABS), as well as other information security recommendations from local and international banking consortiums. Most South African banks are members of the South African Banking Risk Information Centre (SABRIC), a non-profit company formed by the four major South

African banks to assist banking and cash-in-transit companies in combating organised bank-related crimes (SABRIC 2017). SABRIC provides a platform for financial institutions to share information on information security and security threats.

People

The people involved in an online banking system include users, developers, management, and any other stakeholders such as vendors, contractors, etc. Users are the bank's clientele, which includes a diverse group of people with different ages, educational qualifications, computer literacy levels, incomes, languages, and cultures. 'Developers' is an all-encompassing term that includes designers, programmers, testers, usability evaluators, vendors of outsourced products, and any other people directly involved in the development of online banking applications. Management includes top management of the financial institution and the supervisors of the development teams. Those in top management have direct influence on the development of the system, as they make decisions that directly affect the end product, such as controlling the budget and hiring personnel with relevant and needed expertise to improve the final product.

Technology

The technology component involves a wide range of technologies that form part of the online banking system – from the bank's hardware and users' devices to software applications that provide the services. From the bank's side, the technology covers hardware servers, operating systems, networking technologies between data centres, middleware platforms, back-end applications, and the user interfaces that allow employees and users to access information remotely. The bank also provides information security technologies and mechanisms to protect user and company information assets by providing access to authorised users based on predefined access control policies. The technologies include encryption, firewalls, and intrusion detection and prevention systems. User interfaces for both the web and mobile devices need to incorporate current best practices to enhance user-friendly properties, which include acceptable usability, and to enhance user experience. Given the wide range of activities currently accessible through the internet, including games and entertainment, online applications need to be competitive for users to embrace and use them.

Tasks

The structure and technology in a socio-technical system provide the means for people to accomplish certain tasks. An online banking system provides a convenient way for the bank to offer banking activities to its clients 24 hours a day. Apart from an array of online banking transactions, the system must also fulfil the organisational business goals to provide the shareholders with a return on their investment. Users perform banking-related tasks, and the development team ensures that the online banking system is readily available to users and that it is usable and secure to meet users' expectations and fulfil business goals.

Usable Security Design Principles

A great deal of research has been conducted on the design guidelines that are meant to improve security-oriented design. Generally, there is no consensus on exactly what makes one design better than another from a usable security perspective. This section discusses design guidelines that are meant to improve the design of user interfaces of IS applications, particularly those that require information security mechanisms. There are several researchers who have looked at usable security design strategies; among the earliest works are those of Shneiderman (1986), Nielsen (1995), Yee (2002), and Johnston et al. (2003). The researchers identified a gap between usability and security, and to bridge this gap, they came up with numerous design principles, of which some are generic for any kind of application, while others are application-specific. Table 1 provides design principles applicable to the current system under investigation, especially those that enhance system usability while providing adequate security to novice and experienced users, thereby encouraging online banking adoption and continued use.

Principle	Description	Source(s)
Visibility	Keep users informed about the system security status, using appropriate feedback within a reasonable time.	(Nielsen 1995); (Yee 2002); (Katsabas et al. 2005)
Learnability	System security features should be easy to learn and remember.	(Johnston et al. 2003); (Yeratziotis et al. 2012)
Errors	Express error messages in plain language, indicating the problem precisely, and suggest constructive recovery actions. Prevent errors from happening in the first place.	(Shneiderman 1986); (Nielsen 1995); (Katsabas et al. 2005)
Availability	System services must be available all the time, with minimum down time.	(Yeratziotis et al. 2012)
Satisfaction	Ensure good experience in using the system.	(Johnston et al. 2003); (Yeratziotis et al. 2012)
Revocability	Users should be able to revoke serious errors, and the system should give prior warning and confirmation for irreversible actions. Provide support for 'undo' and 'redo' functions.	(Shneiderman 1986); (Yeratziotis et al. 2012)
Expressiveness	Guide users through security features, and allow freedom of expression.	(Yee 2002); (Johnston et al. 2003)
User language	The system should speak the users' language, with words, phrases, and concepts familiar to users, rather than system-oriented terms.	(Katsabas et al. 2005); (Yeratziotis et al. 2012)
User suitability	The system should provide options suitable for users with diverse levels of skill and experience in security.	(Yeratziotis et al. 2012)
Help and documentation	Provide user assistance, with searchable help and documentation for both security and non-security tasks, that is actionable with concrete steps.	(Shneiderman 1986); (Nielsen 1995); (Yeratziotis et al. 2012)
Security	Ensure end-to-end protection of the communication channel between the end-user device and trusted servers.	(Yee 2002); (Yeratziotis et al. 2012)
Privacy	Protect the information provided by users against access by unauthorised parties, and use it only for the purposes for which it was collected.	(Yeratziotis et al. 2012)

Table 1. Design Principles Applicable to the System under Investigation

Conclusion

The goal of this research is to assist the development of online applications with a framework that applies a socio-technical view. Combined with UTAUT2, STS can be used to explain user acceptance and continued use of technology. UTAUT2 essentially predicts users' behaviour in deciding to adopt or reject a technology artefact. Hence, aiding the development of such artefacts through improving aspects that significantly make users reject a technology, such as a lack of usability and security, while optimising positive aspects helps improve the adoption and continued use of such technology.

To achieve this goal, firstly, the factors that affect user behaviour and encourage or prevent users from doing the right thing, even when they know the risks associated with non-compliance with information security requirements, should be identified. Secondly, the design of information security in online applications needs to identify the factors that make users feel inclined to bypass or ignore information security mechanisms. Hence, we assert that a socio-technical approach to information security systems design can fulfil the goal of creating applications that are secure and usable, and the STInfoSec framework is one such approach.

The validation of the preliminary STInfoSec framework is the next step in finalising the framework. This process involves conducting a heuristic evaluation method based on a checklist for each design principle to investigate the compliance of interface features with reputable usability principles. Heuristic evaluation and the use of checklists are closely linked approaches, through which an expert rates the usability of the product based on several criteria (Lehto and Landry 2012). This process allows for the amendment of the design principles based on feedback from field experts and ensuring their suitability in addressing security and usability requirements in an online banking system.

References

Bélanger, F., Watson-Manheim, M. B., and Swan, B. R. 2013. "A Multi-Level Socio-Technical Systems Telecommuting Framework," *Behaviour & Information Technology* (32:12), pp. 1257-1279.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., and Baskerville, R. 2013. "Future Directions for Behavioral Information Security Research," *Computers & Security* (32:2013), pp. 90-101.

Falk, L., Prakash, A., and Borders, K. 2008. "Analyzing Websites for User-Visible Security Design Flaws," in *Proceedings of the 4th Symposium on Usable Privacy and Security (SOUPS),* Pittsburgh, PA, 23-25 July, pp. 117-126.

Ferreira, A., Huynen, J., Koenig, V., and Lenzini, G. 2014. "A Conceptual Framework to Study Socio-Technical Security," in *International Conference on Human Aspects of Information Security, Privacy, and Trust,* Crete, Greece, 22-27 June, pp. 318-329.

Furnell, S. 2005. "Why Users Cannot Use Security," *Computers & Security* (24:4), pp. 274-279.

Holgate, J. A., Williams, S. P., and Hardy, C. A. 2012. "Information Security Governance: Investigating Diversity in Critical Infrastructure Organizations," in *Proceedings of the 25th Bled eConference,* Bled, Slovenia, 17-20 June, pp. 379-393.

Iivari, J., and Hirschheim, R. 1996. "Analyzing Information Systems Development: A Comparison and Analysis of Eight IS Development Approaches," *Information Systems* (21:7), pp. 551-575.

Johnston, J., Eloff, J. H. P., and Labuschagne, L. 2003. "Security and Human Computer Interfaces," *Computers & Security* (22:8), pp. 675-684.

Katsabas, D., Furnell, S., and Dowland, P. 2005. "Using Human Computer Interaction Principles to Promote Usable Security," in *Proceedings of the 5th International Network Conference,* Samos, Greece, 5-7 July, pp. 235-242.

Kirlappos, I., and Sasse, M. A. 2014. "What Usable Security Really Means: Trusting and Engaging Users," in *Human Aspects of Information Security, Privacy, and Trust,* T. Tryfonas and I. Askoxylakis (eds.), Switzerland: Springer, pp. 69-78.

Krombholz, K., Hobel, H., Huber, M., and Weippl, E. 2015. "Advanced Social Engineering Attacks," *Journal of Information Security and Applications* (22:2015), pp. 113-122.

Leary, J. 2016. "The Biggest Data Breaches in 2016," last accessed 20 April 2017, https://www.identityforce.com/blog/2016-data-breaches.

Lehto, M. R., and Landry, S. J. 2012. *Introduction to Human Factors and Ergonomics for Engineers*, Boca Raton, Florida: CRC Press.

McGee, M. K. 2017. "Emory Healthcare Database Breach: What Happened?" last accessed 20 April 2017, http://www.databreachtoday.com/emory-healthcare-database-breach-what-happened-a-9745.

Mumford, E. 1995. "Creative Chaos or Constructive Change: Business Process Reengineering Versus Socio-Technical Design," in *Examining Business Process Re-Engineering: Current Perspectives and Research Directions,* G. Burke and J. Peppard (eds.), London, UK: Kogan Page, pp. 192-216.

Nielsen, J. 1995. "Ten Usability Heuristics," last accessed 20 April 2017, http://www.nngroup.com/articles/ten-usability-heuristics/.

Paja, E., Dalpiaz, F., and Giorgini, P. 2013. "Managing Security Requirements Conflicts in Socio-Technical Systems," in *Proceedings of the 32nd International Conference on Conceptual Modeling,* Hong Kong, 11-13 November, pp. 270-283.

Paja, E., Dalpiaz, F., and Giorgini, P. 2015. "Modelling and Reasoning about Security Requirements in Socio-Technical Systems," *Data & Knowledge Engineering* (98:2015), pp. 123-143.

Pasmore, W. A. 1988. *Designing Effective Organizations: The Sociotechnical Systems Perspective*, New York, NY: John Wiley & Sons Inc.

Ropohl, G. 1999. "Philosophy of Socio-Technical Systems," *Techné: Research in Philosophy and Technology* (4:3), pp. 186-194.

SABRIC. 2017. "South African Banking Risk Information Centre (SABRIC)," last accessed 20 April 2017, https://www.sabric.co.za/about-us.

Sasse, M. A., Brostoff, S., and Weirich, D. 2001. "Transforming the 'Weakest Link'—a Human/Computer Interaction Approach to Usable and Effective Security," *BT Technology Journal* (19:3), pp. 122-131.

Schneier, B. 2000. *Secrets & Lies: Digital Security in a Networked World*, New York, NY: John Wiley & Sons, Inc.

Shneiderman, B. 1986. *Designing the User Interface: Strategies for Effective Human-Computer Interaction*, Boston, MA: Addison-Wesley Longman Publishing Co., Inc.

Sveen, F. O., Torres, J. M., and Sarriegi, J. M. 2009. "Blind Information Security Strategy," *International Journal of Critical Infrastructure Protection* (2:3), pp. 95-109.

Tarazan, Ş, and Bostan, A. 2016. "Customizing SSL Certificate Extensions to Reduce False-Positive Certificate Error/Warning Messages," *International Journal of Information Security Science* (5:2), pp. 21-28.

Trist, E. L., and Bamforth, K. W. 1951. "Some Social and Psychological Consequences of the Longwall Method of Coal-Getting," *Human Relations* (4:3), pp. 3-38.

Venkatesh, V., Thong, J., and Xu, X. 2012. "Consumer Acceptance and Use of Information Technology: Extending the Unified Theory of Acceptance and Use of Technology," *MIS Quarterly* (36:1), pp. 157-178.

Whitten, A. and Tygar, J. D. 1999. "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0," in *Proceedings of the 8th USENIX Security Symposium,* Washington, D.C., 23-26 August, pp. 169-184.

Yee, K. P. 2004. "Aligning Security and Usability," *IEEE Security & Privacy* (1:5), pp. 48-55.

Yee, K. P. 2002. "User Interaction Design for Secure Systems," in *Proceedings of the 4th International Conference on Information and Communications Security,* Singapore, 9-12 December, pp. 278-290.

Yeratziotis, A., Pottas, D., and Van Greunen, D. 2012. "A Usable Security Heuristic Evaluation for the Online Health Social Networking Paradigm," *International Journal of Human-Computer Interaction* (28:10), pp. 678-694.