SACJ 32(1) July 2019
Research Article

Towards a framework for online information security applications development: A socio-technical approach

Mathias Mujinga[a], Mariki M. Eloff[b], Jan H. Kroeze[a]

[a] School of Computing, University of South Africa, Johannesburg, South Africa
[b] Institute of Corporate Citizenship, University of South Africa, Pretoria, South Africa

ABSTRACT
The paper presents a validated socio-technical information security (STInfoSec) framework for the development of online information security (InfoSec) applications. The framework addresses both social and technical aspects of InfoSec design. The preliminary framework was developed using a mixed methods research design that collected data from 540 surveys by online banking users and six interviews with online banking personnel. The preliminary framework was presented in another publication and it is beyond the scope of this paper. The scope of this paper is limited to the validation findings of the evaluation process that involves seven evaluators. In the socio-technical context, the STInfoSec framework facilitates acceptance and usability of online applications based on online banking as a case study. The authors argue that usability of online InfoSec applications such as online banking significantly affects the adoption and continued use of such applications. As such, the paper investigates design principles for usable security and proposes a validated STInfoSec framework that consists of 12 usable security design principles. The design principles have been validated through heuristic evaluation by seven field experts for inclusion in the final STInfoSec framework. The development of InfoSec applications can be improved by applying these design principles.

Keywords: online banking, socio-technical, information security, usable security, STInfoSec, South Africa

Categories: • **Security and privacy** ∼ **Usability in security and privacy**

Email:
Mathias Mujinga mujinm@unisa.ac.za (CORRESPONDING),
Mariki M. Eloff eloffmm@unisa.ac.za,
Jan H. Kroeze kroezjh@unisa.ac.za

Article history:
Received: 6 Sep 2018
Accepted: 21 May 2019
Available online: 24 Jul 2019

1 INTRODUCTION

Information security (InfoSec) is critical for both individuals and organisations, especially now with the prevalence of online activities for every aspect of our daily lives. Organisations that collect citizens' personal information need to safeguard this information against unauthorised access, while individuals need assurances that the information they provide to organisations through applications

Mujinga, M., Eloff, M.M. and Kroeze, J.H. (2019). Towards a framework for online information security applications development: A socio-technical approach. *South African Computer Journal 32*(1), 24–50. https://doi.org/10.18489/sacj.v31i1.587

SACJ is a publication of the South African Institute of Computer Scientists and Information Technologists. ISSN 1015-7999 (print) ISSN 2313-7835 (online).

is safe and their privacy is protected. Unfortunately, protection of personal information is still an issue as shown by numerous data breaches recently reported by organisations that result in leaks of millions of users' personal information (Obermaier, Obermaier, Wormer, & Jaschensky, 2016). At the heart of these high profile security breaches are human behavioural problems. From an individual's perspective, InfoSec awareness is critical to mitigate numerous sophisticated attacks, especially, given the wide range of computer literacy levels possessed by today's online audience. The authors argue that InfoSec effectiveness can be improved by incorporating design principles that address both usability and InfoSec problems in information systems (IS).

There are numerous design principles that are proposed in literature to address usability and InfoSec of IS applications. Such principles range from general usability of IS (Preece, Rogers, & Sharp, 2015) to those developed for specific applications (Yeratziotis, Pottas, & Greunen, 2012). In addition, there are design principles that were proposed to make IS more secure and usable, often referred to as usable security. Given the unique goals of today's online applications that include social media, entertainment, and high-risk applications such as electronic health (ehealth) and online banking, it is apparent that one design strategy does not fit all. As such, developers need dedicated strategies that address specific needs of individual applications. Hence, this study proposes a framework for online InfoSec applications based on online banking that can be applied to other similar applications with little adaptation.

The paper explores the question "How to apply a socio-technical approach in the development of online information security applications?" To answer the question the paper reports on the evaluation process followed to validate a previously-developed preliminary STInfoSec framework, published in the proceedings of the Americas Conference on Information Systems (Mujinga, Eloff, & Kroeze, 2017). The aim of the paper is to provide a solution to assist in the development of usable and secure online InfoSec applications. The authors argue that a secure online environment can only be achieved by developing InfoSec applications that are usable. As such, the authors propose a socio-technical design. The paper reports on the evaluation process followed in validating the proposed socio-technical information security (STInfoSec) framework. The framework consists of 12 usable security design principles that can assist developers of online InfoSec applications—using the online banking service as a case study.

The paper is organised as follows: firstly, InfoSec is discussed as a social problem that requires a multidisciplinary approach. Secondly, a brief discussion of the socio-technical system (STS) theory is given followed by its suitability in IS and InfoSec. This is followed by the methodology followed in the development of the framework. The framework evaluation process is discussed and the validated framework is presented. Finally, the paper concludes with contributions of the study and potential further work.

2 INFORMATION SECURITY AS A SOCIAL PROBLEM

InfoSec is currently receiving more attention, given all the high-profile security breaches involving numerous organisations that deal with online users' personal information. Recently it was disclosed that a data breach at Yahoo initially reported to involve one billion user accounts and dubbed the

largest data breach in history has actually affected all three billion Yahoo user accounts (Oath, 2017). Equifax, a global credit-reporting agency experienced a data breach that exposed 143 million user records in 2017, and in the health sector Anthem had a breach that exposed 80 million patient records in 2015 (Information is Beautiful, 2019). South Africa experienced its biggest data breach in 2017 that exposed 60 million records due to a misconfigured web server (Fraser, 2017). In most cases, such breaches occur due to human error and attackers taking advantage of human weaknesses in interacting with InfoSec mechanisms. These attacks highlight the point that InfoSec problems cannot be solved through technical solutions in isolation, especially in cases where these solutions rely on human behaviour.

A holistic view of InfoSec that combines both technical and social aspects for effective solutions is needed. The unpredictable nature of user behaviour that is highly dynamic (Yee, 2004a) and difficult to objectively conceptualise highlights the need to find different approaches in tackling InfoSec problems. This has resulted in InfoSec being treated—rightly so—as a multidisciplinary field (Sveen, Torres, & Sarriegi, 2009), bringing together input from other disciplines such as computer science, engineering, social sciences, to mention but a few. In this digital age, InfoSec is increasingly becoming more of a social problem than technical. This is highlighted by the prevalence of InfoSec attacks that utilise social engineering through mediums such as social media and email exploiting human weaknesses in the security chain. Social engineering is a non-technical security attack that use deception and make users compromise computer systems by manipulating them into divulging confidential information (Whitten & Tygar, 1999). Therefore, technical solutions used in isolation are inadequate to protect InfoSec assets for both individuals and organisations.

2.1 Humans as 'weakest link'

There have been significant advances in technical aspects of IS security for protecting confidential information and data in storage and transmission. These include the use of data encryption standards, firewalls, intrusion detection systems, and biometric techniques.

Unfortunately, any IS is only as secure as its weakest link and InfoSec attacks generally look for the path of least resistance. It has long been asserted that users are the weakest link in the InfoSec chain (Crossler et al., 2013). Other scholars have argued that the assertion of weakest link is not limited to users only but to all humans that interact with IS in general. These include groups such as employees in organisations (Pfleeger, Sasse, & Furnham, 2014) and application developers (Green & Smith, 2016). The narrow view of singling out users hinders holistic solutions that need to include all aspects of human involvement in the InfoSec environment. Since most systems rely on the actions of humans, the weaknesses brought about by human interactions with the systems usually erode the technical gains. Schneier (2000) notes that the biggest security risk is the interaction between a computer system and the user, and this view is still true today.

Understanding human behaviour and how users interact with IS and InfoSec mechanisms in particular is more important in creating a secure environment and protect information assets from adversaries. Unfortunately, system designers are sometimes culpable due to design flaws that still exist in IS applications. Falk, Prakash, and Borders (2008) identified flaws in high-security

websites that designers overlook, including requesting login options on insecure pages and emailing sensitive information in plain text. Therefore, before designers expect users to comply with InfoSec requirements, the applications need to comply with basic design requirements that goes a long way in assisting a wide range of system users.

Although users have been identified as the weakest link, Green and Smith (2016) argue that most security breaches are not caused by users' errors but by developers. Therefore, effective solutions to InfoSec problems need to address technical issues and the human element (both users and developers) for creating a secure environment. The scope of this paper is limited to the usability of end-user IS that utilise InfoSec mechanisms—using online banking as a case study.

2.2 Usable security

One way to address the 'weakest link' label associated with users in their interaction with InfoSec mechanisms is to develop IS that are usable. The field of usable security essentially deals with developing secure systems that are usable. The term 'usable security' emanates from the fact that InfoSec mechanisms in IS are deemed too complicated, error-prone, and time-consuming to the intended end-users (Green & Smith, 2016). Hence, one of the strategies when developing IS that meet both InfoSec and usability requirements is to address them during system design and development. This need gave rise to the development of usable security design principles that developers can apply using a checklist.

One of the earliest landmark studies on usable security is the work of Whitten and Tygar (1999) that evaluated the usability of an encryption program 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. (Whitten & Tygar, 1999, p. 170)

Usable security strives to give equal importance to both usability and InfoSec in the design and development process of IS applications. The involvement of humans suggests the need to address social aspects of InfoSec, since technical solutions, on their own, are insufficient. Hence, IS that address both InfoSec and usability aspects are essentially a socio-technical system, which must account not only for the technical functionalities of the system, but also for social human behaviour.

3 SOCIO-TECHNICAL SYSTEM

The socio-technical system (STS) theory can be traced back to the work of Eric Trist and other social scientists at the Tavistock Institute of Human Relations in London soon after World War II (Mumford, 1995). Bostrom and Heinen (1977a) developed the STS theory that is applicable to IS as illustrated in Figure 1. In the theory, an IS is theorised as comprising of two subsystems, namely, social and technical that are independent, but interactive.

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, Huynen, Koenig, & Lenzini, 2014). This view highlights the importance of the technical aspects of the socio-technical design, 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 consists of four components, two in each subsystem that are all linked and interactive as illustrated by connection arrows in Figure 1.

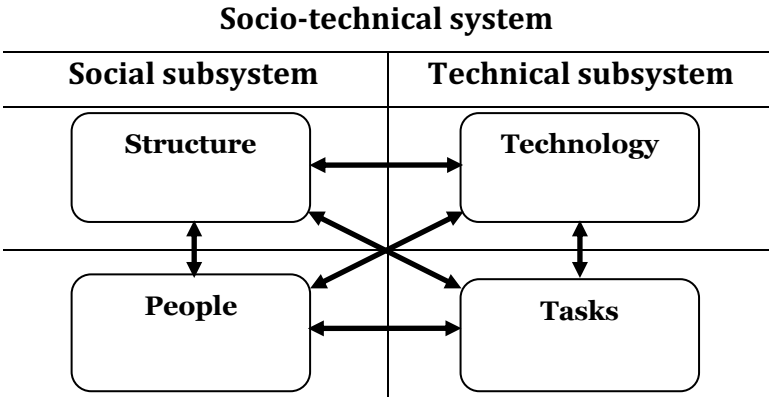

Figure 1: Socio-technical system (Bostrom & Heinen, 1977a)

STS has been used to model and explain complex work systems (Oosthuizen & Pretorius, 2016). An issue identified in the application of STS theory in IS is the lack of clear definitions of the components of the system (Alter, 2015). Given the diverse nature of IS fields, interpretations are bound to be subjective and context-dependent. A detailed discussion of each of the four components in the context of online banking is provided later in the findings section. The discussion provides a link between the design principles and the socio-technical view of online banking.

3.1 Social subsystem

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, Dalpiaz, & Giorgini, 2013). The social subsystem in an organisation may be regarded as the environment in which the organisational work system operates—based on collective attributes rather than an aggregate of individual attributes (Patnayakuni & Ruppel, 2010).

The structure component consists of organisational structures such as rules, roles, and responsibilities that guide system actors on completion of business processes. People are the system actors that include all stakeholders. This subsystem introduces ways to mitigate behavioural problems that have since been attributed to failures of information systems (Bostrom & Heinen, 1977b).

https://doi.org/10.18489/sacj.v31i1.587

3.2 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 can also be viewed as an integration of technologies, policies, and practices that describe the modes of production and users' actions when performing tasks (Bélanger, Watson-Manheim, & Swan, 2013).

3.3 Socio-technical system in information security

IS can be technically secure using advanced encryption mechanisms, but such mechanisms can fail if users misuse or bypass them. Attacks such as social engineering render technical protections ineffective. Achieving effective security, which is inherently challenging, becomes a complex and complicated goal. Hence, there is a need for a socio-technical design that strive to address social aspects of InfoSec in conjunction with technical aspects. Online InfoSec systems fit perfectly into this socio-technical definition; hence, we argue that their design can be improved by applying the approach that brings two often-contradictory fields of InfoSec and usability together. Although technical solutions in InfoSec are necessary, it is widely accepted that they are not adequate in solving InfoSec challenges in complex and ever-changing socio-technical environments (Holgate, Williams, & Hardy, 2012). This paper intends to bring these dynamics together in the context of usable security. A discussion on socio-technical aspects of InfoSec found in previous studies is outlined below.

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 in 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 InfoSec and usability goals to avoid sacrificing one of these aspects has been a challenge and a focus of research studies in both the InfoSec and human-computer interaction (HCI) communities. Essentially, the consideration of HCI elements in IS brings the social aspects of the socio-technical design to the fore. Usability is one such HCI aspect that contributes to the social goals of an IS (Ågerfalk & Eriksson, 2006).

Theoretically, Iivari and Hirschheim (1996) classify InfoSec elements in IS into three categories, namely social, technical, and socio-technical. While the social and technical views place emphasis on either social or technical aspects, respectively, a socio-technical view appreciates social and technical aspects of information system development equally.

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 InfoSec designs. 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 (Mitnick & Simon, 2002). The human element neutralises state-of-the-art technical security mechanisms, mainly

because InfoSec is not perceived as a primary goal by system users based on the unmotivated user property (Whitten & Tygar, 1999). The unmotivated user property states that users are generally unmotivated to perform security tasks, as these are viewed as being in the way of achieving production tasks. Security is usually a secondary goal; therefore, security tasks need to be seamless (Whitten & Tygar, 1999).

3.4 Heuristic evaluation

There are a number of usability inspection methods, which include cognitive walkthroughs, formal usability inspections, pluralistic walk-throughs, feature inspection, consistency inspection, standards inspection, and heuristic evaluation (Nielsen, 1994d). These methods can be used to evaluate proposed usability design principles. The suitability of each method depends on the system under investigation and decisions by the system designers. The current research uses heuristic evaluation to validate the proposed STInfoSec framework.

Oxford University Press (n.d.) defines heuristic in computing terms as "finding a solution by trial and error or by rules that are only loosely defined", with evaluation defined as "the making of a judgement about the amount, number, or value of something; assessment". Heuristic evaluation is a usability inspection method that investigates the compliance of interface features with reputable usability principles (Nielsen, 1994b). Given the subjective nature of what constitutes a usable online application, design principles also referred to as heuristics, have since been used in practice to design and evaluate usability in technology artefacts. Heuristics need to be understood in the context of system design by drawing on experience (Preece et al., 2015).

Heuristic evaluation and the use of checklists are closely linked approaches, through which an expert rates the usability of the product on a number of criteria (Lehto & Landry, 2012). The first step in a heuristic evaluation is to identify a set of usable security guidelines considered most important for the evaluated product or service. A small number of usability experts (usually five) then uses the guidelines to identify usability issues (Nielsen, 1994a). Heuristic evaluation is a cost-effective way compared to other usability testing techniques (Nielsen, 1994b). The current research involves developing a framework evaluation tool for the design of a secure and usable InfoSec system based on the literature review and findings from the quantitative and qualitative data analyses. The framework was evaluated using the heuristic evaluation method, which allows field experts to evaluate design principles based on checklist items.

4 RESEARCH METHODOLOGY

The framework presented in this paper is based on findings of a mixed methods research (MMR) design (Figure 2) that resulted in a preliminary framework published in (Mujinga et al., 2017). The data collection of the main study consisted of a quantitative survey administered to online banking users and qualitative interviews with online banking personnel as participants. There were 540 valid survey responses and six interview participants for the preliminary framework development.

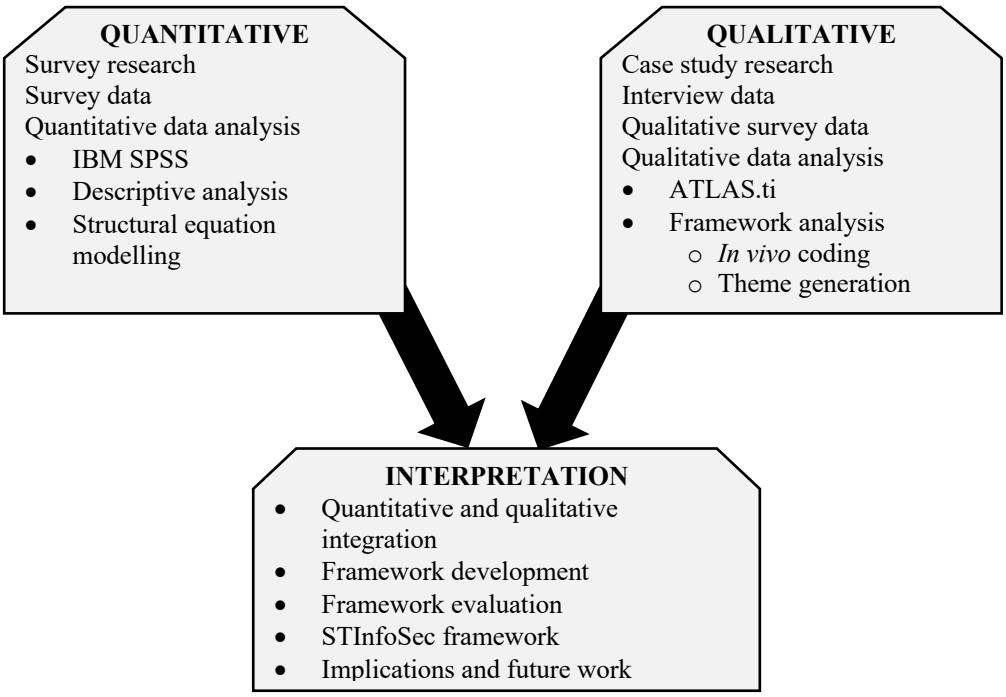

Figure 2: Convergent parallel mixed methods design (Creswell & Clark, 2017)

Creswell and Clark (2017) specifically identify the convergent parallel MMR design (Figure 2) as a suitable design of research under pragmatic philosophical assumptions. The MMR design used in this study had equal standing between quantitative and qualitative research strands, denoted by the QUAN + QUAL notation (Morse, 2010). The quantitative and qualitative research strands collected data independently, which were analysed separately, and these analyses were then combined to feed into the overall final interpretation. The combined findings from the two data sources were integrated in the framework, leading to the development of the preliminary STInfoSec framework. The preliminary framework was developed based on a combination of quantitative and qualitative findings both supplemented by literature review.

The quantitative strand investigated the perceptions of users as they interacted with an online application that significantly relies on InfoSec to fulfil its objectives. A quantitative survey was administered to online banking users to collect data on three aspects, namely, unified theory adoption and use of technology (UTAUT) model, usability principles, and InfoSec principles. The investigated constructs and principles form part of the usable security design principles in the STInfoSec framework. The usability principles belong in the social subsystem as these address the human element with regard to their interaction with IS applications. The InfoSec principles belong in the technical subsystem to provide a holistic socio-technical design.

The qualitative strand used semi-structured interviews to investigate the perceptions of the custodians of online banking on challenges faced when users interact with the service, highlighting

the impact of user behaviour on interactions with InfoSec in online applications, especially in this environment with highly sophisticated attacks and users who are not particularly computer and InfoSec savvy. The identified themes in the analysis of the interview data contribute to the principles in STInfoSec framework.

The current paper reports on the subsequent evaluation process to validate the preliminary framework. The evaluation process uses the heuristic evaluation method, which uses checklist items for the identified design principles. The field experts evaluate the significance of the checklist items for each principle and rate the importance of each in solving the usable security design problems. This paper reports on the subsequent framework evaluation conducted to validate the preliminary framework. The framework's design principles are discussed in the following preliminary framework development section.

5 PRELIMINARY FRAMEWORK DEVELOPMENT

This paper expands on the preliminary STInfoSec framework developed and published at the Americas Conference on Information Systems (Mujinga et al., 2017). The published preliminary framework focuses on identifying usable security design principles that enable developers to create InfoSec online applications that users can use.

5.1 Design principles

The preliminary framework resulted in the identification of 12 usable security design principles based on the case study used in the study—online banking. The design principles were identified through literature review and supported by both survey and interview data collection techniques. These design principles constitute the preliminary framework that is divided into six themes (see Figure 3) identified through thematic framework analysis. The themes are denoted by bold font in solid line boxes, while the corresponding principles for each theme are denoted by dotted line boxes in Figure 3. The government's role and benefits of online banking are depicted by bronze boxes; these are included for illustrative purposes as they are beyond the scope of the paper. The government is responsible for regulating the industry as such, no principles are directly linked to regulations. Nonetheless, developers highlighted the role played by regulations in online banking, as they form part of the terms and conditions that users have to abide with when agreeing to use the service. The benefits of online banking were part of data collection but not reported in this paper.

Each of the design principles is discussed in the following sections to give insights on what aspects of usability and InfoSec the principle addresses.

5.1.1 Visibility

The visibility of the system status that lets users know exactly what the capabilities of the system are, is one of the most important principles addressed by both usability and usable security scholars. Nielsen (1994c) mentions it as a criterion for usability evaluation of the user interface, while Katsabas,

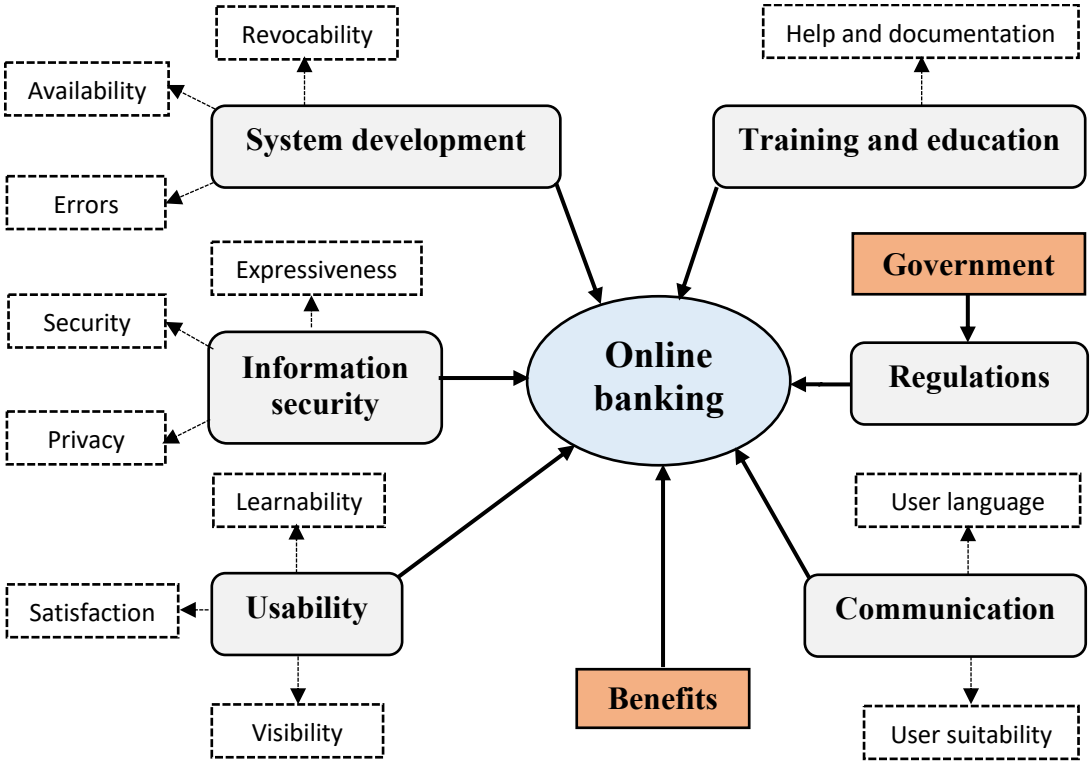

Figure 3: Mapping of themes and principles

Furnell, and Dowland (2005), Yee (2004b), and Yeratziotis et al. (2012) emphasise the principle in the context of usable security in order to let users know whether an application or user interface is using any protection mechanisms.

5.1.2 Learnability

The ability of users to efficiently and effectively use an application or user interface for the first time, as well as subsequent reuse, depends on the ease of learning the system (Preece et al., 2015). As such, learnability has been identified as an essential component in the definition of usability (Nielsen, 2010).

5.1.3 Satisfaction

Satisfaction is one of the five characteristics of usability identified by Nielsen (2010). Essentially, satisfaction in the use of a system extends beyond usability and into the realm of user experience (UX) (Bevan, 2008). User satisfaction is influenced by UX (Deng, Turner, Gehling, & Prince, 2010) through such aspects as social presence (Ogara, Koh, & Prybutok, 2014). Hedonic motivations encourage users to engage with a system, influencing the overall UX, which is a direct enabler of

user satisfaction (O'Brien, 2010; Zahidi, Lim, & Woods, 2014).

5.1.4 Errors

The principle of errors, be it for their prevention in the first place or recovery after they have occurred, is a critical design principle in all systems. Therefore, this principle is important in both usability and InfoSec design strategies. Nielsen (1994c) includes two usability principles that address error-related usability problems, namely, error prevention and help users recognise, diagnose, and recover from errors, while Schneiderman et al. (2016) suggest that user interface design should offer simple error handling to users as one of the 10 golden rules. Error handling is important in usable security to avoid critical mistakes and disclosure of sensitive and confidential digital information assets (Katsabas et al., 2005).

5.1.5 Availability

Availability is essential for online applications, which are often marketed as providing convenience by allowing users to access the service 24 hours a day. In the real world, a certain period of system downtime is expected for reasons such as system upgrades and maintenance, but these activities should be scheduled during off-peak times and kept to a minimum in terms of the frequency and duration of downtime. For example, suggest that usable security design should make sure that system services are available all the time, with minimum downtime.

5.1.6 Revocability

Users should be able to undo actions and errors, and a secure and usable system should give warning and confirmation of actions that are irreversible. Although some actions cannot be reversed after a certain stage of processing, developers need to try, by all means possible, to provide support for 'undo' and 'redo' functions. This principle is one of the ten golden rules of user interface design identified by Schneiderman et al. (2016) and Yeratziotis et al. (2012) as necessary in usable security design.

5.1.7 Expressiveness

The system should inform and guide users through security features and yet allow freedom of expression. The system's InfoSec policy must not be too rigid and difficult for users to comply with; it should, for example, prescribe safe passwords, but still allow users the freedom to create passwords they can easily remember (Yee, 2004b). This, in turn, eliminates the need for writing down passwords, which might be necessary if the system has password requirements that are too stringent.

5.1.8 User language

User language is another principle that is relevant in both the usability and usable security contexts. The principle requires the system to speak the users' language, using terms and concepts familiar

to users, while avoiding the use of technical terms (Nielsen, 1994c). This decreases the chances of users making mistakes or misunderstanding system commands.

5.1.9 User suitability

User suitability ensures that the system provides options suitable for users with diverse levels of skill and experience in security (Yeratziotis et al., 2012). Personalisation and customisation of the system are essential for user suitability and allow users to set up preferences that make it comfortable for them to use the system effectively.

5.1.10 Help and documentation

Users may need assistance, especially for applications that have been developed for a diverse group of users with different levels of skill. Support material that helps new users and system documentation for reference during usage are critical. Such material must be complete, consistent, correct, and usable for it to meet its intended goals. The principle of help and documentation is generic and is essential for all kinds of systems, products, or services. For online applications, the system needs to provide searchable help and documentation for both security and non-security tasks that are actionable with concrete steps (Schneiderman et al., 2016).

5.1.11 Security

The system should ensure a trusted path through the communication channel (usually the internet) between the end-user device and trusted servers, addressing fundamental InfoSec principles such as confidentiality, integrity, and availability, to avoid disclosure and unauthorised access of information assets in storage and in transit. Ensuring the usability of an InfoSec system should not mean a compromise in the technical functionalities of the system to protect information assets.

5.1.12 Privacy

Organisations collect personal information about their customers, some of which is sensitive, such as credit card numbers. Hence, the system should protect information provided by users against access by unauthorised parties, and it should be used only for the purposes for which it was collected in the first place. Unfortunately, organisations still have some way to go in improving protection of personal information, with an increasing number of high-profile privacy breaches.

6 EVALUATION PROCESS

The evaluation process seeks to determine the importance of the identified design principles in addressing usable security problems in online InfoSec applications. The preliminary framework went through a validation process using a heuristic evaluation method with field experts from academia and the banking industry as participants. The evaluators had expertise in InfoSec, usability and

UX. The main objective of this process was to verify the significance of the usable security design principles identified in the preliminary STInfoSec framework in addressing the problem of usable security in an online environment. Using the feedback from the evaluators, some of whom were participants in the qualitative interviews, the preliminary framework is presented as a validated framework see Figure 4 in Section 7. The evaluation process involved the following steps.

6.1 Step 1: Development of checklist items

The heuristic evaluation method uses a checklist to evaluate each identified design principle. Checklist items were created for each of the design principles identified in the preliminary framework. The checklist items came from literature studies that used the design principles. The 12 principles each had between five and nine checklist items (Appendix A).

6.2 Step 2: Data collection on checklist items

The evaluation tool was distributed through an online Google Forms tool. Participants provided importance ratings for each checklist item and the form allowed participants to provide additional comments on either the principle level or individual checklist items. The individual scores of each checklist item give the average score for the principle, thereby determining the overall evaluation of that individual principle.

Each checklist item was evaluated using a four-point Likert scale with the following scores: 1 = not important, 2 = moderately important, 3 = important, and 4 = very important. The participants rated the importance of each checklist item included in a principle to determine whether the system developers needed to consider it during system development. Consequently, the principles that scored well below average will be considered for exclusion.

6.3 Step 3: Identification of participants

The authors identified and selected suitable participants based on the relevant expertise required to obtain valuable feedback. Potential experts for participation were identified based on the expertise needed to obtain insightful feedback. The fields considered were usable security, InfoSec, usability and UX. Participants were selected from both academia and industry in order to obtain relevant knowledge from both theoretical and practical perspectives, respectively. Participants from academia were researchers working in the above-mentioned fields, while industry practitioners were banking personnel who designed and worked with digital channels. There were seven participants, who included three from academia, two from private IT organisations, and two from two of the five major banks in South Africa (see Table 1).

Participants were asked to indicate their level of expertise in the three fields of IT/IS security, usability/UX experience, and usable security using three options, namely, beginner, intermediate, and expert. Five participants were experts in at least one of the three relevant fields. Four participants had 10 or more years of experience in the relevant fields. The profiles show that participants had sufficient experience and knowledge to provide valuable feedback in the evaluation process.

https://doi.org/10.18489/sacj.v31i1.587

Table 1: Participants' profiles

Evaluator	Specialisation	Industry	Experience (years)	IT/IS security experience	Usability/UX experience	Usable security experience
E1	Usability, UI design	Academia	15	Intermediate	Expert	Intermediate
E2	Usability	Academia	11	Intermediate	Expert	Intermediate
E3	Software testing	IT company	2	Beginner	Beginner	Beginner
E4	Usable security, usability, UX	IT company	8	Intermediate	Intermediate	Intermediate
E5	Usable security, usability, UX	Bank	10	Expert	Expert	Expert
E6	Usable security, usability, UX	Bank	5	Expert	Expert	Expert
E7	Information security, usability	Academia	10	Expert	Expert	Expert

6.4 Step 4: Analysis of evaluation feedback

The evaluation feedback on the framework is explained in detail in the next section. The analysis involves incorporating any received feedback from the evaluators at both principle and checklist item levels to improve the framework. Each principle was evaluated based on checklist items distributed through an online evaluation tool. Additional feedback provided by participants is shown in Table 2 as comments for each principle. Each participant's evaluation of individual principle based on scores for individual checklist items all averaged above three (shown 'Average per participant'). The majority of principles were considered to be 'important' except 'expressiveness' that was considered to be 'moderately important' by two evaluators with an average score of 2.4. This indicates that all participants considered each principle at least 'important' for usable security design. In addition, the overall average for each principle across all participants (shown as the 'Average per principle' column) also indicates that the principle was considered by all participants to be at least 'important'. Table 2 provides the average scores for each principle as scored by each participant (denoted by E1 to E7).

Although cumulatively all principles scored above three ('important'), some individual checklist items were scored 'not important' and 'moderately important' by some participants. This was due to some reservations regarding specific checklist items in certain situations. For example, even if it is important to always provide users with detailed error messages, in some instances, too much information helps attackers. An example mentioned by one participant from a bank was not telling users whether the username or password as entered was incorrect, but just indicating that the information did not match, as this would significantly decrease the chances of a brute-force attack being successful.

https://doi.org/10.18489/sacj.v31i1.587

Table 2: Evaluation results

	Principle	E1	E2	E3	E4	E5	E6	E7	Average score
1	Visibility	3.5	4	2.7	3.7	2.7	3.3	3.7	3.4
	System has to be user friendly and direct users as to where to correct populated details.								
2	Learnability	3.3	3.6	2.6	3.8	2.8	3.4	3.4	3.3
	The learnability principle is very important especially to the older generation.								
3	Errors	3	3.6	3.4	3.1	2.5	4	3.5	3.3
	There is still a need to hide some specific error information to avoid attacks that exploit too detailed error messages. Security is always a trade-off with user experience.								
4	Availability	3	3.6	3	3.4	3	3.4	4	3.3
	The new generations want change.								
5	Satisfaction	3.2	3	2.7	3.6	2.9	2.7	4	3.2
	None								
6	Revocability	2.9	3.1	4	2.8	3	3.3	4	3.3
	A provision for cancelling option is necessary.								
7	Expressiveness	3	3.2	3	2.8	2.4	2.4	4	3.0
	None								
8	User language	3.2	4	3.6	3	4	3	4	3.5
	None								
9	User suitability	2.8	3.3	2.5	2.7	2.8	2.7	4	3.0
	Again, too much information might be dangerous. We do not state all the security capabilities of our systems to the end user.								
	Always assume the user is [a] novice especially in the information security field.								
10	Help and documentation	3.1	4	3.4	3	3.9	3.2	4	3.5
	None								
11	Privacy	3.5	4	3.9	3.8	3.8	3.8	4	3.8
	None								
12	Security	3.6	4	3.7	4	4	4	4	3.9
	None								
	Average per participant	3.2	3.6	3.2	3.3	3.2	3.3	3.9	

7 FINAL STINFOSEC FRAMEWORK

The result of the evaluation process is a set of critically informed design guidelines for online InfoSec applications such as online banking. The findings of a heuristic evaluation, which was used to validate the proposed design principles, are presented in this section to justify the retention of these principles in the final framework.

The resulting usable security design principles from both the quantitative and qualitative analyses were evaluated by field experts from both academia and the banking industry who had expertise in InfoSec, usability, and UX. The main objective of this process was to verify the significance of the usable security principles based on experts' experience and knowledge. Using the feedback from the evaluators, some of whom were participants in the qualitative interviews, the preliminary framework was finalised as a validated framework. In line with Nielsen (1994a)'s recommendations of around

five expert evaluators for a heuristic evaluation, the study obtained seven evaluations from a total of 12 invitations that were sent to potential participants.

With regard to the feedback from participants, a few suggestions were provided. One participant had reservations about system customisation to support both novice and expert users, stating the following: "Always assume the user is [a] novice especially in the information security field". This is contrary to suggestions by Nielsen (1994c) to offer support for varying skills sets. The researchers, thus, concluded that, wherever possible, support for diverse skill levels was important. Only when such a design is not possible should the system default to novice-user settings. Hence, wherever possible, support for both novices and skilled users is crucial.

The final validated STInfoSec framework after the evaluation process is presented in Figure 4. The framework provides a mapping of themes and principles in the socio-technical system, with some themes contributing to more than one component of the socio-technical matrix.

The next section briefly explains the four components of the socio-technical subsystems in relation to Figure 3, with emphasis on specific usable security principles to contextualise the framework.

7.1 Discussion

The objective of this paper is to present a validated socio-technical STInfoSec framework that assists in the design of online InfoSec applications. The discussion here outlines the four STS components based on the discussed two subsystems of STS (see Section 3), namely the social subsystem and the technical subsystem, in the context of online banking, describing what constitutes each of the four components. The social subsystem have structure and people components, while the technical subsystem consists of technology and tasks components. All four components are intertwined.

The focus of a socio-technical design is to give equal attention to both social and technical aspects of a system. In the context of InfoSec, this strives to strike a balance by designing applications that are technically secure that users can use with ease. Information systems often provide effective technical functionalities but still fail, as they do not address the complex environments in which these systems have to function (Baxter & Sommerville, 2011). InfoSec applications are not an exception, as they provide technical capabilities to protect information assets and users have since been expected to adapt and use them effectively. The socio-technical design argues for the inclusion of social aspects related to the people (especially the users) into the design, through the social subsystem that considers the role played by stakeholders through identifying such stakeholders and providing policies and procedures that govern their interaction with each other and the system.

7.2 Social subsystem

The social system is concerned with people, the relationship among them, and authority structures (Bostrom & Heinen, 1977a). More specifically, the social system is concerned with how various individuals accomplish their tasks and interact with each in their working environment to get work done (Bostrom & Heinen, 1977b). In the context of this study, the social subsystem introduces the social side of InfoSec by addressing the human element through usability principles that address the human behavioural aspects when users interact with IS.

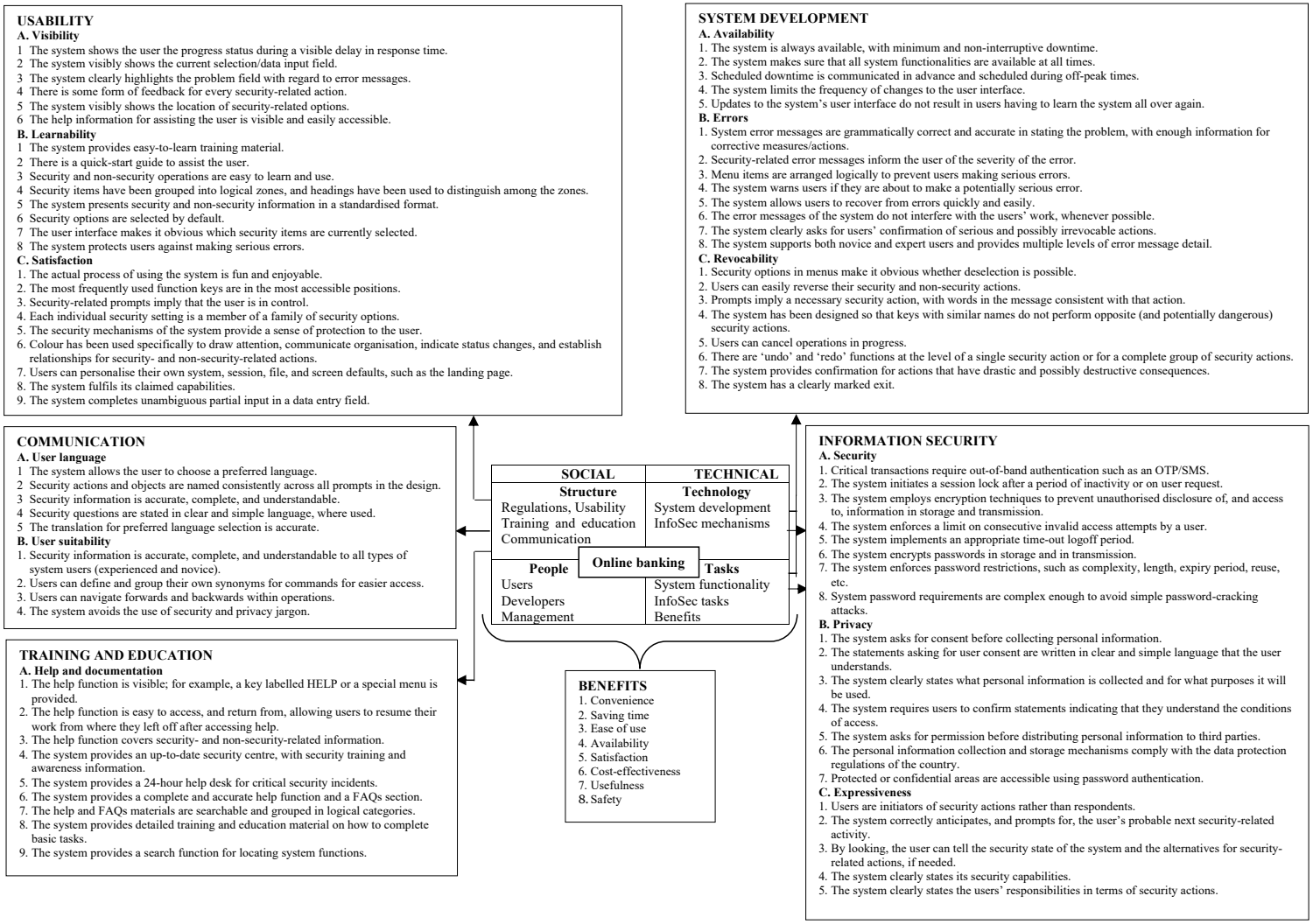

Figure 4: The final validated STInfoSec framework

7.2.1 Structure

The structure component in the social subsystem consists of regulations, communication, usability, and training and education. Regulations are a critical aspect in the structure component. However, there are no principles directly linked to regulations, since these are beyond the control of both users and developers. They are externally formulated and compliance is mandatory. Regulations are fundamental building blocks of a regulated banking environment and form the basis of terms and conditions of using online banking service. The responsibility for formulating regulations falls in the realms of the government, in consultation with business (financial institutions). Financial institutions can also form a coalition, such as the South African Banking Risk Information Centre (SABRIC) consortium, to share ideas on a variety of areas including best practices on common aspects such as InfoSec and regulations.

The government seeks to create a balance between providing a business environment where organisations can operate and make a profit, while—at the same time—protecting and looking after the interests of citizens. Such regulations in the South African context include the Protection of Personal Information (PoPI) Act for the protection of clients' personal information that organisations collect (RSA Government, 2013) and the incoming all-encompassing Cybercrimes and Cybersecurity Bill (RSA Government, 2017). The Cybercrimes and Cybersecurity Bill aims to regulate offences committed in cyberspace, an area that currently has significant shortcomings in South African legislation.

The structure component of the social subsystem also includes usability principles (visibility, learnability, and satisfaction), communication-related principles, namely user language and user suitability, and training and education strategies. Communication strategies are also part of this component. These include the preferred means of communication as selected by the user during registration for services such as online banking. Training and education has only one principle—help and documentation. This consists of any kind of assistance given to users to help them use the system effectively and efficiently. The theme of training and education also applies to the other stakeholders (developers and management) to assist them in carrying out their respective duties efficiently, although this falls outside the scope of this study.

7.2.2 People

The people component consists of stakeholders in the online banking environment; these include users, developers, and management. These people play different roles in creating a secure and usable online banking service. Like in any other system, stakeholder interaction must be coordinated with clearly defined procedures and policies to avoid duplication of duties and conflict. In an STS design, the structure component is responsible for providing these policies and procedures on how the stakeholders interact. However, there are no principles that are directly linked to the people component, since the stakeholders are implicitly responsible for developing and applying all the design principles.

7.3 Technical subsystem

The technical system consists of technology and tasks. The subsystem is concerned with tasks and technology that are needed to turn inputs into outputs (Bostrom & Heinen, 1977a). The technical aspects of InfoSec applications are concerned with protecting the information assets of an organisation. In the context of online banking, this means protecting the personal information of users from unauthorised access by adhering to the principles of the CIA (confidentiality, integrity and availability) triad.

7.3.1 Technology

The technology component in the technical subsystem consists of general system development and InfoSec mechanisms. System development ensures that the system addresses principles such as system availability, prevention of and recovery from errors, and revocability of transactions. In the context of InfoSec, the system provides technical capabilities to protect information assets in transit and in storage, such as system authentication, access control measures, and encryption mechanisms. Hence, the technology component essentially addresses actual development of InfoSec mechanisms that later provide the InfoSec tasks identified below.

7.3.2 Tasks

The second component of the technical subsystem, tasks, ensures that the system provides functionalities as expected by the users. These include actual online banking activities such as paying bills, managing accounts, and applying for new services. In addition, the system provides protection of personal and financial information using InfoSec mechanisms as provided by the system development component. These tasks are provided through the principles of security, privacy, and expressiveness.

8 CONCLUSION

The goal of this research was to assist in the development of online applications with a framework that applied 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 the potential of InfoSec attacks, while optimising positive aspects, helps to 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 InfoSec requirements, should be identified. Secondly, the design of InfoSec in online applications needs to identify the factors that make users feel inclined to bypass or ignore InfoSec mechanisms. For these reasons, we assert that a socio-technical approach to InfoSec systems design can fulfil the

goal of creating applications that are secure and usable, and the STInfoSec framework is one such approach.

The resultant product of this research is the STInfoSec framework that essentially considered InfoSec as a social problem that required a socio-technical approach for a holistic view of the problem. Using online banking as a case study, the STInfoSec framework present 12 usable security design principles for developing and evaluating this service in addressing usable security aspects, given the wide range of computer and security awareness levels of online banking users.

The validation of the preliminary STInfoSec framework was the last step in finalising the framework. This process involved applying a heuristic evaluation method based on a checklist for each design principle to investigate the compliance of interface features with reputable usability principles. This process allowed for the amendment of the design principles based on feedback from field experts, thus ensuring the suitability of the design principles in addressing security and usability requirements in an online banking system. However, no changes were deemed necessary based on the feedback from evaluators, as all 12 design principles were accepted.

In the final STInfoSec framework, the principles include each of the detailed checklist items for easy application during the development process. Besides a few concerns raised by some evaluators on some individual checklist items, none of the feedback provided required amendments to the final framework. The STInfoSec framework can be used in the process of designing and developing online InfoSec applications by applying the checklist items in addressing the identified usability and InfoSec principles.

References

Ågerfalk, P., & Eriksson, O. (2006). Socio-instrumental usability: IT is all about social action. *Journal of Information Technology*, *21*(1), 24–39. https://doi.org/10.1057/palgrave.jit.2000055

Alter, S. (2015). Sociotechnical systems through a work system lens: A possible path for reconciling system conceptualizations, business realities, and humanist values in IS development. In *1st International Workshop on Socio-Technical Perspective in IS Development (STPIS'15), Stockholm, Sweden, 9 June 2015* (pp. 32–39).

Baxter, G., & Sommerville, I. (2011). Socio-technical systems: From design methods to systems engineering. *Interacting with Computers*, *23*(1), 4–17. https://doi.org/10.1016/j.intcom.2010.07.003

Bélanger, F., Watson-Manheim, M., & Swan, B. (2013). A multi-level socio-technical systems telecommuting framework. *Behaviour and Information Technology*, *32*(12), 1257–1279. https://doi.org/10.1080/0144929X.2012.705894

Bevan, N. (2008). Classifying and selecting UX and usability measures. In *International workshop on meaningful measures: Valid useful user experience measurement, Reykjavik, Iceland, 18 June 2008* (pp. 13–18).

Bostrom, R., & Heinen, J. (1977a). MIS problems and failures: A socio-technical perspective, part 1. *MIS Quarterly*, *1*(3), 17–32. https://doi.org/10.2307/248710

Bostrom, R., & Heinen, J. (1977b). MIS problems and failures: A socio-technical perspective, part II: The applications of socio-technical theory. *MIS Quarterly*, *1*(4), 11–28. https://doi.org/10.2307/249019

Creswell, J., & Clark, V. (2017). *Designing and conducting mixed methods research* (3rd ed.). Sage.

Crossler, R., Johnston, A., Lowry, P., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computer Security*, *32*(2013), 90–101. https://doi.org/10.1016/j.cose.2012.09.010

Deng, L., Turner, D., Gehling, R., & Prince, B. (2010). User experience, satisfaction and continual usage intention of IT. *European Journal of Information Systems*, *19*(1), 60–75. https://doi.org/10.1057/ejis.2009.50

Falk, L., Prakash, A., & Borders, K. (2008). Analyzing websites for user-visible security design flaws. In *Proceedings of the fourth Symposium on Usable Privacy and Security (SOUPS), Pittsburgh, PA, 23-25 July 2008* (pp. 117–126).

Ferreira, A., Huynen, J., Koenig, V., & 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 2014* (pp. 318–329).

Fraser, A. (2017). Revealed: The real source of SA's massive data breach. Last accessed 07 Jul 2019. Retrieved from https://techcentral.co.za/revealed-real-source-sas-massive-data-breach/77626/

Green, M., & Smith, M. (2016). Developers are not the enemy! The need for usable security APIs. *IEEE Security and Privacy*, *14*(5), 40–46. https://doi.org/10.1109/MSP.2016.111

Holgate, J., Williams, S., & Hardy, C. (2012). Information security governance: Investigating diversity in critical infrastructure organizations. In *Proceedings of the 25th Bled eConference, Bled, Slovenia, 17-20 June 2012* (pp. 379–393).

Iivari, J., & Hirschheim, R. (1996). Analyzing information systems development: A comparison and analysis of eight IS development approaches. *Information Systems*, *21*(7), 551–575. https://doi.org/10.1016/S0306-4379(96)00028-2

Information is Beautiful. (2019). World's biggest data breaches. Last accessed 07 Jul 2019. Retrieved from https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Katsabas, D., Furnell, S., & 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 2005* (pp. 235–242).

Kirlappos, I., & Sasse, M. (2014). What usable security really means: Trusting and engaging users. In T. Tryfonas & I. Askoxylakis (Eds.), *Human Aspects of Information Security, Privacy, and Trust*. Springer.

Lehto, M., & Landry, S. (2012). *Introduction to human factors and ergonomics for engineers* (2nd). CRC Press.

Mitnick, K., & Simon, W. (2002). *The art of deception: Controlling the human element of security*. Wiley.

Morse, J. (2010). Principles of mixed methods and multimethod research design. In A. Tashakkori & C. Teddlie (Eds.), *SAGE Handbook of Mixed Methods in Social and Behavioral Research* (2nd, pp. 189–208). Sage.

Mujinga, M., Eloff, M., & Kroeze, J. (2017). A socio-technical approach to information security. In *Proceedings of the 23rd Americas Conference on Information Systems (AMCIS), Boston, MA, 10-12 August 2017* (pp. 1–10).

Mumford, E. (1995). Creative chaos or constructive change: Business process reengineering versus socio-technical design. In G. Burke & J. Peppard (Eds.), *Examining Business Process Re-Engineering: Current Perspectives and Research*. Kogan Page.

Nielsen, J. (1994a). Enhancing the explanatory power of usability heuristics. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Boston, MA, 24-28 April 1994* (pp. 152–158).

Nielsen, J. (1994b). Heuristic evaluation. In J. Nielsen & R. Mack (Eds.), *Usability Inspection Methods* (pp. 25–62). John Wiley and Sons.

Nielsen, J. (1994c). Ten usability heuristics. Last accessed 07 Jul 2019. Retrieved from www.nngroup.com/articles/ten-usability-heuristics/

Nielsen, J. (1994d). Usability inspection methods. In *Conference on Human Factors in Computing Systems, Boston, MA, 24-28 April 1994* (pp. 413–414).

Nielsen, J. (2010). What is usability? In C. Wilson (Ed.), *User experience re-mastered: Your guide to getting the right design* (pp. 3–22). Morgan Kaufmann.

O'Brien, H. (2010). The influence of hedonic and utilitarian motivations on user engagement: The case of online shopping experiences. *Interacting with Computers*, *22*(5), 344–352. https://doi.org/10.1016/j.intcom.2010.04.001

Oath. (2017). Yahoo provides notice to additional users affected by previously disclosed 2013 data theft. Last accessed 07 Jul 2019. Retrieved from https://www.oath.com/press/yahoo-provides-notice-to-additional-users-affected-by-previously/

Obermaier, F., Obermaier, B., Wormer, V., & Jaschensky, W. (2016). About the Panama Papers. Last accessed 07 Jul 2019. Retrieved from http://panamapapers.sueddeutsche.de/articles/56febff0a1bb8d3c3495adf4/

Ogara, S., Koh, C., & Prybutok, V. (2014). Investigating factors affecting social presence and user satisfaction with mobile instant messaging. *Computers in Human Behavior*, *36*(2014), 453–459. https://doi.org/10.1016/j.chb.2014.03.064

Oosthuizen, R., & Pretorius, L. (2016). Assessing the impact of new technology on complex sociotechnical systems. *South African Journal of Industrial Engineering*, *27*(2), 15–29. https://doi.org/10.7166/27-2-1144

Oxford University Press. (n.d.). Oxford dictionary. Last accessed 07 July 2019. Retrieved from https://en.oxforddictionaries.com

Paja, E., Dalpiaz, F., & 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 2013* (pp. 270–283).

Pasmore, W. (1988). *Designing Effective Organizations: The Sociotechnical Systems Perspective*. Wiley and Sons.

Patnayakuni, R., & Ruppel, C. (2010). A socio-technical approach to improving the systems development process. *Information Systems Frontiers*, *12*(2), 219–234. https://doi.org/10.1007/s10796-008-9093-4

Pfleeger, S., Sasse, M., & Furnham, A. (2014). From weakest link to security hero: Transforming staff behavior. *Journal of Homeland Security and Emergency Management*, *11*(4), 489–510. https://doi.org/10.1515/jhsem-2014-0035

Preece, J., Rogers, Y., & Sharp, H. (2015). *Interaction design: Beyond Human-Computer Interaction*. Wiley and Sons.

RSA Government. (2013). Protection of Personal Information Act (POPI) 4 of 2013. Last accessed 07 Jul 2019. Retrieved from http://www.justice.gov.za/inforeg/docs/InfoRegSA-POPIA-act2013-004.pdf

RSA Government. (2017). Cybercrimes and Cybersecurity Bill 2017. Last accessed 07 Jul 2019. Retrieved from http://www.justice.gov.za/legislation/bills/CyberCrimesBill2017.pdf

Schneiderman, B., Plaisant, C., Cohen, M., Jacobs, S., Elmqvist, N., & Diakopoulos, N. (2016). *Designing the user interface: Strategies for effective human-computer interaction*. Pearson Education.

Schneier, B. (2000). *Secrets and lies: Digital security in a networked world*. Wiley and Sons.

Sveen, F., Torres, J., & Sarriegi, J. (2009). Blind information security strategy. *International Journal of Critical Infrastructure Protection*, *2*(3), 95–109. https://doi.org/10.1016/j.ijcip.2009.07.003

Whitten, A., & Tygar, J. (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 1999* (pp. 169–184).

Yee, K. (2004a). Aligning security and usability. *IEEE Security and Privacy*, *1*(5), 48–55. https://doi.org/10.1109/msp.2004.64

Yee, K. (2004b). Secure interaction design. In *Proceedings of the 8th International Conference on Financial Cryptography* (pp. 114–115).

Yeratziotis, A., Pottas, D., & Greunen, D. V. (2012). A usable security heuristic evaluation for the online health social networking paradigm. *International Journal of Human-Computer Interaction*, *28*(10), 678–694. https://doi.org/10.1080/10447318.2011.654202

Zahidi, Z., Lim, Y., & Woods, P. (2014). Understanding the user experience (UX) factors that influence user satisfaction in digital culture heritage online collections for non-expert users. In *Proceedings of the Science and Information Conference, London, UK, 27-29 August 2014*.

A APPENDIX: FRAMEWORK EVALUATION TOOL

Biographical Information

Please note that the information requested here is for verification purposes only; your responses will only be identified through a pseudo name/number, with no reference to your name whatsoever.

Full name				
Gender	Male		Female	
Age				
Qualification				
Occupation				
Job title				
Job specialisation				
Years in position				
IT/IS security experience				
Usability/UX experience				
Usable security experience				
Other experience (please specify)				

Checklist Items

Your assessment is based on the importance of the 12 principles and their respective checklist items in addressing security and usability aspects of system development. Additional comments are welcome at both a checklist item and a principle level.

Please indicate your choice by selecting one of the provided options as follows: 1 = Not important, 2 = Moderately important, 3 = Important, and 4 = Very important.

1	Visibility: the system should visibly keep users informed about their security status
1.1	Does the system show the user the progress status during a visible delay in response time?
1.2	Does the system visibly show the current selection/data input field?
1.3	Does the system clearly highlight the problem field with regard to error messages?
1.4	Is there some form of feedback for every security-related action?
1.5	Does the system visibly show the location of security-related options?
1.6	Is help information for assisting the user visible and easily accessible?
	Additional comments (optional)

https://doi.org/10.18489/sacj.v31i1.587

2	Learnability: the system should ensure that security actions are easy to learn and remember
2.1	Does the system provide easy-to-learn training material?
2.2	Is there a quick-start guide to assist the user?
2.3	Are security and non-security operations easy to learn and use?
2.4	Have security items been grouped into logical zones, and have headings been used to distinguish between the zones?
2.5	Does the system present security and non-security information in a standardised format?
2.6	Are security options selected by default?
2.7	Does the user interface make it obvious which security items are currently selected?
2.8	Does the system protect users against making severe errors?
	Additional comments (optional)
3	Errors: the system should provide users with detailed security error messages that they can understand and act on
3.1	Are system error messages grammatically correct and accurate in stating the problem, with enough information for corrective measures/actions?
3.2	Do security-related error messages inform the user of the severity of the error?
3.3	Are menu items arranged logically to prevent users from making serious errors?
3.4	Does the system warn users if they are about to make a potentially serious error?
3.5	Does the system allow users to recover from errors quickly and easily?
3.6	Do the error messages of the system not interfere with the users' work, whenever possible?
3.7	Does the system clearly ask for users' confirmation of serious and possibly irrevocable actions?
	Additional comments (optional)
4	Availability: system services must be available all the time, with minimum downtime, and have minimum interruptions
4.1	Is the system always available, with minimum and non-interruptive downtime?
4.2	Does the system make sure that all system functionalities are available at all times?
4.3	Is scheduled downtime communicated in advance and scheduled during off-peak times?
4.4	Does the system limit the frequency of changes to the user interface?
4.5	Do updates to the system user interface not result in users having to learn the system all over again?
	Additional comments (optional)
5	Satisfaction: the system should ensure that users have a good experience when using the system and its security features
5.1	Is the actual process of using the system fun and enjoyable?
5.2	Are the most frequently used function keys in the most accessible positions?
5.3	Do security-related prompts imply that the user is in control?
5.4	Is each individual security setting a member of a family of security options?
5.5	Do the security mechanisms of the system provide a sense of protection to the user?
5.6	Has colour been used specifically to draw attention, communicate organisation, indicate status changes, and establish relationships for security- and non-security-related actions?
5.7	Can users personalise their own system, session, file, and screen defaults, such as the landing page?
5.8	Does the system fulfil its claimed capabilities?
5.9	Does the system complete unambiguous partial input on a data entry field?
	Additional comments (optional)

https://doi.org/10.18489/sacj.v31i1.587

6	Revocability: the system should allow users to revoke any of their security actions
6.1	Do security options in menus make it obvious whether deselection is possible?
6.2	Can users easily reverse their security and non-security actions?
6.3	When prompts imply a necessary security action, are the words in the message consistent with that action?
6.4	Has the system been designed so that keys with similar names do not perform opposite (and potentially dangerous) security actions?
6.5	Can users cancel operations in progress?
6.6	Are there 'undo' and 'redo' functions at the level of a single security action or for a complete group of security actions?
6.7	Does the system provide confirmation for actions that have drastic, possibly destructive consequences?
6.8	Does the system have a clearly marked exit?
	Additional comments (optional)
7	Expressiveness: the system should guide users on security in a manner that still gives them freedom of expression
7.1	Are users initiators of security actions rather than respondents?
7.2	Does the system correctly anticipate, and prompt for, the user's probable next security-related activity?
7.3	By looking, can the user tell the security state of the system and the alternatives for security-related actions, if needed?
7.4	Does the system clearly state its security capabilities?
7.5	Does the system clearly state the users' responsibilities in terms of security actions?
	Additional comments (optional)
8	User language: the system should use plain language that users can understand with regard to security
8.1	Does the system allow the user to choose a preferred language?
8.2	Are security actions and objects named consistently across all prompts in the design?
8.3	Is security information accurate, complete, and understandable?
8.4	Are security questions stated in clear and simple language, where used?
8.5	If language selection is possible, is the translation accurate, without errors?
	Additional comments (optional)
9	User suitability: the system should provide options for users with diverse levels of skill and experience in security
9.1	Is security information accurate, complete, and understandable to all types of system users (experienced and novice)?
9.2	Can users define and group their own synonyms for commands for easier access?
9.3	Can users navigate forwards and backwards within operations?
9.4	Does the system avoid the use of security and privacy jargon?
9.5	If the system supports both novice and expert users, are multiple levels of error message detail available?
	Additional comments (optional)

https://doi.org/10.18489/sacj.v31i1.587

10	Help and documentation: the system should make security help apparent and easy to find for users
10.1	Is the help function visible, for example, a key labelled HELP or a special menu?
10.2	Is it easy to access, and return from, the help function, allowing users to resume their work from where they left off after accessing help?
10.3	Does the help function cover security- and non-security-related information?
10.4	Does the system provide an up-to-date security centre, with security training and awareness information?
10.5	Does the system provide a 24-hour help desk for critical security incidents?
10.6	Does the system provide complete and accurate help and a FAQs section?
10.7	Is the help and FAQs material searchable and grouped in logical categories?
10.8	Does the system provide detailed training and education material on how to complete basic tasks?
10.9	Does the system provide a search function for locating system functions?
	Additional comments (optional)
11	Security: the system should provide trusted communication channels between the user and the data servers
11.1	Do critical transactions require out-of-band authentication such as an OTP/SMS?
11.2	Does the system initiate a session lock after a period of inactivity or on user request?
11.3	Does the system employ encryption techniques to prevent unauthorised disclosure of, and access to, information in storage and transmission?
11.4	Does the system enforce a limit on consecutive invalid access attempts by a user during a period of time?
11.5	Does the system implement an appropriate time-out logoff period?
11.6	Does the system encrypt passwords in storage and in transmission?
11.7	Does the system enforce password restrictions, such as complexity, length, expiry period, reuse, etc.?
11.8	Are system password requirements complex enough to avoid simple password-cracking attacks?
	Additional comments (optional)
12	Privacy: the system should protect user information against unauthorised access by third parties
12.1	Does the system ask for consent before collecting personal information?
12.2	Are the statements asking for user consent written in clear and simple language that the user understands?
12.3	Does the system clearly state what personal information is collected and for what purposes it will be used?
12.4	Does the system require users to confirm statements indicating that they understand the conditions of access?
12.5	Does the system ask for permission before distributing personal information to third parties?
12.6	Do the personal information collection and storage mechanisms comply with the data protection regulations of the country?
12.7	Can protected or confidential areas be accessed with certain passwords?
	Additional comments (optional)

https://doi.org/10.18489/sacj.v31i1.587