Computers in Human Behavior 61 (2016) 656–666

Contents lists available at ScienceDirect

Computers in Human Behavior

journal homepage: www.elsevier.com/locate/comphumbeh

Full length article

Deciding between information security and usability: Developing value based objectives

Gurpreet Dhillon [a], Tiago Oliveira [b, *], Santa Susarapu [c], Mario Caldeira [d]

[a] School of Business, Virginia Commonwealth University, 301 West Main Street, Richmond, VA, 23284-4000, USA
[b] NOVA, Information Management School, Campus de Campolide, 1070-312, Lisboa, Portugal
[c] KPMG, USA
[d] ISEG, University of Lisbon, Rua Miguel Lupi, 20, 1249-078, Lisboa, Portugal

ARTICLE INFO

Article history:
Received 29 June 2015
Received in revised form
17 March 2016
Accepted 21 March 2016
Available online 31 March 2016

Keywords:
Security values
Usability values
Value focused-thinking
Qualitative methods
Instrument development
Quantitative methods

ABSTRACT

Deciding between security and usability of systems remains an important topic among managers and academics. One of the fundamental problems is to balance the conflicting requirements of security and usability. We argue that definition of objectives for security and usability allows for deciding about the right balance between security and usability. To this effect we propose two instruments for assessing security and usability of systems, and develop them in three phases. In Phase 1 we identified 16 clusters of *means* and 8 clusters of *fundamental* objectives using the value-focused thinking approach and interviews with 35 experts. Based on phase 1, in the second phase we collected a sample of 201 users to purify, and ensure reliability and unidimensionality of the two instruments. In the third phase, based on a sample of 418 users we confirmed and validated the two instruments found in Phase 2. This resulted in 14 means objectives organized into four categories (*minimize system interruptions and licensing restrictions*, *maximize information retrieval*, *maximize system aesthetics*, and *maximize data quality*), and 10 fundamental objectives grouped into four categories (*maximize standardization and integration*, *maximize ease of use, enhance system related communication, and maximize system capability*). The objectives offer a useful basis for assessing the extent to which security and usability has been achieved in systems. The objectives also provide a decision basis for balancing security and usability.

1. Introduction

Bruce Schneier's cynical slogan, “The more secure you make something, the less usable it becomes” sums up the current state of security and usability. As we make systems more secure, genuine users try and find hacks and work around, which result in compromising security. Research in information security and usability has recognized this problem, however not much has been accomplished, largely because of two reasons. First, the requirement for security and usability of systems has always been considered as an afterthought (see, Baskerville, 1988). Two, security and usability issues have not been considered strategically and integrated into the strategic plans for developing systems. These two reason have resulted in systems that are often not aligned in terms of security and usability. Therefore the need is to identify objectives for both security and usability, collectively, that will help with proactively balancing security and usability.

In the literature the value of strategic objectives in guiding decision-making has been well researched. Keeney (1992) for instance argues that objectives and their corresponding attributes guide decision-making. And they are important for developing the overall strategy of an organization. In our case when an enterprise decides that it should strategically focus on aligning security and usability in systems, a decision context gets defined. The task then is to systematically define the objectives such that proper strategic planning can be accomplished. In terms of security and usability it is important to engage in such an exercise since both security and usability, which are two distinct quality dimensions (Kim & Park, 2012), have often been considered as after-thoughts.

In this paper we present such objectives through a detailed two-step process. First, using Keeney (1992), and Gregory and Keeney (1994) we define policy alternatives for ensuring alignment between security and usability of systems. Second, we undertake a

* Corresponding author.
E-mail addresses: gdhillon@vcu.edu (G. Dhillon), toliveira@novaims.unl.pt (T. Oliveira), susarapusr@gmail.com (S. Susarapu), caldeira@iseg.utl.pt (M. Caldeira).

http://dx.doi.org/10.1016/j.chb.2016.03.068
0747-5632/

detailed quantitative analysis to present a parsimonious set of security and usability objectives. These objectives form the basis for any alignment and balancing security and usability.

2. Literature review

Typically, in any discussion of security and usability issues, users are the first to be blamed for being the weakest link and less motivated to adopt any stringent security measures. On the contrary, Adams and Sasse (1999) recognized the importance of challenging the view that "users are never motivated to behave in a secure manner." Adams and Sasse (1999) affirm that user apathy toward not behaving in a secure manner is due to lack of user-centered design in security mechanisms. In spite for the recognition that usability of systems needs to be balanced with the security requirements, not much progress has been made within the researcher and practitioner communities. Chen, Wong, Zhang, and Techonlogies (2015), for instance note, "security for every service and application we depend on and use every day is turning into a major challenge for all of us, not just the designers, the architects, the developers, and implementers alike, but especially so for the users". Indeed security and usability are at odds with each other. Yee (2004) notes that the conflict is because implementers treat security or usability as an add-on to a system. As a result in the literature several calls have been made to consider usability and security considerations coherently.

Hoffman, Grivel, and Battle (2005) argue that "some architecture decisions may unknowingly limit the ability to implement usability requirements" (Hoffman et al., 2005, p. 469). Therefore, it is clear that security is one of the information systems architectural decisions that IT executives focus leaving critical system usability decisions unaddressed. Al Abdulwahid, Clarke, Stengel, Furnell, and Reich (2015) undertook a survey of users where they found that users systematically did not adequately protect themselves, perhaps because of the inconvenience of the technology.

Liimatainen (2005), in a study to search for usability problems of decentralized authorization systems, identifies various usability problems within systems security context and they include "authorization of entities, definition of a security policy for a resource, revocation of rights, checking validity of a set of credentials, privacy of users, and distinguishing trusted channels. Whitten and Tygar (1999) present that a security system is usable if, apart from other aspects, its users are aware of the security risks and know how to perform the necessary tasks. Additionally Al Abdulwahid et al. (2015) found that while users may be aware of the risks, yet they may not use some of the security mechanisms because of usability issues. Johnston, Eloff, and Labuschagne (2003) highlight the seemingly diverse goals of information security and human computer interaction. For example, the implementation of the most common security mechanism, such as passwords, needs to consider appropriately between security and usability. Otherwise, end-users tend to write down the passwords on notes, which completely make all the organizational policies and procedures null and void. Johnston et al. (2003) also point out that "even the most user-friendly interface could be avoided by users unless there are policies in place which enforce the use of security programs" (Johnston et al., 2003, p. 684). Some progress has been made where security and usability are being considered simultaneously. Kainda, Flechais, and Roscoe (2010), report the development of a proposed security-usability threat model, which help "understand and identify both system and external elements that are threats to a system's usability, security, or both". However, further research is required to assess when a user compromises security over usability and vice versa.

As noted, system security and system usability are core elements in the development of computer based information systems. For example, the security and usability are drives of mobile learning application and stakeholder satisfaction (Sarrab, Elbasir, & Alnaeli, 2016); web site security and usability have a significant effect on consumer trust in a financial services web site (Casalo, Flavián, & Guinalíu, 2007). In their detailed analysis of existing information systems and security research, Dhillon and Backhouse (2001) conclude that the overall security can be achieved by analyzing the behavior of constituent elements of the system. We extend this argument to postulate the core argument for this research that understanding the security and usability collectively is critical for the successful development, implementation and usage of computer based information systems. Findings of Andriotis, Oikonomou, Mylonas, and Tryfonas (2016) also support this contention. In their study Andriotis et al. found that most users prefer usability than security, particularly in the context of graphical passwords. Similarly Ruoti et al. (2016), while studying usability of secure emails, found that users prefer integrated solutions, where neither security nor usability is compromised. They also found that clarity of security procedures leads helps in building trust in the system.

As such, Dhillon and Torkzadeh (2006) used the Value Focused Thinking approach to explore and understand information system security in terms of the values of the people such as security professionals. Dhillon and Torkzadeh (2006) proposed a set of information system security objectives. Similarly, understanding the information systems usability from the perspective of the information system users and developing information system usability objectives is critical to align the security and usability objectives.

System security and system usability of computer based information systems can be immensely improved by defining the usability objectives and leveraging the existing security objectives developed by Dhillon and Torkzadeh (2006). Casting choices made by the IT stakeholders during the course of systems development process for information system security and usability as the decision making choices and defining and aligning the security and usability objectives paves the way for better development of computer based information systems.

In addition, the system security depends on the actions undertaken by the users and system administrators. Studying the existing security and usability objectives and their implementation will reveal the existing gaps and deficiencies for better security and usability. The main idea of this research is to understand the security and usability objectives within an information system and present them as design guidance for the software developers and engineers. Such design development guidance may be developed at various levels which will be helpful for the software developers and engineers (Faily, Lyle, Fléchais, & Simpson, 2015; Karat & Karat, 2003).

3. Value focused security and usability objectives

As mentioned above, methodologically this research builds on Keeney (1992) 'value focused thinking' approach. Keeney suggests that most decision-making methods are based on alternative thinking practices. He advocates that choices are made from available alternatives that are not numerous, and that are further constrained by the impositions of decision-makers. Individuals thereby tend to lose sight of what it is that they really hope to achieve. Since reaching a goal is the principal driver for being involved in any decision situation, Keeney argues that one should remain focused on the bottom-line objectives, and make decisions that are focused on meaning and value, instead of choosing only from among the alternatives found at hand. Value focused thinking is proposed as a method by Keeney, to address the most

fundamental questions - what do we want to do and why. Research conducted by Keeney (e.g. Keeney, 1992, 1999), reveals underlying values in a wide array of decision contexts. The value thinking process helps researchers and managers to be proactive, thereby creating more alternatives.

Value focused thinking calls for two main steps: (1) construct a list, based on interviews, of what users want in terms of decision-making, (2) convert these users' wishes into a common format of objectives (an object and a preference). A network hierarchy can also be put together for modeling the means and fundamental objectives. We apply this two-step method in order to assess values attached by users to IS security and usability. We contacted 35 end-users of IS/IT services among the employees of five large businesses in the US from the following industries: IT consulting, Hotel and Casino, Banking, and Education and Training. The values were elicited from the responses received in the interviews.

3.1. Construct a list of what users want

The best way to find out what users value most is to ask them. Also, it is better to ask as many users as possible because different users may have different values and they may express them differently. However, in many cases users' values are hidden under the surface. Keeney recommends several stimulation techniques to bring out these latent values. We chose a combination of two techniques to identify the latent values. The first was a wish list. Each interviewee was asked to express what their needs were in terms of security and usability of systems they used within their organizations. The second method, which augments the simple wish list, was the probing technique. In order to expand the wish list, and whenever subjects were having a problem articulating what it was that they wanted, the interviewer posed several probing questions prepared beforehand. The list of probing questions included: “If you did not have any constraints, what would your objectives be?” “What needs to be changed from the status quo?” “How do you evaluate security and usability of systems?” “What do you expect in terms of security and usability?” “How do they tell if security and usability of systems is good or bad?” Besides asking the interviewees to generate a wish list, we also asked them to generate a list of problems and shortcomings in security and usability of systems they used. The basic idea behind asking problems and shortcomings was to generate objectives by articulating their concerns. The 35 interviews generated 337 wishes/problems/concerns.

3.2. Convert statements into objectives

The interviewees' statements are then converted to objectives, using a verb (direction of change) plus an object (target of change) format. Some statements on the list are compound sentences, which produce more than one objective, and some statements were repeated by several users. For example, one user wishes “to be educated in moving between different applications and wants help when he gets lost.” Two objectives can actually be derived from this wish: (1) ease of navigation through the application and (2) enhance system training quality. To eliminate these ambiguities and redundancies, two researchers reviewed each item on the list independently. This review and refinement produced 130 objectives in a common form of a verb plus an object.

In ensuring security and usability, users wanted to achieve these 130 objectives. However, these objectives do not yet adequately articulate values, and also include duplication. The objectives were then categorized in order to surface the meanings, and the values attached to cluster the objectives. The categorization resulted in 24 clusters of objectives.

As a next step of framing values out of objectives, 24 objectives were classified into two categories: means objectives and fundamental objectives. The criterion of classification is whether an objective is an intermediate one, that is, is it a means to achieve another objective or is it a final and a fundamental one in terms of security and usability? This procedure identified 8 fundamental objectives. The means objectives, a total of 16, are shown in Table 1 and fundamental objectives in Table 2.

4. A parsimonious set of security and usability objectives

4.1. Method

In Phase 1, 150 items that influence information systems' (IS) security and usability were developed. These items were based on the total set of 130 objectives identified in phase 1. The additional 20 items were added to ensure that all objectives were well represented in the survey instrument. These items were grouped into two categories of means and fundamental objectives. The means objectives contain 91 questions (items) grouped in 16 clusters (constructs). The fundamental objectives present 59 items grouped in 8 constructs. The large number of items found in both objective sets may have led to redundancy, but it helped content validity, since we were drawing on a large universe of possible items (Boudreau, Gefen, & Straub, 2001).

Based on items found in Phase 1, we developed a questionnaire using a five-point Likert-type scale ranging from one (strongly disagree) to five (strongly agree). Respondents were asked to express agreement with 150 questions pertaining to the following context statement - *“In order to respond to the questions below, think of any system that you may be using or are familiar with. What would your ideal state be in terms of achieving your objectives?”* We received 201 responses (30.3% male, 69.7% female), for a response rate was 66.3%. The respondents had work experience in a variety of professions such as banking, sales, healthcare, information systems, engineering, and education, among other areas. All participants had experience with security and usability of IS, thus being qualified to answer this survey.

Data analysis was undertaken with several goals: purification, reliability, and unidimensionality. The following three steps were used in the elimination process:

1. We eliminated the items if their corrected item-total correlation (the correlation of each item with the sum of the other items in its category) was less than 0.5, because according to Churchill (1979), all items that belong to the same domain of the concept (construct) should be highly inter-correlated.
2. We eliminated the items if the reliability of the remaining items was at least 0.9. Cronbach's alpha was computed to see if additional items could be eliminated without substantially lowering reliability.
3. A factor analysis with varimax rotation was undertaken with the remaining items for each group to eliminate items that were not factorially pure (Weiss, 1970). We therefore eliminated items that had a loading greater than 0.3 on more than one factor. Other rotations were considered but the results were similar.

The purification of the items was done before the factor analysis, in order to produce fewer dimensions and to avoid confounding the interpretation of the factor analysis (Churchill, 1979). This methodology provides brevity and simplicity of the factor structure.

The two instruments developed in Phase 2 were tested in Phase 3. The last Phase started three months after the end of Phase 2. The instructions for respondents were exactly the same as those used in Phase 2. Participation in this study was voluntary. The respondent

Table 1
Means objectives.

Security and usability - means objectives (92 items)	
Clarify & improve system documentation	**Maximize system access**
Ensure easy access to system documentation	Define role-based external access
Improve system documentation	Ensure authorized external access
Improve system search capability	Minimize unauthorized system access
Ensure semantic based search features	**Maximize system efficiency**
Maximize efficiency of system searches	Ensure process fairness
Maximize quick search options	Ensure system is indispensable
Maximize data quality	Increase understanding of system
Enhance data integrity	Maximize system clarity
Ensure ability to execute data transfer quickly	Maximize the utility of the system
Increase ease in editing and updating of application data accurately	Monitor evolution of system capabilities
Increase timely application data access	**Maximize system esthetics**
Maximize interoperability of data manipulation	Enhance visualization of system security
Minimize redundant data collection	Ensure color combinations are visually appealing
Maximize database and system access	Ensure good application display
Ensure web access to the system	Ensure good system display
Increase consolidation of databases	Ensure visualization of system processes
Maximize accessibility	Maximize ease of navigation in GUIs
Maximize application support by real-time databases	Maximize Graphic User Interfaces
Maximize interoperability of systems and databases with mobile devices	Maximize the esthetic system features
Maximize disaster recovery	**Maximize system integrity**
Ensure data availability	Maximize system adaptability
Increase system availability	Maximize system reliability
Maximize business process continuity	**Maximize system maintainability**
Maximize disaster recovery support	Ensure hardware robustness
Maximize productivity	Ensure systems are up to date
Ensure automated password retrieval	Maximize automatic system upgrades
Increase reliability of system performance	Maximize system version control
Maximize system efficiency	Minimize application licensing restrictions
Maximize system performance	Minimize the total cost of ownership
Maximize the system productivity	**Maximize system dependability**
Maximize security & privacy	Maximize process execution accuracy
Decrease restrictiveness of system	Maximize reliable real-time processing
Maximize automatic data encryption	Maximize system owners' responsibility for errors
Maximize confidentiality of data	Minimize application risks
Maximize identity theft protection features	**Maximize task efficiency**
Maximize multi-layer security	Maximize automation of manual tasks
Maximize recognition of trusted and secure devices	Maximize efficiency of system tasks
Maximize single-sign-on authentication	Maximize flexibility in task processing
Maximize trust in security in network connections	**Minimize system interruptions**
Maximize self-efficacy in training	Minimize system down-time
Enhance system training quality	Minimize system freezes and crashes
Ensure user support is context specific	Minimize system response time
Implement good demos for user support	Minimize unnecessary system lock outs & time outs
Maximize accessibility of user support	
Maximize real-time user support	
Maximize reliable user support	
Minimize the training required to use the system	

rate was 79.6%. We obtained a sample of 418 (179 male, 239 female) respondents; 65.3% had an undergraduate degree and 33.8% a post-graduate degree; ages ranged from 18 to 60 years old (mean, 24.91) All participants had work experience in a variety of professions such as banking, sales, healthcare, information systems, engineering, and education, among other areas. All participants had experience with security and usability of IS, thus being qualified to answer this survey.

Based on the sample of 418 respondents, for the identification of the simplest factor structure and the interpretation solutions for each of the two types of objectives, in Phase 3 we applied one factor analysis to mean objectives and another to fundamental objectives, and in both we used a varimax rotation (we also tried other rotations, but the results were similar). The ratio of the sample to the number of items (28:1 for means objectives and 35:1 for fundamental objectives) was greater than the minimum required for factor analysis, that is of 10 subjects per item (Everitt, 1975; Kerlinger, 1978). We also estimated the internal consistence (corrected item-total correlation) and reliability (alpha) for the two instruments proposed. Finally, the correlation matrix for each instrument was analyzed for convergent and discriminant validity (Doll & Torkzadeh, 1988; Torkzadeh & Dhillon, 2002). The convergent validity was tested if the correlations between measures of the same theoretical construct are different than zero and large enough to warrant further investigation (Campbell & Fiske, 1959). The discriminant validity was tested if for each item it correlates more highly with the item's own theoretical factor than an item of another factor (Doll & Torkzadeh, 1988).

Table 2
Fundamental objectives.

Security and usability - fundamental objective (59 items)	
Enhance system related communications	**Maximize system capability**
Ensure exception reports go to management	Enhance application features
Ensure stakeholders' intentions are considered	Enhance e-commerce features
Increase communication of system enhancements	Enhance explanatory features in the system
Maximize automatic escalation alerts	Enhance geographic location features
Minimize user interaction with system developers	Enhance standard multi-language support
Minimize users' interaction with technical personnel	Ensure tracking of products
Improve data organization	Ensure useful reporting features
Ensure data archival functionality	Maximize global trading features
Ensure data retrieval feature	Maximize speech recognition capabilities
Increase organization of online and offline data	Maximize system reporting capabilities
Maximize ease of use	**Maximize system integration**
Ensure ease of navigation through application	Ensure functionality is designed into system
Ensure simplicity of the applications	Maximize flexibility of system components
Ensure system usage is intuitive	Maximize hardware compatibility
Ensure the user friendly features	Maximize system interoperability
Maximize convenience of application use	Maximize system software compatibility
Maximize ease of system navigation	Minimize multiple system platforms
Maximize ease of system operability	**Maximize user requirements elicitation**
Maximize ease of system use	Ensure system functionality meets requirements
Minimize number of system operating steps	Maximize automated internal controls
Maximize standardization of system features	Maximize collaboration through system use
Enhance customizable interfaces	Maximize intelligence in applications
Ensure clarity and conciseness in standard error messages	Maximize user collaboration in systems
Maximize functional standardization	Maximize user interaction
Maximize standardized automatic user notification alerts	Minimize user confusion
Minimize system configuration or customizations	Proactively design applications
Maximize system administration functionality	
Enhance connectivity at affordable price	
Ensure system features are organized	
Maximize ease of system installation	
Maximize system administration features	

4.2. Data

4.2.1. Phase 2 - means objectives

We performed the item procedure described above to purify the means objectives category. First, a corrected item-total correlation of less than 0.5 suggests the elimination of 29 items. Second, the reliability analysis does not eliminate any item. Finally, the factor analysis suggests an elimination of 47 more items.

After the elimination process, 15 items of the means objectives category were obtained. Table 3 shows the results of the factor analysis using varimax rotation for the retained items. Bartlett's test of sphericity was 1278.4 ($p < 0.001$). This means that the data contain enough common variance to perform a factor analysis. Kaiser-Meyer-Olkin (KMO) measures the adequacy of the sample; KMO is 0.88 (KMO $\geq$ 0.80 is good (Sharma, 1996)), which reveals that the correlation matrix is adequate for the factor analysis. The results of the factor analysis yielded four factors with eigenvalues greater than one. These factors explain 67.5% of the variance contained in the data.

The four factors identified were easily interpreted, they are: minimize system interruptions and licensing restrictions (five items), maximize information retrieval (four items), maximize system esthetics (three items), and maximize data quality (three items). The range of loadings is respectively: 0.55–0.73, 0.62–0.74, 0.59–0.81, and 0.56–0.74. All of the factors have a loading greater than 0.5. This indicates that our analysis employs a well-explained factor structure.

The range of corrected item-total correlation varies between 0.55 and 0.69 for *minimize system interruptions and licensing restrictions*, 0.65 to 0.74 for *maximize information retrieval*, 0.60 to 0.66 for *maximize system esthetics*, and 0.53 to 0.61 for *maximize data quality.*

The reliability for each construct is: 0.84 for minimize system interruptions and licensing restrictions, 0.86 for maximize information retrieval, 0.80 for maximize system esthetics, and 0.75 for maximize data quality. The overall reliability for the 15 item scale was 0.88. The reliability thus exceeds the suggested cutoff value of 0.70 (Nunnally, 1978).

4.2.2. Phase 2 - fundamental objectives

To purify the fundamental objectives category we used the same item purification procedure. The first criterion was to eliminate items below 0.5, allowing us to eliminate 17 of the 59 items obtained in Phase 1. The second criterion, reliability analysis, did not eliminate any items. Finally, the factor analysis suggested eliminating 30 more items.

Following the elimination process, the fundamental objectives scale included 12 items. First, Bartlett's test of sphericity was 1292.3 ($p < 0.001$). These factors explain 76.5% of the variance contained in the data. The KMO is 0.82 (KMO $\geq$ 0.80 is good [29]), revealing that the correlation matrix is adequate for factor analysis, and that the data contain enough common variance to perform the factor analysis. Four factors with eigenvalues greater than one are obtained (Table 4), and the interpretation of each factor was not difficult, i.e.: *maximize standardization, integration and user requirements* (4 items), *maximize ease of use* (3 items), maximize system capability (3 items), and *enhance system related communications* (2 items). The ranges for factor loading were, respectively, 0.61–0.86, 0.56–0.85, 0.62–0.75, and 0.87–0.87. All the factors have a loading greater than 0.5, indicating that our analysis employs a well-explained factor structure.

The range of corrected item-total correlation for each item varies

Table 3
Factor analysis of means objectives in Phase 2 (n = 201).

	F1	F2	F3	F4	Corrected item-total correlation	Alpha	Alpha overall
Minimize system interruptions and licensing restrictions							
Minimize unnecessary system lock outs & time outs	0.73				0.69	0.84	
Minimize system interruptions	0.73				0.64		
Minimize application licensing restrictions	0.71				0.64		
Minimize the total cost of ownership	0.63				0.63		
Minimize system down-time	0.55				0.55		
Maximize information retrieval							
Maximize efficiency of system tasks		0.74			0.74	0.86	
Maximize task efficiency		0.73			0.71		0.88
Maximize system efficiency		0.71			0.72		
Maximize database and system access		0.62			0.65		
Maximize system esthetics							
Ensure color combinations are visually appealing			0.81		0.66	0.80	
Ensure good application display			0.68		0.66		
Maximize system esthetics			0.59		0.60		
Maximize data quality							
Enhance data integrity				0.74	0.61	0.75	
Increase timely application data access				0.68	0.59		
Increase ease in editing and updating of application data accurately				0.56	0.53		
Eigenvalue	5.77	1.70	1.38	1.26	–		
% Variance	38.5%	11.3%	9.2%	8.4%	–		

Note: loadings greater than 0.3 are reported; the items are grouped by highest factor loading and presented in descending order.

from: 0.61 to 0.78 for *maximize standardization, integration and user requirements*, 0.59 to 0.74 for *maximize ease of use*, 0.61 to 0.72 for maximize system capability, and 0.81 to 0.81 for *enhance system related communications*. The reliability scores were 0.87, 0.83, 0.82, and 0.89 respectively for each construct. The overall reliability for the 18 item scale was 0.88, exceeding the suggested cutoff value of 0.70 (Nunnally, 1978).

In short, the results obtained in Phase 2 show good reliability and validity measures for both instruments developed (means objectives: 4-factor with 15 items; fundamental objectives: 4-factor with 12 items).

4.2.3. Phase 3 – means objectives

Based on the 15 items obtained in Phase 2 for means objectives we initialized Phase 3. In this phase a factor analysis with the varimax rotation was applied without specifying the number of factors. Four factors had eigenvalues greater than one and the scree-plot confirmed a four-factor model. One item ("*maximize database and system access*") had a loading of less than 0.5 for all factors. This means that this item did not belong to any factor and for this reason was eliminated. We then applied a factor analysis with the varimax rotation to the 14 remaining items obtained in Phase 2. Table 5 shows the four factors with eigenvalues greater than one, the items are grouped by highest factor loading and presented in descending order. Bartlett's test was statistically significant ($p < 0.001$) and the KMO was 0.86, meaning that the data are adequate for a factor analysis (Sharma, 1996).

Except for one item, the four factors are exactly the same as found in Phase 2. This corroborates the instrument obtained in Phase 2 for means objectives. The four factors explain 68.8% of the variation in the 14 items. The interpretation is uncomplicated, i.e., *minimize system interruptions and licensing restrictions* (five items), *maximize information retrieval* (three items), *maximize system esthetics* (three items), *maximize data quality* (three items), explains respectively 36.3%, 13.4%, 11.0%, and 8.1% of the variance. All the items that belong to the factor have a loading greater than 0.5, indicating that our analysis employs a well-explained factor structure.

All corrected item-total correlations for each item of each factor are greater than 0.5 (Table 5), meaning that the items of each

Table 4
Factor analysis of fundamental objectives in Phase 2 (n = 201).

	F1	F2	F3	F4	Corrected item-total correlation	Alpha	Alpha overall
Maximize standardization, integration and user requirements							
Maximize standardization of system features	0.86				0.78	0.87	
Maximize functional standardization	0.82				0.77		
Maximize system interoperability	0.64				0.67		
Maximize automated internal controls	0.61				0.65		
Maximize ease of use							
Maximize ease of use		0.85			0.74	0.83	0.88
Maximize ease of system use		0.77			0.73		
Maximize ease of system navigation		0.56			0.59		
Maximize system capability							
Enhance explanatory features in the system			0.75		0.72	0.82	
Enhance geographic location features			0.73		0.69		
Enhance e-commerce features			0.62		0.61		
Enhance system related communications							
Minimize user interaction with system developers				0.87	0.81	0.89	
Minimize users' interaction with technical personnel				0.87	0.81		
Eigenvalue	5.17	1.62	1.26	1.13	–	–	–
% Variance	43.0%	13.5%	10.5%	9.4%	–	–	–

Note: loadings greater than 0.3 are reported; the items are grouped by highest factor loading and presented in descending order.

Table 5
Factor analysis of means objectives in Phase 3 (n = 418).

	F1	F2	F3	F4	Corrected item-total correlation	Alpha	Alpha overall
Minimize system interruptions and licensing restrictions							
Minimize unnecessary system lock outs & time outs	0.79				0.72	0.84	
Minimize application licensing restrictions	0.69				0.64		
Minimize system interruptions	0.67				0.63		
Minimize the total cost of ownership	0.63				0.62		
Minimize system down-time	0.61				0.60		
Maximize information retrieval							
Maximize efficiency of system tasks		0.78			0.76	0.86	0.86
Maximize task efficiency		0.76			0.73		
Maximize system efficiency		0.69			0.71		
Maximize system esthetics							
Ensure color combinations are visually appealing			0.84		0.71	0.81	
Ensure good application display			0.69		0.64		
Maximize system esthetics			0.67		0.64		
Maximize data quality							
Enhance data integrity				0.80	0.64	0.75	
Increase timely application data access				0.67	0.57		
Increase ease in editing and updating of application data accurately				0.54	0.53		
Eigenvalue	5.09	1.88	1.55	1.14	–	–	–
% Variance	36.3%	13.4%	11.0%	8.1%	–	–	–

Note: loadings greater than 0.3 are reported; the items are grouped by highest factor loading and presented in descending order.

construct belong to the same domain of the concept (Churchill, 1979). The overall reliability for the 14 items scale is 0.86, and for each construct is 0.84, 0.86, 0.81 and 0.75, respectively for *minimize system interruptions and licensing restrictions*, *maximize information retrieval*, *maximize system esthetics*, and *maximize data quality*. The reliability exceeds the suggested cutoff value of 0.70 (Nunnally, 1978).

We analyzed the item's correlation matrix (Table 6) for convergent and discriminant validity. For the convergent validity test we analyzed the smallest correlations within each factor, which are (respectively): minimize system interruptions and licensing restrictions (0.43); maximize information retrieval (0.63); maximize system esthetics (0.50); maximize data quality (0.42). All are (statistically) significantly different than zero ($p < 0.001$) and large enough to encourage further investigation (Campbell & Fiske, 1959; Doll & Torkzadeh, 1988; Torkzadeh & Dhillon, 2002).

Based on Table 6 we tested discriminant validity. Each of the 14 items is more highly correlated with the other items in its factor (values inside the triangles) than with any item of other factors. This means that there are zero violations (out of 182 comparisons) of condition for discriminant validity. For example, the smallest correlation between the item F1_1 MO and the other items of its factor is 0.49, which is higher than the highest correlation between F1_1 MO with any of the items of the other factors (the highest correlation is 0.34).

Table 6
Correlation matrix of items of means objectives in Phase 3 (n = 418).

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
F1_1 MO (1)														
F1_2 MO (2)	**0.63**													
F1_3 MO (3)	**0.58**	**0.50**												
F1_4 MO (4)	**0.52**	**0.46**	**0.47**											
F1_5 MO (5)	**0.49**	**0.43**	**0.47**	**0.52**										
F2_1 MO (6)	0.28	0.26	0.36	0.33	0.27									
F2_2 MO (7)	0.24	0.22	0.31	0.26	0.27	**0.70**								
F2_3 MO (8)	0.34	0.22	0.39	0.36	0.28	**0.67**	**0.63**							
F3_1 MO (9)	0.29	0.29	0.21	0.25	0.22	0.18	0.14	0.25						
F3_2 MO (10)	0.25	0.24	0.20	0.25	0.24	0.29	0.29	0.37	**0.62**					
F3_3 MO (11)	0.31	0.29	0.22	0.25	0.28	0.22	0.23	0.33	**0.62**	**0.53**				
F4_1 MO (12)	0.19	0.14	0.18	0.24	0.20	0.35	0.34	0.36	0.14	0.18	0.17			
F4_3 MO (13)	0.16	0.10	0.14	0.24	0.20	0.32	0.31	0.29	0.19	0.19	0.16	**0.57**		
F4_3 MO (14)	0.23	0.18	0.19	0.21	0.22	0.36	0.38	0.38	0.14	0.20	0.19	**0.51**	**0.42**	
Mean	4.00	3.76	4.09	4.00	4.06	4.18	4.22	4.20	3.46	3.97	3.60	4.14	4.04	4.13
Sdev	0.97	1.00	0.93	0.95	0.90	0.74	0.72	0.79	1.03	0.83	0.95	0.83	0.78	0.77

Notes: F1_1 MO - Minimize unnecessary system lock outs & time outs; F1_2 MO - Minimize application licensing restrictions; F1_3 MO - Minimize system interruptions; F1_4 MO - Minimize the total cost of ownership; F1_5 MO - Minimize system down-time; F2_1 MO - Maximize efficiency of system tasks; F2_2 MO - Maximize task efficiency; F2_3 MO - Maximize system efficiency; F3_1 MO - Ensure color combinations are visually appealing; F3_2 MO - Ensure good application display; F3_3 MO - Maximize system esthetics; F4_1 MO - Enhance data integrity; F4_2 MO - Increase timely application data access; F4_3 MO - Increase ease in editing and updating of application data accurately.

4.2.4. Phase 3 – fundamental objectives

In Phase 2 of fundamental objectives we obtained 12 items, and based on these items we initialized Phase 3. We also applied a factor analysis with varimax rotation without specifying the number of factors, obtaining four factors with an eigenvalue greater than one. Once more there was an item ("*maximize automated internal controls*") with loading less than 0.5 for all factors. This item did not belong to any factor and for this reason was eliminated. Another item ("*enhance explanatory features in the system*") had loadings greater than 0.30 in two factors, meaning that this item is not pure and for this reason was eliminated. Then, based on the 10 items retained we applied a factor analysis with the varimax rotation. Table 7 shows the four factors with eigenvalues greater than one. The scree-plot also confirmed a four-factor model. The items are grouped by highest factor loading and presented in descending order. Bartlett's test was statistically significant ($p < 0.001$) and the KMO was 0.78, meaning that the data are adequate for a factor analysis (Sharma, 1996).

Except for two items, the four factors are the same as found in Phase 2. This means that the second instrument verifies the results obtained in Phase 2. The interpretations of four factors are simple, i.e., *maximize standardization and integration* (3 items), *maximize ease of use* (3 items), *enhance system related communication* (2 items), and *maximize system capability* (2 items). These four factors explain 79.4% of the variation in the 10 items. The "*maximize standardization and integration*" and "*maximize ease of use*" explain 57.4% of variance. This reveals that these two factors are extremely important for developing of security and usability of the systems.

In Table 7 we can see that the corrected item-totals are greater than 0.5, i.e. items of each construct belong to the same domain. The reliability scores were 0.86 for *maximize standardization and integration*, 0.83 for *maximize ease of use*, 0.85 for *enhance system related communication,* and 0.73 for *maximize system capability*. The overall reliability for the 10 items scale was 0.85. All reliability scores were higher than the cutoff value of 0.7 suggested by Nunnally (1978).

Table 8 shows the correlation matrix of the 10 items, to test convergent and discriminant validity. To test convergent validity we analyzed the smallest correlation within factors, finding: *maximize standardization and integration* was 0.61; *maximize ease of use* was 0.54; *enhance system related communication* was 0.74; *maximize system capability* was 0.66. All are (statistically) significantly different than zero ($p < 0.001$) and large enough to encourage further investigation (Campbell & Fiske, 1959; Doll & Torkzadeh, 1988; Torkzadeh & Dhillon, 2002). To test the discriminant validity we examined the correlation matrix, which reveals zero violations (out of 90 comparisons), i.e. each of the 10 items are more highly correlated with the other items in its factor than with any item of other factors (Campbell & Fiske, 1959).

Fig. 1 summarizes the three phases. In short, the two instruments developed (means objectives: four factors with 14 items; fundamental objectives: four factors with 12 items) have internal consistency, reliability, and convergent and discriminant validity.

5. Discussion

Our research identified four security and usability fundamental objectives, which together guide software development and implementation. The objectives are developed through a rigorous process of interviewing and statistical validation. The objectives are: *maximize ease of use, and enhance system related communication, maximize standardization and integration, maximize system capability*. In the literature, each of the objectives may have been independently considered to be important, albeit not in the context of security and usability. In this paper, we argue that security and usability should be considered collectively, but there is a lack of guidance as to how this task can be accomplished. Strategic objectives help us in providing a frame of reference and a structured approach when involved in software development activities. The importance of structured approaches has previously been highlighted in the literature. Shropshire and Gowan (2015), for instance, argue for simple structured approaches and propose one for updating security controls. In paragraphs below we discuss each of the fundamental objectives.

Maximize ease of use. Earlier research suggests that perceived ease of use affects perceived usefulness and, in turn, behavioral intention to use (Bhattacherjee & Lin, 2015; Venkatesh, 2000). However, the measures are not entirely useful to a typical system developer (*viz.* constructs such as perceptions of internal control, computer anxiety, playfulness, etc.). From a security and usability perspective, perhaps ease of system navigation and the general perception of being easy to use would seem to be more logical.

Enhance system related communication. Another important aspect is linked to system related communications. A variety of proposals have been advanced In the literature, ranging from development of *hybrid managers* (Burgess & Currie, 2013; Earls & Skyrme, 1992) who can help bridge the gap between technical system developers and actual users, to the development of intrinsic competencies for harnessing technology (G. Dhillon, 2008). While all of these may offer theoretical opportunities, in organizations we

Table 7
Factor analysis of fundamental objectives in Phase 3 (n = 418).

	F1	F2	F3	F4	Corrected item-total correlation	Alpha	Alpha overall
Maximize standardization, integration and user requirements							
Maximize standardization of system features	0.85				0.78	0.86	
Maximize functional standardization	0.82				0.77		
Maximize system interoperability	0.60				0.64		
Maximize ease of use							
Maximize ease of use		0.87			0.74	0.83	
Maximize ease of system use		0.76			0.72		
Maximize ease of system navigation		0.58			0.59		0.85
Enhance system related communications							
Minimize users' interaction with technical personnel			0.84		0.74	0.85	
Minimize user interaction with system developers			0.83		0.74		
Maximize system capability							
Enhance geographic location features				0.74	0.58	0.73	
Enhance e-commerce features				0.67	0.58		
Eigenvalue	4.28	1.47	1.19	1.01	–	–	–
% Variance	42.7%	14.7%	11.9%	10.1%	–	–	–

Note: loadings greater than 0.3 are reported; the items are grouped by highest factor loading and presented in descending order.

Table 8
Correlation matrix of items of fundamental objectives in Phase 3 (n = 418).

	1	2	3	4	5	6	7	8	9	10
F1_1 FO (1)										
F1_2 FO (2)	**0.79**									
F1_3 FO (3)	**0.61**	**0.61**								
F2_1 FO (4)	0.33	0.34	0.34							
F2_2 FO (5)	0.44	0.41	0.46	**0.74**						
F2_3 FO (6)	0.39	0.34	0.42	**0.57**	**0.54**					
F3_1 FO (7)	0.20	0.20	0.18	0.17	0.29	0.19				
F3_2 FO (8)	0.27	0.28	0.19	0.24	0.31	0.26	**0.74**			
F4_1 FO (9)	0.33	0.37	0.39	0.27	0.30	0.27	0.28	0.27		
F4_2 FO (10)	0.29	0.30	0.29	0.25	0.27	0.29	0.30	0.27	**0.58**	
Mean	3.94	3.90	3.88	4.31	4.26	4.26	3.48	3.46	3.65	3.78
Sdev	0.77	0.77	0.82	0.75	0.77	0.79	1.09	1.10	1.01	0.95

Notes: F1_1 FO(1) - Maximize standardization of system features; F1_2 FO(2) - Maximize functional standardization; F1_3 FO(3) - Maximize system interoperability; F2_1 FO(4) - Maximize ease of use; F2_2 FO(5) - Maximize ease of system use; F2_3 FO(6) - Maximize ease of system navigation; F3_1 FO(7) - Minimize users' interaction with technical personnel; F3_2 FO(8) - Minimize user interaction with system developers; F4_1 FO(9) - Enhance geographic location features; F4_2 FO(10) - Enhance e-commerce features

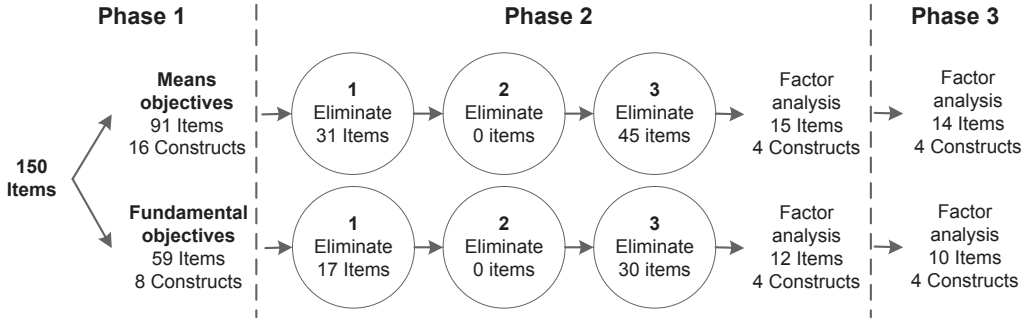
are typically still waiting to see adequate management of interactions between users and the technical staff. Inability to deal with such relationships results in systems being abused or used improperly, thereby posing considerable security challenges.

Maximize standardization and integration. The importance of standardization and integration in security and usability cannot be overestimated (Seckler, Heinz, Forde, Tuch, & Opwis, 2015; Yoon & Steege, 2013). A casual review of various security and usability standards itself suggests a great many options. Although ISO standards such as ISO 9241 1995 exist, in the usability community there is lack of consensus regarding the conformance methods. Dzida (1996) notes:

> "If a product is claimed to meet a standard, the procedure used in testing the product against the requirements should be specified to guarantee reproducibility of results. Some standards prescribe a certain test method, some recommend a method, and some inform the reader that the procedure used in testing is a matter of negotiation between the parties involved."

While ISO 27799 standard benefits the information security community, yet there are also other competing standards (*viz*. SSE-CMM among others). Perhaps one of the reasons for the inadequacy of existing standards, as well as their large number, is a lack of a core of objectives that need to be achieved in managing security and usability. More often than not the standards seem to be cobbled together to fit an *ad hoc* purpose.

Our research has identified four very interesting standardization requirements – standardization of features, functional standardization, interoperability, and automated internal controls. As a case in point, the reader might simply consider academic university websites across institutions. Perhaps some functional and feature standardization would be convenient, as would access and availability of information. Failure to build such features not only makes it difficult to navigate systems, it also exposes institutions to a number of vulnerabilities (e.g. see website breaches at Utkal University India and St Louis University USA, among others).



Note: 1 – Eliminate items if item-total correlation were less than 0.5; **2** – eliminate items if the reliability of the remaining items was at least 0.9; **3** – eliminate items that were not pure (loading on more than one factor at 0.30 or above) were also eliminated.

Fig. 1. Three phases of item purification process.

Maximize system capability. It goes without saying that enhancing system capability ensures increased security and usability. The challenge, however, is to identify features that need enhancing. Prior research often points to increased explanatory features in systems. Researchers have argued that explanation of features allows systems to be more usable (e.g. see Hof, 2013 among others). Alpár, Hoepman, and Siljee (2013) have also argued that enhancing capability ensures that security, privacy and usability issues are adequately addressed.

Our research reveals that fundamental benefits for security and usability can be realized if there is a corresponding appreciation of the means to achieve the fundamental objectives. Means objectives identified in this study include: *minimize system interruptions and licensing restrictions*, *maximize information retrieval*, *maximize system aesthetics*, and *maximize data quality*.

Our study finds that the higher licensing costs and poor quality of systems and data result in bypassing legal software and many of its controls. This poses a serious threat to the integrity of systems. A well-known consequence of circumventing properly licensed software is that virus and malware problems creep in. Grabosky and Smith (2001) argue that proper guardianship helps to prevent such vulnerabilities. Guardians are also known to facilitate system usability. Retrieval of information from systems is also a well-researched topic area and resides at the intersection of security and usability dimensions. Griffith and Jakobsson (2005) note that mother's maiden name, a usual means to retrieve data from financial institutions, can actually be obtained with great accuracy from public records. Some progress has been made by adding personal knowledge questions for information retrieval, but more so for fallback authentication. From a security and usability perspective enough thought has not gone into the strategic aspects of information retrieval and their relationship to security and usability. Our research indicates that this is an important objective for consideration. The issue of guardianship also related to managing tradeoffs between security and usability. Nguyen, Rosoff, and John (2016) found, "in the trade-off between encryption and usability, we found that the privacy premium in the unspecified condition is significantly greater than the privacy premium in the government condition. However, the privacy premiums in the snooping, crime, and marketing conditions were not significantly differed from the unspecified group. Furthermore, the privacy premium under the government condition was significantly less than the premium under the crime."

Another important aspect identified in our study pertains to data quality. Poor data quality has been recognized in the literature as having two implications. First, the security of an enterprise becomes compromised (see, Redman, 1998). This is because security is directly linked to the accuracy of data. Second, usability of the system comes into question. If the system and the data therein are not useful (Arts, de Keizer, & Scheffer, 2002), or if the data are out of context, there is typically a loss of ownership. This results in very serious security problems.

Theoretical and practical contributions. The major theoretical contribution of the security and usability objectives discussed in this paper is their intertwined nature. Security and usability have been routinely treated as separate constructs. Researchers have given slight consideration to the security implications of low usability systems or to the implications of highly secure systems on lack of usability (see, Arts, et al., 2002; DeWitt & Kuljis, 2006; Redman, 1998; Yee, 2004). While both of these issues are worthy of investigation, the research on them to date falls short of providing a strategic direction for secure and usable system development. We believe that our research provides a theoretical framework for addressing security and usability. The major tenets of our theoretical contribution are:

- Well-grounded security and usability objectives that are based on the values of individuals. Value based objectives are considered much better for strategic planning relative to the alternative based objectives (see, Leon, 1999).
- Our value proposition combines security and usability. While calls for aligning the two have been made in the literature (DeWitt & Kuljis, 2006), there has been almost no follow up research. By combining the two constructs we have in many ways presented a well-aligned set of security and usability objectives.

At a practical level, the findings reported in this paper offer requirement objectives that system developers should use to design security and usability into the systems. Typically security has been considered as an afterthought in the design process (G. Dhillon & Torkzadeh, 2006), and usability has been addressed in a like manner. While system developers seem to develop their own processes in addressing security and usability concerns, putting a structured framework into place is certainly a preferred way to move forward. The guidance provided by the security and usability objectives described herein forms a solid, theoretically grounded, empirically derived basis for the range of development tasks.

6. Conclusion

This paper examines the combination of security and usability of systems in three phases. In Phase 1 we developed value-focused security and usability objectives. A qualitative approach revealed 150 objectives, 91 means objectives, and 59 fundamental objectives, grouped respectively into 16 and 8 means and fundamental objectives. A quantitative approach was developed in Phases 2 and 3. In Phase 2 the aim was the purification, reliability, and unidimensionality, from which a parsimonious set of security and usability objectives were derived. Fifteen means objectives were obtained, grouped in four constructs, and 12 fundamental objectives were obtained, grouped in four constructs. In Phase 3, based on the sample of 418 users, we confirmed and validated the two sets of objectives developed in Phase 2. For means objectives we found four factors (based on 14 items), which are: *minimize system interruptions and licensing restrictions*, *maximize information retrieval*, *maximize system aesthetics*, and *maximize data quality*. For fundamental objectives, we also found four factors (based on 10 items) which are: *maximize standardization and integration*, *maximize ease of use*, *enhance system related communication, and maximize system capability*. In summary, the two instruments proposed have internal consistency, reliability, and convergent and discriminant validity. We believe that this paper offers a good basis for better understanding of security and usability objectives. With further research the instruments presented in this paper could be validated even further.

References

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

Al Abdulwahid, A., Clarke, N., Stengel, I., Furnell, S., & Reich, C. (2015). Security, privacy and usability–a survey of users' perceptions and attitudes. In *Trust, privacy and security in digital business* (pp. 153–168). Springer.

Alpár, G., Hoepman, J.-H., & Siljee, J. (2013). The identity crisis security, privacy and usability issues in identity management. *Journal of Information System Security, 9*(1), 23–53.

Andriotis, P., Oikonomou, G., Mylonas, A., & Tryfonas, T. (2016). A study on usability and security features of the android pattern lock screen. *Information & Computer Security, 24*(1), 53–72.

Arts, D. G. T., de Keizer, N. F., & Scheffer, G. J. (2002). Defining and improving data quality in medical registries: a literature review, case study, and generic framework. *Journal of the American Medical Informatics Association, 9*(6), 600–611.

Baskerville, R. (1988). *Designing information systems security*. John Wiley & Sons, Inc.

Bhattacherjee, A., & Lin, C.-P. (2015). A unified model of IT continuance: three

complementary perspectives and crossover effects. *European Journal of Information Systems, 24*(4), 364–373.
Boudreau, M. C., Gefen, D., & Straub, D. W. (2001). Validation in information systems research: a state-of-the-art assessment. *MIS Quarterly, 25*(1), 1–16.
Burgess, N., & Currie, G. (2013). The knowledge brokering role of the hybrid middle level manager: the case of healthcare. *British Journal of Management, 24*(S1), S132–S142.
Campbell, D. T., & Fiske, D. W. (1959). Convergent and discriminant validation by the multitrait-multimethod matrix. *Psychological Bulletin, 56*(2), 81–105.
Casalo, L. V., Flavián, C., & Guinalíu, M. (2007). The role of security, privacy, usability and reputation in the development of online banking. *Online Information Review, 31*(5), 583–603.
Chen, J., Wong, M., Zhang, L., & Techonlogies, H. (2015). Security and usability. In L. T. Sørensen, & K. E. Skouby (Eds.), *User requirements for wireless* (pp. 77–98). Denmark: River Publishers.
Churchill, G. A. (1979). Paradigm for developing better measures of marketing constructs. *Journal of Marketing Research, 16*(1), 64–73.
DeWitt, A. J., & Kuljis, J. (2006). Aligning usability and security: a usability study of Polaris. In *Proceedings of the second symposium on Usable privacy and security* (pp. 1–7). Pittsburgh, Pennsylvania: ACM.
Dhillon, G. (2008). Organizational competence for harnessing IT: a case study. *Information & Management, 45*(5), 297–303.
Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: towards socio-organizational perspectives. *Information Systems Journal, 11*(2), 127–153.
Dhillon, G., & Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. *Information Systems Journal, 16*(3), 293–314.
Doll, W. J., & Torkzadeh, G. (1988). The measurement of end-user computing satisfaction. *MIS Quarterly, 12*(2), 259–274.
Dzida, W. (1996). International usability standards. *ACM Computing Surveys, 28*(1), 173–175.
Earls, M. J., & Skyrme, D. J. (1992). Hybrid managers — what do we know about them? *Information Systems Journal, 2*(3), 169–187.
Everitt, B. S. (1975). Multivariate analysis: the need for data and other problems. *British Journal of Psychiatry, 126*, 237–240.
Faily, S., Lyle, J., Fléchais, I., & Simpson, A. (2015). Usability and security by design: a case study in research and development. In *NDSS workshop on usable security*. Edinburgh: Heriot Watt University.
Grabosky, P., & Smith, R. (2001). Telecommunication fraud in the digital age: the convergence of technologies. In D. S. Wall (Ed.), *Crime and the internet*. London: Routledge.
Gregory, R., & Keeney, R. L. (1994). Creating policy alternatives using stakeholder values. *Management Science, 40*(8), 1035–1048.
Griffith, V., & Jakobsson, M. (2005). Messin' with Texas deriving mother's maiden names using public records. In J. Ioannidis, A. Keromytis, & M. Yung (Eds.), *Applied cryptography and network security, proceedings* (pp. 91–103). Berlin: Springer-Verlag Berlin.
Hof, H.-J. (2013). Towards enhanced usability of it security mechanisms-how to design usable it security mechanisms using the example of email encryption. *International Journal on Advances in Security, 6*(1&2), 78–87.
Hoffman, D., Grivel, E., & Battle, L. (2005). Designing software architectures to facilitate accessible web applications. *IBM Systems Journal, 44*(3), 467–483.
Johnston, J., Eloff, J. H., & Labuschagne, L. (2003). Security and human computer interfaces. *Computers & Security, 22*(8), 675–684.
Kainda, R., Flechais, I., & Roscoe, A. (2010). Security and usability: analysis and evaluation. In *Availability, reliability, and security, 2010. ARES'10 international conference on* (pp. 275–282). IEEE.
Karat, J., & Karat, C.-M. (2003). The evolution of user-centered focus in the human-computer interaction field. *IBM Systems Journal, 42*(4), 532–541.
Keeney, R. L. (1992). *Value-focused thinking*. Cambridge, Massachusetts: Harvard University Press.
Keeney, R. L. (1999). The value of internet commerce to the customer. *Management Science, 45*(4), 533–542.
Kerlinger, F. N. (1978). *Foundations of behavioral research*. New York: McGraw-Hill.
Kim, B. C., & Park, Y. W. (2012). Security versus convenience? An experimental study of user misperceptions of wireless internet service quality. *Decision Support Systems, 53*(1), 1–11.
Leon, O. G. (1999). Value-focused thinking versus alternative-focused thinking: effects on generation of objectives. *Organizational Behavior and Human Decision Processes, 80*(3), 213–227.
Liimatainen, S. (2005). Usability of decentralized authorization systems-a comparative study. In *System sciences, 2005. HICSS'05. Proceedings of the 38th Annual Hawaii International Conference on*. IEEE, 186b–186b.
Nguyen, K. D., Rosoff, H., & John, R. S. (2016). The effects of attacker identity and individual user characteristics on the value of information privacy. *Computers in Human Behavior, 55*, 372–383.
Nunnally, J. C. (1978). *Psychometric theory*. New York: McGraw-Hill.
Redman, T. C. (1998). The impact of poor data quality on the typical enterprise. *Communications of the ACM, 41*(2), 79–82.
Ruoti, S., Andersen, J., Heidbrink, S., O'Neill, M., Vaziripour, E., Wu, J., et al. (2016). "We're on the same page": a usability study of secure email using pairs of novice users. In *CHI'16. San Jose, CA, USA*.
Sarrab, M., Elbasir, M., & Alnaeli, S. (2016). Towards a quality model of technical aspects for mobile learning services: an empirical investigation. *Computers in Human Behavior, 55*, 100–112.
Seckler, M., Heinz, S., Forde, S., Tuch, A. N., & Opwis, K. (2015). Trust and distrust on the web: user experiences and website characteristics. *Computers in Human Behavior, 45*, 39–50.
Sharma, S. (1996). *Applied multivariate techniques*. New York: John Wiley & Sons, Inc.
Shropshire, J., & Gowan, A. (2015). Towards structured implementation of network security policies. *Journal of Information System Security, 11*(1), 2–27.
Torkzadeh, G., & Dhillon, G. (2002). Measuring factors that influence the success of internet commerce. *Information Systems Research, 13*(2), 187–204.
Venkatesh, V. (2000). Determinants of perceived ease of use: integrating control, intrinsic motivation, and emotion into the technology acceptance model. *Information Systems Research, 11*(4), 342–365.
Weiss, D. J. (1970). Factor analysis and counseling research. *Journal of Counseling Psychology, 17*(5), 477–485.
Whitten, A., & Tygar, J. D. (1999). Why Johnny can't encrypt: a usability evaluation of PGP 5.0. In *Usenix security* (Vol. 1999).
Yee, K. P. (2004). Aligning security and usability. *IEEE Security & Privacy, 2*(5), 48–55.
Yoon, H. S., & Steege, L. M. B. (2013). Development of a quantitative model of the impact of customers' personality and perceptions on internet banking use. *Computers in Human Behavior, 29*(3), 1133–1141.