Exploring End-User Smartphone Security Awareness within a South African context

Jacques Ophoff* and Mark Robinson†
Centre for Information Technology and National Development in Africa (CITANDA)
Dept. of Information Systems
University of Cape Town
Cape Town, South Africa
Email: *jacques.ophoff@uct.ac.za †mark@linecom.co.za

***Abstract*—International research has shown that users are complacent when it comes to smartphone security behaviour. This is contradictory, as users perceive data stored on the 'smart' devices to be private and worth protecting. Traditionally less attention is paid to human factors compared to technical security controls (such as firewalls and antivirus), but there is a crucial need to analyse human aspects as technology alone cannot deliver complete security solutions. Increasing a user's knowledge can improve compliance with good security practices, but for trainers and educators to create meaningful security awareness materials they must have a thorough understanding of users' existing behaviours, misconceptions and general attitude towards smartphone security.**

The primary purpose of this research was to assess the level of smartphone security awareness displayed by the public, determining whether a general level of security complacency exists amongst smartphone users. The study was undertaken in a South African context (a multi-cultural developing nation) and included demographics as a variable in assessing any differences in smartphone security awareness between population groups. A modified version of the instrument developed by [1] was used.

A survey of 619 South African users examined trust of smartphone application repositories, users' considerations when installing new applications and their use of protection mechanisms (security controls). The sample proved complacent in their smartphone security behaviours with users displaying high levels of trust towards smartphone application repositories, rarely considering privacy and security considerations when installing new applications and also not adequately protecting themselves through adopting smartphone protection mechanisms (controls). The research did not find any conclusive associations to suggest that a user's home language impacts their information security behaviour or trust. However, an association between IT expertise and the adoption of smartphone security controls was found.

***Index Terms*—Smartphone, Awareness and Training in Security, Mobile Computing Security.**

I. Introduction

International research has shown that users, and university students in particular, are complacent when it comes to security behaviour in using smartphones [1]–[3]. This is a contradictory phenomenon as users perceive data stored on the 'smart' devices to be private and worth protecting [4], [5]. Smartphone adoption is ever-increasing with sales forecasts showing that the number of smartphones shipped now exceeds that of basic and feature phones. These devices are prone to theft, loss and damage and resultantly pose a significant information security risk to individuals and organisations alike.

Traditionally less attention is paid to human factors compared to technical security controls (such as firewalls and antivirus), but there is a crucial need to analyse human aspects as technology alone cannot deliver complete security solutions [6]. Understanding users is necessary to bridge the perceived disconnect between security managers and users in creating more effective and workable security measures; as well as sustaining good security practice by ensuring cooperation and engagement [6]–[8].

Increasing a users knowledge can improve compliance with good security practices [9]. However, for trainers and educators to create meaningful security awareness materials they must have a thorough understanding of users' existing behaviours, misconceptions and general attitude towards smartphone security [10]. The main objective of this research is to explore the level of smartphone security awareness in South Africa through analysing security perceptions (knowledge) and related behaviours.

The paper proceeds as follows: first a literature review of security, specifically related to smartphones is presented. Next the chosen research methodology is discussed. Thereafter the collected data is analysed and findings are presented. The paper concludes with recommendations for future research.

II. Literature Review

Information security can be defined as "the protection of information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability" [11]. Information security and privacy is a key concern for modern enterprise with the Society for Information Management (SIM) survey consistently ranking security and privacy in the top ten concerns facing US IT managers and top twenty concerns globally [12]. Information security and privacy is not only a concern for organisations but should be mirrored by individual end-users who also perceive their information to be private and worth protecting [4], [5].

End-users are increasingly reliant on mobile devices and it is expected that the stated growth in smartphone adoption will result in mobile internet usage exceeding that of traditional desktop computers by the year 2015; with the stated change in device adoption, consumers are increasingly using mobile

978-1-4799-3383-9/14/$31.00 ©2014 IEEE

devices for sensitive tasks such as email, banking and purchasing goods and services [5]. This is evidenced by the gradual conversion from E-Commerce to M-Commerce [13].

Information security research and practice has traditionally focused on mostly external facing technical solutions (such as firewalls and antivirus) to secure information assets and has paid little attention to behavioural information security but this is no longer effective [6]. Security controls also have to be designed with human behaviour in mind [8]. Information security should be a holistic approach involving technical, behavioural, philosophical and organisational approaches [14]. That said, this paper is primarily focused on the behavioural aspects of information security.

A. Security-related Theories

Behavioural information security focuses on human behaviour through awareness and education and aims to protect information systems from a human perspective. Information security awareness is defined as an end-users general knowledge about information security and their ramifications [8]. Researchers have used or adapted several theories in assessing users' behaviour and security awareness – the most frequently used theories include:

- The theory of reasoned action (TRA), or the extended theory of planned behaviour (TPB), posits that intentions are rational antecedents of any actions or behaviour [15]. [16] applied the framework to information security, suggesting that an employees intentions are positively influenced by normative beliefs and self-efficacy to comply with security policies.
- General deterrence theory (GDT) focuses on rational decision making to misuse information systems based on knowledge of sanctions or punishment [17].
- Protection motivation theory (PMT) posits that dealing with threats is a result of predicting protective behaviours. Research into employees has shown that attitudes are shaped by evaluating the threat and coping appraisal [16].
- The technology acceptance model (TAM) introduced by [18] has been applied in an information systems context to suggest that the intention to safeguard information assets is influenced by both perceived usefulness and perceived ease-of-use [19].

When combined these theories tend to suggest that security awareness (knowledge) influences users attitude to information security and their behaviour. This is supported by research by [16]. Further research has shown that the perception of information security may be likened to a type of risk perception and that there is a positive correlation between this perception (through knowledge) and both the adoption of IT appliances and the following of security practices [9].

B. Smartphone Risks and Threats

Smartphones are mobile phones which have advanced beyond ubiquitous telephony functionality; increasingly mirroring functionality found on computers as a result of having modern mobile operating systems which support a wide range of general-purpose applications termed apps [20]. Applications range from familiar web browsing, email and calendaring applications to interactive 3D applications, social networking and mapping tools [5]. Smartphones do not run uniform operating systems or hardware platforms; as a result each available operating system or variant thereof, has its own unique attributes and employs different approaches. Currently there is a global convergence in the market towards two operating systems: Google's Android and Apple's iOS.

Smartphones face several of the same threats as traditional computers but are different in that they are prone to physical loss and theft, physical damage and are often improperly disposal of which results in these devices being of considerable risk [21]. [22] identified several threats which are not dissimilar to those of traditional computers: malware, attacks on individuals, hacking and denial of service [3]. The term attacks on individuals is vague, and is likely to include several threats such as eavesdropping, unwarranted surveillance and tracking, identity theft, social-engineering, phishing and the increasing direct billing fraud [23].

C. App Repositories as an Attack Vector

A salient difference between traditional shrink-wrapped software and smartphone applications is the manner in which applications are disseminated. Smartphones increasingly make use of centralised distribution architectures termed app repositories or marketplaces – which may be operated by platform vendors or third parties [1]. Smartphone vendors have taken different approaches to the installation of third-party applications which can be placed on a continuum depending on the amount of control retained by the vendor [24]:

- The *walled garden* model is characterised by the vendor retaining full control as users can only install applications distributed through the vendors official application repository. These applications are vetted and monitored and can be removed, remotely uninstalled or disabled by the vendor at will. This is the strongest approach in terms of security as most security decisions are retained by the vendor.
- The *guardian* model is similar to the walled garden but security decisions are left to a trusted third party.
- Unlike the walled garden the *end-user control* model leaves the user responsible for security decisions and users are able to install software from any source; consequently this is a far more flexible approach but is also weaker as all control and vetting by the vendor are lost.

D. Smartphone Security Controls

Approaches and controls are not dissimilar from traditional PCs but smartphone platforms are not as mature and as such often limit users ability to secure their devices and information properly [26]. Fragmentation in smartphone user interfaces result in various menus and settings for configuring smartphone security controls which decreases the ease in which security controls can be deployed [27]. Security controls include but are not limited to: authentication – password and personal

TABLE I
RELATED RESEARCH ON SMARTPHONE SECURITY AWARENESS

Authors	Sample Demographic	Findings
Chin, Felt, Sekar, and Wagner (2012) [2]	USA	Users are less likely to perform sensitive tasks on mobile devices as there is a lack of edification and misconceptions about security of applications exist.
Jones and Heinrichs (2012) [3]	USA	College students do not practice good smartphone security; partaking in high-risk activities while not making use of security controls. This study confirmed previous research.
Kelley, Cranor, and Sadeh (2013) [25]	USA	Android respondents view and read permissions screens but have limited understanding of the messages. Sample was unaware of security risks associated with mobile apps and market places.
Mylonas, Kastania, and Gritzalis (2013) [1]	Greece	General security complacency exists, with smartphone users: trusting application repositories, not fully using security controls and disregarding security during application selection and installation.

identification number (PIN), firewalls, remote management, and encryption and antivirus software [21].

Passwords, which are more complex in nature, allow for better protection than PINs; however their use is curtailed by users preferring the convenience of not entering passwords each time they wish to use their device [21]. Antivirus software is available for most smartphone platforms with numerous vendors supporting products; however the efficacy of the solutions is questionable [4].

E. Related Research

Previous research has shown that users, and university students in particular, are complacent when it comes to their security behaviour. A summary on related studies is shown in Table I.

Historically there is a lack of academic research to assess general security awareness in developing countries where socio-cultural environments, constrained resources and limited knowledge present higher barriers to the promotion of security awareness [28]. In addition, [1] and [3] are limited as the research does not compare security awareness across different demographics and user sub-groups. The next section discusses the research methodology employed in the current study.

III. RESEARCH METHODOLOGY

The intention of this research is to provide an exploratory and descriptive examination of users' smartphone security awareness. A survey strategy was used, with a positivist approach to guide the quantitative analysis. An inductive approach formed the basis of the research by providing answers to the exploratory research questions within a South African context.

A. Research Questions

The primary purpose of this research is to assess the level of smartphone security awareness displayed by users in a South African context (a multi-cultural developing nation). It includes demographics as a variable in assessing any differences in smartphone security awareness between population groups. The potential relationship between home language and smartphone security awareness is also explored. This leads to the following research questions:

1) Do smartphone users trust applications from the official app repository?
2) Do users consider security while choosing and downloading applications?
3) Do smartphone users enable security controls on their devices?
4) Does home language or culture influence user security awareness?

B. Research Instrument

A modified online instrument based on the questionnaire by [1] was used. Modifications consisted mainly of additional control questions, additional response options and rewording of questions for improved understanding. The final research instrument consisted of 35 questions. The research instrument questions were intended to answer one, or several, of the research questions, as mapped in Table II.

A pilot study was undertaken to ensure that there were no technical problems with the online survey platform, instructions and questions were clear and unambiguous, and to gauge the questions' validity and reliability.

C. Target Population and Sampling

The target population for the study was smartphone users whose devices were not controlled and protected by organisational IT policies using tools such as mobile device management (MDM) or mobile application management (MAM). Security controls imposed on users by IT managers potentially impacts their ability to install applications at will, and the proposed research intends to assess user perception of applications and official application repositories.

Non-probability, self-selection sampling was used as it was difficult to ascertain potential respondents' characteristics, beliefs or practices when it comes to security awareness. A link to the online research instrument was distributed electronically to various segments of the population using social media platforms and a mailing list at a large university.

The next section presents the data analysis and findings of the primary data collected from the research instrument.

IV. DATA ANALYSIS AND FINDINGS

A total of 856 recorded questionnaire responses were received. Of the 856 recorded responses, 100 (11.7%) were

TABLE II
RESEARCH QUESTION TO INSTRUMENT MAPPING

Research Question	Instrument Questions
1) Do smartphone users trust applications from the official app repository?	15, 16, 17, 18, 34, 35
2) Do users consider security while choosing and downloading applications?	16, 19, 20, 22, 23, 24
3) Do smartphone users enable security controls on their devices?	25, 26, 27, 28, 29
4) Does home language or culture influence user security awareness?	7, 8

rejected during the analysis, as the respondents failed to fully complete the questionnaire. Of the remaining 756 complete responses, 12 respondents stated that they do not reside in South Africa and their responses were rejected as the research is intended to assess smartphone security awareness domestically. Of the remaining 744 participants a respondent indicated that he/she was less than 18 years old and for ethical reasons the respondent was not allowed to continue with the research questionnaire. Furthermore 81 respondents indicated that they did not own smartphones and of the smartphone owners 43 indicated that their devices were managed by a third party. All of these responses were rejected. After the aforementioned data cleaning, the remaining 619 responses will hereafter be referred to as 'the sample' for analysis.

A. Demographic Profile

The majority of respondents were between the age of 18–25 (64.9%), with a further minority (12.9%) being between 26–30. The sample predominantly consisted of students (62.8%) and working adults (36.67%), with the remainder stating that neither was applicable to them. The recorded responses were almost equal among males (53.8%) and females (46.2%). The majority of respondents stated their native language as *English* (66.88%). While the majority of respondents were white (51%) all other race groups (in a South African context) were represented in the sample, as illustrated in Figure 1.

As illustrated in Figure 2 most respondents had a self-perception that their level of IT expertise was above average, with the majority of respondents classifying their IT expertise as *Good* (38.4%), followed by *Moderate* (30.69%) and *Excellent* (17.93%).

Only a small minority of respondents had completed an information security course (7.4%), most of whom work in the Information Technology, Telecommunications, and Software and Computer Services industries. There was a definite association between having an information security qualification and perceived IT expertise, as expected.

The breakdown of top mobile platforms used by respondents is shown in Table III. The dominant platform is Google's *Android* (46.7%) with even more adoption than in [1]. For comparison South African industry statistics from 2012 is also shown [29].

Answer		Response	%
Black		142	23%
Chinese		7	1%
Coloured		66	11%
Indian		40	6%
White		317	51%
Other		7	1%
Prefer not to answer		40	6%
Total		619	100%

Fig. 1. Respondents' Ethnicity

B. Trust in App Repositories

As expected the majority of respondents who use iOS (88.6%) trust the official Apple app store as Apple has taken a walled-garden approach where they retain full control over the installation [24]. What is of concern is that the majority of Symbian users (88.89%) trust the official Symbian repository, as Nokia has chosen an application installation approach that lies between the guardian and end-user control.

Among the sample respondents woman were more trusting than men (85% vs. 77%) concerning the official application repositories of their chosen platforms. In addition, users who shared their phones with others were more likely to trust application repositories (87.33% who share vs. 73.98% who don't).

Although high levels of trust were displayed towards application repositories, 64% of respondents were unaware as to whether applications available in the official repository have undergone any form of security testing. Only a small minority (25.7%) stated that they believed applications had undergone some form of testing. This finding reinforces the fact that respondents blindly trust application repositoriesand are similar to [1], who found 54.6% of respondents were unaware. As expected, respondents who believed that application repositories do test applications were more likely to exhibit trust towards official application repositories.

Smartphone vendors have taken different approaches to security and the installation of third-party applications. Not

Answer		Response	%
Excellent		111	18%
Good		238	38%
Moderate		190	31%
Fair		66	11%
Poor		14	2%
Total		619	100%

Fig. 2. Respondents' Self-Perceived IT Expertise

TABLE III
RESPONDENTS' BY MOBILE PLATFORM

Platform	Current Research	RSA 2012 [29]	GRC 2013 [1]
Android	46.7%	8%	38.4%
Blackberry	26.2%	48%	9.2%
iOS	18.4%	<4%	23.8%
Symbian	4.4%	40%	16.6%

all applications repositories test and vet applications before allowing distribution to users and as such it is useful to assess differences between platform user groups. A significant number of respondents from each platform incorrectly stated that applications available on the official application repositories are not tested: Android 13.49%; iOS 6.14%; Blackberry 8.64%; Windows Phone: 10.53%. Interestingly, of those who (incorrectly) stated that applications available on the official application repositories are not tested, 53.13% trusted application repositories as secure. Additionally, it is of concern that a majority of users who perceived their IT expertise as *Excellent* were the same users who incorrectly stated that application repositories do not test applications.

C. Security in Application Selection and Installation

It was found that 99.03% of participants install additional third-party applications on their smartphones (an illustrative example of the popular WhatsApp application was given in the questionnaire). Data utilised in this sub-section was a subset of the filtered dataset – only including those that expressly state that they install third-party applications. The most cited consideration for installing new third-party applications was perceived usefulness (47%), followed by price (9%), ratings and reviews (9%), popularity (9%), and perceived ease of use (8%).

The majority (76.3%) of respondents were aware of the existence of smartphone malicious software. Understandably users who perceive their IT expertise to be better, or those with information security training, were more knowledgeable about the existence of malicious smartphone software. It was also found that men were more likely to be aware of malicious software than women (84.68% vs. 66.43%).

Only 6.95% of respondents claimed to consider privacy and security ramifications before installing new applications. The majority of respondents (51%) stated that they only sometimes pay attention to security messages during the installation of a new application; only 10% stated that they never pay any form of attention to security messages. There was no significant difference between life stages. Symbian users (48%) were most likely to always pay attention to security messages during installation, followed by 41.32% of Android users. Blackberry users were the least likely to pay attention to security messages.

Respondents seemed to be more concerned with security messages than licensing messages (agreements) with an alarming total of 37.6% of respondents never paying any attention to licensing messages – a mere 18.7% always pay attention to licensing messages. 41.1% of students never pay any attention to licensing messages. Windows Phone users were the most likely to pay attention to licensing messages (27.78%) followed by Android (20.14%) and Blackberry users (18.63%). iOS users were the most ignorant when it comes to paying attention to licensing messages. Those that paid attention to licensing messages were more inclined to pay attention to security messages as well.

Answer		Response	%
Smartphone		163	27.03%
PC/Laptop/Netbook		584	96.85%
Tablet		81	13.43%
Other		17	2.82%

Fig. 3. Respondents' Use of Security Software in Various Devices

Not surprisingly 80.3% of all respondents (74.8% of students) stated that they do not prefer pirated applications to the purchasing of authentic applications. Respondents who use the Android platform showed the highest propensity to prefer pirated applications, whereas iOS users displayed the least – this could be because of the difficulty in installing pirated applications on iOS devices where devices need to be *jail-broken* to circumvent the control over the installation of applications imposed by Apple. South African respondents were far less likely to prefer pirated applications than in [1]. Younger respondents were more likely to favour pirated applications than older respondents.

A small, yet significant 9.5% of respondents (8.5% of students) admitted to *jail-breaking* their devices. Respondents who have actively jail-broken their devices were more likely to prefer pirated applications but this was to be expected as jail-breaking circumvents certain application installation security model controls to allow users to install pirated applications.

D. Security Controls Used

As Figure 3 illustrates, few users use smartphone security software (27.03%), compared to a traditional PC/Laptop/Netbook (96.85%). Of the respondents, 61.4% indicated that they were aware of the existence of smartphone security software and 50.52% stated that they have searched an application repository for free smartphone security software. Strangely, of the respondents who were aware of smartphone security software and believed it to be essential (55.53%) only 42.11% used smartphone security software.

Users of Apple's iOS were the least likely to have adopted security software, which is likely a result of limited availability of such software given Apple's garden-wall approach to application installations. Android users were the most likely to have adopted security software. [1] suggests this could be because of perceived resource (battery) usage, however very few respondents indicated that 'resource intensity' was a consideration when installing applications. Respondents who were aware of smartphone security software were more inclined to consider smartphone security software as being essential. In addition such users were also more inclined to search application repositories for free smartphone security software.

A large proportion of respondents (72.24%) have adopted the most basic smartphone protection mechanism (SIM PIN). However, this may be historically enabled on old SIM cards – SIM PINs are part of GSM specifications and not new to smartphones. The second most popular security control was device password/pattern lock (with or without data wipe), which when combined was adopted by 59.07% of participants.

Answer		Response	%
SIM PIN		406	72.24%
Device Password/Pattern Lock (with data wipe)		140	24.91%
Device Password/Pattern Lock (without data wipe)		192	34.16%
File Encryption		71	12.63%
Remote Wipe		157	27.94%
Device Location Service		209	37.19%

Fig. 4. Respondents' Use of Smartphone Protection Mechanisms

Device location service was adopted by 37.19% of participants. The responses to all protection mechanisms are shown in Figure 4.

Concerning all controls men were significantly more inclined to adopt security controls than woman, which may be related to the fact that woman are more trusting of application repositories.

Of the respondents 35.38% have had their phone stolen. In addition, 30.05% have their phone insured against loss, theft, or damage. Thus a general awareness of risk should be present amongst users.

E. The Influence of Language and Culture

No significant security relationships were found when considering home language and culture. This is surprising, as smartphones almost exclusively use English as the language of choice, which may lead to uncertainty and misconceptions regarding security. The result could be attributed to the sample or the fact that the business language in South Africa is predominantly English – the relatively high purchase price of smartphone devices may limit the population to individuals of higher economic means, purely on affordability, which could imply that the same population has a good command of the English language.

F. Comparison with International Data

Similar to [1] the South African sample did not display good information security behaviour and could also be deemed complacent as they place undue trust in official application repositories, do not assess privacy and security implications when installing new applications, and do not adequately protect themselves through adopting pre-installed security mechanisms. Table IV provides a further comparison of these two studies.

It can be seen that this research sample appears similar in age, with a better gender balance. The security knowledge and IT expertise of the current sample is less than [1]. Additionally, there is less concern about privacy despite a similar amount of personal data on the smartphone. In addition there is a lesser awareness of malicious smartphone software.

A summary of the most significant findings – in order of the research questions – conclude this section.

G. Summary of Findings

Users place significant amounts of trust on application repositories which can leave them vulnerable. Most users (80.45%) trust official application repositories as they believe they are secure. This trust may be founded on a perception that the applications available on official application repositories have been tested. Respondents who perceive their IT expertise to be better or those who have completed information security courses have more deterministic views on application testing which affects levels of trust.

Users pay very little attention to privacy and security when installing applications on their device. The majority of respondents (76.3%) claimed to be aware of malicious smartphone software (especially men with higher perceived levels of IT expertise or information security training) but very few considered privacy and security when choosing to install smartphone applications on their devices. Only 39% of respondents habitually reviewed security messages before installing new application with an even smaller number (18.7%) having reviewed licensing messages; however respondents that reviewed either message type were likely to review the other type as well. A small minority (predominantly younger respondents) preferred pirated applications which were potentially compromising their security.

Although there were differences between adoption levels of smartphone security controls, specifically related to gender, there was not a satisfactory level of smartphone security control adoption prevalent in the sample.

From the research data it was not evident that home language or culture influences user security awareness in a significant way.

TABLE IV
CURRENT RESEARCH VS. [1]

Item	Current Research	[1]
Sample	619	458
Age	18–30 (77.8%)	15–30 (81%)
Gender (Male)	53.8%	70.1%
Information security training	7.4%	43.7%
IT expertise	Good	Excellent
Concerned about privacy	83.8%	95.2%
Personal data on mobile phone	75.9%	75.8%
Business data on mobile phone	30.2%	35.8%
Aware of malicious software	76.3%	81.4%

V. Conclusion

This research shows that in a South African context users are complacent in their smartphone security behaviours, displaying high levels of trust towards smartphone app repositories. Users rarely consider privacy and security when installing new applications and also do not adequately protect themselves by adopting smartphone protection mechanisms (controls). This research contributes to the existing body of knowledge on smartphone security behaviour, adding knowledge from a developing country (South African) context.

The research did not find any conclusive associations to suggest that a users home language impacts their information security behaviour or trust. However, an association between IT expertise and the adoption of smartphone security controls was found.

Gender has shown unexpected relationships with security behaviour, which should be explored further. In addition the African continent, with its diverse set of languages and ethnicities, provides an opportunity to study the influence of culture on user behaviour and the adoption of smartphone security controls. Future research should add rich qualitative data to answer deeper 'why' questions related to these issues.

References

[1] A. Mylonas, A. Kastania, and D. Gritzalis, "Delegate the smartphone user? security awareness in smartphone platforms," *Computers & Security*, vol. 34, pp. 47–66, May 2013.

[2] E. Chin, A. P. Felt, V. Sekar, and D. Wagner, "Measuring user confidence in smartphone security and privacy," in *Proceedings of the Eighth Symposium on Usable Privacy and Security*, ser. SOUPS '12. New York, NY, USA: ACM, 2012, p. 1:11:16.

[3] B. H. Jones and L. Heinrichs, "Do business students practice smartphone security," *Journal of Computer Information Systems*, vol. 53, no. 2, pp. 22–30, 2012.

[4] S. Mansfield-Devine, "Paranoid android: just how insecure is the most popular mobile platform?" *Network Security*, vol. 2012, no. 9, pp. 5–10, Sep. 2012.

[5] J. M. Urban, C. J. Hoofnagle, and S. Li, "Mobile phones and privacy," Social Science Research Network, Rochester, NY, SSRN Scholarly Paper ID 2103405, Jul. 2012.

[6] S. Furnell and N. Clarke, "Power to the people? the evolving recognition of human aspects of security," *Computers & Security*, vol. 31, no. 8, pp. 983–988, Nov. 2012.

[7] E. Albrechtsen and J. Hovden, "The information security digital divide between information security managers and users," *Computers & Security*, vol. 28, no. 6, pp. 476–490, Sep. 2009.

[8] C. Colwill, "Human factors in information security: The insider threat who can you trust these days?" *Information Security Technical Report*, vol. 14, no. 4, pp. 186–196, Nov. 2009.

[9] D.-L. Huang, P.-L. Patrick Rau, G. Salvendy, F. Gao, and J. Zhou, "Factors affecting perception of information security and their impacts on IT adoption and security practices," *International Journal of Human-Computer Studies*, vol. 69, no. 12, pp. 870–883, Dec. 2011.

[10] R. S. Shaw, C. C. Chen, A. L. Harris, and H.-J. Huang, "The impact of information richness on information security awareness training effectiveness," *Comput. Educ.*, vol. 52, no. 1, p. 92100, Jan. 2009.

[11] R. Kissel, "Glossary of key information security terms," National Institute of Standards and Technology, Tech. Rep. NISTIR 7298 Revision 2, 2013.

[12] J. Luftman and H. S. Zadeh, "Key information technology and management issues 201011: an international study," *Journal of Information Technology*, vol. 26, no. 3, pp. 193–204, Sep. 2011.

[13] U. Sumita and J. Yoshii, "Enhancement of e-commerce via mobile accesses to the internet," *Electronic Commerce Research and Applications*, vol. 9, no. 3, pp. 217–227, May 2010.

[14] H. Zafar and J. Clark, "Current state of information security research in IS," *Communications of the Association for Information Systems*, vol. 24, no. 1, Jun. 2009.

[15] M. Fishbein and I. Ajzen, *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research*. Reading, Mass: Addison-Wesley Pub, Jun. 1975.

[16] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness," *MIS Q.*, vol. 34, no. 3, p. 523548, Sep. 2010.

[17] B. Lebek, J. Uffen, M. H. Breitner, M. Neumann, and B. Hohler, "Employees' information security awareness and behavior: A literature review," in *2013 46th Hawaii International Conference on System Sciences (HICSS)*, Jan. 2013, pp. 2978–2987.

[18] F. D. Davis, R. P. Bagozzi, and P. R. Warshaw, "User acceptance of computer technology: A comparison of two theoretical models," *Management Science*, vol. 35, no. 8, pp. 982–1003, Aug. 1989.

[19] A. Al-Omari, O. El-Gayar, and A. Deokar, "Security policy compliance: User acceptance perspective," in *2012 45th Hawaii International Conference on System Science (HICSS)*, Jan. 2012, pp. 3317–3326.

[20] T. Dorflinger, A. Voth, J. Kramer, and R. Fromm, "'My smartphone is a safe!' The user's point of view regarding novel authentication methods and gradual security levels on smartphones," in *Proceedings of the 2010 International Conference on Security and Cryptography (SECRYPT)*, Jul. 2010, pp. 1–10.

[21] M. Landman, "Managing smart phone security risks," in *2010 Information Security Curriculum Development Conference*, ser. InfoSecCD '10. New York, NY, USA: ACM, 2010, p. 145155.

[22] R. Panko, *Corporate Computer and Network Security*, 2nd ed. Boston: Prentice Hall, Jul. 2009.

[23] M. Theoharidou, A. Mylonas, and D. Gritzalis, "A risk assessment method for smartphones," in *Information Security and Privacy Research*, ser. IFIP Advances in Information and Communication Technology, D. Gritzalis, S. Furnell, and M. Theoharidou, Eds. Springer Berlin Heidelberg, Jan. 2012, no. 376, pp. 443–456.

[24] D. Barrera and P. Van Oorschot, "Secure software installation on smartphones," *IEEE Security Privacy*, vol. 9, no. 3, pp. 42–48, May 2011.

[25] P. G. Kelley, L. F. Cranor, and N. Sadeh, "Privacy as part of the app decision-making process," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ser. CHI '13. New York, NY, USA: ACM, 2013, pp. 3393–3402.

[26] R. A. Botha, S. M. Furnell, and N. L. Clarke, "From desktop to mobile: Examining the security experience," *Computers & Security*, vol. 28, no. 34, pp. 130–137, May 2009.

[27] S. Furnell, "Securing mobile devices: technology and attitude," *Network Security*, vol. 2006, no. 8, pp. 9–13, Aug. 2006.

[28] Y. Rezgui and A. Marks, "Information security awareness in higher education: An exploratory study," *Computers & Security*, vol. 27, no. 78, pp. 241–253, Dec. 2008.

[29] T. Mochiko, "BlackBerry and nokia dominate local smartphone market." [Online]. Available: http://www.bdlive.co.za/business/technology/2012/08/14/blackberry-and-nokia-dominate-local-smartphone-market