Security behaviors of smartphone users

Amit Das and Habib Ullah Khan
College of Business and Economics, Qatar University, Doha, Qatar

Received 21 April 2015
Revised 21 July 2015
Accepted 18 August 2015

Abstract

Purpose – This paper aims to report on the information security behaviors of smartphone users in an affluent economy of the Middle East.

Design/methodology/approach – A model based on prior research, synthesized from a thorough literature review, is tested using survey data from 500 smartphone users representing three major mobile operating systems.

Findings – The overall level of security behaviors is low. Regression coefficients indicate that the efficacy of security measures and the cost of adopting them are the main factors influencing smartphone security behaviors. At present, smartphone users are more worried about malware and data leakage than targeted information theft.

Research limitations/implications – Threats and counter-measures co-evolve over time, and our findings, which describe the state of smartphone security at the current time, will need to be updated in the future.

Practical implications – Measures to improve security practices of smartphone users are needed urgently. The findings indicate that such measures should be broadly effective and relatively costless for users to implement.

Social implications – Personal smartphones are joining enterprise networks through the acceptance of Bring-Your-Own-Device computing. Users' laxity about smartphone security thus puts organizations at risk.

Originality/value – The paper highlights the key factors influencing smartphone security and compares the situation for the three leading operating systems in the smartphone market.

Keywords Security, Information security

Paper type Research paper

1. Introduction

The proliferation of smartphones has brought mobile computing to the masses. By the end of 2014, approximately 1.76 billion people were expected to own and use smartphones, up more than 25 per cent over 2013 (eMarketer, 2014). This means that there are more smartphones in use today than personal computers (PC) (Business Insider, 2013). A separate (online) survey, supported by Google, claimed that smartphone penetration would exceed 50 per cent in 19 countries over the same period (Our Mobile Planet, 2014).

Today's smartphones possess significant processing power, typically 2-4 processor cores each clocked at 1-2 GHz, matched with 1-2 GB of RAM and 8-32 GB of flash storage (GSMArena, 2014). Apart from their primary function of text/voice/video messaging, today's smartphones are capable of content creation, sharing and consumption, as well as location services [global positioning system (GPS), maps, navigation, and location-aware search] and financial transactions (electronic payments, online banking). In most ways, the smartphones of today are more

Information & Computer Security
Vol. 24 No. 1, 2016
pp. 116-134

2056-4961
DOI 10.1108/ICS-04-2015-0018

powerful than the desktop computers of the past decade. Atop this hardware run operating systems provided by a handful of firms (IDC, 2014), over which literally millions of third-party applications (apps) – free and paid – perform almost all conceivable computing functions (TechCrunch, 2014).

While the formidable processing power and vibrant ecology of app developers provides a solid platform for applications such as mobile commerce, a potential Achilles' heel lies in the security of smartphones (Consumer Reports, 2013). News reports present an alarming picture of how smartphone users do little, if anything, to secure the data on their devices (CNBC, 2014). Their propensity to install third-party apps without due scrutiny is a cause for concern (Mylonas *et al.*, 2013). Coupled with the prospect of physical loss of the device, and its casual use on unsecured public networks such as coffee shops and airports, smartphones present significant risks to information security (ENISA: European Union Agency for Network and Information Security, 2010). Smartphones being essentially "social" devices, contagion of malware on networks is likely to be rapid and far-reaching (Peng *et al.*, 2014). As was anticipated a decade ago, the growing processing power and widespread adoption of mobile devices has made them "the target of viruses, worms and other malware programs" (Furnell, 2005).

In this study, we examine the security behaviors of smartphone users in an affluent Middle-Eastern country with 75 per cent smartphone penetration (Go-Gulf, 2013). We relate these behaviors to users' appraisal of security threats and coping responses (Model 1) as well as the demands of the specific threats of malware, data leakage and data theft (Model 2). By measuring the current state of smartphone security in the region, we establish a baseline against which future progress in smartphone security behaviors might be measured. Our study of smartphone security behaviors responds to the call of Crossler *et al.* (2013) for more behavioral research into information security, to supplement technical innovations in computer and network security.

The attachment of employees to their personal smartphones has pushed most organizations to support "Bring-Your-Own-Device" (BYOD) computing. In this way, smartphones are making the transition from personal-use devices to organizational computing. French *et al.* (2014) note that BYOD boosts employee satisfaction and productivity but creates issues with respect to security and regulatory compliance. They call for timely research and ongoing knowledge sharing between industry and academia. Harris and Patten (2014) agree that BYOD support for smartphones brings anytime-anywhere capability to organizational computing but raises security concerns in the process. Finally, in their extensive review of the information security literature, Silic and Back (2014) concur that attention to the mobile revolution is necessary to close the gap between academic and business aspects of information security.

2. Literature review

As research on smartphone security evolves in different directions: technical (Fang *et al.*, 2014; Peng *et al.* 2014), behavioral (Allam *et al.*, 2014; He, 2013; Mylonas *et al.*, 2013) and policy-oriented (French *et al.*, 2014; Harris and Patten, 2014), we seek to apply the insights contained in the prior literature on IT security behaviors to the mobile context. From this prior literature, we identify constructs relevant to smartphone security (including security behaviors, our outcome of interest, as well as their likely antecedents) and their theoretical inter-relationships. We expect that many of the theoretical insights into information security behaviors and practices accumulated in

the era of PC-centric computing can be adapted to the smartphone context. We summarize below some of the significant prior research on security behaviors that informs our exploration of smartphone security.

Ng and Rahim (2005), applying the technology acceptance model to security behaviors, found that perceived usefulness, peer and media influence, and self-efficacy strengthened users' intentions to adopt backups, anti-virus software and personal firewalls. Later, Jones *et al.* (2010) found that subjective norms and management support increased the intention to adopt information system security measures, while perceived usefulness and perceived ease of use did not.

Much of the subsequent research on security behaviors has implicitly or explicitly adopted an *expectancy-based* framework where perceived vulnerability and perceived severity jointly drive the process of *threat appraisal*, which complements an appraisal of *coping responses* based on a cost-benefit analysis of security measures and how likely such measures are to succeed in neutralizing threats. This converges with a number of business frameworks used for information security risk management, which also view security behaviors as a tradeoff between risk – operationalized as annualized loss expectancy– and cost (Fenz *et al.*, 2014).

As an example of research that found significant impact of *threat appraisal*, Ng *et al.* (2009) used an expectancy-value framework, as applied to preventive healthcare behaviors – often referred to as the health belief model, or HBM (Rosenstock, 1966) – to model computer security behaviors. They found support for perceived susceptibility and perceived benefit (of the prevention behavior), but not perceived severity or barrier (to the adoption of the behavior), as determinants of their chosen aspect of computer security behavior – care in the handling of e-mail attachments. Independently, Workman *et al.* (2008) investigated security lapses in organizations and found that higher levels of perceived vulnerability and severity, and self- and response efficacy reduced the likelihood of omissions that compromise security.

An example of research focusing on the appraisal of *coping responses* is the work of Beautement *et al.* (2008) who analyzed data from 17 semi-structured interviews in two organizations to conclude that when an individual is faced with a compliance decision, the costs represented by additional effort on tasks are weighed up and measured against the benefits. Along the same lines, Bulgurcu *et al.* (2010) found that employees' attitude toward compliance with information security policies is influenced by their beliefs about benefit and cost of compliance, the cost of non-compliance, as well as their information security awareness. Herath and Rao (2009a) found security compliance intentions to be boosted by peer pressure and the likelihood of facing penalties for non-compliance. A companion paper (Herath and Rao, 2009b) suggests that compliance intentions are also affected by the perceived severity of threats and the availability of resources (guidance and training) to support compliance. Johnston and Warkentin (2010), in their study of user intentions to adopt anti-spyware measures, found that such intentions are affected directly by response efficacy, self-efficacy and social norms, but not by the susceptibility and severity of threats as portrayed in fear appeals. Ifinedo (2012) found that compliance intentions depend on perceived efficacy of security responses as well as users' self-efficacy in terms of carrying out the responses. Threat appraisal (under a susceptibility – severity framework) did not have much effect on compliance intentions.

Examples of research that found significant effects of *both* threat appraisal and assessment of coping behaviors include the work of Lee *et al.* (2008) who applied Rogers' (1975) protection motivation theory (similar to the health belief model) to users' intentions to adopt PC anti-virus software and concluded that perceived vulnerability, response efficacy, self-efficacy, expected positive outcomes and prior virus infection experiences all strengthened such intentions. Along similar lines, Chenoweth *et al.* (2009) showed that perceived vulnerability, perceived severity, response efficacy and response cost influence the behavioral intention to use anti-spyware software as a protective technology.

Lee and Larsen (2009) studied the adoption of anti-malware software by executives of small and medium businesses. They found positive effects of perceived severity, perceived vulnerability, response efficacy, self-efficacy, social influence, vendor support and IT budget on the intention to adopt anti-malware software, and a positive correlation between expressed intention and actual adoption *behavior*. Liang and Xue (2009, 2010) developed and tested a technology threat avoidance model to find that the motivation to avoid spyware was affected positively by the perceived threat (susceptibility and severity), response and self-efficacy and negatively by the cost of response. Avoidance motivation was positively related to avoidance behavior ($r = 0.43$).

Not all research into security behaviors has focused on threat appraisal and/or coping responses. Early work by Frank *et al.* (1991) found that PC users' security behaviors were positively correlated with informal social norms and users' knowledge and experience in computing. Rhee *et al.* (2009) argue for the central role of self-efficacy in the use of security technologies and other security behaviors. Stanton *et al.* (2005) classified computer security behaviors in terms of a two-way taxonomy of expertise and intentions, recommending that organizations train as well as monitor their employees to improve security. Vroom and von Solms (2004) also discuss the role of audit (monitoring) but suggest that it be supplemented with culture change to promote security in organizations. Greene and D'Arcy (2010) found security compliance intentions to be related positively to the organization's security climate and the user's job satisfaction. Pahnila *et al.* (2007) found that the information quality of security policies had a positive effect on compliance intention and behavior, apart from users' attitudes, beliefs and habits. In a later paper (Siponen *et al.*, 2010), the same authors discuss the conditions under which rewards and sanctions might enhance compliance behavior. Hedström *et al.* (2013) applied Weber's Social Action Theory to a case study of information security non-compliance at a Swedish hospital to conclude that non-compliance is mostly deliberate and instrumental, based on means–end calculation by users. An extensive meta-analysis by Sommestad *et al.* (2014), however, suggests that beliefs and values influence compliance intention more than incentives do.

Evidence for the effect of training on information security compliance continues to be mixed. Furnell and Thomson (2009) emphasize the role of context-sensitive training (promoting awareness and providing the necessary skills) as a step toward a security culture. Davinson and Sillence (2010) found that security behavior with respect to phishing threats improved somewhat with risk warnings, though the content of such warnings did not seem to matter. Security behavior also did not respond to a training program developed to educate users about phishing threats and counter-measures. In a laboratory experiment conducted by Komatsu *et al.* (2013), users' response behaviors bore a complex relation to their comprehension of the security threat and their trust in

the sender of persuasive messages. But Al-Omari *et al.* (2012) present evidence that information security awareness can play a major role in shaping users' intentions to comply with information security policies.

Table I below provides a chronological summary of the relationships between information security behaviors and their determinants observed in prior empirical research.

Two main trends seen in Table I above are:

(1) the predominance of *intention*, rather than *behavior*, as the dependent variable of interest; and

(2) the frequent appearance of perceived *vulnerability*, perceived *severity*, response *efficacy*, self-efficacy and response *cost* as predictors of security intentions.

As Sommestad *et al.* (2014) note in their systematic review of variables influencing information security policy compliance, most research focuses on attitudes and intentions; very few examine actual behavior. Unfortunately, attitudes do not always coincide with behavior. Workman *et al.* (2008) refer to a knowing–doing gap in the practice of information security, where intentions might not translate directly into behaviors. In a carefully designed laboratory experiment, Komatsu *et al.* (2013) showed that a user's attitude (based on stated preference) does not match that users' behavior (based on revealed preference). Lee and Larsen (2009) found a positive correlation between expressed intention and actual adoption behavior ($0.20 \leq r \leq 0.40$, for different sub-groups in their sample). Liang and Xue (2009, 2010) found that avoidance motivation toward spyware was positively related to avoidance behavior ($r = 0.43$). Pahnila *et al.* (2007) also found a significant link between intention and actual compliance behavior (standardized beta of 0.40, $p = 0.05$), but most of the variables that affected intention significantly had no effect on behavior.

Most of the work above was undertaken in organizations (Guo, 2013), which have explicit information security policies and some degree of enforcement of these policies – ranging from having one's computer kicked off the network to losing one's job altogether. In contrast, the mobile devices that are the subject of our study are owned by individuals and supervised very weakly, if at all, by organizations (Allam *et al.*, 2014). The security of these devices is, at this point in time, almost purely an individual responsibility, a situation that is changing, as BYOD computing matures with respect to organizational policies and user education.

3. Model development

3.1 Classification of threats to smartphone security

The numerous security threats to smartphones (FCC: Federal Communications Commission, 2012; Ofcom, 2013; ENISA: European Union Agency for Network and Information Security, 2010) can be grouped into at least three categories (He, 2013):

(1) *Malware*, such as worms and viruses, aimed at damaging the device or rendering it unavailable. Malware may delete critical files, drain the battery or disrupt the communication capability of the smartphone.

(2) *Data leakage*, i.e. the unauthorized collection and transmission of data such as location, contacts and usage behavior. Many third-party apps (and providers of operating systems, potentially) collect user data surreptitiously, without or

Table I.
Relationships in research on security behaviors

Study	Dependent variable	Significant independent variables
Frank *et al.* (1991)	PC users' security behaviors	Informal social norms and users' knowledge and experience in computing
Ng and Rahim (2005)	Intention to adopt backups, anti-virus software and personal firewalls	Perceived usefulness, peer and media influence, and self-efficacy
Pahnila *et al.* (2007)	Compliance intention and behavior	Information quality of security policies
Workman *et al.* (2008)	(Reduced) likelihood of omissions that compromise information security	Perceived vulnerability and severity, response efficacy, self-efficacy
Lee *et al.* (2008)	Intention to adopt PC anti-virus software	Perceived vulnerability, response efficacy, expected positive outcomes, self-efficacy, prior virus infection
Chenoweth *et al.* (2009)	Intention to use anti-spyware software	Perceived vulnerability, perceived severity, response efficacy, response cost
Furnell and Thomson (2009)	Security compliance	Context-sensitive training, organizational security culture
Herath and Rao (2009a)	Security compliance intentions	Peer pressure, likelihood of penalties for non-compliance
Herath and Rao (2009b)	Security compliance intentions	Perceived severity of threats, resources to support compliance
Lee and Larsen (2009)	Adoption of anti-malware software by executives of small and medium businesses	Perceived severity, perceived vulnerability, response efficacy, self-efficacy, social influence, vendor support, IT budget
Ng *et al.* (2009)	Care in the handling of e-mail attachments	Perceived susceptibility, perceived benefit of the prevention behavior
Rhee *et al.* (2009)	Use of security technologies	Self-efficacy
Bulgurcu *et al.* (2010)	Attitude toward compliance with information security policies	Beliefs about benefit and cost of compliance, cost of noncompliance, information security awareness
Davinson and Sillence (2010)	Behavior with respect to phishing threats	Risk warnings
Greene and D'Arcy (2010)	Security compliance intentions	Organization's security climate, user's job satisfaction
Johnston and Warkentin (2010)	Intention to adopt anti-spyware	Response efficacy, self-efficacy, social norms
Jones *et al.* (2010)	Intention to adopt IS security measures	Subjective norms, management support
Liang and Xue (2010)	Motivation to avoid spyware	Perceived susceptibility, perceived severity, response efficacy, self-efficacy, cost of response
Pahnila *et al.* (2007)	Intention to comply, actual compliance	Normative beliefs, threat appraisal, self-efficacy, visibility, deterrence
Al-Omari *et al.* (2012)	Intention to comply with IS security policies	Information security awareness
Ifinedo (2012)	Compliance intentions	Response efficacy, self-efficacy
Komatsu *et al.* (2013)	Behavior with respect to an induced botnet infection	Comprehension of security threat, trust in sender of advice

beyond the user's consent, sending back these data to the developers for data mining or marketing purposes, thus violating the privacy of the user.

(3) *Deliberate theft of confidential information*, such as passwords and credit card data. Targeted hacking attacks to intercept and decrypt communications, installation of Trojans and spyware, as well as phishing attacks by spoofing or impersonation, might be used to steal confidential information for espionage, blackmail or ransom.

Category 1 includes malicious software designed to damage/degrade the smartphone device itself. Category 2 refers to unauthorized harvesting of user data by writers of operating systems and apps. Category 3 refers to the targeted theft of information from storage (e.g. photos) or transit (e.g. passwords). The distinction between Categories 2 and 3 is that Category 2 affects all users of the OS/application, while Category 3 refers to targeted attacks on individuals (possibly soft and/or high-value targets).

3.2 Operationalization of constructs

Noting the success of expectancy-based models, such as the health belief model in Ng *et al.* (2009), or the protection motivation model in Pahnila *et al.* (2007), we cast our first model (Model 1) of security behaviors in terms of *threat appraisal* – perceived susceptibility and severity – and the assessment of *coping responses* – their efficacy and cost. Later, we re-group our questionnaire items in a different way (Model 2) to assess the relative contribution of the three threats – malware, data leakage and data theft – to security behaviors.

Following the expectancy-based approach, we model security behaviors (our dependent variable) as a function of perceived *susceptibility* to and *severity* of threats, the *interaction* of these two independent variables, the perceived *efficacy* of security measures and the *cost* (including peer reaction) of adopting these security measures. Each of the explanatory constructs is operationalized with three facets, one each for:

(1) *malware* (such as worms and viruses);

(2) *data leakage* (unauthorized collection and transmission of data such as location and communication habits); and

(3) the deliberate *theft* of confidential information (such as passwords and credit card data).

Thus, *susceptibility* is operationalized with three questions about the vulnerability to security issues: one for malware, another for data leakage and a third for data theft. The same is true of *severity*: it is composed of one item each for the perceived damage potential of malware, data leakage and data theft.

In addition to the direct effects of susceptibility and severity on security behaviors, we also admit into our model a multiplicative *interaction* term constituted by these two independent variables. The statistical adjustment needed to accommodate this interaction term is discussed in the data analysis section.

The three items for response *efficacy* refer to the perceived effectiveness of security measures against malware, data theft and data leakage. *Cost* also includes a fourth item in addition to the loss of convenience, functionality and time in protecting against malware, data leaks and theft. This element of cost refers to the *social* cost of not using

smartphone features or applications popular among one's friends: likely exclusion from conversations, discussions and activities conducted over social media.

As our study targets realized behaviors rather than attitudes, we chose a demonstrated measure of *user sophistication* instead of perceived self-efficacy. User sophistication is to our study of security behaviors what self-efficacy is to a study of intentions: a measure of the ability of the user to defend herself/himself against security threats. In this study, we use the *number of installed apps* on a user's smartphone as a proxy for the user's sophistication. We expect "power users" to have installed more apps than more novice users.

In using a social technology, smartphone users may be influenced by their overall level of *trust* in other users. Trust, in this sense, is central to information security (which aims to establish and maintain trust), and there have been calls to make the role of such trust explicit (Jensen, 2012) and unambiguous (Gollmann, 2006). We use a three-item measure of trust derived from the American General Social Survey (GSS), 2014 and the German Socio-Economic Panel questionnaires (SOEP: Socio-Economic Panel, 2014). More trusting smartphone users may be expected to display lower levels of security behaviors, as they are less likely to expect malicious actions from others.

We add two control variables that might have a potential bearing on computer security behaviors: g*ender* and *age* of the respondent. We do not hypothesize a priori any direction for the effects of these control variables. There exists a literature claiming women are more risk-averse than men (hence, more cautious) in economic decision-making (Charness and Gneezy, 2012; Croson and Gneezy, 2009), but we do not see a direct connection between such risk aversion and smartphone security behaviors. Similarly, as far as age is concerned, older people might be more circumspect in general, but also less familiar with mobile computing technology in particular; hence, it is hard to predict whether they will show more or fewer security behaviors.

Our measure of the dependent variable, *security behaviors*, is adapted from Microsoft's Computing Safety Index (Microsoft, 2014). The index is computed from an inventory of six security-enhancing actions: password protection, keeping systems software up-to-date, use of anti-virus software, encryption, not storing sensitive information and reviewing security features of apps before installing them. An individual's score on security behaviors is equal to the *number* of such actions practiced, the maximum being 6. The more security behaviors undertaken, the higher the score. Figure 1 below shows our research model in detail, down to the level of individual questionnaire items. Signs on the arrows show the *expected* direction of relationships.

To determine the relative contribution of the three threats – *malware*, *data leakage and data theft* – to smartphone users' security behaviors, we also estimate an alternative model (Model 2). The response to a security threat has been almost universally viewed as a cost–benefit decision: adopt a countermeasure if the cost of doing so is less than the expected loss from the threat it protects against. Therefore, we relate security behaviors directly to the user-perceived *cost-benefit* of responding to the three threats – malware, data leakage and data theft. As such, it only requires the same questionnaire items to be grouped differently – this time along threat lines. Henceforth, we refer to this alternative model as the "threat-based" model of smartphone security behaviors.

For each threat, we define the *cost-benefit* of responding to the threat as the sum of its susceptibility and severity, plus the efficacy of the security response, less the cost of protecting against it. This reflects our intuition that security behavior is more likely to

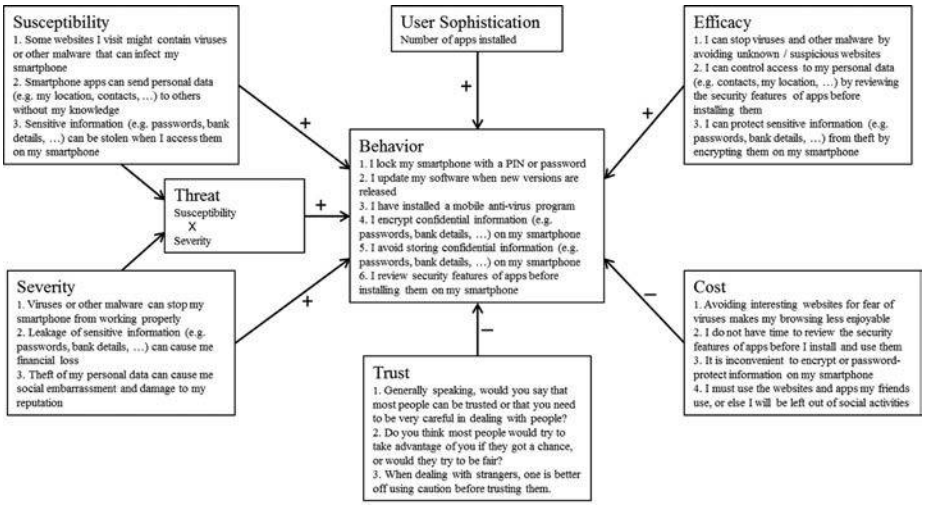

Figure 1.
Expectancy-based model and operationalization

be undertaken for threats of high susceptibility and severity, and when the efficacy of response is perceived to be high. The cost of undertaking security behavior (in functionality, convenience or time) reduces the attractiveness of a security behavior and makes it less likely to be undertaken. For each threat *i*, we define its *cost-benefit* as follows:

$$(\text{Cost-Benefit})_i = \text{Susceptibility}_i + \text{Severity}_i + \text{Efficacy}_i - \text{ResponseCost}_i \quad (1)$$

The cost-benefit of responding to the three distinct threats to smartphone security – malware, data leakage and data theft – are the independent variables in the alternative model. As *social cost* arising from refusal to use features and apps used by one's friends is not tied to a particular threat, it needs to be included in the model as a separate independent variable. As before, in addition to *user sophistication* (proxied by the number of apps installed) and *trust*, we continue to include *gender* and *age* as control variables in the model.

Figure 2 below shows the conceptual structure of the alternative threat-based model. We expect all three threats to have a positive impact on security behaviors. As before, more sophisticated users are expected to display more security behaviors, while trust and cost (in this case, the social cost of exclusion) are expected to have negative effects on security behaviors. As before, signs on the arrows show the expected direction of relationships.

3.3 Sample

Data were collected by face-to-face surveys in the Fall of 2013 from a convenience sample of smartphone users in shopping malls and other public places who were willing to spend a few minutes answering a short survey administered by two young adults paid out of our research funds. Contact details of respondents were collected whenever possible, so as to enable audit of the completed questionnaires. Some respondents, mostly women, declined to provide contact information. The Institutional Review Board

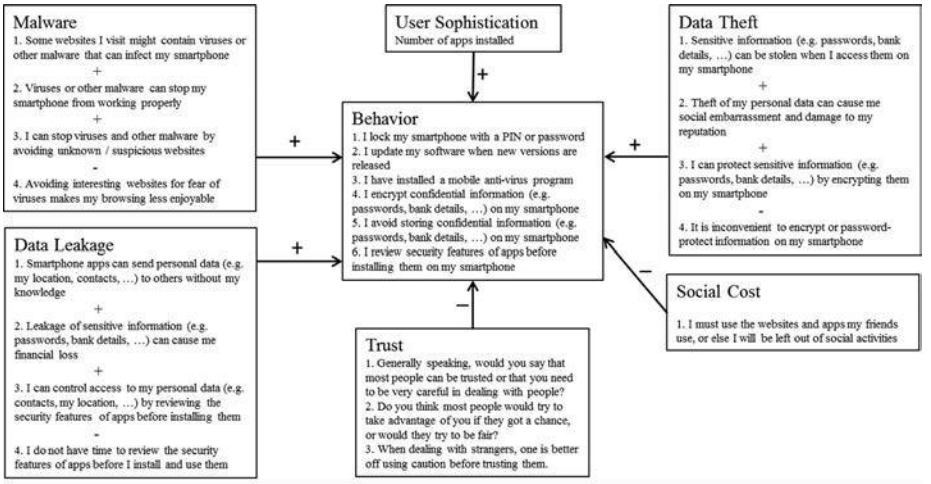

Figure 2.
Alternative threat-based model

of the university, overseeing ethical compliance, advised discretion in the collection of personally identifiable information.

In all, a total of 500 smartphone users were surveyed. Excluding incomplete responses, a total of 484 questionnaires were analyzed. The majority of these users (195) use the Android operating system, followed by Apple iOS (142 users) and BlackBerry (128 users). The remaining users came from Windows Phone or other unspecified operating systems. In terms of smartphone operating systems, the sample is reasonably representative of the user population: 40 per cent Android, 35 per cent iOS, 15 per cent BlackBerry and 10 per cent Windows Phone (Go-Gulf, 2013). The sample included 302 men and 182 women users. The most common age-group was 21-25 years (44 per cent), followed by 15-20 years (33 per cent). Respondents aged 26-30 years (11 per cent), 31-35 years (5 per cent) and > 35 years (8 per cent) made up the rest of our sample. A total of 63 per cent of the respondents hold undergraduate degrees, and 12 per cent have post-graduate qualifications; the rest either indicated high school education or did not answer the question.

4. Data analysis

Table II below shows the mean levels of the independent and dependent variables for the overall sample and the three sub-groups.

ANOVA analyses of the different constructs (independent and dependent) across the three smartphone platforms are included in Table II using the following (common) notation:

(1) A line over A and B indicates NO significant difference ($p > 0.05$) between **A**ndroid and **B**lackBerry users.

(2) A line over B and I indicates NO significant difference ($p > 0.05$) between **B**lackBerry and **i**OS users.

(3) A line over A, B and I indicates NO significant difference ($p > 0.05$) among all three pairs of platforms (AB, BI and AI).

Variable	All	Android	BlackBerry	iOS	Comparison of means (ANOVA)
n	465	195	128	142	
Susceptibility	3.16	3.30	3.10	3.02	$\overline{I\,B\,A}$
Severity	3.38	3.45	3.40	3.25	$\overline{I\;B\;A}$
Susceptibility × severity	33.05	35.21	32.67	30.43	$\overline{I\;B\;A}$
Response efficacy	3.61	3.64	3.63	3.56	$\overline{I\;B\;A}$
Cost	4.17	4.18	4.23	4.11	$\overline{I\;A\;B}$
Number of apps	1.87	1.91	1.53	1.97	$\overline{B\;\;A\;I}$
Trust	3.96	3.82	3.95	4.15	$\overline{A\;B\;I}$
Security behavior	2.75	2.92	2.72	2.55	$\overline{I\,B\,A}$

Table II.
Mean levels of independent and dependent variables

Notes: *highlights regression coefficients significant at the 5% level; data in bold refer to results at the model (as opposed to variable) level, suggest leaving them that way

The first row of Table II shows that Android users perceive themselves as significantly more susceptible to smartphone security threats than iOS users who see less need to protect their devices (and have fewer solutions to choose from); BlackBerry users fall in the middle, and their differences from both Android and iOS users are statistically insignificant. Perhaps in response to the heightened awareness of threats, Android users also carry out significantly more security behaviors than iOS users, as shown by the last row of Table II.

Multiple regression coefficients of the two models described above (expectancy-based and threat-based), evaluated separately for users of Android, BlackBerry and iOS platforms, as well as jointly (including the small number of users of Windows Phone and other less common operating systems) are presented below in Table III. As advised in the Friedrich procedure (Friedrich, 1982; Aiken and West, 1991) for dealing with multiplicative interaction terms (susceptibility × severity, in our case), we report the *unstandardized* coefficients from a model estimated using standardized values of independent and dependent variables.

5. Findings

Table III, with significant regression coefficients highlighted, shows that:

- The expectancy-based health belief model explains slightly more variance (10-25 per cent) than the threat-based model (7-20 per cent) across all operating systems.
- *Susceptibility* and *severity* of security threats influence security behaviors *only* for BlackBerry users. It is possible that BlackBerry users *assess* security threats more seriously than their iOS and Android counterparts. The negative interaction term for this sample indicates that the joint effect of susceptibility and severity is less than the sum of their individual effects. For iOS users, the effect of severity on security behaviors is negative, defying theoretical explanation.
- The most consistent predictors of security behavior, across all smartphone operating systems, are the perceived *efficacy* of security responses and the *cost* of adopting them (including the social cost of alienation from peers). Efficacy has a positive effect on security behaviors and cost a negative effect.

	All OS (n = 484)		Android (n = 195)		BlackBerry (n = 128)		iOS (n = 142)	
	B	*p-value*	*B*	*p-value*	*B*	*p-value*	*B*	*p-value*
Model 1 (Expectancy-based)	**R^2 = 0.096**		**R^2 = 0.097**		**R^2 = 0.243**		**R^2 = 0.128**	
Susceptibility	0.088	0.502	−0.068	0.766	1.025	0.000*	−0.251	0.202
Severity	0.009	0.944	0.023	0.906	0.786	0.002*	−0.469	0.026*
Susceptibility × severity	−0.005	0.980	0.060	0.858	−1.277	0.002*	0.571	0.088
Response efficacy	0.129	0.005*	0.165	0.032*	0.168	0.051	0.161	0.030*
Cost	−0.225	0.000*	−0.173	0.015*	−0.271	0.001*	−0.213	0.019*
Number of apps	0.205	0.006*	0.170	0.169	0.273	0.059	0.098	0.457
Trust	−0.040	0.377	−0.008	0.910	0.005	0.955	0.051	0.480
Gender (female = 1)	0.048	0.285	0.003	0.958	0.117	0.222	0.086	0.225
Age	−0.094	0.034*	−0.030	0.654	−0.039	0.761	−0.137	0.048*
Model 2 (Threat-based)	**R^2 = 0.093**		**R^2 = 0.070**		**R^2 = 0.192**		**R^2 = 0.077**	
Malware	0.159	0.001*	0.142	0.051	0.234	0.016*	0.031	0.681
Data leakage	0.183	0.000*	0.119	0.091	0.346	0.001*	0.186	0.012*
Data theft	−0.059	0.216	−0.007	0.931	0.023	0.814	−0.103	0.167
Social cost	−0.091	0.041*	−0.093	0.146	−0.135	0.143	−0.006	0.948
Number of apps	0.229	0.002*	0.216	0.083	0.205	0.184	0.133	0.335
Trust	−0.036	0.424	0.012	0.863	0.020	0.831	−0.012	0.864
Gender (female = 1)	0.030	0.505	0.003	0.966	0.087	0.393	0.076	0.288
Age	−0.082	0.066	−0.009	0.888	0.002	0.988	−0.080	0.251
	All OS (n = 484)		Android (n = 195)		BlackBerry (n = 128)		iOS (n = 142)	

Table III.
Regression coefficients of expectancy- and threat-based models

- Over all respondents, user *sophistication* as measured by the number of apps loaded is significantly positively related to security behaviors. The relationship is positive but not significant in each of the three sub-groups.
- *Older* users are slightly *less* likely to adopt security measures (true overall, and for iOS users in particular). Increasing age had a negative effect on the adoption of security measures, and this effect was strongest among iOS users.
- According to the threat-based model, *malware* and *data leakage* are the two threats that are most likely to induce security behaviors among smartphone users. *Social cost* hinders the adoption of security measures, but the tendency of older users to adopt fewer security behaviors is not significant in this model.

The statistical significance of the predictor (independent) constructs in the two models is summarized in Table IV below:

As Table IV shows, our study aligns with the view that users' assessment of *coping responses* – their efficacy and cost – has more impact on the adoption of security behaviors than their *appraisal* of susceptibility and severity. More sophisticated users (in terms of number of apps installed) undertake more security behaviors. The threat-based alternative model shows that the threats of malware and data leakage are more salient to users than deliberate data theft.

6. Discussion

The overall level of security behaviors among smartphone users in our sample is rather low, with an average score of 2.75 of a maximum of 6. Though statistically significant, the difference in security behaviors between Android and iOS users (BlackBerry users fall in between) is not large (2.92 vs 2.55). With 60 per cent of our respondents being

Table IV. Statistical significance of predictors in regression models

Model/construct	Significance
Model 1 (Expectancy-based)	
Susceptibility	BlackBerry users only
Severity	BlackBerry users only
Susceptibility × severity	None
Response efficacy	Overall, and for all groups
Cost	Overall, and for all groups
Number of apps	Overall
Trust	None
Gender	None
Age	Overall, and for iPhone users
Model 2 (Threat-based)	
Malware	Overall, and for BlackBerry users
Data leakage	Overall, and for BlackBerry and iPhone users
Data theft	None
Social cost	Overall
Number of apps	Overall
Trust	None
Gender	None
Age	None

young adults aged between 21 and 35 years, laxity about security in the personal use of smartphones could easily emerge as an enterprise issue in a BYOD environment. As He (2013) notes, BYOD defeats parameter-based defenses (as network connections span multiple service providers), and user indifference to basic security practices such as updating systems software, or exercising caution in installing third-party apps, can threaten the security of enterprise networks. Sophisticated mobile device management software is too expensive for all but the largest organizations (Harris and Patten, 2014).

Having noted the overall low level of security behaviors among smartphone users, we turn to the factors that influence security behavior. In line with meta-analyses of the health belief model (Carpenter, 2010), the perceived efficacy of security behaviors and the cost of adopting them ("benefits and barriers" in HBM parlance) appear to have the greatest influence on the adoption of security behaviors. Threat appraisal via susceptibility, severity and their interaction does not impact security behavior significantly in our data. The weak link between perceived severity and security behaviors has been noted by earlier research (Ng *et al.*, 2009), but the lack of effect of perceived susceptibility suggests that smartphone users may not be fully aware of the risks of mobile computing. Our results follow those of Tan and Aguilar (2012) who found student users to be largely oblivious to the security issues of Bluetooth wireless networking technology. User education remains one of the main ways to remedy the lack of security awareness. The work of Frank *et al.* (1991), Pahnila *et al.* (2007), Herath and Rao (2009b), Bulgurcu *et al.* (2010), Davinson and Sillence (2010), Greene and D'Arcy (2010) and Jones *et al.* (2010) all point to the potential of user education to promote security behaviors among users.

Just as susceptibility and severity do not drive behavior, the susceptibility–severity interaction does not have a significant effect on security behaviors either.

Smartphone users appear to be choosing opportunistically from the set of available security measures by focusing on their efficacy and the cost of deploying them. Besides user education, one way to ensure adoption of security practices (e.g. secure connections, disk encryption and limited privileges for apps) is to enable them by default in the operating system.

Malware and the leakage of data appear to be the most salient threats facing smartphone users. The targeted theft of data stored on smartphones or transmitted in transactions is not yet an issue of widespread concern. However, given that the storage capacity of smartphones is increasing rapidly, enabling more and more personal data (e.g. photographs and videos) to be stored on them, the threat of data theft is increasing. In BYOD computing, smartphones may also be exploited as gateways to data in the cloud, including enterprise financials (Allam *et al.*, 2014).

While all smartphone operating systems are vulnerable, Android users appear to be most at risk of security breaches (Fang *et al.*, 2014). This is borne out by press reports (Forbes, 2014), as well as the "open" nature of the Android ecosystem, where third-party apps traditionally received relatively less scrutiny from Google, the sponsor of the platform. Google now takes a more active role in scanning Android apps, so as to protect users from malware and data leakage (the Android Official Blog, 2014). The latest report from Google (2015) on Android security reports a relatively low level (below 1 per cent) of installation of "potentially harmful applications", though the level may be higher for users who install apps from unauthorized sources.

Our survey-based approach complements technical analyses of smartphone security, e.g. the permissions-based model underlying the Android and BlackBerry operating systems. An Android app may request between 1 and 100 permissions from the OS (Barrera *et al.*, 2010); researchers such as Fang *et al.* (2014) have called for even finer granularity. While rogue applications can act in concert to subvert permissions-based security (Orthacker *et al.*, 2012), the more common problem is that these permissions are granted at install time and thereafter enforced whenever the apps are invoked. As Mylonas *et al.* (2013) and others point out, most users are blissfully oblivious of the security characteristics of apps they install, routinely ignoring warning messages. Such user behavior undermines permissions-based security, forcing us to take note of user attitudes and behaviors in a broad view of smartphone security.

Our study may be viewed as an early attempt to apply an existing theory of information security behavior (the health belief model) to the relatively new domain of smartphone security. Based on the statistical analysis of survey data, it describes the current state of security behaviors and their antecedent attitudes. With its focus on behaviors (rather than just attitudes), it can inform technical measures and/or organizational policies; however, it does not, by itself, specify such measures or policies. As security threats and counter-measures co-evolve over time, the perceptions and behaviors of smartphone users may also change; hence, our findings should be updated accordingly.

References

Aiken, L.S. and West, S.G. (1991), *Multiple Regression: Testing and Interpreting Interactions*, Sage, Newbury Park.

Allam, S., Flowerday, S.V. and Flowerday, E. (2014), "Smartphone information security awareness: a victim of operational pressures", *Computers & Security*, Vol. 42 (May), pp. 56-65.

Al-Omari, A., El-Gayar, O. and Deokar, A. (2012), "Security policy compliance: user acceptance perspective", *Proceedings of the 45th Hawaii International Conference on System Sciences*, *Maui, HI*, pp. 3317-3326.

Android Official Blog (2014), "Expanding Google's security services for Android", available at: http://officialandroid.blogspot.com/2014/04/expanding-googles-security-services-for.html (accessed 17 August 2015).

Barrera, D., Kayacik, H.G., Van Oorschot, P.C. and Somayaji, A. (2010), "A methodology for empirical analysis of permission-based security models and its application to Android", *17th ACM Conference on Computer and Communications Security*, *Chicago, IL*.

Beautement, A., Sasse, M.A. and Wonham, M. (2008), "The compliance budget: managing security behavior in organizations", *Proceedings of the NSPW'08 Workshop on New Security Paradigms*, *Lake Tahoe, CA*, pp. 47-58.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010), "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness", *MIS Quarterly*, Vol. 34 No. 3, pp. 523-548.

Business Insider (2013), "The number of smartphones in use is about to pass the number of PCs", available at: www.businessinsider.com/number-of-smartphones-tablets-pcs-2013-12 (accessed 17 August 2015).

Carpenter, C.J. (2010), "A meta-analysis of the effectiveness of health belief model variables in predicting behavior", *Health Communication*, Vol. 25 No. 8, pp. 661-669.

Charness, G. and Gneezy, U. (2012), "Strong evidence for gender differences in risk taking", *Journal of Economic Behavior and Organization*, Vol. 83 No. 1, pp. 50-58.

Chenoweth, T., Minch, R. and Gattiker, T. (2009), "Application of protection motivation theory to adoption of protective technologies", *Proceedings of the 42nd Hawaii International Conference on System Sciences*, *Big Island, Hawaii*, pp. 1-10.

CNBC (2014), "Most Americans don't secure their smartphones", available at: www.cnbc.com/id/101611330# (accessed 17 August 2015).

Consumer Reports (2013), "Keep your phone safe: how to protect yourself from wireless threats", available at http://consumerreports.org/privacy0613 (accessed 17 August 2015).

Croson, R. and Gneezy, U. (2009), "Gender differences in preferences", *Journal of Economic Literature*, Vol. 47 No. 2, pp. 448-474.

Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M. and Baskerville, R. (2013), "Future directions for behavioral information security research", *Computers & Security*, Vol. 32 (February), pp. 90-101.

Davinson, N. and Sillence, E. (2010), "It won't happen to me: promoting secure behavior among internet users", *Computers in Human Behavior*, Vol. 26 No. 6, pp. 1739-1747.

eMarketer (2014), "Worldwide smartphone usage to grow 25% in 2014", available at: www.emarketer.com/Article/Worldwide-Smartphone-Usage-Grow-25-2014/1010920 (accessed 17 August 2015).

ENISA: European Union Agency for Network and Information Security (2010), "Smartphone security: information security risks, opportunities and recommendations for users", available at: www.enisa.europa.eu/activities/identity-and-trust/risks-and-data-breaches/smartphones-information-security-risks-opportunities-and-recommendations-for-users/at_download/fullReport (accessed 17 August 2015).

Fang, Z., Han, W. and Li, Y. (2014), "Permission based Android security: issues and countermeasures", *Computers & Security*, Vol. 43 (June), pp. 205-218.

FCC: Federal Communications Commission (2012), "FCC Smartphone security checker", available at: www.fcc.gov/smartphone-security (accessed 17 August 2015).

Fenz, S., Heurix, J., Neubauer, T. and Pechstein, F. (2014), "Current challenges in information security risk management", *Information Management & Computer Security*, Vol. 22 No. 5, pp. 410-430. doi: 10.1108/IMCS-07-2013-0053.

Forbes (2014), "Report: 97% of mobile malware is on Android. this is the easy way you stay safe", available at: www.forbes.com/sites/gordonkelly/2014/03/24/report-97-of-mobile-malware-is-on-android-this-is-the-easy-way-you-stay-safe/ (accessed 17 August 2015).

Frank, J., Shamir, B. and Briggs, W. (1991), "Security-related behavior of PC users in organizations", *Information & Management*, Vol. 21 No. 3, pp. 127-135.

French, A.M., Guo, C. and Shim, J.P. (2014), "Current status, issues, and future of Bring Your Own Device (BYOD)", *Communications of the Association for Information Systems*, Vol. 35 Article 10, pp. 191-197.

Friedrich, R.J. (1982), "In defense of multiplicative terms in multiple regression equations", *American Journal of Political Science*, Vol. 26 No. 4, pp. 797-833.

Furnell, S. (2005), "Handheld hazards: the rise of malware on mobile devices", *Computer Fraud & Security*, Vol. 2005 No. 5, pp. 4-8.

Furnell, S. and Thomson, K.L. (2009), "From culture to disobedience: recognising the varying user acceptance of IT security", *Computer Fraud & Security*, Vol. 2009 No. 2, pp. 5-10.

Go-Gulf (2013), "Smartphone usage in the Middle East – Statistics and trends", available at: www.go-gulf.ae/blog/smartphone-middle-east/ (accessed 17 August 2015).

Gollmann, D. (2006), "Why trust is bad for security", *Electronic Notes in Theoretical Computer Science*, Vol. 157 No. 3, pp. 3-9. doi: 10.1016/j.entcs.2005.09.044.

Google (2015), "Android security 2014 year in review", available at: https://static.googleusercontent.com/media/source.android.com/en//security/bulletin/Google_Android_Security_2014_Report_Final.pdf (accessed 17 August 2015).

Greene, G. and D'Arcy, J. (2010), "Assessing the impact of security culture and the employee-organization relationship on IS security compliance", *Proceedings of the 5th Annual Symposium on Information Assurance (ASIA '10)*, *Albany, NY*, pp. 42-49.

GSMArena (2014), "GSMArena smartphone shopping guide: August 2014", available at: www.gsmarena.com/smartphone_buyers_guide_august_2014-review-1122.php (accessed 17 August 2015).

GSS: General Social Survey (2014), "Dataset: General Social Surveys, 1972-2006", available at: www3.norc.org/GSS+Website/Browse+GSS+Variables/Subject+Index/ (accessed 17 August 2015).

Guo, K.H. (2013), "Security-related behavior in using information systems in the workplace: a review and synthesis", *Computers & Security*, Vol. 32 (February), pp. 242-251.

Harris, M.A. and Patten, K.P. (2014), "Mobile device security considerations for small- and medium-sized enterprise business mobility", *Information Management & Computer Security*, Vol. 22 No. 1, pp. 97-114. doi: 10.1108/IMCS-03-2013-0019.

He, W. (2013), "A survey of security risks of mobile social media through blog mining and an extensive literature search", *Information Management & Computer Security*, Vol. 21 No. 5, pp. 381-400. doi: 10.1108/IMCS-12-2012-0068.

Hedström, K., Karlsson, F. and Kolkowska, E. (2013), "Social action theory for understanding information security non-compliance in hospitals", *Information Management & Computer Security*, Vol. 21 No. 4, pp. 266-287. doi: 10.1108/IMCS-08-2012-0043.

Herath, T. and Rao, H.R. (2009a), "Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness", *Decision Support Systems*, Vol. 47 No. 2, pp. 154-165.

Herath, T. and Rao, H.R. (2009b), "Protection motivation an deterrence: a framework for security policy compliance in organizations", *European Journal of Information Systems*, Vol. 18 No. 2, pp. 106-125.

IDC (2014), "Smartphone OS market share, Q2 2014", available at: www.idc.com/prodserv/smartphone-os-market-share.jsp (accessed 4 October 2014).

Ifinedo, P. (2012), "Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory", *Computers & Security*, Vol. 31 No. 1, pp. 83-95.

Jensen, C.D. (2012), "The role of trust in computer security", *Proceedings of the 2012 Tenth Annual International Conference on Privacy, Security and Trust (PST)*, *Paris*, p. 236. doi: 10.1109/PST 2012.6297950.

Johnston, A.C. and Warkentin, M. (2010), "Fear appeals and information security behaviors: an empirical study", *MIS Quarterly*, Vol. 34 No. 3, pp. 549-566.

Jones, C.M., McCarthy, R.V., Halawi, L. and Mujtaba, B. (2010), "Utilizing the technology acceptance model to assess the employee adoption of information systems security measures", *Issues in Information Systems*, Vol. 11 No. 1, pp. 9-16.

Komatsu, A., Takagi, D. and Takemura, T. (2013), "Human aspects of information security: an empirical study of intentional vs actual behavior", *Information Management & Computer Security*, Vol. 21 No. 1, pp. 5-15. doi: 10.1108/09685221311314383.

Lee, D., Larose, R. and Rifon, N. (2008), "Keeping our network safe: a model of online protection behaviour", *Behaviour & Information Technology*, Vol. 27 No. 5, pp. 445-454. doi: 10.1080/01449290600879344.

Lee, Y. and Larsen, K.R. (2009), "Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software", *European Journal of Information Systems*, Vol. 18 No. 2, pp. 177-187.

Liang, H. and Xue, Y. (2009), "Avoidance of information technology threats: a theoretical perspective", *MIS Quarterly*, Vol. 33 No. 1, pp. 71-90.

Liang, H. and Xue, Y. (2010), "Understanding security behaviors in personal computer usage: a threat avoidance perspective", *Journal of the Association for Information Systems*, Vol. 11 No. 7, pp. 394-413.

Microsoft (2014), "Microsoft's Computing Safety Index (MCSI)", available at: www.microsoft.com/security/resources/mcsi.aspx (accessed 4 October 2014).

Mylonas, A., Kastania, A. and Gritzalis, D. (2013), "Delegate the smartphone user? Security awareness in smartphone platforms", *Computers & Security*, Vol. 34 (May), pp. 47-66.

Ng, B.Y., Kankanhalli, A. and Xu, Y. (2009), "Studying users' computer security behavior: a health belief perspective", *Decision Support Systems*, Vol. 46 No. 4, pp. 815-825.

Ng, B.Y. and Rahim, M.A. (2005), "A socio-behavioral study of home computer users' intention to practice security", *Proceedings of the Ninth Pacific Asia Conference on Information Systems*, *Bangkok, Thailand*, 7-10 July 2005, pp. 234-247.

Ofcom (2013), "Safer smartphones – keeping your device secure", available at: http://consumers.ofcom.org.uk/files/2013/10/mobile-guideV8.pdf (accessed 17 August 2015).

Orthacker, C., Teufl, P., Kraxberger, S., Lackner, G., Gissing, M., Marsalek, A., Leibetseder, J. and Prevenhueber, O. (2012), "Android Security permissions – can we trust them?", *Security and Privacy in Mobile Information and Communication Systems*, *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, Vol. 94 (May), pp. 40-51.

Our Mobile Planet (2014), "Interactive survey data repository", available at: http://think.withgoogle.com/mobileplanet/en/ (accessed 17 August 2015).

Pahnila, S., Siponen, M. and Mahmood, A. (2007), "Employees' behavior towards IS security policy compliance", *Proceedings of the 40th Hawaii International Conference on System Sciences*, *Big Island, Hawaii*, pp. 1561-1570.

Peng, S., Wu, M., Wang, G. and Yu, S. (2014), "Propagation model of smartphone worms based on semi-Markov process and social relationship graph", *Computers & Security*, Vol. 44 (July), pp. 92-103.

Rhee, H.S., Kim, C. and Ryu, Y.U. (2009), "Self-efficacy in information security: its influence on end users' information security practice behavior", *Computers & Security*, Vol. 28 No. 8, pp. 816-826.

Rogers, R.W. (1975), "A protection motivation theory of fear appeals and attitude change", *Journal of Psychology*, Vol. 91 No. 1, pp. 93-114.

Rosenstock, I.M. (1966), "Why people use health services", *Milbank Memorial Fund Quarterly*, Vol. 83 No. 4, pp. 1-32.

Silic, M. and Back, A. (2014), "Information security: critical review and future directions for research", *Information Management & Computer Security*, Vol. 22 No. 3, pp. 279-308. doi: 10.1108/IMCS-05-2013-0041.

Siponen, M., Pahnila, S. and Mahmood, M.A. (2010), "Compliance with information security policies: an empirical investigation", *Computer*, Vol. 43 No. 2, pp. 64-71.

SOEP: Socio-Economic Panel (2014), "SOEP survey papers", available at: http://panel.gsoep.de/soep-docs/surveypapers/diw_ssp0180.pdf (accessed 17 August 2015).

Sommestad, T., Hallberg, J., Lundholm, K. and Bengtsson, J. (2014), "Variables influencing information security policy compliance", *Information Management & Computer Security*, Vol. 22 No. 1, pp. 42-75. doi: 10.1108/IMCS-08-2012-0045.

Stanton, J.M., Mastrangelo, P.R., Stam, K.R. and Jolton, J. (2005), "Analysis of end user security behaviors", *Computers & Security*, Vol. 24 No. 2, pp. 124-133.

Tan, M. and Aguilar, K.S. (2012), "An investigation of students' perception of Bluetooth security", *Information Management & Computer Security*, Vol. 20 No. 5, pp. 364-381. doi: 10.1108/09685221211286539.

TechCrunch (2014), "iTunes app store now has 1.2 million apps, has seen 75 billion downloads to date", available at: http://techcrunch.com/2014/06/02/itunes-app-store-now-has-1-2-million-apps-has-seen-75-billion-downloads-to-date/ (accessed 17 August 2015).

Vroom, C. and von Solms, R. (2004), "Towards information security behavioural compliance", *Computers & Security*, Vol. 23 No. 3, pp. 191-198.

Workman, M., Bommer, W.H. and Straub, D. (2008), "Security lapses and the omission of information security measures: a threat control model and empirical test", *Computers in Human Behavior*, Vol. 24 No. 6, pp. 2799-2816.

About the authors

Amit Das (PhD, Minnesota) is an Associate Professor of Management in the College of Business & Economics at Qatar University. His current research interests include e-Business, e-Government and information security. Amit Das is the corresponding author and can be contacted at: amit.das@qu.edu.qa

Habib Ullah Khan (PhD, Leeds Met University) is an Associate Professor of Management Information Systems in the College of Business & Economics at Qatar University. His current research interests include mobile commerce, mobile security and e-learning.