COMPUTERS & SECURITY 42 (2014) 56–65

Available online at www.sciencedirect.com

ScienceDirect

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

Computers & Security

Smartphone information security awareness: A victim of operational pressures☆

Sean Allam [a], Stephen V. Flowerday [a,*], Ethan Flowerday [b]

[a] Information Systems Department, University of Fort Hare, 50 Church Street, East London 5200, South Africa
[b] King's College, University of London, United Kingdom

ARTICLE INFO

Article history:
Received 16 August 2013
Received in revised form
16 January 2014
Accepted 20 January 2014

Keywords:
Smartphone
Information security
Awareness
Bring your own device (BYOD)
Mobile computing

ABSTRACT

Smartphone information security awareness describes the knowledge, attitude and behaviour that employees apply to the security of the organisational information that they access, process and store on their smartphone devices. The surge in the number of smartphone devices connecting to organisational systems and used to process organisational data has enabled a new level of operational efficiency. While employees are aware of the benefits they enjoy by bringing their personal devices into the workplace, managers too are aware of the benefits of having a constantly connected workforce. Unfortunately, those aware of the risks to information security do not share an equal level of enthusiasm. These devices are owned by employees who are not adequately skilled to configure the security settings for acceptable security of that information. Moreover, routine information security awareness programmes, even if applied, gradually fade into the daily rush of operations from the day they are completed.

This paper explores the factors which influence these oscillating levels of information security awareness. By applying an adapted version of an awareness model from the domain of accident prevention, the factors which cause diminishing awareness levels are exposed. Subsequently, information security awareness emerges as a symptom of such factors. Through geometrical modelling of the boundaries and pressures that govern our daily operations, an awareness model emerges. This model ensures that organisations are better equipped to monitor their information security awareness position, their boundaries and the daily pressures affecting the organisation, thus allowing them to design better integrated policies and procedures to encourage safe operating limits. The model is evaluated using a theory evaluation framework through an expert review process.

1. Introduction

A myriad of devices accompany employees, contractors, business partners and other stakeholders into organisations daily as part of the 'bring your own device' (BYOD) phenomenon. Smartphone devices are often the personal property of the users, but are increasingly being used to access and process organisational information in addition to personal information. However, users are often unaware of the risk these

* *Corresponding author*. Tel.: +27 43 7047071.
E-mail address: sflowerday@ufh.ac.za (E. Flowerday).

0167-4048/$ – see front matter © 2014 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.cose.2014.01.005

devices introduce or, even if they have some degree of awareness, how to mitigate these risks. This situation is exacerbated by the fact that smartphone owners are solely responsible for the ultimate administration of their own devices. Research by the Ponemon (2012) institute found that in the past three years mobile devices have become a major threat for 73% of their respondents, up from only 9% in 2010. A study by Cisco (2013) found that almost 40% of smartphone users do not have a password enabled on their device. A similar study by PricewaterhouseCoopers (2012) estimated that as many as one in three small businesses, and 75% of large businesses, allow smartphones and tablets to connect to their systems, many without taking any steps to mitigate potential risk.

Theoharidou et al. (2012) list many the different types of data that may be stored on smartphone devices, including personal, business, government, financial, authentication and connection or service data. This combination of data stored on personal devices raises the risks for organisations in terms of having their information, or that of their clients, compromised. Compromised data may result in identity theft, the loss of corporate trade secrets or in another undesirable outcome. This information is not protected by organisational security when it exists on personal devices. Information which for many years found protection behind firewalls, servers and other security controls is being exposed by end users who are not adequate in their actions to protect their personal devices.

In the academic literature, information security awareness has been promoted as a means of reducing security risk across a number of threat areas. Kruger and Kearney (2006), Eminagaoglu et al. (2009), Albrechsten and Hovden (2010), and Bulgurcu et al. (2010) all promote awareness as a means of reducing security risk. These authors explain that increasing awareness influences behaviour, which ultimately reduces risk by focussing on the user and not the device. Unfortunately, as security risk areas are continuously changing and evolving, existing awareness quickly becomes obsolete, and therefore ineffective, with behaviour having been found to slowly migrate back to higher risk patterns. This degenerative migration takes place without malicious intention. It has also been found that, as the operating environment changes and as risk changes, awareness levels are found to adjust accordingly.

The paper begins by introducing an existing awareness model from Rasmussen (1997), and builds on prior adaptations of this model for the purposes of improving smartphone information security awareness. Although some findings may be applicable to other mobile devices, the assessment is targeted at smartphone devices for the purpose of specifically refining the scope of the model assessment phase. Following the introduction of the adapted model, an assessment framework is introduced and the components of this framework are applied to the adapted model. The purpose of this framework is to ensure that the adapted model satisfies the criteria for a theory in the information systems domain. The paper follows by assessing the components of the adapted model and the way the model components apply to both the problem area (smartphone security awareness) and the model validation framework criteria. Finally, the paper concludes with a new theoretical model in the field of smartphone information security awareness.

This model provides organisations with a better understanding of the impact that operational pressures have on smartphone information security awareness, allowing for the improvement of policy relating to those elements. Mahesh and Hooter (2013) note the importance of not only providing organisational policy to govern the use of smartphone devices by employees, but also explaining the purpose and intention of the policy to the employees. The paper shows how seemingly positive efforts to improve operational efficiencies may actually be the cause of incidents, with lowered levels of user awareness in fact being one of the symptoms of a broader set of influencing factors. This is illustrated by the geometrical transformation of an established awareness model from the domain of accident prevention. In using this model, policy makers will be better equipped to understand the relationship between the forces at play that influence smartphone information security awareness.

2. Background: the awareness conundrum

Security awareness programmes are often instituted to raise the level of participants' awareness of risk factors in a specific risk area. Unfortunately, improved understanding of the risk associated with a specific area does not guarantee any specific outcomes. Kruger and Kearney (2006) explain the following factors which should result from addressing awareness levels in an organisation:

- Knowledge: what people know
- Attitude: what people think
- Behaviour: what people do

Awareness programmes are instituted to improve these factors in the hope that information security risk will be reduced. Rasmussen (1997) notes that while improved awareness levels may provide temporary relief from risk, over time employees find themselves returning to previous levels through either productivity or workload pressures. Rasmussen (1997) warns that efforts to produce a safety culture will be never-ending because they are only effective as long as a continuous set of pressure is compensating for the functional pressure of the work environment. This effect is most notable in once-off awareness 'programmes', as awareness levels diminish post event due to routine organisational pressures. This points to the existence of external influencing factors which contribute to the information security awareness level at an organisation.

Smartphone information security awareness determines the level of knowledge employees and managers of an organisation possess relating to the mobile security of the information contained on such devices. Further to this it defines the attitude which these groups respond to the knowledge that they possess, and what specific behaviour they take in response to their combined attitude and knowledge. The awareness level includes these factors as they relate not only to the device and its capabilities, but also the changing context within which the device is being used as a mobile user travels throughout the day. Current awareness efforts focus on once off training with very little monitoring of organisational behaviour in the long term.