Available online at www.sciencedirect.com

ScienceDirect

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

Computers & Security

Can perceptual differences account for enigmatic information security behaviour in an organisation?

W.D. Kearney, H.A. Kruger [*]

School of Computer, Statistical and Mathematical Sciences, North-West University, Potchefstroom, South Africa

ARTICLE INFO

Article history:
Received 13 February 2016
Received in revised form 28 April 2016
Accepted 27 May 2016
Available online 31 May 2016

Keywords:
Information security awareness
Phishing
Social engineering
Information security behaviour
Trust
Perceptual differences

ABSTRACT

Information security in organisations is often threatened by risky behaviour of users. Despite information security awareness and training programmes, the human aspect of information security remains a critical and challenging component of a safe and secure information environment, and users reveal personal and confidential information regularly when asked for it. In an effort to explain and understand this so-called privacy paradox, this paper investigates aspects of trust and perceptual differences, based on empirical research. Two preceding social engineering exercises form the basis of the research project and are also presented as background information. Following the empirical work, a safe and secure information model is proposed. It is then argued that perceptual alignment of different organisational groups is a critical and prerequisite requirement to reach information security congruence between groups of people. In the context of the proposed model, the perceptual differences also offer some explanation as to why users with high levels of security awareness as well as high levels of trust in own and organisational capabilities so often fall victim to social engineering scams. The empirical work was performed at a large utility company and results are presented together with appropriate discussions.

1. Introduction

Information security has become one of the most critical and important areas of interest in modern-day business. It is unlikely that information security specialists will not acknowledge the importance of the human factor in information security. This acknowledgement has led, and still leads, to a large number of different studies on how to understand and manage the various human aspects such as knowledge, attitude and behaviour in information security.

A number of researchers and practitioners argue that the solution to the general information security problem lies in the existence and quality of an information security policy. Sommestad et al. (2014), for example, have identified variables that may influence compliance with information security policies, whereas Ifinedo (2014) has studied information systems security policy compliance, taking the effects of socialisation, influence and cognition into account. It is interesting to note that a wide variety of studies exists in this context; in some cases, human characteristics that may seem to be rather unusual are linked to the compliance or non-compliance of information security policies. Kelecha and Belanger (2013) have illustrated this by investigating religiosity as a possible role player in the intention to comply with an information security policy. Other instances of studies in the area of information security policies can be found in Bulgurcu et al. (2010) and Whitman and Mattord (2003). Information security awareness

[*] Corresponding author.
E-mail addresses: Kearneys@iinet.net.au (W.D. Kearney), Hennie.Kruger@nwu.ac.za (H.A. Kruger).

http://dx.doi.org/10.1016/j.cose.2016.05.006

is an area that is often associated with information security policies and a large number of studies are regularly conducted in an effort to address the awareness and human factor in information security. These studies are normally focused on how to raise information security awareness levels (Alnatheer, 2015; Da Veiga, 2015; Safa et al., 2015), how to measure these levels (Chandrashekhar et al., 2015; Keser and Gulduren, 2015; Parsons et al., 2014), and the monitoring and management of security awareness levels (Rantos et al., 2012; Spandonidis, 2015).

There is also a significant number of security specialists who contend that the problem should be addressed by creating (and maintaining) a suitable security culture in an enterprise. A large body of knowledge on security culture exists and examples of the existing literature include the work of Da Veiga and Martins (2015), who focus on an information security culture assessment process to improve an information security culture, specifically in financial institutions. In a study by Alhogail (2015), the design and validation of an information security culture framework is described. This framework incorporates the domains of preparedness, responsibility, management and society and regulations, and should be useful to organisations who want to develop an effective information security culture. Critical success factors for an information security culture can be found in Alnatheer (2015), whereas Alhogail and Mirza (2014) provide an overview of the different information security culture definitions as well as a review of literature sources that deal with information security culture studies. Closely related to security culture studies is the trend to borrow from the social sciences and to use psychological, sociological and other models in the endeavour to gain more insight into the complexities of human behaviour in information security. Studies using this type of approach can be found in Enrici et al. (2010), Lafrance (2004) and Tsohou et al. (2015).

The abovementioned models and approaches are not solely capable of explaining human activities when it comes to information security – other issues and factors may also play an important role. One such an important aspect is trust, which may be considered as a “soft” security property (Jensen, 2015) that interacts with other perceptual, attitudinal and behavioural factors. The importance of trust as a key element in information security has resulted in many research studies (Martin et al., 2015; Miltgen and Smith, 2015). It is also not unusual to find examples of studies where trust is evaluated in a specific information area. Examples include studies of trust in Internet of Things (Sicari et al., 2015), trust in cloud computing (Shaik and Sasikumar, 2015) and trust in e-payment systems (Kim et al., 2010).

Despite all these and other studies, the concept of a “privacy paradox” still exists. The privacy paradox refers to individuals with an apparently high level of security awareness who place a high premium on their privacy, but are easily persuaded to reveal their personal or other confidential information. The reader is referred to the studies by Hull (2015), who discusses the problem from a more philosophical viewpoint, and Kokolakis (2015), who presents the results of a review of research literature on the privacy paradox. A further complicating factor is that organisations do not really collect or have data available on the impact of IT and information security. This means that perceptions play a key role when decisions pertaining to information security have to be made. Not only do these differences occur in perceptions amongst various industry types, but there may also be perceptual differences between staff and management in the same organisation. Tallon (2014), for example, points out that there is a lack of consensus amongst executives’ perceptions of IT impact and value. Albrechtsen and Hovden (2009) go even further by referring to a digital divide between information security managers and users when it comes to information security practices. The study by Martin et al. (2015) provides further proof of the importance of expectations in information security. The authors examined the expectations of IT professionals towards online privacy and concluded that expectations often go unsatisfied – a finding that, according to the authors, builds further understanding of expectations and associated behaviours.

It is interesting to note Kokolakis’s suggestion (2015) that future studies regarding the privacy paradox should report evidence that is based on actual behaviour. In line with this suggestion and with the brief introductory comments in mind, this study investigates aspects of trust and perceptual differences that are based on empirical research. The empirical research was done in Australia at a large utility company that is a capital-intensive and customer-focused entity with over 2 million customers. To put the size of the company into perspective, one can only mention that during the last financial year, it had over 750 million AU$ in capital works and over 850 million AU$ in direct operating expenditure. There are over 3500 IT users, and with regard to its external IT presence, the company recorded 1.4 million visitors to its website and answers over 800,000 telephone calls from customers annually. The work that was performed includes two practical social engineering exercises that formed part of the regular control testing at the organisation in question, a survey to determine the role of trust in these security breaches, as well as a follow-up survey to determine the perceptual differences (if any) between management and users. The first practical social engineering experiment was reported in Kearney and Kruger (2013), whereas the results of the second experiment and the trust survey were detailed in Kearney and Kruger (2014). These first three studies and the results that were obtained constitute the first part of a larger research project that has ultimately led to the exercise on perceptual differences. It is therefore important to refer to these studies as part of the larger study; they will thus be presented briefly as background information. The focus of this paper is to report on the methodology and results of the perception survey.

The remainder of the paper is organised as follows: The next section will provide the background information on the two social engineering experiments and the trust survey. These studies led to the investigation of possible perceptual differences that will be described in the third section. The paper is then concluded with some general remarks.

2. Background

A popular and frequently used technique to study human behaviour in information security is the use of practical experiments that are associated with social engineering and, more specifically, with phishing (Jansson and Von Solms, 2013; Kumaraguru et al., 2009; Pattinson et al., 2012). Owing to its