COMPUTERS & SECURITY 70 (2017) 663–674

Available online at www.sciencedirect.com

ScienceDirect

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

Computers & Security

Persona-centred information security awareness

Duncan Ki-Aries *, *Shamal Faily*

Bournemouth University, Department of Computing & Informatics, Fern Barrow, Poole, UK

ARTICLE INFO

Article history:
Received 24 January 2017
Received in revised form 27 July 2017
Accepted 1 August 2017
Available online 9 August 2017

Keywords:
Information security
Security awareness
Risk
Human factors
Personas

ABSTRACT

Maintaining Information Security and protecting data assets remains a principal concern for businesses. Many data breaches continue to result from accidental, intentional or malicious human factors, leading to financial or reputational loss. One approach towards improving behaviours and culture is with the application of on-going awareness activities. This paper presents an approach for identifying security related human factors by incorporating personas into information security awareness design and implementation. The personas, which are grounded in empirical data, offer a useful method for identifying audience needs and security risks, enabling a tailored approach to business-specific awareness activities. As a means for integrating personas, we present six on-going steps that can be embedded into business-as-usual activities with 90-day cycles of awareness themes, and evaluate our approach with a case study business. Our findings suggest a persona-centred information security awareness approach has the capacity to adapt to the time and resource required for its implementation within the business, and offer a positive contribution towards reducing or mitigating Information Security risks through security awareness.

1. Introduction

Information Security issues are now prevalent concerns for organisations, specifically where issues directly impact upon regulatory, risk-based or reputational concerns resulting from intrusions and losses of data. Industry reports such as the PwC 2015 Data Breach report (PricewaterhouseCoopers LLP, 2015) highlight a large number of internal data breaches are still directly attributed to human factor issues, either intentional, accidental or with malicious intent. Businesses can no longer rely solely on process and technology for risk reduction of security issues, and need a greater consideration towards people integration with process and technology.

Although mandated for some, security education, awareness and training can support general understanding of issues through mandatory or annual refresher content. Several approaches exist for addressing security awareness, however, their focus is generally towards achieving compliance aspects. For example, applying and maintaining data confidentially, integrity and availability risk reducing controls. In most cases, a blanket approach would be applied without tailoring to the actual human factors involved. Human interaction that is central to business, processes, and system interaction therefore needs to be understood if security awareness needs are to be effectively addressed.

Research suggests current security awareness approaches do not entirely meet this requirement of designing for the user.

* *Corresponding author.*
E-mail addresses: dkiaries@bournemouth.ac.uk (D. Ki-Aries), sfaily@bournemouth.ac.uk (S. Faily).
http://dx.doi.org/10.1016/j.cose.2017.08.001

As a means to bridge this gap, an opportunity is presented to explore Human Computer Interaction (HCI) techniques that could be incorporated into a security awareness approach. We illustrate the application of such techniques through the use of *personas*. Personas are archetypical descriptions of users that embody their goals (Cooper, 1999). By representing archetypes of business users, personas offer insights into users that may otherwise be overlooked. Personas as user models can also be useful for identifying threats, vulnerabilities and likely areas of risk in their given environment (Faily and Fléchais, 2010a). The output of the personas could, therefore, be used to tailor security awareness needs using relevant topics and content addressing current business and people risks. Personas may also be incorporated into the awareness content itself, or potentially used for other process and procedure modification or security and risk assessment purposes.

To explore the potential of adopting a user-centred approach to security awareness, this paper illustrates an approach where the creation and application of personas was used to address business specific human factors within awareness activities. Our approach uses personas as a means of identifying audience needs and goals for security awareness requirements. These aim to address relevant human factors to reduce risk and improve a security minded culture. To demonstrate how personas may be integrated into an on-going cycle of security awareness, the steps taken leading to the design and implementation are incorporated within six on-going awareness programme steps. These build on positive features of other awareness approaches where they apply, making it relevant to persona integration and business tailored security awareness output. This can be embedded into business-as-usual activities with 90-day cycles of awareness themes to ensure a more frequent up-to-date approach towards addressing relevant security risks through security awareness.

To provide an overview in support of our approach, we begin by first considering existing frameworks and communication approaches for security awareness in Section 2. We consider current challenges, benefits and drawbacks, and how the use of personas may be integrated. Based on the research findings, we address the research gap by presenting a process for a persona-centred methodology in Section 3, integrating personas to help identify and reduce risk through tailored security awareness. Findings from testing elements of the approach with a case-study business, referred to as Company X, are detailed throughout Section 4. In Section 5 we discuss observations from the application of one approach towards combining HCI techniques into security awareness design requirements, aiming to reduce or mitigate Information Security risks. We then conclude in Section 6 and detail directions for future work.

2. Related work

2.1. *Information security awareness challenges and opportunities*

Raising awareness and changing security behaviour can be challenging, given the audience must be engaged with the reality of threats, and understand the process for identifying and addressing issues or concerns. The audience must then be motivated into applying positive behaviours, change risk perceptions (Roper et al., 2006) and engrained behaviours, supported by relevant topics that are not overly information-heavy (ENISA, 2006).

Challenges identified by Bada et al. (2015) found annual awareness and compliance orientated programmes were often treated as tick-box exercises and do not always lead to desired behaviours. Some approaches rely on invocations of fear to change behaviours, or result in a lack of motivation and ability to meet unrealistic expectations, which may derive from poorly designed security systems and policies (Bada et al., 2015). In some cases, security awareness goals were clearly identified and communicated. However, on a cultural level, people did not feel a need to browse internal security guidance as users did not believe they had security concerns (Maqousi et al., 2013). Some felt a lack of reward or recognition for applying positive behaviours, or did not feel empowered to make information or technology security decisions (Dominguez et al., 2010).

Awareness programmes were more likely to be successful when receiving top-level buy-in, business-wide support engaging with awareness, commitment and co-operation towards a security culture, using a participative creative design process tailored to business needs. Awareness should be communicated by a variety of means relevant to the business, its people and culture, and is best reinforced using an on-going 90-day programme (Manke and Winkler, 2012).

Delivery of awareness content should be engaging, appropriate and on-going, with a range of relevant topics that are targeted, actionable, doable and provides feedback to help sustain people's willingness to change (Bada et al., 2015). Communications must reinforce each other with a consistent message delivered across a number of channels to a culture addressed in a synchronous manner that supports the goals of the awareness programme (Beyer et al., 2015; Roper et al., 2006). Also, consider effectiveness across genders, generations or roles, of focusing on communicating how to achieve something, rather than dictating what should not be done (Manke and Winkler, 2012).

Baseline measures should be taken to establish needs and metrics relevant to the target audience and programme output (ENISA, 2006). Measuring the level of awareness is, however, more complicated, given that questionnaires can indicate a level of knowledge, but may not imply levels of motivation to improve behaviours (Bada et al., 2015). Awareness evaluation may be built-in using evaluation cycles embedded into the programme's awareness activities, and be considered at levels of Management, Audience, and Effectiveness against measurable performance objectives of awareness topics (Roper et al., 2006). Breach notifications or queries may also increase, therefore clarity may be required as to whether more issues are occurring or the increases are due to raised awareness (Roper et al., 2006).

An awareness programme should use simple consistent rules of behaviour for employees, offering increased perception of control and better acceptance of suggested behaviours. Cultural differences in risk perceptions should be considered when