Available online at www.sciencedirect.com

ScienceDirect

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

Computers & Security

Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs

Aggeliki Tsohou [a,*], *Maria Karyda* [b], *Spyros Kokolakis* [b]

[a] *Dept. of Informatics, Ionian University, Corfu, Greece*
[b] *Dept. of Information and Communication Systems Engineering, University of the Aegean, Samos GR-83200, Greece*

ARTICLE INFO

Article history:
Received 18 December 2014
Received in revised form
23 March 2015
Accepted 17 April 2015
Available online 29 April 2015

Keywords:
Information security awareness
Security policy compliance
Cognitive bias
Cultural bias
Security behavior
Risk decision-making

ABSTRACT

Standards and best practices for information security awareness programs focus on the content and processes of the programs, without taking into consideration how individuals internalize security-related information and how individuals make security related decisions. Relevant literature, however has identified that individual perceptions, beliefs, and biases significantly influence security policy compliance behavior. Security awareness programs need, therefore, to be aligned with the factors affecting the internalization of the communicated security objectives. This paper explores the role of cognitive and cultural biases in shaping information security perceptions and behaviors. We draw upon related literature from contiguous disciplines (namely behavioral economics and health and safety research) to develop a conceptual framework and analyze the role of cognitive and cultural biases in information security behavior. We discuss the implications of biases for security awareness programs and provide a set of recommendations for planning and implementing awareness programs, and for designing the related material. This paper opens new avenues for information security awareness research with regard to security decision making and proposes practical recommendations for planning and delivering security awareness programs, so as to exploit and alleviate the effect of cognitive and cultural biases on shaping risk perceptions and security behavior.

1. Introduction

Information security research has its focus on the "human factor", as humans are considered to be information security's weakest link. Information security management employs security policies as a means to define what is expected from individuals in an organization, including end-users, IT personnel, contractors and decision makers, in relation to information security. It is often the case, however, that information system users fail to comply with security policies. To tackle this problem, but also to address regulatory compliance requirements (e.g., HIPAA, FISMA), information security awareness programs have become key components of security management.

* *Corresponding author*. Ionian University, Department of Informatics, 7 Tsirigoti Square, Corfu, 49100, Greece. Tel.: +30 22610 87738.
E-mail addresses: atsohou@ionio.gr (A. Tsohou), mka@aegean.gr (M. Karyda), sak@aegean.gr (S. Kokolakis).
http://dx.doi.org/10.1016/j.cose.2015.04.006
0167-4048/

Awareness programs include activities that aim to make users "aware" of security issues and policies. Widely used security awareness standards and guidelines (ENISA, 2010; NIST 800-16, 1998; NIST 800-50, 2003; NIST 800-53, 2013) provide directions on developing material that informs employees about the importance of information security and the content of security policies. Standards and guidelines mainly focus on the processes and contents of the awareness program, addressing the question "*What behaviour do we want to reinforce?*" (NIST 800-50, 2003). Awareness programs are compiled following the assumption that users fail to adopt secure practices either because they are not aware of the risks, or because they do not understand the implications of security violations, or because they do not understand how they are expected to act. Security standards and guidelines, however, do not take into consideration whether knowledge of the awareness material will actually result to improved security behavior.

Transforming security behavior goes beyond the acquisition of knowledge of security policies and awareness of the importance of security. Research on security policy compliance (e.g., Bulgurcu et al., 2010; D'Arcy et al., 2009; Herath and Rao, 2009b) indicates that, in order to influence users' security behavior, we need to affect the way in which users perceive risks and make security-related decisions. Awareness programs need to go beyond the simple communication of security-related information and align with the process of individual decision-making.

Awareness programs, in this perspective, fall short in examining how individuals formulate their perceptions and beliefs about security, and in taking into consideration the role of beliefs and biases for shaping users' security behavior. A number of studies have identified this gap, highlighting the need to alter the view for designing awareness strategies. Karjalainen and Siponen (2011) indicate that programs that rely on one-way transmission of predetermined contents are not suitable for security awareness. Rhee et al. (2012) show that optimism biases of MIS executives affect vulnerability perceptions and call for more systematic awareness efforts taking into account the role of relative biases. However, extant literature lacks a systematic examination of the implications of biases for information security awareness programs. Security awareness research and practice needs to understand '*how to bolster security behaviour*', besides identifying what security behavior to promote. To do that, we need to understand how individuals internalize security awareness information and illuminate the role of biases for shaping security-related decision making.

The role of biases has been extensively studied with regard to raising health and safety awareness. Relevant literature in health and safety, as well as in other disciplines such as behavioral economics, has identified that the thinking processes behind perceiving risks and making risk-related decisions are subject to specific cognitive and cultural biases, such as the *affect heuristic* (i.e., a mental shortcut in which current emotional state influences decisions) and *optimism bias* (Gilovich et al., 2002). For example, research suggests that the *affect heuristic* leads many young people to initiate cigarette smoking, ignoring the severe health risks of this activity (Slovic et al., 2004). Based on this finding, modern anti-smoking campaigns use advertisements that evoke strong negative emotions, such as fear or sadness (Biener et al., 2004). On the contrary, information security awareness is still dominated by a "normative paradigm" of communicating facts and figures (Stewart, 2009; Stewart and Lacey, 2012), assuming that increased knowledge will inescapably result to enhanced security behavior.

This paper argues that individuals receive and process information security awareness information through the filter of cognitive and cultural biases. Drawing on the fact that both information security awareness programs and safety awareness programs seek to manage risk by influencing individual behavior, we identify and analyze security-related biases from contiguous disciplines (such as behavioral economics and health and safety). We then discuss the implications of these biases on formulating risk perceptions and shaping information security behavior and finally propose a set of recommendations for designing security awareness programs so as to accommodate the traits of security decision-making. Research implications for this study involve a call for exploring the role of individual information internalization processes for information security awareness and information security behavior research. Practical implications involve recommendations for planning and executing security awareness programs to avoid neglecting the effect of cognitive and cultural biases.

The paper continues with an analysis of information security policy compliance literature that identifies the role of individual perceptions and beliefs, as well as the influence of information security awareness on security compliance. In Section 3 we draw on relevant research to compile a conceptual framework of cognitive and cultural biases, which is employed on the following section to analyze the role of biases for information security behavior. We then propose a set of recommendations for the implementation of information security awareness programs with respect to the internalization processes of information security information by individuals (Section 5). Finally, we present the conclusions and implications of the study.

2. Background: factors affecting information security compliance

Information security policy (ISP) compliance studies draw on various theoretical backgrounds (e.g. *theory of reasoned action*, *theory of planned behavior*, *protection motivation theory* and *neutralization theory*) to identify factors that affect users' intention to comply with information security policies. Sommestad et al. (2014) reviewed 29 quantitative studies and found more than 60 variables that are determinants of ISP compliance and incompliance. Common variables identified to determine compliance behavior include *subjective norms, self-efficacy, response efficacy, response cost, perceived severity of sanctions* and *perceived certainty of sanctions*. Other antecedents of ISP compliance are *habits* (Vance et al., 2012), *perceived probability and perceived severity of security breach* (Herath and Rao, 2009b; Vance et al., 2012).

Bulgurcu et al. (2010) propose a comprehensive model of ISP compliance that focuses on the role of information