Information & Management 51 (2014) 551–567

Contents lists available at ScienceDirect

Information & Management

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

Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders

Clay Posey [a,*], Tom L. Roberts [b], Paul Benjamin Lowry [c], Ross T. Hightower [d]

[a] Department of Information Systems, Statistics, and Management Science, Culverhouse College of Commerce, The University of Alabama, Tuscaloosa, AL 35487, USA
[b] School of Accounting and Information Systems, College of Business, Louisiana Tech University, Ruston, LA 71272, USA
[c] Department of Information Systems, College of Business, City University of Hong Kong, Hong Kong, People's Republic of China
[d] University Competence Center, Lubar School of Business, University of Wisconsin-Milwaukee, Milwaukee, WI 53201, USA

ARTICLE INFO

Article history:
Received 2 July 2012
Received in revised form 25 March 2014
Accepted 31 March 2014
Available online 13 April 2014

Keywords:
Behavioral information security
Risk assessment
Qualitative analysis
Organizational insiders
Security professionals
Protection motivation theory

ABSTRACT

Organizational insiders have considerable influence on the effectiveness of information security efforts. However, most research conducted in this area fails to examine what these individuals believe about organizational security efforts. To help bridge this gap, this study assesses the mindset of insiders regarding their relationship with information security efforts and compares it against the mindset of information security professionals. Interviews were conducted with 22 ordinary insiders and 11 information security professionals, an effort that provides insight into how insiders gauge the efficacy of recommended responses to information security threats. Several key differences between insiders' and professionals' security mindsets are also discussed.

1. Introduction

Information security is a major concern for most organizations [13,25,73] and is a key focus of information technology (IT) spending, despite the recent economic downturns [43]. The security market grew 12% in 2010 to US$16.5 billion—an increase of 6% compared with 2009 [12]—and is expected to exceed $125 billion globally by 2015 [23], due in part to security issues stemming from organizational insiders' behavior [32,85]. *Ordinary organizational insiders* (i.e., *insiders*) are part-time employees, full-time employees, temporary workers, and consultants who have access to an organization's information and/or information systems [62,69]. These insiders pose considerable intentional [85,62,15,80,88,89] and accidental [31] security risks to firms, both of which are extremely costly [32]. Despite this evidence, more than 70% of security professionals who responded to a global information security survey in 2012 expressed confidence that their approaches were effective [44].

Technical methods have traditionally received the most attention from information security professionals as the primary means of preventing breaches [1,16,18,72]. However, over-reliance on technical solutions and authoritarian mandates leads to security practices that users find ineffectual because these methods cannot solve the underlying behavioral causes of the problems [62,11,20,68,79]. Worse yet, recent evidence suggests that if authoritarian approaches go too far, they can backfire, causing insider-related problems to increase rather than decrease [60]. Accordingly, to understand the effects of user behavior on information security, researchers and practitioners must incorporate behavioral frameworks from disciplines outside of computer science and electrical engineering that examine human perceptions, beliefs, motivations, and behaviors [62,31,11].

Another potential issue in the extant security research is that much of the knowledge base concerning the behaviors of organizational insiders has been accumulated largely from the opinions and experiences of information security and technology professionals [80,42,64,86]. Although these information security professionals, who themselves represent an advanced breed of insiders, provide a valuable perspective, they could suffer from an

* Corresponding author. Tel.: +1 2053480728.
E-mail addresses: cposey@cba.ua.edu (C. Posey), troberts@latech.edu (T.L. Roberts), paul.lowry.phd@gmail.com (P.B. Lowry), hightowe@uwm.edu (R.T. Hightower).

http://dx.doi.org/10.1016/j.im.2014.03.009
0378-7206/

elite bias [51] due to their removal from the day-to-day tasks and vulnerabilities faced by ordinary organizational insiders [79,3]. Conversely, insiders make daily, routine decisions that have a direct impact on their organizations' security [62,3,2]. Regardless of the technological security measures in place, the success or failure of an organization's security efforts relies on these insiders' diligence and knowledge [63]. Effective security requires information security professionals to create policies and technologies that ensure security and are consistent with insiders' work practices [1]. At the same time, insiders must share the information security professionals' goals and understand the required security practices. With this in mind, there is a high likelihood that information security professionals do not understand ordinary insiders as well as they think they do. If true, this gap would indicate that existing security practices are disconnected from the reality of organizational insiders' day-to-day jobs.

More explicitly, research on risk and risk perceptions provides evidence that expert opinions and general opinions do not align well and that risk perceptions are inherently subjective [35,76]. This misalignment is derived from the fact that experts tend to view risk on the bases of probability calculus and formal risk assessment, whereas laypeople form risk perceptions based on intuition, which is closely tightly to emotion and affect [57,78]. These dichotomous approaches have been termed *analytic systems* (i.e., risk as analysis) and *experiential systems* (i.e., risk as feelings), respectively. The first approach is based on mathematics and logic, and the second is based on the 'goodness' or 'badness' of a decision (i.e., the affect heuristic) [78,77]. Both, however, are vital in assessing and combating risk:

> There is wisdom as well as error in public attitudes and perceptions. Lay people sometimes lack certain information about hazards. However, their basic conceptualization of risk is much richer than that of experts and reflects legitimate concerns that are typically omitted from expert risk assessments. As a result, risk communication and risk management efforts are destined to fail unless they are structured as a two-way process. Each side, expert and public, has something valid to contribute. Each side must respect the insights and intelligence of the other. ([76], p. 285)

Given that organizational security and risk have many commonalities [56,82,83] and that many opinions regarding security fail to account for the public (i.e., organizational insider) perspective, we take this opportunity to elicit and compare the perspectives of information security professionals and organizational insiders, using an analysis of semi-structured interviews with 33 individuals from various organizations and industries. Previous research typically has viewed organizational insiders as security threats who must be controlled through organizational mandates (e.g., [15,80,7,14,17,29,52]). In contrast, we examine insiders' beliefs and motivations that positively influence their organizations' security from both perspectives. We use protection-motivation theory (PMT) [66] to understand these groups' perceptions of how insiders become motivated protective agents against organizational information security threats.

To proceed, we first review PMT's theoretical foundation. Next, we discuss our approach to examining insiders and security experts' perceptions about security behaviors and their antecedents from a PMT-based framework. We conduct that examination by interviewing ordinary insiders and organizational information security experts, and then analyzing the results using thematic coding. We note important findings about the differences in how insiders and security experts view organizational security matters. We discuss these findings, along with their contributions to research and practice, and conclude by discussing the limitations and future research opportunities that emerge from this study.

2. Theoretical foundation: protection–motivation theory

PMT is a general theory of persuasive communication with an emphasis on understanding the cognition, attitudes, and behavioral intentions of individuals in response to threat information—especially threats received via fear appeals [6]. A *fear appeal* is a message designed to increase awareness of an environmental threat, to motivate the target to take a course of action to reduce the fear of the threat and ultimately, the harm stemming from the threat [33]. PMT suggests that two types of behaviors are possible when an individual faces a threat: adaptive and maladaptive [66]. *Adaptive behaviors* are those activities that successfully lessen the effects of the threats, and thus are beneficial in subduing the danger; *maladaptive behaviors* only reduce the fear experienced by individuals, rather than the danger presented by those threats [67]. As a result, maladaptive behaviors often lull individuals into a false sense of safety because they do not eliminate danger—they focus on downplaying the fear that should alert them to danger. Examples of adaptive behaviors in a security context include installing and using anti-malware software, backing up data, and adhering to organizational data-retention policies. Examples of maladaptive behaviors in this context include *avoidance* (e.g., "I try not to think about security threats on the Internet"), *fatalism* (e.g., "I will be attacked by a hacker regardless of whether I do anything about it or not"), and *religious faith* (e.g., "I think the best way to deal with the security of my organization's information resources is to pray to God and ask Him to handle it").

Engagement in either of these behavior sets in an organizational context is preceded by the individual's assessment of both positive and negative factors associated with the security threats and that individual's potential subsequent reactions. These two assessments are termed the *threat appraisal* and *coping appraisal processes*. Table 1 describes these assessments proposed by PMT

Table 1
PMT components.

Assessment	Definition	Proposed influence on protection motivation
Threat appraisal		
Maladaptive rewards	Potential rewards (intrinsic and extrinsic) that individuals expect to receive for engaging in maladaptive behaviors	Negative
Threat severity	The extent to which individuals believe that a threat or danger is severe	Positive
Threat vulnerability	The extent to which individuals believe that they are susceptible to a threat or danger	Positive
Coping appraisal		
Response efficacy	The perception that a particular behavior to cope with a threat would successfully attenuate the threat	Positive
Self-efficacy	The belief that individuals are personally capable of appropriately implementing a recommended protective response	Positive
Response costs	Any perceived, potential negative side effects of the protective strategy or of the actions associated with a specific response	Negative