Chapter 39
Management of Technical Security Measures:
An Empirical Examination of Personality Traits and Behavioral Intentions

Jörg Uffen
Leibniz Universität Hannover, Germany

Michael H. Breitner
Leibniz Universität Hannover, Germany

ABSTRACT

Organizations are investing substantial resources in technical security measures that aim at preventively protecting their information assets. The way management – or information security executives – deals with potential security measures varies individually and depends on personality traits and cognitive factors. Based on the Theory of Planned Behavior, the authors examine the relationship between the personality traits of conscientiousness, neuroticism and openness with attitudes and intentions towards managing technical security measures. The highly relevant moderating role of compliance factors is also investigated. The hypothesized relationships are analyzed and validated using empirical data from a survey of 174 information security executives. Findings suggest that conscientiousness is important in determining the attitude towards the management of technical security measures. In addition, the findings indicate that when executives are confronted with information security standards or guidelines, the personality traits of conscientiousness and openness will have a stronger effect on attitude towards managing security measures than without moderators.

INTRODUCTION

The proliferation of interconnected networks results in a variety of complex, multinational information security risks. Research studies emphasize management's increasing concerns about the protection of organizational information assets (Straub & Welke, 1998). Hence, it is important that today's organizations determine how to employ effective technical security measures to secure

DOI: 10.4018/978-1-4666-8111-8.ch039

organizational networks against external threats (Cavusoglu et al., 2009). The management of (technical) security measures is defined as a part of daily tasks of an information security executive, whose activities, such as administration or running Virtual Private Networks (VPN), or being suspicious of and reacting to current security breaches aim at hindering network attacks. But the way information security executives deal with potential information security measures varies individually and depends on personality and other cognitive factors (Straub & Welke, 1998; Vroom & von Solms, 2004). Individual management differences have become an important area of focus in information security research. For example, Sharma and Yetton (2003) investigated the positive influence of management on an employee's cognitive beliefs, attitudes, and behavioral patterns when dealing with information security. Ashenden (2008) emphasized the need for managing soft skills to effectively change organizational culture and to improve communication between end-users, information security executives, and senior managers.

Little effort has yet been made to examine the influence of individual differences and attitudes or behavioral patterns among information security executives. In information systems (IS) research, a useful way to integrate individual differences into IS models and theories is the adoption of the Five Factor Model (FFM) (Bansal, 2011; Devaraj et al., 2008). Drawing on the well-established and widely accepted Theory of Planned Behavior (TPB) (Ajzen, 1991) we demonstrate the potential influence of personality traits on an information security executive's attitude or beliefs towards managing technical security measures. In addition, standards and guidelines that support information security executives in their daily tasks are becoming more and more important (Siponen & Willison, 2009). In order to obtain a better understanding of the external factors that might affect an information security executive's attitude towards management of security measures, compliance, as a potential moderator between personality traits and attitudes was included. We explore the following research questions by testing an integrated model:

1. Which and how do personality traits of an information security executive affect their attitude towards managing technical security measures?
2. To what extent are compliance factors potential moderators between personality traits and attitude towards managing technical security measures?

The roles and responsibilities of executives in information security have been shown to be the main predictors of success (Straub & Welke, 1998). In this context, personality traits can illustrate how individual differences determine the strength of an individual's attitude in a specific context (Devaraj et al., 2008). Incorporating personality traits with a focus on cognitive processes of information security executives has largely been ignored.

THEORETICAL FOUNDATIONS

Information Security

Researchers and practitioners have addressed information security from multiple perspectives, including the design and implementation of security measures and socio-organizational treatments (Anderson & Agarwal, 2010; D'Arcy et al., 2008). Very often, organizations are faced with contradictory requirements to deal with open systems on the one hand and assure high protection standards on the other. The aim of information security management is to maximize the number of prevented and deterred security breaches (D'Arcy et al., 2008) by adopting an efficient set of technical security measures (Cavusoglu et al., 2009). The effectiveness of security measures in general has to be balanced with a variety of organizational issues which include the impact on employee