
Teodor Sommestad, Swedish Defence Research Agency (FOI), Linköping, Sweden
Henrik Karlzén, Swedish Defence Research Agency (FOI), Linköping, Sweden
Jonas Hallberg, Swedish Defence Research Agency (FOI), Linköping, Sweden

ABSTRACT

Individuals’ willingness to take security precautions is imperative to their own information security and the information security of the organizations they work within. This paper presents a meta-analysis of the protection motivation theory (PMT) to assess how its efficacy is influenced by the information security behavior it is applied to. It investigates if the PMT explains information security behavior better if: 1) The behavior is voluntary? 2) The threat and coping method is concrete or specific? 3) The information security threat is directed to the person itself? Synthesized data from 28 surveys suggests that the answers to all three questions are yes. Weighted mean correlation coefficients are on average 0.03 higher for voluntary behavior than mandatory behavior, 0.05 higher for specific behaviors than studies of general behaviors, 0.08 higher to threat appraisal when the threat targets the individual person instead of the person’s organization or someone else.

Keywords  Information Security Behavior, Information Security, Meta-Analysis, Policy Compliance, Protection Motivation Theory

1. INTRODUCTION

The behavior of individuals handling information resources significantly influences the information security of organizations (R. J. Anderson, 2008; Gollmann, 2006; Shostack & Stewart, 2008). Understanding the variables influencing the security behavior of individuals is important. For instance, by understanding the reasoning of employees, a manager can formulate and justify the information security policy so that it gains wider acceptance or government can educate the public on how to avoid computer malware.

The protection motivation theory (PMT) is an established theory, originally developed to explain how to influence risky behavior and which components a persuasive message should

DOI: 10.4018/IJISP.2015010102
include. The PMT builds on the theory of fear appeals and at its core lies the idea that the behavior of individuals is influenced by their threat appraisal (how thrilling, severe and likely an unwanted consequence is) and their coping appraisal (how efficient, manageable and costly the risk reducing behavior is) (Rogers, 1983). Loosely put, the PMT posits that individuals form their behavior from a cost-benefit analysis where risks associated with the behavior are compared to the costs of trying to reduce or eliminate the risks. This is very similar to the way of thinking promoted in security standards like the ISO 27000 series (IEEE/IEC, 2012), where a selection process focusing on cost-effectiveness is endorsed. In a sense, PMT describes a homo securitas which is rational from a security perspective in the same way as homo economicus (see Persky (1995)) is rational from an economic perspective.

From published tests of relationships described by the PMT it is clear that the theory is able to explain a fair share of intentions related to information security behavior. However, there are good reasons to expect that the accuracy of the theory depends on the type of security behavior it is applied to. First, the PMT has been developed to explain how fear appeals influence voluntary behavioral intentions related to the health. In the information security domain several studies have investigated variables related to the PMT in the context of information security policy compliance or other mandatory behaviors. Second, the theory was developed to explain cognitive processes related to specific threats (e.g., cancer) and specific coping methods (e.g., stop smoking). However, it has also been applied to information security behaviors that are abstract or complex, like behaving securely. Third, the theory was developed for (health) threats against individuals themselves, and not threats against an organization or others. For these reasons this paper revisits the published literature and presents a meta-analysis aiming at answering the following three questions:

1. Does the PMT explain information security behavior better if the behavior is voluntary?
2. Does the PMT explain information security behavior better if the threat and coping method is concrete or specific?
3. Does the PMT explain information security behavior better if the information security threat is directed to the person itself?

The remainder of this paper is outlined as follows. In the subsequent section the PMT is described. Thereafter the review protocol and review method is presented. In the fourth section the results are presented. Last, the results are discussed together with suggestions for future research.

2. PROTECTION MOTIVATION THEORY

When Rogers (Rogers, 1975) formulated the first version of the PMT in 1975, the variables said to determine protection motivation were: the severity or noxiousness of an event (severity), the probability that the event occurs if no protective behavior is performed (vulnerability), and the efficacy of the recommended behavior (response efficacy). According to the original theory, cognitive processes cause these variables to mediate each other, e.g., the importance of the perceived probability of an event is irrelevant if the by the perceived severity of the event is low.

When the PMT was updated in 1983 (Maddux & Rogers, 1983; Rogers, 1983), it was presented as a more general theory of persuasive communication, and stimulus variables (e.g., personality and past experience) believed to influence the cognitive processes indirectly were identified. In addition, the theory was extended with constructs believed to be of importance to the cognitive processes, namely: rewards associated with the threat (e.g., stolen identity) as well as response.
IPHDBCM: Inspired Pseudo Hybrid DNA Based Cryptographic Mechanism to Prevent Against Collaborative Black Hole Attack in Wireless Ad hoc Networks
www.igi-global.com/article/iphdbcm/160774?camid=4v1a

A Distributed and Secure Architecture for Signature and Decryption Delegation through Remote Smart Cards
Giuseppe Cattaneo, Pompeo Faruolo and Ivan Visconti (2012). Threats, Countermeasures, and Advances in Applied Information Security (pp. 53-65).
www.igi-global.com/chapter/distributed-secure-architecture-signature-decryption/65762?camid=4v1a