Chapter XIX
Do Information Security Policies Reduce the Incidence of Security Breaches:
An Exploratory Analysis

Neil F. Doherty
Loughborough University, UK

Heather Fulford
Loughborough University, UK

ABSTRACT

Information is a critical corporate asset that has become increasingly vulnerable to attacks from viruses, hackers, criminals, and human error. Consequently, organizations are having to prioritize the security of their computer systems in order to ensure that their information assets retain their accuracy, confidentiality, and availability. While the importance of the information security policy (InSPy) in ensuring the security of information is acknowledged widely, to date there has been little empirical analysis of its impact or effectiveness in this role. To help fill this gap, an exploratory study was initiated that sought to investigate the relationship between the uptake and application of information security policies and the accompanying levels of security breaches. To this end, a questionnaire was designed, validated, and then targeted at IT managers within large organizations in the UK. The findings presented in this chapter are somewhat surprising, as they show no statistically significant relationships between the adoption of information security policies and the incidence or severity of security breaches. The chapter concludes by exploring the possible interpretations of this unexpected finding and its implications for the practice of information security management.

INTRODUCTION

It has been claimed that "information is the firm's primary strategic asset" (Glazer, 1993), as it is the critical element in strategic planning and decision making as well as day-to-day operational control. Consequently, organizations must make every effort to ensure that their information resources retain their accuracy, integrity, and availability. However, ensuring the security of corporate information assets has become an extremely complex and challenging activity, due to the growing value of information resources and the increased levels of interconnectivity among information systems both within and among organizations (Garg et al., 2003). Indeed, the high incidence of security breaches suggests that many organizations are failing to manage their information resources effectively (Straub & Welke, 1998). One increasingly important mechanism for protecting corporate information, and in so doing reducing the occurrence of security breaches, is through the formulation and application of a formal information security policy (InSPy) (Hinde, 2002; von Solms & von Solms, 2004). Gaston (1996, p. 175) defines an InSPy as: "broad guiding statements of goals to be achieved; significantly, they define and assign the responsibilities that various departments and individuals have in achieving policy goals."

The role and importance of information security policies and the incidence and severity of security breaches are both topics that have attracted significant attention in the literature, but there is little evidence that these topics have been explicitly linked. Consequently, there has been little empirical exploration of the extent to which information security policies are effective, in terms of reducing security breaches. The aim of this chapter is to help fill this gap by reporting upon the results of a study that sought to empirically explore the relationship between the uptake and application of information security policies and the incidence of security breaches. The remainder of this chapter is organized into the following five sections: a review of the literature and a description of the conceptual framework; a discussion of the research methods employed; a presentation of the findings; a discussion of their importance and finally the conclusions and recommendations for future research.

LITERATURE REVIEW AND CONCEPTUAL FRAMEWORK

This section aims to present a discussion of the literature with regard to the role and importance of the InSPy and the common security threats, which such policies are intended to prevent. The section concludes with a critique of this literature, and the presentation of the conceptual framework for our study.

The Role of the Information Security Policy

The broad aim of the information security policy is to provide the "ideal operating environment" for the management of information security (Barnard & von Solms, 1998), by defining: "the broad boundaries of information security" as well as the "responsibilities of information resource users" (Hone & Eloff, 2002b, p. 145). More specifically, a good security policy should: "outline individual responsibilities, define authorized and unauthorized uses of the systems, provide venues for employee reporting of identified or suspected threats to the system, define penalties for violations, and provide a mechanism for updating the policy" (Whitman, 2004, p. 52).

The InSPy also has an important role to play in emphasizing management's commitment to, and support for, information security (Gaston, 1996; Hone & Eloff, 2002b; Kwok & Longley, 1999). While the InSPy provides the framework for facilitating the prevention, detection, and response to security breaches, the policy document