IGI PUBLISHING **ITB14761**

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.igi-pub.com

This paper appears in the publication, **Emerging Information Resources Management and Technologies**
edited by **Mehdi Khosrow-Pour, DBA © 2007, IGI Global**

Chapter III

Exploring the Effectiveness of Information Security Policies

Neil F. Doherty, Loughborough University, UK

Heather Fulford, Loughborough University, UK

Abstract

Ensuring the security of corporate information assets has become an extremely complex, challenging and high-priority activity, due partly to their growing organisational importance, but also because of their increasing vulnerability to attacks from viruses, hackers, criminals, and human error. Consequently, organisations are having to prioritise the security of their computer systems, to ensure that their information assets retain their accuracy, confidentiality, and availability. Whilst the importance of the information security policy (InSPy) in ensuring the security of information is widely acknowledged, there has, to date, 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 organisations in the United Kingdom. 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

For the past two decades it has been argued that an "*information revolution*" is taking place within organisations, which has made information the critical input to strategic planning and decision making, as well as the day to day control of organisational operations. Indeed, it is often contended that information is now analogous to an organisation's lifeblood: should the flow of information become seriously restricted or compromised, then the organisation may wither and die. However, if applied effectively as a strategic resource, information investments can result in the realisation of significant corporate benefits. As McPherson (1996) argues, "information is vital to the success of the business and will be accountable for a significant share of the business's various indicators of success, including its cash flow and market value." Consequently, organisations 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 between information systems, both within and between organisations (Garg, Curtis, & Halper, 2003). Indeed, the high incidence of security breaches suggests that many organisations are failing to manage their information resources effectively (Dhillon, 2004b). 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) (e.g., Baskerville & Siponen, 2002; Doherty & Fulford, 2006). Rees, Bandyopadhyay, and Spafford (2003, p. 101) provide a useful overview of the role of the information security policy, when they suggest that it should be "high-level, technology-neutral, concern risks, set directions and procedures, and define penalties and counter-measures, if the policy is transgressed."

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 the results of a study that sought to empirically explore the relationship between the uptake and