ABSTRACT

Personal Web usage (PWU) in the workplace is a matter of considerable concern to organizations today. However, human resources managers are not fully aware of the range of actions they can take to reduce PWU. This chapter examines general deterrence theory in the context of PWU and identifies actions that managers can take to reduce PWU. It uses a two-stage research methodology consisting of: (1) interviews with managers to gather qualitative data, and (2) a field survey of end users to gather quantitative data on PWU. It finds support for the deterrence theory and recommends that managers use a sequential implementation of four deterrence stages to contain PWU. These are: (1) framing an ‘Internet use
policy,’ (2) implementing measures to prevent PWU such as restricting Internet access only to certain employees, (3) implementing appropriate content management software to detect PWU, and (4) standardizing policies to remedy non-acceptable Web usage. These four deterrence stages can protect an organization from the harmful effects of PWU of its employees.

INTRODUCTION

Personal Web usage (PWU) in the workplace is defined as “any voluntary act of employees using their companies’ Internet access during office hours to surf non-work-related websites for non-work purposes” (Lim, Teo, & Looh, 2002). The occurrence of PWU may be viewed as a kind of systems risk, i.e., the likelihood that a firm’s information systems (IS) are insufficiently protected against certain kinds of damage or loss. As with systems risk, managers are generally unaware of the full range of actions they can take to reduce PWU (Straub & Welke, 1998; Lim, Teo, & Looh, 2002). The general deterrence theory, drawn from the field of criminology, suggests that sanctions and disincentive measures can reduce systems abuse by making potential abusers aware that their unethical behavior will be detrimental to their own good (Pearson & Weiner, 1985).

According to this theory, strategies that can be adopted to reduce systems risk fall into four distinct, sequential activities, i.e., (1) deterrence, (2) prevention, (3) detection, and (4) remedies. Deterrent measures include policies and guidelines for proper system use. They tend to be passive in that they have no inherent provision for enforcement. They depend wholly on the willingness of system users to comply. Preventive measures include for example locks on computer room doors and password access controls. They are active measures with inherent capabilities to enforce policy and ward off illegitimate use. If deterrent and preventive measures are unsuccessful in containing abuse, then detection measures can be deployed. These include proactive security responses such as suspicious activity reports, system audits and virus scanning reports, or reactive responses such as detective work after a documented breach in security. These measures gather evidence of abuse and identify perpetrators. Finally, remedies are measures that can correct the harmful effect of an abusive act and punish the perpetrators. Internal actions include warnings, reprimands, and termination of employment. Legal actions include criminal and
Mostly Co-Lated
www.igi-global.com/chapter/mostly-lated/31467?camid=4v1a