Chapter XI

Managing Corporate E-Mail Systems: A Contemporary Study

Aidan Duane, Waterford Institute of Technology, Ireland
Patrick Finnegan, University College Cork, Ireland

Abstract

As the criticality of e-mail for electronic business activity increases, ad-hoc e-mail implementation, prolonged management neglect and user abuse of e-mail systems have generated negative effects. However, management's ability to rectify problems with e-mail systems is hindered by our understanding of its organisational use. Research on e-mail systems is often dated and based on quantitative methodologies that cannot explain the interaction between various controls in organisational settings. Updating our understanding of the organisational aspects of e-mail systems utilizing qualitative methods is necessary. This chapter presents a multiple case study investigation of e-mail system monitoring and control. The study examines the interaction between key elements of e-mail control identified by previous researchers and considers the role of such controls at various implementation phases. The findings reveal eight major elements to be particularly important in monitoring and controlling e-mail systems within the organisations studied. These are: (1) form a cross-functional e-mail system management team; (2) implement and regularly update e-mail management software; (3) formulate a detailed and legally sound e-mail policy; (4) engage...
Introduction

Internet-based electronic commerce applications constitute a significant departure from traditional information technologies, posing more risks to the organisation because of their extensive direct electronic interaction with other entities (De & Mathew, 1999). In particular, an e-mail system introduces a new set of threats and legal issues to an organization, and the dramatic increase in e-mail usage is commensurate with the rising number of workplace incidents and disputes (American Management Association (AMA), 2003; Attaran, 2000; Hancock, 1999; PriceWaterhouseCoopers (PWC), 2002; Simmers, 2002; Weber 2004). As organisations struggle to derive value from information technologies (Agarwal, 2001) and scrutinise spending on all applications, including e-mail (Graff, 2002c), particularly in periods of reduced information technology (IT) budgets (PWC, 2002), organisations waste money buying technology if they don’t create the human infrastructure, policies and procedures to curb information systems abuses (Hancock, 1999).

E-mail systems have traditionally been initiated by IT departments without being part of a business-led strategy. Nevertheless, e-mail has evolved over time to become more of a corporate-wide service (Jackson, Dawson, & Wilson, 2000). The e-mail infrastructure is now a mission critical component of the enterprise information infrastructure and an essential component in all implementations of e-commerce platforms, especially for enterprises striving to become more virtual, resilient, and efficient (Graff, 2002b). E-mail systems have also become heavily integrated with mobile technologies, particularly portable telephones, and thus there is an increasing importance on Web or wireless access to central e-mail servers (Graff & Grey, 2002). This mobile e-mail access provides users with more flexibility and mobility but increases the pressure on the organisation to maintain and improve the reliability of the core e-mail system infrastructure (Graff & Grey, 2002). Mobile e-mail access also brings new pathways for the entry of viruses or the exit of confidential information (Graff & Grey, 2002). The more that organisations rely on e-mail, the more reliable it must be, because the risk of business interruption increases dramatically (Graff & Grey, 2002). Organisations must secure, expand and manage this communication medium effectively to meet new challenges (Graff & Grey, 2002; Weber, 2004).

Simmers (2002) contends that vague, unmonitored, unenforced, or absent e-mail policy exposes the organisation to a number of legal, financial, and operational risks such as losses of confidential information, network congestion, threats to network integrity, diversion of employee attention, and increased liability. Simmers (2002) and Weber (2004) contend that the nature and incidence of problematic e-mail use requires particular attention because of the costs it imposes on organisations. Consequently, organisations are increasingly challenged to get e-mail under control (Graff, 2002e) and must become more focused on stabilising and protecting their e-mail systems, gaining more control over the use of their systems and...