Chapter VII
Managing E-Mail Systems:
An Exploration of Electronic Monitoring and Control in Practice

Aidan Duane
Waterford Institute of Technology (WIT), Ireland

Patrick Finnegan
University College Cork (UCC), Ireland

ABSTRACT

An email system is a critical business tool and an essential part of organisational communication. Many organisations have experienced negative impacts from email and have responded by electronically monitoring and restricting email system use. However, electronic monitoring of email can be contentious. Staff can react to these controls by dissent, protest and potentially transformative action. This chapter presents the results of a single case study investigation of staff reactions to electronic monitoring and control of an email system in a company based in Ireland. The findings highlight the variations in staff reactions through multiple time frames of electronic monitoring and control, and the chapter identifies the key concerns of staff which need to be addressed by management and consultants advocating the implementation of email system monitoring and control.

INTRODUCTION

The email infrastructure is now a mission critical component of the enterprise information infrastructure and an essential component in all implementations of eCommerce platforms, especially for enterprises striving to become more virtual, resilient and efficient (Graff, 2002a). Email systems have also become heavily integrated with mobile technologies, thus there is an increasing importance on Web or wireless access to central email servers (Graff and Grey, 2002). Mobile email access also increases the pressure on the organisation to maintain and improve the reliabil-

ity of the core email system infrastructure (Graff and Grey, 2002). The more organisations rely on email, the more reliable it must be, because the risk of business interruption increases dramatically (Graff and Grey, 2002). Organisations must secure, expand and manage this communication medium effectively to meet new challenges (Graff and Grey, 2002; Weber, 2004).

However, the dramatic increase in email usage is commensurate with the rising number of email related workplace incidents and disputes (Simmers, 2002; American Management Association (AMA), 2004; Weber 2004). Personal use of email remains the number one use of email in the workplace (Russell et al., 2007). Organisations are all too aware of the problems associated with email use and are becoming more determined to reduce these threats (Burgess et al., 2005). Organisations must become more focused on stabilising and protecting their email systems, gaining more control over the use of their systems and managing risk associated with these systems (Graff and Grey, 2002).

Some organisations employ technology based solutions to control the email system including electronically monitoring all email activities, electronically filtering and blocking incoming and outgoing emails and restricting email systems for personal use (Sipior and Ward, 2002; Stanton and Stam, 2003). However, organisations can rarely dominate staff with the unilateral imposition of technology (Stanton and Stam, 2003). Although, technical controls are necessary, their effectiveness is questionable if organisations fail to look at the contextual issues of information systems (Dhillon, 1999).

Some organisations do little more than ask their employees to comply with a formal email policy (Simmers, 2002) while other organisations enforce hard-line email policies that exert zero tolerance of personal email use that are so nebulous that every employee could be deemed in violation (Oravec, 2002). However, Simmers (2002) contends that vague, unmonitored, unenforced or absent email 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.

What is know for certain, is that too much or too little email systems management can be dysfunctional for an organisation (Simmers, 2002). Thus, Weber (2004) argues that 'in our efforts to improve email technology, we need to take care that we do not exacerbate problems with email use'. Weber (2004) suggests that technological developments associated with email use may prove to be ineffective if they are not informed by social science research. Burgess et al. (2005) reveal that training staff on the best practices of email use is a critical factor to reducing email defects within an organisation. Sipior and Ward (2002) argue that it is imperative that organisations formulate a coordinated and comprehensive response to email system management. Stanton and Stam (2003) suggest that this should occur within the context of a negotiatory process involving management, employees and IT professionals.

Weber (2004) contends that we lack a deep understanding of the impacts of email on organisations and our understanding of these impacts remains fragmented and superficial. The majority of the research produced over the past two decades on email systems utilizes quantitative methods to examine the social and technical concerns of email systems. Laboratory-like experiments and mass surveys dominate the literature on email studies. As a result, there has been relatively little published advice on how to take an organisational view of email systems (Ruggeri et al., 2000). As a result, Weber (2004) believes that we still have 'human, technological, and organisational problems to solve' in relation to email systems and calls for 'better ways of managing email and assisting users to deal with the problems it poses'. It is imperative that underlying all uses of email, current and expanded, is careful planning, monitoring and management of the email