View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by WIT Repository

MANAGING CORPORATE EMAIL SYSTEMS: A CONTEMPORARY STUDY

Aidan Duane

Waterford Institute of Technology,

The School of Business,

Cork Road, Waterford, Ireland.

+353 51 302686

ADuane@wit.ie

Patrick Finnegan

University College Cork,

Department of Accounting, Finance & Information Systems,

Western Road, Cork, Ireland.

+353 21 4903344

P.Finnegan@ucc.ie

ABSTRACT

As the criticality of email for electronic business activity increases, ad-hoc email implementation, prolonged management neglect and user abuse of email systems have generated negative effects. However, managements ability to rectify problems with email systems is hindered by our understanding of its organisational use. Research on email 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 email systems utilizing qualitative methods is necessary. This paper presents a multiple case study investigation of email system monitoring and control. The study examines the interaction between key elements of email 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 email systems within the organisations studied. These are: (1) form a cross-functional email system management team; (2) implement and regularly update email management software; (3) formulate a detailed and legally sound email policy; (4) engage in structured email system training; (5) create and maintain ongoing awareness of email policy; (6) engage in a process of hybrid feedback and control based email monitoring; (7) firmly enforce discipline in accordance with the email policy; and (8) conduct regular reviews and updates of the email management programme.

KEYWORDS

Email System(s); Email Policy (Policies); Systems Abuse(s); Monitoring; Control; Monitoring and Control; Time Frame Analysis; Case Studies

MANAGING CORPORATE EMAIL SYSTEMS: A CONTEMPORARY STUDY

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 and Mathew, 1999). In particular, an email system introduces a new set of threats and legal issues to an organisation and the dramatic increase in email usage is commensurate with the rising number of workplace incidents and disputes (Hancock, 1999; Attaran, 2000; PriceWaterhouseCoopers, 2002; Simmers, 2002; American Management Association (AMA), 2003; Weber 2004). As organisations struggle to derive value from information technologies (Agarwal, 2001) and scrutinise spending on all applications including email (Graff, 2002c), particularly in periods of reduced 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).

Email systems have traditionally been initiated by IT Departments without being part of a business-led strategy. Nevertheless, email has evolved over time to become more of a corporate-wide service (Jackson et al., 2000). 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, 2002b). Email 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 email servers (Graff and Grey,

2002). This mobile email access provides users with more flexibility and mobility but increases the pressure on the organisation to maintain and improve the reliability of the core email system infrastructure (Graff and Grey, 2002). Mobile email access also brings new pathways for the entry of viruses or the exit of confidential information (Graff and Grey, 2002). The more that organisations rely on email, the more reliable if 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).

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. Simmers (2002) and Weber (2004) contend that the nature and incidence of problematic email use requires particular attention because of the costs it imposes on organisations. Consequently, organisations are increasingly challenged to get email under control (Graff, 2002e) and 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). Only when an email system is used and managed properly will an organisation be able to reap its benefits (Ruggeri et al., 2000; Graff, 2002e). Thus, it is imperative that underlying all uses of email, current and expanded, is careful planning, monitoring and management of the email infrastructure (Graff and Grey, 2002; Simmers, 2002; Sipior and Ward, 2002; Weber, 2004). In particular, organisations should anticipate the potentially harmful effects of email systems and seek to prevent them from occurring (Van den Hooff, 1997). However, organisations

lack analytical tools and understanding to examine their existing practices and to assist in reasserting email systems for corporate rather than individual purposes (Ruggeri et al., 2000; Weber, 2004).

The appropriate design, management and application of any communication system depends to a great extent upon appropriate ongoing research of those systems from technical, organisational and social perspectives (Rice, 1990). However, Weber (2004) contends that we still lack a deep understanding of the impacts of email on organisations and our understanding of these impacts remains fragmented and superficial. Although the unsatisfactory understanding of the impacts of communication media provided by quantitative research has long been recognised (Rogers, 1986), it is evident that the majority of the research produced over the past two decades on email systems research utilizes quantitative methods to examine the social and technical concerns of email systems. The need for organizationally-based research has been highlighted in the past by researchers such as Fulk and Desanctis (1995) and Rudy (1996) in calling for situational studies which recount organisational environments in which electronic communications systems are used. Nevertheless, laboratory-like experiments (Culnan and Markus, 1987; Fulk et al., 1990; Mantovani, 1994; Cappel, 1995) and mass surveys (AMA, 2000; Schulman, 2001; Lim et al., 2002; A.M.A 2003; Hoffman et al., 2003) 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; Weber 2004). Weber (2004) comments that ‘many of us claim that as members of the information systems discipline we are well placed to study phenomena associated with human-computer interactions. It is somewhat ironic, therefore, that with few exceptions we find little research on email published in our major journals’.

Weber (2004) argues 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 of email to deal with the problems it poses’.

This paper presents the results of multiple case studies that investigate how organisations monitor and control their email systems. The next section examines the theoretical grounding for the study. This is followed by a discussion of the research method and a presentation of the research findings. The paper concludes by identifying key factors in a programme for email system electronic monitoring and control.

THEORETICAL GROUNDING

In the push to increase business use of email, many organisations failed to fully consider the implications of its implementation (Ruggeri et al., 2000) and many have not attended to developing or communicating email polices (Urbaczewski and Jessup, 2002). Other organisations left staff to establish the purpose and use of email systems (Ruggeri et al., 2000) while some organisations even encouraged playful use of the email system without controlling activities, to facilitate learning (Belanger and Van Slyke, 2002). However, as IT evolves its social construction changes (Benbunan-Fich, 2002). Users do not passively receive the technology in a pre-existing form; rather, they actively adapt the technology to their own ends. IT users choose what features of the technology they will use, and how they will use those features (Benbunan-Fich, 2002). Therefore, a technology in use should be conceived as a set of social practices that emerge and evolve over time (Giddens, 1979; Poole and DeSanctis, 1990).

Consequently, the initial technical success of email system implementation does not guarantee long term usefulness or political harmony, and can culminate in devastating side-effects during latter stages of implementation (Romm et al., 1996; Graff, 2002e; PWC, 2002). In fact,

numerous organisations worldwide are repeatedly reporting increasing negative effects of email systems (Attaran, 2000; PWC, 2002; Weber 2004). Some major companies have settled multimillion dollar sexual harassment lawsuits as a result of internally circulated email (Siau et al., 2002; Sipior and Ward, 2002). In many instances, it is reported that adequate systems control structures are absent (PWC, 2002; Sipior and Ward, 2002; Weber, 2004). Rice and Aydin (1991) suggest that organisations fail to anticipate and control the negative effects of information systems because they are less visible and expected, and thus, less assessed or managed. Noticeably, PWC (2002) report that it tends to be organisations that have experienced information systems abuse that implement controls. However, such results are not confined to email systems. Rogers' (1986) work on communications technology concluded that those who introduce communication technologies must see beyond the desirable, direct and anticipated impacts, and realise that more of the indirect, undesirable and unanticipated impacts of communication technologies occur as time elapses. Weber (2004) suggests that technological developments associated with email use may prove to be ineffective if they are not informed by social science research.

It has been proposed that the effects of computer-mediated communication can be categorised from a two level perspective as technology can have both first-level and second-level effects (Sproull and Kiesler, 1991). Researchers have identified the first level negative effects of email systems as: productivity drain (Anderson, 1999; Graff and Grey, 2002; Lim et al., 2002; PWC, 2002); security breaches; urgent communications overlooked; excessive non-business communication (PWC, 2002; Sipior and Ward, 2002; Lim et al., 2002); an increasing cost of usage; information overload and redundancy (Sproull and Kiesler, 1991; Graff and Grey, 2002; Lim et al., 2002; Weber, 2004). Researchers have identified the second level negative effects of email systems as: depersonalization; disinhibition (Markus, 1994; Siau et al., 2002; Weber, 2004); profanities, bad

news, negative sentiment and illicit use (Hodson et al., 1999; Siau et al., 2002); deindividuation (Sproull & Kiesler, 1991; Kwong and Lee, 2002); gender imbalance; electronic protestation and revolt (Sproull and Kiesler, 1991; Sipior and Ward, 2002); and gaining leverage (Rudy, 1996).

When electronic communication can potentially undermine management control, management predictably assert that control more vigorously (Sproull and Kiesler, 1991). The negative effects of information systems challenge managers to formulate policies and procedures that control but do not discourage use (Anadarajan et al., 2000). An effective programme of monitoring and control is a commonly identified success factor in assimilating new technologies (Hoffman and Klepper, 2000). Control in organisations is achieved in many ways, ranging from direct surveillance to feedback systems, to social and cultural controls (Simons, 1995). Control can be interpreted as both monitoring activities, and then taking action to ensure a preferred behaviour of a system being controlled (Aken, 1978; Otley and Berry, 1980). Electronic monitoring extends the scope of control, transforming personal control to systemic control and as technical controls emerge, personal, social, structural, and cultural controls extend through electronic mediation (Orlikowski, 1991). Thus, monitoring and control are intertwined (Otley and Berry, 1980).

There is increasing sentiment among managers that a more hands-on approach to email systems management is needed (Simmers, 2002). However, too much or too little email systems management can be dysfunctional for an organisation (Simmers, 2002). Many organisations do little more than ask their employees to comply with a formal email policy (Simmers, 2002). However, Oravec (2002) suggests that some hard-line email policies that exert zero tolerance of personal email use are so nebulous that every employee could be deemed in violation. 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’. Thus, some organisations adopt electronic monitoring of email and restrict

email use (Ruggeri, et al., 2000; Belanger and Van Slyke, 2002; Weber, 2004). In fact, the number of organisations engaging in some form of electronic monitoring of email is steadily increasing year on year as is reflected in studies by Hodson et al. (1999), AMA (2000), Lim et al. (2002), PWC (2002), Sipior and Ward (2002) and AMA (2003). The main arguments in justification of email monitoring practices include prevention of systems abuse; to detect non-business use; to capture communication metrics; prevention of the loss of confidential information; prevention of competition; quality control; avoidance of liability for defamation; prevention of harassment and pornography; protection from computer viruses; and security (Oliver, 2002; PWC, 2002; Sipior and Ward, 2002). Simmers (2002) contends that managing the usage of the policy and enforcing the policy by monitoring/filtering software, enhances alignment of individual usage with organisational priorities.

However, email monitoring is contentious as it may conflict with staff privacy expectations (Sipior and Ward, 2002) and erode the trust between employer and staff (Urbaczewski and Jessup, 2002). Furthermore, zero-tolerance of personal use of email is debatable as organisations lose an effective means to increase their staffs work-related knowledge (Belanger and Van Slyke, 2002). Weber (2004) argues that organisations must permit some level of non-business email as 'organisations cannot expect employees to engage in work activities outside of work hours yet totally prohibit personal work during work hours'. Thus, well intended but non-analytical efforts by organisations to manage email, will result in problems at later stages of its diffusion (Ruggeri, et al., 2000). Thus, it is imperative that underlying all uses of email, current and expanded, is careful planning, monitoring and management of the email infrastructure (Graff and Grey, 2002; Simmers, 2002; Sipior and Ward, 2002; Weber, 2004). Sipior and Ward (2002) suggest that a strategic response to information systems abuse can consist of a combination of factors including assessing

current operations, implementing proactive measures to reduce potential misuse, formulating a usage policy, providing ongoing training, maintaining awareness of issues, monitoring internal sources, regulating external sources, securing liability insurance, keeping up-to-date with technological advances, legislative and regulatory initiatives, and identifying new areas of vulnerability. However, individual controls can have dysfunctional effects if isolated solutions are provided for specific problems (Dhillon, 1999). Thus, the key to an effective control environment is to implement an strong 'set' of controls (Dhillon, 1999).

Some classifications of control exist, as shown in table 1, and are used here even though the distinction between categories is open to debate. Formal controls (Dhillon, 1999) or 'control through social structure' (Pennings and Woiceshyn, 1987), involve developing rules that reflect the emergent structure with control embedded in explicit policies, procedures, and rules. Informal controls (Dhillon, 1999) or 'control through culture' (Pennings and Woiceshyn, 1987), consist of increased awareness supplemented with ongoing education and training so that the shared norms and values of workers shape behaviour, order perception and influence attitudes. With technical control (Dhillon, 1999) or 'control through technology' (Pennings and Woiceshyn, 1987), the role of management changes from direct supervision to enforcing the operation of the technical system. Thus, electronic monitoring and control enables a matrix of control, fusing together a range of capabilities to facilitate a more embedded means of control (Orlikowski, 1991). Applying the classification of technical, formal and informal controls identified by Dhillon (1999) to email systems monitoring and control, table 2 summarises the conclusions from a number of studies to identify some dysfunctional effects associated with certain controls.

Weber (2004) suggests that somehow technological developments need to reinforce and reward appropriate behaviours and curb inappropriate behaviours among email users. Organisations

must strive to identify a strategy of email system monitoring and control that simultaneously enables managers to influence employees and is acceptable to employees (Urbaczewski and Jessup, 2002).

However, Ruggeri et al. (2000) and Weber (2004) report that there is little support or insight to assist organisations in reasserting email systems for business use. Despite the importance of an email system, and even though for many of us it represents perhaps the most significant computer application we use, it is an under-researched topic within the information systems discipline and there is little published research about email in the major information systems journals (Weber, 2004). Weber (2004) calls for a deeper understanding of the impacts of email on organisations and contends that 'by focusing research on developing improved protocols to guide behaviours when we use email, we can be more confident in the appropriateness of any measures we use to enforce use of these protocols'. Rudy (1996) reported that the continued experience of the negative effect of email systems may imply that not enough research has been done in this area. Little appears to have changed. Thus, email phenomena provide a rich lode to mine for research purposes (Weber, 2004).

METHOD

This study aims to provide an organisational analysis of the monitoring and control of email systems. The case studies method is considered suitable as it is a rich source of data, and analytic generalisation can be applied where prior theory is used as a template for comparing the empirical results (Yin, 1994). Multiple case designs are desirable when the intent of the research is description as it allows for cross analysis and extension of theory (Benbasat et al., 1987). The appropriateness of the multiple case approach for this study is clarified in table 3. Four organisations (see table 4) were deemed suitable for participation in this study based on the following criteria:

- the organisation agrees to participate fully in the study;
- the organisation has a large community of email users;

- the email system is installed for a long period of time;
- the organisation considers the email system to be a vital component of their electronic business infrastructure; and,
- the organisation is taking measures to exert control over its email system.

According to Rogers (1986), high quality communications research should:

- obtain multiple measures from several independent sources;
- use objective data-sources such as computer monitored data, corporate records, archival materials, etc., rather than just individuals' self-reports as gathered in personal interviews and by questionnaires; and,
- utilise unobtrusive measures so that obtaining the data does not affect the data being gathered.

Following the approach outlined by Rogers (1986), data collection in each organisation took place over a fifteen month period using semi-structured interviews, focus group interviews, document analysis, and electronic data collection. A semi-structured interview method was used to facilitate a more contextual understanding of the phenomena and to develop a rich, descriptive impression of the events while exploring their occurrence in each organisation. Such interviews took place with the HR and IT Managers in each organisation as existing studies indicate that such managers play an integral role in managing organisational email systems. Semi-structured focus group interviews with other staff were conducted in order to triangulate findings. Documents analysed included email policies, manuals, documentation and email notifications about email use from each organisation. Finally, fifteen months of email monitoring data gathered from each organisation was gathered and analysed. These data flows provide opportunities to understand the application, management and consequences of email systems. The data gathered was analysed

through ‘time frame analysis’ denoted by pre, initial, early and latter implementation of email monitoring similar to those utilised by Rice (1990).

RESULTS

All four companies exercised little control over email system use in the early stages of diffusion, allowing staff unrestricted email communication. This approach to email management changed dramatically after the introduction of email monitoring software in each company in 2002. Table 5 presents the time frame analysis of the technical, formal and informal controls adopted by each organisation pre-implementation and during the initial, early and latter stages of email monitoring implementation. Table 5 also illustrates that there are a number of differences in how each of these organisations monitor and control their email systems. All four IT Managers were concerned that there was a problem with email use. Prior to implementing email monitoring they had no way of achieving an organisational perspective of email use. HealthCo decided to implement monitoring in order to establish greater transparency and visibility of email use, to ensure it wasn’t negatively effecting business transactions, and to smooth movement to future communication tools. InsureCo’s and TeleCo’s primary objectives were to improve the management and efficiency of email and to control personal use. InvestCo were directed by Corporate Headquarters to monitor email after productivity concerns related to personal use arose in another division.

Technical controls formed the thrust of all four organisations efforts to monitor and control email use prior to the implementation of email monitoring software in 2002. Yet these technical controls were poorly implemented with redundant anti-virus software and ineffective filtering/blocking rules. Furthermore, the IT Department dominated systems implementation and management, relying on technically focused training and/or technically written user manuals. Email policies, where they did exist, were poorly written and inadequately communicated. Email accounts

were not audited as it was considered too time consuming. Accounts were only accessed to eliminate viruses or to rectify malfunctions. Initial monitoring reveals quite a number of problems with email use in each of these organisations as outlined in table 6. Interestingly, it took the implementation of another technical control (i.e.) email monitoring software, to inject some effort by each of the companies into developing formal email system controls. It is also worth noting, that after the implementation of email monitoring software, feedback from this technical control was also the primary motivator for every update and fine-tuning of formal and informal controls, while also identifying areas where further controls were necessary.

ANALYSIS AND DISCUSSION

The case studies reveal eight major elements to be particularly important in monitoring and controlling email systems within the organisations studied. These are: (1) form a cross-functional email system management team; (2) implement and regularly update email management software; (3) formulate a detailed and legally sound email policy; (4) engage in structured email system training; (5) create and maintain ongoing awareness of email policy; (6) engage in a process of hybrid feedback and control based email monitoring; (7) firmly enforce discipline in accordance with the email policy. Finally, it is imperative to recognise that this is an ongoing process that the management team should (8) conduct regular reviews and updates of the email management programme, to adapt for changes in technology, changes in work-practices, changes in legislative and industry requirements, etc.

Form a Cross-Functional Email System Management Team

Stanton and Stam (2003) suggest that email management should occur within the context of a negotiatory process that brings management, employees and IT professionals to the same table. Previous research (Wolinsky and Sylvester, 1992) has suggested that organisations should establish

a formal committee, consisting of the IS manager, a company lawyer, a HR official, an executive management representative, a union representative and a general power user to oversee email management. Siau et al. (2002) consider it imperative for staff to be involved in the email management process. Table 7 outlines the organisational members responsible for email management in each of the four companies. HealthCo established the EMail Management Group (EMMG), consisting of the IT and HR Managers, a Business Process Improvement Manager and an Operations Manager. Interestingly, InvestCo was the only company to seek legal input and to allow an elected staff representative to join the email management committee. Responsibility in InsureCo was reluctantly accepted by the IT Manager. Wolinsky and Sylvester (1992) concluded that failing to formally appoint an individual or to form a committee to manage the email system, may mean that nobody will assume this responsibility, leading to an uncoordinated and disjointed approach to managing the system and a lack of direction for users, which could result in systems failure. TeleCo failed to formalise responsibility for pursuing improvements in email use and neither the HR or IT managers voluntarily accepted the task. Although processing and analysis of monitored data occurred monthly, neither manager reviewed the data effectively.

Implement and Regularly Update Email Management Software

There are an estimated thirty thousand viruses in existence with approximately three hundred new viruses created monthly (Sipior and Ward, 2002). Thus, protecting the email environment from viruses, malicious code and SPAM is now keenly appreciated as the cost of doing business as failure to protect the email environment will result in a real loss of system availability and productivity and a real loss of income (Graff and Grey, 2002). Although each of the companies had some version of email installed for 4-7 years, anti-virus software updates were extremely irregular. Only three of the companies had installed email filtering/blocking software, but again, this was very basic and was

largely ineffective. HealthCo installed an upgraded email system during the initial implementation of email monitoring software in 2002 but each of the other organisations persisted with their existing email system. However, the more communication metrics that were generated by the email monitoring software, the more apparent it became to all of the organisations that their email systems technical controls were seriously flawed. Only HealthCo took the initiative and installed more powerful anti-virus software following the feedback from the email monitoring software in the early stages. InsureCo and InvestCo took more of a big-bang approach in the latter stages, implementing anti-virus software automatically updated online and installing updated filtering/blocking software. Metrics in the latter stages of email monitoring also prompted HealthCo, InsureCo and InvestCo to extensively reconfigure their filtering/blocking software to limit personal email use and to block incoming/outgoing web-based email (e.g. to/from yahoo email addresses) and attachments unless necessary for business use. InsureCo also reduced email transmission/receipt capacity for some staff while InvestCo also reconfigured the email system to automatically purge deleted email every 48 hours. TeleCo took the least robust approach, choosing to only update the anti-virus software for automatic online updates in the latter stages of email monitoring whilst paying little attention to filtering/blocking incoming/outgoing email. According to PWC (2002), virus infection is the single largest cause of serious security breaches in organisations because organisations often fail to regularly update the email system anti-virus software, rendering it ineffective.

Formulate a Detailed and Legally Sound Email Policy

Graff (2000d) suggests that organisations should formulate an email system policy to maximise user efficiency, protect sensitive data and to reduce the risk of inappropriate message content. However, Attaran (2000) suggests that organisations often lack clear policies to prevent the negative effects of email. Siau et al. (2002) also suggests that most email policies are not formally

worded or legally sound and strongly recommend that legal assistance should be obtained in developing email policies. This view is confirmed by this study as the policies analysed were generally found to be poorly written, often confusing and contradictory and predominantly lacking any legal basis. Furthermore, Siau et al. (2002) and Graff (2000d) recommend that organisations should make it clear in the email policy that the primary purpose of an email system is for business purposes. In this research it was found that although the email policy of each company stated that email should only be allocated if the user had an explicit business use for it, each organisation provided universal access to the corporate email system. Some researchers would argue that this may not be detrimental as email is an essential business tool (Anderson, 1999), and if there is no access or if access is severely limited, organisational outcomes may suffer (Simmers, 2002). However, only InvestCo and TeleCo clearly describe and explain the value of email as a critical business tool in their email policies and manuals. Furthermore, despite several managers being involved in drafting HealthCo's email policy during the implementation of monitoring, their combined contributions amounted to copy/pasting paragraphs from the policies of other organisations. TeleCo's revised email policy, drafted six weeks after implementing monitoring, is fifteen pages in length, legalistic and jargon laden. The informal management of the email system effectively led the HR Manager to modify the email policy of a corporate division based in the US to fit the Irish division, rather than engage in a discussion with other stakeholders. InvestCo's HR Manager believes the implementation of monitoring forced a rethink about email policy and its communication, as the HR and IT Managers, Corporate Legal Department and a staff representative were engaged to draft the new policy. InsureCo never updated their email policy after implementing monitoring. Some authors (Wolinsky and Sylvester, 1992) suggest that staff should sign the email policy to acknowledge an

understanding of its contents and compliance, but none of the managers interviewed believed this prudent as failure to sign updates could be problematic.

Hodson et al. (1999), Oliver (2002), Hoffman et al. (2003) and Weber (2004) believe that the need for employees to rely on email to manage personal matters is particularly true in an era of longer workdays, multiple career households, and the increased sharing of earning and household management responsibilities. However, this personal use of email is only appropriate as long as it does not affect work patterns, productivity, performance or compromise the organisation in any way (Hoffman et al., 2003). Zero-tolerance of personal use of email is unacceptable to staff in each organisation investigated for this study, as many staff depend on email to maintain personal communications with family and friends. Limited personal use appears to be acceptable to management and staff in all companies. Confusingly, this is not reflected in HealthCo's email policy which explicitly prohibits personal use of email while the email policies of InsureCo and TeleCo only permit personal use of email outside of working hours. InvestCo's policy permits limited personal use during working hours only. Interviewees at all companies believe that policies should outline prohibited keywords and attachments to increase compliance and reduce misunderstandings, yet only HealthCo attempted to do so. However, HealthCo's HR Manager warns that 'specific definitions leave you open to oversights and the possibility of definition expiry'. This seems consistent with Hoffman et al. (2003), who found that although ninety two percent of organisations surveyed allowed employees reasonable personal use of email, fewer than half of these organisations clearly defined what they considered reasonable use.

According to Simmers (2002) organisations must be honest about monitoring, announcing when the monitoring will happen, and why and how it will be done. However, only HealthCo and TeleCo have clear references to email monitoring in their email policy. InsureCo's policy expresses

"the right to monitor <u>all</u> email" but specifically refers to *"MAILsweeper filtering software"*. InsureCo's *"Email Procedures"* document states that *"internal email shall not be subject to interception or inspection"*. InvestCo's policy does not mention monitoring but states that staff *"should have no reasonable expectation of privacy of communication"*. Many researchers recommend that organisations should also define how breaches of email policy will be dealt with (Banerjee et al., 1998). Only HealthCo's and TeleCo's policies assert the right to take disciplinary action up to, and including, dismissal. However, TeleCo's policy cites heavily from several Acts of US Law which have no legal basis in Ireland. In addition, interviewees found such laws difficult to assimilate. InsureCo's email policy does not mention disciplinary action anywhere. Although InvestCo's policy cautions that *"improper email use is subject to disciplinary action"*, staff members are referred to a *"Corporate Code of Discipline"* which contains no reference to email abuse. Table 8 reveals the attitude of the study participants to elements of an email policy identified as important by previous researchers. Furthermore, table 8 evaluates the inclusion of such elements in each company's policy.

Engage in Structured Email System Training

According to Jackson and Edwards (2005) email training is significantly successful at improving an employees ability to write emails, to use a subject line to convey information about the content more effectively and to write clearer emails that are more concise, thus reducing the cost associated with email. However, research (Attaran, 2000) has shown that organisations rarely train employees not to misuse email systems. The majority of managers interviewed in this study cite the allocation of staff, time and financial resources as major detractions from the training and education process. This contributes to a greater reliance on technical controls. Consequently, none of the managers initially had a positive attitude to training. Only one company made any significant effort

to rectify its approach to training staff to use and manage email more effectively. However, the majority of managers interviewed believed focusing primarily on technical issues when training staff to use email is an oversight and that an equal, if not greater portion of training, should focus on email behaviour and policy. InvestCo trained all staff when introducing the monitoring software as the HR Manager was confident that 'once staff knew the negative impacts of email and how it could affect the company, better email management would prevail'. The IT Manager believes that allowing the 'staff representative to deliver a large portion of the non-technical training, greatly contributed to staff acceptance of email policy' as training was 'delivered at their level of understanding by one of their colleagues so staff were supportive of the process'. InsureCo waited fourteen months after implementing monitoring to conduct a security awareness course highlighting technical, content and legal issues for all staff. While permanent staff at HealthCo had availed of initial technical training on email, the withdrawal of email privileges from summer interns, who had received no training whatsoever, revealed a glaring need for ongoing training. After eleven months of monitoring, HealthCo tried to redress training by holding a one day course for managers and supervisors, but yet again other staff members were overlooked. However, this approach is questionable as some researchers (Banerjee et al., 1998) argue that one-off training sessions may not be sufficient to combat email system abuse.

Weber (2004) considers it essential that employees be familiar with and capable of using technologies that will assist them to deal effectively with the negative effects of email. However, with the general exception of staff from InvestCo, focus group participants were rather critical of the support and training provided by the IT Department with filtering and mailbox maintenance. Interestingly, informal controls in the guise of staff coaching, became very appropriate after a failed attempt in InsureCo to create a technical control to force time limits on unopened customers email

enquiries for more efficient response times. Unable to reconfigure the email software, staff supervisors were charged with providing staff with further instruction on reducing volumes of unopened email and responding to email more efficiently. At no point have TeleCo engaged in email training, despite taking serious disciplinary against one employee. Table 9 reveals the attitude of the study participants to elements of email training identified as important by previous researchers. In particular, table 9 highlights the time line for the delivery of these elements in each of the companies.

Create and Maintain Ongoing Awareness of Email Policy

According to Sipior and Ward (2002) the primary defense against inappropriate information systems activities is to increase the awareness and understanding of what the risks are and how they arise. Simmers (2002) suggests that once the policy is written and reviewed by the organisations management and legal staff, it should be widely publicised through seminars, performance reviews and informal discussion sessions and it should be given to all new employees. Lim et al. (2002) and Sipior and Ward (2002) also propose that organisations can create awareness of email policy by formally presenting it to all employees, including it in the employee handbook, in memos, at meetings and by publishing it on the company Intranet. Nevertheless, creating and maintaining awareness of email policy is weak in three of the companies. Table 10 shows that only InvestCo formally presented the email policy to all staff, while HealthCo only presented the policy to managers and supervisors. The primary method for conveying email policy appears to be by email. However, this may not be sufficient or appropriate to achieve a change in user's attitudes towards email systems use. Overt communication approaches, such as broadcasting the email policy on the computer screen every time the email system is accessed (Hoffman et al., 2003) and frequent reminders to staff that their computer activities are subject to monitoring (Panko and Beh, 2002)

should be adopted by organisations. Although TeleCo is the only company to place the email policy on the email system log-in screen, it is the only way in which the company creates and maintains awareness of the email policy, and only consists of a rather brief synopsis of the policy. Rather than choose any form of personal communication, it is clearly evident from table 10 that each organisation depends on the email system to convey reminders, updates, feedback, warnings and user tips. However, interviewees in two companies revealed that notifications were often deleted or filed without been read.

Engage in a Process of Hybrid Feedback and Control Based Email Monitoring

Urbaczewski and Jessup (2002) argue that a hybrid of feedback and control monitoring is most appropriate for most organisations. Simmers (2002) suggests that the monitoring function should be more than the technology and that it should include periodic (weekly, monthly, bimonthly) generation of usage reports to allow feedback on policy compliance and discussion of these reports at appropriate levels of the organisation to enable action taken against those who violate the policy. It is reasonable to suggest that the four companies participating in this study focused more on the control aspects of the monitoring software than the extensive possibilities for providing positive feedback to staff on their email activities. This appeared to be because management were desperate to bring email under control and predominantly believed that this could only be achieved by formal warnings and coercions to bring email use back in line with business needs. Management in HealthCo, InsureCo and InvestCo provided monthly communications to staff on overall email use but HealthCo's and InsureCo's communications were primarily hostile and provided little in the way of positive feedback to staff. InvestCo's approach was much more positive from the early stages, providing staff with positive and encouraging feedback whilst requesting staff to add their own suggestions as to how email can be managed more effectively. InvestCo also emailed staff with tips

on improving mailbox management. The resultant effect of this was a much more positive email management environment according to staff in InvestCo. TeleCo's sole effort at providing any feedback was to implement a monthly automated email policy reminder sent to all staff.

Firmly Enforce Discipline in Accordance with the Email Policy

Siau et al. (2002) argue that organisations should always back up policies with decisive actions if a violation of policy occurs. In the US, this seems to be in practice as the AMA (2003) report that over twenty five percent of US organisations have terminated an employee contract for email infractions. Three of the four companies in this study took decisive disciplinary action. InvestCo were the only company to not punish staff for infringements. Both HealthCo and InsureCo initiated disciplinary action from the early stages of email monitoring. HealthCo formally reprimanded staff and revoked email privileges for some staff after gross violations of the email policy were detected. InsureCo issued verbal and written warnings to some staff for email policy breaches before finally disabling some staffs send email option and placing a disciplinary report on their staff file. However, this was later rescinded. TeleCo initiated the strongest response to a breach of email policy when suspending a staff member for disclosing sensitive business data by email. This prompted an extensive review of the email audit trail for all staff. Furthermore, Siau et al. (2002) encourage establishing a chain of command between the IT department and other departments as this is enables the supervisors of those who violate the policy to be responsible for discipline instead of overloading the IT department. This chain of command is reflected in the formation of a cross-functional email systems management team in HealthCo and InvestCo and appeared to work quite effectively. However, the IT Managers still suggested that too much responsibility for detecting email policy violations and enforcing discipline was placed on their shoulders.

Conduct Regular Reviews and Update of the Email Management Programme

Continuous evaluation for technology misuse is needed (Romm et al., 1996) and as email monitoring evolves, organisations need to review their policies and practices and revise them (Flood, 2003; Hoffman et al., 2003). As the evidence from these cases suggest, organisations do conduct regular reviews of their email management programmes. These reviews predominantly revolve around the feedback from the email monitoring data and are usually accompanied by one or more changes to how email is managed. These changes vary from minor adjustments to how email is filtered or blocked to more significant changes such as disabling the send email function on some staff email accounts. Siau et al. (2002) recommend that when there is a new policy or changes to an existing policy, employees should be notified. However, none of the organisations updated their policies since implementing email monitoring despite making changes to email management procedures on a number of occasions.

CONCLUSIONS

Careful planning, monitoring and management of the email infrastructure must underlie all uses of email, current and expanded. Failing to protect the email environment will result in possible losses to system availability, productivity and income. It is evident that a clear vision of controls should be developed as implementing patches in an illogical and incoherent manner, particularly when something goes wrong, may further compromise an organisation. This study aims to improve our understanding of the operation of email monitoring and control methods in organisational contexts. The findings highlight the need to formulate a coordinated response consisting of technical, formal and informal controls as part of an organisational approach to email management. Based on the analysis of the study findings, table 11 identifies the key technical, formal and informal controls for monitoring and control of email systems. These controls are a subset of those identified by

previous researchers (outlined earlier in table 1), and reflect the findings of the study on the interaction between controls. This conclusion is not an attempt to downplay the importance of other controls, but rather to highlight the importance of certain controls in an organisational context. Overall, the study has advanced our understanding of the application of email monitoring and control methods in an organisational context by applying a qualitative methodology to complement the results of previous quantitative studies. Nevertheless, the findings from the study are tentative and further research is required.

ACKNOWLEDGEMENTS

The researchers would like to acknowledge the assistance of the Irish Research Council for the Humanities and Social Sciences (IRCHSS) without whose kind support, this project would not have been possible. The researchers would also like to thank the organisations and individuals who participated in this study for their generous cooperation and contribution.

REFERENCES

Agarwal, R. (2001) Research in Information Systems: What We Haven't Learned. *MIS Quarterly*, 25, 4, v-xv.

Aken, J.E. (1978) On the Control of Complex Industrial Organisations. American Bank Association (1972) *Results of the National Automation Survey*, Washington, DC.

American Management Association (AMA) (2000) *Workplace Testing: Monitoring and Surveillance.* NY, US.

American Management Association (AMA) (2003) *Email Rules, Policies And Practices Survey*. New York, US.

Anandarajan, M., Simmers, C. and Ibgaria, M. (2000) An Exploratory Investigation of the Antecedents and Impact of Internet Usage: An Individual Perspective. *Behaviour and Information Technology*, 19, 1, 69-85.

Anderson, S. (1999) Managing Agency Email Systems. *Rough Notes*, 142, 12, Indianapolis, Dec, 16-18.

Attaran, M. (2000) Managing Legal Liability of the Net: A Ten Step Guide for IT Managers. *Information Management and Computer Security*, 8, 2, 98-100.

Banerjee, D., Cronan, T.P. and Jones, T.W. (1998) Modeling IT Ethics: A Study in Situational Ethics, *MIS Quarterly*, Mar, 31-60.

Belanger, F. And Van Slyke, C. (2002) Abuse Or Learning? *Communications Of The ACM*, 45, 1, 64-65.

Benbasat, I., Goldstein, D.K. and Mead, M. (1987) The Case Research Strategy in Studies of Information Systems. *MIS Quarterly*, 368-385.

Benbunan-Fich, Raquel (2002) Information Technology In Organisations: Paradigms And Metaphors. *CIS Working Paper Series*, Zicklin School Of Business, Baruch College, City University Of New York. Http://Cisnet/Baruch.Cuny.Edu/Fich.

Cappel, J.J. (1995) A Study of Individuals' Ethical Beliefs and Perceptions of Email Privacy. *Journal of Business Ethics*, 14, 819-827.

Culnan, M.L. and Markus, L.M. (1987) Information Technologies. *In Handbook of Organisational Communication: An Interdisciplinary Perspective*, Jablin, F.M., Roberts, K.H., Putnam, L.L. and Lyman W.P (Eds.), Newbury Park, CA, Sage, 420-443.

De, R. and Mathew, B. (1999) Issues in the Management of Web Technologies: Conceptual Framework, International *Journal of Information Management*, 19, 427-447.

Dhillon, G. (1999) Managing and Controlling Computer Misuse, *Information Management and Computer Security*, 7, 4, 171-175.

Flood, L. (2003) Close Monitoring Provides Protection. *The Sunday Business Post*. Ireland, Feb 9.

Fulk, J. and Desanctis, G. (1995) Electronic Communication and Changing Organisational Forms. *Organisation Science*, 6, 6, Jul-Aug, 337-349.

Fulk, J., Schmitz, J. and Steinfield, C.W. (1990) A Social Influence Model of Technology Use. *In Organisations and Communication Technology* (Fulk, J. and Steinfield, C., Eds.), Sage, London, 117-140.

Galliers, R.D. (1992) Choosing information systems research approaches. In Galliers, R.D. (ed.) *Information Systems Research: Issues, Methods and Practical Guidelines*, Alfred Waller Ltd., Henley-on-Thames pp. 144-162.

Giddens, A. (1979) *Central Problems In Social Theory*. Berkeley, University Of California Press.

Gray and Grey (2002) Email And IM As Essential Platform Components in 2002. *Gartner Group*, 13th December, Note Number SPA-15-0931. Located At Http://www.gl.iit.edu/gartner2/research/103200/103210/103210.html.

Graff, J. (2002a) Management Update: How To Set Up An Email Retention Policy. Gartner Group, 10th April, Note Number IGG-04102002-02. Located At Http://www.Gl.Iit.Edu/Gartner2/Research/105800/105861/105861.Html

Graff, J. (2002b) Building Email: Economy, Resilience And Business Value. Gartner Group, 22nd March, Note Number LE-15-6155. Located At Http://www.Gl.Iit.Edu/Gartner2/Research/105300/105369/105369.Html

Graff, J. (2002c) Maximising Business Value Through Email. Gartner Group, 22nd March, Note Number AV-15-6154. Located At Http://www.Gl.Iit.Edu/Gartner2/Research/105300/105366/105366.Html

Graff, J. (2002d) Establishing And Reinforcing An Email Usage Policy. Gartner Group, 13th March, Note Number TU-15-8120. Located At Http://www.gl.iit.edu/gartner2/research/105000/105085/105085.html.

Graff, J. (2002e) Building A High Performance Email Environment. Gartner Group, 21st March, Note Number M-15-8182. Located At Http://www.gl.iit.edu/gartner2/research/105300/105322/105322.html.

Hancock, B. (1999) Security Views, *Computers and Security*, 18, 184-198.

Hodson, T.J., Englander, F. and Englander, V. (1999) Ethical, Legal and Economic Aspects of Monitoring of Employee Email, *Journal of Business Ethics*, 19, 99-108.

Hoffman, N. and Klepper, R. (2000) Assimilating New Technologies: The Role of Organisation Culture, *Information Systems Management*, Summer, 36-42.

Hoffman, M.W., Hartman, L.P. and Rowe, R. (2003) You've Got Mail and the Boss Knows: A Survey by the Center for Business Ethic, Email and Internet Monitoring. *Business and Society Review*, 108, 3, 285-307.

Jackson. T.W. and Burgess. E. (2005) Optimising The Email Communication Environment. *Proceedings of the International Resources and Management Association Conference*, Managing Modern Organisations With Information Technology, San Diego, May 14-18th, 819-820.

Jackson, T.W., Dawson, R. and Wilson, D. (2000) The Cost of Email Within Organisations, *Proceedings of the Information Resources Management Association Conference (IRMA'00)*, Anchorage, Alaska, May.

Kwong, T.C.H. and Lee, M.K.O. (2002) Behavioral Intention Model for the Exchange Mode Internet Music Piracy. Proceedings of the 35th Hawaii International Conference on Systems Sciences, IEEE Computer Society.

Lim, V.K.G., Thompson, S.H.T. And Geok L.L. (2002) How Do I Loaf Here? Let Me Count The Ways. *Communications Of The ACM*, 45, 1, 66-70.

Mantovani, G. (1994) Is Computer-Mediated Communication Intrinsically Apt to Enhance Democracy in Organisations? *Human Relations*, 47, 1, 45-62.

McFarlan, F.W. and McKenney, J.L. (1982) The Information Archipelago: Gaps and Bridges. *Harvard Business Review*, 60, 5, Sept/Oct.

Markus, L.M. (1994) Finding A Happy Medium: Explaining the Negative Effects of Electronic Communication on Social Life at Work. *ACM Transactions on Information Systems*, 12, 2, Apr, 119-149.

Oliver, H. (2003) Email And Internet Monitoring In The Workplace: Information Privacy And Contracting Out. *The Industrial Law Jour*nal, 31, 4, Dec, 321-352.

Oravec, J.A (2002) Constructive Approaches To Internet Recreation In The Workplace. *Communications Of The ACM*, 45, 1, 60-63.

Orlikowski, W.J. (1991) Integrated Information Environment or Matrix of Control? The Contradictory Implications of Information Technology, *Accounting, Management and Information Technology*, 1, 1, 9-42.

Otley, D. T. and Berry, A. J. (1980) Control, Organisation and Accounting. *Accounting, Organisation and Sociology*. 5, 2, 231-244.

Panko, R.R. And Beh, H.G. (2002) Monitoring For Pornography And Sexual Harassment. *Communications Of The ACM*, 45, 1, 84-87.

Pennings, J.M. and Woiceshyn, J. (1987) A Typology of Organisational Control and its Metaphors, *In Research in Sociology of Organisations*, Greenwich, JAI Press, 73-104.

PriceWaterhouseCoopers (PWC) (2002) *Information Security Breaches Survey 2002*. Located at http://www.Pwc.Com.

Poole, M.S. & Desanctis, G. (1990) Understanding The Use Of Group Decision Support Systems: The Theory Of Adaptive Structuration. *In Organizations And Communication Technology*, Fulk, J. And Steinfeld, C. (Eds.), Sage.

Rice, R.E. (1990) Computer-Mediated Communication System Network Data. *International Journal of Man-Machine Studies*, 32, 627-647.

Rice, R.E. And Aydin, C. (1991) Attitudes Towards New Organisational Technology: Network Proximity As A Mechanism For Social Information Processing. *Administrative Science Quarterly*, 36, 219-244.

Rogers, E.M. (1986) *Communication Technology: The New Media in Society*. NY, Free Press.

Romm, C.T., Pliskin, N. and Rifkin, W.D. (1996) Diffusion of Email: An Organisational Learning Perspective. *Information and Management*, 31, 37-46.

Rudy, I.A. (1996) A Critical Review of Research on Email. *European Journal of Information Systems*, 4, 4, 198-213.

Ruggeri, G. Stevens and McElhill, J. (2000) A Qualitative Study and Model of the Use of E-Mail in Organisations, *Internet Research: Electronic Networking Applications and Policy*, 10, 4, 271-283.

Schulman, A. (2001) The Extent of Systematic Monitoring of Employee E-Mail and Internet Use. Located at http://www.privcyfoundation.org/workplace/technology

Siau, K., Fui-Hoon Nah, F. And Teng, L. (2002) Acceptable Internet Use Policy. *Communications Of The ACM*, 45, 1, 75-79.

Simmers, C.A. (2002) Aligning Internet Usage With Business Priorities. *Communications Of The ACM*, 45, 1, 71-74.

Sipior, J.C. and Ward, B.T. (2002) A Strategic Response to the Broad Spectrum of Internet Abuse, *Information Systems Management*, Fall, 71-79.

Sproull, L. and Kiesler, S. (1991) *Connections: New Ways of Working in the Networked Organisation.* MIT Press, Cambridge, Massachusetts.

Stanton, J.M. And Stam, K.R. (2003) Information Technology, Privacy And Power Within Organisations: A View From Boundary Theory And Social Exchange Perspectives. *Surveillance & Society*, 1, 2, 152-190.

Urbaczewski, A. And Jessup, L.M. (2002) Does Electronic Monitoring Of Employee Internet Usage Work? *Communications Of The ACM*, 45, 1, 80-83.

Van Den Hooff, B. (1997) Incorporating Email: Adoption, Use and Effects of Email in Organisations. Universite IT van Amsterdam. ISBN 90-75727-72-0.

Weber, R. (2004) The Grim Reaper: The Curse Of Email. Editor's Comments, *MIS Quarterly*, . 28, No.3, Iii-Xiii, September.

Whitman, M.E., Townsend, A.M. and Aalberts, R.J. (1999) The Communications Decency Act: An Update for IS Management. *Information Systems Management*, Winter, 91-94.

Wolinsky, C. and Sylvester, J. (1992) Privacy in the Telecommunications Age. *Communications of the ACM*, 35, 2, 23-25.

Yin, R.K. (1994) Case Study Research, Design and Methods. Sage, London.

Table 1

The components of a strategy of email system electronic monitoring and control

Category of Email System Control	Components of a Strategy of Email System Electronic Monitoring and Control
Technical Email System Controls	1. Reconfigure the email system software
	2. Implement email system anti-virus software
	3. Implement email system scanning, filtering and blocking software
	4. Implement email system monitoring software
Formal Email System Controls	5. Formulate an email system policy
	6. Form an email system management team
	7. Audit email system accounts
	8. Create and maintain awareness and provide feedback on email system controls
	9. Discipline email system policy abuse
	10. Adopt email system pricing structures
	11. Establish methods of email system buffering
	12. Formulate an automatic email system disclaimer
Informal Email System Controls	13. Engage in email system training
	14. Create incentives to contribute to email management
	15. Enable email system social forums
Professional / Legislative Email System Controls	16. Incorporate professional and legislative email system controls

Table 2

The possible dysfunctional effects of the components of a strategy of email system electronic monitoring and control

Components of a Strategy of Email System Electronic Monitoring and Control		Possible Dysfunctional Effects
Technical	1. Reconfigure the email system software.	Organisations fail to adequately consider the configuration of the email application (Rudy, 1996).
	2. Implement email system anti-virus software.	Organisations fail to update anti-virus software (Lindquist, 2000).
	3. Implement email system scanning, filtering and blocking software	Organisations fail to use filtering software effectively (Jackson et al., 2000).
	4. Implement email system monitoring software.	Email monitoring can be contentious for economic, ethical, legal (Hodson et al., 1999) and health reasons (Clement and McDermott, 1991).
Formal	5. Formulate an email system policy.	Email policies can be poorly designed (Sproull and Kiesler, 1991).
	6. Form an email system management team.	Organisations fail to appoint an individual/committee to oversee email management (Sipior et al., 1996).
	7. Audit email system accounts.	Organisations fail to assess policy effectiveness and resolve problems (Flood, 2003).
	8. Create and maintain awareness and provide feedback on email system controls	Management fail to raise awareness against risks associated with inappropriate email activities (Sipior and Ward, 2002); fail to communicate the policy effectively (Whitman et al., 1999); and fail to continually raise awareness of the policy, particularly to new employees (Sipior and Ward, 2002).
	9. Discipline email system policy abuse.	Organisations fail to consistently and fairly enforce email policies (Flood, 2003).
	10. Adopt email system pricing structures.	Pricing structures penalise those with fewer resources to pay for communications or have more useful information to communicate (Sproull and Kiesler, 1991).
	11. Establish methods of email system buffering.	Buffering, by limiting interaction and information exchange to work-compatible colleagues/group members can re-establish hierarchical channels of communication by pre-defining who staff can communicate with, but separates staff from critical information or personnel (Sproull and Kiesler, 1991).
	12. Formulate an automatic email system disclaimer	May be insufficient protection for an organisation against a lawsuit if badly written (Graff, 2002d).
Informal	13. Engage in email system training.	Training is inadequate, voluntary or one-shot (Banerjee et al., 1998).
	14. Create incentives to contribute to email management	Employees should not be encouraged to seek rewards to comply with organisational policy as it effectively holds the organisation to ransom (Ruggeri et al. 2000).
	15. Enable email system social forums.	May lead to conflict where in self-policing behaviour, forum members point out inappropriate emails (Steinfield, 1990)
Professional / Legislative	16. Incorporate professional and legislative email system controls.	Government or Legislative authorities may fail to develop clear and concise directives for organisations to follow when formulating and implementing email policy or may be reactive rather than proactive in developing directives for controlling problems encountered with electronic communication technologies (Sipior and Ward, 1995; Chociey, 1997).

Table 3

The suitability of a case study for the requirements of the research

Research Requirements	Case Study Method
To address the lack of research into how to take an organisational view of email.	Enables exploration of an area in which few previous studies have been carried out (Benbasat et al., 1987), focusing on organisational rather than technical issues (Yin, 1994).
To establish how organisations control and monitor their email systems.	Enables the capture of reality in more significant detail, permitting analysis of more variables than possible with other research method (Galliers, 1992) .
To gain an understanding of the contextual environment in which the email system functions.	Provides a natural context within which a contemporary phenomenon is to be studied where the focus is on understanding the dynamics present (Benbasat et al., 1987).

Table 4

Organisational input into the study

	HealthCo	InsureCo	InvestCo	TeleCo
Industry	Manufacturing	Financial Services	Financial Services	Telecommunications
No. employees	1200	500	600	650
Year that email was installed	1995	1998	1998	1998
Managers and no. of interviews	HR (x5), IT(x5).	HR (x5), IT(x5).	HR (x5), IT(x5), Rep.	HR (x5), IT(x5).
No. of group interviews	5 (staff) x 3 (interviews)	5 (staff) x 3 (interviews)	5 (staff) x 3 (interviews)	5 (staff) x 3 (interviews)
Documentation	Email Policy, Logs, Notices, Handbook	Email Policy, Logs, Notices, Handbook	Email Policy, Logs, Notices, Handbook	Email Policy, Logs, Notices, Handbook
Research period	Jul02-Sept03	Feb02-Apr03	May02-Jul03	Apr02-Jun03

Table 5

Email controls prior, during and post email monitoring implementation

Controls	HealthCo	InsureCo	InvestCo	TeleCo
Pre-Implementation of email monitoring				
Technical	Installed email in 1995. Irregularly updated anti-virus software since 1996.	Installed email in 1998. Irregularly updated anti-virus software since 1998. Basic filtering/blocking software since 1998.	Installed email in 1998. Irregularly updated anti-virus software since 1998. Basic filtering/blocking software since 1998.	Installed email in 1998. Irregularly updated anti-virus software since 1998. Basic filtering/blocking software since 1998.
Formal	IT formally responsible for email. Email accounts only examined to eliminate viruses or technical errors. Staff email contacts buffered internally.	IT formally responsible for email. Basic informal local policy, but poorly communicated and poor availability. Email accounts audited if incidents reported by staff.	IT and HR formally responsible for email. Basic informal local policy, but poorly communicated and poor availability. Mailboxes only examined to eliminate viruses/technical errors.	IT and HR informally responsible for email. Basic informal local policy, but poorly communicated and poor availability. Mailboxes only examined for viruses/technical errors.
Informal	Basic email training on technical issues for all staff.	Technical email manual provided.		
Initial implementation of email monitoring (first month)				
Technical	Initial covert monitoring begins in July 2002 to generate metrics. New email application installed. Basic email filtering.	Initial covert monitoring begins in March 2002 to generate metrics.	Overt monitoring begins in May 2002.	Initial covert monitoring begins in April 2002 to generate metrics.
Formal	EMail Management Group (EMMG) assumes formal email management. Basic email policy created. Gradual implementation of monitoring and control chosen in order to set and visibly attain targets.	IT reluctantly continue email management.	Email management committee assume formal email management. Email policy updated. Policy published on intranet and in staff handbook. Presentation and copy of policy on email for all staff.	HR and IT continue informal email management. New email policy drafted from US policy.
Informal			Staff trained on email, filtering, anti-virus software & monitoring.	
Early implementation of email monitoring (2 - 7 months)				
Technical	New anti-virus software.	Receipt facility disabled except for urgent email.	IT support filtering, virus and mailbox management.	
Formal	Staff emailed about policy and monitoring. Email presentation for managers and supervisors.	Staff and managers emailed about policy and monitoring. Policy on intranet and in staff handbook.	Dedicated email address created for the email management committee so that staff can	Policy only available by emailing HR. Overview of policy on login screen.

	Policy only available by emailing HR. Staff emailed to compel relevant email subject headings. Staff formally reprimanded for email abuse. All staff reminded by email to read and adhere to policy.	Some staff warned by email about abuse. Staff emailed over email abuse and policy. Staff emailed to compel relevant subject headings. Some staff given verbal warning. Some staff receive second warning.	provide feedback or queries about email use and management. Staff sent monthly feedback on monitoring. Email policy sent to staff for suggestions.	
Informal			Supervisors urged to coach staff after minor policy infractions.	
Latter implementation of email monitoring (8-15 months)				
Technical	Automatic online anti-virus software updates. Extensively reconfigured filtering/blocking software. Many file attachments blacklisted. Web-based email accounts blocked except for contact with five nominated family/friends.	Filtering/blocking software upgraded for internal email. Failed attempt to technically configure time limits on unopened email. Automatic online anti-virus updates. Email reconfigured for receipt only and reduced storage for some staff. All Web-based email blocked.	Email system reconfigured to automatically purge deleted email. Filtering/blocking software upgraded to filter internal email and attachments. Automatic online anti-virus updates enabled. Attachments to/from web-based email accounts subject to permission.	Automatic online anti-virus software updates.
Formal	Email privileges revoked for gross violations of policy and backup failure. Staff emailed monthly with feedback to encourage policy compliance. Business contacts warned that non-business email would be reported. Staff must sign liability form to accept private attachments	Disciplinary report placed in some staff files but later rescinded.	Staff informed that attachments to/from web based email accounts would be subject to permission. Staff informed that attachments transmitted internally would be limited to a list of approved file types. Staff emailed monthly feedback and tips on improving mailbox management.	Staff member suspended for disclosing sensitive data by email. Extensive review of the audit trail generated by email monitoring undertaken. Automatic email policy reminder sent.
Informal	Staff contribute addresses to anti-SPAM catalogue. One day email course for managers and supervisors	Email security awareness course covering technical, content and legal issues for all staff . Supervisors instructed to coach staff individually.	Training programme devised for new members of staff. Supervisors asked to coach staff.	

Table 6

Initial problems exposed by email monitoring in each organisation

Organisation	% Non-Business Email	Initial Problems Exposed by Monitoring in each of the Organisations
HealthCo	40%	Substantial non-business use; group specific information emailed company-wide; excessive email storage; volumes of undeleted email.
InsureCo	32%	Relatively high level of non-business email use; widespread forwarding internally; email unopened for excessive periods.
InvestCo	15%	Knee-jerk reaction to overt monitoring may have contributed to low levels of non-business email abuse.
TeleCo	28%	Reasonably high level of non-business email use; relative efficiency when managing email; satisfactory email-turnaround; attachments infrequent.

Table 7

Delegation of responsibility for email management in each company

	HealthCo	InsureCo	InvestCo	TeleCo
Legal input	No	No	Yes	No
User input	No	No	Yes	No
HR input	Yes	Yes	Yes	Yes
IT input	Yes	Yes	Yes	No
Other managers	Yes	No	No	No
Email management style	Formal	Formal	Formal	Informal

Table 8

The consideration of important elements of email policy by each company

	HealthCo	InsureCo	InvestCo	TeleCo
1. Ensure that policy is easy to read	Adequate	Adequate	Extensive	Not
2. Personally present the email policy to staff	Not	Not	Extensive	Not
3. State critical nature of email	Not	Not	Extensive	Extensive
4. Explain technical implications of email use	Poor	Poor	Adequate	Adequate
5. Explain legal implications of email use	Poor	Poor	Poor	Extensive
6. Explain ethical implications of email use	Poor	Poor	Poor	Extensive
7. Establish rules for sending/receiving email	Adequate	Poor	Poor	Poor
8. Establish rules for receiving/sending attachments	Extensive	Poor	Poor	Poor
9. Establish rules for virus and security checks	Poor	Poor	Poor	Poor
10. Explain why email folders need to be managed	Not	Adequate	Adequate	Not
11. Explain why monitoring is necessary	Adequate	Poor	Not	Adequate
12. Explain how email is monitored	Adequate	Not	Not	Adequate
13. Explain why filtering is necessary	Adequate	Not	Poor	Adequate
14. Explain how email is filtered	Poor	Extensive	Poor	Poor
15. Define prohibited content and attachments	Adequate	Not	Not	Not
16. Define limitations on internal and external contacts	Extensive	Not	Not	Not
17. Define limitations on personal use of email	Poor	Adequate	Adequate	Poor
18. Establish privacy of personal use	Poor	Poor	Adequate	Poor
19. Describe disciplinary action for violating policy	Adequate	Not	Poor	Poor
20. Identify what training/support is available for staff	Not	Not	Extensive	Not
21. Obtain written/electronic confirmation of policy acceptance	Not	Not	Not	Poor
22. Schedule regular reviews of policy content	Not	Not	Not	Not

Legend: Not = Not Performed; Poor = Performed Poorly; Adequate = Performed Adequately; Extensive = Performed Extensively

Table 9

The delivery of important elements of email training/coaching in each company

	HealthCo	InsureCo	InvestCo	TeleCo
1. Explain how to send an email	Pre*	Latter	Initial	Never
2. Explain how to send and receive and attachment	Pre*	Latter	Initial	Never
3. Explain how to archive, backup, delete and empty folders	Never	Never	Initial	Never
4. Explain emails impact on the corporate network	Never	Latter	Initial	Never
5. Describe how to deal with SPAM/unsolicited/unwanted email	Pre*	Latter	Initial	Never
6. Explain how to check for and remove viruses or suspicious files	Pre*	Latter	Initial	Never
7. Explain how to setup and use internal distribution lists	Never	Never	Never	Never
8. Explain how to deal with inappropriate email	Never	Never	Never	Never
9. Explain how to establish personal filtering rules	Pre*	Never	Initial	Never
10. Discuss the critical nature of email as a business tool	Never	Never	Initial	Never
11. Discuss the current email practices of staff in the organisation	Latter**	Latter	Never	Never
12. Discuss the legal and ethical implications of email abuse	Latter**	Latter	Initial	Never
13. Describe what communications are unsuitable for email	Never	Never	Never	Never
14. Discuss the organisations efforts to filter and monitor email	Latter**	Latter	Never	Never
15. Discuss prohibited email addresses and content	Latter**	Latter	Initial	Never
16. Discuss how staff report violations of email policy	Latter**	Never	Never	Never
17. Request staff to encourage more appropriate email use by colleagues	Latter**	Never	Never	Never
18. Discuss disciplinary action for violations of email policy	Latter**	Latter	Initial	Never
19. Obtain feedback on further training requirements	Never	Never	Latter	Never

*Legend: Never = Never Implemented; Pre = Pre-implementation of email monitoring; Initial = initial implementation-1st month; Early = early implementation-1-6 months; Latter = latter implementation-7-15 months; *All Staff; **Supervisors & Managers Only*

Table 10

Creating awareness of email policy in each company

	HealthCo	InsureCo	InvestCo	TeleCo
Policy on the intranet	No	Yes	Yes	No
Policy emailed to staff	Yes	Yes	Yes	No
Copies of policy distributed	No	No	Yes	No
Policy in the handbook	No	Yes	Yes	No
Policy on log-in screen	No	No	No	Yes
Presentations on email use	Managers and Supervisors only	No	Yes	No

Table 11

Key factors of an effective strategy of email system electronic monitoring and control

Technical	• implement and regularly update email management software
Formal	• form a cross-functional email system management team • formulate a detailed and legally sound email policy • create and maintain ongoing awareness of email policy • engage in a process of hybrid feedback and control based email monitoring • firmly enforce discipline in accordance with the email policy • conduct regular reviews and updates of the email management programme
Informal	• engage in structured email system training