Monitoring and Controlling E-Mail Systems:
A Cross Case Analysis

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 organizational use. Research on e-mail systems is often dated and based on quantitative methodologies that cannot explain the interaction between various controls in organizational settings. Updating our understanding of the organizational aspects of e-mail systems utilizing qualitative methods is necessary. This paper 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 the effectiveness of e-mail committees, training, policies, and sustained awareness when combined with e-mail monitoring, and concludes by identifying key formal, informal, and technical controls.

Keywords: case study; electronic mail; formal, informal, and technical controls; information systems abuse; monitoring and control; negative effects

INTRODUCTION

Electronic commerce applications place additional security risks on organizations because of their extensive electronic interaction with other entities (De & Mathew, 1999). As organizations struggle to derive value from information technologies (Agarwal, 2001), particularly in periods of reduced IT budgets (PWC, 2002), organizations waste money buying technology, if they don't

create the human infrastructure, policies, and procedures to curb abuses (Hancock, 1999). In particular, increasing reports of e-mail systems abuse and the proliferation of e-mail-born viruses (Attaran, 2000; PWC, 2002) are of concern.

E-mail systems traditionally have 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 et al., 2000). The strategic importance of e-mail systems increases as they evolve (Van den Hooff, 1997), but the benefits of e-mail do not accrue automatically (Ruggeri et al., 2000). It is imperative that organizations formulate a coordinated and comprehensive response to e-mail system management (Sipior & Ward, 2002). In particular, organizations should anticipate the potentially harmful effects of e-mail systems and seek to prevent them from occurring (Van den Hooff, 1997). However, organizations lack analytical tools to examine their existing practices and to assist in reasserting e-mail systems for corporate rather than for individual purposes (Ruggeri et al., 2000).

The appropriate design, management, and application of any communication system depends to a great extent upon appropriate ongoing research of those systems from technical, organizational and social perspectives (Rice, 1990). Although the unsatisfactory understanding of the impacts of communication media provided by quantitative research has long been recognized (Rogers, 1986), the majority of the research produced over the past two decades on e-mail systems research utilizes quantitative methods to examine the social and technical concerns of e-mail systems. The need for organizationally based research has been highlighted by researchers such as Fulk and Desanctis (1995) and Rudy (1996) in calling for situational studies that recount varying organizational environments in which electronic communications systems are used. Nevertheless, laboratory-like experiments (Cappel, 1995; Culnan & Markus, 1987; Fulk et al., 1990; Mantovani, 1994) and mass surveys (AMA, 2000; Hoffman et al., 2003; Schulman, 2001) dominate the literature on e-mail studies. As a result, there has been relatively little published advice on how to take an organizational view of e-mail systems (Ruggeri et al., 2000).

This paper presents the results of multiple case studies that investigate how organizations monitor and control their e-mail 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 for effectively monitoring and controlling e-mail use.

THEORETICAL GROUNDING

Research (Ruggeri et al., 2000) has shown that many organizations fail to consider the full implications of implementing e-mail systems and often leave employees to establish the system's purpose and use. Indeed, the motivating factors for implementing e-mail systems rarely are communicated; thus, it is difficult to expect employees to use e-mail effectively.

Consequently, the initial technical success of e-mail system implementation does not guarantee long-term usefulness or political harmony and can culminate in devastating side effects during the latter stages of implementation (Romm et al., 1996). Such results are not confined to e-mail systems. Rogers' (1986) work on communications technology concluded that those who introduce communication technologies must see beyond the desirable, direct, and anticipated impacts, and realize that more of the indirect, undesirable, and unanticipated impacts of communication technologies occur as time elapses It has been proposed that the effects of computer-mediated communication can be categorized from a two-level perspective, as technology can have both first-level and second-level effects (Sproull & Kiesler, 1991).

Researchers have identified the first level negative effects of e-mail systems as productivity drain (Anderson, 1999), security breaches, urgent communications overlooked, excessive non-business communication (Sipior & Ward, 2002), increasing cost of use, information overload, and redundancy (Sproull & Kiesler, 1991). Researchers have identified the second level negative effects of e-mail systems as depersonalization; disinhibition (Markus, 1994); profanities, bad news, negative sentiment, and illicit use (Hodson et al., 1999); gender imbalance; deindividuation; electronic protestation and revolt (Sproull & Kiesler, 1991); and gaining leverage (Rudy, 1996).

The negative effects of information systems challenge managers to formulate policies and procedures that control but do not discourage e-mail usage (Anadarajan et al., 2000). An effective program of monitoring and control is a commonly identified success factor in assimilating new technologies (Hoffman & Klepper, 2000). Control can be defined as the use of interventions by a controller to promote a preferred behavior of a system being controlled (Aken, 1978). 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 & Berry, 1980).

Evidence suggests that e-mail monitoring is becoming more widespread because of its ability to capture communication metrics and detect non-business use (Sipior & Ward, 2002) and as a security tool (PWC, 2002). However, e-mail monitoring is contentious (Sipior & Ward, 2002). Sipior and Ward (2002) conclude 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.

Thus, the key to an effective control environment is to implement an adequate set of controls, as individual controls can have dysfunctional effects, if isolated solutions are provided for specific problems

Table 1. The practical measures involved in e-mail system monitoring and control and their possible dysfunctional effects

E-Mail System Monitoring and Control		Possible Dysfunctional Effects of E-Mail System Monitoring and Control
Technical	Reconfiguring e-mail system software	Organizations fail to adequately consider the configuration of the e-mail application (Rudy, 1996).
	Implementing e-mail system anti-virus software	Organizations fail to update anti-virus software (Lindquist, 2000).
	Implementing e-mail system filtering software	Organizations fail to use filtering software effectively (Jackson et al., 2000).
	Implementing e-mail system monitoring software	E-mail monitoring can be contentious for economic, ethical, legal (Hodson et al., 1999) and health reasons (Clement & McDermott, 1991).
Formal	Formulating e-mail system policy	E-mail policies can be poorly designed (Sproull & Kiesler, 1991).
	Forming an e-mail system management team	Organizations fail to appoint an individual or committee to oversee e-mail system management (Sipior et al., 1996).
	Communicating e-mail policy	Management fails to communicate the policy effectively (Whitman et al., 1999).
	Auditing e-mail system accounts	Organizations fail to assess policy effectiveness and resolve problems (Flood, 2003).
	Disciplining e-mail system abuse	Organizations fail to consistently and fairly enforce e-mail policies (Flood, 2003).
	Adopting e-mail system pricing structures	Pricing structures penalize those with fewer resources to pay for communications or have more useful information to communicate (Sproull & Kiesler, 1991).
	Establishing methods of e-mail buffering	Buffering, by limiting interaction and information exchange to work-compatible colleagues/group members, can re-establish hierarchical channels of communication by predefining with whom staff can communicate but separates staff from job-critical information or personnel (Sproull & Kiesler, 1991).
Informal	Engaging in e-mail system training.	Training is inadequate, voluntary, or one-shot (Banerjee et al., 1998).
	Maintaining awareness of e-mail system policy	Organizations fail to continually raise awareness of the policy, particularly to new employees (Sipior & Ward, 2002).
	Enabling self-policing of e-mail system through social forums	Self-policing of e-mail by social forums leads to conflict among staff (Sproull & Kiesler, 1991).

(Dhillon, 1999). Some classifications of control exist and are used here, even though the distinction between categories is open to debate. Formal controls (Dhillon, 1999) or control through social structure (Pennings & 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 & Woiceshyn, 1987) consist of increased awareness supplemented with ongoing education and training so that the shared norms and values of workers shape behavior, order perception, and influence attitudes. With technical control, the role of management changes from direct supervision to enforcing the operation of the technical system (Dhillon, 1999). Applying the classification of technical, formal, and informal controls identified by Dhillon (1999) to e-mail systems monitoring and control, Table 1 summarizes the conclusions from a number of studies to identify dysfunctional effects associated with certain practices.

It is evident that a clear vision of controls should be developed, since implementing patches in an illogical and incoherent manner, particularly when something goes wrong, may further compromise an organization. Nevertheless, researchers, such as Ruggeri, et al. (2000), report that there is little support or insight to assist organizations in reasserting e-mail systems for business use. Indeed, Rudy (1996) reported that the continued experience of the negative effect of e-mail systems may imply that not enough research

Table 2. 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 organizational view of e-mail	Enables exploration of an area in which few previous studies have been carried out (Benbasat et al., 1987), focusing on organizational rather than technical issues (Yin, 1994).
To establish how organizations control and monitor their e-mail systems	Enables the capture of reality in more significant detail, permitting analysis of more variables than possible with other research methods (Galliers, 1992).
To gain an understanding of the contextual environment in which the e-mail 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 3. Organizational input into the study

	Company A	Company B	Company C	Company D
Industry	Manufacturing	Financial Services	Financial Services	Telecommunications
No. of employees	1200	500	600	650
Year that e-mail 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	E-mail policy, logs, notices, handbook	E-mail policy, logs, notices, handbook	E-mail policy, logs, notices, handbook	E-mail policy, logs, notices, handbook
Research period	Jul02-Sept03	Feb02-Apr03	May02-Jul03	Apr02-Jun03

has been done in this area. Despite this, few studies of e-mail systems have been conducted in recent years.

METHOD

This study aims to provide an organizational analysis of the monitoring and control of e-mail systems. The case study method is considered suitable, as it is a rich source of data; and analytic generalization 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 2. Four organizations (see Table 3) were deemed suitable for participation in this study, based on the following criteria:

- The organization agrees to participate fully in the study;
- The organization has a large community of e-mail users;
- The e-mail system is installed for a long period of time;
- The organization considers the e-mail system to be a vital component of their electronic business infrastructure; and
- The organization is taking measures to exert control over its e-mail 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, and so forth, rather than just individuals' self-reports, as gathered in personal interviews and

by questionnaires; and
- Utilize 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 organization took place over a 15-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 organization. Such interviews took place with the human resources (HR) and information technology (IT) managers in each organization, as existing studies indicate that such managers play an integral role in managing organizational e-mail systems. Semi-structured focus group interviews with other staff were conducted in order to triangulate findings. Documents analyzed included e-mail policies, manuals, documentation, and e-mail notifications about e-mail use from each organization. Finally, 15 months of e-mail monitoring data gathered from each organization were gathered and analyzed. These data flows provide opportunities to understand the application, management, and consequences of e-mail systems. The data gathered were analyzed through time frames denoted by pre, initial, early, and later implementation of e-mail monitoring similar to those utilized by Rice (1990).

RESULTS

All four companies exercised little control over e-mail system usage in the early stages of diffusion, allowing staff unrestricted e-mail communication. This approach to e-mail management changed dramatically after the introduction of e-mail monitoring software in each company in 2002. Table 4 describes the technical, formal, and informal controls adopted by each organization in pre-implementation and during the initial, early, and later stages of e-mail monitoring implementation. Table 4 also illustrates that there are a number of differences in how each of these organizations monitor and control their e-mail systems. All four IT managers were concerned that there was a problem with e-mail usage. Prior to implementing e-mail monitoring, they had no way of achieving an organizational perspective of e-mail use. Company A decided to implement monitoring in order to establish greater transparency and visibility of e-mail usage, to ensure that it wasn't negatively affecting business transactions, and to smoothly move to future communication tools. Company B's and Company D's primary objectives were to improve the management and efficiency of e-mail and to control personal use. Company C was directed by corporate headquarters to monitor e-mail after productivity concerns related to personal use arose in another division.

Technical controls formed the thrust of all four organizations' efforts to monitor and control e-mail usage prior to the implementation of e-mail monitoring software in 2002. Yet these technical controls

Table 4. E-mail controls prior, during and post e-mail monitoring implementation

Controls	Company A	Company B	Company C	Company D
Pre-Implementation of E-Mail Monitoring				
Technical	Installed e-mail in 1995. Irregularly updated anti-virus software since 1996.	Installed e-mail in 1998. Irregularly updated anti-virus software since 1998. Basic filtering since 1998.	Installed e-mail in 1998. Irregularly updated anti-virus software since 1998. Basic filtering since 1998.	Installed e-mail in 1998. Irregularly updated anti-virus software since 1998. Basic filtering since 1998.
Formal	IT formally responsible for e-mail. E-mail accounts only examined to eliminate viruses or technical errors. Staff e-mail contacts buffered internally.	IT formally responsible for e-mail. Basic informal local policy, but poorly communicated and poor availability. E-mail accounts audited if incidents reported by staff.	IT and HR formally responsible for e-mail. Basic informal local policy, but poorly communicated and poor availability. Mailboxes only examined to eliminate viruses/technical errors.	IT and HR informally responsible for e-mail. Basic informal local policy, but poorly communicated and poor availability. Mailboxes only examined for viruses/technical errors.
Informal	Basic e-mail training on technical issues for all staff.	Technical e-mail manual provided.		
Initial Implementation of E-Mail Monitoring (First Month)				
Technical	Initial covert monitoring begins in July 2002 to generate metrics. New e-mail application installed. Basic e-mail 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	E-mail Management Group (EMMG) assumes formal e-mail management. Basic e-mail policy created. Gradual implementation of monitoring and control chosen in order to set and visibly attain targets.	IT reluctantly continued e-mail management.	E-mail management committee assumed formal e-mail management. E-mail policy updated. Policy published on intranet and in staff handbook. Presentation and copy of policy on e-mail for all staff.	HR and IT continue informal e-mail management. New e-mail policy drafted from US policy.
Informal			Staff given training on e-mail, filtering, anti-virus software, and monitoring.	
Early Implementation of E-Mail Monitoring (2-7 Months)				
Technical	New anti-virus software	Receipt facility disabled except for urgent e-mail.	IT support filtering, virus, and mailbox management.	
Formal	Staff e-mailed about policy and monitoring. E-mail presentation for managers and supervisors. Policy only available by e-mailing HR. Staff formally reprimanded for e-mail abuse.	Staff and managers e-mailed about policy and monitoring. Policy on intranet and in staff handbook. Some staff warned by e-mail about abuse. Some staff given verbal warning.	Dedicated e-mail address created for the e-mail management committee so that staff can provide feedback or queries about e-mail use and management.	Policy only available by e-mailing HR. Overview of policy on login screen.
Informal	Staff e-mailed to compel relevant e-mail subject headings. All staff reminded by e-mail to read and adhere to policy.	Staff e-mailed to compel relevant subject headings. Staff e-mailed regarding e-mail abuse and policy. Some staff receive second warning about abuse.	Staff sent monthly feedback on monitoring. Supervisors asked to coach some staff after minor policy infractions. E-mail policy sent to staff for suggestions.	

Table 4 cont. on next page

were poorly implemented with redundant anti-virus software and ineffective filtering rules. Furthermore, the IT department dominated systems implementation and management, relying on technically focused training and/or technically written user manuals. E-mail policies, where they did exist, were poorly written and inadequately communicated. E-mail accounts were not audited, as it was considered too

Table 4. E-mail controls prior, during and post e-mail monitoring implementation (cont.)

Controls	Company A	Company B	Company C	Company D
Latter Implementation of E-Mail Monitoring (8-15 Months)				
Technical	Automatic online anti-virus software updates. Extensively reconfigured filtering software. Many file attachments blacklisted. Web-based e-mail accounts blocked except for contact with five nominated family/friends.	Filtering software upgraded for internal e-mail. Failed attempt to technically configure time limits on unopened e-mail. Automatic online anti-virus updates enabled. Reconfigured e-mail to receive only and reduced storage for some staff. Web-based e-mail blocked.	E-mail system reconfigured to automatically empty deleted e-mail. Filtering software upgraded to filter internal e-mail and attachments. Automatic online anti-virus updates enabled. Attachments to/from Web-based e-mail accounts subject to permission.	Automatic online anti-virus software updates.
Formal	E-mail privileges revoked for gross violations of policy and backup failure. Business contacts warned that non-business e-mail 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 e-mail accounts would be subject to permission. Staff informed that attachments transmitted internally would be limited to a list of approved file types.	Staff member suspended for disclosing sensitive data by e-mail. Extensive review of the audit trail generated by e-mail monitoring undertaken.
Informal	Staff e-mailed monthly with feedback to encourage policy compliance. Staff contributes addresses to anti-SPAM catalogue. One-day e-mail course for managers and supervisors	E-mail security awareness course covering technical, content, and legal issues for all staff . Supervisors instructed to coach staff individually.	Staff e-mailed monthly feedback and tips on improving mailbox management. Training program devised for new members of staff. Supervisors asked to coach staff.	Automatic e-mail policy reminder sent.

Table 5. Initial problems exposed by e-mail monitoring in each company

Company	Level of Non-Business E-Mail Transmitted	Initial Problems Exposed by Monitoring in Each of the Companies
Company A	40%	Substantial non-business use; group-specific information e-mailed company-wide; excessive e-mail storage; volumes of undeleted e-mail.
Company B	32%	Relatively high level of non-business e-mail use; widespread forwarding internally; e-mail unopened for excessive periods.
Company C	15%	Knee-jerk reaction to overt monitoring may have contributed to low levels of non-business e-mail abuse.
Company D	28%	Reasonably high level of non-business e-mail use; relative efficiency when managing e-mail; satisfactory e-mail-turnaround; attachments infrequent.

time consuming. Accounts were accessed only to eliminate viruses or to rectify malfunctions. Initial monitoring revealed quite a number of problems with e-mail usage in each of these organizations, as outlined in Table 5. Interestingly, it took the implementation of another technical control (i.e., e-mail monitoring software) to inject some effort by each of the companies into developing formal e-mail system controls. It is also worth noting that, after the implementation of e-mail 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 study reveals four elements to be particularly important in monitoring and

Table 6. Delegation of responsibility for e-mail management in each company

	Company A	Company B	Company C	Company D
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
E-mail management style	Formal	Formal	Formal	Informal

controlling e-mail systems within the organizations studied. These elements are (1) forming an e-mail system management team, (2) formulating an e-mail policy, (3) engaging in e-mail system training, and (4) creating and maintaining awareness of e-mail policy.

Forming an E-Mail System Management Team

Previous research (Wolinsky & Sylvester, 1992) has suggested that organizations should establish a formal committee consisting of the IT manager, a company lawyer, an HR official, an executive management representative, a union representative, and a general power user to oversee e-mail management. Table 6 outlines the organizational members responsible for e-mail management in each of the four companies. Company A established the E-Mail Management Group (EMMG), consisting of the IT and HR managers, a business process improvement manager, and an operations manager. Interestingly, Company C was the only company to seek legal input and to allow an elected staff representative to join the e-mail management committee. Responsibility in Company B 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 e-mail 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. Company D failed to formalize responsibility for pursuing improvements in e-mail usage, and neither the HR manager nor the IT manager voluntarily accepted the task. Although processing and analysis of monitored data occurred monthly, neither manager reviewed the data effectively.

Engaging in E-Mail System Training

It has been proposed that organizations should have e-mail system training programs for new and existing employees, as these programs may reverse the trend in computer misuse (Banerjee et al., 1998). However, research (Attaran, 2000) has shown that organizations rarely train employees not to misuse e-mail systems. The majority of managers interviewed 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 e-mail more effectively. However, the majority of managers interviewed believed focusing primarily on technical issues when training staff to use e-mail is an oversight, and that an equal, if not greater, portion of training should focus on e-mail behavior and policy. Company C trained all staff when introducing the monitoring software, as the HR manager was confident that once staff knew the negative impacts of e-mail and how it could affect the company, better e-mail management would prevail. The IT manager believed that allowing the staff representative to deliver a large portion of the non-technical training greatly contributed to staff acceptance of e-mail policy, as training was delivered at their level of understanding by one of their colleagues, so staff was supportive of the process. Company B waited 14 months after implementing monitoring to conduct a security awareness course highlighting technical, content, and legal issues for all staff. While permanent staff at Company A had availed of initial technical training on e-mail, the withdrawal of e-mail privileges from summer interns, who had received no training whatsoever, revealed a glaring need for ongoing training. After 11 months of monitoring, Company A tried to redress training by holding a one-day course for managers and supervisors, but other staff members were overlooked yet again. However, this approach is questionable, as some researchers (Banerjee et al., 1998) argue that one-off training sessions may not be sufficient to combat e-mail system abuse.

With the general exception of staff from Company C, focus group participants were rather critical of the support 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 Company B to create a technical control to force time limits on unopened customers' e-mail inquiries for more efficient response times. Unable to reconfigure the e-mail software, staff supervisors were charged with providing staff with further instruction on reducing volumes of unopened e-mail and responding to e-mail more efficiently. At no point had Company D engaged in e-mail training, despite taking serious disciplinary action against one employee. Table 7 reveals the attitude of the study participants to elements of e-mail training identified as important by previous researchers. In particular, Table 7 highlights the time line for the delivery of these elements in each of the companies.

Formulating an E-Mail Policy

Research by Attaran (2000) has shown that organizations often lack clear policies to prevent the negative effects of e-mail. This view is confirmed by this study, as the policies analyzed were generally found to be poorly written and often confusing and contradictory. Although the e-mail policy of each company stated that e-mail should be allocated only if the user had an explicit business use for it, each organization provided universal access to the corporate e-mail system. Some researchers would argue that this may not be detrimental, as e-mail is an essential business tool (Anderson, 1999), and prohibiting access eliminates its benefits (Sproull & Kiesler, 1991). In such circum-

Table 7. The delivery of important elements of e-mail training/coaching in each company

	CompanyA	CompanyB	CompanyC	CompanyD
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 e-mail monitoring; Initial = initial implementation (1st month); Early = early implementation (1-6 months); Latter = latter implementation (7-15 months); *All Staff; **Supervisors & Managers Only*

stances, it has been argued that it is essential for organizations to establish a clearly defined e-mail policy (Whitman et al., 1999). However, only Company C and Company D clearly described and explained the value of e-mail as a critical business tool in user policies and literature. However, despite several managers being involved in drafting Company A's e-mail policy during the implementation of monitoring, their combined contributions amounted to copying and pasting paragraphs from the policies of other organizations. Company D's revised e-mail policy, drafted six weeks after implementing monitoring, was 15 pages in length, legalistic- and jargon-laden. The informal management of the e-mail system effectively led the HR manager to modify the e-mail policy of a corporate division based in the US to fit the Irish division rather than engaging in a discussion with other stakeholders. Company C's HR manager believed the implementation of monitoring forced a rethink about e-mail policy and its communication, as the HR and IT managers, the corporate legal department, and a staff representative were engaged to draft the new policy. Company B never updated its e-mail policy after implementing monitoring. Some authors (Wolinsky & Sylvester, 1992) suggest that employees should sign the e-mail policy to acknowledge an understanding of its contents and compliance, but none of the managers interviewed believed this was prudent, as failure to sign updates could be problematic. Recommendations that an e-mail policy should be reviewed and updated at least once a year are not uncommon (Flood, 2003). However, none of the organizations updated their policies since

implementing e-mail monitoring, despite making changes to e-mail management procedures on a number of occasions.

Zero tolerance of personal use of e-mail is unacceptable to staff in each organization, as many staff members depend on e-mail 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 Company A's e-mail policy, which explicitly prohibits personal use of e-mail, while the e-mail policies of Company B and Company D only permit personal use of e-mail outside of working hours. Company C'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 Company A attempted to do so. However, Company A's HR manager warned that specific definitions leave you open to oversights and the possibility of definition expiry. Only Company A and Company D had clear references to e-mail monitoring. Company B's policy expresses the right to monitor all e-mail but specifically refers to MAILsweeper filtering software. Company B's E-Mail Procedures document states that internal e-mail shall not be subject to interception or inspection. Company C's policy does not mention monitoring but states that staff should have no reasonable expectation of privacy of communication. Many researchers recommend that organizations also should define how breaches of e-mail policy will be dealt with (Banerjee et al., 1998). Only Company A's and Company D's policies assert the right to take disciplinary action up to and including dismissal. However, Company D's policy cites heavily from several acts of US law that have no legal basis in Ireland. In addition, interviewees found such laws difficult to assimilate. Company B's e-mail policy does not mention disciplinary action. Although Company C's policy cautions that improper e-mail use is subject to disciplinary action, staff members are referred to a Corporate Code of Discipline that contains no reference to e-mail abuse. Table 8 reveals the attitude of the study participants to elements of an e-mail policy identified as important by previous researchers. Furthermore, Table 8 evaluates the inclusion of such elements in each company's policy.

Creating and Maintaining Awareness

It has been proposed that organizations must create awareness of e-mail policy by formally presenting it to all employees; by including it in the employee handbook, in memos, and at meetings; and by publishing it on the company intranet (Sipior & Ward, 2002). Nevertheless, creating and maintaining awareness of e-mail policy are weak in three of the companies. Table 9 shows that only Company C formally presented the e-mail policy to all staff, while Company A only presented the policy to managers and supervisors. The primary method for conveying e-mail policy appears to be by e-mail. This may not be sufficient or appropriate to achieve a change in users' attitudes toward e-mail systems usage. It has been proposed that the primary defense against inappropriate

Table 8. The consideration of important elements of e-mail policy by each company

	CompanyA	CompanyB	CompanyC	CompanyD
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. Creating awareness of e-mail policy in each company

	Company A	Company B	Company C	Company D
Policy on the intranet	No	Yes	Yes	No
Policy e-mailed to staff	Yes	Yes	Yes	No
Copies of policy distributed	No	No	Yes	No
Policy in the handbook	No	Yes	Yes	No
Policy on login screen	No	No	No	Yes
Presentations on e-mail use	Managers and Supervisors only	No	Yes	No

information systems activities is to increase the awareness and understanding of what the risks are and how they arise (Sipior & Ward, 2002). Consequently, overt communication methods, such as broadcasting the policy on the computer screen when accessing the e-mail system is advised (Sipior et al., 1996). Although Company D is the only company to place the e-mail policy on the e-mail system log on screen, it is the only way in which the company creates and maintains awareness of the e-mail policy, and it consists only of a rather brief synopsis of the policy. Rather than choose any form of personal communication, it is clearly evident from Table 9 that each organization depends on the e-mail system to convey reminders, updates, feedback, warnings, and user tips. However, interviewees in two companies revealed that notifications often were deleted or filed without being read.

CONCLUSION

This study aims to improve our understanding of the operation of e-mail

Table 10. Key factors for effective monitoring and controlling of e-mail use and management

Technical	• Management must ensure that anti-virus software is effective and regularly updated. • Management must ensure that effective filtering rules are developed and applied.
Formal	• Management must delegate responsibility for managing e-mail to a committee. The task is too great and too complex for one or two individuals. • Management must put a lot of time and effort into drafting and updating the e-mail policy. • Management must devote substantial time to creating awareness of the e-mail policy. • Management must explain to staff the critical nature of e-mail to the organization.
Informal	• Management must continuously maintain awareness of e-mail controls. E-mail notifications may not be sufficient. • Management must educate and train existing, new, and temporary staff about the technical, legal, ethical, and social aspects of e-mail.

monitoring and control methods in organizational contexts. The findings highlight the need to formulate a coordinated response consisting of technical, formal, and informal controls as part of an organizational approach to e-mail management. Based on the analysis of the study findings, Table 10 identifies the key technical, formal, and informal controls for monitoring and controlling e-mail 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 organizational context. Overall, the study has advanced our understanding of the application of e-mail monitoring and control methods in an organizational 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.

REFERENCES

Agarwal, R. (2001). Research in information systems: What we haven't learned. *MIS Quarterly*, *25*(4), 5-15.

Aken, J.E. (1978). On the control of complex industrial organisations. *Results of the National Automation Survey*, Washington, D.C.

Anandarajan, M., Simmers, C., & 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 e-mail systems. *Rough Notes*, *142*(12), 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., & Jones, T.W. (1998, March). Modeling IT ethics: A study in situational ethics, *MIS Quarterly*, (pp. 31-60).

Benbasat, I., Goldstein, D.K., & Mead, M. (1987). The case research strategy in studies of information systems. *MIS Quarterly*, (pp. 368-385).

Cappel, J.J. (1995). A study of individuals' ethical beliefs and perceptions of e-mail privacy. *Journal of Business Ethics*, *14*, 819-827.

Culnan, M.L. & Markus, L.M. (1987). Information technologies. In F.M. Jablin, K.H. Roberts, L.L. Putnam, & W.P. Lyman W.P (Eds.), *Handbook of organisational communication: An interdisciplinary perspective* (pp. 420-443). Newbury Park, CA: Sage.

De, R. & 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, February 9). Close monitoring provides protection. *The Sunday Business Post*.

Fulk, J. & Desanctis, G. (1995). Electronic communication and changing organisational forms. *Organisation Science*, *6*(6), 337-349.

Fulk, J., Schmitz, J., & Steinfield, C.W. (1990). A social influence model of technology use. In J. Fulk & C. Steinfield (Eds.), *Organisations and communication technology* (pp. 117-140). London: Sage.

Galliers, R.D. (1992). Choosing information systems research approaches. In R.D. Galliers (Ed.), *Information systems research: Issues, methods and practical guidelines* (pp. 144-162). Henley-on-Thames: Alfred Waller Ltd.

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

Hodson, T.J., Englander, F., & Englander, V. (1999). Ethical, legal and economic aspects of monitoring of employee e-mail. *Journal of Business Ethics*, *19*, 99-108.

Hoffman, M.W., Hartman, L.P., & Rowe, R. (2003). You've got mail and the boss knows: A survey by the center for business ethic, e-mail and Internet monitoring. *Business and Society Review*, *108*(3), 285-307.

Hoffman, N. & Klepper, R. (2000). Assimilating new technologies: The role of organisation culture, *Information Systems Management*, (pp. 36-42).

Jackson, T.W., Dawson, R., & Wilson, D. (2000). The cost of e-mail within organisations. In M. Khosrow-Pour (Ed.), *Proceedings of the Information Resources Management Association International Conference (IRMA'00)*, Anchorage, Alaska, May (pp. 1093-1094). Hershey, PA: Idea Group Publishing.

Mantovani, G. (1994). Is computer-mediated communication intrinsically apt to enhance democracy in organisations? *Human Relations*, *47*(1), 45-62.

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), 119-149.

McFarlan, F.W. & McKenney, J.L. (1982). The information archipelago: Gaps and bridges. *Harvard Business Review*, *60*(5).

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. & Berry, A.J. (1980). Control, organisation and accounting. *Accounting, Organisation and Sociology, 5*(2), 231-244.

Pennings, J.M. & Woiceshyn, J. (1987). A typology of organisational control and its metaphors. In *Research in sociology of organisations* (pp. 73-104). Greenwich: JAI Press.

PricewaterhouseCoopers (2002). *Information security breaches survey 2002*. Retrieved from *http://www.Pwc.Com*

Rice, R.E. (1990). Computer-mediated communication system network data. *International Journal of Man-Machine Studies, 32,* 627-647.

Rogers, E.M. (1986). *Communication technology: The new media in society*. New York: Free Press.

Romm, C.T., Pliskin, N., & Rifkin, W.D. (1996). Diffusion of e-mail: An organisational learning perspective. *Information and Management, 31,* 37-46.

Rudy, I.A. (1996). A critical review of research on e-mail. *European Journal of Information Systems, 4*(4), 198-213.

Ruggeri, G.S. & 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. Retrieved from *http://www.privcyfoundation.org/workplace/technology*

Sipior, J.C. & Ward, B.T. (2002, Fall). A strategic response to the broad spectrum of Internet abuse. *Information Systems Management,* (pp. 71-79).

Sproull, L. & Kiesler, S. (1991). *Connections: New ways of working in the networked organisation.* Cambridge, MA: MIT Press.

Van Den Hooff, B. (1997). *Incorporating e-mail: Adoption, use and effects of e-mail in organisations*. Universite IT van Amsterdam.

Whitman, M.E., Townsend, A.M., & Aalberts, R.J. (1999, Winter). The communications decency act: An update for IS management. *Information Systems Management,* (pp. 91-94).

Wolinsky, C. & Sylvester, J. (1992). Privacy in the telecommunications age. *Communications of the ACM, 35*(2), 23-25.

Workplace testing: Monitoring and surveillance. (2000). New York: American Management Association (AMA).

Yin, R.K. (1994). Case study research, design and methods. London: Sage.

ACKNOWLEDGMENTS

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 also would like to thank the organizations and individuals who participated in this study for their generous cooperation and contribution.

Aidan Duane holds an MSc from University College Cork (UCC). At present he is following the PhD program at UCC at the Department of Accounting, Finance and Information Systems. He also currently lectures in information systems and electronic business at Waterford Institute of Technology (WIT), Ireland. His research interests include electronic business, electronic communication systems, electronic monitoring, and IS ethical issues.

Pat Finnegan holds a PhD from the University of Warwick and currently lectures in electronic business at University College Cork (UCC), Ireland. His research interests include electronic business, IS strategy, inter-organisational systems and data warehousing. His research has been published in leading IS journals and conferences.