Dissent, Protest and Transformative Action: An Exploratory Study of Staff Reactions to Electronic Monitoring and Control of Email Systems in one Company based in Ireland

Aidan Duane

Waterford Institute of Technology (WIT),

The Business School,

Cork Road, Waterford City, Ireland.

+353 51 302686

ADuane@wit.ie

Patrick Finnegan

University College Cork (UCC),

Department of Accounting, Finance & Information Systems,

Western Road, Cork City, Ireland.

+353 21 4903344

P.Finnegan@ucc.ie

ABSTRACT

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

Keywords: information technology; control; electronic mail; electronic monitoring.

INTRODUCTION

An email system introduces a new set of threats and legal issues to an organisation. Indeed, the dramatic increase in email usage is commensurate with the rising number of workplace incidents and disputes (Attaran, 2000; PWC, 2002; Weber 2004). PWC (2002) report that email security risks, such as email borne viruses, and the deliberate abuse of email have become major concerns for organisations. Some organisations limit abuse by electronically monitoring email activities, drafting email policies and prohibiting email systems use (Sipior and Ward, 2002). However, organisations can rarely dominate staff with the unilateral imposition of technology (Stanton and Stam, 2003). Although, Dhillon (1999) believes that technical controls are necessary, he questions their effectiveness if organisations fail to look at the contextual issues of information systems. Sipior and Ward (2002) argue that it is imperative that organisations formulate a coordinated and comprehensive response to

email system management. Stanton and Stam (2003) suggest that this should occur within the context of a negotiatory process involving management, employees and IT professionals.

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

This paper presents the results of a single case study investigation of an Irish-based organisation's strategy to monitor and control an email system. In Ireland, there is no specific legislation addressing email system monitoring and a person has no expressed right to privacy in the Constitution. Ireland's Electronic Commerce Act (2000) indicates that if employees clearly understand that email is a business tool and if the employer has established a clear policy that emails are subject to monitoring and it is conducted in a reasonable manner, it is difficult for employees to object. The next section examines the theoretical grounding for the study and is followed by a discussion of the research method and a presentation of the findings. The paper reveals a number of key concerns of staff which should be addressed by management or consultants advocating the implementation of email system monitoring and control in its pre, initial, early and latter stages of implementation.

THEORETICAL GROUNDING

Sipior and Ward (2002) propose a strategic response to information systems abuse, consisting of; 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, and keeping up-to-date with technological advances, legislative / regulatory initiatives and new areas of vulnerability. Dhillon (1999) argues that the key to an effective control environment is to implement an adequate set of technical, formal and informal controls. Technical control comprises of complex technological control solutions, often mechanistic in fashion. Formal control involves developing controls and rules that reflect the emergent structure and protect against claims of negligent duty and comply with the requirements of data protection legislation. Informal control consists of increasing awareness supplemented with ongoing education and training.

Electronic monitoring extends the scope of control, transforming personal control to systemic control and enabling control over behaviour as well as outcomes (Orlikowski, 1991). However, Dhillon (1999) questions the effectiveness of technical controls if organisations become over-reliant and don't consider the contextual issues of information systems. Furthermore, staff can act to change a control through dissent, protest, and potentially transformative action (Orlikowski, 1991). Failing to fairly apply discipline for email abuse can upset staff, while failing to properly train staff on email system use can lead to its misuse (Attaran, 2000). Furthermore, a poorly designed email policy reduces information exchange, while its poor communication diminishes staff understanding. Email monitoring may also conflict with staff privacy expectations (Sipior and Ward, 2002) and affect staff morale (Hodson et al., 1999). The main dysfunctional effects that can arise from electronic monitoring and control of email systems are outlined in table 1.

THE RESEARCH METHOD

The objective of this study is to '*investigate the reactions of staff to the implementation of electronic monitoring and control of an email system in a single organisation'*.

The choice of a single case study for this study was based on the arguments put forward by Steinfield (1990), Van den Hooff (1997) and Weber (2004). In particular, Steinfield (1990) suggests that 'case studies of what happens after new media are implemented can help to expand our awareness of the range of possible uses and effects, as well as arm future planners with a broader understanding of the ways in which people adapt technological systems for purposes beyond those envisioned by system designers'.

HealthCo Ireland (pseudonym) was chosen as a suitable case site after multiple site visits and negotiations. HealthCo is a large multinational involved in the manufacturing of well-known healthcare products. It has employees in over thirty countries and sells products in 120 countries. The company has 1,200 employees in Ireland making it one of its largest operations worldwide.

Miles and Huberman (1994) emphasise the importance of 'prestructured theory' when researching areas where some understanding has already been achieved but where more theory building is required before theory testing can be done. They propose that a loose-linkage between induction and deduction is suited for locally focused site sensitive studies. In adopting a loose-linkage inductive and deductive approach, this study utilizes prestructured theory in the form of the main dysfunctional effects that can arise from a strategy of electronic monitoring and control of email systems (see table 1) to scope of the research.

Data collection took place over a fifteen-month period from July 2002 to September 2003 using a combination of indepth interviews, focus groups, computer monitored data, and other documents. Data collection was structured using four time frames; (i) pre-implementation; (ii) initial implementation (iii) early implementation, and (iv) latter

implementation. Data collection was triangulated throughout the four time frames in order to attain an improved understanding of what was occurring in the organisation.

Semi-structured indepth interviews were used to gain an understanding of management's perceptions of how organisational strategies to control and monitor email use impacted on staff perception and use of email systems. The IT and HR managers were interviewed separately during the four key time frames, and once more upon exiting the organisation. Other managers (the financial controller, the manufacturing managers and the managing director) were also interviewed. Prior to each interview, the interviewee was sent a brief list of questions. Following each interview, the interviewee reviewed a transcript for verification and in some instances, provided additional information or clarification by phone.

Focus groups were conducted with ten interviewees at the initial, early and latter time frames of implementation. The focus groups were conducted after the management interviews had been conducted and the monitoring data had been gathered during each time frame. Focus group participants ranged in age from 27 to 49, and had between 2 to 7 years experience of working in HeathCo in various job functions.

Other documentation analysed included the email policy, corporate records, archival material, staff handbooks, codes of ethics, disciplinary codes, internal communications documentation, policies and other email systems management notifications.

FINDINGS

HealthCo implemented an email system in 1995 but exercised little control over email use at this stage. This approach changed dramatically when HealthCo began to implement numerous controls as a result email monitoring feedback. The IT Manager describes how the decision to monitor and control email was not so much driven by business factors, but because of his preference for 'greater transparency of how email is used'. The IT Manager describes his desire 'to put a bit of a squeeze on email, so that we are ready to move onto the

next communication tool whenever that may arrive'. Table 2 outlines the technical, formal and informal controls adopted during the initial, early and latter stages of implementing electronic monitoring and control of the email system, and also illustrates the reactions of staff to electronic monitoring and control of the email system.

Initial Implementation of Electronic Monitoring and Control of the EMail System

HealthCo implemented email monitoring software as a result of a decision taken by the EMail Management Group (EMMG), a group specially convened to oversee email monitoring and management. The EMMG initially implemented email monitoring in a covert fashion for a month in order to generate metrics. The IT Manager considered staff to be 'familiar with being monitored electronically' as HealthCo had monitored telephone calls since 1998 and Internet use since 2001. The HR Manager argued that 'as the first months statistics were just used as a benchmark, nobody suffered by not knowing'. Monitoring revealed substantial non-business email use, group-specific information emailed company-wide, excessive email storage, large volumes of undeleted email and disproportionate email volumes for some staff. There were no discussions with staff about the initial covert monitoring as the HR Manager was fearful staff would be suspicious.

Early Implementation of Electronic Monitoring and Control of the Email System

HealthCo chose a gradual implementation of email monitoring and control as 'trying to do too much too quickly would end in failure' according to the HR Manager. One month after implementing monitoring and control, HR/IT notified staff of monitoring and issued a new locally drafted email policy by email. The email policy stated that *"the email system is to be used for the business purposes of the company and not for the personal purposes of employees unless permission has been granted"*. None of the staff identified any concerns over the introduction of electronic monitoring. . An Electrical Engineer explained that 'some people were actually surprised that it wasn't done already because they monitor telephone

and Internet use. We haven't had any problems with those so nobody felt email would be any different'. However, the monitoring data from month 2 reveals that in reaction to the implementation of email monitoring and control, the number of non-business emails sent internally declined by 21% and by 24% externally.

As had occurred in month 1, the data for month 2 revealed that the top twenty highest users still accounted for a disproportionate number of emails. Despite a decline in volume by 27% from the baseline metrics, further analysis revealed that many of these emails were non-business related. In month 3, each of the top twenty users were personally admonished for 'misuse of the email system'. HealthCo had never disciplined staff for misuse of the telephone or the Internet, thus the disciplining of staff in month 3 for email misuse was a talking point. A Production Operative commented that 'it reverberated around the company pretty quickly that these guys had been reprimanded for breaching email policy. Everybody wanted to know what they had done wrong'. A Sales Representative contended that 'people were more concerned about the software now'. A Production Operative revealed that he 'didn't use email for anything other than work for several weeks' because he was 'afraid of being fired'. Staff limiting personal use of email in month 3 was very evident in the monitoring data as the total number of non-business email sent internally and externally declined by 30%. A Process Technician described how she 'deleted a lot of stored email because its content was not work related and could be considered a violation of the email policy'. This mass purging of stored email was quite evident in month 3 as the number of emails stored in users accounts fell by 26%.

After the formal reprimands, a number of staff members emailed the EMMG seeking clarification of the email policy. In response, the EMMG emailed all staff encouraging them to read and adhere to the policy while again explaining the need for monitoring. The email policy states that "*the company reserves and intends to exercise the right to review, audit,*

intercept and disclose all messages created, filed, received or sent over the email system without the permission of the employee". With regard to privacy, the policy contends that *"email communications should not be assumed to be private"* and *"all information and messages that are created, sent, received or stored on the company's email system are the sole property of the company"*. Although month 4 revealed a 3% increase from month 3 in non-business email sent internally and externally, the EMMG emailed staff to thank them for their efforts in improving email management while informing them that the top ten users with the lowest annual percentage non-business email would be taken to dinner.

Staff were reasonably familiar with the email policy having received a copy by email. A Process Technician suggested however that 'the email policy should outline what content and attachments are prohibited as this would increase compliance and eliminate any misunderstandings'. However, the HR Manager stated that 'if you start getting into specific definitions you leave yourself open to oversights and the possibility of definition expiry'. Nevertheless, after discussing requests from staff, the EMMG issued an email stating *"emails should not contain statements or content that are libelous, offensive, harassing, illegal, derogatory, or discriminatory while foul, inappropriate or offensive messages such as racial, sexual, or religious slurs or jokes are prohibited"* and prohibited use of the email system *"to solicit for commercial ventures, religious or political causes, outside organisations, or other non-job related solicitations including chain letters"*. Staff were satisfied with the clarification but it was never appended to the email policy.

The EMMG attributed the significant reductions in email use in month 4 to their tough approach to email misuse. The total number of non-business email sent and received internally/externally fell by 27%, the number of unopened email fell by 22%, the average age of unopened email fell by 35%, the number of non-business attachments sent internally had fallen by 22% and the number of deleted emails stored in users accounts fell by 35%. An

email was again sent to all staff in month 5 informing them that their efforts were appreciated but that these efforts had to be maintained indefinitely. However, in month 5, a rumour began to circulate amongst staff that if the subject heading was omitted from an email, the monitoring software would not detect if an email was business or non-business. Focus group participants admitted that none of them had ever intentionally omitted or falsified a subject heading from an email but acknowledged the practice amongst staff. The monitoring data supports this as a disproportionate number of emails began to surface with absent or falsified subject headings and the number of non-business attachments forwarded internally increased by 9% on month 4. The number of non-business email sent internally and externally, the average age of unopened email and the number of email stored in users accounts, also showed a slight relapse of 1-2% on the improvements made in month 4. The EMMG believed staff were intentionally trying to circumvent monitoring and in turn, emailed staff in month 6 insisting that all email have a relevant subject heading and that non-business email must be further reduced.

The EMMG believed that ‘festive factors’ played a significant part in higher email volumes in months 6 and 7 (December and January), as the number of non-business email sent externally rose by 19% above the baseline metrics in month 6. The total number of non-business email sent internally and externally also rose by 26% on month 5. Large volumes of email received during the festive period may have contributed to unopened email increasing by 5% above the baseline metrics. Little improvement occurred in month 7 with a 10% increase in non-business email sent externally compared to the baseline metrics and the total number of non-business email sent internally and externally still 22% higher than month 5. The number of non-business attachments sent internally also rose by 15% on month 5. The HR Manager commented that ‘we were riding the crest of a wave after our early success, but

you have to remember that email monitoring does not actually control how email is used, it just lets you see how your controls are working'.

Latter Implementation of Electronic Monitoring and Control of the EMail System

According to the IT Manager 'after email monitoring software was installed for a few months, we began to get a picture of how poorly the filtering software was working'. He revealed that 'although we found that a lot of these rogue attachments came from web-based email accounts, we also found that a sizeable proportion came from business addresses'. In month 8, the EMMG reconfigured the filtering software, extensively updating the keyword, phrase, the SPAM address library, and the blacklist of attachments. The EMMG emailed staff thanking them for their cooperation to date, but informing them that by the end of month 8, all communications with web-based email accounts would be blocked except for staff handling recruitment or public enquiries and that email filtering had been extensively reconfigured. The EMMG also requested staff to inform all of their business contacts that incoming emails containing questionable content or non-business related attachments would be blocked and reported to their systems administrator.

The decision to blacklist file attachments was not well received as staff felt that they had not being fully briefed. Staff were also incensed at the decision to block web-based email addresses, and were further annoyed when their email contacts immediately began to receive an automated response to some email communications stating *"this email address may not receive this attachment file type"*. The IT Manager explained that the attachment filter had been prematurely implemented but chose not to deactivate the filter despite the EMMG being inundated with complaints. An online poll to determine staff attitudes proved to be overwhelmingly against the changes. Subsequently, over three hundred staff members sent protest emails, resulting in four staff members meeting the EMMG to discuss a compromise. These negotiations led the EMMG to implement a probationary process in month 9 whereby

staff were allowed to designate five personal web-based email accounts with which to communicate under the guidance of the email policy. Staff were satisfied with the outcome. A Sales Representative explained ‘its nice to see management listen to reason. Nobody was out to flout the policy or to be confrontational for the sake of it. We just wanted a reasonable solution to the problem’. A Production Operative commented ‘they explained to us how these addresses were a problem for our email system because of junk mail and we accept that. However, we explained to them how these addresses were the only way that some of us could keep regular contact with our friends and family’. The impact of the reconfiguration of the filtering and blocking software was clearly evident in the monitoring data in month 9. The average number of email sent by the top 20 email users fell by 35%, the number of non-business email sent internally fell by 39%, the number of non-business attachments sent internally fell by 33%, the average age of unopened email fell by 65% and the number of deleted emails stored in users accounts fell by 46%. In addition the total number of non-business email sent internally and externally matched its highest point of a 30% reduction which had previously been achieved in month 3.

The monitoring data from month 10 was mixed as some measurements showed further or on a par improvements with month 9 while other metrics showed some deterioration. The number of non-business attachments sent externally increased by 6% on month 9 while the number sent internally decreased by a further 9%. Further investigation of attachments revealed alternative file types were being used to circumvent blacklists but only to external recipients. The greatest concern to the HR Manager was the nature of some attachments sent to client email addresses. At the end of month 10, twelve staff members had their email access revoked for what the IT Manager described as ‘gross violations of email policy’. The IT Manager believed these staff should have been fired as they ‘had already received verbal and written warnings’. The email policy states *“any employee who violates*

this policy or uses the email system for improper purposes shall be subject to discipline up to and including dismissal". Interestingly, the revoking of email access was received with an attitude of indifference by staff. A Sales Representative explained staff 'were aware of what they can and can't do with email, so if they have had their email facilities withdrawn, it must be for a good reason'.

In month 11, staff discovered that some staff could receive blacklisted attachments. The IT Manager reveals 'engineers are exempt from blacklisted attachments because of their jobs'. Other staff members are occasionally allowed to receive these files if IT are supplied with the attachment details and the nature of the contents of the attachment in advance. However, these emails are always opened and checked. A Sales Representative argued that if staff are given permission 'these files should not be opened…as it is an invasion of privacy'. Over one hundred and sixty staff emailed the EMMG to protest about 'double standards' and 'invasion of privacy'. The EMMG adopted a process in month 12 whereby permitted attachments were no longer opened if an electronic liability form was completed. The form required the individual to accept responsibility for any consequential effect the attachment may have on network or business transactions. However, staff would not accept responsibility for rogue attachments. A Process Technician revealed 'it's too risky given the kind of material that comes through our system'. Staff no longer contested their right to receive blacklisted attachments as this reinforced the EMMG's argument that greater control over attachments was needed. Only three staff ever completed the form.

From month 12 the EMMG emailed feedback on the monitoring process to staff at the end of every month and encouraged continued compliance with the email policy. However, in month 13, a failure to communicate the email policy to new staff culminated in what the IT Manager described as 'a systematic failure (in month 13) when a network backup failed. We had six interns (who had only been employed in month 12) with their drive full of Mpegs

(movie files)'. Staff believed this highlighted their earlier assertions that engineers were as likely to flout email policy. The IT Manager immediately shut the interns email accounts and one week later all six interns were released from their internship.

Revoking email privileges in month 10 significantly impacted the average number of non-business emails sent by the top twenty email users which fell by 41% from months 11 to 15. The IT Manager believes this demonstrates that enforcing discipline is essential to reducing non-business email use. Furthermore, two staff members rewarded for effective email management in month 14 had been among those initially reprimanded. In the fifteen months, the number of non-business email sent internally fell by 57% while the number of non-business email sent externally fell by 39%. The blocking of attachments had a significant impact on the number of non-business attachments sent internally and externally. Internal non-business attachments fell by 65% from month 10 to month 15 while non-business attachments sent externally fell by 20%.The HR Manager claimed 'this proves monitoring works'. However, one staff member revealed he now sent personal email by 'a web-based email account' and felt he hadn't reduced his non-business email communication dramatically. The IT Manager suggests 'it is only a small few staff and we will have that eradicated with WebSense very shortly'. Other significant improvements made in the fifteen months of monitoring included reducing the number of unopened email by 53%, the average age of unopened email by 76%, the number of deleted emails in users accounts by 69%, while the total number of non-business email sent was reduced by 49%.

Staff Overview of Electronic Monitoring and Control of the Email System

Staff believed that email monitoring acts as a control, diminishing the likelihood of email being used for non-productive behaviour. However, staff felt that the sudden shift in management attitude to their email use required greater explanation of the rules governing email use. An Electrical Engineer who had initially expressed little concern, reported that

‘email monitoring is quite different (from telephone and Internet monitoring) because the information communicated is often more personal and the method by which it is monitored and stored is more invasive’. For these reasons, the engineer admitted to curtailing email use for business and personal use and believes it now takes him longer to write an email.

Staff suggested that tighter control over email use and in particular email monitoring, had created an untrustworthy communication medium because their communications are open to greater scrutiny and staff still felt unsure about the rules of the game. A Manufacturing Engineer believed that email is of far greater value if ‘staff have confidence in using the system to voice their opinions, make decisions and group communicate over ideas’. A Sales Representative stated that ‘social communication via email is part of decision making and idea generation’. Other staff believe that email use had never negatively affected their productivity. A Process Technician argued that ‘email enables more rapid communication because you are more to the point unlike when you are on the phone, but you still need to create personal relationships with the people you communicate with through email’.

Staff are critical of management’s efforts to maintain awareness of the email policy, pointing out that the policy is only available by emailing the HR Manager. A Manufacturing Engineer highlighted that ‘new staff are never informed of the policy and the problems they create have a direct effect on all other staff’. A Sales Representative believes that ‘she shouldn’t be ‘subject to the same sanctions as those who don’t use the email responsibly’.

CONCLUSION

This exploratory study showed that staff can react in a number of negative ways to electronic monitoring and control of email systems. However, it is evident that staff mostly reacted negatively to poor implementation of controls rather than to the controls per se. the study revealedt that staff had six primary concerns which should be addressed by management and consultants advocating the implementation of email system monitoring and control:

(1) Staff felt that tighter control over email use had created an untrustworthy communication medium and that the social communication necessary for effective business relationships had been negatively affected.

(2) Staff felt isolated and under greater scrutiny since the introduction of electronic monitoring and control of the email system.

(3) Some staff felt they were punished for policy breaches committed by other staff.

(4) Staff believed that email monitoring was more invasive than other forms of monitoring. Although non-business email communication was reduced, staff carefully considered everything they wrote, taking longer to write business emails.

(5) Staff attempted to transform and/or circumvent controls if it was perceived to be poorly implemented and/or they felt they had not been adequately consulted or informed. Staff reacted by protesting via email, conducting online polls, removing or falsifying subject headings to circumvent monitoring or using web based email accounts to send non-business communications.

(6) Staff were unsure about the rules of the game in the early stages, possibly contributing to greater abuse of the email system. Staff believed that training is essential, and that email policy needs to be more highly visible.

REFERENCES

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.

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

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

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.

Jackson, T.W., Dawson, R. and Wilson, D. (2000). The Cost of Email Within Organisations. *Proceedings of the IRMA 2000*, Anchorage, Alaska, May.

Lindquist, C. (2000). You've Got Dirty Mail. *ComputerWorld*, 34, 11, 72-73.

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.

Miles, M.B., And Huberman, M.A. (1994). An Expanded Sourcebook Of Qualitative Data Analysis, Sage Publications, California.

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.

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

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 EMail in Organisations. *Internet Research, Special Issue on Electronic Networking Applications and Policy*, 10, 4, 271.

Sipior, J.C., Ward, B.T. and Rainone, S.M. (1996). The Ethical Dilemma of Employee Email Privacy in the US. *Proceedings of European Conference on Information Systems (ICIS)*.

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*. Cambridge, Massachusetts: MIT Press.

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.

Steinfield, C.W. (1990). Computer-Mediated Communications in the Organisation: Using Email at Xerox. In *Case Studies in Organisational Communication*, 282-294, Guilford Press.

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*, Vol. 28, No.3, iii-xiii, September.

Table 1 - *Electronic monitoring and control of an email system and possible dysfunctional effects*

Electronic monitoring and control of email		**Possible dysfunctional effects**
Technical Control	Reconfigure the email system software	Organisations fail to adequately consider the configuration of the email application (Rudy, 1996).
	Implementing email system anti-virus software	Organisations fail to update anti-virus software (Lindquist, 2000).
	Implement email system scanning, filtering and blocking software	Organisations fail to use filtering software effectively (Jackson et al., 2000).
	Implement email system monitoring software	Monitoring is contentious for economic, ethical, legal (Hodson et al., 1999) or health reasons (Markus, 1994); may conflict with staff privacy expectations (Sipior and Ward, 2002) and; may erode the bond of trust between employer and staff (Urbaczewski and Jessup, 2002)
Formal Control	Formulate an email system policy	Policies can be poorly designed (Sproull and Kiesler, 1991).
	Form an email system management team	Organisations fail to appoint an individual or committee to oversee email system management (Sipior et al., 1996).
	Communicate the email policy	Organisations fail to communicate the policy effectively (Sipior and Ward, 2002).
	Audit email system accounts	Organisations fail to assess policy effectiveness and resolve problems (Flood, 2003).
	Discipline staff for email system policy abuse and reward compliance	Organisations fail to consistently and fairly enforce email policies (Flood, 2003).
	Adopt email system pricing structures	Pricing penalises staff with less resources or with more to communicate (Sproull and Kiesler, 1991).
	Establish methods of email system buffering	Buffering separates staff from job critical information or personnel (Sproull and Kiesler, 1991).
Informal Control	Engage in email training	Failing to adequately train staff on email system use can lead to misuse of these systems (Attaran, 2000).
	Maintain awareness of email system policy	Organisations fail to continually raise awareness of the policy, particularly with new staff (Sipior and Ward, 2002).
	Enable self-policing of email system through social forums	Self-policing of email by social forums leads to conflict among staff (Steinfield, 1990).

Table 2 - *Electronic monitoring and control of the email system and staff reactions*

Category	Control Type	Staff Reactions
Initial implementation of electronic monitoring and control of the email system (July)		
Technical	Covert monitoring begins to generate metrics. Introduction of new email application and basic email filtering for SPAM. Staff requested to forward unsolicited emails to quarantine box.	Staff unaware of covert monitoring. Staff very supportive of SPAM filtering and actively engage in effort to reduce unsolicited email. Staff lack confidence in applying filtering rules.
Formal	An EMail Management Group (EMMG) is formally convened to oversee monitoring and email management. Staff are not formally informed of role. A basic email policy is created using policies from other organisations. No staff disciplined on the basis of covert monitoring data.	Staff suspicious of the EMMG and fear the establishment of a big-brother scenario in the long run.
Informal	Training was not considered necessary	Staff criticise lack of training on email and filtering software.
Early implementation of electronic monitoring and control of the email system (2-7 months - August to January)		
Technical	New anti-virus software implemented.	Despite receiving no training, staff are comfortable with using the anti-virus software.
Formal	A gradual implementation of electronic monitoring and control was chosen in order to set and visibly attain targets. Staff sent the email policy by email and informed about monitoring. Presentation on email policy and monitoring for managers and supervisors. Supervisors requested to enforce the email policy on their subordinates. Policy only available from HR and not included in handbook or on intranet. Some staff formally reprimanded for email abuse. After initial resistance, EMMG sent email to clarify prohibited email use. Email policy not updated to include the clarification.	Initially, staff made no complaints or queries and there were no signs of discontent or trepidation amongst staff. Staff surprised that email wasn't already monitored as telephone and Internet was already monitored. Staff became concerned when some staff were disciplined. Some staff severely curtailed their use of email out of fear. Staff familiar with email policy but email the EMMG seeking clarification of prohibited email use. Staff satisfied with clarification of prohibited email use.
Informal	Staff thanked by email for their efforts to improve email use. Staff emailed to compel relevant email subject headings. All staff reminded by email to read and adhere to policy.	Incentive created to reward staff for good mailbox management. Staff try to circumvent monitoring by omitting and falsifying subject headings for email.
Latter implementation of electronic monitoring and control of the email system (8-15 months - February to September)		
Technical	Filtering software reviewed and extensively reconfigured. Many file attachments blacklisted and communication with web based email addresses blocked. Staff informed by email that this would occur at the end of February to allow alternative arrangements to be made. However, filtering of attachments was inadvertently applied before end of February. After consultation, staff permitted to nominate five family/friends web based email addresses with which to communicate. Automatic online anti-virus software updates.	Staff pleased that filtering reduced their levels of SPAM and that they had been kept informed why certain material was being filtered. The blacklisting and filtering of certain file attachments was resented by staff and they felt they were poorly informed when filtering was applied before the end of February. Staff incensed at the decision to block all communication with web based email addresses. Three hundred members of staff emailed the EMMG to protest. Some staff conduct an online poll to gauge resistance to blacklisting of attachments and blocking of email addresses revealing widespread rejection. EMMG meet with a group of four staff to discuss a compromise. Staff satisfied with the outcome.
Formal	Staff informed that business contacts transmitting non-business related content and attachments would be reported to their systems administrator. Email privileges temporarily revoked from twelve staff members for gross violations of email policy. Staff presented with a liability form to accept the contents and any consequences of receiving private attachments. Summer interns are not informed about the email policy, even after been exposed by monitoring. Email privileges revoked for summer interns after network backup failure in second month of placement. Summer interns released from work placement one week later.	The revoking of staff privileges received with an attitude of indifference by staff, feeling staff should be aware of the email policy by now. Staff annoyed after discovering that some staff were exempt from ban on blacklisted file attachments and that IT open all attachments. Mixed reaction from those exempt and subject to the ban. One hundred and sixty staff emails the EMMG to protest at double standards and invasion of privacy. Some staff suggest a liability form to the EMMG to accept the contents of personal attachments. Poor take up of liability form as staff refuse to accept the consequences of rogue attachments. Summer interns misuse the email system in first month of work placement. Some staff find situation with interns amusing, because as engineers the system automatically exempted them from the ban on attachments.
Informal	Staff emailed monthly feedback to encourage continued policy compliance. One day course for managers and supervisors on email management. Staff still do not receive any formal training. Ten staff taken to dinner to reward them for good mailbox management.	Staff circumvent controls by using web based email accounts to send personal email.