IDEA GROUP PUBLISHING

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

ITP5227

This paper appears in *Managing Modern Organizations Through Information Technology*, Proceedings of the 2005 Information Resources Management Association International Conference, edited by Mehdi Khosrow-Pour.

Staff Reactions to the Implementation of Electronic Monitoring and Control of Email Systems: A Contemporary Case Study

Aidan Duane

Waterford Institue of Technology (WIT), School of Accountancy & Business Studies, Cork Rd., Waterford City, Ireland, aduane@wit.ie

Patrick Finnegan

University College Cork, Dept of Accounting, Finance & IS, College Rd., Cork City, Ireland, p.finnegan@ucc.ie

ABSTRACT

An email system is a critical business tool, and an essential part of organisational communication. However, many organisations have experienced negative impacts from email systems recently due to ad-hoc implementation, prolonged management neglect and user abuse. Organisations 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. The findings highlight the variations in staff reactions through multiple time frames and the different interpretations by management and staff of electronic monitoring and control of an email system. The paper concludes by identifying a number of key concerns of staff about electronic monitoring and control of an email system.

CONTROLLING EMAIL SYSTEM USAGE

Internet based electronic commerce applications pose greater risks to the organisation because of their direct electronic interaction with other entities (De and Mathew, 1999). In particular, an email system introduces a new set of threats and legal issues (Attaran, 2000). Email borne viruses and deliberate abuse of email have become major concerns (PriceWaterhouseCoopers, 2002). Organisations waste resources by not creating the human infrastructure, policies and procedures to curb systems abuses (Hancock, 1999). Some organisations adopt electronic monitoring of email and restrict its use, but this can erode the trust between employer and staff (Urbaczewski and Jessup, 2002).

Often, email systems have not had a rational implementation process (Van den Hooff, 1997). In the push to increase business use of email, many organisations failed to consider the implications of email implementation and often left staff to establish its purpose and use (Ruggeri, et al., 2000). Some organisations encouraged playful use of the email system without controlling activities, to facilitate learning (Belanger and Van Slyke, 2002). However, if the reasons for implementing email systems were never communicated, it is difficult to expect staff to use email effectively at a later stage (Ruggeri, et al., 2000). Thus, the initial technical success of email systems implementation can culminate in serious side-effects in later stages (Romm et al., 1996).

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 and 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 (Orlikowski, 1991), but Dhillon (1999) questions the effectiveness of technical controls if organisations become over-reliant and don't consider the contextual issues of information systems. Therefore, it is essential to identify an electronic monitoring scheme acceptable to staff which simultaneously enables managers to influence staff (Urbaczewski and Jessup, 2002). However, control systems can at best only proscribe, rather than fully prescribe, staff behaviour (Dermer and Lucas, 1986). 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 (Sipior and Ward, 2002). Email monitoring may also conflict with staff privacy expectations (Sipior and Ward, 2002) and affect staff morale (Hodson et al., 1999).

METHODOLOGY

Much of the published email systems research uses laboratory experiments or mass surveys. Quantitative research seldom provides a satisfactory understanding of the impacts of communication systems (Rogers, 1986), particularly when many studies portray electronic monitoring as a uniform practice with the same negative effects on staff (George, 1996). This qualitative study investigated the reactions of staff to the implementation of electronic monitoring and control of an email system in a single organisation. Communication research should obtain multiple measures from several independent sources and use objective data-sources including computer monitored data, records and archives, rather than just individuals' self-reports (Rogers, 1986). As shown in table 1, this study used personal and focus group interviews, observation, documentation and email monitoring data.

FINDINGS

HealthCo exercised little control over the email system in its early diffusion. This approach was dramatically changed in 2002 as HealthCo implemented numerous controls as a result email monitoring feedback. 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. Table 2 also illustrates the

Table 1. Organisation's Details and Research Input

Industry	Manufacturing (Health Care).
Email introduction	Since 1995.
Staff	1200 staff.
Management interviews	HR and IT Managers interviewed on five occasions.
Group interviewees	Five focus group participants interviewed on three occasions.
Documentation	Email policy, monitoring data, notifications and staff handbook.

reactions of staff throughout its implementation. The following sections discuss the findings in more detail.

Initial Implementation of Electronic Monitoring and Control of the EMail System

In July 2002, HealthCo implemented email monitoring software as a result of a decision taken by the EMail Management Group (EMMG). This group was convened to oversee email monitoring and management. The group initially implemented email monitoring in a covert fashion in order to generate metrics. The IT Manager considered staff to be 'familiar with being monitored electronically' as HealthCo had been monitoring 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. HealthCo did not support discussions with staff about the initial covert monitoring to ascertain their opinion.

Early Implementation of Electronic Monitoring and Control of the EMail System

One month after implementing monitoring and control, HR/IT issued a new locally drafted email policy, notifying staff of monitoring and prohibiting personal use of email. Initially, staff did not express any concerns over electronic monitoring and control of the email system. An Electrical Engineer believed staff 'were 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 revealed that staff immediately reduced the number of non-business emails they sent internally and externally. Furthermore, after twenty staff were reprimanded for misuse of email in September 2002, staff became increasingly concerned about monitoring. A Sales Representative contended that 'people were more concerned about monitoring now because staff had never been reprimanded for internet or telephone use'. In response to staff enquiries, the EMMG urged staff to read and adhere to the policy while again explaining the need for monitoring. Initially, the EMMG were reluctant to clarify what specifically constituted a breach of email policy. However after consulting staff, the EMMG released a list of infringements which while satisfying staff, they were never appended to the email policy. Staff were emailed in October 2002 informing them of improvements but that these efforts had to be maintained indefinitely. In November 2002 staff attempted to circumvent monitoring by omitting subject headings from emails. In response, the EMMG informed staff that email must have a relevant subject heading. The HR Manager attributed the significant reductions in non-business email in the first three months to a 'tough approach to email misuse'.

Latter Implementation of Electronic Monitoring and Control of the EMail System

Six months of monitoring revealed that the email filtering software was ineffective. In February 2003, the EMMG blocked communication with web-based email addresses for the majority of staff and requested staff to inform their business contacts that non-business emails would be reported to their systems administrator. Over three hundred staff emailed the EMMG to protest. After negotiations, HealthCo permitted staff to designate five personal web-based email accounts with which to communicate subject to email policy guidelines. Despite concessions problems continued, as in April 2003, twelve staff had their email privileges revoked for a month. The IT Manager believed these cases advocated dismissal in line with the email policy. On this occasion, the revoking of email privileges was received by an attitude of indifference by staff. A Sales Representative stated that 'people can't argue that they haven't had any warnings'.

Although HealthCo's ban on blacklisted attachments was accepted initially, staff were angered that the ban was not applied uniformly. According to the IT Manager, 'staff such as engineers are exempt from the ban because of their job requirements. Other staff can occasionally receive these attachments if the IT Department is notified. However, these are always opened and checked regardless of their nature'. Some staff were unaware this occurred. A Sales Representative argued that 'these attachments should not be opened as it's an invasion of privacy'. In May 2003, one hundred and sixty staff emailed the EMMG protesting about 'double standards' and 'invasion of privacy'. However, some staff supported the EMMG, as a Manufacturing Engineer exempt from the ban, argued that 'most staff have no business need for certain file types and shouldn't receive them as it consumes network resources. Engineers continuously seeking permission to receive technical drawings and multimedia files would be time consuming'. However, one Process Technician argued that 'there are double standards because it doesn't apply to everyone'. In a further concession, the EMMG introduced a process in June 2003 whereby permitted personal attachments would no longer be opened by the IT Department if staff completed an electronic liability form accepting responsibility for any consequential effect the attachments may have on the organisational network. However, staff were unwilling to sign these forms. A Process Technician revealed that 'it's too risky given the kind of material that comes through our system'. Staff no longer protested and only three ever signed the liability form.

LESSONS LEARNED

The HR Manager now believes that 'trying to solve all the problems with email instantly will not work. The way people use email is something they have learned over a number of years and you can't change it overnight'. It is important to remember that 'email, and how staff use it, becomes ingrained very quickly. Correcting that behaviour and making this modified behaviour the norm, is difficult both for management and staff". The HR Manager believed that failing to provide training was a significant oversight, as 'the technical side was easy for staff to understand whereas complying with the policy was more difficult'. Staff shared this sentiment and felt that the sudden shift in management attitude to their email use required far greater communication of the rules. A Sales Representative suggested that staff felt 'a bit isolated when monitoring was introduced because they 'were rather naïve about how it affected everyday communication'. An Electrical Engineer who had initially expressed little concern over monitoring because telephone/Internet use was already monitored, remarked that 'email monitoring is quite different because the information communicated is often more personal and the method by which information is monitored is more invasive'.

The HR Manager believes that by 'setting goals and working at improving mailbox management bit by bit, gradual progression toward proper mailbox management is more acceptable than an all sweeping clampdown'. However, staff reported that tighter control over email use and in particular email monitoring, has created an untrustworthy communication medium. A Manufacturing Engineer who has worked in HealthCo for seven years 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 ideas'. One Sales Representative stated that 'social communication via email is part of decision making and idea generation. We banter to open up to those in our groups, as getting to know more about them than just their job title makes you more willing to contribute without feeling exposed'.

Staff in HealthCo are critical of management's efforts to maintain awareness of the policy. A Manufacturing Engineer commented that

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 (July 2002)		
Technical	Covert monitoring begins in July to generate metrics. Introduction of new email application and basic email filtering. 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 convened to oversee monitoring and email management. Staff are informed of monitoring by email. A basic email policy is created using policies from other organisations. Staff are not disciplined based on 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 (August 2002 to January 2003)		
Technical	Anti-virus software upgraded.	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 like telephone and Internet use. Staff became concerned when some staff were disciplined for email abuse. 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 (February to September 2003)		
Technical	Filtering software extensively reconfigured. Many 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 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 for gross violations of email policy. Staff presented with a liability form to accept the contents and any consequences of receiving private attachments. Interns are not informed of the email policy, even after been exposed by monitoring. Email privileges revoked for interns after network backup failure in second month of placement. Interns released 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 email 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. 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 email management course for managers and supervisors. No formal training for staff. Ten staff rewarded for good email management.	Staff circumvent WebSense blocks on popular web-based email services by using less popular services.

Table 3. Key Concerns of Staff About Electronic Monitoring and Control of the Email System

1.	Staff felt that tighter control over email had created an untrustworthy communication medium and that the social communication necessary for effective business relationships had been negatively affected.
2.	Staff feel isolated and under greater scrutiny since electronic monitoring of the email was introduced.
3.	Staff believed that email monitoring was more invasive than other forms of monitoring. Staff carefully considered everything they wrote. Business as well as non-business email communication was reduced.
4.	Some staff felt that they had always used the email responsibly and they felt that they were being unfairly punished for policy violations committed by other staff.
5.	Staff attempted to transform and/or circumvent controls when the control was perceived to be poorly implemented and/or when they felt they had not been adequately consulted or informed. Staff reacted by protesting via email, conducting online polls, attempting to circumvent monitoring by removing or falsifying subject headings 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 email. Staff believed that training is essential and the email policy needs to be more highly visible.

'this policy should be contained in the handbook and should be published on the Intranet'. The engineer highlighted that new staff are never informed of the policy, and the problems they create subsequently have a direct effect on all staff'. One Sales Representative believed that 'all staff are being punished for the sins of a few'. She stated that 'I shouldn't be subject to the same sanctions as those who don't use the system responsibly'. Although, staff believed that email has never affected their productivity negatively, they agreed that monitoring acts as a control, diminishing the likelihood of email being used for non-productive behaviour.

CONCLUSION

The potential for an organisation to experience problems with email system use if it is left uncontrolled as it evolves is particularly evident in HealthCo as it experienced significant non-business usage of the system and poor mailbox management in the early stages. HealthCo failed to develop and communicate policies for email usage leaving staff to determine their own use of the system during the early stages of email diffusion. HealthCo only implemented controls after monitoring revealed the true state of email use. The study shows that getting the correct balance of controls is difficult and quite often staff react negatively to the poor implementation of controls rather than to the control per se. Further research is required to examine the details of electronic monitoring and control of email systems in other organisations, to determine if staff respond similarly or whether different approaches produce different reactions. Nevertheless, table 3 illustrates how the study has revealed a number of key concerns of staff about electronic monitoring and control of an email system, extending our knowledge of electronic monitoring and control systems in relation to staff issues.

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

BIBLIOGRAPHY

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.

Belanger, F. and Van Slyke, C. (2002) Abuse or Learning?, Communications of the ACM, 45, 1, 64-65.

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

Dermer, J.D. and Lucas, R.G. (1986) The Illusion of Managerial Control, Accounting, Organisations and Society, 11, 6, 471-482.

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

George, J.F. (1996) Computer Based Monitoring: Common Perceptions and Empirical Results. MIS Quarterly, Dec.

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

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

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.

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

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

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

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

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

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.