Preventing e-mail abuse in the workplace

Report by Martino Corbelli

MARTINO CORBELLI OF SURFCONTROL argues that good policy management, backed up with the right technology, can help employers strike a balance between employee privacy and the protection of business interests.

A recent survey we commissioned illustrated that nearly 30 per cent of white collar workers in the UK admit to sending racist, sexist, pornographic or discriminatory e-mails whilst at work. Despite all of the awareness campaigns focussing on businesses, it would appear from the statistics that much of it is still falling on deaf ears at employee level.

The current estimate is that 25 per cent of working hours are spent reading and answering e-mails, with 15 billion e-mails sent worldwide each day. Taking this into account, inappropriate use of the company e-mail system is one of the biggest concerns for employers.

REGULATORY DIFFICULTIES

Currently, laws on e-mail monitoring in the workplace are in a state of flux. A number of countries, including Sweden, Hong Kong and the UK, are introducing codes of practice that limit the extent to which businesses can check up on their staff. The UK Code, for example, recommends that blanket e-mail monitoring should not be conducted across the enterprise, but instead be used as a "spot check" measure. Furthermore, it recommends businesses ought to implement manual checking of employees' e-mail systems.

Needless to say, the practicalities of enforcing the above are out of synch with any business' requirement to protect its intellectual property, confidential information and corporate reputation from a wanton e-mail sent by one of its employees.

Whilst misusing the web creates productivity problems and hampers the company network's performance, divulging sensitive data is more often than not borne out of e-mail misconduct.

Contrary to popular opinion, the backlash against e-mail monitoring in the workplace did not really happen.

> ...divulging sensitive data is more often than not borne out of e-mail misconduct.

After initial cries of employee privacy, employers and employees recognised very quickly that the work e-mail system is precisely for just that; work-related communication.

Businesses now recognise that content in an electronic form needs to be managed as meticulously as confidential data stored in paper filing systems. Thought has now turned from the headline-grabbing cases of e-mail abuse, to those where competitive advantage can be either deliberately or inadvertently leaked to those outside of the corporate firewall.

Given that e-mail is an instantaneous mode of communication, which holds the same legal gravitas as if it were written on company letterhead, there is a significant increase in companies turning to e-mail filtering technologies to protect their corporate and intellectual assets.

Every organisation has information that is not intended for the public domain. Whether contracts, legal advice, business plans or internal memos, leaking one of these can be publicly embarrassing as well as costing the company in lost business and commercial confidence.

84 per cent of all confidential information loss is generated internally by employees - in the majority of cases unintentionally. Whether done with the intent of damaging the company or purely by accident, these judgement errors are only too easy to make.

STAFF E-MAIL POLICIES

The first step before applying any technical solution to combat e-mail misuse in the workplace is to create something commonly known as an 'Acceptable Use Policy'.

In essence, an 'Acceptable Use Policy', or AUP, clearly tells employees how the company reasonably expects them to use its e-mail system. The UK's Regulation of Investigatory Powers Act (RIPA), for example, states that any company wanting to monitor employee communications needs to communicate its policy

clearly to staff so that they understand that monitoring will take place. A properly implemented AUP satisfies this crucial requirement.

The AUP should always begin by specifying the general principles governing employee e-mail use, both in the course of business and in other activities. This should then be followed by clear conditions of use, and specification of what behaviour constitutes an abuse of company resources (eg. sending racist or sexist jokes or divulging corporate information to third parties outside the company). The AUP should conclude by explaining the consequences of a proven breach of the policy and request that all employees signify their consent to abide by the policy code.

It is sacrosanct that companies considering drafting an AUP avoid unilateral policy making. Setting limits on e-mail use is always going to be emotionally charged - highlighting issues of personal privacy and individual responsibility. It is advisable for the development and communication of the policy to involve every part of the business: senior management, information technology, business unit managers, human resources, legal and interested user groups.

The AUP can be incorporated into company practice in a number of ways. The important thing to remember is that it needs to be communicated to all concerned. This can be achieved by bringing to the employees' attention the company's new code of practice on e-mail use, and with new joiners, by incorporating the AUP into the employer's handbook.

FILTERING TECHNOLOGIES

With a policy in place, it is then necessary to have the means to enforce it. The optimal method of achieving this is by installing e-mail content management software on the network that has the capacity to manage employee e-mail traffic by (where necessary) blocking, filtering and monitoring messages sent and received.

Essentially, the majority of solutions on the market today help companies with an AUP in place to manage e-mail and web usage on several levels - securing networks against e-mail viruses, optimising employee productivity and network performance, as well as protecting confidential information and minimising exposure to e-mail-related defamation claims.

Fundamentally, e-mail content management software has to be able to protect the company from the e-mails deemed inappropriate in its AUP. Dangerous attachments, racist and sexist material, and confidential information can all be added to the software's filtering list to provide the company and its employees with the protection they require. The e-mail content management software has to be flexible. With every employee having different requirements from the corporate e-mail system, any software needs to take into account these needs, but still offer protection. For example, there is no point blocking everyone from e-mailing out their Curriculum Vitae, which would then prevent the HR department from fulfilling its recruitment requirements.

To conclude, e-mail content management with an enforceable Acceptable Use Policy has become one of the most powerful security measures any company today can introduce. Companies now need to consider e-mail filtering technology as an equal to the corporate firewall. With industry analysts predicting that by 2005, 35 billion e-mails a day will be sent worldwide, the argument for e-mail content management is unquestionably clear.

Martino Corbelli is Marketing Manager at SurfControl, a provider of e-mail and web filtering solutions. For further information: Tel: +44 (0)112 60 296 200, E-mail: martino.corbelli@surfcontrol.com, Website: www.surfcontrol.com

US employers are respecting privacy

For once, workers seem to be happy with the actions of their employers, according to a US-based survey conducted by Harris Interactive. Even more surprising is that the subject of the survey is employee privacy. Some 76 per cent of workers now consider their employers' privacy practices to be "pretty good to excellent". An almost perfect 94 per cent said that their employers had never released personal information in an improper manner. Concerns over the processing of sensitive data scored fairly low, with only 24 per cent suggesting that there may be a problem.

However, following the September 11th attacks, employees have become increasingly concerned over workplace security. Some 81 per cent of respondents said they would accept a work ID card, containing a photo, some personal data, and a biometrics identifier.

Public policy think tank, *Privacy & American Business*, commissioned the survey. Its founder, Dr Alan F Westin, said: "This survey finds a trend that runs counter to current findings of consumer privacy surveys. Where 80-90 per cent say they are concerned about how businesses are collecting and using their personal information, and express low trust in business privacy notices, here, confidence in employers is high..."

For more information on the survey, visit the Privacy & American website at:
www.pandab.org
See PL&B UK, May 2002, p.16 for article on balancing privacy in the workplace.