Email and Internet usage policy – Not enough by itself

Over the last couple of weeks we have been reading in the media about the dismissal of staff, and disciplinary actions taken against others as a result of allegedly pornographic emails. These were allegedly being forwarded within a group of around twenty staff in the Irish back-office operation of the global financial services firm, Merrill Lynch

Whilst this is nothing new, the number of people affected in a single disciplinary action in a company in Ireland is certainly newsworthy.

In 2000, one Bradley Chait gained infamy and notoriety, as did his employers, London law firm Norton Rose, as a result of a lewd email exchange between himself and his girlfriend (Claire Swire). While Bradley kept his job, with a strong reprimand, more than 50 other people in the United Kingdom alone lost their jobs for forwarding these offensive emails to others.

One of the frequent comments that have been made on the recent dismissals from the Dublin office of Merrill Lynch was that a clear breach of the email and Internet usage policy had taken place. Many legal commentators were reinforcing the need for a clear and unambiguous acceptable usage policy for the use of Information Technology (IT) resources such as web browsing and email. This is the cornerstone of any action that an employer wishes to take against employees that have been abusing the IT facilities provided in the workplace.

It is critical that employers have this policy in place to support any sanction they wish to introduce in the future as a result of unacceptable behaviour. The employer has a duty of care to the other employees in its care, and also to it's business partners. It would appear from media reports that in the Merrill Lynch case, a complaint was received from a client about the content of emails received from two Merrill Lynch employees. As a result of the investigation into these complaints, offensive email content was discovered in the mailboxes of up to twenty staff.

What is important to take from these reports is that an external party receiving these emails highlighted the abuse. This could be both embarrassing for an organisation and also potentially lead to loss of revenue.

Not only is it important to have an acceptable usage policy in place for the use if IT resources such as email and web browsing, there are a number of extra steps that must be taken. These would include a record of the employee having read, understood and agreed with the content of the policy, a regular update of the policy to staff to inform them of changes with regard to new technologies and risks such as Instant Messaging and Phishing. It must also be laid out in clear and simple English and not as a legalistic document too complex to read, let alone comply with. These are just a few examples, not a complete set of steps.

If a policy is to be considered effective, it is very important that there are appropriate technologies implemented to monitor the content of emails and web sites visited for compliance with the policy. These tools should inform the user, for instance, that a particular web site that they are attempting to access is prohibited under the usage policy. This attempt to access the site should be recorded and a report on this

provided, possible via the Human Resources function, to a Line Manager for discussion with the employee. The same principle should also apply to highlighted exceptions to the email usage policy.

One area where many companies that have email monitoring controls implemented have a potential weakness is that of internal email communication. Many of the technologies that are being deployed today are designed to be located at the perimeter of the organisation. At this point, typically where the connection to the Internet is firewalled, all incoming and outgoing email is monitored. However, this means that there is often no monitoring of the emails sent between employees in a company, as the email never leaves the internal network.

Where there is a policy, and there should always be, in place, consistency in the application of the policy and the tools used to police the policy is very important in ensuring compliance. If employees are aware of the policy and understand it, and they are also aware that there are technologies in place to measure compliance, they are more likely to willingly abide by it.

Contact Information

Rits Group Head Quarters
Information Security Centre
2052 Castle Drive
Citywest Business Campus
Co. Dublin
Ireland

Tel: +353 (0) 1 6420500
Fax: +353 (0) 1 4660468
Email: info@ritsgroup.com
Web: www.ritsgroup.com