

Don't be exposed by e-mail abuse

SINGAPORE

The article was contributed by Bob Yap, Head of Forensic, KPMG Advisory Services to Business Times on 25 May 2009.

The consensus that businesses need to get more serious about inappropriate e-mail usage has been building for some time. But, in an environment where many businesses are struggling simply to stay afloat, warnings about inappropriate use of business e-mail might seem untimely.

However, while healthy profit margins in happier economic times can disguise the potential costs, such risks can cause disproportionate damage to an already fragile company. The economic crisis may actually provide an impetus for tackling this issue, rather than sweeping it under the carpet.

Many people will have heard of at least one story of how some unfortunate person was exposed, sometimes literally, using business e-mail in an inappropriate fashion.

One example comes from 2005, when an e-mail made the rounds on the Internet and even on news channels such as CNN and the BBC. The incident involved a UK-based partner in a law firm whose e-mail to his personal assistant demanding £4 recompense for a small ketchup spill became a matter of public record. It was no laughing matter for him, since the negative publicity allegedly forced him out of his post.

For businesses which run the daily risk of an employee abusing their business e-mail account, it is similarly no laughing matter. Millions of e-mails are constantly circulating, and literally billions more are archived or stored on servers. Many of these have the potential to expose businesses to security or privacy risks or result in law suits for breach of contract, libel or workplace harassment.

One of the greatest dangers to business is cultural - the style we use to communicate, which is surely a corollary of mobile devices and messaging software. This has spawned abbreviated, rapid-fire communication; a sort of 'see it, send it' approach to personal communication.

Webmail accounts, such as those offered by Google, Microsoft and Yahoo, are rarely subject to the same security controls as business e-mail accounts. These may allow malware to circumvent corporate firewalls, and are a potential source of leakage of confidential or unencrypted data.



Finding an answer to these problems is challenging. No business wants to come across as a 'Big Brother', implementing endless guidelines and stifling creativity. Neither, though, should an absence of appropriate guidelines and security measures expose an organisation to unnecessary risks. There has to be a sensible middle ground.

At a bare minimum, companies should have an Acceptable Use Policy for workplace information technology and staff should be familiar with its guidelines. Going further, our experience suggests that companies should ask themselves three basic questions:

Should workplace machines require administrator authority to install software or alter key settings? Alternative browsers or messaging applications can circumvent controls you have in place. These can allow attacks on the integrity of your network which are not anticipated by your IT department.

Should personal webmail use be restricted? By blocking webmail domains, you can lock out webmail. Alternatively, you could choose to allow it on non-networked machines only. If staff need webmail access, they should understand what is or is not acceptable use.

Consider whether outgoing business e-mail should be subject to the same conditions as hardcopy correspondence. Not comfortable with all staff communicating in writing on the organisation's behalf? Implement a process to ensure business communications are cleared with an appropriate supervisor.

If a tougher regime is the answer, changes need to be implemented sensitively. An individual's business e-mail is, rightly or wrongly, often seen as an extension of their work - and sometimes personal - identity.

Encouraging responsible use of e-mail starts with staff training: employees who understand the dangers will accept restrictions more readily. They are also markedly less likely to set out to circumvent security measures.

Training in e-mail security need not be dull - a quick Google search for 'embarrassing e-mails' will provide all the examples you need to persuade staff that it might be worth their while to exercise a little discretion.

Contact us

Bob Yap

Executive Director
Head, KPMG Forensic

Tel: +65 6213 2677

Fax: +65 6223 0428

byap@kpmg.com.sg

KPMG Advisory Services

16 Raffles Quay #22-00

Hong Leong Building

Singapore 048581

Tel: +65 6213 3388

Fax: +65 6225 0984