



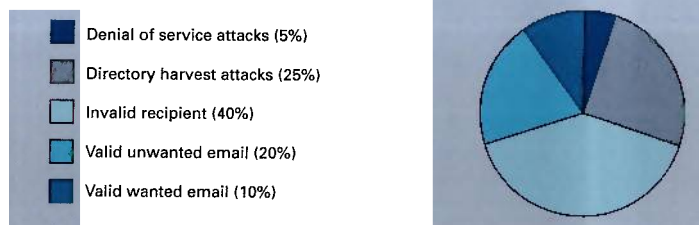
# Mail domination

**Email has become an invaluable business tool, but its ubiquity has brought some unique management challenges.**

The popularity of the BlackBerry is testament to the corporate love affair with email: in meetings, on commuter trains, in conference sessions, the now familiar buzz of the mobile device's incoming email alert sends a flurry of hands towards jacket pockets and bags.

What that behaviour highlights is the fact that email has become the primary business communications tool, easily overtaking the previous stalwarts of the telephone and paper documents. But as simple as email is, there are considerable challenges associated with its management: email is insecure; the majority of networks are clogged with unwanted messages; and, increasingly, email needs to be made accessible and carefully archived to ensure organisations meet their compliance obligations.

## BREAKDOWN OF INBOUND EMAIL TRAFFIC



Source: TUMBLEWEED COMMUNICATIONS

For many businesses, email management may mean little more than storing every email that enters or leaves their email gateway. The advantage of this approach is that it provides "a consistently applied policy, a single place in which to perform supervision activities, a reduced number of locations for search and discovery and reduced training requirements," says Erica Rugullies from Forrester Research.

But this approach also risks clogging up huge amounts of storage with unnecessary and unwanted material. According to IBM's 2004 Security Threats and Attacks Report, as much as 70% of all email traffic is spam – and businesses end up storing much of that alongside their own communications.

The problem is that "email was never designed to be secure," says Jeff Smith co-founder of messaging

security specialist Tumbleweed. "It was designed to be easy to use and to be anonymous" – traits that spammers readily exploit.

Even the most aggressive email filtering system is likely to let some unwanted traffic through. And the problem of spam extends well beyond the deluge of unsolicited emails: it is increasingly used as a vehicle for cybercrime, carrying such malicious code as spyware and Trojans designed to capture private data.

The cost of storing emails was brought home to London-based global insurance broker Willis following the 9/11 attacks on the World Trade Center. Having brokered the insurance on the Twin Towers, Willis found itself embroiled in court action related to the vast insurance claim that forced it to disclose millions of emails – a huge cost to the company, and one which prompted it to review its email retention policy. Willis now deletes emails after only a few months, unless they relate to customer transactions or to some legal obligation.

As that suggests, deletion policies must be able to cope with exceptions. "If something is due to expire and there's a court case coming up where it could be relevant, it needs to be kept," says Mark Donkersley of records management software vendor AXS-One.

If the cost of email management is high – industry researcher Gartner estimates that spending on email management at large companies is running at around \$1,600 per user per year – the cost of not doing it, both in terms of the financial impact and the potential damage to the organisation's reputation, can be enormous. When Perot Systems Europe was recently defending itself against claims of providing a defamatory reference for an ex-employee, for example, the outsourcer claimed in court that it would cost it more than £4 million to search five years of old emails for relevant documents.

The cost of providing a spam- and threat-free email service has led many organisations to hand the task to managed service providers, in much the same way most now rely on third parties to handle the complex task of keeping up-to-date with the ever-changing landscape of viruses and worms.

But whichever the option, there is a growing recognition that email is a 'smoking gun'. A survey by compliance security specialist Cryoserver of 100 CIOs found that 99% felt email issues could harm their company's reputation. And that is a potentially fatal side of email's attraction they would rather avoid. ⓘ

Article by **Abi Carter**  
[acarter@infoconomy.com](mailto:acarter@infoconomy.com)