



# PIM and proper

## The risks and compliance issues for public instant messaging.

– By Mark Padginton, Information Safe, Channel Development Manager.

Instant messaging, or IM as it is commonly known, has in the past been a fun and cost-effective tool for staying in touch with family and friends. As with many other communication technologies, it has not taken long for IM to creep into the workplace.

Today's younger workforce expects instant messaging and other collaboration tools to be available to them as the workforce of the 1990s did email. Organisations today are recognising the benefit of instant messaging and are deploying enterprise-class IM solutions such as Microsoft Office Communicator or IBM Sametime.

However, even if an organisation deploys a corporate IM solution, the general use of public instant messaging applications still remains. As with email, where we saw a noticeable increase in the use of public email accounts alongside the corporate email account, the use of Public based IM (PIM) applications will also be implemented by staff alongside corporate-sanctioned IM solutions.

Recent research has shown that three out of four employees in organisations where an enterprise IM platform has been deployed continue to use public instant messaging systems. What makes public IM applications so attractive is their ability to work no matter where you are; behind a corporate firewall, at the airport or at a coffee shop. This ease of connection is what makes public IM a threat to corporate security.

The increased popularity of instant messaging has also created new concerns around network security. Inbound threats are becoming increasingly complex to manage with viruses, malware, SPIM (spam over IM) and inappropriate content being propagated over

IM channels. Outbound threats can be in the form of organisational information leakage of intellectual property, corporate or personal financial information, which could lead to identity theft.

The challenge for administrators is to be able to identify non-sanctioned IM applications on a network. The goal of many IM applications is to provide ubiquitous connection and to create a positive end-user experience. Simply blocking specific native ports will cause the application to find another route to connect with its intended recipient. Many of these applications will apply Port/Protocol Tunnelling, P2P/Onion Routing or Random Session Behaviour to ensure connectivity.

Many applications use encrypted protocols, making it impossible for an intrusion protection system to detect or to control them. In addition, they use peer-to-peer connections. Skype, for instance, uses a peer-to-peer connection and is encrypted end-to-end, often even tunnelling through HTTP if that is the only port that it finds open on the firewall, negating the use of a URL filtering solution to control it. Few tools exist that can provide even the visibility of these applications, let alone the control. Consequently, many organisations do not even realise that their users have installed real-time applications.

However, if an organisation wishes to allow specific public IM accounts to be utilised on a network to save on costs, this will open the organisation to a number of risks if the content is not identified and managed.

Even enterprise IM is subject to increasingly new variants of security risks. Traditional malware is finding ways to hop from a public IM network

to enterprise IM networks. This risk is increased when two separate organisations decide to 'federate' or connect to each other through the use of an IM communication platform. All of these threats are multiplied by the increasing use of mobile devices such as Windows Mobile, BlackBerry and iPhones. A recent study in Europe found that 36 out of every 100 messages sent via a mobile phone is an instant message.

The impact that an unmanaged IM may have on an organisation may include:

- Information leakage (loss of confidential information and privacy issues)
- Increased help desk calls and support costs to clean up spyware infections
- Decreased network security from Trojans, viruses and worms spread through instant messaging
- Network bandwidth abuse due to P2P file sharing over IM
- Loss of productivity from non-business related IM chatting and video or music file sharing.

If left unidentified and unmanaged, instant messaging will leave a 'hole' in an organisation's regulatory compliance and standards. Regardless of whether an enterprise-grade instant messaging solution exists, employees will continue to use public instant messaging applications.

As organisations have applied to email, so compliance and best practices should be applied to IM. Many compliance regulations largely apply in the same way to IM conversations as they do to email records such as PCI (credit card), Sarbanes-Oxley Act, HIPAA (health insurance) and New Zealand's Public Records Act. ■