Strategic Guide

Instant Messaging and Security

Businesses recognise that instant messaging can help to improve employee productivity, but are often reluctant to sanction its use due to concerns about security. This Strategic Guide examines the real risks associated with instant messaging in corporate environments and explains how to mitigate them.

October 2009

Introduction

No longer just a forum for 'chatting' with friends, instant messaging is becoming a valuable form of communication in business environments, alongside the telephone and email. It can be used to get instant answers to questions, bring mobile colleagues together and provide a quick and convenient forum for sharing ideas. Analyst firm Gartner predicts that 95% of workers in global 100 organisations will use instant messaging "as their primary interface for computer-based, real-time communications" by 2013.[1]

74% of businesses recognise that instant messaging improves employee collaboration, but 72% block its use due to security fears.

According to a survey conducted by independent market research company Vanson Bourne[2], businesses are very much aware of the benefits of instant messaging. Among the organisations that participated in the survey, 74% recognise that instant messaging improves employee collaboration. However, 88% of the organisations surveyed reported that they are concerned about the implications for security. Indeed, 72% of businesses have taken measures to block and forbid the use of instant messaging within their business because of their security fears.

While understandable, this reaction is, in most cases, an overreaction. The risks of using instant messaging in a corporate environment are far fewer than is often feared. Sometimes, IT departments are just not familiar with new technologies like instant messaging and therefore do not fully understand how it can be used securely in a corporate environment.

Nevertheless, some concerns are very genuine, and businesses are right to proceed with caution. What is needed is a considered approach to instant messaging that proactively minimises the risks, while allowing employees to use this new technology to improve their ability to collaborate with colleagues and work more productively.

[1] *MarketScope for Enterprise Instant Messaging and Presence, The Gartner Group, 26 June 2009*

[2] *Survey conducted with 100 senior IT decision makers from enterprises of 1000 or more employees. Vanson Bourne, sponsored by ProcessOne, July 2008*

The danger within

The sudden increase in the popularity and use of instant messaging has taken many organisations by surprise. While they have deferred decisions about investing in corporate systems, instant messaging has in the meantime crept into their business by the back door.

Fuelled by social networking sites and the growth in text messaging, interest in instant messaging has been increasing steadily over the last two years. In fact, IDC, a global provider of market intelligence, has defined a new category of individuals - the 'hyper-connected' - who are passionate about the convenience of instant and text messaging. The firm calculated that 16% of the global information workforce is already 'hyper-connected' and another 36% would soon be joining them[3].

Just because you don't have an instant messaging platform or instant messaging policy, it doesn't mean that your employees aren't using it.

These 'hyper-connected' individuals are taking advantage of public Instant messaging service, like Gmail and MSN, which are available to download and use free of charge. But this is how the danger arises. Many individuals do not only downloaded public instant messaging software onto their home computers, but also install it on their desktops at work, without the knowledge of the IT department. While they initially only use the service to exchange messages with friends and family, they do, over time, come to accept it as a part of their own daily life and start to use it for business contacts too. These employees are not acting maliciously; they simply do not realise the potential danger to which they are exposing their employers.

[3] *The Hyperconnected: Here they come!*
A report by IDC, sponsored by Nortel, May 2008

Public instant messaging services have not been designed for corporate connectivity and do not provide the level of security that is essential in a business environment. These services allow users to attach files to their communications and exchange them with an unlimited number of other users, in any organisation, in any country. It is, therefore, easy for confidential information to escape from the company and for virus-infected materials to slip in.

Is your business already exposed?

In research conducted with 2,400 working individuals in 17 countries, IDC found that two thirds of 'hyper-connected' individuals use text or instant messaging for both work and personal use. More than a third also use social networking for both.[4]

[4] *The Hyperconnected: Here they come!*
A report by IDC, sponsored by Nortel, May 2008

What are the risks?

Uncontrolled use of instant messaging by employees exposes businesses to a number of risks, including:

ATTACK FROM WORMS, VIRUSES AND TROJAN HORSES

Most security fears concern the propagation of viruses, worms and Trojan horses. For the operators of large public instant messaging networks, like Yahoo, GoogleTalk and MSN, these are indeed very real threats. Worms and viruses are often delivered by 'Spam over Instant Messaging' or SPIM. Users receive an unsolicited email inviting them to click on a link. However, when they do this they inadvertently either launch an infection or a spy-ware programme that will harvest details of their contacts and infiltrate their communications.

Users of the ICQ public instant messaging service are particularly at risk from SPIM, because their user IDs are just numbers. It is therefore relatively easy for people with malicious intent to generate random addresses and bombard thousands of users with infected communications.

LOSS OF INTELLECTUAL PROPERTY

The loss of confidential information is a major concern and one that all organisations must take seriously. Even though it may seem unlikely, businesses must also protect against the malicious actions of disaffected employees, who could potentially use instant messaging as a means of transferring secrets to the media or competitors.

The risk of intellectual property loss is heightened due to the lack of encryption on public instant messaging systems. In a survey conducted by Cnet.com in June 2008[5], only half of the providers of public instant messaging services contacted offered complete encryption. Well-known services, including Facebook Chat, Microsoft's Windows Live Messenger and Yahoo Messenger failed (at the time) to offer the full protection that all users - and especially corporate users - require.

The risk of intellectual property is heightened due to the lack of encryption on public instant messaging systems.

THEFT OF PASSWORDS AND USER IDENTITIES

Users of public instant messaging accounts are also at risk of having their passwords and user IDs stolen. In February 2009, many users of Gmail and Yahoo were targeted by a major phishing attack on their instant messaging accounts. When users clicked on a link contained in the bogus message, they made themselves vulnerable to identity theft. Unfortunately, phishing attacks on public instant messaging services are likely to become more - not less - common. This is because, as users numbers grow, it becomes easier for malevolent individuals to anticipate user names.

It could be said that the onus is on users to make sure that they don't open files and click on links from contacts that they don't know. However, with public instant messaging networks, it can be very hard for users to verify who a sender is. With unspecific user names like Fred1234, users can easily be mistaken into thinking that they know the sender of the message.

[5] *http://news.cnet.com/8301-13578_3-9962106-38.html*

LACK OF CORPORATE CONTROL

It is very difficult to effectively monitor and audit the use of public instant messaging services. As a result, some large organisations may find themselves in breach of government and industry-specific legislation that requires them to keep auditable records of all business transactions and communications.

Most significantly, the Sarbanes Oxley Act of 2002 (also known as the Public Company Accounting Reform and Investor Protection Act) requires all US organisations and their overseas subsidiaries to be able to provide rigiorous audit trails for all transactions. In addition, the Health Insurance Portability and Accountability Act (HIPAA) for the healthcare industry in the USA and the Gramm-Leach-Bliley (GLB) Act for financial institutions in the USA demand auditable communciations records. In Europe and other countries around the world, there are other similar pieces of legislation that affect a range of sectors. If organisations cannot provide audit trails, they risk non-compliance and costly legal action, as well as a potential loss of earnings from the damage to reputation that is likely to occur.

And how can these challenges be overcome?

Dedicated corporate information messaging systems give organisations greater control over security.

1. TAKE CONTROL

The principal step that organisations need to take is to bring instant messaging into their control, by deploying a dedicated corporate instant messaging system. All instant messages sent and received by employees can then be channelled via a central server, archived for future reference, encrypted and subjected to corporate security processes and policies. Anti-virus solutions can also be used in association with the corporate instant messaging server, to prevent viruses from being inadvertently propagated within the business by instant messages.

With corporate instant messaging systems, users have well defined, explicit user names (which are often the same as email addresses). As a result, it is much easier for employees to verify whom they are chatting with and make sure that they don't fall victim to a phishing attack. The use of encryption in corporate instant messaging systems further improves the confidentiality and security of exchanges.

Bringing instant messaging in-house doesn't mean that employees have to be cut off from the public instant messaging networks that they are familiar with. Corporate systems are available that offer gateways to the well-established networks, such as MSN, GoogleTalk and others. Some systems, such as those offered by ProcessOne, go one step further and offer secure bridges to social networks such as Twitter. However, despite their flexibility and openness, these corporate instant messaging systems nevertheless permit businesses to exercise a great deal of control over usage. For example, all exchanges of messages can be archived, including those exchanged via external or public networks.

2. MINIMISE THE RISKS

Organisations can further improve the security of instant messaging by monitoring the domains of users who contact employees. Unlike email, instant messaging allows the systems administrator to verify the domains that can send or receive messages, through the use of certificates. This precaution makes it difficult for SPIM and phishing attacks to succeed, because it is possible to identify the sender of messages with absolute certainty. The system administrator can then block the source of potentially malicious messages.

The purpose of instant messaging in a corporate environment is to improve collaboration between employees, or between employees and selected partners. The aim is not to facilitate the use of instant messaging for social and personal communications during work time (or the effects of instant messaging on productivity would, of course, be counter productive). Many organisations therefore decide to only allow communications between certain domains and block other destinations. Systems administrators can use certificates to limit usage to within the organisation itself, partner organisations, subsidiaries and other 'approved' contacts.

If the company policy forbids (and prevents) the transfer of files with unspecified external organisations, the risks associated with loss of confidential information and infection from viruses is immediately minimised.

3. EDUCATE USERS

The introduction of any new corporate instant messaging solution should be preceded by a period of education for users. This important stage is necessary to:

a) Position instant messaging as a valuable communications tool, next to email and telephone, and explain how it can be used to help them work more effectively

b) Give users the knowledge to understand the security risks and instil responsible behaviours for usage

It is necessary, for example, to explain the risk of theft of intellectual property through identity theft. Employees can then interrogate a contact to verify their identity prior to sending them sensitive information. Better employee vigilance can lead to reduced risks, without hindering the likely productivity gains.

Instant messaging systems can be very versatile and packed with added features that employees will need to get familiar with. For example, users can set their accounts to 'busy' or 'offline' when they are in meetings or focusing on a project. They can also set their account to 'delay' the delivery of messages. While these features do not in themselves, enhance security, they will help to ensure that the investment in a corporate instant messaging system delivers the greatest improvement in productivity.

Conclusion

While there are many security concerns associated with instant messaging in general, the risks are greater for users of public instant messaging services. Designed for social and personal usage, public networks frequently do not offer the encryption and protection that is absolutely essential for corporate environments. If employees are using their private instant messaging accounts on their desktops for personal and business communications, they are almost certainly placing themselves and their organisation at risk. Hundreds or thousands of unsecured and un-audited communications may be slipping quietly past an organisation's firewalls every day.

The risks are known and can be controlled.

The best way to reduce the risks is to bring instant messaging in-house with the deployment of a central instant messaging server. In this way, IT departments can take measures to protect users and intellectual property through the use of encryption, anti-virus software, corporate policy and domain certificates. In a corporate setting, the risks of using instant messaging are very much reduced. This is mainly because messages sent and received are usually exchanged within organisations and their reach is limited to the perimeter of the enterprise or between trusted partners. Organisations can therefore take advantage of instant messaging to improve employee collaboration and productivity, without placing their business in jeopardy.

Security is, however, an ever changing challenge and not something that can be addressed just once. Therefore, when organisations deploy their own instant messaging servers, they should take the precaution of obtaining a support contract with a company that is an expert in the field. Then, if a new security threat does appear, IT departments are not left in the dark and can gain rapid access to the very latest information. The best defence is constant vigilance and specialist advice.

For more information, contact ProcessOne.

process one
INSTANT MESSAGES | CREATIVE BUSINESSES

ProcessOne
58, Boulevard de Strasbourg
75010 Paris France

Tel: +33 963 282 049
Fax: +33 142 012 547
Email: info@process-one.net