Instant Messaging:
Managing and Securing IM in the Workplace

Introduction

This white paper provides a best practice overview for companies seeking to use IM effectively in a corporate context whilst managing the associated security and productivity-related risks.

IM As A Business Tool

Originally created in the late 1980s, Instant messaging (IM) technologies are the fastest growing application ever to hit the corporate desktop. Gartner recently predicted that 95% of global enterprise workers will use instant messaging (IM) as their primary method of real-time communication by 2013.

IM is here to stay—and is increasingly replacing more traditional forms of mainstream business communication. Employees at IBM send over 3 million IMs every day and the technology is now embraced by a growing number of organisations as a critical application for workplace connectivity.

The adoption of IM in the workplace has wide ranging benefits. As a fast and efficient way of sharing information with colleagues or customers, real-time communication can bring significant operational advantages, saving businesses money on phone calls and travel costs and facilitating far faster responses. With Instant Messaging it is often easier to get a quick response via an IM chat than chasing up a reply to an email. Fast, immediate contact is also vital for some (such as stockbrokers who need to share the latest market information) and IM can be an extremely valuable communication tool for remote or roaming workers (such as technicians working with customers on site needing to relay information from their support teams).

When permitted in the workplace, IM conversations can appear to be more prolific than those via email but they are usually briefer and more efficient, allowing workers to get quick answers without the ‘niceties’ that come with email communications.

Although critics cite IM as a constant distraction, when used properly IM conversations actually offer more convenient communication because users will check first to see if colleagues are available (via their IM status) and it is often more socially acceptable to ignore or postpone responding to an IM as opposed to a telephone call. It is also possible to hold several IM conversations simultaneously and share web links in real time - so everyone is on the same page.

For businesses with geographically distributed teams in multiple office locations, IM can aid e!ective communication by providing an informal and spontaneous way for teams who need to work together in a virtual capacity to interact and build bonds. Some companies find IM particularly useful when it comes to exchanging quick comments or action points with colleagues during webinars, virtual meetings or video conferences.

However, in circumstances where IM use is uncontrolled, the legal and security risks, (not to mention the productivity pitfalls) far outweigh the bene" ts. Too many organisations are taking unnecessary risks with outdated policies and unmonitored usage.

What Are The Risks?

The risks of uncontrolled use of IM in a corporate context are similar to email, but more serious since communications and file transfers are less frequently monitored and usually don't come with legal disclaimers. Where employees know that IM is unmonitored, they are often more likely to use it as a way to share information
without 'red tape' or risk of retribution from their line managers, heightening the risks.

Data Leaks/Unlawful Disclosure

Where IM communications go uncontrolled and unmonitored, organisations risk losing control over confidential or sensitive information which could be accidentally or purposefully leaked outside the company. Countless organisations have suffered embarrassment and fines as a result of losing or exposing personal data records or commercially valuable information. The copying and sending of copyright data (without the permission of the copyright holder) is also a significant risk since breaches or infringements of the UK copyright act (1988) and the US Intellectual Property Protection Act (2008) come with prosecutions and steep fines.

Harassment

IM communications carry similar risks to emails when it comes to harassment or discrimination cases involving employees, customers or suppliers. Cyberbullying is far from limited to schools, and all companies have a legal obligation to provide a safe place of work and take reasonable steps to protect their employees from abuse, harassment, discrimination and personal defamation.

Where companies fail to take such steps, employees can cite a breach of contract, leading to 'constructive dismissal', and in some cases are entitled to claim for damages. Employers can face legal liabilities in connection with defamatory statements made about colleagues or competitors. This can apply to both external AND internal IM communications.

Productivity

Without proper control, IM has the potential to impact significantly on productivity levels. Organisations who allow IM without monitoring and strict usage guidelines run the risk of it becoming a constant distraction and a disruptive interruption to normal working tasks. Without supervision, IM can actually increase timewasting, since staff can 'appear' to be working quietly whilst they engage in IM-based office chatter or private unmonitored chats with their buddies.

Network Security

Uncontrolled IM traffic can also provide a route into networks for destructive viruses and malware which can impact heavily on operations and critical services. Messages often aren't encrypted (although most standard IM clients encrypt authentication
credentials, the session itself is rarely encrypted) and so could potentially be intercepted or eavesdropped upon. Phishing and social engineering attacks are also becoming more common across IM platforms, especially with public IM applications such as MSN, where chat buddies are easily impersonated.

From a technical standpoint, IM tools (like P2P file sharing tools) are classed as 'wild' (as opposed to standard) application protocols. They can often tunnel over HTTP and can be difficult to control effectively using firewalls or simple web filters. In terms of the potential to carry viruses, worms, Trojans and other malware, IM is equally as dangerous as other flows of data in or out of the company via email or web and potentially more so, since viruses sent via IM can be distributed much faster. Unsolicited ads and spam are less of a problem than with email but are increasing (SPIM is now a fast growing phenomenon).

Why Monitoring Is Important

Vicarious liability

Vicarious liability is a legal term used for when unlawful acts are undertaken in the course of employment –i.e. by an employee. It covers anything an employee does at work or for work purposes. Even if the act is forbidden by the AUP, and the software is not provided by the employer, the employer can still be held liable.

Record-Keeping & Regulatory Requirements

All organisations need to keep records as evidence in the event that they need to defend their legal rights in court. In the course of legal proceedings, logs may be required to prove a case & courts consider IM logs in the same way now as they do letters or emails. In circumstances where electronic documents are needed as evidence, failing to produce records of relevant IM conversations could significantly damage an organisation's case.

In the finance and public sectors in particular, there are also legal requirements for record-keeping, dictated by the Freedom of Information Act, the FSA in the UK and Sarbanes Oxley in the US. Organisations are required to keep records of all communications (including IM) for at least 6 months. Some records need to be kept for up to 10 years depending on the critical nature of the content. Failure to comply with such regulatory requirements can carry stiff penalties.

About IM Applications

IM applications range from free public clients to fully-featured commercial enterprise applications and sessions can be either encrypted or unencrypted depending on the application. The overwhelming majority of public IM users use one of the big three: AOL, MSN, or Yahoo Messenger. Generally speaking, free applications are unencrypted but there are some exceptions such as Jabber and GoogleTalk. Organisations employing foreign speaking staff may also encounter less well known applications such as GaduGadu (a popular Polish IM client).

Security Steps To Control IM

Block installation of unauthorized clients

If software downloads are not restricted, some staff may already have downloaded software and be using IM applications without your knowledge or permission. In addition to the risks associated with unsupervised IM use, user-installed clients might be poorly configured & could have the potential to conflict with or disrupt other critical network services. Self-installed IM clients can also be set up to bypass firewalls & gateway AV by using non-restricted ports or to route traffic through an external proxy server.

Firewall protection

From a gateway and port access perspective, it usually makes sense to ‘deny all’ and allow applications as needed – whilst making sure that everything you allow can be filtered. Forcing or re-routing traffic via an HTTP proxy can also provide an additional layer of security.

Block attachments & file transfers

Attachments and file transfers sent via IM can carry destructive viruses or malware and large file downloads have the potential to cause network congestion or disruption. There is also the danger that a staff member might send or download a file transfer quickly via IM without considering the possible consequences, leaving the organisation open to data leaks. It is advisable to block all IM attachments (so files can be transferred in a more controlled environment) but if IM transfers are required, a secure IM client is best, preferably one that offers at least 128bit encryption of both the authentication credentials and the IM session itself.

Monitor Everything

IM monitoring should cover private as well as public chats. Some IM monitoring products (e.g. Guardian) offer keyword alert facilities which can help IT Managers to filter out conversations with dubious content in data-heavy logs, so they can respond more rapidly to incidents or policy violations.

This can be a particularly useful feature in sensitive circumstances such as a takeover or float, where alerts on words such as 'shares' can help to alert organisations to potential problems or breaches of confidentiality. Censoring out swear words and other inappropriate phrases is also wise since it significantly reduces the chance of unwelcome litigation as a result of discrimination or harassment in the workplace. Where monitoring is in place, staff must be informed (this is a legal requirement) and will in most cases act more responsibly if they know their IM use is supervised.

Update Policies

Acceptable Use Policies should be updated to cover IM and reissued to staff so they are aware of the changes. The policy should expressly state that the IM system is not to be used for the creation or distribution of any offensive, or disruptive messages, including messages containing offensive comments about race, gender, age, sexual orientation, pornography, religious or political beliefs, national origin or disability. It is also important to mention that employees should not use IM to discuss competitors, potential acquisitions or mergers or to give their opinion about another organisation.

Educate Staff on IM use

Training on effective use of IM in a work context is extremely valuable, so staff can be educated NEVER to send sensitive data and can learn how to signal their availability and distinguish between a professional and a casual conversation. Training is the key to getting the best out of IM communications since the most significant security risks always stem from users - not systems. The same is true of productivity as although security measures can help to discourage timewasting, a company's capacity is far more contingent upon factors such as employee work ethic and self discipline.

Other security considerations

IM applications must be kept up to date with latest security patches – rapid patching is important as IM clients are even more vulnerable than web browsers as a threat vector. Having both gateway and desktop AV protection is also a sensible precaution, as is creating an IM-specific disclaimer. Although disclaimers can't go with every conversation (as they can with emails), the alternative is to create an online disclaimer and include a hyperlink at logon. As with email, it is also sensible to keep the number of people with access to logs to a minimum, and ensure you have sufficient confidentiality and security agreements in place with those individuals.

How Guardian IM Controls Work

The Guardian web filter offers comprehensive control over IM applications (including encrypted ones). Conversations can be monitored in real time and selected words or phrases can be both censored and set to trigger alerts. File transfers and attachments can be logged or blocked as required. Unlike many vendors, Smoothwall does not charge extra for filtering and managing IM content alongside other web traffic. IM control is provided free of charge with the Guardian content filter, simplifying security with a single point of contact for one unified solution.

UK + INTERNATIONAL

Smoothwall Ltd
1 John Charles Way
Leeds LS12 6QA
United Kingdom

+44 (0)800 5 999 040 UK
+44 (0)870 1 999 500 International
sales@smoothwall.net
www.smoothwall.net

USA + CANADA

Smoothwall Inc.
6201 Fairview Road, Suite 320
Charlotte, NC 28210-4274
United States of America

1-800-959-3760 US + Canada
1-888-899-9164 Fax
sales@smoothwall.com
www.smoothwall.com