Risk-Free Instant Messaging

- Have the Cake and Eat it Too!
Contents

Introduction .................................................................................................................. 1
IMs Aid Productivity, Efficiency in Organizations ............................................. 1
The Dark Side of IMs ................................................................................................. 1
Risks of Using an Instant Messenger ...................................................................... 2
The IM “Hydra” - There’s no stopping it! ............................................................ 4
Secure IMs Aid Productivity & Data Security ...................................................... 4
Securing Instant Messengers .................................................................................... 4
Cyberoam UTM Controls and Manages IMs ......................................................... 6
Introduction

Instant Messengers came on-air during the 1990s. Their first avatar was ICQ - homophone for the phrase “I Seek You”, developed by Mirabilis, that merged online contacts and allowed them to exchange messages. Public Instant Messengers (IMs) like Yahoo, Windows Live Messenger and others started as a personal chat and entertainment tool for home users and teenagers and gradually entered the corporate grounds to become the official, or rather the “unofficial”, means of instant communication among corporate users.

Its multiplying popularity in enterprises is obvious from the leading analyst firm Gartner’s prediction that 95% of workers in global 100 organizations will use instant messaging “as their primary interface for computer-based, real time communications” by 2013.

IMs Aid Productivity, Efficiency in Organizations

IM adoption continues unabated in organizations today because of the speed and ease of communication it offers over emails. They add immediacy and efficiency to business communication and information sharing. Whether it is about exchanging information with partners or suppliers, or getting help from colleagues that maybe across the floor, department, branch offices or countries - it is just a 'ping' away with IMs. Such instant and real-time information exchange without boundaries enhances workforce productivity and efficiency. For a business, it accelerates decision-making and operations and improves team-work.

Instant Messengers give you real-time status of a person. They let you know right away whether the person you are trying to reach is available. This means fewer phone calls in trying to reach the person - which saves time and cost for the organization.

The Dark Side of IMs

If IMs add to an organization’s productivity along with many other benefits, why do they still carry the “unofficial” tag in corporate environments? That’s because IMs were not created keeping corporate usage in mind - they lack the much-needed security policies and safeguards, controls and management, logging and reporting abilities to handle sensitive corporate information traveling through them.

Majority of IM traffic travels through public networks without any encryption - which means that they are easily susceptible to eavesdropping by others. At the same time, it is difficult to block users from accessing IMs as they can hop ports to outsmart firewall rules that are applied to block native IM ports. Lack of audit logs and reports means your IT administrator may not be aware how many users have IM clients installed on their machines or more importantly, who is talking to whom in your organization. Wouldn’t that be a big security nightmare for any organization? And what about the employee productivity issues that may arise if your employees indulge in personal chat sessions over IM because they know the IT administrator is blind to their IM activities?
What looks ‘productive’ is actually a ‘productivity killer’!

Risks of Using an Instant Messenger:

a) Productivity Loss
Lack of IT administrative controls over IM activities and the lack of trail on who the employees talk to and for how much time encourages idle chat by users. If you thought Fred, Joe and Martha were busy pulling up your sales figures by chatting with your customers or partners over IM, you will be disappointed to know that Fred was busy sending a birthday card attachment to his girlfriend, Joe was discussing the stock market with his stock analyst while Martha was exchanging beauty tips with her best friend - all over IM and at the cost of your organization’s productivity!

b) Data Protection
Besides chat conversations, IMs are today used to send data, audio and video files too. However, the most widely used IMs like Yahoo! and Windows Live Messenger run on public networks that lack any security mechanism. Chat conversations or files sent over IMs mostly travel unencrypted over the Internet from the sender’s client to the IM server and back to the recipient’s client.
Files containing trade secrets or sensitive information sent over IMs are thus readily available for eavesdropping anywhere along the internet path it travels or within the IM provider’s network. Let’s say, Fred uses IM to send a confidential product presentation to his team member Joe, believing that IM is the quickest and easiest way to send it. The product presentation travels unencrypted over the IM network and can be easily intercepted and read by a competitor.

Now imagine what would have happened if Fred had asked Joe over IM for the password to access their CRM application. The company’s entire customer database would be up for reading by a competitor!

If Fred were a malicious insider who intended to send out confidential data to a competitor firm, he could have easily done so, thanks to the ability of firewall tunneling of IM client installed on his machine.

c) Malware Threats:
IMs have the ability to tunnel through the firewalls and take viruses, spam or other unauthorized files inside the organization. Sometimes, a malware code may be hidden in the file your user wants to share over IM. When the recipient on the other end opens the file, the malicious code spreads in your entire network. The problem multiplies with the real-time nature of instant messaging that spreads malware to the entire contact list without giving time to counter the threat.

d) Legal Compliance Risks:
The growing list of regulatory compliances like HIPAA and PCI DSS make it mandatory for organizations to protect privacy of individuals and maintain proper records of their account activities. Uncontrolled and unsecure IM sessions and lack of log records and monitoring weaken an organization’s stance on satisfying legal requirements. This could mean escalated legal and financial costs for using IM.
The IM “Hydra” - There's no stopping it!
Organizations fearing productivity and security risks of IMs may wish to block their employees from accessing them by creating adequate firewall rules. But IMs are port-agile and they look for open ports in the network to tunnel their traffic through the firewall. For example, if their native ports are blocked by the firewall, they may knock the HTTP Port 80, the port used by browsers to surf the Internet - which is usually kept open by most organizations for their web traffic. The IM traffic may even masquerade within the legitimate traffic for Port 80 or other allowed ports to enter the organization. In this case, if the organization decides to block Port 80 in order to block IMs, it will also be closing down all access to the web, which does not make much business sense!

Secure IMs Aid Productivity & Data Security
Denying the use of Instant Messengers will be like denying the many business benefits of using them. This may not be a wise stand for an organization as it will be losing out on an efficient business communication tool by blocking IMs. However, using IMs along with their current security loopholes for business communication does not make good business sense.

While private IMs using protected networks are available, the popularity and free-availability of public IMs is silencing the need to use private IMs among organizations. Good news is that there are Instant Messenger management tools available today that allow you to apply controls over public IMs to personalize them according to the security needs of your organization.

Securing Instant Messengers
An Instant Messenger management solution enables organizations to control the use of Instant Messengers viz. who will be allowed access to IM, whom can they communicate with, guidelines on prohibitive IM activities, and more; enabling them to derive benefits of productivity and data security. It logs IM activities that may help organizations in forensics and investigative purposes.

The IM management solution intercepts IM traffic and applies controls over it, based on user-specific IM policies.
a) Ensuring Productivity
An organization can control productivity of its employees by completely blocking IM access for specific users whose job does not demand its need. An IM management solution allows it to control which user or user group can logon to an IM by knowing his username or IM address. For eg., Jack in the Finance team does not need IM access for his day-to-day job functions. The organization can deny him access when he tries to logon to the application. If the organization wishes to block IM access for the entire Finance team, it can create a user group, say the 'Finance group', and block IM access by their usernames.

An IM management solution archives IM activities that allow IT administrators to review IM conversations, especially while investigating an incident. If a user is found to extensively use IM for personal use, a warning message can be sent to him, allowing the organization to ensure productivity of its employees is not compromised by excessive personal use of IM.

b) Ensuring Data Security
An IM management solution enables an organization to keep its data secure from unauthorized or insecure sharing over IMs. This can be done by controlling chat conversations, file transfers and form of IM communication i.e. Chat, voice and video.

By using an IM management solution, an organization can control (allow or block) one-to-one or group conversations that may risk sensitive data leaving the organization. The content filtering feature searches specific keywords like “confidential”, “social security number”, and more, in the IM conversation, enabling educational institutes to block child-abuse content and also protecting organizations from disobeying regulatory compliance requirements.

The solution can block file-transfer from taking place between two users or groups. For eg., it can block file transfer over IM between sales and R&D teams. This also helps the organization ensure that regulatory compliance requirements on data security are met. It can also control voice or video chat between two users.

In addition to all these measures, awareness about the presence of an IM management solution should be passed on to internal IM users to discourage them from using it for personal conversations.
Cyberoam UTM - Controls & Manages IMs

Cyberoam UTM offers identity-based IM controls for Yahoo messenger and Windows Live Messenger. It can scan, log and control access, conversation, file transfer, and audio/video chat between users and user groups in the network. A user can be denied access to IM by his username or his IM address. File transfer can be blocked by applying identity-based policies for users. Cyberoam’s IM controls offer logs of all communication between users that can alert IT administrators in case of security breach issues.

Cyberoam can scan, log and control access, conversation, file transfer, and audio/video chat between users and user groups in the network.

Cyberoam UTM IM Controls

- Log Communication
- Data Protection
- Control File transfers
- Productivity

Control who can chat with whom

Control communication medium
(chat, video, voice)

Data Protection

Productivity

Control File transfers

Log Communication

Control who can chat with whom

Cyberoam can scan, log and control access, conversation, file transfer, and audio/video chat between users and user groups in the network.