Risk and Reward

The role of Instant Messaging in your UC Strategy
Risk and Reward

Contents

Introduction: Risks in Real Time ...................................................... 1
Isn’t there another way? ................................................................. 1
Impact: Value and Versatility ......................................................... 1
Imperfect: Facing the Threats .......................................................... 2
Impasse: The Policy Problem ......................................................... 3
An Instant Cure ............................................................................ 4
Introduction: Risks in Real Time
In a world where fast is good and instant's better, it's no surprise that Instant Messaging (IM) now rivals email as a must-have communications medium. Over a billion users worldwide, sending over 30 billion messages a day\(^1\), can’t be wrong.

But for businesses, IM poses a dilemma. Undeniably, it offers real-time communications capability whose speed, immediacy and flexibility dovetail perfectly with today’s breakneck business environment – an environment where keeping in touch with colleagues and customers is increasingly an ‘anytime, anywhere’ requirement.

Yet for every benefit, there’s a very real risk. IM’s key strength is also a source of serious weakness. Its informal nature can make IM difficult to rein in, exposing organisations to data leakage and legal/compliance dangers, and offering business-bruising, data-stealing malware an under-policed point of entry into IT networks.

Inevitably, some businesses see this as a binary choice: adopt IM and accept the risks, or reject it and forgo the benefits. Others opt for an uneasy compromise, banning ‘official’ use but turning a blind eye to staff harnessing public IM clients for business purposes – a decision that can easily come back to bite them.

Isn’t there another way?
This White Paper demonstrates how your business can exploit IM’s enormous potential – and mitigate against risks that, all too readily, come as part of the package.

BUSINESS AT RISK!
Just 15% of organisations using a Unified Communications service choose not to use the IM function but...
Only 30% of organisations have malware protection in place for all their IM traffic\(^2\).

Impact: Value and Versatility
IM began as a way of staying in touch. But it’s evolved into a multi-faceted medium that – whether harnessed via public IM clients or enterprise-grade solutions – not only boosts the efficiency of business processes but also shapes the way business is conducted. IM now incorporates mobile, video and other capabilities that have transformed it into a collaborative, problem-solving tool that can bind together office-based staff, remote workers and mobile employees into effective teams.

The tangible impact of IM can be felt across every key metric of business performance:

- Increased efficiency, productivity and profitability.
- Sharper decision-making.
- Enhanced business agility and continuity.
- Improved customer satisfaction.

---

\(^1\) Instant Messaging Market, 2010-14’, The Radicati Group, Inc. (October 2010).
\(^2\) All facts/figures in inset boxes are sourced from a survey of 144 UK-based organisations carried out by eMedia in conjunction with Symantec.cloud (March 2011).
IM also now plays a pivotal role in the Unified Communications (UC) packages deployed by an increasing number of organisations. UC utilises software-based architecture to streamline all communications devices and applications (email, IM, video conferencing etc), enabling messages sent using one medium to be received using another and taking into account both the recipient's location and their preferred method of receipt. IM also now plays a pivotal role in the Unified Communications (UC) packages deployed by an increasing number of organisations.

Underpinning the concept is UC’s ability to integrate real-time and non-real-time media. Consequently, as many people’s real-time communications tool of choice, IM stands at the apex of the UC pyramid – and will continue to do so as more businesses recognise UC’s potential and buy into it. Quite simply, it’s becoming ever harder for businesses to turn their backs on IM if they value their commercial competitiveness.

**BUSINESS AT RISK!**

58% of organisations believe they face medium, high or very high risk of data loss due to employees communicating via IM with federated partners or users of public IM clients

but...

Just 19% have policies in place specifically governing use of IM.

**Imperfect: Facing the Threats**

The trouble is, alongside the benefits, IM conceals a Pandora’s box of potential problems that can ensnare users (see table on p.3). Because IM operates at the blurred boundary between work and home life, users are often less guarded than when using email and liable to treat IM conversations as a quick 'chat' rather than as on-the-record exchanges. This is compounded by many users’ habit of switching from work-related to personal use and back again, harnessing the same public IM or enterprise system for both.

Moreover, IM’s inherent ‘throwaway’ feel makes it a prime target for cyber-criminals. They know many businesses are blissfully unaware of IM’s vulnerability to the same cyber-threats as email and web. They know many organisations simply don’t realise IM has to operate within the same legal and regulatory parameters as other protocols – even where employees use consumer IM software for work purposes, off-site and out of hours. And they’re highly attuned to the corollary of all this - that IM is often imperfectly monitored and controlled by businesses.

---

1. In the recent emedia/Symantec.cloud survey, 44% of respondents said they either already had a UC package in place or were looking to deploy one in the next 12 months.
2. Two-thirds of users utilise IM for both business and private purposes ('The Hyperconnected – Here They Come!', IDC 2008).
<table>
<thead>
<tr>
<th>Type of risk</th>
<th>Subcategories</th>
<th>Characteristics, etc</th>
</tr>
</thead>
</table>
| Non-compliance | • Legal requirement to produce records of IM conversations (e.g. in court cases)  
• Failure to protect employees from inappropriate material sent via IM from internal or external sources | • Contravention of legislation and regulations on e-discovery, Acceptable Usage Policy, etc  
• Potential outcomes: legal actions; court fines; negative publicity |
| Data leakage    | • Accidental (active): confidential information communicated to a third party because sender unaware of its sensitive/restricted nature  
• Accidental (passive): confidential information intercepted because transmitted unsecured/ unencrypted  
• Deliberate: confidential information wilfully disclosed to a third party | • Data frequently lost as a result of (often illegal) file-sharing  
• Hacker may ‘sniff’ (i.e. electronically eavesdrop) IM messages sent ‘in the wild’ until valuable data detected in a message or attachment  
• Potential outcomes: loss of competitive edge, customer confidence and corporate reputation |
| Cyber-threats   | • Viruses, spyware, trojans and other malware, e.g. hidden in files attached to apparently innocuous messages, or in infected websites accessed via URL links contained in messages  
• SPIM, the IM equivalent of unsolicited emails or ‘spam’  
• Phishing messages impersonating banks etc and asking for personal/ financial data | • Messages often appear to come from a trusted source, as they are typically propagated via buddy lists  
• In 2010, an IM message entitled ‘Is this your picture?’ enticed users to click on a link to a website where a virus downloaded itself  
• Potential outcomes: loss of confidential data; infected computers recruited to ‘botnets’; loss of bandwidth; financial loss |
| Inappropriate use | • Use of Public IM for personal communications  
• Use of enterprise IM systems for personal communications  
• Use of IM as a medium for cyber-bullying, sexual harassment, etc | • Exploitation of informal, immediate, often unmonitored nature of IM  
• In 2006, a US congressman resigned following allegations about sexually suggestive IM messages  
• Potential outcomes: loss of productivity; court fines; damage to corporate reputation |

Table: Key IM Threats to Businesses
Impasse: The Policy Problem
Given the range of dangers that IM can expose you to, it’s easy to sympathise with the blanket ban on IM once famously imposed on White House staff. Since businesses may be vicariously liable even where specific abuses by employees are expressly forbidden – and even where the software used wasn’t actually provided by the business – this might look like the only sensible decision.

But a ban can have precisely the opposite effect from the one intended. In view of IM’s ubiquity, such a step is almost certain to be ineffective – quite apart from the commercial cost of taking such an extreme measure. Realistically, many of your employees will use IM for work purposes, whatever policy you put in place. Perhaps it’s better to retain some element of control than push IM underground where it can’t be controlled at all.

So is there a way out of the policy impasse? Above all, can you pinpoint a way forward that enables you to:
1. Authorise and encourage – use of IM by employees to the benefit of your business.
2. Frame/implement an acceptable use policy customised to your organisation’s needs.
3. Avoid the expense of investing in an enterprise-grade solution.
4. Reduce all IM-related risks that could undermine your business.

An Instant Cure
Releasing IM’s potential doesn’t just mean putting a clear policy in place. It also means having the ability to put that policy into effect. It means, too, being capable of meeting the challenge of cyber-criminals who increasingly mix and match their vectors of attacks, deploying common techniques across email, web and IM and integrating elements of all three in their assaults on business.

All these requirements are addressed by Symantec.cloud’s fully managed Instant Messaging Security Service. Enabling businesses to utilise public IM clients with increased safety and security, and seamlessly interlocking with Symantec.cloud’s Email and Web Security Services, its core capabilities include:

• A policy-building engine that allows rules to be adjusted down to group or individual employee level.
• Content control that can block messages identified as violating your acceptable use policy and help to protect you against data loss.
• Advanced malware detection and URL filtering, based on Skeptic™ predictive technology, which is able to identify threats from known and previously unknown sources.
• Full message logging plus comprehensive report generating capabilities, facilitating audit/e-discovery requirements.

The result? IM usage with minimal risk – and an instant cure to your instant messaging dilemma.

BUSINESS AT RISK!

Only 5% of organisations log and store all their IM conversations and...

Only 15% check/audit federated partners in relation to IM use and...

Just 17% check partner organisations’ anti-malware controls in place for IM.

1 http://www.topnews.in/no-instant-messaging-obama-s-white-house-2111699
Office Locations

EUROPE

HEADQUARTERS
1270 Lansdowne Court
Gloucester Business Park
Gloucester GL3 4AB
United Kingdom
Main +44 (0) 1452 627 627
Fax +44 (0) 1452 627 628
Freephone +44(0)800917 7733

DACH
Wappenhalle,
Konrad-Zuse-Platz 2-5,
81829 München,
Deutschland
Tel +49(0)89 94320 120
Support +44(0)870 8503014

NETHERLANDS
WTC Amsterdam
Zuidplein 36/H-Tower
NL-1077 XV
Amsterdam
Netherlands
Tel +31 (0) 20 799 7929
Fax +31 (0) 20 799 7801

LONDON
3rd Floor
40 Whitfield Street
London, W1T 2RH
United Kingdom
Main +44 (0) 203 009 6500
Fax +44 (0) 203 009 6552
Freephone +44(0)800 917 7733

NORDICS
St. Kongensgade 128
1264 Copenhagen K
Danmark
Tel +45 33 32 37 18
Fax +45 33 32 37 06
Support +45 88 71 22 22

BELGIUM/LUXEMBURG
Symantec Belgium
Astrid Business Centre
Is. Meyskensstraat 224
1780 Wemmel
Belgium
Tel +32 2 257 13 00
Fax +32 2 257 13 01

AMERICAS

UNITED STATES
512 Seventh Avenue
6th Floor
New York, NY 10018
USA
Toll-Free +1 866 460 0000

CANADA
170 University Avenue
Toronto ON M5H 3B3
Canada
Toll-Free +1 866 460 0000

NETHERLANDS
WTC Amsterdam
Zuidplein 36/H-Tower
NL-1077 XV
Amsterdam
Netherlands
Tel +31 (0) 20 799 7929
Fax +31 (0) 20 799 7801

ASIA PACIFIC

HONG KONG
Room 3006, Central Plaza
18 Harbour Road
Tower II
Wanchai
Hong Kong
Main: +852 2528 6206
Fax: +852 2526 2646
Support: +852 6902 1130

SINGAPORE
6 Temasek Boulevard
#11-01 Suntec Tower 4
Singapore 038986
Main: +65 6333 6366
Fax: +65 6235 8885
Support: +800 120 4415

AUSTRALIA
Level 14
207 Kent Street
Sydney NSW 2000
Australia
Main: +61 2 8220 7000
Fax: +61 2 8220 7075
Support: 1800 088 099

JAPAN
Akasaka Intercity
1-11-44 Akasaka
Minato-ku
Tokyo 107-0052
Japan
Main: + 81 3 5114 4540
Fax: + 81 3 5114 4020
Support: +531 121917
About Symantec.cloud
More than 31,000 organisations ranging from small businesses to the Fortune 500 across 100 countries use Symantec.cloud’s MessageLabs services to administer, monitor and protect their information resources more effectively. Organisations can choose from 14 pre-integrated applications to help secure and manage their business even as new technologies and devices are introduced and traditional boundaries of the workplace disappear. Services are delivered on a highly scalable, reliable and energy-efficient global infrastructure built on 14 data centers around the globe. A division within Symantec Corporation, Symantec.cloud offers customers the ability to work more productively in a connected world.