Six Steps to Reduce Risk and Improve Control over Real-time Communications

This whitepaper was written for Quest Software by TechTarget Windows Media Group Custom Media.

QUEST SOFTWARE®

SIX STEPS TO REDUCE RISK AND IMPROVE CONTROL OVER REAL-TIME COMMUNICATIONS

EXECUTIVE SUMMARY

Instant messaging (IM) and other real-time communications are widely used throughout most enterprises today, but their use remains largely unmanaged. That puts organizations at risk for loss of intellectual property and crucial data, rising costs around e-discovery, fines for noncompliance, legal exposure from inappropriate use, and network vulnerabilities resulting from unauthorized access. To mitigate real-time communications risks and maintain accountability, organizations must secure buy-in from top management, establish strong policies for message archiving and appropriate use, and adopt good tools to enforce those policies. This paper identifies key concerns and identifies six steps to improve control over organizational use of real-time communications.

KEY CONCERNS ABOUT REAL-TIME COMMUNICATION IN BUSINESS TODAY

IM has emerged as a key channel of business communication, and its use is widespread and growing. Research firm Gartner estimates that by 2010, 90 percent of people with business email accounts will also have IM accounts. It's no wonder that employees have embraced IM. Compared to email, it offers users instant gratification: they can "see" who is online, send short messages, and get fast answers.

Initially, employees relied on IM primarily for casual exchanges, pinging each other about lunch plans, or checking in with friends and family. But many found that IM also fits well with the way they like to do business. Because IM eliminates the email latency problem—there's no way to know when a recipient will actually receive and read the message, let alone respond to it—IM allows for faster problem solving and decision making. The resulting boost in productivity has led to increasingly strategic use. At some Wall Street firms, for example, brokers are authorized to accept and issue stock trade orders via IM.

Despite potential efficiency gains, there is a serious downside to real-time communications use, which includes public IM, enterprise IM, conferencing, voice over IP (VoIP) and mobile messaging. It is exposing organizations to significant security risks. Left unmanaged, IM use leaves the corporate network vulnerable to viruses and worms. It can result in the loss of intellectual property (such as trade secrets around R &D efforts) and leakage of confidential information (such as impending acquisition plans). Other risks associated with unmanaged real-time communication use include: loss of sensitive data pertaining to customers and employees; legal exposure resulting from IM messages that contain inappropriate content; and fines for noncompliance with government regulations that mandate record retention, among other measures.

Organizations typically have some awareness of these risks around e-mail use. Many—particularly those in highly regulated industries such as financial services—have taken measures, such as message archiving, to mitigate the risks. But most organizations have not adequately applied those same measures to IM and other real-time communications platforms. To effectively manage business risk, organizations must get their arms around multiple forms of communication: e-mail, public IM, enterprise IM, mobile messaging, conferencing and VoIP. Failure to do so can result in fines for non-compliance, loss of critical data and intellectual property, damaged reputations, and further liability.

WHY IS BUSINESS RISK DIFFICULT TO UNCOVER?

According to the 2008 CSI Computer Crime and Security Survey, It's difficult to assign real costs to risks, because organizations don't explicitly incorporate the cost of the vast majority of computer security incidents into their accounting (as opposed to, say, accounting for the "shrinkage" of goods from retail stores). But the survey estimates the cost of losses resulting from various types of security incidents at $288,618 per respondent, up from $167,713 two years ago. In fact, while many security assessments and audits uncover business risks associated with real-time communications, many other risks have simply flown under the radar—something that hardly any business can afford to miss.

Some key factors led to this situation, making business risks difficult to uncover.

Separate silos hindered communication. One reason why real-time communications use grew quickly out of control is that most companies operate separate silos for e-mail, IM, mobile messaging, VoIP, and so forth. In other words, one team is responsible for e-mail; another handles mobile messaging; a third team deals with VoIP communications. Managing technologies this way is commonplace and can be an efficient means of organizing work. But the silo approach makes it hard for organizations to get a handle on the big picture. That makes it difficult to ensure appropriate use, block viruses and worms, minimize legal exposure, archive messages for compliance, and apply usage policies across the board. In short, silos make it nearly impossible for an organization to gain a unified view of its communications technologies. Without that unified view, businesses can't move forward to establish and enforce strong policies and maintain accountability across the organization.

"The 2008 CSI Computer Crime and Security Survey estimates that security incidents cost $288,618 per respondent"

Good tools were lacking. Until relatively recently, tools to centrally manage real-time communications across the enterprise simply didn't exist. To get a handle on real-time communications use, some organizations attempted to put technical controls in place. They blocked certain ports at the firewall. They set up sniffers to keep an eye on traffic flowing into and out computers attached to the network.

They logged IM messages. But lacking an organization-wide mandate, controls were implemented locally. With everyone doing their own thing, there was no overall accountability, and no way to get a handle on the big picture and achieve centralized control of real time communications.

IM came in under the radar. Also contributing to the lack of governance around real-time communication is the way IM entered the workplace. The technology emerged through unofficial channels. Instead of being ushered in by IT or management, IM took off at a grassroots level, when employees signed up for free accounts on public IM networks such as AOL Instant Messenger, MSN Messenger, and Yahoo! Messenger. Unlike corporate e-mail, which requires IT professionals to set up accounts and issue employee e-mail addresses and passwords, public IM is simple, free, and widely available. And because it was designed to use existing communications channels and thus evade firewalls and other perimeter security devices, IM was initially challenging for IT to gain control of. That meant use of public IM networks rapidly expanded, as employees encouraged colleagues, friends, and business partners to get in on it the new communications medium. While IT organizations were not unaware that employees were using public IM networks, many underestimated the extent of use. As a result, they did not adequately protect against worms and viruses entering their networks through this new communications channel. IT also overlooked threats arising from peer-to-peer networks such as BitTorrent, OpenNapster, and Gnutella. Because P2P networks are designed to share files housed on the computers of individual users, they make it difficult to verify whether the source of the files is trustworthy.

"While IT organizations were not unaware that employees were using public IM networks, many underestimated the extent of use."

The boss was in the dark. Worst of all, there was often a sense that top management simply wasn't paying attention to real-time communication use and as a result did not recognize the significant business risks associated with it. Some high-ranking executives had limited, or no awareness of IM use at all. Others simply ignored the new communications medium. Overall, senior managers failed to grasp the risks it presented around information security and information retention. Nor did they understand the negative impact IM could have on productivity, as

employees wasted time exchanging frivolous messages. Many top managers falsely assumed all users could be trusted. And they did not recognize the need to archive IM messages for e-discovery and compliance. This lack of understanding meant they could not maintain accountability and ensure compliance and appropriate usage across their organizations.

Employees put their employers at risk. Employees made some miss steps too, and that exacerbated the problem. They failed to understand that employers could be held liable for inappropriate IM content, such as messages that contained statements that could be construed as sexual harassment. Because no one had told them otherwise, many employees assumed they could do whatever they wanted. Others were warned by IT staff not to use public IM networks, but ignored the warnings because they believed that IT had no right to govern their behavior or ban public IM use. What's more, even in organizations where e-mail use was tightly governed, there was a widespread perception that e-mail rules don't apply to public IM networks. That led to a free-for-all situation. Employees wasted time chatting with friends, family and co-workers, sending and receiving frivolous messages. Even those who were using IM to conduct real business often put their organizations at risk, inadvertently revealing sensitive customer and employee data or trade secrets in the messages they sent. Without thinking, they used IM to ask time-sensitive, business critical questions, such as: "Have we announced the acquisition yet? I have an investor on the line."

"Even in organizations where e-mail use was tightly governed, there was a widespread perception that e-mail rules don't apply to public IM networks. That led to a free-for-all situation."

Keeping up with compliance. At the same time that employees were engaging in this free-for-all of real-time communications, the regulatory environment was growing increasingly complex. There are dozens of laws that impact real-time communications use. Which ones an organization is subject to depends largely on what industry it's in, or whether or not the company is publicly traded. The Federal Deposit Insurance Corporation (FDIC), for example, mandates that member banks and financial institutions retain and review all electronic communications. The Sarbanes-Oxley Act requires publicly traded companies to make historical communi-

cations available for audit. The Freedom of Information Act stipulates that federal government agencies and contractors must control and retain all records. HIPAA mandates that healthcare-related organizations protect all information pertaining to patient healthcare records. And the Gramm-Leach-Bliley Act requires companies in the financial industry to protect customer financial data. Demonstrating compliance with these rules and standards—and those of many other regulations--presents an ongoing challenge for all organizations. The consequences of failing to meet that challenge are clear: Out-of-control real-time communications can lead to fines for non-compliance, lost reputation, lost intellectual property, and further liability to your business.

Real-time communications are out of control. From technical vulnerabilities, to inappropriate use, fines for noncompliance with government regulations, and damage to reputation, real-time communications use is putting organizations everywhere at risk. The free-form use of all communications applications and protocols with few constraints on usage has created an out-of-control situation. With no central accountability and oversight, no one knows what is going on in the network.

SIX STEPS TO REIN IN REAL-TIME COMMUNICATIONS

1. Enforce policy using good technologies wherever possible. Policies provide guidelines that prevent employees from leaking sensitive data and using abusive or otherwise inappropriate language in the messages they exchange. Appropriate use policies should also define which IM services employees are permitted to access, who they can IM with, what they can and cannot discuss, and when they are allowed to use IM. Policies must be enforced by tools, and applied across all communications platforms, based on a single network profile for each employee. Good tools allow management to prevent inappropriate conversations by using key word and phrase filters to block people from discussing certain topics, such as a top secret R&D project. Letting employees know that IM conversations—and any message they type—are being recorded, regardless of whether they are carried out on email, public IM or other communication platforms, helps ensure appropriate use. In turn, clear, enforceable corporate policies on use generate the added benefits of reducing wasted time and boosting productivity. To establish such policies, it's imperative that organizations put together a security committee that includes representatives from legal, IT, security, HR, audit, and compliance.

"Good tools prevent inappropriate conversations by using keyword, and phrase filters."

2. Protect against data loss. It's virtually impossible to prevent leakage of confidential information unless conversations with outsiders are controlled across all communications platforms. Confidential information includes sensitive data such as customer credit card numbers and employee social security numbers. Also crucial to protect are things like financial results that have not been officially released, and news of product launches or planned acquisitions prior to formal announcements. To guard against all kinds of data loss, organizations should use tools that support filtering and tagging, preventing employees from leaking information deemed confidential.

3. Block unwanted protocols and malware. Organizations that rely on real-time communications to conduct business must take appropriate measures and use good tools to defend themselves against IM borne viruses, worms, phishing, spam, and other threats that could infect their networks. That includes filtering all IM traffic for viruses, spyware, and worms; checking for messages that contain unknown

URLs against a list of disallowed Web addresses, and blocking them if necessary. It's also essential to correlate end user identities from the corporate directory to user handles and phone number for all real-time communications platforms. That can help prevent rogue users from impersonating others and falsely representing the company.

4. Preserve messaging for compliance and archive it in a single repository. Archiving messaging in a single repository reduces the burden of e-discovery by eliminating the need to manage and search multiple sources. Most important, it ensures an organization maintains a complete record of all communications, easing compliance with federal and state mandates. But determining what to archive and how long to archive it for, is challenging for most organizations. Given the vast array of data, including log files and backup files, it's difficult to know where to begin. Good tools designed to deal with information overload can help organizations identify what to preserve, including IM conversation transcripts, voice and conferencing logs, file transfers, SMS communications, BlackBerry PIN-to-PIN messages and call logs. An effective archiving strategy enables organizations to stay compliant and legal. And it eliminates the high cost of engaging an outside provider to do e-discovery.

"Letting employees know that IM conversations are being recorded helps ensure appropriate use."

5. Enhance visibility and oversight. Effective management of real-time communications provides a centralized view of risks across all electronic means of communications. By eliminating multiple silos for record retention for example, organizations can reduce the total of ownership around operating and managing real time communications platforms. While managing these platforms is challenging, the risks themselves are not new. They are much the same as those associated with email. With IM and other real-time communications, it's really only the transportation medium has that has changed. A unified view of all communications platforms enables organizations to establish and enforce policies across multiple silos, reaping new productivity benefits from real-time communications.

6. Maintain accountability. Establishing policies is a crucial first step, but the only reasonable to way to actually enforce those policies is to put technical controls in place. Some companies attempt enforcement by asking supervisors to keep an eye

on employees. But relying on human resources alone simply isn't realistic. Tools can automate enforcement, enabling management to address security risks proactively and reactively. They can block an employee from sending an inappropriate message in real time. Or they can take action behind the scenes, automatically alerting managers when an employee sends a message deemed inappropriate—even though the employee remains unaware of what is happening in the background.

THE BOTTOM LINE ON MANAGING REAL-TIME COMMUNICATIONS

IT professionals play a pivotal role in implementing tools to help enforce policies. But without the backing of top management, tools alone can't address the challenges of real-time communications. It's imperative that senior managers lead the effort by taking the following six steps:

- Enforce policy using good technologies wherever possible. Specify employee guidelines for real time communication use and implement tools to enforce those guidelines.
- Protect against data loss, including trade secrets and sensitive data about employees or customers.
- Block unwanted protocols and malware. Filter all traffic, and map user IM handles to user identities in a single corporate directory.
- Preserve messaging for compliance and archive it in a single repository, simplifying the e-discovery process and controlling costs associated with it.
- Enhance visibility and oversight, enabling a centralized view of business risks across all means of electronic communication.

Protecting real time communication and mitigating business risks associated with it requires organization to make a significant investment, and that directive must come from the top. ■

ABOUT THE AUTHORS

Jennifer deJong: An independent technology journalist for more than 20 years, Jennifer deJong has written for professional audiences on wide range of topics including return on technology investments, aligning software development efforts with strategic goals, and mitigating security risks. Her articles have appeared in *Software Development Times, Information Week, VAR Business, Investor's Business Daily, Inc. Technology* and on www.monster.com. Jennifer has also developed white papers, case studies and e-newsletters for technology firms including Microsoft, BEA, IBM and Software AG.

Kevin Beaver: Founder and president of Principle Logic, LLC. Kevin has more than 15 years of experience in IT, specializing for the past 9 years in information security. His areas of information security expertise include network and messaging security, security assessments, security policy development, HIPAA security readiness, and incident response. You can read more about Kevin Beaver and the books he has written at: http://www.principlelogic.com/about.html

ABOUT THE SPONSOR

About Quest Policy Authority for Unified Communications: Quest Policy Authority for UC enforces policies on and archives instant messaging and other real-time communications. Its flexible architecture blocks unwanted protocols, improves security and hygiene, protects sensitive data, and enforces regulatory compliance. Policy Authority captures IM and file transfers, PIN-to-PIN and SMS messages further helping IT organizations create a true compliance archive.

Policy Authority is part of Quest's solutions for Archiving, e-Discovery and Compliance which help you control the huge repository of data your organization has that must be managed securely and efficiently through email retention and file storage optimization, messaging compliance and policy enforcement. Quest can help you capture, retain, discover and manage this data to satisfy legal and regulatory requirements and control storage costs. For more, visit www.quest.com/unified-communications/archiving-ediscovery-compliance.aspx.

About Quest Software: Quest Software, Inc., a leading enterprise systems management vendor, delivers innovative products that help organizations get more performance and productivity from their applications, databases, Windows infrastructure and virtual environments. Through a deep expertise in IT operations and a continued focus on what works best, Quest helps more than 90,000 customers worldwide meet higher expectations for enterprise IT. Quest provides customers with client management as well as server and desktop virtualization solutions through its subsidiaries, ScriptLogic and Vizioncore. Quest Software can be found in offices around the globe and at www.quest.com.