Endeavors TECHNOLOGY

Trusting Technology

Secure Instant Messaging is Ready for Enterprise Adoption

A White Paper |

Gregory Alan Bolcer
Chief Technology Officer, Endeavors Technology, Inc.

Instant Messaging (IM) is proving to be no longer a consumer phenomenon. With over 40 million enterprise users, it is becoming de rigueur as a real-time business collaboration tool.

To date, enterprises have had to make the hard choice between inside-the-firewall, self-managed solutions with little or no external interaction or an outside-the-firewall approach with little or no security, trust, or control. Enterprises refusing to land on either side of the issue have resorted to draconian measures to lock down IM use at a great expense to their users. This has met with very little success due to the ease of which users can circumvent these policies.

This white paper covers some of the social and technical issues surrounding this hot button topic as well as some of the choices enterprises are currently making. These choices become increasingly important as history provides us with a not-so-subtle guide to adopting technologies that work across trust boundaries, provide cross-organization benefits, and yet allow IT control. Like enterprise email adoption from 1985-1995 or Web server adoption from 1991-1997, enterprise instant messaging is at a point in its adoption cycle where organizations are starting to see value in extending it securely beyond their current borders.

ABOUT THE AUTHOR

GREGORY ALAN BOLCER is a co-Founder of Endeavors Technology, Inc. and is currently its Chief Technology Officer.

At Endeavors Technology, Dr. Bolcer founded the Magi™ project, a lightweight, open protocol, thin server infrastructure for forming ad hoc, peer-to-peer networks and accessing embedded systems through standard Web protocols.

Prior to co-founding Endeavors Technology, Dr. Bolcer's research team at UCI received $4 million in grants from the Defense Advanced Research Project Agency (DARPA). His project at one point was the largest Java-built, non-Sun Microsystems project in the country. He was one of the key working group participants and co-Author for the widely supported Simple Workflow Access Protocol (SWAP/WF-XML) extensions to HTTP/1.1 and WebDAV (the Web Distributed Authoring and Versioning Protocol).

Dr. Bolcer has a PhD and BS degree in Information and Computer Science from the University of California, Irvine, and an MS degree from the University of Southern California.

A History of "Crossing the Trust Boundary"

"`Those who cannot remember the past are condemned to repeat it', George Santayana (1863-1952) U.S. philosopher, poet. I've got news for Mr. Santayana: we're doomed to repeat the past no matter what. That's what it is to be alive."

– Kurt Vonnegut.

A ***trust boundary*** is a physical or conceptual barrier in which internally, a level of policy and control can be enforced, but the ability to do so rapidly degrades once beyond it. A network firewall is the best example of a trust boundary. Other trust boundaries can be social such as "friends and family" or professional contacts at other companies. You implicitly trust these colleagues not to misuse information you share with them.

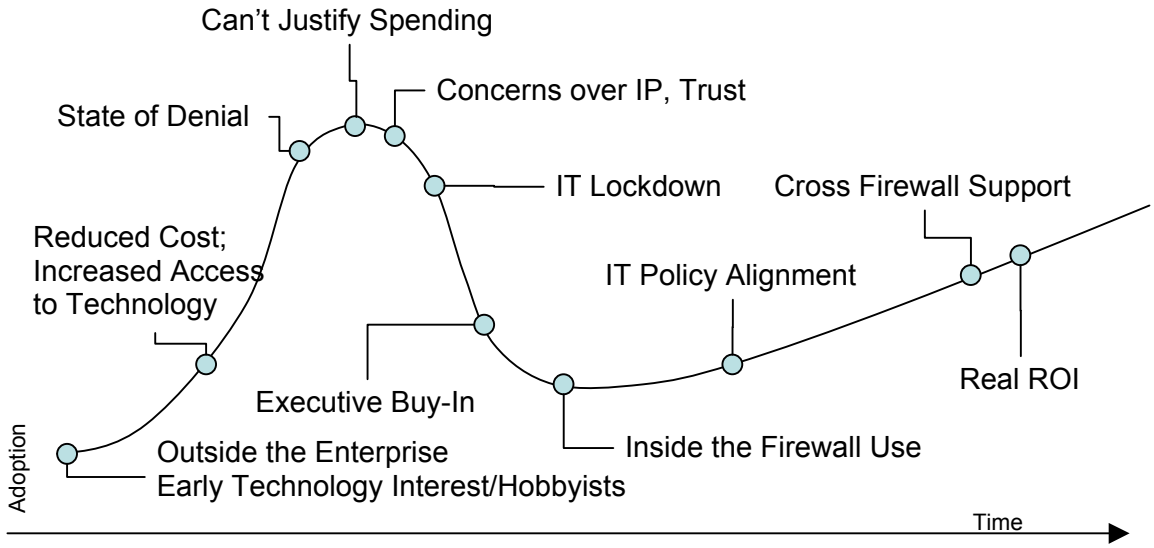
Social trust networks, by their nature, are much more dynamic than technical ones as participants are constantly evaluating and redefining their trust boundaries according to comfort levels and past experience. Individuals can choose, on the fly, whether or not to share information based on whether or not someone can be trusted to keep their co-worker in confidence.

The bar for redefining technical trust boundaries, however, isn't so easily hurdled. Again, taking the example of a firewall, the IT staff have little motivation to provide remote access for a 3rd party in another company, even if sharing information with that individual is of very high value to the company as a whole. There is very little incentive for opening up access when the tools to carefully limit the scope of interaction require careful consideration for even the smallest of changes and the dictate for doing is handed down rather than building up a trusted relationship from the bottom up. Enterprises have been dealing with these issues for close to two decades now—first with email, next with Web server adoption. Now, IM appears to be the next cross-firewall enterprise technology that's heading for primetime corporate use.

The Adoption Cycle

The adoption cycle into widespread enterprise use is easy to track for a variety of new technologies. The story is always the same:

- Early interest in technology.
- Free or nominal availability of software for experimentation.
- Propagation of tools without knowing how widespread the usage is.
- Enterprises can't justify the ROI on spending for experimental technology.
- The cost and adoption barriers are lowered for individual use.
- Bottom-up support in the corporation occurs due to efficiency or expedience.
- Executive support for the technology grows due to end use.
- IT tries to bring the technology under enterprise control first by:
    - Locking down or disallowing it
    - Permitting inside the firewall only use, and then
    - Aligning the technology with other policies and practices across the whole enterprise



Both email and the World Wide Web have already matured as enterprise tools through this adoption cycle. Other non-software technologies like enterprise wide laptop deployments are starting to justify real ROI numbers. PDAs, mobile phones, and even 802.11 wireless network cards have enjoyed first wave adoption into the enterprise, but as networking and data access using these devices becomes more ubiquitous, enterprise concerns about controlling access and locking down usage are starting to appear as major concerns.

For instant messaging, some of the early movers in the enterprise space are coming out of the lockdown phase and starting to evaluate inside-the-firewall use with servers like Lotus Sametime™ or Jabber™. These products, however, only provide a partial solution. Instant Messaging needs to be consistent with other collaboration tools within the enterprise like secure Web or email. Misalignment of these strategies can be the cause of major IT and user headaches at the expense of the speed by which the organization communicates internally and externally with its partners.

Email as the Cross-Enterprise "Killer App"

Not many people remember the early beginnings of email. Email use was typically limited to government funded research labs, military, universities, and some non-research government use. As military contractors became more engaged with their government counterparts, email became a useful tool for efficient electronic information sharing.

The problem at the time was the information would enter into the enterprise in electronic form, but then be redistributed through the standard paper-based information processes. Large enterprises needed to find a way to bring the efficiency and ease-of-distribution benefits inside the corporation. In April 1982, Lotus Development Corp. was formed by Mitch Kapor to enable greater collaboration across an enterprise. The focus of the company until 1989 was the single desktop Lotus 1-2-3 desktop tool.

Along the way, Lotus discovered that enterprises weren't just buying Lotus for their desktop tools, they were buying Lotus for their ability to support email inside the enterprise. In February 1991, Lotus acquired, what would become their most successful product, cc:Mail. When IBM bought them in 1995 for $3.5 Billion, the stated goal was to marry IBM's market share in enterprise-wide hardware with Lotus' unique groupware expertise. The real goal was to gain access to the tens of millions of corporate email users.

Early enterprise cc:Mail deployments were entirely limited to inside the corporation. Workers were trusted to send anything and everything they wanted as long as the recipient was another cc:Mail user within the enterprise. Outside the enterprise, email wasn't allowed as most organizations felt that email could be used to leak intellectual property and corporate secrets. Users that needed or wanted to communicate outside of the corporation were faced with either: 1) *trying to convince IT and executives that they had a legitimate need in the face of un-interoperable email packages and incompatible protocols*, or 2) *circumventing IT lockdown of outside-the-firewall email through alternate clients or home email use.*

At that time, home use was beginning to blossom. Sky Dayton founded Earthlink in March 1994 and by May 1995 had made the process of obtaining direct, open Internet access as easy as installing a software package. In the same year, AOL had already reached 1 Million subscribers and allowed links to the Internet for the first time. The "killer app" for these services was email un-encumbered by a single company's recipient restrictions.

As these public email services became popular, it was very common for most users to have multiple email accounts—one for inside the company email and one for outside. Workers began to discover that personal email was a tremendous time saving tool for sharing information across companies. By early to mid-1990's, enterprise IT staff had to concede that inside-only email restrictions as a policy was failing miserably.

"Blessed" corporate email was being used less and less. Personal email was becoming the standard as it was less likely to get "bounced" (i.e. get through without arbitrary corporate restrictions on both the sending and receiving sides). A few attempts were made to "lock down" personal email use. But in the end, IT set about the task of putting in the tools and safeguards of protecting enterprise intellectual property and information rather than preventing its use altogether. Mail system deployments that originally allowed outside delivery as an alternative were now expected to include such capabilities out-of-the-box.

Network Effects on the World Wide Web

Pick your favorite cutting-edge enterprise. If you were to travel back in time, between 1991 and 1993, and find the CIO or IT manager within that organization and try to convince him of the benefits of using the World Wide Web, you'd be surprised at the issues he would raise. The concept of a Web server would seem entirely foreign to him, as it would be using a machine that: a) the enterprise purchased, b) is unprotected outside of the firewall, c) is for the benefit of users that weren't under his corporate control, and d) is for sharing internal company files and documents. In fact, if you were to set up a Web server you probably would be reprimanded for misuse of corporate equipment or even worse, dismissed for making it easy to divulge or steal corporate secrets.

Tens of millions of Web servers later, it's hard to imagine not having a Web presence for disseminating critical information to customers and partners. So, what happened? How did the Web overcome this adoption barrier to show the cost was negligible compared to the benefit of providing that information service?

Sometime in the Fall of 1993, there were over 200 known HTTP servers running on the Internet. Most of these were research sites for disseminating information to other collaborators. By 1994, the world's first full time Web server (info.cern.ch) was starting to track up to 1000 times the traffic than it had 3 years earlier. Browsers like Viola and later Mosaic were starting to incorporate more robust graphics and layout. O'Reilly and Spry announced their "Internet in a Box" product, which helped increase the adoption and take up for "hobbyists" and home use.

In April that same year, Jim Clark and Mosaic author, Marc Andreesen, founded Netscape. In October, they posted their first Netscape Navigator on the net. In parallel and out of the same research center, the National Center for Supercomputing Applications, Rob McCool's open source Web server implementation was being widely distributed. By February of 1995, McCool's NCSA HTTP server had become the most popular server on the Web.

Many Webmasters had developed their own extensions to the open source, and a small group gathered through email for the purposes of sharing and standardizing improvements called the Apache Group. Their work on the Apache HTTP server would consequently lay the groundwork for Apache to be the world's most popular Web server. The existence of a best-of-breed, evolving Web client and server set the stage for early enterprise adoption.

In the beginning, developers or IT workers used their own machines as test beds. They would compile, configure, and experiment with their own personal Web server and share the IP address or internal machine name with their buddies or co-workers. Developers had the luxury of hosting their own server as they typically had a static IP address, a fixed number. Internally, users would share documents and files on their servers with co-workers. Others were even more daring and provided both public and password protected access outside the firewall so that they could download and use information from home or on the road. Eventually, even some corporate brochures and information were informally made available.

A funny thing happened along the way. It turns out that the ability to pull information from a remote site was just as important and often more convenient than having someone email the information after requesting it.

Even more important, users would refer other users that the enterprise didn't even know about to the site to collect more information. This causes a *network effect*.

A network effect can be explained this way. Suppose you have a telephone and no one else does. The network effect is zero. Every phone you add increases the total endpoints that can receive a phone call and the network effect becomes greater. It works the same way with the Web. The number of Web servers and clients proliferated. The quality of information increased. The usability and access dramatically improved. This caused the *value of the network to go up exponentially*.

It was this cumulative effect that caused the Vice President of Marketing or Sales to suddenly realize that the 15,000 or so downloads from their Web site that month were potential partners and customers that he or she wanted to reach. It was this epiphany that caused the Web to become a strategic business tool for communicating with customers and partners.

IM Breaking the "Hurry Up and Wait" Business Cycle

Revisiting our adoption curve, we can walk through the various points for enterprise instant messaging:

- IM clients are freely available for download from multiple services including AOL®, Yahoo!®, and Microsoft®/MSN®.
- Most enterprises have moved past the "denial" stage and recognized that they potentially have a large internal IM user base that they need to bring back under IT control.
- Many enterprises haven't considered budgeting IM products and are just now starting to survey their own requirements. In addition, emerging IM tools are proving to be a cost cutting mechanism.
- Concerns about information leakage, legal exposure, identity spoofing, or even cyber-loafing have caused companies to attempt to lock down IM use.
- IM has recently started to receive executive sponsorship largely due to the tendency for email and voicemail pile up, the majority of business phone calls never reaching their intended recipients, and the need for a simpler, quicker communication alternative. According to Gartner, 42% of business Internet users use IM in the workplace even though 70% of IT departments don't. Gartner also estimates that IM potentially may reduce voicemail up to 15% and email up to 40%. This is starting to tantalize companies into considering IM because these reductions have real costs associated with them across an enterprise.
- Leading-edge enterprises are starting to consider and deploy inside-the-firewall IM solutions. Similar to the email and the Web adoption cycle, they are finding that IM across the firewall is a necessity.
- This brings us to where we are today in the adoption cycle. Enterprises are now starting to look for ways to bring their IM solution in line with email and Web browsing. They generally recognize the value of IM to the enterprise, and are willing to budget accordingly to find a solution that aligns with their security and auditing needs.

Many enterprises are revisiting old questions of auditing, content filtering and personal use. They are using instant messaging adoption to revisit their policies in the same way many have done before for outside Web and email use. When considering this type of deployment, it's important to ask:

What percentage of email is personal versus work related?
What percentage of Web browsing is personal versus work related?

You'd be surprised to find the answer to these questions yields standard percentages. An employee with equal access to phone, fax, email, Web browsing, mail, and IM will use all channels to communicate. Out of a 50-hour workweek, CMP estimates that 3 hours a week are spent on personal communications, or about 6%, independent of medium.

Instant Messaging is the exact same way. Typically there is an initial honeymoon period where users explore new and old personal contacts and social networks, but after that, interaction always ends up following established work patterns in the end because that is the context in which users interact. Related to the "personal use" issue is the intellectual property. Another sticky issue is that unregulated communication medium will allow intellectual property theft or leakage of confidential company information. IM tools that allow auditing and content filtering at the same level as email or Web blocking are starting to become available. As we've seen with Web and email, IM users will adjust their behavior if they know network traffic is audited.

In the end, enterprises will find that support for instant messaging is valuable to the enterprise in order to stay competitive, cut costs, and secure the integrity of the company. The value of commercial IM extensions to bring IM back under IT control through security and auditing is starting to make senses as a broad enterprise initiative. Like email and the Web, business is finding IM a "must have" and IT is being asked to wrap enterprise services around it.

About Endeavors Technology

Endeavors Technology grew from research carried out at the University of California, Irvine, and was partly funded by the United States Defense Advanced Research Project Agency (DARPA). Endeavors' founders and technical advisory board has an unrivaled history in developing Internet infrastructures, both as co-authors of the Web's more commonly used protocols and software, including HTTP, Web Distributed Authoring and Versioning (WebDAV) and the Simple Workflow Access Control (SWAP/WF-XML), and as team members of the Apache Web Server project.

Endeavors Technology, Inc. is a wholly owned subsidiary of Tadpole Technology plc (LSE-TAD, www.tadpole.com), which has offices in Irvine (California), and Cambridge, Edinburgh, and Bristol (UK). Endeavors' Magi technology transforms today's Web into a highly secure inter- and intra-enterprise collaboration network for the delivery and interaction of files, Windows applications and instant messaging. For further information on Endeavors' Web software, call 949-833-2800, email to info@endeavors.com,

Endeavors Technology Inc.

North America:
19600 Fairchild, Suite 350
Irvine, CA 92612
Telephone: 949 833 2800

Europe, Middle East and Africa:
Trinity House
Cowley Road
Cambridge, UK CB4 0WZ
Telephone: 44 1223 393 552

www.endeavors.com