

## Prepare Now for the Growing IM Security Threat

Lawrence Orans

A flaw in MSN Messenger shows that instant messaging (IM) presents a serious security threat. Enterprises should implement comprehensive IM policies now.

## NEWS ANALYSIS

---

### Event

On 11 February 2005, Microsoft restricted access to its MSN Messenger IM service to prevent the spread of a security-flaw exploit. Microsoft "locked out" any users not running the latest versions of the MSN Messenger and Windows Messengers clients after proof of concept of a vulnerability was posted on the Internet. Older versions of MSN Messenger and Windows Messenger do not properly handle corrupted image files. By exploiting this vulnerability, an attacker could take control of an affected system.

### Analysis

The MSN Messenger exploit highlights the risks of not establishing and implementing an enterprise IM policy. The MSN Messenger client — like those for Yahoo! Messenger, AOL Instant Messenger and other IM services — is available for download free of charge. As a result, IM is so widely used that most enterprises have no idea how many IM clients are installed on their systems or how much IM traffic passes over their networks.

Microsoft acted quickly to control this malicious-code outbreak by denying access to clients that were not up-to-date. However, the next time an IM exploit emerges, Microsoft or another IM provider may not be able to respond as quickly or as effectively. Enterprises must take responsibility for ensuring that the use of IM does not compromise their security. If necessary, they must be able to temporarily shut it down when a serious security threat emerges.

**Recommendations:** IM is now so popular that it is rapidly becoming unrealistic to block IM traffic entirely. In many enterprises, one or more business units can make a compelling case for the need to use IM. Enterprises have three options: Implement an enterprise IM solution, deploy a solution that makes it possible to build policies around public IM services, or do both. Vendors such as Akonix, IMlogic and FaceTime Communications offer solutions for instituting policies for the public IM services. (Each of these vendors is a certified partner of one or more of the services.) Many solutions that enterprises may already have installed (for example, secure e-mail, file transfer, URL filtering, firewall and proxy cache solutions) also provide IM security capabilities, though with less granular policies.

**Analytical Source:** Lawrence Orans, Gartner Research

### Recommended Reading and Related Research

- "Network Access Control Market Overview" — The market for network access control solutions is crowded, with many vendors providing point products. **By Lawrence Orans and others**
- "Protect Your Resources With a Network Access Control Process" — A network access control process will protect enterprise systems and resources from corruption. **By John Pescatore and others**

(You may need to sign in or be a Gartner client to access the documents referenced in this FirstTake.)

## REGIONAL HEADQUARTERS

---

### **Corporate Headquarters**

56 Top Gallant Road  
Stamford, CT 06902-7700  
U.S.A.  
+1 203 964 0096

### **European Headquarters**

Tamesis  
The Glanty  
Egham  
Surrey, TW20 9AW  
UNITED KINGDOM  
+44 1784 431611

### **Asia/Pacific Headquarters**

Gartner Australasia Pty. Ltd.  
Level 9, 141 Walker Street  
North Sydney  
New South Wales 2060  
AUSTRALIA  
+61 2 9459 4600

### **Japan Headquarters**

Gartner Japan Ltd.  
Aobadai Hills, 6F  
7-7, Aobadai, 4-chome  
Meguro-ku, Tokyo 153-0042  
JAPAN  
+81 3 3481 3670

### **Latin America Headquarters**

Gartner do Brazil  
Av. das Nações Unidas, 12551  
9º andar—World Trade Center  
04578-903—São Paulo SP  
BRAZIL  
+55 11 3443 1509