FDIC FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

DEPOSIT INSURANCE | CONSUMER PROTECTION | INDUSTRY ANALYSIS | REGULATION & EXAMINATIONS | ASSET SALES | NEWS & EVENTS | ABOUT FDIC

Home > News & Events > Financial Institution Letters

Financial Institution Letters

Guidance on Instant Messaging

FIL-84-2004
July 21, 2004

TO:	CHIEF EXECUTIVE OFFICER (also of interest to Chief Information Officer)
SUBJECT:	Guidance on the Risks Associated With Instant Messaging
Summary:	*The FDIC is providing guidance to financial institutions on the risks associated with publicly available instant messaging and network file-sharing. This guidance includes background information on the risks and how they can be mitigated through an effective management program.*

The Federal Deposit Insurance Corporation (FDIC) has prepared the attached guidance to assist financial institutions in protecting themselves against the vulnerabilities of instant messaging (IM) and establishing policies and procedures concerning its usage.

Instant messaging has become a popular communication channel because it facilitates real-time communication from any computer connected to the Internet by either connecting to a Web browser or by downloading free IM software. Newer versions also permit users to share files in addition to messaging. IM technology is used by financial institution employees at the workplace both officially, as approved by senior management, and unofficially, where users access IM directly from the Internet. IM access may expose financial institutions to security, privacy, and legal liability risks. Institutions should assess the risks and the business needs for IM and establish policies to allow, restrict or deny IM usage based on these risk assessments and business needs.

Customer information security guidelines require that periodic risk assessments and status reports be submitted to the board of directors. These periodic assessments and reports should include the institution's position on IM. Any control weaknesses should be identified and addressed during the normal course of business.

For more information, please contact your FDIC Division of Supervision and Consumer Protection (DSC) Regional Office or Kathryn M. Weatherby, Examination Specialist in DSC, at (202)-898-6793.

For your reference, FDIC Financial Institution Letters may be accessed from the FDIC's Web site at http://www.fdic.gov/news/news/financial/2004/index.html

Michael J. Zamorski
Director
Division of Supervision and Consumer Protection

# # #

Attachment

Distribution: FDIC-Supervised Banks (Commercial and Savings)

NOTE: Paper copies of FDIC financial institution letters may be obtained through the FDIC's Public Information Center, 801 17th Street, NW, Room 100, Washington, DC 20434 (1-877-275-3342 or 202-

416-6940).

Last Updated 07/21/2004 communications@fdic.gov

Financial Institution Letters

Guidance on Instant Messaging

This guidance identifies risks associated with public Internet instant messaging (IM)[1] and how they can be mitigated through an effective management program. Public IM may be used by employees both officially and unofficially in work environments. The use of public IM may expose financial institutions to security, privacy, and legal liability risks because of the ability to download copyrighted files. Technology vendors have released IM products for corporate use that authenticate, encrypt, audit, log and monitor IM communication. These new corporate enterprise products help financial institutions use IM technology in a more secure environment and assist in compliance with applicable laws and regulations.

Background

IM originated as a free software download for consumers in 1996. The technology provides the ability to chat on-line, as well as to share files. Public IM was not originally developed for commercial use and lacks standard security features. IM has become a popular communication channel because this software is free, easy to install and easy to use. If software is not permitted to be downloaded in a work environment, IM can still be accessed by sending messages directly from a Web browser, such as Microsoft's Internet Explorer. Employees restricted by slow home dial-up connections may take advantage of faster networks at work to access public IM and share and download files. (See Technical Note 1: IM Types.)

Risk-Management Considerations

Viruses

The lack of built-in security, the ability to download files and the built-in "buddy list" of recipients create an environment in which viruses and worms can spread quickly. This threat has additional risks to the workplace network because public IM does not travel through a central server where traditional corporate anti-virus protection software is located. Instant messaging virus protection should include network desktop and laptop solutions to handle both IM methods of delivery (Server Broker and Server Proxy). Since effective virus protection specifically for IM is still being developed, senior management will need a comprehensive anti-virus program to detect the many blended threats that currently exist with the technology.

Privacy

Public IM transmits unencrypted information, so it should never be used for sensitive or confidential information. The information is on the Internet and may be accessed by anyone. In addition, file-sharing exposes the user's Internet protocol (IP) address and increases the risk that unauthorized parties could gain access to the computer.

Hijacking

Information received by IM is not authenticated. There is no way to verify that a message really originated from the sender with whom the recipient believes he or she is communicating during the session. Chat sessions can be hijacked and users can be impersonated.

Firewalls

Firewalls should be configured to block incoming and outgoing public IM traffic. Senior management should also consider blocking known Web sites that broadcast nuisance material. This can be difficult to manage because Internet names and addresses may change and senior management may have other legitimate reasons for allowing activity based upon legitimate business purposes. (See Technical Note 2: Firewalls and Router Considerations.)

Intrusion Detection Systems (IDS)

An institution's information security program should address preventing, detecting and responding to threats. Institutions should consider the use of IDS to detect the unauthorized use of IM.[2] Intrusion detection software may be installed on primary computer systems that actively searches for and monitors Internet traffic.

Mitigating Risks Associated with IM

The numerous vulnerabilities inherent in IM dictate that senior management perform a risk assessment on the business benefit of allowing the use of public IM on financial institution networks. Financial institutions should consider the following practices regarding IM as part of an effective information security program:

- Establish a policy to restrict public IM usage and require employees to sign an acknowledgement of receipt of the policy.
- Consider implementing an intrusion detection system to identify IM traffic. Assess the need for other IM security products.
- Create rules to block IM delivery and file-sharing.
- Consider blocking specific IM vendors.
- Ensure a strong virus protection program.[3]
- Ensure a strong patch (software update) management program.[4]
- Include the vulnerabilities of public IM in information security awareness training.

Conclusion

The risks associated with the use of IM include revealing confidential information over an unsecured delivery channel, spreading viruses and worms, and exposing the network to backdoor Trojans which are hidden programs on a system that perform a specific function once users are tricked into running it. IM is vulnerable to denial-of-service attacks, hijacking sessions and legal liability resulting from downloading copyrighted files.

Financial institutions are required to design and implement a comprehensive written information security program.[5] The security program should include appropriate controls and training to address the risks posed by the use of public IM.

Technical Notes:

1. IM Types – IM products available on the Internet are unofficially used in many organizations. There are two ways that IM products enter the workplace. The first is referred to as Server Proxy, in which messages pass through the IM vendor's computer and are forwarded to the user. The second is by Server Broker, in which messages are passed to the IM vendor only to initiate the communication between users, who then communicate directly with each other.
2. Firewall and Router Considerations – Default destination ports for the major IM vendors include ports 5190, 1863 and 5050. Although major Internet IM vendors use well-known ports, it is difficult to block all IM at the firewall. IM has a "port crawling" or "port agile" feature that allows messages to travel through legitimate open ports if others are unavailable. Common destination ports include Telnet (port 23); File Transfer Protocol (port 20) and Simple Mail Transfer Protocol (port 25). IM can also use Hypertext Transfer Protocol (port 80) in an attempt to bypass the firewall.[6]

[1] Enterprise IM products are beyond the scope of this guidance.

[2] Financial Institution Letter, “Risk Assessment Tools and Practices for Information Systems Security,” FIL 68-99, dated July 7, 1999.

[3] Financial Institution Letter, “Guidance on Developing an Effective Virus Protection Program,” FIL64-04, dated June 7, 2004.

[4] Financial Institution Letter, “Computer Software Patch Management,” FIL 43-03, dated May 29, 2003.

[5] Financial Institution Letter, “Security Standards for Customer Information,” FIL 22-01, dated March 14, 2001.

[6] Symantec Security Response, “Malicious Threats and Vulnerabilities in Instant Messaging,” dated September 2003.

Last Updated 7/21/2004 communications@fdic.gov