Office of Inspector General

February 14, 2002
Audit Report No. 02-003

Controls Over Outlook Resources

OFFICE OF INSPECTOR GENERAL
DELIVERING QUALITY TIMELINESS VALUE
OFFICE OF AUDITS

FDIC
Federal Deposit Insurance Corporation
Washington, D.C. 20434

Office of Audits
Office of Inspector General

DATE: February 14, 2002

TO: Carol M. Heindel
Acting Director, Division of Information Resources Management

FROM: Russell A. Rau [Electronically produced version; original signed by Russell A. Rau]
Assistant Inspector General for Audits

SUBJECT: *Controls Over Outlook Resources* (Audit Report No. 02-003)

The Federal Deposit Insurance Corporation's (FDIC) Office of Inspector General (OIG) has completed an audit of the controls associated with shared access to Microsoft Outlook (Outlook) folders. We conducted this audit to assess the effectiveness of controls used to protect access to resources and sensitive data that reside in Outlook folders. These folders include: Calendar, Contacts, Deleted Items, Drafts, Inbox, Journal, Notes, Outbox, Sent Items, and Tasks. We initiated the audit because an FDIC employee inadvertently gained unrestricted access to another employee's Outlook inbox when attempting to view the latter employee's appointment calendar.

BACKGROUND

The FDIC uses Outlook to provide electronic mail (e-mail) and calendar services to its employees. In addition to e-mail and group scheduling, Outlook provides for the creation and storage of information in folders. One Outlook feature is the capability to share access to all folders, including the Inbox. Individuals can set the properties for their Outlook account at their desktop to assign various permissions to others, including the ability to send messages; and read, modify, create, or delete information in any of the Outlook folders. These permissions can be useful when responding to important issues in situations where the assigned Outlook user is unavailable. Some agencies expressly forbid individuals from sharing access to personal e-mail accounts, but the FDIC does not want to limit this capability. The Corporation's position increases the need for controls over the assignment of Outlook permissions to provide adequate security over sensitive information that may reside in e-mail messages or Outlook folders.

OBJECTIVE, SCOPE, AND METHODOLOGY

The objective of the audit was to assess the effectiveness of controls used to protect sensitive data that reside in Outlook folders. We performed our audit between May and July of 2001 in accordance with generally accepted government auditing standards.

To accomplish our objective, we assessed Outlook sharing capabilities by reviewing documents and information obtained by the Corporation from Microsoft. We reviewed backup files and audit logs and interviewed Division of Information Resources Management (DIRM) personnel involved with maintaining Outlook, including individuals in the Local Area Network Management, Helpdesk, and Desktop Management sections. We also evaluated the relative impact of the Corporation's anticipated upgrade to Windows 2000 and Office XP to determine whether the Outlook upgrade will improve security controls. We reviewed the Outlook settings of selected FDIC executives to determine the vulnerability of their personal Outlook accounts.

Additionally, the Corporation requested that we obtain "best practices" of other federal agencies regarding sharing access to e-mail accounts. We obtained e-mail security procedures from the United States Departments of Defense and Agriculture and the Board of Governors of the Federal Reserve System.

RESULTS OF AUDIT

The FDIC's policies and procedures did not adequately protect data residing in Outlook folders. DIRM had not issued guidance to properly control the use of Outlook settings that can permit other system users to have access to information created by or intended for the original user. In addition, DIRM could not effectively monitor the individual settings of all employees because Outlook permissions are set at the user's desktop. Therefore, sensitive data residing in e-mail messages and Outlook folders may not have been adequately secured against unauthorized disclosure, deletion, or modification. This security risk was increased because a feature of the current version of Outlook can contribute to users inadvertently assigning access to their personal folders to all Outlook users.

POLICIES AND PROCEDURES FOR ACCESS TO OUTLOOK RESOURCES

The FDIC had not established policies and procedures that adequately addressed security over sensitive data that may reside in Outlook folders. Additionally, the FDIC had not alerted users of the risks associated with sharing access to their Outlook folders, nor instituted a process to identify users who had assigned Outlook permissions to others so that the Corporation could monitor and control the permissions assigned. Without adequate security controls, sensitive data residing in Outlook folders and e-mail messages were susceptible to unauthorized disclosure, deletion, or modification.

Office of Management and Budget (OMB) Circular A-130, Appendix III, *Security of Federal Automated Information Resources*, establishes security requirements for federal automated information resources. The circular requires federal agencies to implement and maintain a program to ensure that adequate security is provided for all information collected, processed, transmitted, stored, or disseminated. Such a security environment includes having qualified, trained security staff responsible for determining the sensitivity of the data and controlling access to the data.

Sensitive information requires protection because of the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information. Sensitive information includes information whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary data, records about individuals requiring protection under the Privacy Act,[1] and information not releasable under the Freedom of Information Act.[2]

Sensitive information is often included in e-mail messages and stored in Outlook folders. For example, the Division of Supervision's bank-related information is considered highly sensitive, and information security officers control data access. In addition, other divisions and offices transmit personal and financial data via e-mail. Sensitive data should be protected against unauthorized disclosure. Accordingly, the FDIC is implementing security enhancements such as the ability to encrypt e-mail messages.

However, the FDIC had not developed policies and procedures regarding Outlook security. Specifically, FDIC Circular 1360.1, *Automated Information Systems Security Policy*, requires that information be protected at a level commensurate with the sensitivity of information processed, stored, or transmitted and provides that access to sensitive information will be based on business needs. Sensitive data residing in the Outlook folders should be protected by the same level of security controls as other sensitive data, but the circular does not address shared access to e-mail accounts. Further, FDIC Circular 1370.3, *Use of Electronic Communications*, provides guidance to employees concerning their responsibilities with respect to the use of e-mail, but does not address sharing access to accounts or sensitive data.

In addition, if individual users share access to their Outlook account, the assigning user determines who may read the sensitive data. If the assigning FDIC user has not received appropriate training regarding their security responsibilities, there is increased risk of unauthorized disclosure and misuse of sensitive information.

Other Federal agencies such as the Department of Defense and the Board of Governors of the Federal Reserve System expressly forbid individuals from granting access to their personal e-mail accounts. However, the FDIC does not want to limit this capability. Accordingly, the Corporation needs to develop additional policies and procedures to protect sensitive data residing in Outlook folders and provide its employees with guidance regarding the appropriate circumstances under which to do so.

[1] The Privacy Act of 1974 regulates the collection, maintenance, use, and dissemination of personal information by federal government agencies.

[2] The Freedom of Information Act generally provides that any person has a right to obtain access to federal agency records, except to the extent that such records are protected from disclosure by exception or law.

OUTLOOK FEATURES FOR ASSIGNING ACCESS

The risk of unauthorized access and misuse of data residing in Outlook folders was increased because a feature of the current version of Outlook can contribute to a user inadvertently assigning access to their personal Inbox to all Outlook users. This risk became evident when an OIG employee inadvertently gained access to another user's Outlook Inbox while attempting to view the user's appointment calendar.

Outlook properties are set at the user's desktop. When a user assigns permissions to share his or her Outlook folders, the cursor will not automatically move to the intended assignee and may cause the user to select the default setting of all FDIC users. Additionally, because Outlook properties are set at the user's desktop, DIRM could not effectively monitor the individual settings of all employees.

We reviewed the Outlook settings of selected FDIC executives to ensure they had not been inadvertently set to the default setting and found no such instances. In addition, by June 2002, DIRM plans to upgrade to Windows 2000 and the Office XP application suite. Our review of Office XP showed that the Outlook default settings in this version are not automatically highlighted when a user attempts to assign permissions to share Outlook access with other users.

However, until the upgrades are completed, the risk of unauthorized access will remain. Therefore, DIRM has agreed to develop procedures for security personnel to monitor shared access to Outlook folders. DIRM security personnel or division and office Information Security Managers (ISM) established under the Corporation's new ISM program will be notified of individuals who have provided shared access to their Outlook folders and will periodically sample users to determine if access permission has been set as intended. In addition, a discussion of shared access to Outlook folders and approaches for controlling access to sensitive data will be included in the FDIC's security awareness efforts.

RECOMMENDATIONS

The Acting Director, Division of Information Resources Management should:

(1) Establish procedures for employees to notify DIRM security personnel or ISMs when sharing access to Outlook folders so that the permissions assigned are consistent with what the user intended.

(2) Establish procedures to monitor the settings of individuals who have been authorized to share access to Outlook folders to ensure that the permissions have been properly granted.

(3) Include in the FDIC's security awareness efforts a discussion of shared access to Outlook folders and approaches for controlling access.

CORPORATION COMMENTS AND OIG EVALUATION

On January 28, 2002, the Acting Director of DIRM provided a written response to the draft report. Management's response, without the attachment suggesting editing changes, is presented in Appendix I to this report. The Corporation concurred with recommendations 1 through 3. These recommendations will remain undispositioned and open for reporting purposes until we have determined that agreed-to corrective actions have been completed and are effective. At DIRM's request we made several wording changes to clarify terminology in the report.

Federal Deposit Insurance Corporation
3501 North Fairfax Dr., Arlington, VA 22226
Office of the Director

January 28, 2002

TO: Russell A. Rau
Assistant Inspector General for Audits

FROM: Carol M. Heindel [Electronically produced version; original signed by Carol Heindel]
Acting Director, Division of Information Resources Management

SUBJECT: Response to the Audit, *Controls Over Outlook Resources* (2001-918)

The Division of Information Resources Management (DIRM) has reviewed the subject draft audit report, as revised and reissued electronically to DIRM by your staff January 14, 2001, and generally agrees with the findings. Responses to the recommendations are provided below.

DIRM is also providing an edited copy of the draft report as an attachment to this response. The attachment provides requested language changes that our technical staff believe are important for clarity.

Management Decision:

Recommendations: The Acting Director, Division of Information Resources Management should:

(1) Establish procedures for employees to notify DIRM security personnel or ISMs when sharing access to Outlook accounts so that the permissions assigned are consistent with what the user intended.

and

(2) Establish procedures to monitor the settings of individuals who have been authorized to share access to Outlook accounts to ensure that the permissions have been properly granted.

DIRM Response: As indicated in the OIG's report, the primary risk associated with the current Outlook product will be resolved by the FDIC's conversion to Windows XP. In the interim, DIRM management has agreed to send out a global email to all employees by February 15, 2002 explaining the importance of controls associated with shared access to the Microsoft Outlook folders. The global will provide the user with instructions on how to review their individual properties within their Outlook account and determine that the settings are appropriate. Questions or support issues will be directed to their individual Information Security Managers (ISM) or the DIRM Helpdesk.

(3) Include in the FDIC's security awareness efforts a discussion of shared access to Outlook accounts and approaches for controlling access.

DIRM Response: DIRM ISS will update the Information Security Website to include a statement on effective controls used to protect access to resources and sensitive data that reside in the Outlook folders. The website is updated quarterly. The next update will be completed by April 15, 2002.

Please address any questions to DIRM's Audit Liaison, Rack Campbell, on (703) 516-1422.

Attachment

cc: Vijay Deshpande, Director, OICM
Janet Roberson, Deputy Director, ITM
Michael Wong, Deputy Director, TIM
Sandy Velasquez, Assistant Director, Operations
Ned Goldberg, Assistant Director, Information Security