UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, D.C. 20549

OFFICE OF
INSPECTOR GENERAL

MEMORANDUM

March 1, 2010

TO: Carlo V. di Florio, Director, Office of Compliance Inspections and Examinations
Charles L. Boucher, Director and Chief Information Officer, Office of Information Technology

FROM: H. David Kotz, Inspector General, Office of Inspector General

COPY: Kayla Gillan, Deputy Chief of Staff, Office of the Chairman
John Walsh, Associate Director/Chief Counsel, Office of Chief Counsel, Office of Compliance Inspections and Examinations

SUBJECT: Management Alert – *Data Security Vulnerabilities*, Report No. 477

Three recent investigations undertaken by the Securities Exchange Commission (SEC or Commission), Office of Inspector General (OIG) have raised concerns about data security at the SEC. In 2008 and 2009, the OIG undertook two investigations involving the unauthorized release of non-public records available on the Office of Compliance Inspections and Examinations (OCIE) intranet sites and/or shared network drives. In a third investigation, the OIG learned that files pertinent to our investigation had been deleted or removed from an OCIE shared network drive and have not been recovered. Despite the OIG conducting extensive e-mail review and witness interviews, the sources of the release of non-public information and file removal have not be identified because OCIE's intranet sites and shared network drives do not employ auditing[1] systems.

The purpose of this Management Alert is to present our concerns to you in writing. We ask that you respond within five business days of receipt of this letter and identify the actions your offices have taken, or plan to take, to address two significant areas of data security concern:

1. Vulnerability of the OCIE intranets and
2. Vulnerability of the OCIE shared network drives.

This review was not conducted in accordance with government auditing standards.

[1] Auditing as used in this Management Alert refers to blocking, tracking, or controlling data.

BACKGROUND

Summary

The SEC does not have in place an auditing system for OCIE intranet sites or its shared network drives. OCIE's intranet sites and shared network drives store extensive non-public information, including inspection and examination reports, deficiency letters, and other documents containing confidential registrant information. Approximately 2,000 employees have access to OCIE's intranet sites or shared network drives. However, use of the OCIE intranet sites and shared network drives is not audited, which allows users to view, print, copy, download, move, edit, or delete documents and files without detection.[2]

1. The OCIE Intranet Sites

The OCIE intranet sites are internal Commission websites designed to allow for data sharing and to provide historical reference and training materials for inspections and examinations. OCIE has a central intranet site, an intranet site containing training materials, and additional intranet sites for certain sub-groups within OCIE. The OCIE intranet sites contain confidential non-public information, such as inspection and examination reports, communications with registrants, deficiency letters, and policies and procedures for examination staff. Many of these documents are also stored on OCIE's shared network drives.

According to information provided by OCIE's information technology staff and OCIE's Office of Chief Counsel, the OCIE intranet sites pose a serious security threat as they are accessible to nearly 2,000 Commission employees, including over 1,000 OCIE employees and over 1,300 Division of Enforcement staff.[3] According to OCIE's information technology staff, the OCIE intranet sites are vulnerable to having information, such as registrant data, misappropriated by OCIE intranet site users.[4]

Despite that many OCIE intranet site users do not have full access rights to the sites, limited access is sufficient to pose a serious data security risk. Many OCIE intranet site users have "read-only" access, meaning that they are unable to alter the text of documents on the OCIE Intranet sites. However, read-only users are still able to view, print, copy, and download information. Because use of the OCIE intranet sites is not audited, those with access to the OCIE intranet sites

[2] Controls over the OCIE intranets and shared network drives are interrelated because many of the documents available on the shared network drives are also available on the intranet.
[3] The central OCIE intranet site containing registrant materials is accessible to approximately 1,000 OCIE staff, 16 executive staff, 124 Division of Investment Management staff, and 17 Division of Trading and Markets staff. The OCIE intranet site containing non-public OCIE training materials is available to OCIE staff and approximately 1,325 Division of Enforcement staff.
[4] OCIE information technology staff stated that they are aware of at least one data theft.

are able to take data and other information from the OCIE intranet sites without detection.

2. OCIE Shared Network Drives

Shared network drives[5] are depositories for shared projects for each office or division. According to OCIE's Office of Chief Counsel, the shared network drives promote knowledge and information sharing by allowing open access to employees with rights to a particular drive. The OCIE shared network drives hold documents containing highly confidential information, including examination and inspection reports, electronic productions from registrants, correspondence, work papers, registration materials, spreadsheets, and work product. Each regional office has its own shared network drive. Most users can view, print, copy, download, edit, move, and even delete files from the shared drives.

Currently the SEC does not audit who accesses the shared network drives or who deletes or alters files contained therein. When items are deleted from shared network drives, they are sent to a recovery bin with limited storage capacity. Once the bin's capacity is reached, the older files are purged. In OCIE, the purge occurs in less than [redacted] days. Once purged, those files often cannot be recovered.[6]

Recent Incidents

The following three recent OIG investigations have involved the removal or deletion of documents from OCIE's shared network drives or the unauthorized release of confidential information that was stored on OCIE's intranet sites and/or shared network drives. The sources of these data security breaches have not been identified because OCIE's intranet sites and shared network drives do not employ an auditing system.

3. Documents Deleted from an OCIE Shared Network Drive

As part of Case No. OIG-496, a staff accountant discovered in January 2009 that all of the files regarding a particular registrant were missing from an OCIE shared network drive. The missing files included work product generated by OCIE staff, such as an examination report, interoffice memoranda, correspondence, and relevant e-mail gathered during an 18-month examination.

The files were necessary for an OIG investigation involving serious allegations about the registrant and the SEC's actions in response to those allegations. The

[5] The shared network drives are often referred to as the "J: drive," but within SEC Headquarters, the shared network drives are comprised of the J:, K:, and L: drives.
[6] Forensic experts can be retained to attempt to recover the files, but it is very costly and may not be successful.

Office of Information Technology was unable to determine who deleted the files or when the files were deleted.

4. OCIE Examination Report Leaked to the Press

At the request of an SEC registrant, [redacted], the OIG opened PI No. 09-62, a preliminary inquiry into the leak of confidential [redacted] e-mail to the Wall Street Journal. The OIG found that the excerpts of the confidential e-mail that had appeared in the Wall Street Journal in [redacted] were from e-mail provided to OCIE during a routine examination of [redacted] and had been included in an OCIE examination report of Bernard L. Madoff Investment Securities LLC.

The OCIE examination report was stored on the OCIE intranet site and an OCIE shared network drive and had been circulated to a variety of officials within the Commission. The OIG reviewed the e-mail of report recipients, but has been unable to narrow down and locate the source of the leak because the OCIE intranet and shared network drives were unaudited.

[redacted] was outraged by the public release of its internal e-mail communications. Personnel from OCIE's Office of Chief Counsel have reported that [redacted] was less cooperative in a recent examination and used the leak of its confidential e-mail as a reason for not producing requested documents.

5. Non-public Version of an SEC Report Leaked to the Press

In Case No. OIG-500, the OIG investigated the disclosure of a non-public version of an SEC report containing issues identified in the SEC staff's examination of select nationally recognized statistical rating organizations (NRSROs). The SEC report was harshly critical of the NRSROs. The public version of the SEC's report contained the critical findings, but redacted the names of the NRSROs and quotations from confidential e-mail because the SEC staff had assured the participating NRSROs that their identities would be kept confidential. However, the non-public version of the report that was leaked to the Wall Street Journal in August 2008 contained the names of the NRSROs examined, the identities of certain individuals, and excerpts from confidential e-mail.

The non-public version of the report provided to the Wall Street Journal had been stored on an OCIE Shared Network Drive and was circulated to a small number of people. Despite reviewing over 130,000 emails and taking the testimony of 25 SEC employees, the OIG was unable to identify the source of the leak because drafts of the report were available on an OCIE shared network drive and could have been accessed and printed by any OCIE employee without detection.

The OIG investigation found that the Wall Street Journal's publication of this information was disturbing to the firms and embarrassing to the SEC staff who had assured the participating NRSROs of confidentiality.

Effects

The failure to audit the use of the OCIE intranet and shared network drives has allowed the sources of the unauthorized release of confidential non-public information and the deletion/removal of OCIE files to remain undetected.

Leaks, such as those discussed above, have negatively impacted the relationship of the SEC with its registrants. Registrants regularly provide the SEC with confidential information, and the release of this information to the press may cause registrants to be reluctant to cooperate in SEC examinations and investigations, for fear that their confidential information will become public. Moreover, failure to audit the use of OCIE's shared network drives and intranet sites poses a grave data security concern because it makes registrant data vulnerable to undetected theft. Hence, we believe that prompt action should be taken to address these data security vulnerabilities.

Memorandum

Date: March 10, 2010

To: David Kotz, Inspector General, OIG

From : Charles Boucher, Chief Information Officer, OIT

CC: Carlo di Florio, Director, OCIE
Kayla Gillan, Deputy Chief of Staff, Office of the Chairman
John Walsh, Associate Director and Chief Counsel, OCIE
Diego Ruiz, Executive Director, OED

Subject: OIG Management Alert - Data Security Vulnerabilities, Report #477

This memo acknowledges receipt of the subject OIG Management Alert, dated March 1, 2010. In summary, the OIG is requesting that the system feature of auditing access to files on the shared drives and intranet for OCIE be turned on so that it may be easier to identify who has used files for unauthorized purposes. There are a number of different options on how auditing could be implemented, and a substantial investment is likely to be required due to the additional processing, storage, access tools, and staff resources to support such an activity. In addition, management needs to consider whether the benefits of auditing file access justify the investment, and if so whether it should be implemented beyond OCIE, as well as if there are any business process changes which should be considered.

OIT has begun analysis on the technology aspects of the OIG's request and will work with the businesses and agency management to decide a course of action.

MEMORANDUM

TO: David Kotz, Inspector General, Office of Inspector General ("OIG")

FROM: Carlo di Florio, Director, Office of Compliance Inspections and Examinations ("OCIE")
John Walsh, Associate Director – Chief Counsel, OCIE JW by JCE
Greg Cobert, Assistant Director, Information Technology, OCIE
Steve Haupt, Branch Chief, Information Technology, OCIE
Kris Easter, Assistant Director, OCIE

CC: Charles Boucher, Chief Information Officer, Office of Information Technology ("OIT")

RE: Office of Compliance Inspections and Examinations' Response to the Office of Inspector General's Management Alert, *Data Security Vulnerabilities*, Report No. 477

DATE: March 11, 2010

OCIE agrees with the need to have in place an auditing system for OCIE intranet sites and OCIE's shared network drives. OCIE Technical Staff is currently working with OIT Staff to review the various audit solutions and to determine the impact of those solutions on OCIE's current business practices. It is expected that it may take some time to evaluate, test and implement a solution and also determine if there is an impact on OCIE's current business processes.