The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

MEMO# 23453

May 15, 2009

Study Finds Firms May Be Vulnerable To Ex-Employees Stealing Data Loss During Downsizing

[23453]

May 15, 2009

TO: COMPLIANCE MEMBERS No. 23-09
PRIVACY ISSUES WORKING GROUP No. 6-09
TECHNOLOGY COMMITTEE No. 12-09
RISK MANAGEMENT ADVISORY COMMITTEE No. 5-09
TRANSFER AGENT ADVISORY COMMITTEE No. 34-09
OPERATIONS MEMBERS No. 12-09 RE: STUDY FINDS FIRMS MAY BE VULNERABLE TO EX-EMPLOYEES STEALING DATA LOSS DURING DOWNSIZING

The Ponemon Institute [1] recently published a report, Data Loss Risks During Downsizing, that contains the results of a study finding that employees exiting their current jobs – through downsizing or otherwise – may be walking off with sensitive and confidential data. [2] The report is based on a survey conducted in January 2009 of 945 adult-aged participants located in the U.S. who were laid-off, fired, or changed jobs within the past 12 months. [3] All participants reported that, at their previous employer, they were assigned a desktop or laptop computer for use in the work place and had access to and use of proprietary information such as customer data, contact lists, employee records, financial reports, confidential business documents, software tools, and intellectual properties. Twenty percent (20%) of the participants were from the financial services industry. In addition to finding that 59% of survey participants reported stealing company data, almost a fourth (24%) were able to access their former employer's computer system or network after departure. As noted in the report, such thefts could affect the employer's competitiveness or result in data breaches. The report's other key findings and recommendations are briefly summarized below.

Key Findings

The key findings from the survey, which are discussed in more detail in the report, include the following:

- Former employees are stealing data and are more likely to do so when they don't trust their employer. Fifty-nine percent (59%) of employees report keeping company data after leaving their employer. Employees who were negative about the employer account for 61% of these employees. Seventy-nine percent (79%) of employees stealing data know that they did not have permission to do so or that they were defying company rules.
- The data stolen includes email lists (65%), non-financial business information (45%), and customer information, including contact lists (39%) – information that might affect their previous employer's competitiveness or could result in a data breach. Sixty-seven (67%) percent of employees reported they used the stolen data to secure a new position; 68% reported that they are using or planning to use such information.
- With respect to the manner in which data is stolen, most occurs in the form of paper documents or hardcopy files (61%) followed by downloading information onto a CD or DVD (53%) , downloading to a USB memory stick (42%), and sending documents as attachments to a personal email account (38%).
- Companies are failing to take proper steps to stop data theft. Only 15% of companies conducted a review or performed an audit of the paper and/or electronic documents taken by employees. For those 15% that conducted reviews or audits, 45% of former employees said it was incomplete and 29% said it was superficial. Approximately 89% reported that the company did not perform an electronic scan of devices such as portable data-bearing equipment or USB memory sticks.
- Many participants reported that their former employers did not prevent them from accessing the employer's computer system or network after departure. Twenty-four percent (24%) of participants continued to have access to company data after they left the company, and 35% of these employees said the access continued for one week or longer. When asked how these employees knew they had continued access to their former employer's system or network, 32% said they accessed the system and their credential worked and 38% said their former co-workers told them their access rights continued after their departure.

Recommendations

Based on the above findings, the Ponemon Institute recommends, with respect to employees leaving the firm, that:

- Company policies and procedures clearly deny former employees access to sensitive and confidential information used in their jobs;
- Companies take steps to deny such access once an employee is terminated;
- Supervisors or business unit managers and someone from IT security conduct a thorough review and audit of an employee's paper and electronic documents;
- Prior to the employee leaving, companies should monitor the employee's access to the network or system to make sure sensitive and confidential data is not being downloaded or sent to the employee's personal email account; and
- Extra precautions should be taken with former employees who have been asked to leave or who are disgruntled because such employees are more likely to steal data.

The full report is attached. The appendix to the report includes the survey questions and their related results.

Tamara K. Salmon
Senior Associate Counsel

Attachment

endnotes

[1] The Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. The head of the Ponemon Instituate, Dr. Larry Ponemon, has spoken at ICI conferences and assisted the ICI on various projects.

[2] The Institute has received permission from the Ponemon Institute to circulate this copyrighted report. The report, which was sponsored by Symantec Corporation, was published on February 23, 2009.

[3] Thirty-seven percent (37%) of survey participants were asked to leave their employer; 38% found a new job; 21% left because they anticipated a layoff; and 4% left for personal reasons. Eighty percent (80%) of the participants are currently employed.

Copyright © by the Investment Company Institute. All rights reserved. Information may be abridged and therefore incomplete. Communications from the Institute do not constitute, and should not be considered a substitute for, legal advice.