Office of Inspector General
Legal Services Corporation

Inspector General
Jeffrey E. Schanz

3333 K Street, NW, 3rd Floor
Washington, DC 20007-3558
202.295.1660 (p) 202.337.6616 (f)
www.oig.lsc.gov

GRANTEE ADVISORY
12-02-JS

TO: All LSC Executive Directors

FROM: Jeffrey Schanz, Inspector General

DATE: March 27, 2012

SUBJECT: Preventing Information Security Breaches

The purpose of this Grantee Advisory is to stress the importance of securing confidential information entrusted to LSC grantees by illustrating the fallout that can occur when valued data is compromised, as well as to share good practices that can help prevent information security incidents.

Three Illustrative Instances

In the fall of 2011, a five-year employee of an LSC grantee deleted over 13 gigabytes of data (855,000 pages) from two database systems in the closing days of their employment. This included the grantee's fund-raising database system that was maintained outside the grantee's network, unknown to the Executive Director. The other database system inside the grantee's network was routinely backed up, but some of the restored files were found to be corrupted and unusable. At least five grantee staff-members have spent a great deal of time on clean-up and recovery tasks, including reporting the loss to the police and the LSC OIG, sorting files, attempting to restore data, contracting with a computer forensics company, and negotiating insurance claims under their *General Commercial Insurance policy (Valuable Papers coverage)*. The computer forensics company's preliminary assessment determined that potential criminal activity had occurred, and estimated their data restoration work at a cost of $35,000. This cost is expected to substantially increase as the grantee's policy analysts have to sort through and reassemble the restored files (both of these costs are expected to be reimbursable by the insurance company). The ongoing investigation will allow the grantee and/or insurance company to consider pursuing possible legal recourse.

A second instance further illustrates the severity of information security breaches when client files are involved. In 2008, an attorney at another LSC grantee took several boxes of case files home to perform quality assurance reviews. The attorney's car was stolen with the case files in the back seat. The approximately 300 lost files contained clients' personal and private

information (including Social Security numbers), and sensitive case information. The grantee spent considerable time and effort to recreate the missing files, to notify the affected parties, and to assist with contacting the credit reporting companies to mitigate the risk of identity theft.

A third instance, while outside of the immediate legal services environment, also serves as a cautionary tale regarding information security. A data analyst at the Department of Veterans Affairs took home a laptop and an external hard drive containing unencrypted information on 26.5 million people, and it was stolen in a burglary of the analyst's home. The agency waited over 2 weeks to inform those who were affected. They estimated that it would cost between $100 million to $500 million to prevent and cover possible losses from the data theft.[i] In 2009, the agency agreed to a $20 million settlement from a class action lawsuit, "even though the Department has said that there is no evidence that the information on the stolen laptop was used or that any person involved was harmed by it."[ii]

Considerations

- LSC's 2012 Grant Assurance 8(a) requires grantees to have "...an information security system that ensures confidentiality and security of its operations, assets, data, and files."

- There are many types of informational assets to protect within a legal services grantee, including: client case, employee personal and private information, financial assets, fundraising and vendor data, technology assets, as well as, proprietary business papers and information.

- When confidential information is lost, business entities potentially become legally liable for that information and any subsequent use.

- Presently, data breach notification laws apply in forty-six states, the District of Columbia, Puerto Rico and the Virgin Islands, which have enacted legislation requiring notification of security breaches involving personal information to affected parties.[iii] Yet, data breaches still appear to be considerably underreported. The 2010/2011 survey from the Computer Security Institute (CSI), which annually conducts one of the largest surveys on the topic of information security, reports that out of the 138 respondents who had a security incident occur the previous year, only 27% reported the intrusion(s) to a law enforcement agency and only 18% reported intrusions to the individuals whose personal data was breached.[iv]

- Data breaches are costly in a number of areas. Direct losses from data breaches include: hiring a forensic investigator; sending out breach notification letters; and any other remediation and patching activity for which the organization writes a check. Indirect breach losses could include: loss of future income, lost employee time, potential negative publicity and damaged relationships with those parties adversely impacted.

Information Security Good Practices

The following are good practices which can help prevent information security incidents and mitigate potential damages:

- Have up-to-date written security policies and procedures in place.
- Conduct information security trainings for new and current employees, reviewing: relevant federal and state data security laws and associated criminal and civil liabilities, applicable professional standards, and office policies and procedures.
- Have all employees and consultants sign non-disclosure agreements.
- Identify the confidential information the organization has, where it is stored, and who has access to it.
- Consult with your insurance provider to ensure the organization has adequate coverage.
- Ensure the safeguarding of paper files with policies governing the removal of files from the secure office environment.
- Make a record of any electronic business data stored outside the grantees network (e.g., cloud computing) and review the backup and restoration capabilities of the vendor.
- Advise employees not to download confidential information on home computers and personal devices.
- Ensure proper handling of passwords for all devices and drives.
- Make sure to use trusted and secured web sites when sharing information over the Internet.
- Consider encryption software to protect confidential information stored on portable devices and drives.
- Review data access privileges to ensure there is not overly permissive access to confidential information on shared servers.
- Back up confidential information on a server or detachable device - regularly.
- With all backup systems, test and restore regularly to ensure they actually recover the data and operations as intended.

Conclusion:

In all three of the illustrative instances, losses could have been minimized or prevented if greater information security had been applied. Your organization may benefit from a review of your organization's information security system's policies and practices in light of the good practices described above. Additional resources about information security are provided below for further information.

I hope you find this grantee advisory helpful. If you have any questions, please do not hesitate to call David Maddox, Assistant Inspector General for Management and Evaluation at (202) 295-1653, or by email at dm@oig.lsc.gov.

Additional Information:

SANS Institute: Understanding the Importance of and Implementing Internal Security Measures, http://www.sans.org/reading_room/whitepapers/policyissues/understanding-importance-implementing-internal-security-measures_1901 .

SANS Institute: Computer Security Policy Templates, http://www.sans.org/security-resources/policies/computer.php .

Endnotes

i. Electronic Privacy Information Center, Veterans Affairs Data Theft, http://epic.org/privacy/vatheft/ .

ii. Government Computer News, http://gcn.com/articles/2009/02/02/va-data-breach-suit-settlement.aspx .

iii. States without security breach laws are: Alabama, Kentucky, New Mexico, and South Dakota. National Conference of State Legislatures, http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx .

iv. 2010/2011 Computer Security Institute, Computer Crime and Security Survey, http://gocsi.com/survey .