Office of Inspector General
Legal Services Corporation

# The Fraud Corner

6/24/2019

## Best Practices for Preventing and Detecting Insider Threats

As part of its Fraud Corner series, the Office of Inspector General (OIG) is providing Legal Services Corporation (LSC) grantees with the following information on "best practices" to aid a grantee in preventing and detecting insider threats. The purpose of this article is to provide guidance to grantees on the red flags, or circumstances providing the opportunity for insider threats, and the necessary policies and procedures to prevent and detect insider threats by current and former employees, contractors, and any other individuals who have, or once had, authorized access to grantee's IT systems and functions.

Similar to fraud, insider threats generally follow a triangle. Typically, the insider has pressure (or some other motive) triggered by a negative work-related event. Then the insider has an opportunity, through insufficient policies or internal controls, to compromise the program's IT systems by causing damage to a component within the IT system or by deleting, stealing, or changing sensitive information stored in the IT system. (The damage or intrusion can slow or stop business operations, cause financial loss, or damage the program's reputation). Routinely, the insider rationalizes their conduct based on a perceived negative work-related event.

The OIG has investigated insider threats, for example, where management emails were compromised, donor lists and forms were accessed and deleted, client information was provided to third parties, fake administrator accounts were created, and wireless networks were deleted. The motives triggering the above incidents included employees being denied a raise or promotion, learning of an impending termination, or receiving a demotion or reprimand. The disgruntled employees were able to cause damage due to missed red flags and improper controls on IT systems and functions.

The following provides information on potential red flags as well as best practices to assist grantees in detecting and preventing insider threats.

### Implement Strict Password and Account Management Policies and Practices

- **Red Flag:** Most employees are provided network access on-site and remotely through network logins and passwords. Employees also may have access, through additional logins and passwords, to financial, employee, and client software applications and database systems. When passwords are shared, an insider can perpetrate a breach by causing damage or accessing sensitive information without being identified.

- **Best Practice:** Grantees should ensure that each employee granted access to the IT system or a database is provided a unique login, that the sharing of logins and passwords is prohibited, and that employees are frequently reminded that improper access may result in disciplinary action. Toward that end, grantees should have a computer usage policy as well as a computer warning banner indicating that, if consistent with law, employees have no reasonable expectation of privacy while using grantee owned computers and equipment. Use policies should also contain end-user responsibilities, including protecting sensitive client and grantee information. Grantees should also conduct periodic account reviews to determine whether any employee's role has changed and ensure that the access employees are provided matches the duties of their current positions.

**Develop Comprehensive Employee Termination Procedures**

- **Red Flag:** Employees who become insider threats typically do so just prior to their departure or immediately after their departure through continued access to networks and databases.
- **Best Practice:** Immediately after an employee departs, all remote and on-site access should be revoked. Be sure to track all accounts assigned to employees during the course of their employment so it is known what account access should be revoked upon their departure. Management should have termination policies and procedures that instruct how to revoke remote and physical access by recently departed employees. Once a former employee's access to the office is revoked, all other employees should be notified of the former employee's departure to ensure improper access is not granted. Grantees also should consider prohibiting employees who quit or resign with time pending (for example two-weeks' notice) from accessing office systems and premises if they pose a security threat.

**Control and Monitor Remote Access from All Endpoints, including Mobile Devices**

- **Red Flag:** Many times, as a default, employees are provided remote access even if the employee is not permitted to work from home and does not conduct off-site outreach. Also, many programs do not periodically audit remote access logins to ensure former employee or contractor logins are deleted or that fake logins have not been created.
- **Best Practice:** Grantees should ensure that, consistent with law, grantee policies and procedures allow for management to monitor an employees' remote system activities and level of access. Ensure that only employees whose duties or work situation require remote access are provided with a remote access account that includes a personalized login and password. Periodically, management should audit remote logins to ensure employees have the appropriate level of access and there are no active remote access accounts for employees who have separated, no fake logins exist, and guest or test accounts are properly configured and give

no unintended access to critical systems. Additionally, grantee management should monitor network logs to detect questionable access by an employee.

**Identify Risky Employees/Contractors and Respond Promptly to Suspicious Behavior**

- **Red Flag:** Most internal threats begin with a disgruntled employee or contractor. Individuals who become internal threats may have demonstrated behavioral red flags such as airing grievances or mentioning harm to the program. Many grantee employees do not report the red flags but often recall them after the fact.
- **Best Practice:** Grantees should ensure that managers and other employees have a means for reporting behavioral problems that indicate a threat to grantee operations, IT systems and functions.

**Ensure Separation of Duties for System Administrators and Least Privilege**

- **Red Flag:** Insider threats can be posed by employees who are provided improper rights and access to IT systems. Administrator rights allow a user to have full access and privileges to retrieve sensitive information, install updates, and change settings. For example, an employee provided with administrator rights could delete critical data stored on the program's IT systems without the system requiring a secondary approval from another grantee employee. An employee without the need for administrator rights, for example those lacking specific IT duties or technical skills, can be seen as a potential insider threat.
- **Best Practices:** Ensure that only those with the specific need for administrator rights are given such access. Those employees with administrator rights should be monitored with proper internal controls. When a system administrator changes settings, creates new users, or accesses sensitive information, the administrator should be required to use the administrator login which should require multi-factor authentication. To the extent possible, other employees with administrative oversight responsibilities should be involved in the decision-making, sign-off approval, and implementation process for sensitive changes. Also, specific to legal services, employees with administrator rights with the ability to add or change client information in the case management system (CMS) should be monitored through proper internal controls, including transaction tracking within the software and periodic monitoring of their CMS log.

**Additional Best Practices Related to System Administrators:**

- Ensure at least two employees have administrator rights.
- Have network administrators sign a Network Administrator Use policy which details their responsibilities and requires them to act in the best interest of the grantee.
- When a system administrator is released from employment, plan ahead to limit any risks, including changing all system passwords.

- If the departed system administrator is considered high risk, consider hiring an IT contractor to orchestrate the required system changes including changing all system passwords and have all staff change their network passwords. Also, consider reviewing and monitoring accounts in all systems to ensure a backdoor, false account or trojan etc., were not added into the system.

**Additional Steps to Prevent and Detect Insider Threats:**

1. Your best defense is to properly control, manage, and monitor your computer network.
2. Establish an effective IT security policy and institute periodic IT security awareness training for all employees.
3. Do not neglect physical security of your IT infrastructure, i.e., limit access.
4. Ensure that necessary security software and appliances are in place to prevent an insider threat.
5. Defend against the introduction of malicious code into your system.
6. Continually evaluate any upgrades to your current vendor products or invest in new security technologies.
7. Log, monitor, and audit suspicious employee activity.
8. Ensure an audit trail of employee IT activity is available and recoverable for a specified time-period.
9. Develop secure back-up and recovery processes for file and mailbox activity.
10. Ensure historic back-ups of IT systems and data files are created to offer a safe roll-back position.
11. Use encryption software to protect sensitive information.
12. Do not leave disabled or inactive accounts in your system. Delete and purge these accounts on a regular basis.

The OIG's Audit Unit conducts vulnerability assessments of grantees' information systems and networks to identify potential security vulnerabilities, flaws, and weaknesses. The assessments scan for internal and external vulnerabilities. At the conclusion of each assessment, the OIG issues a report to grantee management that summarizes the results of the tests and provides corrective actions and best practices to address vulnerabilities. To provide insight regarding common security issues, on March 20, 2018, the OIG issued a report to Executive Directors of LSC grantees summarizing vulnerabilities identified in recent tests and scans. The report outlined best practices to mitigate vulnerabilities. For additional information regarding the OIG's IT vulnerability program, please contact Roxanne Caruso, OIG Assistant Inspector General for Audit at (202) 295-1582 or by email RCaruso@oig.lsc.gov.

Additional information on understanding, managing and controlling cybersecurity risk can be found at the National Institutes of Standards and Technology (NIST) online resources and its Interagency Report (NISTIR), which provides guidance on how small businesses

(such as most LSC grantees) can provide basic security for their information, systems, and networks, at: https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf.

The OIG received significant input and assistance from LSC's Office of Information Technology regarding the information in this Fraud Corner article.

If you have any questions or comments or would like additional information about this post, please contact Daniel O'Rourke, OIG Assistant Inspector General for Investigations, at (202) 295-1651 or by email DOrourke@oig.lsc.gov.