Assessing Supervisor Reporting to Improve Insider Threat Detection Resilience

Michael C. Theis, CISSP, SSA (ret.)
Chief Engineer, Strategic Engagements

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Document Markings

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM20-0608

Agenda

Background

Problem Statements

Methodology

Transition Opportunities

Background

Supervisors needed to be trained on how to use a new computer-based tool that is used annually to assess each of their subordinates.

- The behaviors that are reviewed help assess the reliability of personnel to handle sensitive and formerly controlled materials.
- The answers that are submitted assist personnel reliability program (PRP) managers to determine if an employee may need additional attention or assistance in order to avoid a potential insider threat incident.

This presentation does *not* address the tool nor the organization that is deploying the tool.

Problem Statements

Supervisors are often considered the first line of defense in counter-insider detection. But there are problems associated with this:

- How reliable are supervisors at reporting issues of concern? (*"We are told there are no issues until suddenly one day it's, 'this person has to go!'" – a PRP case manager*)

- How do we make accurate counter-insider detection investments?
  - If supervisor accuracy and reliability is high, no further investment may be needed.
  - If accuracy and reliability is low, additional detectors may be needed to supplement supervisors.

- Can a methodology developed for the current requirement be generalized to address these problems?

Methodology

Methodology -1

Create scenarios containing potential risk indicators (PRI) that could realistically be encountered at the test site.

- Conducted multiple sessions with supervisors that represented all lines of business at the test site.
- Affinity grouped examples provided by supervisors into four categories.
  - Absentees/Tardy(s)
  - Financial Stressors (Lifestyle vulnerabilities)
  - Life Stressors (Affecting work)
  - Unauthorized Work Activities (Procedure violations)

Methodology -2

We created a scenario containing potential risk indicators (PRI) for each of the four categories.

- Each category then received three versions of the same scenario.
  - v1 – intended to elicit a response of “no concern”
  - v2 – intended to elicit a response of “some concern”
  - v3 – intended to elicit a response of “significant concern”

Notional Scenario – Absentee/Tardy (v1)

“The employee has had unscheduled absences 4 times in the last year. The employee is a single parent with a small child in daycare. On each absence the child was sick and could not attend day care, or be watched by the normal babysitter. The employee let you know immediately (before start of work) and either took Paid Time Off or made-up the work. The absences did not affect the mission or the overall performance of the employee.”

Notional Scenario – Absentee/Tardy (v2)

"The employee has had unscheduled absences 6 times in the last year. The employee said each time that they were sick. On two of those occasions, the employee did not inform you that they were sick until almost and hour after they were supposed to be at work. One of the employees' co-workers has mentioned to you that it puts a burden on them to have to "pull their weight" when the employee does this."

Notional Scenario – Absentee/Tardy (v3)

"The employee has had unscheduled absences 9 times in the last year. The employee said each time that they were sick. On four of those occasions, the employee did not inform you that they were sick until almost and hour after they were supposed to be at work. These absences tend to happen on Mondays. One of the employee's co-workers has told you that the employee tends to "party pretty hard" on the weekends. Three or four of the employees' co-workers has mentioned to you that it puts a burden on them to have to have to cover the workload for when the employee does this."

Methodology -3

Scenarios were then internally scored by nine volunteers with differing levels of experience in supervision and insider threat knowledge.

- Five experienced supervisors
- Four non-supervisors
- Six with knowledge of some/most PRI
- Three with little/no knowledge of PRI

Methodology -3

Results of internal scenario scoring indicated potential for developing baselines of over/under reporting for:

- Experienced supervisors (>5 years)
- Supervisors with some experience (2-5 years)
- New supervisors (<2 years)
- Those with good knowledge of PRI
- Those with little knowledge of PRI

Methodology -4

The scenarios were then provided to 12 PRP case managers at the test site for their scoring.

- All results not yet received (~40%)
- Final results will establish baseline expectations of case managers
- Once training of supervisors is completed, results from the training scenarios will be compared to the case manager expectations to attempt to produce the five baselines:
  - Experienced supervisors (>5 years)
  - Supervisors with some experience (2-5 years)
  - New supervisors (<2 years)
  - Those with good knowledge of PRI
  - Those with little knowledge of PRI

Transition Opportunities

Transition Opportunities

This methodology could be used in counter-insider training for:

- supervisors
- Practitioners (including role-based: HR, IA, IT, Security, etc.)
- case managers

Results from baselines could inform:

- investment spending for detection technologies
- changes to policies, procedures, and practices
- counter-insider training needs

Results compared over time could modify baselines and indicate improved resilience for organizations and counter-insider threat programs