<table>
<thead>
<tr>
<th>1. REPORT DATE</th>
<th>2. REPORT TYPE</th>
<th>3. DATES COVERED</th>
</tr>
</thead>
<tbody>
<tr>
<td>01 OCT 2014</td>
<td>N/A</td>
<td>-</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>4. TITLE AND SUBTITLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insider Threat Models</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>5a. CONTRACT NUMBER</th>
<th>5b. GRANT NUMBER</th>
<th>5c. PROGRAM ELEMENT NUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>5d. PROJECT NUMBER</th>
<th>5e. TASK NUMBER</th>
<th>5f. WORK UNIT NUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>6. AUTHOR(S)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Matthew L. Collins</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>8. PERFORMING ORGANIZATION REPORT NUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>10. SPONSOR/MONITOR’S ACRONYM(S)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>11. SPONSOR/MONITOR’S REPORT NUMBER(S)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>12. DISTRIBUTION/AVAILABILITY STATEMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approved for public release, distribution unlimited</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>13. SUPPLEMENTARY NOTES</th>
</tr>
</thead>
<tbody>
<tr>
<td>The original document contains color images.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>14. ABSTRACT</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>15. SUBJECT TERMS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>16. SECURITY CLASSIFICATION OF:</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. REPORT unclassified</td>
</tr>
<tr>
<td>b. ABSTRACT unclassified</td>
</tr>
<tr>
<td>c. THIS PAGE unclassified</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>17. LIMITATION OF ABSTRACT</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAR</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>18. NUMBER OF PAGES</th>
</tr>
</thead>
<tbody>
<tr>
<td>17</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>19a. NAME OF RESPONSIBLE PERSON</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>
Notices

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

This material has been approved for public release and unlimited distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

Carnegie Mellon® and CERT® are registered marks of Carnegie Mellon University.

DM-0001680
System Dynamics Approach

A method and supporting toolset

- To holistically model, document, and analyze
- Complex problems as they evolve over time
- And develop effective mitigation strategies
- That balance competing concerns

System Dynamics supports simulation to

- Validate characterization of problem
- Test out alternate mitigation strategies
The dynamic behavior of a system is captured by its feedback structure.

- By decomposing the causal structure of the system into its feedback loops, and
- Understanding which loop is strongest (dominating) at a given point in time,
- One can understand and communicate the system’s behavior over time

SD approach emphasizes endogenous viewpoint

- “System” boundary is defined based on scope of the problem
- Includes soft as well as hard factors
- Different than conventional (“hard”) operations research
Typical SD Modeling and Analysis Approach

1. Define problem
2. Develop initial dynamic hypothesis

→
3. Refine SD model of problematic behavior

→
4. Analyze/test model and propose mitigations

→
5. Show how proposed mitigations reduce the problematic behavior

→
6a. Refine dynamic hypothesis or proposed mitigations and iterate

OR

6b. Declare modeling effort complete
Payoffs for SD Analysis

Policy/practitioner guidance for improvement

Training course development and enhancement

Management decision support tool development

Depending on assumptions made, payoffs may benefit

- Individual organization
- Select group of organizations (e.g., critical infrastructure sector)
- Organizations in general
Representing Feedback Structure

System Dynamics models represent abstract behavior of system over time

Model variables represent system elements that are important to understand and represent essential behavior

Feedback structure represented using influence diagrams
Variable – anything of interest in the problem being modeled.

Ghost Variable – variable acting as a placeholder for a variable occurring somewhere else

Positive Influence – values of variables move in the same direction (e.g., source increases, target increases)

Negative Influence – values of variables move in the opposite direction (e.g., source increases, the target decreases)

Delay – significant delay from when Var1 changes to when Var2 changes
Balancing Loop – a feedback loop that moves variable values to a goal state; loop color identifies circular influence path.

Reinforcing Loop – a feedback loop that moves variable values consistently upward or downward; loop color identifies circular influence path.

Stock – special variable representing a pool of materials, money, people, or other resources.

Flow – special variable representing a process that directly adds to or subtracts from a stock.

Cloud – source or sink (represents a stock outside the model boundary)
Abstract Model of Insider IT Sabotage

disgruntlement

sanctions

insider's unmet expectation

insider's expectation

personal predisposition

expectation fulfillment

precipitating event

behavioral monitoring

technical monitoring

discovery of precursors

behavioral precursor

technical precursor

actual risk of insider attack

perceived risk of insider attack

org's trust of insider

ability to conceal activity

unknown access paths

acquiring unknown paths
Insider Fraud Model: High Level Positions

1. **Insider's Incentive**
   - Having "no other option"
   - Will "make things right"

2. **Insider's Rationalization**
   - Insider's personal need
   - Insider's financial benefit due to fraud

3. **Insider's Opportunity**
   - Insider's activities related to fraud

4. **Resolving Problems**
   - Insider's perceived need
   - Insider's perceived loss if caught
   - Insider's actual risk of getting caught
   - Insider's perceived weakness of fraud controls

5. **Growth of Need**
   - Insider's financial benefit due to fraud

6. **Social Engineering**
   - Other employees
   - Employees' suspicions

7. **Anonymous Reporting**
   - Insider's concealment
     - Limiting exposure of fraud
     - Flying Below the Radar

8. **Fraud Prevention Controls**
   - Insider promoted to more trusted position
   - Duration of insider's loyal service in positions of trust
   - Total loss to org
   - Avg org loss per month

9. **Org Opportunity to Detect**
   - Insider's age
   - Duration of fraud
   - Org opportunity to detect

10. **Mandatory Vacations**
    - Org knowledge of fraud

11. **Privilege Given to Insider**
    - Org trust through tenure
    - Insider promoted to more trusted position

12. **Extant Insider Trusted by Org**
    - Insider promoted to more trusted position

13. **Insider Trust Trap**
    - Insider promoted to more trusted position
    - Duration of insider's loyal service in positions of trust
    - Total loss to org
    - Avg org loss per month

14. **Deterrence Effect of Fraud Detection**
    - Insider's perceived need
    - Insider's perceived risk overall

15. **Org Knowledge of Fraud**
    - Insider's actual risk of getting caught
    - Insider promoted to more trusted position

16. **Avg Org Loss per Month**
    - Insider's actual risk of getting caught
    - Insider promoted to more trusted position

17. **Total Loss to Org**
    - Insider's actual risk of getting caught
    - Insider promoted to more trusted position

18. **Org Opportunity to Detect**
    - Insider's actual risk of getting caught
    - Insider promoted to more trusted position

19. **Mandatory Vacations**
    - Insider's actual risk of getting caught
    - Insider promoted to more trusted position

20. **Privilege Given to Insider**
    - Insider's actual risk of getting caught
    - Insider promoted to more trusted position

21. **Org Knowledge of Fraud**
    - Insider's actual risk of getting caught
    - Insider promoted to more trusted position

22. **Deterrence Effect of Fraud Detection**
    - Insider's perceived need
    - Insider's perceived risk overall

23. **Insider Trust Trap**
    - Insider's actual risk of getting caught
    - Insider promoted to more trusted position

24. **Org Knowledge of Fraud**
    - Insider's actual risk of getting caught
    - Insider promoted to more trusted position

25. **Mandatory Vacations**
    - Insider's actual risk of getting caught
    - Insider promoted to more trusted position

26. **Privilege Given to Insider**
    - Insider's actual risk of getting caught
    - Insider promoted to more trusted position

27. **Org Knowledge of Fraud**
    - Insider's actual risk of getting caught
    - Insider promoted to more trusted position

28. **Deterrence Effect of Fraud Detection**
    - Insider's perceived need
    - Insider's perceived risk overall

29. **Insider Trust Trap**
    - Insider's actual risk of getting caught
    - Insider promoted to more trusted position

30. **Org Knowledge of Fraud**
    - Insider's actual risk of getting caught
    - Insider promoted to more trusted position

31. **Mandatory Vacations**
    - Insider's actual risk of getting caught
    - Insider promoted to more trusted position

32. **Privilege Given to Insider**
    - Insider's actual risk of getting caught
    - Insider promoted to more trusted position

33. **Org Knowledge of Fraud**
    - Insider's actual risk of getting caught
    - Insider promoted to more trusted position

34. **Deterrence Effect of Fraud Detection**
    - Insider's perceived need
    - Insider's perceived risk overall

35. **Insider Trust Trap**
    - Insider's actual risk of getting caught
    - Insider promoted to more trusted position

36. **Org Knowledge of Fraud**
    - Insider's actual risk of getting caught
    - Insider promoted to more trusted position

37. **Mandatory Vacations**
    - Insider's actual risk of getting caught
    - Insider promoted to more trusted position

38. **Privilege Given to Insider**
    - Insider's actual risk of getting caught
    - Insider promoted to more trusted position

39. **Org Knowledge of Fraud**
    - Insider's actual risk of getting caught
    - Insider promoted to more trusted position

40. **Deterrence Effect of Fraud Detection**
    - Insider's perceived need
    - Insider's perceived risk overall

41. **Insider Trust Trap**
    - Insider's actual risk of getting caught
    - Insider promoted to more trusted position

42. **Org Knowledge of Fraud**
    - Insider's actual risk of getting caught
    - Insider promoted to more trusted position

43. **Mandatory Vacations**
    - Insider's actual risk of getting caught
    - Insider promoted to more trusted position

44. **Privilege Given to Insider**
    - Insider's actual risk of getting caught
    - Insider promoted to more trusted position

45. **Org Knowledge of Fraud**
    - Insider's actual risk of getting caught
    - Insider promoted to more trusted position

46. **Deterrence Effect of Fraud Detection**
    - Insider's perceived need
    - Insider's perceived risk overall

47. **Insider Trust Trap**
    - Insider's actual risk of getting caught
    - Insider promoted to more trusted position

48. **Org Knowledge of Fraud**
    - Insider's actual risk of getting caught
    - Insider promoted to more trusted position

49. **Mandatory Vacations**
    - Insider's actual risk of getting caught
    - Insider promoted to more trusted position

50. **Privilege Given to Insider**
    - Insider's actual risk of getting caught
    - Insider promoted to more trusted position

51. **Org Knowledge of Fraud**
    - Insider's actual risk of getting caught
    - Insider promoted to more trusted position
Insider Fraud Model: Low Level Positions

- Insider's perceived risk overall
- Insider's personal problems
- Insider's perceived loss if caught
- Insider's perceived weakness of fraud controls
- Insider's low position in org

- Desire to help family and friends
- Insider's incentive
- Insider's rationalization
- Insider's opportunity

- Insider's activities related to fraud
- Insider's financial benefit due to fraud
- Insider's actual risk of getting caught
- Insider's perceived need

- Resolving Problems
- Growth of Need
- Deterrence Effect of Fraud Detection

- Org opportunity to detect insider activities
- Fraud detection controls
- Mandatory vacations
- Employees' suspicions
- Anonymous reporting

- Org opportunity to detect outsider activities
- Outsider financial benefit due to fraud
- Outsider facilitation of fraud

- Outsider pressure on insider to continue fraud
- Will "make things right"
- Having "no other option"

- Growing Pressure from Outsiders
- Fraud prevention controls
- Employees' suspicions
- Org knowledge of fraud

- Growing of Fraud Business
- Extent of fraud committed

- Cert Software Engineering Institute | Carnegie Mellon
Insider IP Theft Model: Entitled Independent

1. Insider predisposition to feeling entitled
2. Insider contribution to developing information or product
3. Insider sense of entitlement to products of the group
4. Insider desire to contribute to organization
5. Insider sense of loyalty to organization
6. Insider planning to go to competing organization
7. Precipitating event (e.g., proposal by competitor)
8. Information stolen
9. Exposure of theft to org
10. Insider concern over being caught
11. Insider time and resources invested in group
12. Insider dissatisfaction with job/organization
13. Organization denial of insider requests
14. Insider desire to steal org information

(R1) Insider contribution to organizational group
(R2) Insider sense of entitlement to products of the group
Insider IP Theft Model: Ambitious Leader

- **Insider commitment to competitor/side business**
- **Insider time and resources invested in plan**
- **Insider planning to go to competing organization**
- **Insider recruitment of other insiders**
- **Insider increasing access to information**
- **Precipitating event (e.g., proposal by competitor)**
- **Information stolen**
- **Exposure of theft to org**
- **Org knowledge of theft**
- **Org discovery of deceptions**

- **Insider desire to contribute to organization**
- **Insider sense of loyalty to organization**
- **Insider desire to steal org info**
- **Insider concern over being caught**
- **Insider perpetrated deceptions related to the info theft**
- **Insider’s awareness that org cares about theft**
- **Org discovery of deceptions**

- **Insider planning to steal org info**
- **Insider extent of planning to steal org info**

- **Insider sense of entitlement to products of the group**
- **Insider sentiment toward group**
- **Insider organizational group commitment**
- **Insider organizational group focus**
- **Insider organizational group contribution**
- **Insider organizational group mindset**
- **Insider organizational group planning**
- **Insider organizational group commitment to competitor/side business**

- **Insider predisposition to feeling entitled**
- **Insider organizational group contribution**
- **Insider organizational group desire to contribute to organization**
- **Insider organizational group desire to steal org info**
- **Insider organizational group concern over being caught**
- **Insider organizational group perpetrated deceptions related to the info theft**
- **Insider organizational group’s awareness that org cares about theft**
- **Org organizational group discovery of deceptions**

- **Org organizational group knowledge of theft**
- **Org organizational group discovery of deceptions**
- **Org organizational group level of technical and behavioral monitoring**

- **Org organizational group extent of technical and behavioral monitoring**
- **Org organizational group contrary to the organization**
- **Org organizational group desire to contribute to organization**
- **Org organizational group desire to steal org info**
- **Org organizational group concern over being caught**
- **Org organizational group perpetrated deceptions related to the info theft**
- **Org organizational group’s awareness that org cares about theft**
- **Org organizational group discovery of deceptions**

- **Org organizational group extent of technical and behavioral monitoring**
- **Org organizational group contrary to the organization**
- **Org organizational group desire to contribute to organization**
- **Org organizational group desire to steal org info**
- **Org organizational group concern over being caught**
- **Org organizational group perpetrated deceptions related to the info theft**
- **Org organizational group’s awareness that org cares about theft**
- **Org organizational group discovery of deceptions**
Points of Contact
Matthew Collins
CERT Insider Threat Center
Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh, PA 15213-3890
+1 412 268-9152 – Phone
mlcollins@cert.org – Email

Questions?