Insider Threat Models

Matthew Collins
CERT Insider Threat Center

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
01 OCT 2014	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Insider Threat Models	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
Matthew L. Collins	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**SAR**	**17**	

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.

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

Powerful Tenet of SD

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

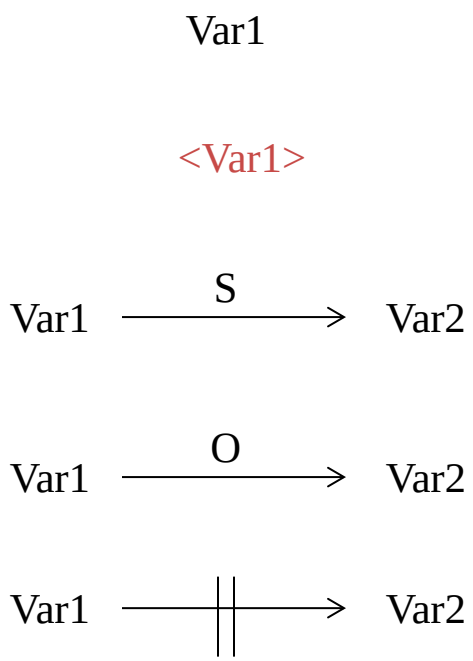
Representing Feedback Structure

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

System Dynamics Primer



Variable – anything of interest in the problem being modeled.

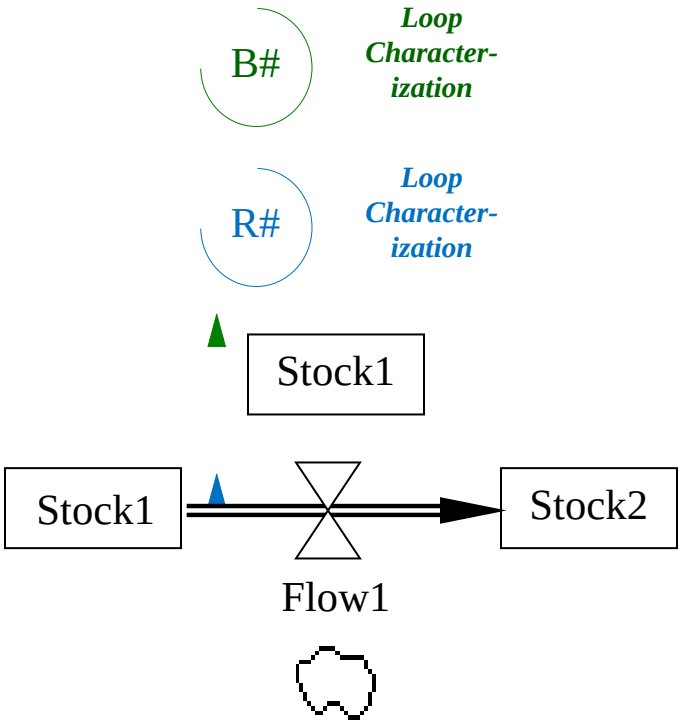
Ghost Variable – variable acting as a placeholder for a variable occurring somewhere else

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

System Dynamics Primer – Continued



Balancing Loop – a feedback loop that moves variable values to a goal state; loop color identifies circular influence path

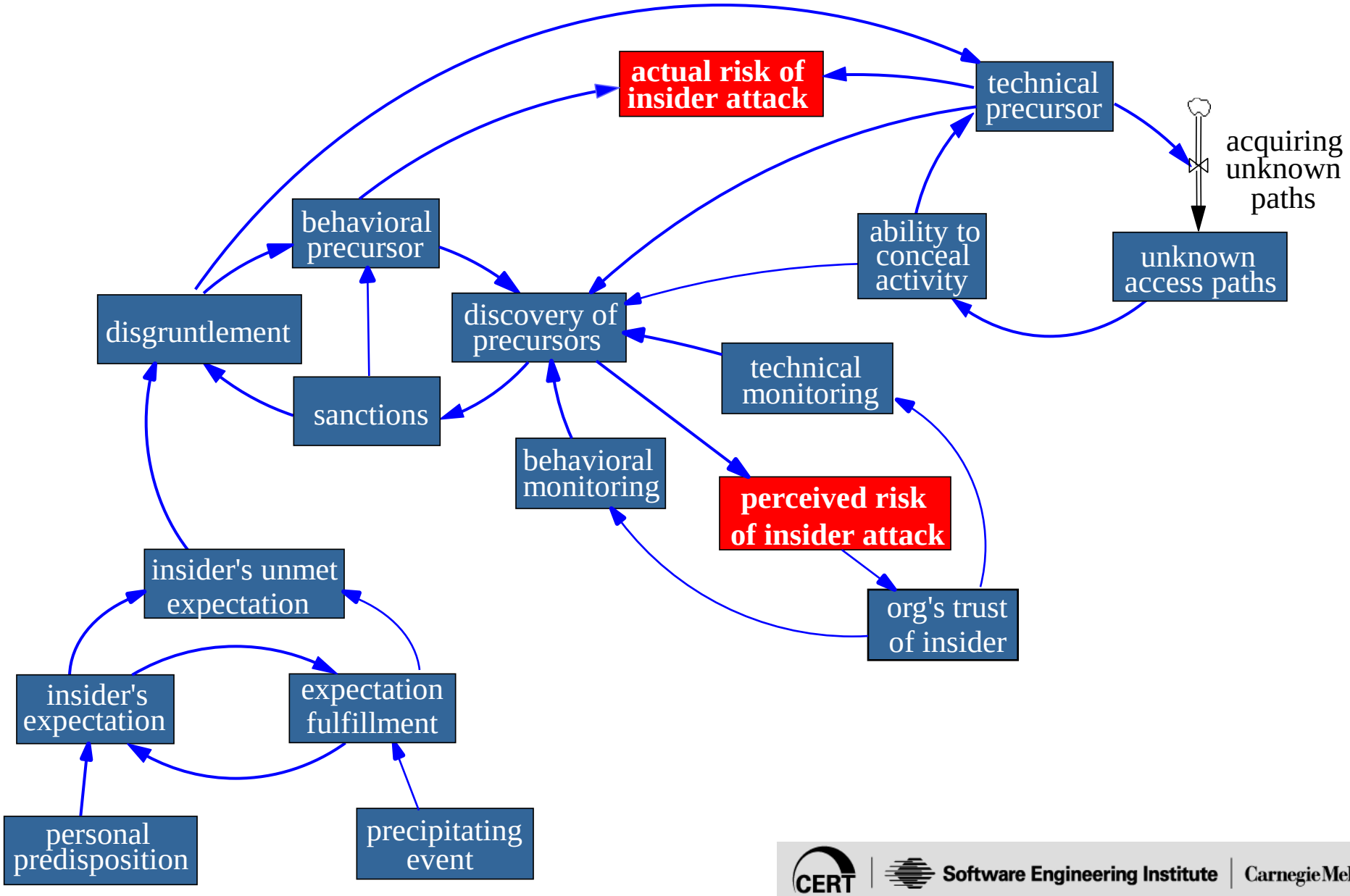
Reinforcing Loop – a feedback loop that moves variable values consistently upward or downward; loop color identifies circular influence path

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

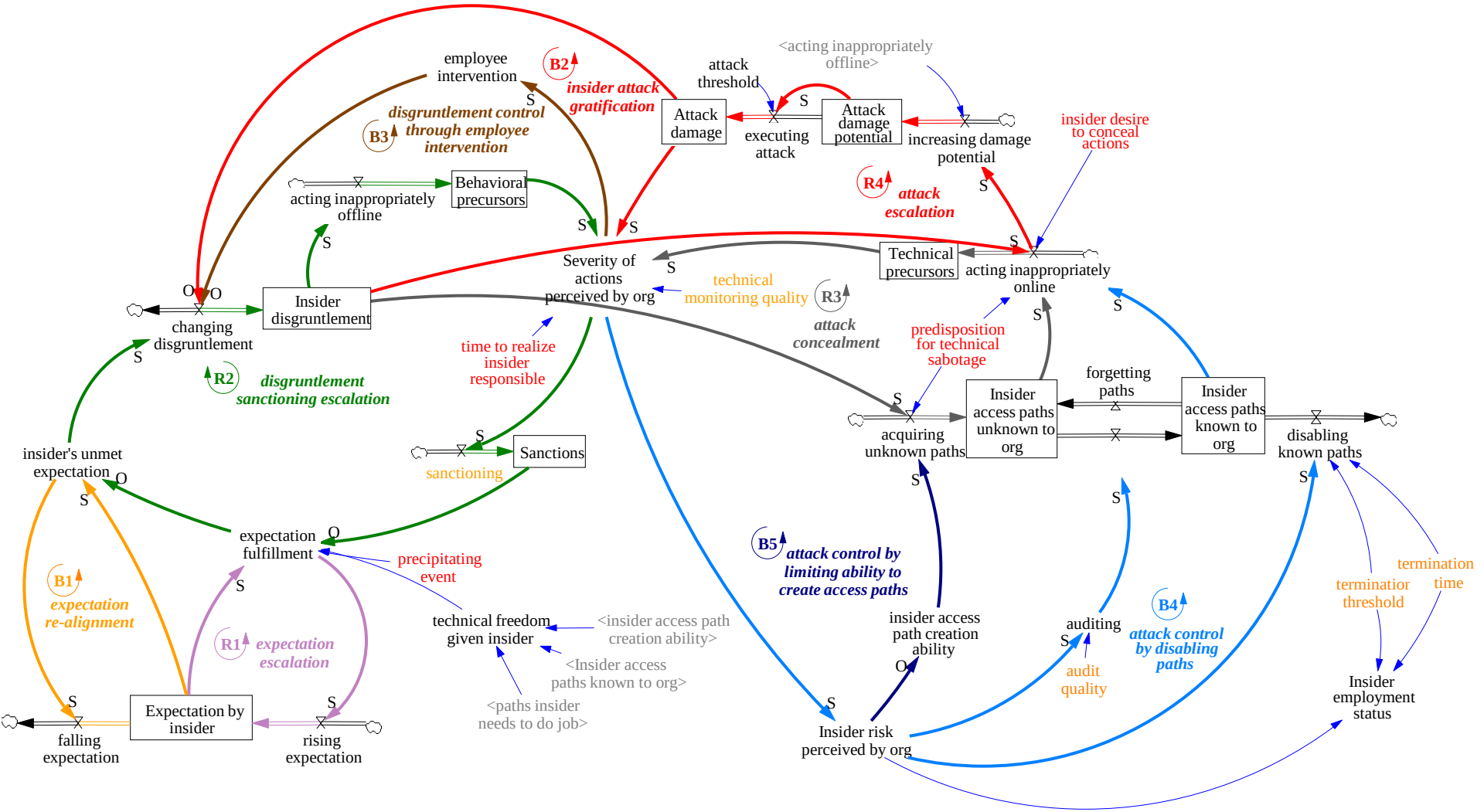
Flow – special variable representing a process that directly adds to or subtracts from a stock.

Cloud – source or sink (represents a stock outside the model boundary)

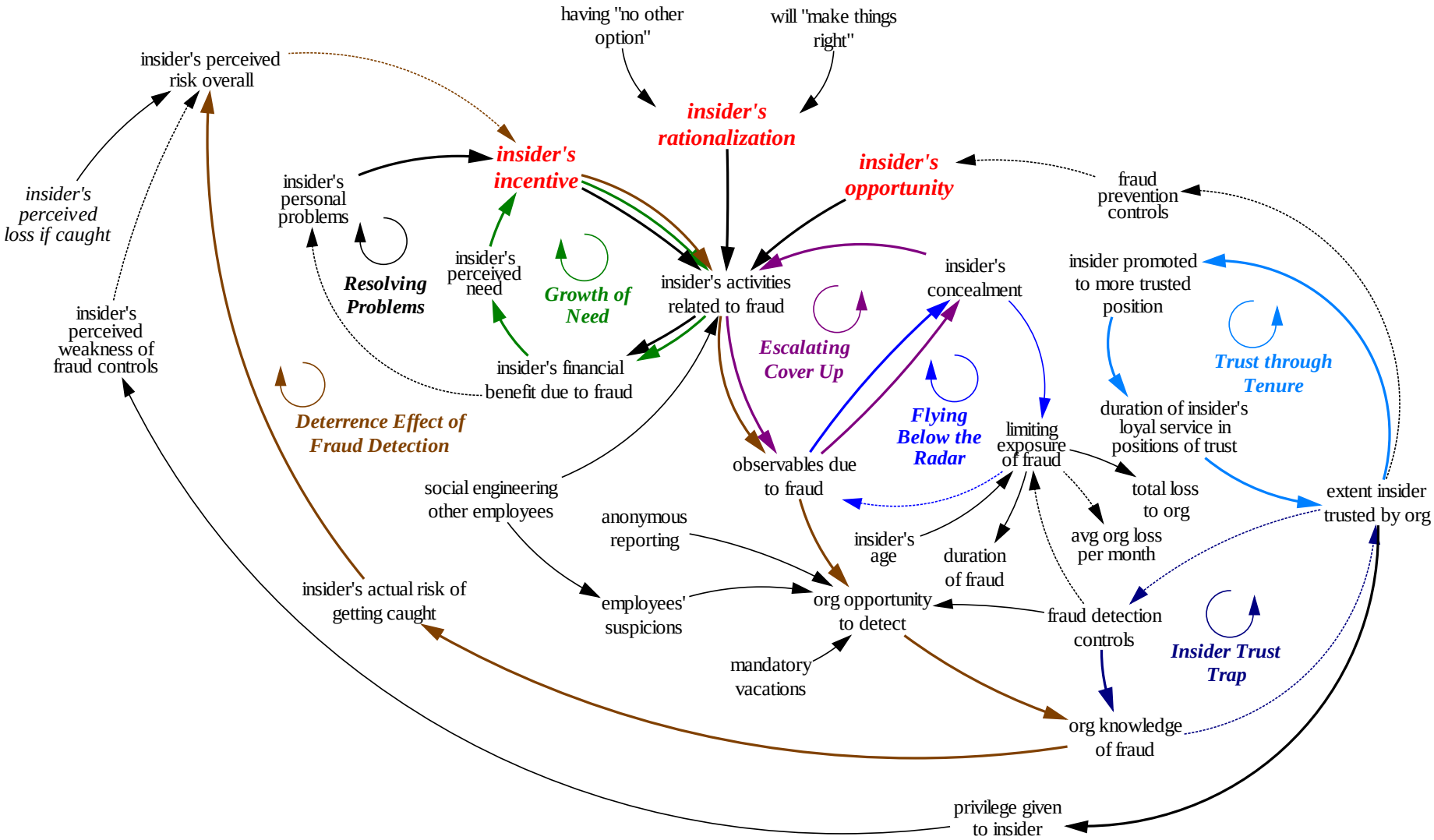
Abstract Model of Insider IT Sabotage



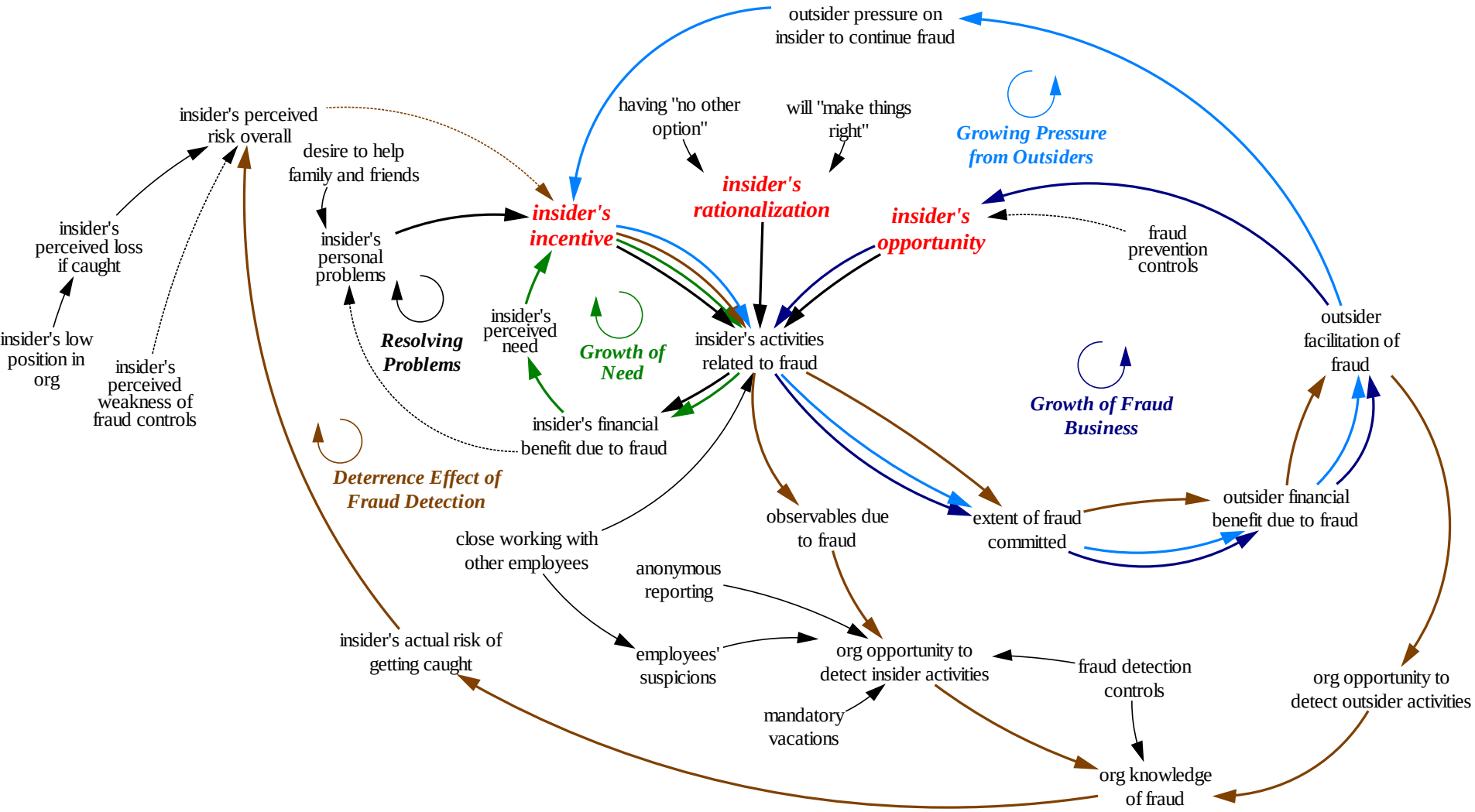
Simulation Model of Insider IT Sabotage



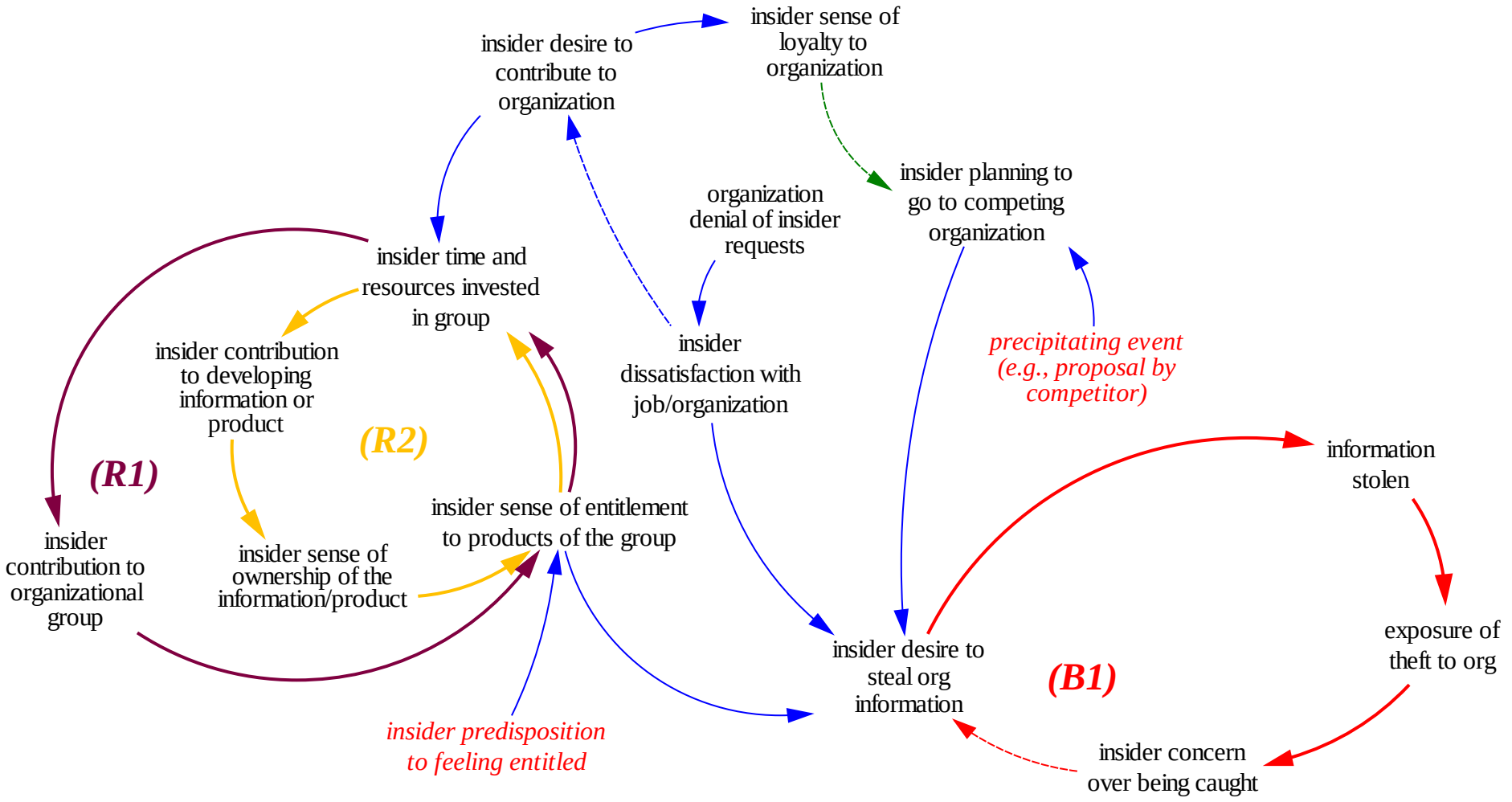
Insider Fraud Model: High Level Positions



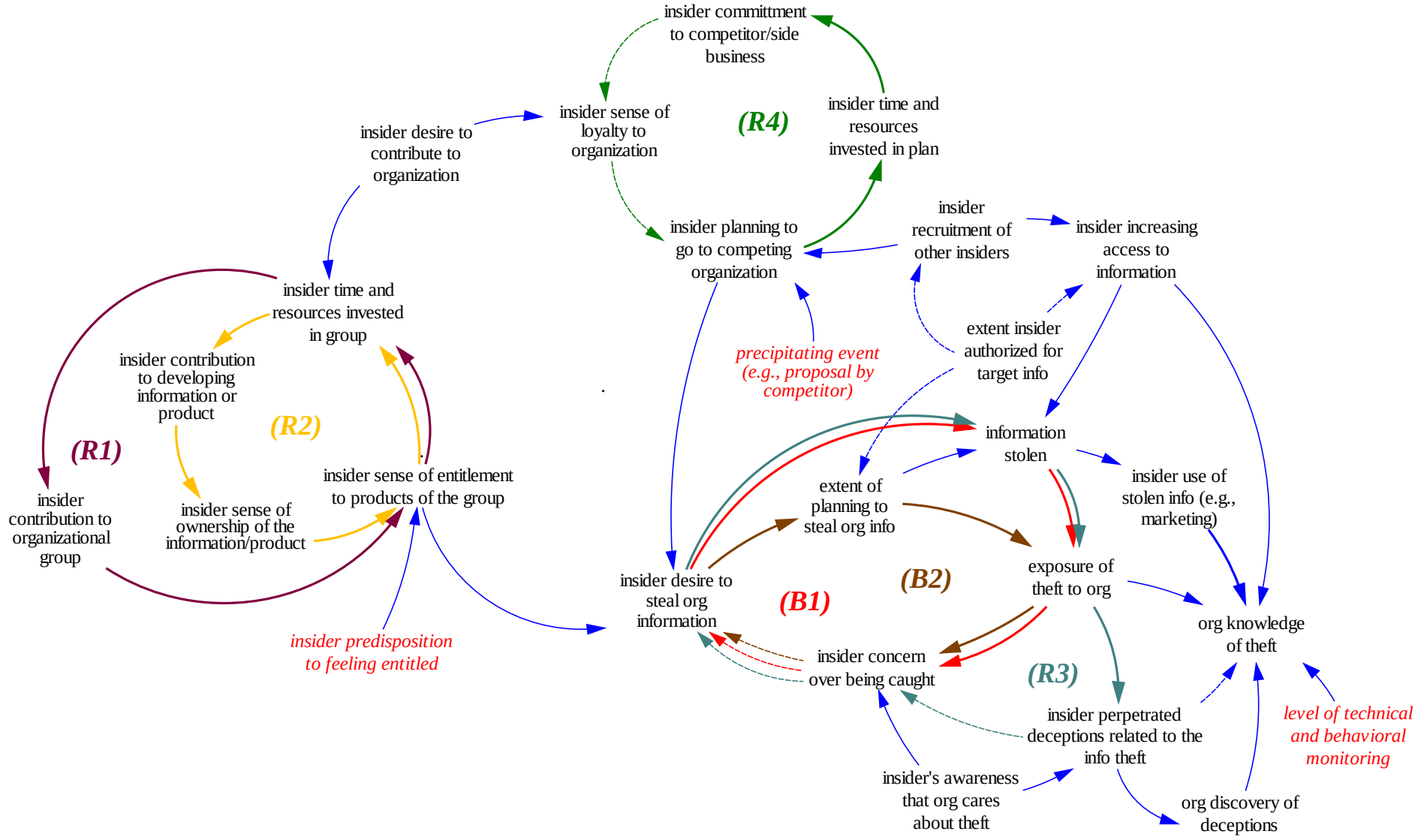
Insider Fraud Model: Low Level Positions



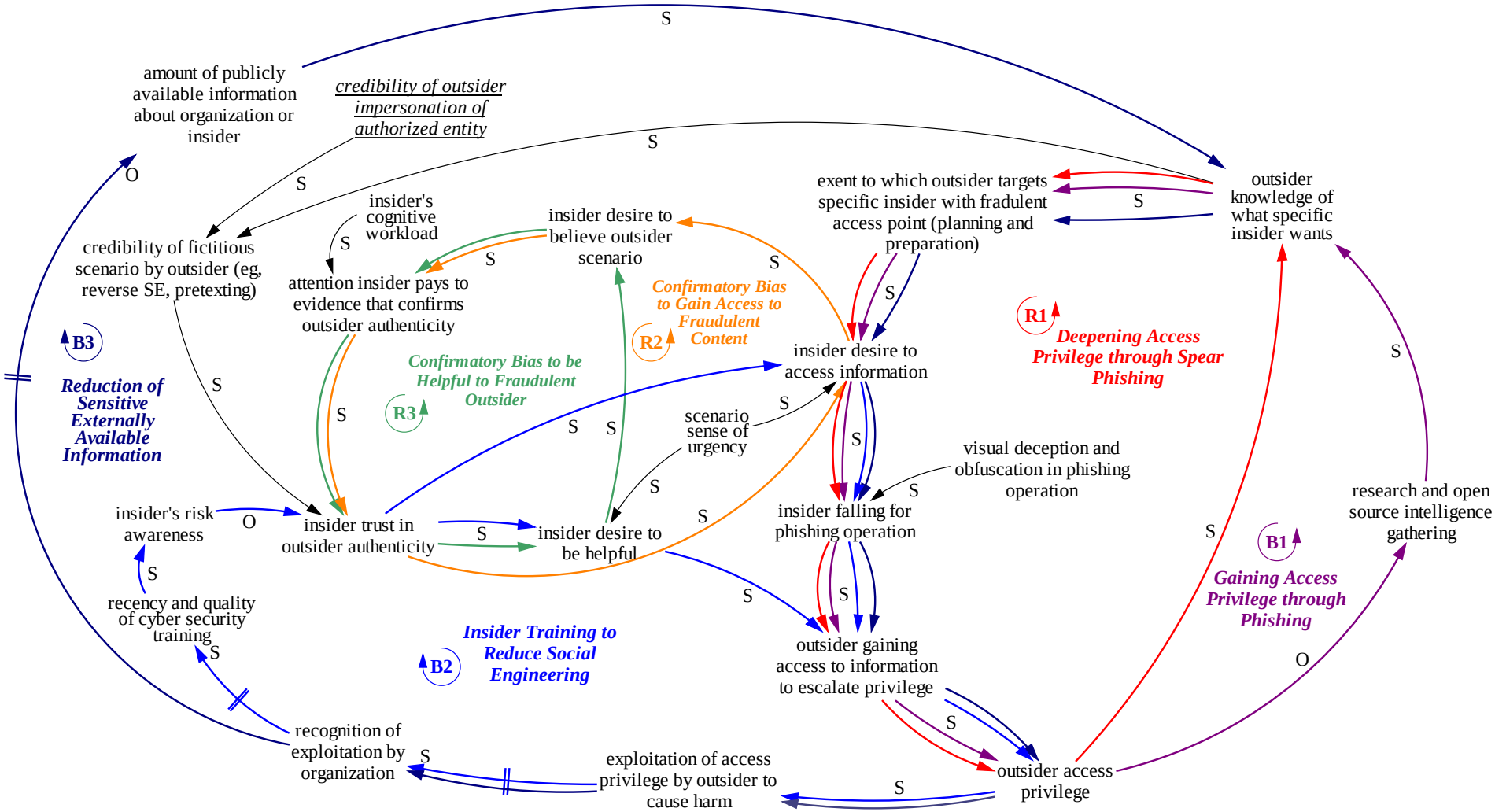
Insider IP Theft Model: Entitled Independent



Insider IP Theft Model: Ambitious Leader



Unintentional Insider Threat Model



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?