



Insider Threat Models

Matthew Collins
CERT Insider Threat Center



Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE 01 OCT 2014		2. REPORT TYPE N/A		3. DATES COVERED -	
4. TITLE AND SUBTITLE Insider Threat Models				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S) Matthew L. Collins				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213				8. PERFORMING ORGANIZATION REPORT NUMBER	
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 unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

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

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

Var1

<Var1>

Var1 \xrightarrow{S} Var2

Var1 \xrightarrow{O} Var2

Var1 $\xrightarrow{||}$ Var2

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



Flow1



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

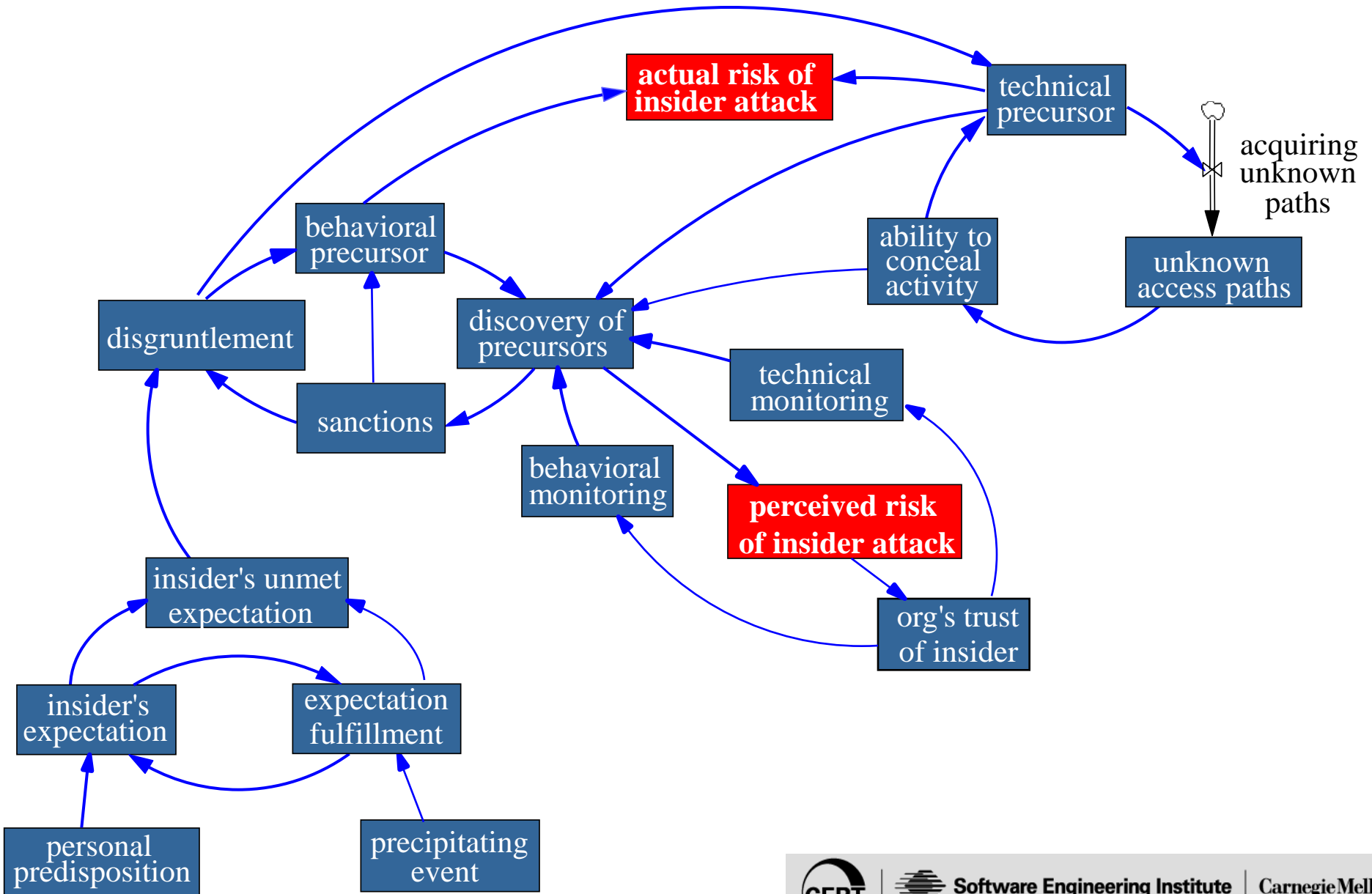
Reinforcing Loop – a feedback loop that moves variable values consistently upward or downward; loop color identifies circular influence path

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

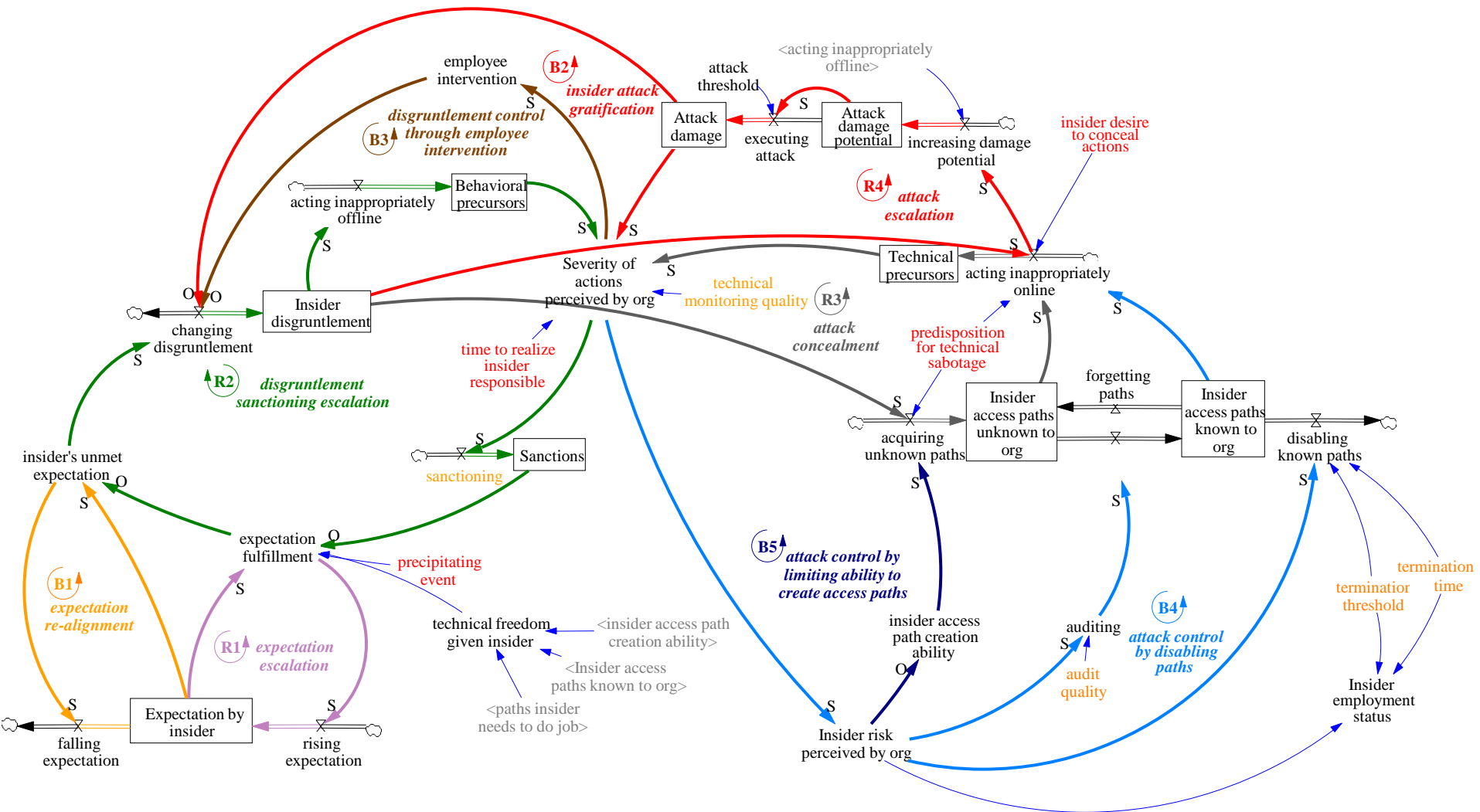
Flow – special variable representing a process that directly adds to or subtracts from a stock.

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

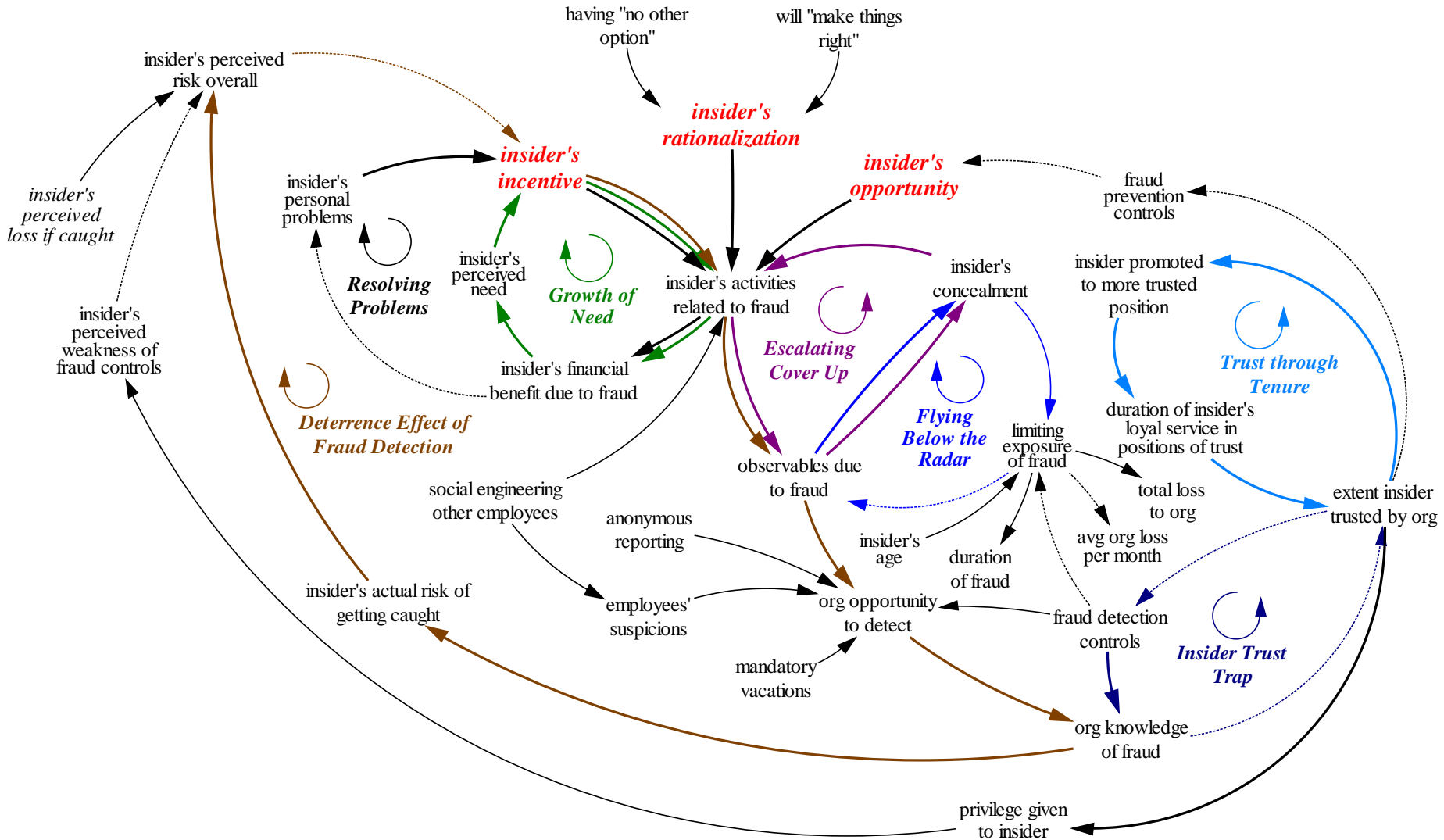
Abstract Model of Insider IT Sabotage



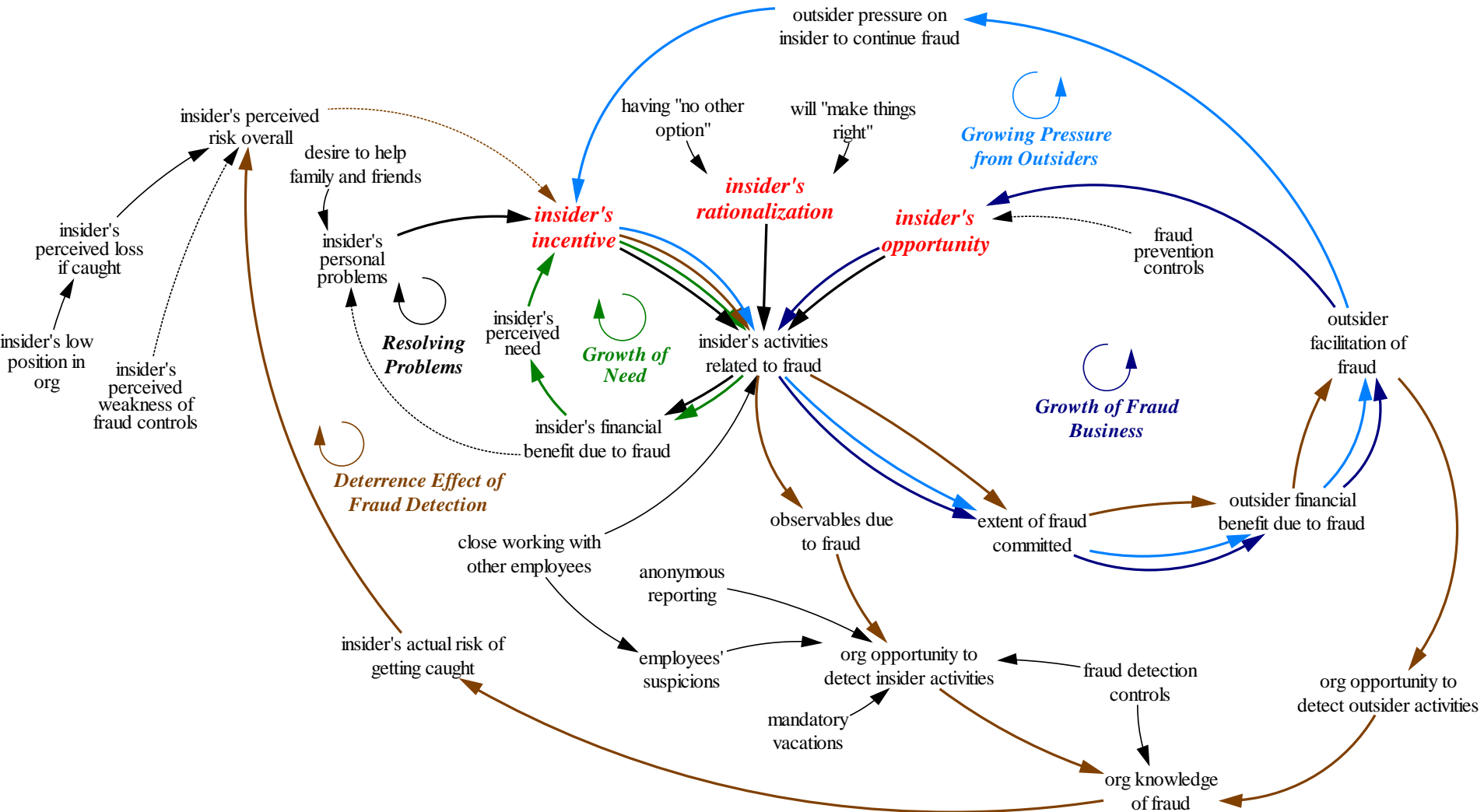
Simulation Model of Insider IT Sabotage



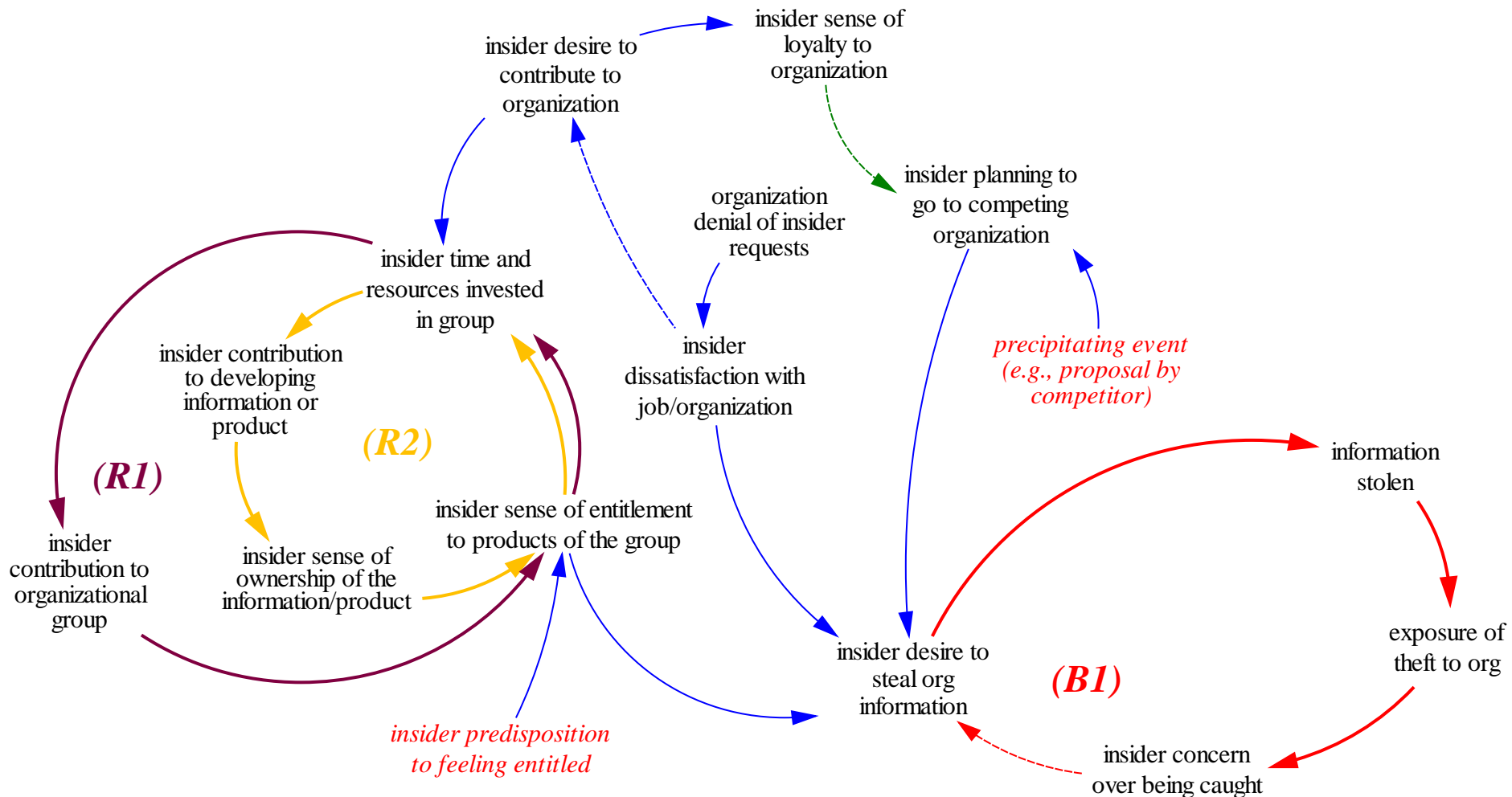
Insider Fraud Model: High Level Positions



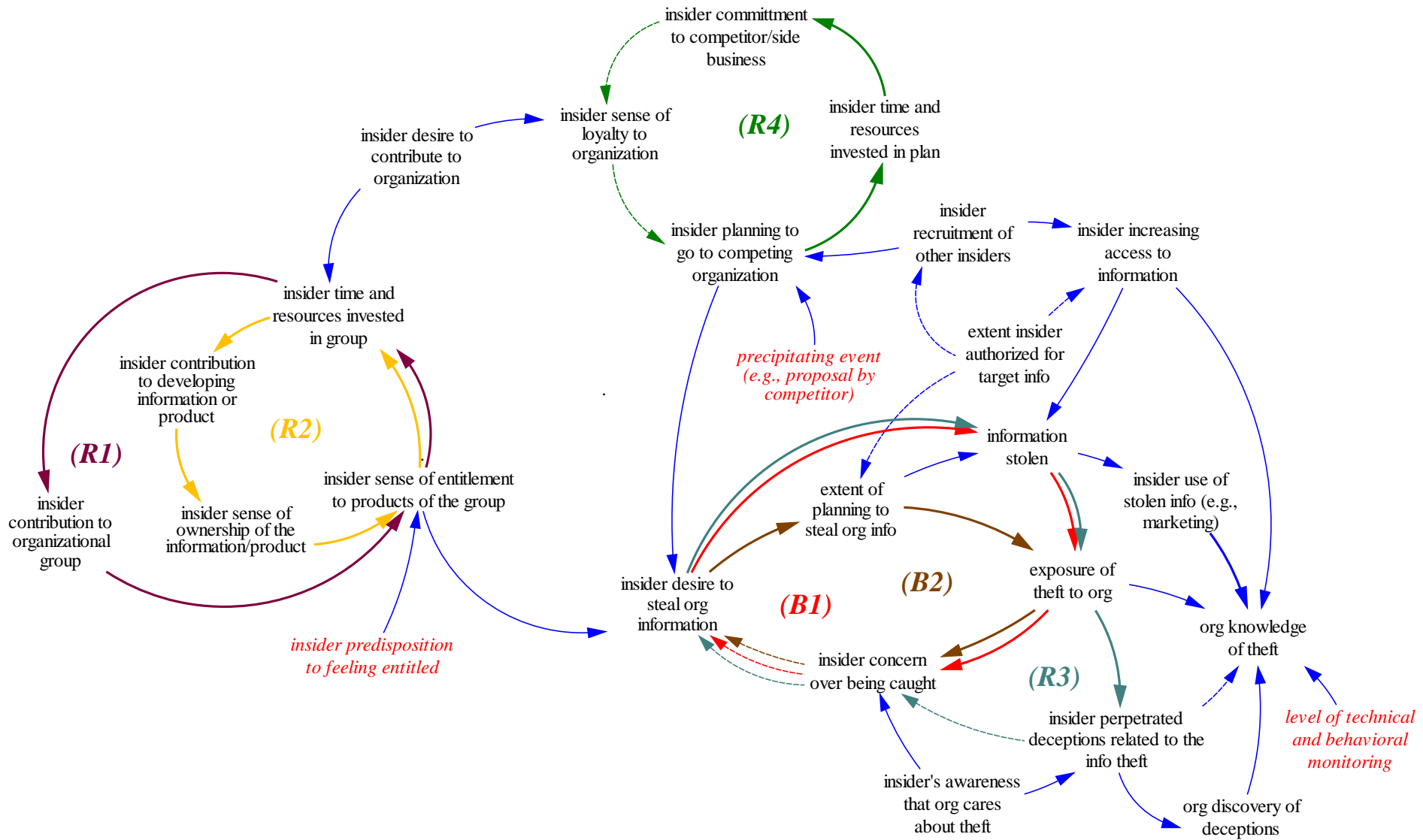
Insider Fraud Model: Low Level Positions



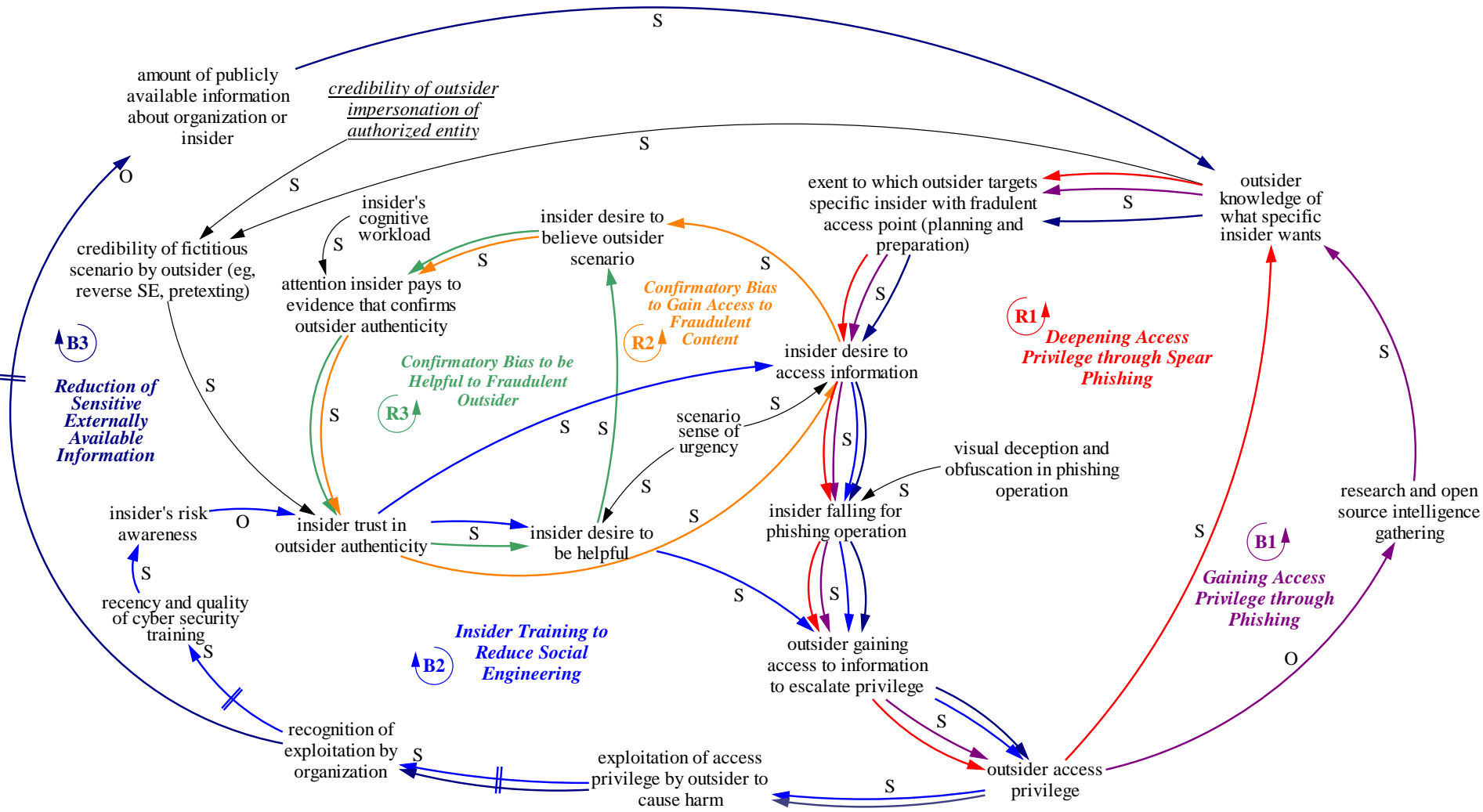
Insider IP Theft Model: Entitled Independent



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?

