Social Network Dynamics of Insider Threats: How do Job Engagement & Insider Espionage Relate?

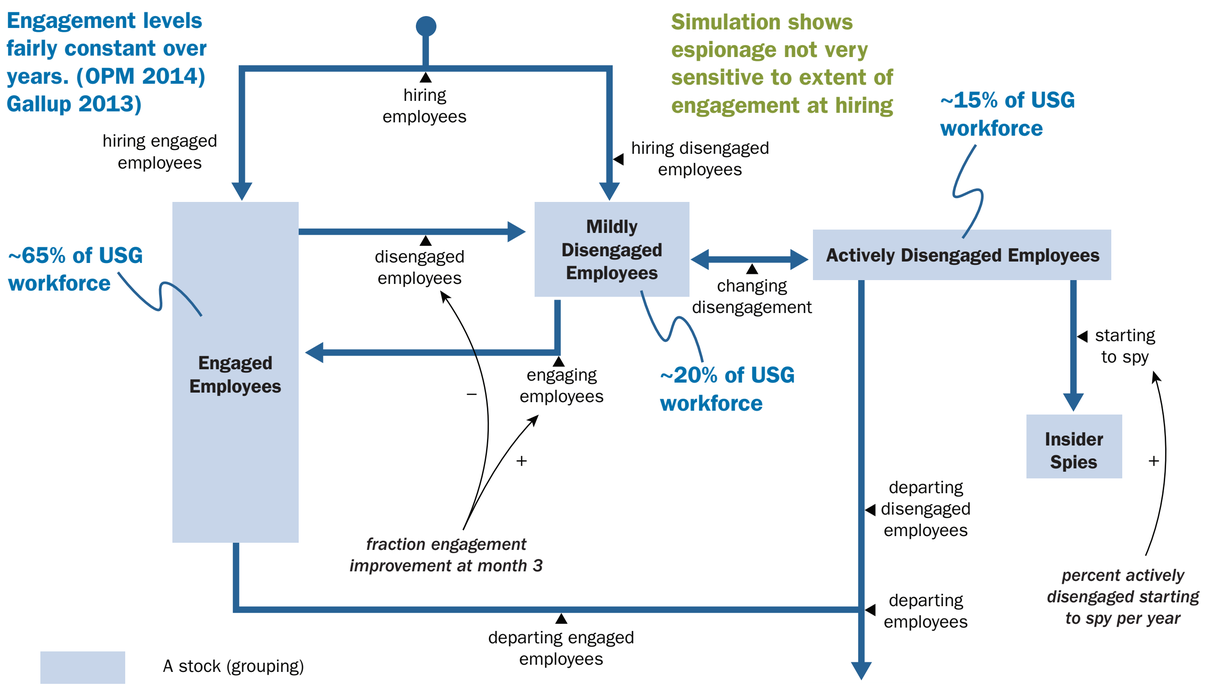
Empirical analysis of insider espionage incidents (non-moles) show spy disengagement at work and home. A system dynamics (SD) model explains social network changes & helps analyze benefits of greater job engagement.

Approach:

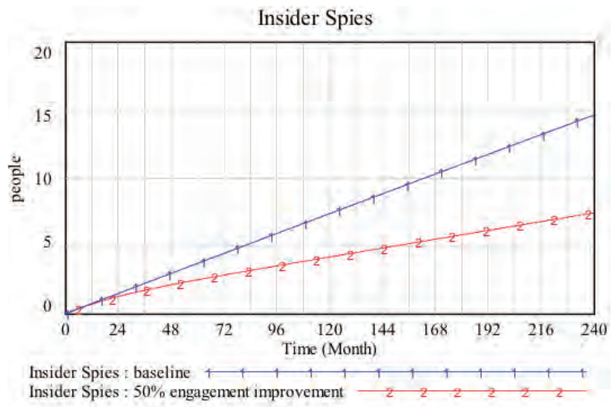
- Disincentive espionage by attracting cooperation through positive incentives, complementing coercive approaches
- Indicators of disengagement alert first-line managers to sustain productivity/retention (lessens impact of false positives)
- Serious or continuing disengagement reviewed by investigators for action
- Social network analysis of spy incidents with SD model providing link to theory

Key Challenge: Distinguish employee engaged in job from spy gathering intel

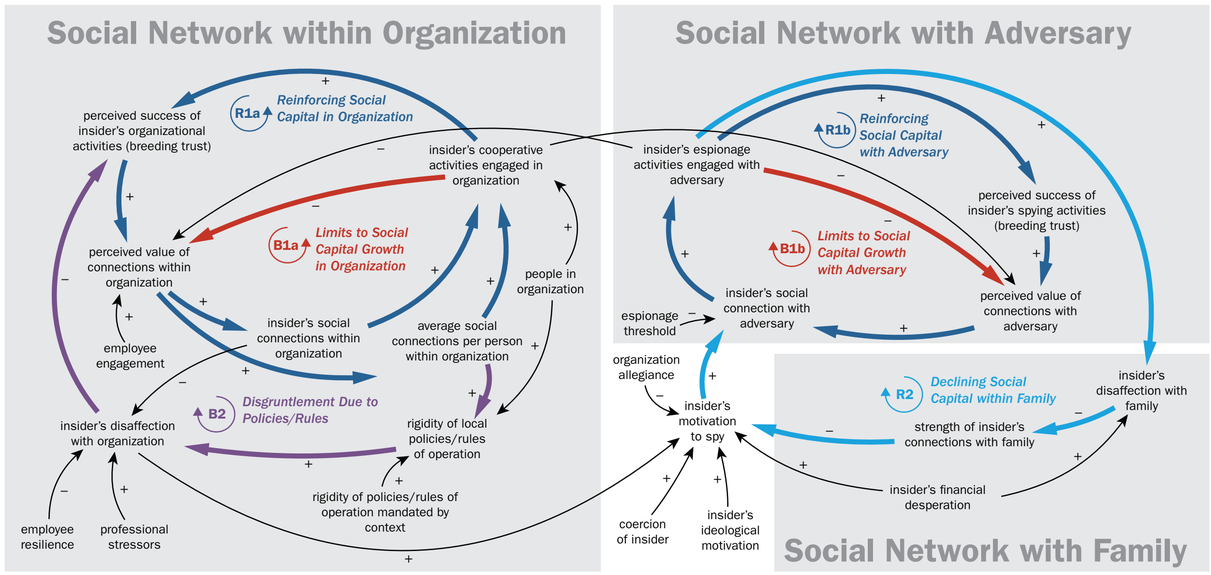
An Emerging Physics of Job Engagement and Insider Espionage



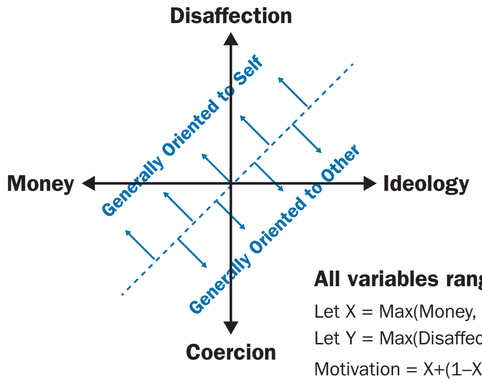
Preliminary Finding: Spying decreases with greater employee job engagement, but other sociotechnical measures likely needed.



Social Network Dynamics of Spy Disengagement with Work and Family

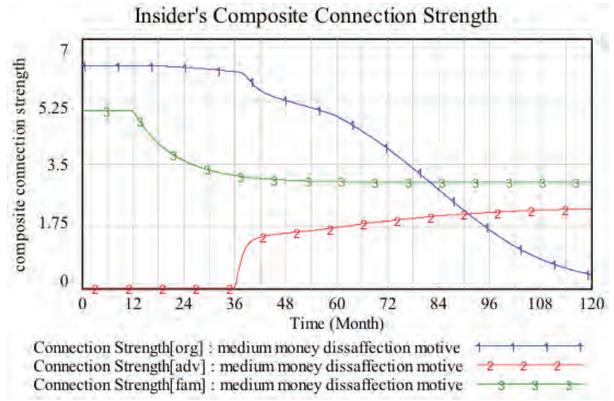


Two-Dimensional Spy Motivation Space



All variables range 0 to 1:

Let X = Max(Money, Ideology)
Let Y = Max(Disaffection, Coercion)
Motivation = X+(1–X)*Y
Motivation to Spy
= Motivation
* (1 – Org Allegiance)
* (1 – Family Connection)



Future Work: Refine & Validate Model

- Measure level of spy disengagement
- Interview orgs to determine relationship among engagement, practices, & theft
- Develop a disengagement analysis and response tool based on SD model/ORA

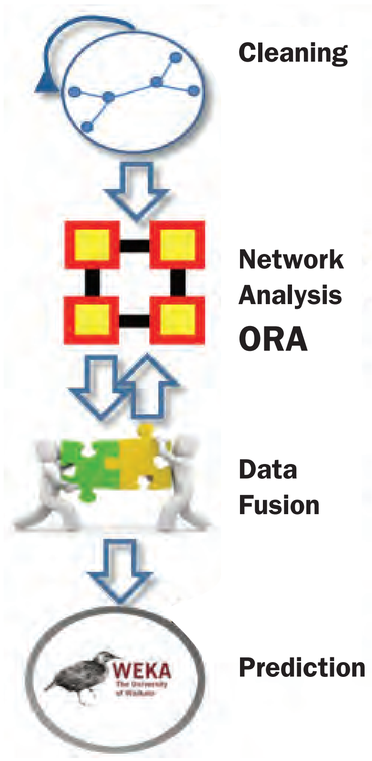
Neal W. Altman, Matthew L. Collins
Contact: Andrew P. Moore apm@cert.org Kathleen M. Carley kathleen.carley@cs.cmu.edu

Dynamic Networks of Insider Threats – Growing Holes

Dynamic network metrics can be used to identify those people who are potential insider threats. The key: they grow structural holes and have unusual betweenness.

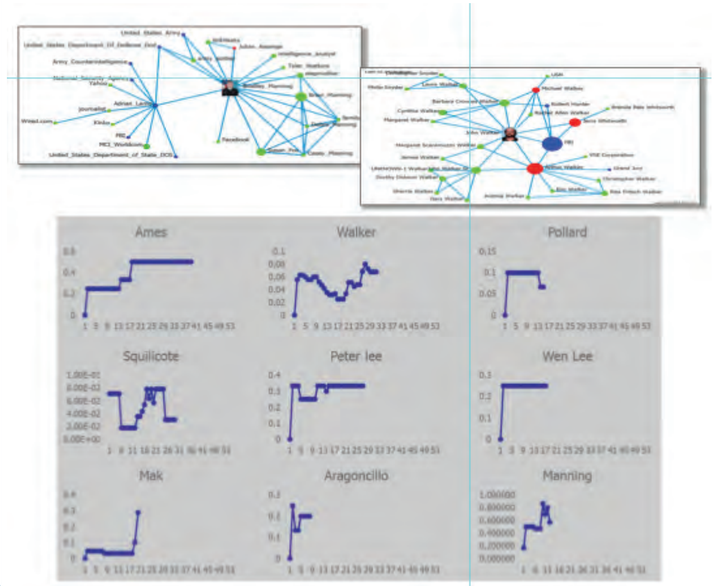
Approach

- Dynamic meta-networks—linking people, personality traits, organizational role traits
- Case Studies: 9 espionage cases
  - Extract dynamic networks
  - Compare networks using graph techniques
- Email Studies: Enron corpus
  - Use machine learning to characterize insiders based on network metrics
  - Use machine learning to characterize insiders using other features derived from case studies
- Identify commonalities across two sub-studies



Espionage Case Studies

Extracted people, traits, and task features
People classified as in organization, external, or family



Key Findings

Characteristics of Insider threats

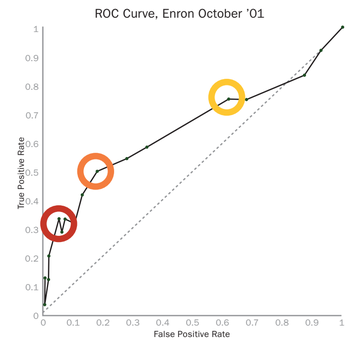
Disengagement with work and family, increasing ties outside

- Network features
  - Build structural holes
  - NOT: degree centrality
  - Member of multiple local clusters
  - Increasing betweenness at "group" level
  - Decreasing ties to family or break with significant other
- Social or Organizational features
  - Access
  - Had or was in military service
  - Minimal supervision
- Psychological features
  - Intelligent
  - Wanted to "use-the-system" for own gain
  - Wanted change (money/psych change)
- Network features similar to other covert actors
- Complimentary patterns in case studies and email
- Not testable
- To be tested

ENRON Email

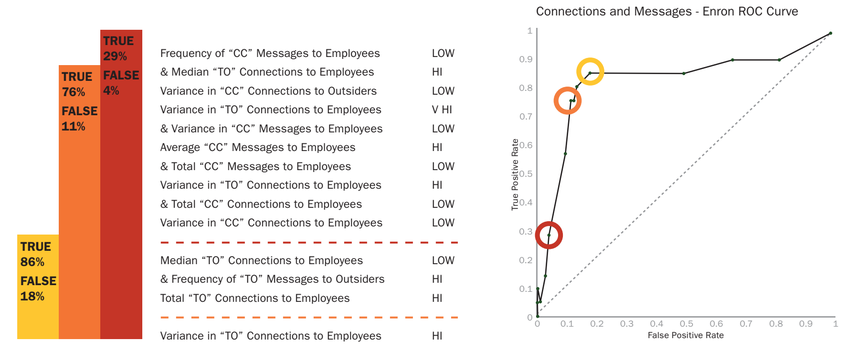
ORA for Network metrics, JRIP for ML

Individual Level Network Metrics



TRUE 50% FALSE 60%	(InverseClosenessCentrality_TO	HI
	OR CliqueCount_TO	LO
	& (CorrelationResemblace_TO	LO
	OR May2001_InDegree_TO_Internal)	HI
	& (CognitiveSimilarity_TO	HI
	OR ClusteringCoefficient_TO	LO
	OR AuthorityCentrality_TO)	LO
TRUE 50% FALSE 60%	& (Constraint_TO	Not VERY HI
	ColumnGiniMeansDifference_TO	POS
	OR InverseClosenessCentrality_TO	LO
	&	
	(InverseClosenessCentrality_BCC	HI
	OR InverseClosenessCentrality_TO	LO
	& (Oct01_InDegree_TO_Internal	POS
	OR WeakComponentMembers_BCC)	VERY HI
TRUE 50% FALSE 60%	&	
	(ColumnGiniMeansDifference_TO	POS
	OR WeakComponentMembers_BCC	HI
	& May2001_InDegree_TO_All	Not VERY LO

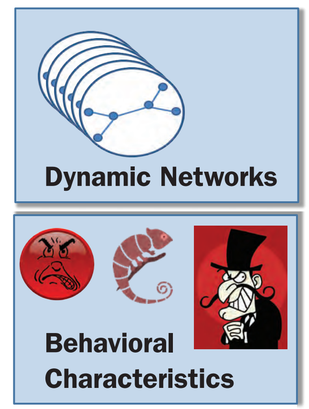
Group Level Network Metrics



Frequency of "CC" Messages to Employees	LOW
& Median "TO" Connections to Employees	HI
Variance in "CC" Connections to Outsiders	LOW
Variance in "TO" Connections to Employees	V HI
& Variance in "CC" Messages to Employees	LOW
Average "CC" Messages to Employees	HI
& Total "CC" Messages to Employees	LOW
Variance in "TO" Connections to Employees	HI
& Total "CC" Connections to Employees	LOW
Variance in "CC" Connections to Employees	LOW
Median "TO" Connections to Employees	LOW
& Frequency of "TO" Messages to Outsiders	HI
Total "TO" Connections to Employees	HI
Variance in "TO" Connections to Employees	HI

Future Work: Add "psychological" features to "network

Characteristics	Proxy	Source
Aggressive	Repeated Interrogatives ???	Behavior
Aggressive	Repeated Exclamations !!!	Behavior
Aggressive	Sentiment	Behavior
Aggressive	Email Length (Short)	Behavior
Smart	Characters Per Word	Behavior
Smart	Characters Per Sentence	Behavior
Smart	Sentence Length	Behavior
Smart	AVG Reading Ease	Behavior
Chameleon	Variability of Behavior	Network
Chameleon	High Shared Symbols across groups	Network
Compartmentalization	Local Betweenness	Network
Compartmentalization	High Variability in Reciprocity	Network
Compartmentalization	High Number of External Connections	Network



Geoffrey Morgan, Neal Altman, Matt Collins
Contact: Andrew Moore apm@cert.org, Kathleen M. Carley kathleen.carley@cs.cmu.edu

Network Dynamics Poster

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-0002735

Social Network Dynamiss Poster

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-0002734