

# **System Dynamics Modeling for Information Security: Invitational Group Modeling Workshop**

## ***Preliminary Description of Thread on the Insider Threat Problem***

### **Proposal Contributors**

- SEI/CERT, USA (PA): Chris Bateman, Dawn Cappelli, Casey Dunlevy, Andrew Moore, Dave Mundie, Stephanie Rogers, Tim Shimeall
- TECNUN, University of Navarra, Spain: Jose Maria Sarriegui
- Syracuse University, USA (NY): Jeff Stanton
- Agder University College, Norway: Jose J. Gonzalez

### ***Proposal history***

Proposed: January 23, 2004

Revised: January 29, 2004

### ***Objectives of the Insider Threat Problem Thread***

- to develop a preliminary System Dynamics model of some important aspect of the insider threat problem, based in part on an ongoing study of insider compromises across the US critical infrastructure sectors conducted by the U.S. Secret Service and the SEI/CERT
- to determine whether it is feasible to develop a generic system dynamics model for insider threat that will be useful to all organizations, or at least all organizations within a single critical infrastructure sector

### ***Objectives of this Proposal***

- to scope the aspect of the insider threat problem to be dealt with in the workshop
- to describe the problem in sufficient detail so as to provide a good starting point for the workshop and to ensure a good chance of success
- to provide a range of options in problem formulation that allows quick narrowing of problem scope at the beginning of the workshop according to the interests of the participants
- to provide the opportunity for other workshop participants to review and provide feedback for further refinement of this proposal prior to the actual workshop

### ***Insider Threat Thread Problem Outline***

1. *What is the real problem (not just a symptom of the difficulty)?*
  - a. Insider attacks cause organizations major damage to their reputation, employee morale, and bottom line.

2. *Why is it a problem?*
  - a. Explanation 1: Insider threat is a low base rate problem (similar to workplace violence, natural disasters)
    - i. Meaning that management does not see any way to predict or protect against insider attacks (insider compromises are often a direct or indirect result of abuses of legitimate authorization, which makes it very difficult to protect against or to detect once it occurs)
    - ii. And, because management views insider attacks as unpreventable, there is an associated loss of perceived control or self-efficacy on the part of management
    - iii. This loss of perceived control or self-efficacy leads to management inaction on the insider threat problem.
  - b. Explanation 2: Management misperceives the risk due to insider threat. They do not perceive the risk because they do not “measure” it, and they do not measure it because they do not think that it is a real threat or because they are unaware of tools and techniques that may be available for measuring it.
    - i. Organizations often concentrate on outsider attacks to the near exclusion of insider attacks
      1. Unfortunately, more *successful* attacks on organizations come from the inside than the outside (Schultz 2002)
      2. Insider attacks pose far greater *risk* to organizations than do outsider attacks (Schultz 2002)
      3. Situation analogous to looking for your lost watch where the light is, rather than where you lost it, because it would be easier to see
3. *How have organizational policies exacerbated the problem?*
  - a. Giving star players free reign because of fear of losing those employees.
  - b. Ignorance (either on purpose or due to naiveté) of indicators of insider threat
  - c. Disregard for information security best practices.
  - d. Poor human resource practices with respect to pre-hire screening of employees, ongoing monitoring of employees, and provision of facilities to help employees deal with problems (e.g., employee assistance programs, AKA EAPs)
  - e. Lack of training and education of employees on the reliance and trust that the company has in employee job performance
  - f. Lack of training and education of employees on the consequences of violations of employee trust, e.g., prosecution
  - g. The tendency of organizations not to report the problem and seek legal remedy for fear of damage to their reputation does not deter future insider threat attacks.

4. *What is the purpose of the model?*
  - a. To show that the observance of key indicators and taking preventive action based on those indicators could substantially reduce the likelihood of insider attack in organizations that fit a certain profile
  - b. To study the effective balance between all the measures oriented to increment the security of information systems for those organizations
  
5. *What is the approach to modeling?*
  - a. To analyze the processes within a generic organization (people, incidents, or processes as the unit of analysis)
    - i. Identify multiple key exemplars of the generic organization to indicate the importance of the problem and to enable validation of reference modes of behavior
    - ii. Approach is not to analyze the dynamics of a grouping of organizations (organizations or groups of organizations as the unit of analysis)
  - b. Handle the low base rate problem by identifying a *proxy measure* that
    - i. is relatively easy, inexpensive, and/or convenient to obtain from the generic organization, e.g., measuring employees' *intentions to quit* as a proxy for *voluntary turnover* in a company
    - ii. occurs frequently or can be captured frequently or continuously (in contrast to the capture of low base rate events, which by definition happen only rarely)
    - iii. on conceptual or empirical grounds, can be shown to be substantially connected to actual insider malicious activity
  - c. Identify key behavior patterns that
    - i. indicate the likelihood or existence of insider threat compromises in the generic organization (as derived from its exemplars)
    - ii. represent suitable proxy measures for the insider threat problem
  
6. *What is the generic organization to be modeled?*
  - a. Primary candidate
    - i. Generic organization reference modes
      1. Very trusted environment for certain classes of employees (including the insider)
      2. Management recognition and/or response to security threats (indicators) posed by insider were minimal or non-existent
      3. Successive lessening of security controls to prevent detection and to magnify the damaging impacts of the attack

- ii. Exemplars (we continue to look for good public references to these)
  - 1. Timothy Lloyd case targeting Omega Engineering Corporation
    - a. Good public source:  
<http://www.nwfusion.com/research/2000/0626feat.html>
    - b. Prior system dynamics analysis:  
<http://www.systemdynamics.org/conf2003/proceed/PAPERS/294.pdf> (Melara 2003)
  - 2. John Rusnak case targeting AllFirst Bank
    - a. Good public sources:  
<http://www.usdoj.gov/dag/cftf/chargingdocs/allfirst.pdf>  
[http://www.erisk.com/LearningCenter/CaseStudies/ref\\_case\\_aib.asp](http://www.erisk.com/LearningCenter/CaseStudies/ref_case_aib.asp)
    - b. News article: [http://www.sunspot.net/business/balte.bz.allfirst06jun06\\_0\\_4228032.print.story?coll=bal-business-indepth](http://www.sunspot.net/business/balte.bz.allfirst06jun06_0_4228032.print.story?coll=bal-business-indepth)
  - 3. Thomas Varlotta case targeting the FAA
    - a. Primary public source: court records
    - b. Bit news article:
      - i. <http://archives.californiaaviation.org/airport/msg02974.html>
      - ii. <http://www.landfield.com/isn/mail-archive/2001/Jun/0068.html>
      - iii. <http://www.thetracon.com/news/trib092200.htm>
  - 4. Bahram Saghari case targeting TVI Interactive
    - a. Primary public source:
      - i. Lexis Nexis: 2002 Cal. App. Unpub. Lexis 4790 (SEI can supply upon request)
  - 5. Christopher Harn case targeting paramutual betting via Autotote Systems processing.
    - a. Good public sources
      - i. Burrough, "Winner Lose All," Vanity Fair, March 2003 (SEI can supply upon request)
      - ii. [http://www.baselinemag.com/print\\_article/0\\_3668,a=34708,00.asp](http://www.baselinemag.com/print_article/0_3668,a=34708,00.asp)

6. Roger Duronio case targeting Paine Webber
  - a. Primary public source:
    - i. [http://www.njusao.org/files/PDF%20files/Duronio\\_indictment.pdf](http://www.njusao.org/files/PDF%20files/Duronio_indictment.pdf)
  - b. Bit new clips (widely reported):
    - i. <http://www.usdoj.gov/criminal/cybercrime/duronioIndict.htm>
    - ii. <http://www.philly.com/mld/inquirer/news/local/4763384.htm>
- b. Other Candidate Generic Organizations
  - i. Generic organization that hires very young individuals at low salaries (often data entry clerks) to perform functions that require great trust in handling company assets (6 cases)
    1. Cases would seem to have been prevented through some training about the trust that the organization has in their performance, organizational development procedures that increase the levels of commitment on the part of employees, auditing procedures to detect abuses, and warnings about prosecution of violations of that trust
      - a. Although there seems to be a frequent thread of romance playing a motivational role in these cases: young insider romanced by an outsider to extract/falsify internal information; not clear how the above training would help there.
    2. Cases not very rich and therefore may not be a good target of system dynamics (some simple best practices seem to suffice)
    3. Could study the reasons why organizations do not have the insider threat problem on their radar screens; when simple security best practices are sufficient, why don't organizations implement and maintain them? This would seem to involve the organization's larger business missions and objectives.
  - ii. Generic organization that provides a rich environment for insiders to take company assets to create competitive product/service (3 cases)
    1. Feeling of entitlement to products/customers created by insider to the point of taking those products/customers along to next job

7. *What are the key variables and concepts (proxy measures for insider threat)?*
  - a. Classes of variables indicating “precursor events” (Schultz 2002)
    - i. deliberate markers
    - ii. meaningful errors
    - iii. preparatory behavior (e.g., testing reaction to security threats, questions unrelated to job performance)
    - iv. correlated usage patterns
    - v. verbal behavior (e.g., aggressive, domineering, angry, frustrated)
    - vi. personality traits (e.g., aggressive, domineering, introverted, depressed, poor at handling stress and conflict, frustrated with work (Schultz 2002))
    - vii. changes in responsibility or position – demotions, reorganizations, ...
  - b. other variables/measures possibly of interest
    - i. IT total investments / Total budget of the firm
    - ii. Security investments / IT total investments
    - iii. "Hard" Security investments / Total security investments
    - iv. Software security investments / Total security investments
    - v. Losses due to Security incidents / Total budget of the firm
    - vi. Security people / Total people of the firm
    - vii. Reported insider incidents per year
    - viii. Total incomes of consulting firms working on security
    - ix. Number of firms which already have implemented structured security policies per year
8. *What is the time horizon for the analysis (cause and effect are often distant in time and space)?*
  - a. Insider threat problems seem to be roughly partitioned into cases that are motivated by personal gain (e.g., greed) and cases that are motivated by a grudge against the organization. Cases due to grudge are usually crimes of emotion for which the time horizon is relatively short (often less than a year). Cases due to personal gain are often much better thought out and can occur over a longer time span (up to 5 years in duration).
  - b. In some cases it could be interesting to establish an extended time horizon that permits simulating the growth of the Information Systems into the company and, perhaps, the “decline” of the insider
  - c. The sampling interval of measurement should be fine enough to accurately capture important changes to the dynamics of hiring, retention, and layoffs, insofar as these are important events that modify the composition of the workforce in substantial ways. Sampling daily is probably too fine; sampling quarterly may be too gross.

9. *What is the historical behavior of the key concepts and variables?*
  - a. Preliminary causal loop diagrams?
    - i. We are still considering this question. Our plan is to prepare chronologies for the exemplars of the generic organization. These chronologies would help in detailing the reference modes and causal loop diagrams.

## References

Melara, C., Sarriegui, J.M., Gonzalez, J. J., A. Sawicka, D.L. Cooke, "A System Dynamics Model of an Insider Attack on an Information System," in *Proc. of the 21<sup>st</sup> International Conference of the System Dynamics Society*, New York, NY, 20-24 July 2003 (also appears in *From Modeling to managing Security: A System Dynamics Approach*, J.J. Gonzalez (ed.), Norwegian Academic Press, Norway, 2003).

Schultz, E.E., "A Framework for Understanding and Predicting Insider Attacks," *Computers and Security*, Elsevier Science Ltd., 21 (6) October 2002, 526-31.

## Bibliography

- Shaw, E. D., Post, J. M., & Ruby, K. G. (2002). *Inside the Mind of the Insider*. Available at: <http://www.securitymanagement.com/library/000762.html>.
- Siponen, M. T. (2001). On the role of human morality in information systems security. *Information Resources Management Journal*, 14 (4), 15-23.
- Brennan, R. O. (2001). Research on Mitigating the Insider Threat to Information Systems. Santa Monica, CA: Rand Corporation.
- Anderson, R. H., Bozek, T., Longstaff, T., Meitzler, W., Skroch, M., & Van Wyk, K. (2000). Research on Mitigating the Insider Threat to Information Systems #2. Santa Monica, CA: Rand Corporation.
- Anderson, R. H., (1999). Research and development initiatives focused on preventing, detecting, and responding to insider misuse of critical defense information systems. Santa Monica, CA: Rand Corporation.