SAND2011-0254C

Establishing Resistance to Malevolent Insider Behavior

February 25, 2011

Greg Conrad
Manager, Application Infrastructure & Analytics

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Overview

- Philosophical / Theoretic Underpinnings
  - Cultural Setting
  - R&D Systems Approach
  - Employee Lifecycle Model

- The Organization – Culture – System
  - The Emerging Organizational Protection System
    - Integrated Security Information
  - Building Cultural Resistance
    - Counterintelligence Awareness

Systems and Cultural Approach

- Sandia is a Systems Engineering organization that seeks to find solutions to National Security issues
- An R&D view for mitigation of the insider threat is founded in a systems perspective of the entire organization in which the insider operates
- How can we utilize attributes of an organizational system to resist malevolent insider behavior?

Sandia National Laboratories

Malicious Insider Threat Perspective

- The threat is extremely agile, adaptable, persistent, and capable
  - The same reasons we need people to work for us
- The insider threat is a multifaceted human behavioral issue – motivation, susceptibility …
- We may not find the spy
  - But can we harden the target?

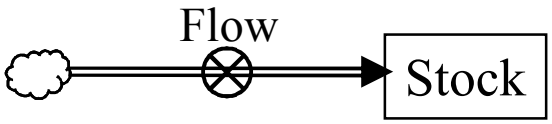
The Employee Lifecycle Model

- **Laboratory Directed Research and Development (LDRD) project – 2009**
- **Computational System Dynamics model – developed with :**
  - **Computational Modeling, Physical Security, Cyber Security, and Counterintelligence Expertise**
- **Purpose:**
  - **Provide systems assessment of a national security organization to protect itself against malicious insiders**
  - **From this baseline, we can investigate the effects and tradeoffs of policy decisions before they are implemented.**
- **The model creates a visualization of the various intervention points as workers flow through the system.**

Sandia National Laboratories

System Dynamics Modeling Background

Basic Features of a System Dynamics Model

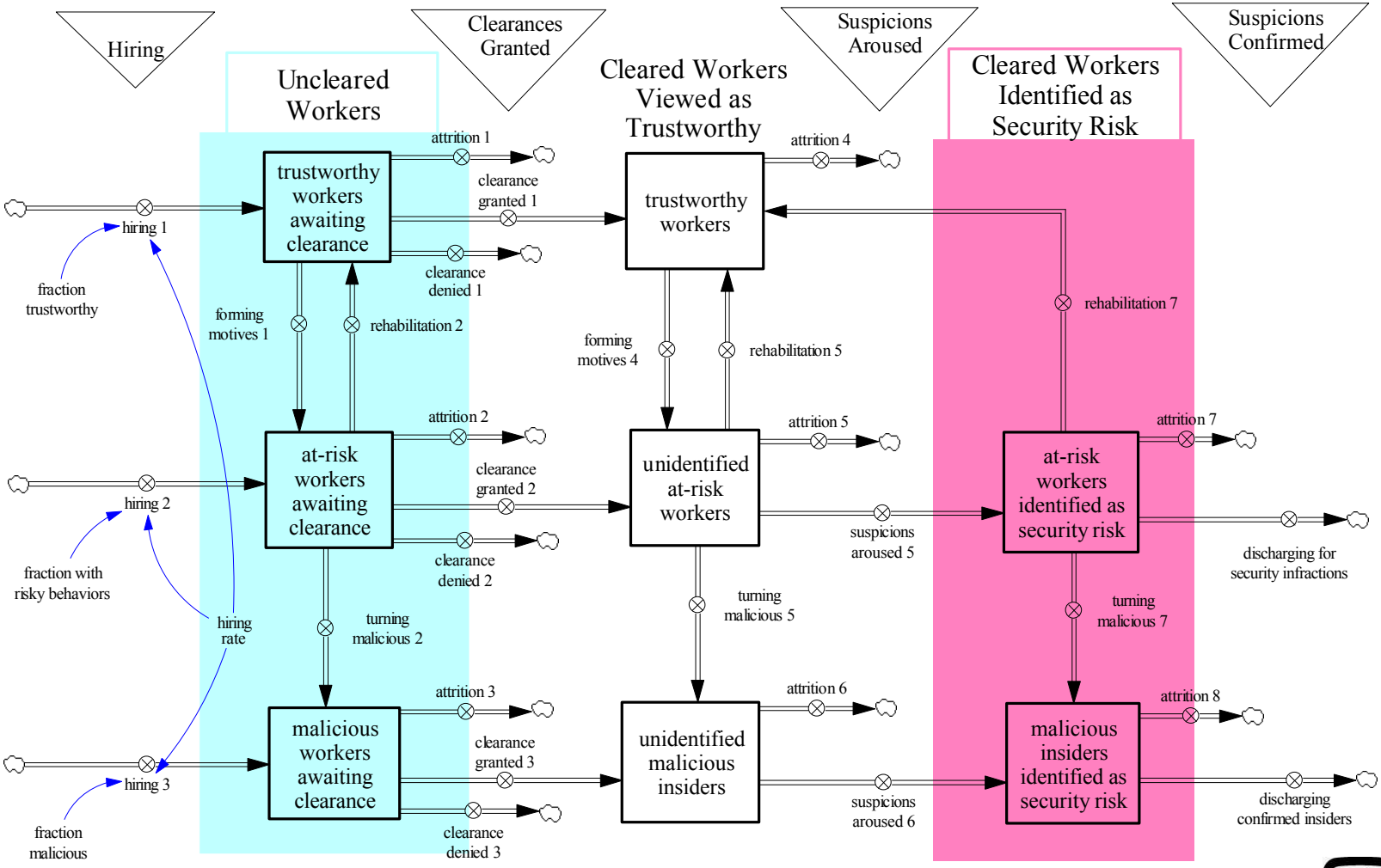


Simple Example of a System Dynamics Model

System dynamics is an approach to understanding the behavior of complex systems over time. It deals with internal feedback loops and time delays that affect the behavior of the entire system. What makes using system dynamics different from other approaches to studying complex systems is the use of feedback loops and stocks and flows. These elements help describe how even seemingly simple systems display baffling nonlinearity.

"All models are wrong, but some are useful" – George Box (Quality and Statistics Engineer)

Employee Lifecycle Model



Sandia National Laboratories

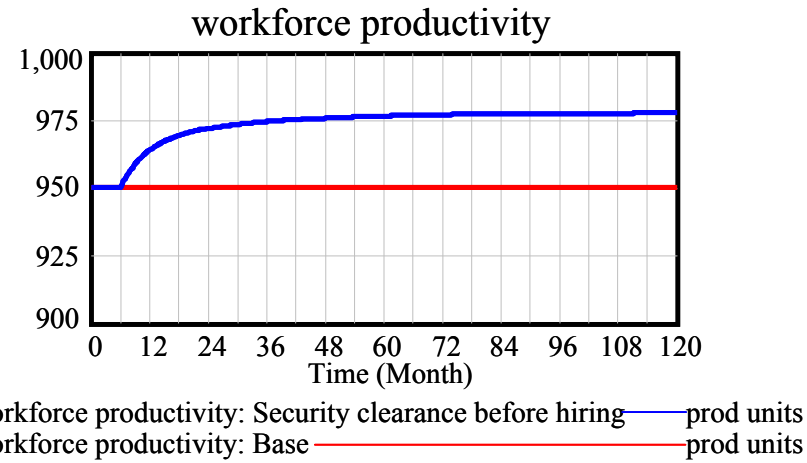
Model Example Test Case
(Mission versus Security)

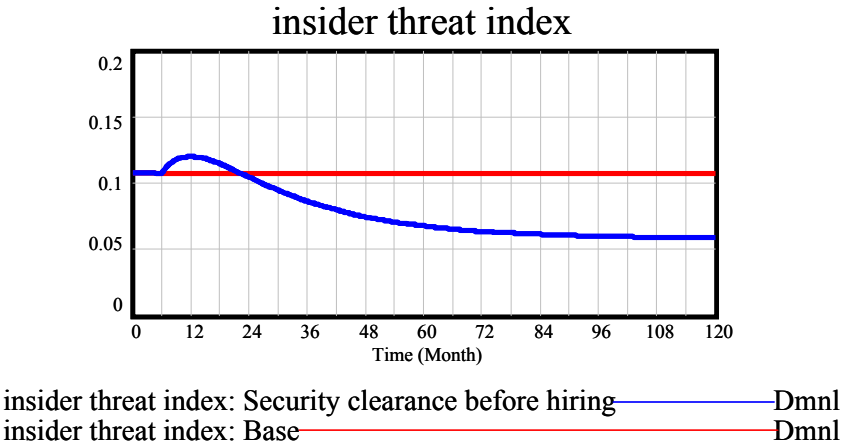
Conventional wisdom has it that the ability to achieve mission success must be balanced against maintaining security. However, not ***every*** policy necessarily need represent a tradeoff between these competing goals. For this project, we identified a high-leverage policy option that appears to improve both security and productivity.

Policy hypothesis – Screening prospective hires for a security clearance will increase security while lowering costs.

Assumptions –

- Pre-hire screening
  - Increases fraction of trustworthy employees
  - Reduces overall clearance processing time
- Cost = implementation cost – increase in worker productivity
- Security is inversely proportional to the number of unidentified at-risk workers & malicious insiders





Sandia National Laboratories

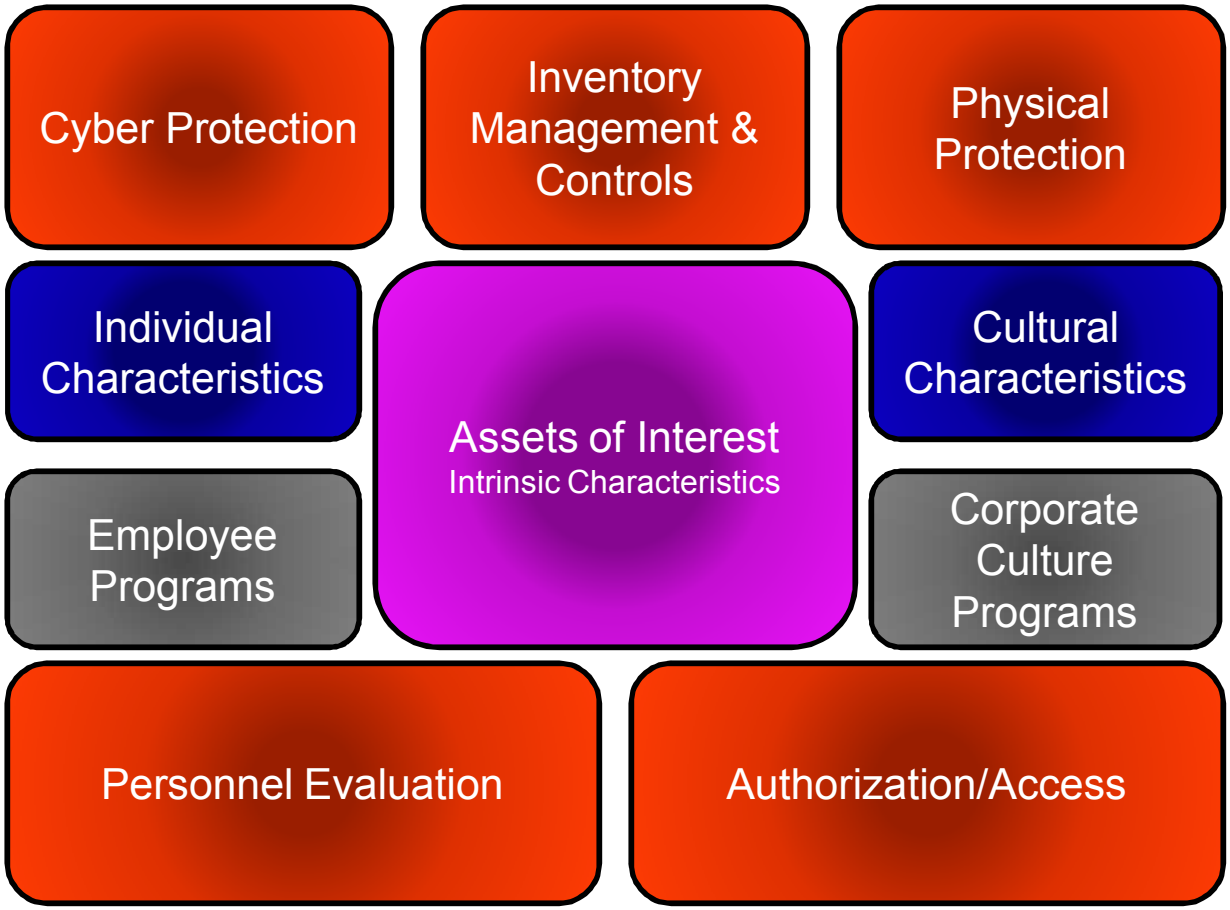
Emergent Security Systems

An **emergent behavior** or **emergent property** can appear when a number of simple entities (agents) operate in an environment, forming more complex behaviors as a collective

- Ad-hoc
- Evolutionary
- Stove-piped
- Complex
- No Grand Design

Sandia National Laboratories

Emergent Insider Threat Protections



- **No over all design**
- **A loose federation of functions that independently address portions of the problem**
- **Intercommunication is sparse**
- **It generally works but may be due to the strongest component – Individual Characteristics**
  - **Morals**
  - **Values**
  - **Ethics**
- **An opportunity exists to bind these components together through Integrated Security Information and Analytics**

Sandia National Laboratories

Integrated Security Information & Analytics

- Integration of Cyber System, Physical Security System, and HR information systems
  - Signature based anomalies
    - Lost/Stolen credential usage
    - Physical/Cyber discontinuities – credential usage when individuals are not physically present
  - Model based anomalies
    - Out-of-the-ordinary activity – internet, file upload/download
  - Correlation and trending
    - Are there individuals with patterns of “almost” significant behaviors – security events, cyber behaviors, HR events

Examples

- Testing behaviors detected
  - Repeated use of an unauthorized credential to attempt access over more than a year, different assets, different days of the week, different times of the day, inconsistent patterns
  - Attempted usage of credentials that had been reported as “lost”
- Anomalous behaviors detected
  - Overwhelmingly busy use of credentials over a hours and days
- Waste, fraud, and abuse detected
  - Pornography, social networking sites, compulsive web searches

Cultural Resistance

Pervasive Counterintelligence Attitudes

- **Workforce & Office of Counterintelligence (OCI) Partnership**
  - **The agreement …**
    - **Designed to develop trust**
    - **Workforce**
      - **Recognize the reality of the threat**
      - **Accept their role and responsibility to apply their human capabilities to recognize suspicious or unusual behaviors**
      - **Report those behaviors to the OCI**
    - **OCI**
      - **Recognize that at not all suspicious or unusual behaviors represent a threat**
      - **Protect the reputations of all innocent parties (Those reporting and those being reported upon)**
      - **Act in an appropriate and judicious manner to protect national security, company, and individual interests**

Sandia National Laboratories

Cultural Resistance

Pervasive Counterintelligence Attitudes

- **Agreement Implementation**
  - **Awareness Briefings**
    - **Consistent and repeated discussions across the organization with up-to-date information regarding the threat with real-life scenarios**
  - **CI Focused Security Awareness Training**
    - **Three year focus on Insider Threat**

Cultural Resistance

Pervasive Counterintelligence Attitudes

- **Security Awareness Training**
  - **Three year focus on Insider Threat**
  - **Required for entire workforce**
  - **Key elements**
    - **Adversaries targeting a well secured organization require an insider's cooperation**
    - **When an insider is detected it's too late to prevent significant consequences**
    - **Workforce population that's aware of the threat and comfortable with reporting can prevent insider events and protect themselves and other employees**
    - **Threat aware organizations that recognize the concern and openly and honestly communicate with staff create a vigilant community that can exert maximum deterrence**

Cultural Resistance

Pervasive Counterintelligence Attitudes

- **Results**
  - **Survey included in the 2006 & 7 training**
    - **20K responses indicate a greater sensitivity to the insider**
    - **25% increase in those who thought the probability of the insider threat in the organization was “almost certain” or “above 50-50.”**
    - **9% drop in those indicating that the organization “almost certainly not” having an insider**
  - **Employee CI reports have increased**
    - **The proportion of reports over investigations is significant as is the number of investigations over the number of actions taken**

Questions

Sandia National Laboratories