Modeling the Employee Life Cycle to Address the Insider Threat*

Stephen H. Conrad
Infrastructure Modeling and Analysis – Sandia National Laboratories
P.O. Box 5800, MS-1138, Albuquerque, NM 87185-1138
Phone: (505) 844-5267 Fax: (505) 284-3850
Email: shconra@sandia.gov

Felicia A. Durán
Security Systems Analysis – Sandia National Laboratories
P.O. Box 5800, MS-0757, Albuquerque, NM 87185-0757
Phone: (505) 844-4495 Fax: (505) 844-2932
Email: faduran@sandia.gov

Gregory N. Conrad
Threat Analysis Technologies – Sandia National Laboratories
P.O. Box 5800, MS-1235, Albuquerque, NM 87185-1235
Phone: (505) 844-0471 Fax: (505) 284-3977
Email: gnconra@sandia.gov

David P. Duggan
Networked Systems Survivability and Assurance – Sandia National Laboratories
P.O. Box 5800, MS-0672, Albuquerque, NM 87185-0672
Phone: (505) 845-8100 Fax: (505) 845-7065
Email: dduggan@sandia.gov

E. Bruce Held
Office of Counterintelligence – Sandia National Laboratories
P.O. Box 5800, MS-1227, Albuquerque, NM 87185-1227
Phone: (505) 284-5404 Fax: (505) 284-6844
Email: ebheld@sandia.gov

ABSTRACT

Within an organization, the employee population is the source of potential malicious insiders. To investigate the evolution of the insider within an organization, we are developing a model of the employee life cycle. In addition, the employee life cycle model is being applied to define and analyze interactions of the employee population with insider security protection strategies. The model was exercised for an example scenario that focused on human resources and personnel security activities, specifically, pre-hiring screening and security clearance processes. Additionally, we have developed and tracked through the model several case studies of malicious insider activity. This modeling effort provides a framework to understand important interactions, interdependencies, and gaps in insider protection strategies. This work is part of a larger effort to develop the basis for an integrated systems-based process for designing and evaluating effective insider security systems.

* Sandia National Laboratories is a Multiprogram Laboratory Operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under Contract DE-AC04-94AL85000. This work is funded by the Laboratory Directed Research and Development Program at Sandia National Laboratories.

INTRODUCTION

This paper presents the initial iteration of an ongoing system dynamics (SD) modeling effort to support the development of a systems-based approach for addressing insider threats. Malicious insiders are among the most ubiquitous, numerous, and capable of potential security threats to any organization. This threat can range from petty theft and fraud to espionage and terrorism. Organizational and societal costs are immense – up to and including national security breaches. Many organizations and agencies have a keen interest in this problem, as well as a need to demonstrate effective insider security simultaneously with operational efficiency. Insider attacks continue to be discovered, indicating that many current protection strategies can be defeated. Current protection strategies against insider adversaries are expensive, intrusive, not systematically implemented, and operate independently. Typically, the individual facets of insider security strategies are implemented extemporaneously, creating an *ad hoc* system of protection. Each individual component tends to be evaluated in isolation; seldom is a holistic evaluation of the overall security system performed.

The source of the insider threat for an organization is its employee population. Therefore, it is important to develop an understanding of how an employee interacts with the security and operational elements that provide protection, either directly or indirectly, against the insider threat. A key idea developed in this work is that the employee life cycle provides a means for investigating the evolution of the insider threat within an organization. In this employee life cycle model (ELCM), interactions of the employee population with insider security systems and operational procedures can be defined and analyzed. The model was exercised for an example scenario that focused on personnel security and human resources activities, specifically the hiring and clearance processes. The model provides a framework to investigate further and understand important interactions, interdependencies, and gaps in insider protections. It also supports the basis for an integrated systems-based process, including principles, methods, tools and practices for designing, evaluating and operating security systems effective insider security systems.

BACKGROUND

An insider is anyone with knowledge of, access to, and authority at a facility. This definition implies that every employee in an organization is an insider, and any employee may pose an insider threat. Additionally, contract employees, consultants, service providers (for example material/equipment suppliers and maintenance personnel), and others who are not direct employees may also be considered a part of the population that has access inside an organization. For facilities that have security systems in place to protect critical assets, insiders have access "inside" the protective measures. Of most concern is the malicious insider who might attempt theft of critical assets (including information and property), sabotage of equipment or operations, or other criminal activities.

The 1990 RAND insider crime study (Hoffman et al. 1990) applied 62 case studies to potential attacks against nuclear facilities. Ten years later, the RAND Corporation coordinated a workshop on mitigating the insider threat to information systems (Anderson et al. 2000). The workshop organizers described the insider problem as a human problem and argue that "human

problems cannot be solved with technological solutions." They presented a critical path model that consisted of "characteristics of perpetrators, but also the chain of events which [lead] to their acts of treason," noting that personal intervention can break this chain.

A more recent *Insider Threat Study* (Keeney et al. 2005) examines 49 case studies of insider attacks to critical infrastructures, with an emphasis on computer system sabotage. The case studies show that the persons involved committed "sabotage through insider manipulation of computer systems and networks," but not necessarily for "financial gain or theft." The researchers traced insider incidents "from the initial harm backwards in time to when the idea of committing the incident first occurred to the insider." They concluded that the typical insider:

- At some point was a system administrator, but not at the time of the incident.
- Suffered a "negative work-related event."
- Wanted revenge.
- Planned a possibly unsophisticated incident using remote access that exploited or compromised a backdoor or shared account.
- Communicated negative sentiments and indicated signs of planning their activities in advance.

Most often, insiders were identified by a manual review of system logs, primarily remote access logs. The study emphasized one factor – that management should have some standard policy for addressing "negative, work-related events." The study also recommended implementing an operational procedure to provide a means to report problematic behavior, to manage and disable accounts, to oversee system administrators, to enforce password policies, to monitor system integrity, to limit remote access, to protect system logs, and to have a disaster recovery plan (including backups). Currently, most every security protection systems have a cyber component, and understanding cyberthreats is an important aspect in addressing malicious insider activity.

One unique aspect of the *Insider Threat Study* is that it devoted equal attention to the technical and psychological aspects of the problem. Band et al. (2006) reviewed 39 cases of espionage and insider attacks to "examine psychological, technical, organizational, and contextual factors" that could lead to espionage and sabotage. The study makes the following observations:

- Saboteurs and spies share personal predispositions (e.g., need for money or attention), and their acting out implies that they are under stress.
- Their behavior changes prior to acting out (e.g., spies access data outside their need-to-know).
- They violate technical controls before acting out.
- Organizations fail to see or ignore the warning signs. (Audits were poor and/or no one looked at logs.)
- Poor access control enables acting out.

The *Insider Threat Study* showed that to detect insider cyberthreats as early as possible or to prevent insider attacks altogether, "management, IT, human resources, security officers, and others in the organization must understand the psychological, organizational, and technical aspects of the problem as well as how they coordinate their actions over time…" (Band et al. 2006). Researchers at Carnegie Mellon University also concluded that there are "limitations of a strictly technological approach" to the insider problem (Andersen et al. 2004). Detection, response, policies and procedures all contribute to the solution.

MOTIVE, OPPORTUNITY, AND MEANS

"Every investigator is familiar with the old maxim of "MOM," the three theoretical elements required to solve a murder case: motive, opportunity, and means" (Hodel 2004). This concept of MOM is extended to other criminal and like behaviors, including the insider threat (Crayton 2003). "Insiders have two of the three things needed for an attack" – means and opportunity (Gregg 2007).

For the insider threat, *motive* represents what the insider will gain from malicious activity. Malicious insiders may be internally motivated or externally coerced. Studies on the motives of individuals committing espionage identify several motivators. The Department of Defense Personnel Security Research Center (PERSEREC) study (Herbig and Wiskoff 2002) lists primary and secondary motivators as:

- Money
- Divided loyalties
- Disgruntlement (including revenge)
- Ingratiation
- Coercion
- Thrills
- Recognition.

The PERSEREC study (Herbig and Wiskoff 2002) found that motivations of the insider are rarely singular; individuals often exhibited multiple motives. On the other hand, because the insiders studied in the RAND Insider Report (Hoffman et al. 1990) seemed to act for the money involved, even though they had no financial need, the authors concluded that perhaps "a terrorist group could secure an insider's assistance simply by paying him or her."

Rich et al. (2005) look at another case study that involves a lone insider who probes systems and then mounts attacks over a long period, motivated by disgruntlement and financial need. The insiders include information workers and security officers who commit long-term fraud. In more recent related work (Martinez-Moyano et al. 2008), additional modeling efforts characterized insiders with other types of motives, such as those exemplified by "minimum-wage data entry clerks" who the organization trusted, those who were manipulated by emotional pressure stemming from an intimate relationship, or those who felt entitled. The insider also balanced

probability of detection against probability of ill-gotten gain in the model. The study indicated that insiders are not insiders by nature; rather, they make a decision to attack.

Opportunity implies that a malicious insider has access to assets (people, information, or physical items) that can be used to fulfill his or her motives. For example, a spy needs to have access to protected information before money can be negotiated for its release. In addition to access, knowledge of system vulnerabilities offers opportunity to conduct malicious activity. The RAND report (Hoffman et al. 1990) found that insider success depended more on "exploitation of existing security flaws" than it does on "planning or expert execution." The insider attacked "targets of opportunity." For example, "Guards were responsible for 41 percent of the crimes committed *against guarded targets*" (emphasis in the original).

Means are defined as an insider's ability to carry out the malicious activity and imply that the person can perform some malicious action against the assets to which he or she has access. Means is defined as both the capability to acquire the asset and access to an interested third party. In the case of espionage, the person has the means to exfiltrate critical information, as well as to establish contact with a person to receive the data.

PERSONALITY STYLES

A discussion of MOM is not complete without a discussion of the personality styles that indicate a potential risk from malicious insiders. Geller and Turner (2003) compiled the following "Personality Styles as Behavioral Indicators of Insider Risk." These attributes are not indicators or predictors of malevolence, but are factors that should be considered in risk mitigation strategies:

- Self-centered: self important, and resentful; constantly seeks recognition and admiration.
- Arrogant: the "rules" don't apply; indifferent to the rights of others.
- Adventurous: Seems attracted to risk, danger, and harm. Dislikes boredom and inactivity; unconventional lifestyle.
- Manipulative: takes others for granted and uses them; disregards obligations.
- Cold: indifferent to the feelings of others; not empathetic.
- Grandiose: exhibits a preoccupation with immature fantasies of success, beauty, or love; suffers from self-illusions; speech is characterized by exaggeration and hyperbole.
- Self-deception: justifies self-centered and socially inconsiderate behaviors; fails to believe his or her behavior will be punished.
- Defensive: reacts to criticism with anger/rage; overreacts to constructive criticism.

The RAND report (Hoffman et al. 1990) divided the set of insider threats into three groups:

- Insiders conspiring with outsiders,
- Insiders conspiring with other insiders, and
- Lone insiders.

Most organizations interested in protecting assets from insider threats typically consider two types of insiders: those working alone and those who are in collusion with others. The RAND report indicated that insider type is a function of the target and concluded that insiders who target nuclear facilities or nuclear material are insiders conspiring with outsiders. Stealing nuclear material is fundamentally different than pilfering a dollar a day from the till, which would be the work of a lone insider. For organizations that have effective security systems in place to protect critical assets, successful attacks almost always require the participation of a willing insider.

PROTECTING AGAINST THE INSIDER THREAT

In establishing a systems-based approach for addressing the insider threat, it is critical to develop an understanding of how an employee interacts, throughout the life cycle of employment, with the security and operational elements that provide protection against the insider threat. Organizations employ a variety of protection measures and operational procedures to address the insider threat. In addition to the traditional physical protection and cybersecurity systems, personnel security, human resources, management, training, and employee assistance programs are essential operational activities for addressing the insider threat. Some important activities include:

- Employee screening investigations (human resources and personnel security).
- Activity auditing and monitoring (cybersecurity, access monitoring, self-reporting, and counterintelligence).
- Security procedures and practices (physical security, cybersecurity, material control, and counterintelligence).
- Access controls (safes, guards, and fences).

To develop an overall view of insider security, subject matter experts from different security domains have provided their perspectives on insider threats and current protections. This information is being incorporated in this model development effort. A holistic, systems-based approach for insider security views the problem as more than detection, and instead considers all operational activities. We view the entire organization as a system that includes elements that not only provide protection against the insider threat, but also influence the insider's characteristics, motives, and capabilities. To date, it is clear that none of the identified system elements has a primary mission to directly address the insider threat. Thus, in most organizations, a dedicated insider security system does not exist, and a holistic evaluation of the effectiveness of insider protections is not possible.

PREVIOUS INSIDER SYSTEM DYNAMICS MODELING

Previous system dynamics modeling for the insider threat include six papers that explore the application of system dynamics to the insider problem (Andersen et al. 2004; Rich et al. 2005; Martinez-Moyano et al. 2006a, 2006b, and 2008; and Band et al. 2006). Andersen et al. (2004) produced a system dynamics model of insider cyber-threat interactive loops, three of which were considered to be key reinforcing loops (see Figure 1). Each of these three loops reinforces itself until it triggers action. The thresholds for action are considered dynamic; thus each loop is

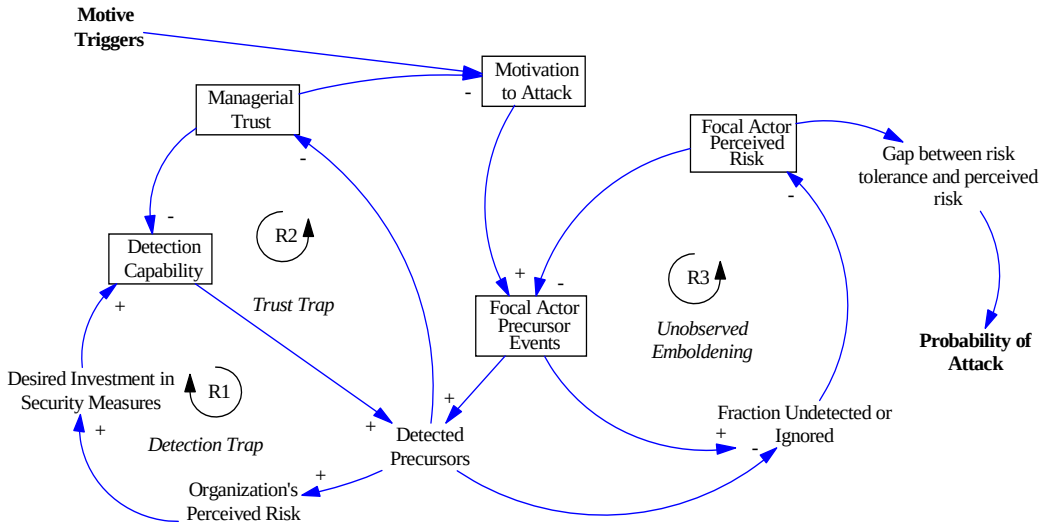


Figure 1. System dynamics model of the insider cyber-threat (Anderson et al. 2004)

considered to be a dynamic trigger hypothesis, which shows how motives and conditions conducive to attack (means and opportunity) transform into attack behavior. This work hypothesizes that two reinforcing loops (R1, R2) can impair the organization's ability to detect insider activity. A third reinforcing loop (R3) encourages the insider to engage in progressively greater system-testing precursor activity until they feel emboldened enough to launch an attack. They conclude that "simply claiming that identifying feedbacks responsible for the patterns of precursors mounting up before the actual strike would make precursors more conspicuous and, hence, improve the chance to prevent the strike, or at least mitigate its consequences." The authors conclude that there are "limitations of a strictly technological approach" to the insider problem. Detection, response, policies, and procedures are all part of the solution.

Martinez-Moyano et al. (2006a) build on this dynamic trigger hypothesis. Their enhanced model adds judgments, decisions, decomposition of possible outcomes, and a learning process. This model produces behavior consistent with "more than 200 cases of discovered malicious insider activity," according to the authors. Six enhancements—such as assuming that workers adhere to security policy—enable a user to experiment with the model. The same authors developed a further enhancement to the model (Martinez-Moyano et al. 2008), one aspect of which is helpful – the further definition of precursor events, which are probes by the insider into the security of the system. The authors only consider test and probe precursor events, but note two other types of precursor events: stepping stones and ones that lower detection. The insider watches to see whether the probe is discovered and how the system responds. As these increasingly intrusive probes are successful, the insider's willingness to attack increases. The insider balances probability of detection against probability of ill-gotten gain in this model. Insiders are not insiders by nature; rather, they make a decision to attack.

Band et al. (2006) developed a system dynamics model for PERSEREC that used nine espionage cases from the PERSEREC research (and 30 other cases of insider attacks) to "examine

psychological, technical, organizational, and contextual factors" that could lead to espionage and sabotage. The report makes the following observations:

- Saboteurs and spies share personal predispositions (e.g., need for money or attention), and their acting out implies that they are under stress.
- Their behavior changes prior to acting out (e.g., spies access data outside their need-to-know).
- They violate technical controls before acting out.
- Organizations fail to see or ignore the warning signs. (Audits were poor and/or no one looked at the logs.)
- Poor access control enables the acting out.

Based on these observations, Band et al. (2006) recommend the development of a "risk-indicator instrument" that could flag predispositions. They recognize that progress has been made in using system dynamics to analyze the insider, but that there is more work to be done.

THE EMPLOYEE LIFE CYCLE MODEL

The employee life cycle provides a means for investigating the evolution of the insider threat within an organization. We have initiated development of an employee life cycle model (ELCM). Using this approach, we can define and analyze interactions of the employee population with a given combination of insider security protection strategies. The model provides a means to understand the current level of protection provided by an organization's overall security posture with regard to the insider threat – and importantly, to identify any major inadequacies in that system as it is currently configured. We are also using the model to develop a process with which to identify an improved set of protection measures and operational procedures that would comprise an effective insider security system for a given organization or facility.

Figure 2 represents the system dynamics model of the employee life cycle. On the left side of the figure, the flows labeled ***hiring*** represent the movement of new workers into the organization. This particular model represents a national security organization that requires its employees to have clearance to access certain facilities and information. Newly-hired workers flow into the three stocks of uncleared workers (blue-shaded background, on the left side of the figure) and reside in these stocks until their clearances are either granted or denied, or they separate from the organization (attrition). The workers who are granted clearances migrate to the next column of stocks to the right (white background, in the middle of the figure). These are the stocks of cleared workers. They are viewed by the organization as being trustworthy and they have access to protected information. (The level of their access to protected information depends on their need-to-know and the adequacy of the administrative controls that are in place.) The workers who reach the two stocks on the right (red-shaded background, on the right side of the figure) have managed to arouse suspicions by the organization about their behavior. Assuming adequate administrative controls, the access to protected information is appropriately restricted.

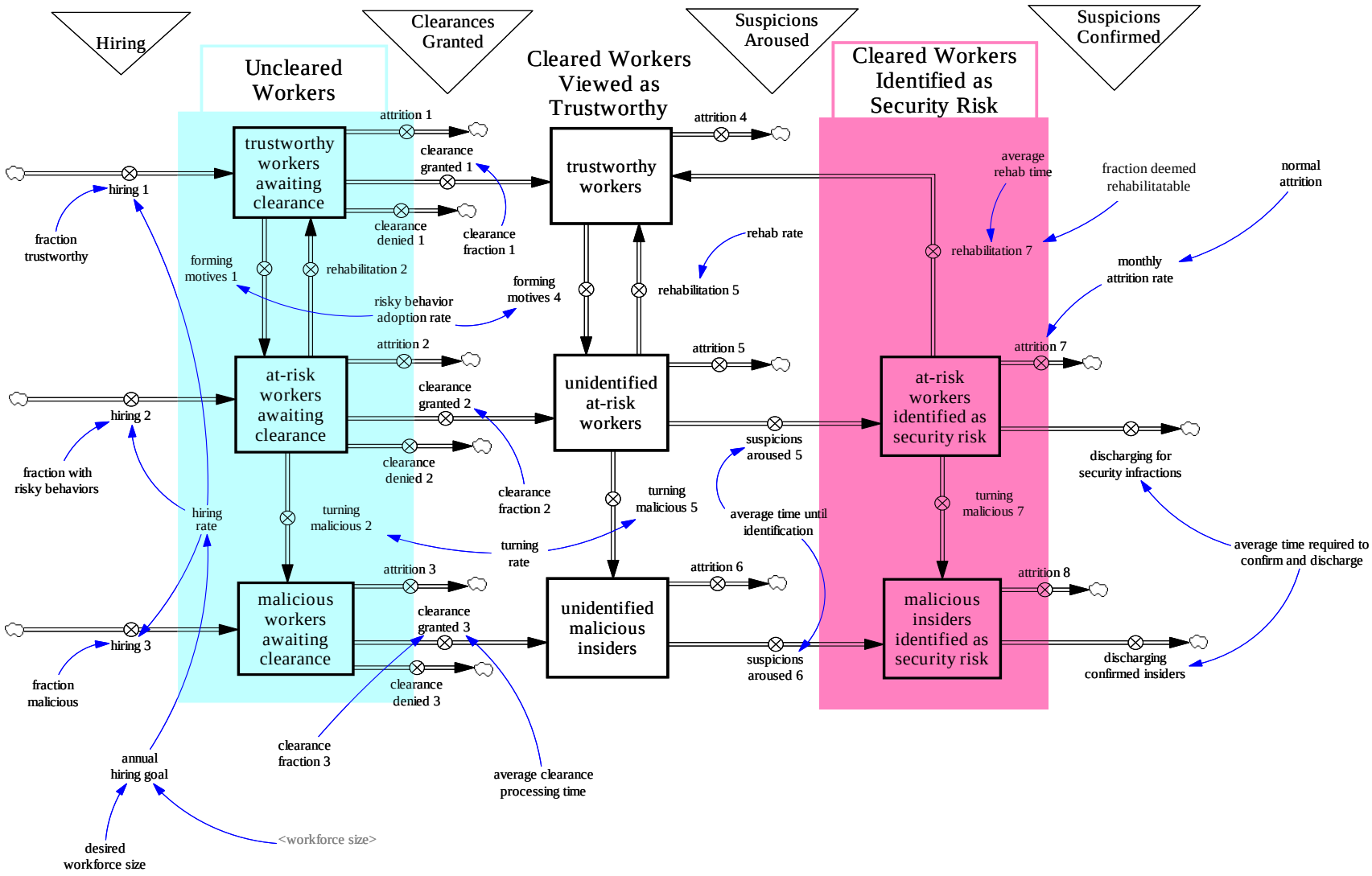


Figure 2. Stock-and-flow diagram of the Employee Life Cycle

These workers can either: (1) leave the organization by normal attrition, (2) be rehabilitated (where appropriate), or (3) be discharged for breach of security.

The three columns of stocks represent how workers are viewed *by the organization* – either uncleared, trustworthy, or identified as a security risk. The three rows of columns represent the true states of the employees. The top tier represents the vast majority of workers who are truly trustworthy. The middle tier represents workers who are ***at-risk***. These workers may have alcohol or substance abuse problems or financial difficulties that may cause them to consider malicious activities. They may be disgruntled. They may be subject to blackmail. They may have the character traits or they may have developed the motives we discussed previously. As can be seen from the flows into these stocks on the middle, ***at-risk*** tier, these workers may bring their risky behavior attributes with them as they hire into the organization, or they may develop them sometime subsequent to joining the organization. The bottom tier represents the stocks of malicious insiders. They can either infiltrate the organization through the hiring process (moles), or they can be recruited from the stocks of ***at-risk*** workers (those susceptible to being turned). Alternatively, they may voluntarily seek out buyers for the protected information they have attained.

The vast majority of workers are trustworthy when they are hired. They inhabit the stock of ***trustworthy workers awaiting clearance*** (left column, upper tier) until their clearances are granted. They spend the majority of their careers as ***trustworthy workers*** (center column, upper tier). Eventually, they leave the organization, either by retirement or to take a new job elsewhere. Of most concern are workers who engage in behaviors that constitute a security risk. Especially of concern are ***unidentified at-risk workers*** (center column, middle tier). These are cleared workers viewed as trustworthy who have access to protected information. The concern is that they may become a malicious insider before suspicions are aroused, and they are identified by the organization as a security risk. But by far, the most damaging to the security of any organization is the presence of ***unidentified malicious insiders*** (center column, bottom tier). They have access to protected information and will conduct malicious activity until they are detected.

MOM was also considered as this model was developed. Figures 3, 4, and 5 highlight where MOM, respectively, is represented in the model. Figure 6 indicates where evaluation of different security systems and operational procedures can be incorporated to determine their effectiveness against the insider threat.

An example scenario developed to demonstrate the utility of the modeling approach to a lay audience focused on human resources and personnel security activities:

- ***Pre-hiring screening***—An initial strategy for addressing the insider threat is an employee pre-hiring screening process to remove from the hiring pool potential employees that may indicate a predisposition to becoming a malicious insider.
- ***Security clearance processes***—For high-security facilities, this screening also considers factors that may indicate a potential employee will or will not qualify for a security clearance required for access to certain facilities and information. Even if a potential employee passes the initial pre-hiring screening and is hired, some risk will still exist that

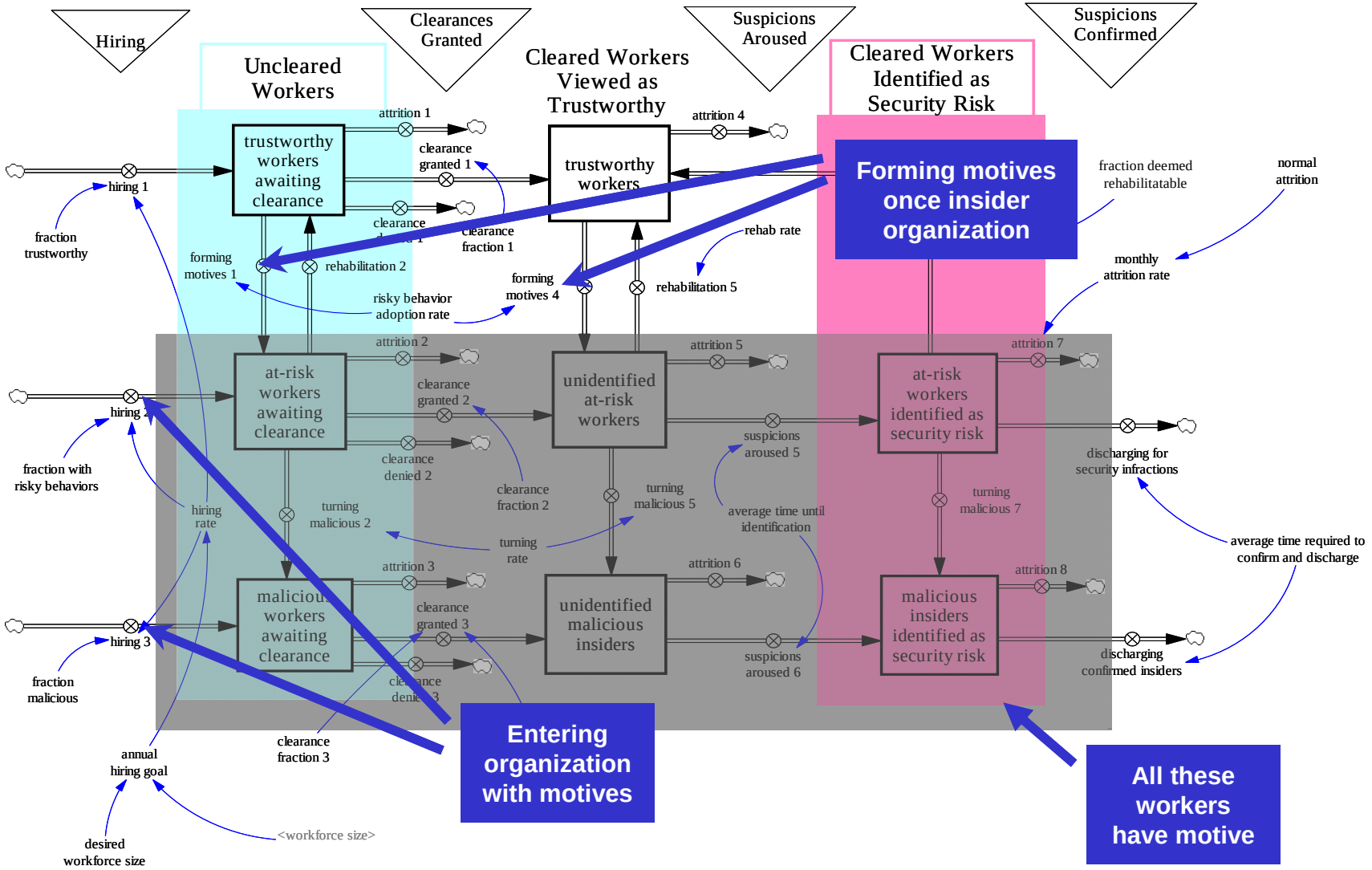


Figure 3. Model elements that address the formation of Motive

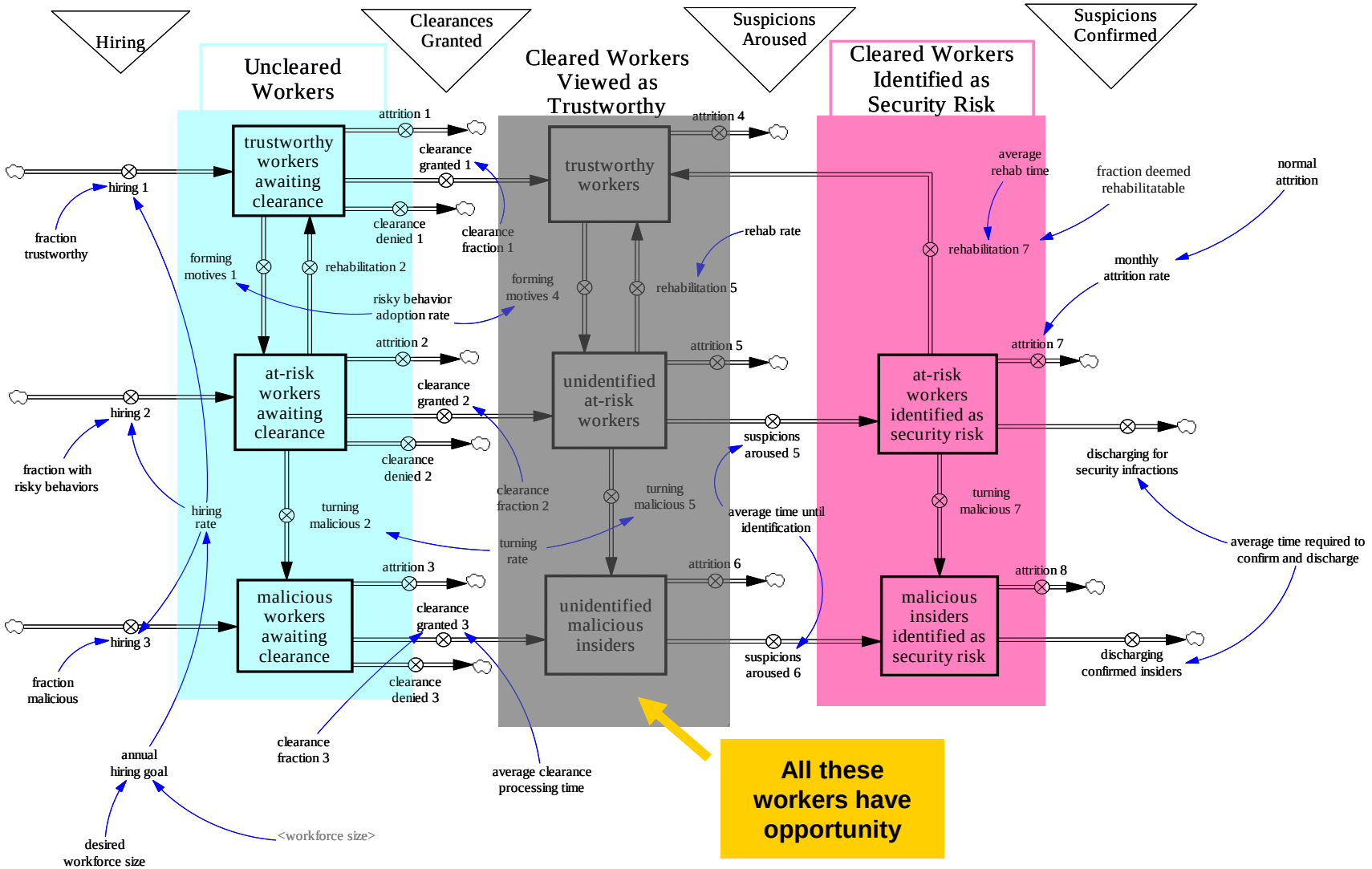


Figure 4. Model elements that address Opportunity

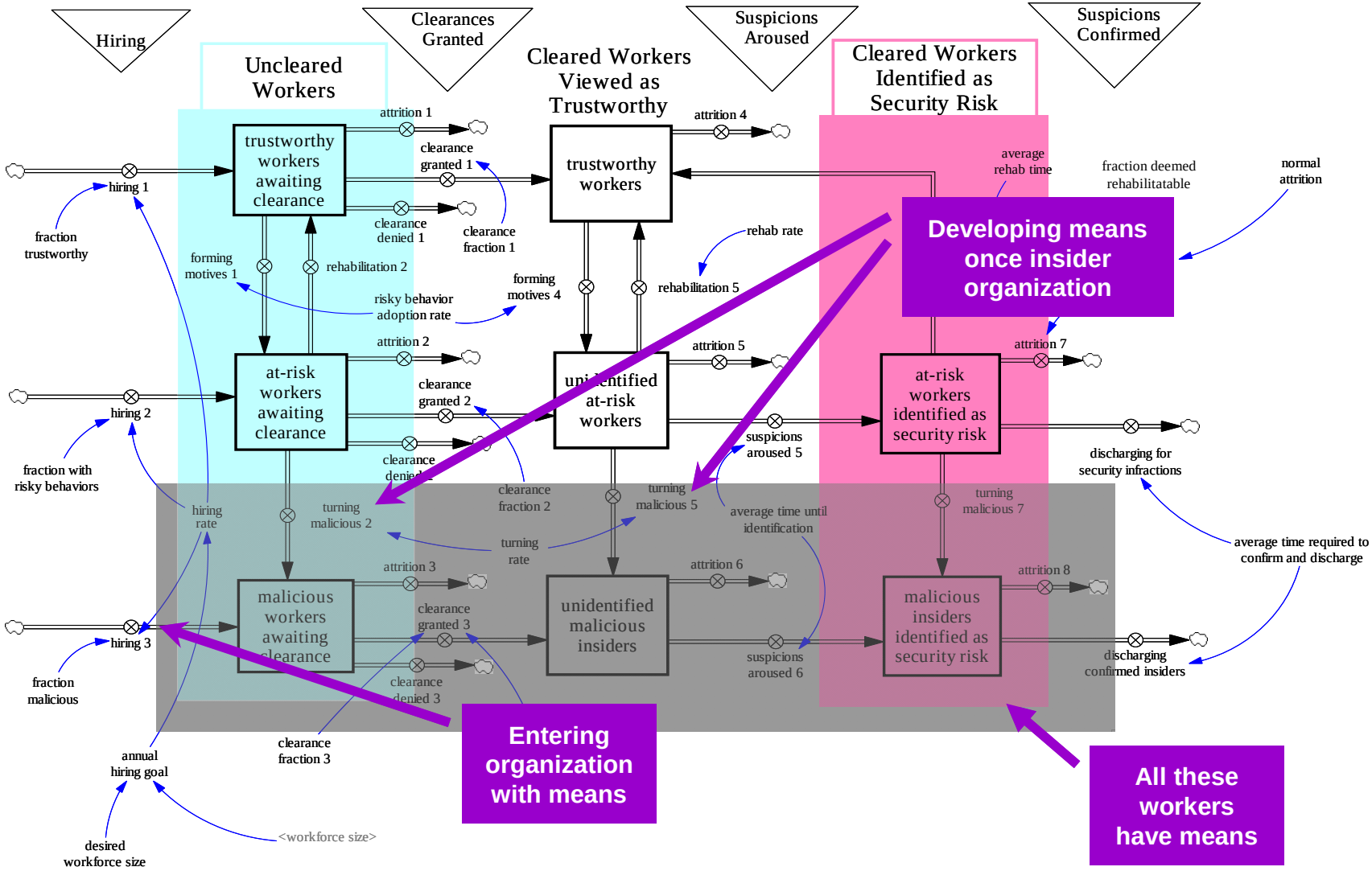


Figure 5. Model elements that address Means

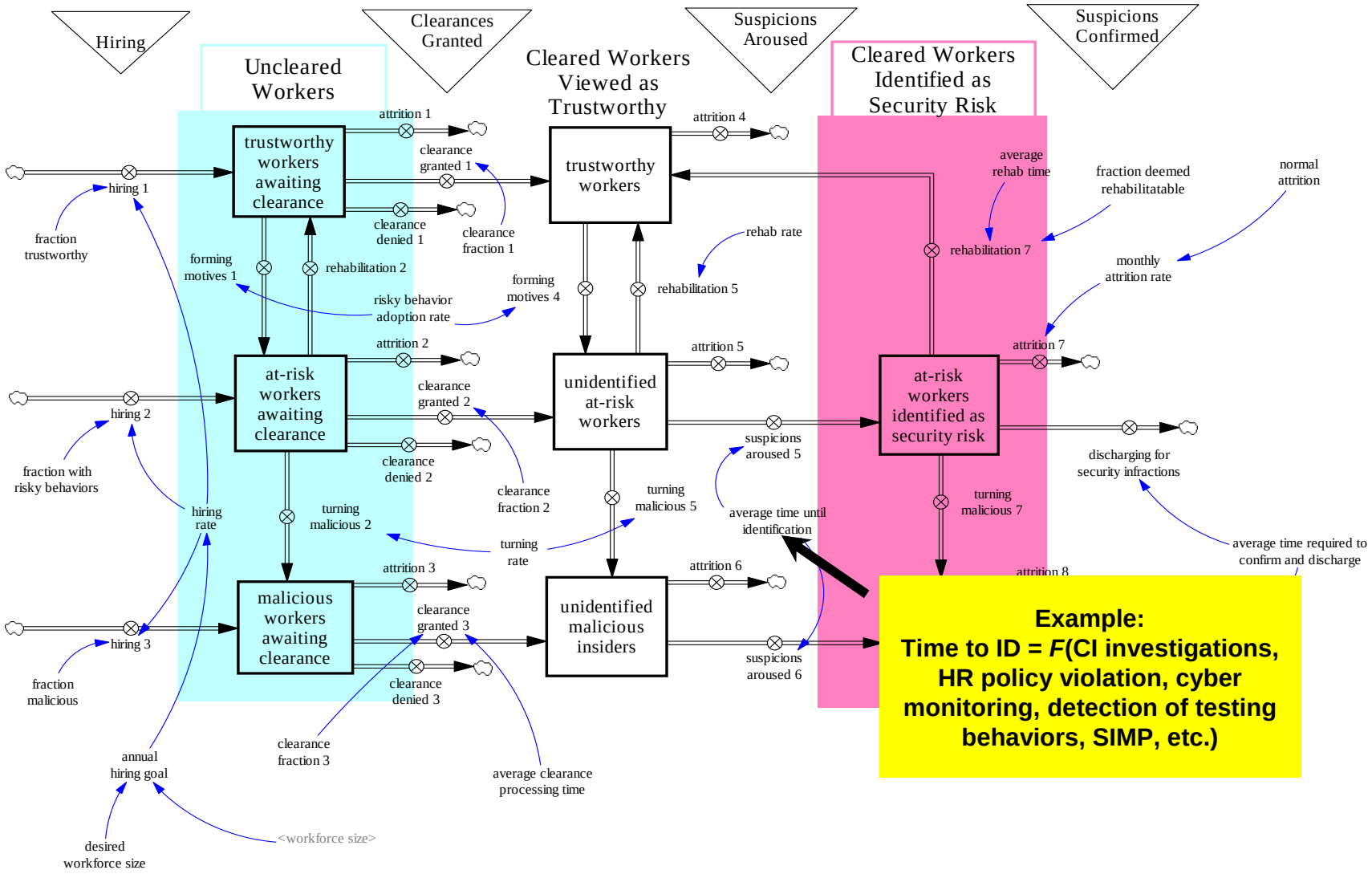


Figure 6. Incorporating security systems and operational procedures within the model.

the employee will not pass the more in-depth investigation to obtain the security clearance required for their job position.

The scenario looked at a change in policy regarding hiring: what would be the effect of hiring already cleared versus uncleared personnel that must wait their security clearance, sometimes 12 to 24 months? The proposed process would require an applicant to receive a minimum-level security clearance before being hired. The model was exercised for this scenario to explore the impacts of system changes. Organizational costs or risks were defined as

- the cost of maintaining employees with less than 100% productivity because they cannot fully perform their job assignments,
- the possibility that the employees would not be granted clearances, and
- the costs of maintaining a separate infrastructure for uncleared employees.

This scenario was expected to reduce the potential insider threat and increase productivity for new employees.

The results generated by the model for the example scenario are representative based on hypothetical data. They show that the model yields reasonable and credible results and, with accurate data and refinement, the model shows promise as a tool in analyzing insider security systems. For the example scenario, the metrics included workforce productivity and an insider threat index. Conventional wisdom has it that the ability to achieve organizational mission success must be balanced against maintaining security. However, not every policy decision need represent a tradeoff between these two often competing goals. The results for the example scenario, shown in Figure 7, appear to improve both security and productivity. The results indicate that requiring a security clearance for new hires yields an increase in workforce productivity, as well as a desired reduction in the insider threat index. It also supports a burgeoning new hypothesis that much more emphasis should be placed on *preventing* the infusion of malicious insiders into the system (as compared to the current system that emphasizes detection). Such a system would stress up-stream, proactive, preventative policies that promote principles of deterrence, rehabilitation, and more care in the granting of access.

CASE STUDIES OF MALICIOUS INSIDER ACTIVITY

As part of the model development activities, the project team also developed examples of malicious insider activity from actual cases. These included a review of the following:

- Five counterintelligence (CI) investigations of malicious insider activity that have occurred in the U.S. provided by the SNL Office of Counterintelligence (OCI); and
- Famous U.S. espionage cases.

The following sections present a summary of these cases and track these examples through the ELCM. In tracking the cases through the ELCM, an icon of Figure 2 is used to indicate the insider's path through the model.

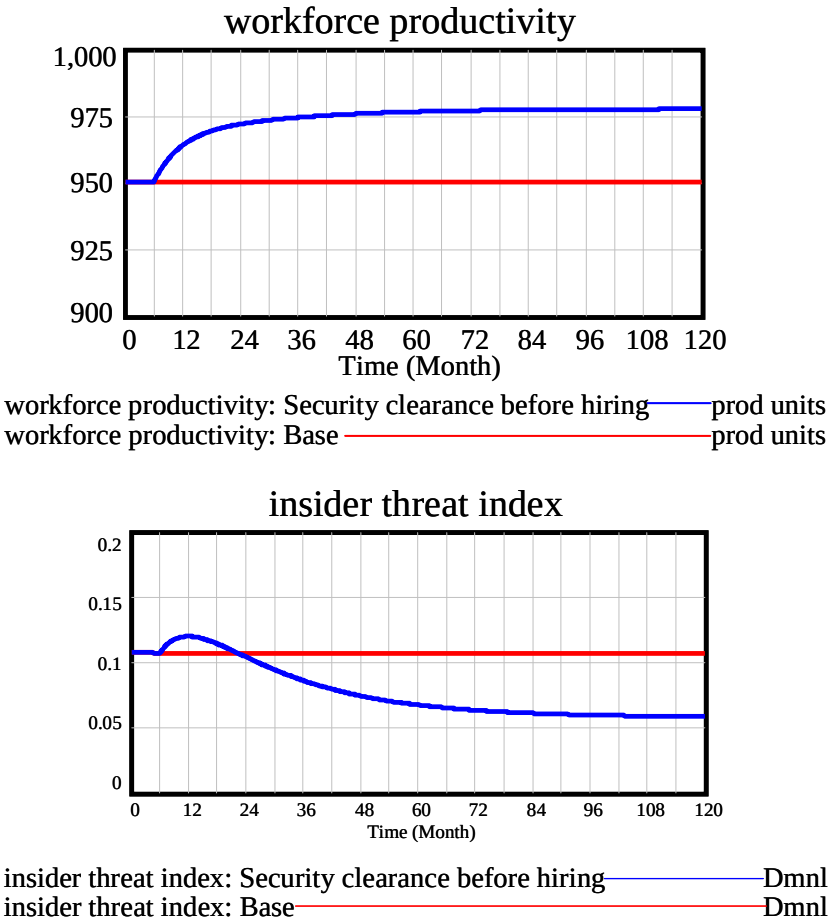


Figure 7. Modeling results for the example scenario.

Counterintelligence Investigations

To obtain intellectual property from Department of Energy (DOE) facilities, such as SNL, foreign intelligence services generally have two options – infiltrate a facility with an insider or recruit an employee as an insider. On average in a year, the SNL OCI undertakes 20 to 25 investigations into reports of malicious insider activity. This is a fraction of the reports that are made, typically by co-workers, to the SNL OCI. Overall, in the four years between 2004 and 2008, the SNL OCI completed over 100 investigations. Ten of those (~10%) uncovered significant CI concerns that resulted in action by SNL executive management, including people being separated from the SNL workforce or other response to the identified threats. The following sections present five cases of these types of CI investigations of malicious insider activity that have occurred in the U.S. and track these cases through the ELCM.

CI Investigation Case 1 – Summary

The first case concerned a foreign national from a sensitive country who was a permanent resident alien pursuing U.S. citizenship. This person did not hold a U.S. government security clearance, but was slated to complete the U.S. citizenship and government security clearance processes. He had established experience and a professional reputation working as a contractor

on U.S. government projects. He was well-liked by the personnel he had worked with on these projects. The CI investigation began after this person's involvement as a contractor on a national security program with his sensitive country of birth. His role was as an intermediary and liaison between program participants from the U.S. and this sensitive country. Although he held no clearance, in this role he had privileged access to U.S. government staff and computer systems. The CI review of his background indicated no derogatory information. Suspicions of his involvement in project activities were reported when it appeared he was targeting specific data with a focus to get additional detailed information. The CI investigation revealed that he had close connections with intelligence service personnel from his home sensitive country – foreign national relationships that he had not divulged. In retrospect, his prior positions as a contractor to the U.S. government could be interpreted as maneuvering toward the position he had with this national security program. At a minimum, the investigation determined that he was being co-opted by this country's foreign intelligence service to obtain information about the national security program.

CI Investigation Case 1 – Tracking through the ELCM

It appears that this person did not report significant foreign national relationships, probably to maintain an appearance of suitability and trustworthiness for employment as a contractor on U.S. government projects and with the intent to successfully obtain a U.S. government security clearance and additional access to information. This indicates that this person had motive and means (allegiance to his home country and significant contacts with its foreign intelligence service) and was seeking opportunity (access to sensitive information) to undertake malicious insider activity. In the ELCM, this person enters the organization at the point of *hiring 3* as a ***malicious worker awaiting clearance*** (left column, bottom tier). Although he was not yet eligible to obtain a security clearance and migrate to become an ***unidentified malicious insider*** (center column, bottom tier), with the privileged access he had established, he was attempting malicious insider activity and perhaps targeting other project staff with actual access sensitive information. As a result of the effective CI reporting and the subsequent investigation, this person essentially was removed from the organization at the point of *clearance denied 3*. The path of this person through the ELCM is shown in Figure 8.

CI Investigation Case 2 – Summary

For the second CI case, the person was born, educated, and worked professionally in a sensitive country. He later came to the U.S. for his graduate education, completed a PhD, became a naturalized citizen, had a job doing unclassified work for a defense contractor, and eventually obtained a U.S. government security clearance. A CI investigation was initiated when he attempted to obtain sensitive information outside his assigned work for which he had no need to know. The deeper investigation revealed that he had worked in his home country for an institution that is known to target the U.S. government for highly sensitive information related to its area of work, including the type of sensitive information he had been seeking. The period of this previous employment was more than seven years before his security clearance application, and therefore he was not required to include it. The information on the security clearance application was technically compliant.

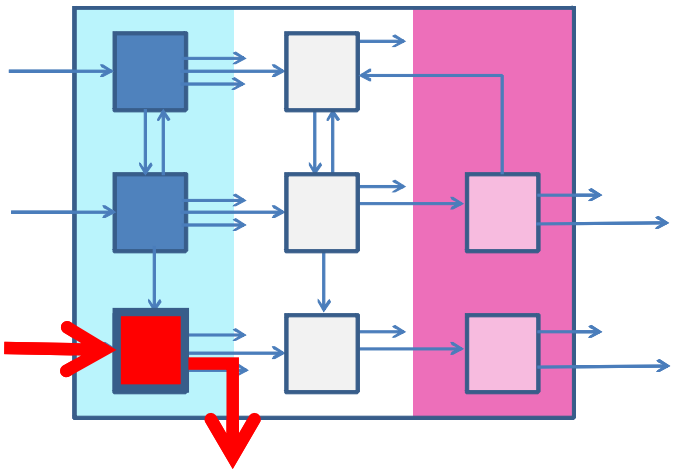


Figure 8. Tracking of CI investigation Case 1 through the ELCM.

CI Investigation Case 2 – Tracking through the ELCM

This case is another example of a person who has motive and means (allegiance to his home country and significant contacts with its foreign intelligence service) and was also able to obtain opportunity (access to sensitive information) to undertake malicious insider activity by successfully obtaining a security clearance. In the ELCM, this person enters the organization at the point of *hiring 3* as a ***malicious worker awaiting clearance*** (left column, bottom tier). He was able to obtain a security clearance, become an ***unidentified malicious insider*** (center column, bottom tier) through the point of *clearance granted 3,* and establish the opportunity to undertake malicious insider activity. As a result of the CI reporting and the subsequent investigation, suspicions were aroused. Subsequently, this person became a ***malicious insider identified as security risk*** (right column, bottom tier) and was removed from the organization at the point of *discharging confirmed insiders.* The path of this person through the ELCM is shown in Figure 9.

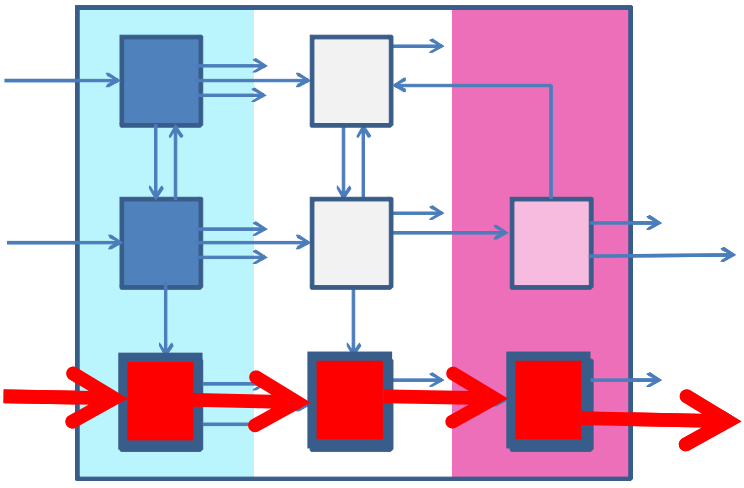


Figure 9. Tracking of CI investigation Case 2 through the ELCM.

CI Investigation Case 3 – Summary

Case three involved possible recruitment of a person born in the U.S. to immigrants from a sensitive country. The parents returned to their home country. This person held dual citizenship and was still eligible for employment with the U.S. government and for a security clearance. He eventually obtained a position in an area that was targeted by his home country intelligence service. He began traveling to his home country every six months to visit his parents because of a reported family illness. During these trips, he did have contact with foreign government officials that he did not report. These contacts were technically not reportable because they were considered personal or incidental contacts. He was still in compliance with reporting requirements, but did try to hide these contacts.

CI Investigation Case 3 – Tracking through the ELCM

For this case, we could assume that the person entered the organization as a ***trustworthy worker awaiting clearance*** (left column, top tier) of the ELCM through the point *hiring 1* and then proceeded to be a ***trustworthy worker*** (center column, top tier) through the point *clearance granted 1* after he received his security clearance. As a result of the combination of the family connections to his home country and the employment position he was able to obtain, he was targeted as an insider asset and moved through the point of *forming motives 4* to become as an ***unidentified at-risk worker*** (center column, middle tier). As a result of his activities revealed through the CI reporting and investigation process, he moved through the point of *suspicions aroused 5* to become an ***at-risk worker identified as security risk*** (left column, middle tier). He then proceeded to be removed from the organization through the point of *discharging for security infractions.* The path of this person through the ELCM is shown in Figure 10.

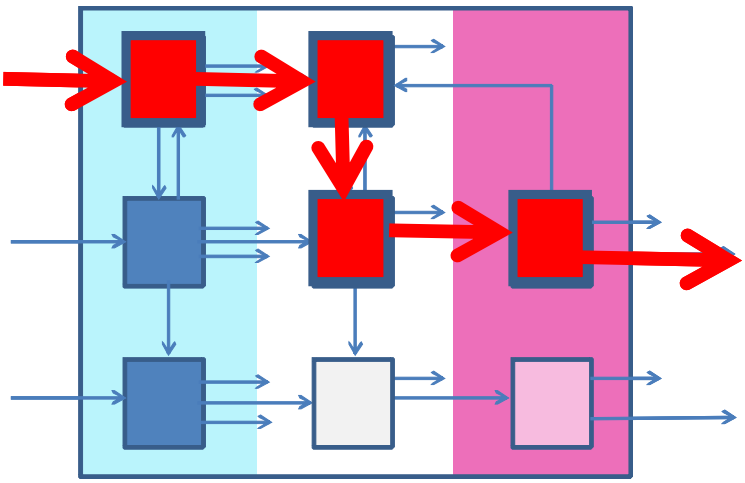


Figure 10. Tracking of CI investigation Case 3 through the ELCM.

Famous Espionage Cases

In addition to the CI case studies, the project team also reviewed famous U.S. espionage cases and tracked these through the ELCM. The cases of Robert Philip Hanssen, George Koval, and Jonathan Jay Pollard are discussed in the following sections.

Robert Philip Hanssen – Case Summary[1]

In February 2001, Robert Hanssen, a veteran CI agent with the Federal Bureau of Investigation (FBI) was arrested and charged with committing espionage by providing highly classified national security information to Russia and the former Soviet Union. Hanssen was employed by the FBI in 1976 and first volunteered in 1985 to furnish sensitive documents to KGB intelligence officers assigned to the Soviet embassy in Washington DC. The most obvious motive for Hanssen's activities was that he began spying when he was in debt, but Hanssen also developed a strong interest and capability in espionage and revealed other psychological issues and behavioral tendencies characteristic of malicious insiders. As a spy, he was able to achieve success he was not able to attain, but felt he deserved, in his legitimate activities. During his career with the FBI, he held key CI positions in New York and Washington DC which afforded him direct and legitimate access to a large volume of information about sensitive programs and operations. Over his career with the FBI, he systematically transferred highly classified national security information in exchange for diamonds and cash worth more than $600,000.

Hanssen Case – Tracking through the ELCM

Hanssen is an example of a person who has motive and was seeking opportunity and means when he obtained employment with the FBI. As he obtained access to sensitive information, he made the decision to develop means as well when he volunteered to the KGB. His path through the ELCM begins at the point of *hiring 2* as an ***at-risk worker awaiting clearance*** (left column, middle tier), through *clearance granted 2* to become an ***unidentified at-risk worker*** (center column, middle tier). At the point of *turning malicious 5*, he became an ***unidentified malicious worker*** (center column, bottom tier) undertaking malicious insider activity for more than 20 years. As his activities were revealed he proceeded through the point of *suspicions aroused 6*, he became a ***malicious insider identified as security risk*** (right column, bottom tier). His arrest removed him from the FBI through the point of *discharging confirmed insiders.* This path for Hanssen through the ELCM is shown in Figure 11.

George Koval – Case Summary[2]

George Koval was a Soviet spy who provided information about the U.S. atomic weapons program during World War II. He was born in Sioux City, IA, the second son of Belarus immigrants whose family emigrated back to the Soviet Union in 1932, where he studied chemical technology and received Soviet citizenship. He was recruited by Soviet Intelligence (the GRU) and in 1940 returned to the U.S. where he worked under the cover of the Raven Electric Company gathering chemical weapons information from U.S. companies. During World War II, he was drafted into the U.S. Army, studied electrical engineering, and was eventually selected for the Special Engineer Detachment that was part of the Manhattan Project. He was very personable and held the position as a health physics officer at Oak Ridge National Laboratory with a high level security clearance and access across the facility. His espionage

---

[1] This summary of the Hanssen case was compiled from the following sources: (1) "Federal Bureau of Investigation – FBI History – Famous Cases – Robert Philip Hanssen," http://www.fbi.gov/libref/historic/famcases/hanssen/hanssen.htm, accessed July 6, 2009; (2) "CI Centre – Counterintelligence – Espionage – Spy Case – Hanssen, Robert Philip," http://www.ciacademy.com/Documents/DOC_Hanssen_1.htm, accessed July 6, 2009; and (3) Wise, David. 2002. *Spy: How the FBI's Robert Hanssen Betrayed America*, New York, NY: Random House.

[2] This summary of the Koval case was compiled from the following source: Walsh, Michael. May 2009. "George Koval: Atomic Spy Unmasked," *Smithsonian*, Vol. 40, No. 2, pp. 40-47.

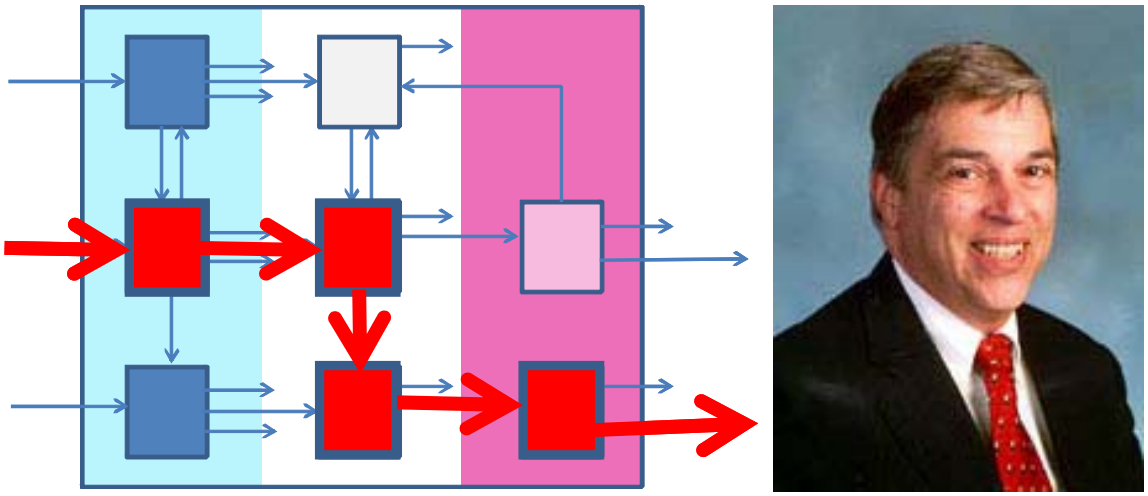


Figure 11. Tracking of Hanssen Case through the ELCM.

activities included providing atomic secrets that accelerated the Soviet's bomb development program. He left the U.S. in 1948, building a new life in the Soviet Union where he died in 2006. The FBI investigated his activities in 1950s, but kept the matter confidential. The 2002 book, *The GRU and the Atomic Bomb*, mentioned Koval by his code-name and revealed his role in Soviet espionage activities during the Manhattan Project. In 2007, he was posthumously awarded the title of Hero of the Russian Federation by Russian President Vladimir Putin.

Koval Case – Tracking through the ELCM

Koval's connection to Soviet intelligence established his motive and means. His path through the ELCM begins at the point of *hiring 3*, seeking opportunity a ***malicious worker awaiting clearance*** (left column, bottom tier). His career in the U.S. Army provided the opportunity for access to sensitive information as he obtained high level clearances – the point of *clearance granted 3* – to become an ***unidentified malicious worker*** (center column, bottom tier). He operated as malicious insider, then exited the organization at the point *attrition 6*, when he left the U.S. in 1948. This path for Koval through the ELCM is shown in Figure 12.

Jonathan Jay Pollard – Case Summary[3]

Jonathan Jay Pollard is a former U.S. Naval civilian intelligence analyst who was convicted in 1987 of spying for Israel. He developed strong interest in Israel as a teen. After graduate school, he began applying for intelligence service jobs in 1979 and was turned down by the Central Intelligence Agency (CIA) after taking a polygraph test, which indicated drug use. He was hired for a position by Naval intelligence, which required a background check and security clearance, but no polygraph test. Early in his career, Pollard demonstrated significant inappropriate behavior and had significant problems including requests for termination and termination of his clearances by two of his superiors. When he was reassigned to less sensitive duties, Pollard filed a grievance to recover his top level clearance. Because of series of transfers and reorganizations

[3] This summary of the Pollard case was compiled from the following source: "Jonathan Pollard – Wikipedia, the free encyclopedia," http://en.wikipedia.org/wiki/Jonathan_Pollard, accessed July 7, 2009.

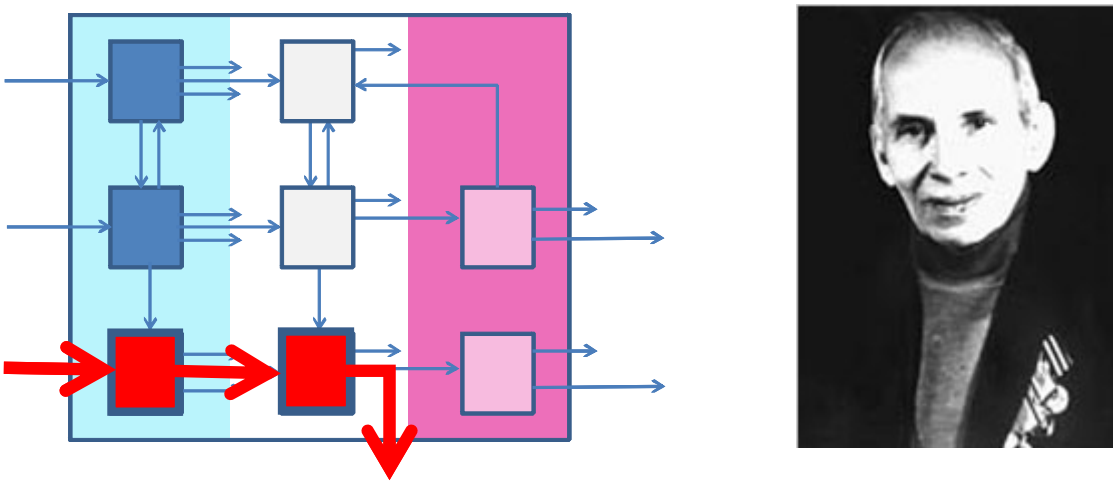


Figure 12. Tracking of Koval Case through the ELCM.

and excellent performance reviews he received after he filed his grievance, Pollard was able to move into a position as an intelligence analyst for the Naval Intelligence Service. He met an Israeli Air Force veteran in 1984, and began providing classified information shortly after for which he received a diamond and sapphire ring and $10,000 cash. He agreed to additional monthly payment for further espionage. Pollard spent about 18 months committing espionage before an anonymous report of his suspicious removal of classified material. The subsequent investigation revealed that Pollard had supplied Israel with a tremendous number of classified documents. He pleaded guilty in May 1986.

Pollard Case – Tracking through the ELCM

Tracking Pollard through the ELCM begins at the point *hiring 2*, where he enters the organization as an ***at-risk worker awaiting clearance*** (left column, middle tier). He proceeds through the point *clearance granted 2* to become an ***unidentified at-risk worker*** (center column, middle tier), where his career problems provide him with motive and opportunity. When he establishes contact with the Israeli veteran, he develops means and proceeds through the point *turning malicious 5* to become an ***unidentified malicious insider*** (center column, bottom tier). With the report of his removal of classified information, he proceeds through the point *suspicions aroused 6* as an ***identified malicious insider*** (left column, bottom tier). He is removed from the organization through the point *discharging confirmed insiders*. This path for Koval through the ELCM is shown in Figure 13.

FUTURE EFFORTS

It is evident from this development of a prototype model that there is utility in framing the insider threat in terms of the employee lifecycle, supporting the development of a holistic approach security system design and evaluation. The ELCM provides a promising tool for evaluating how the insider threat evolves in an organization and what protection measures and operational procedures will reduce this threat most effectively.

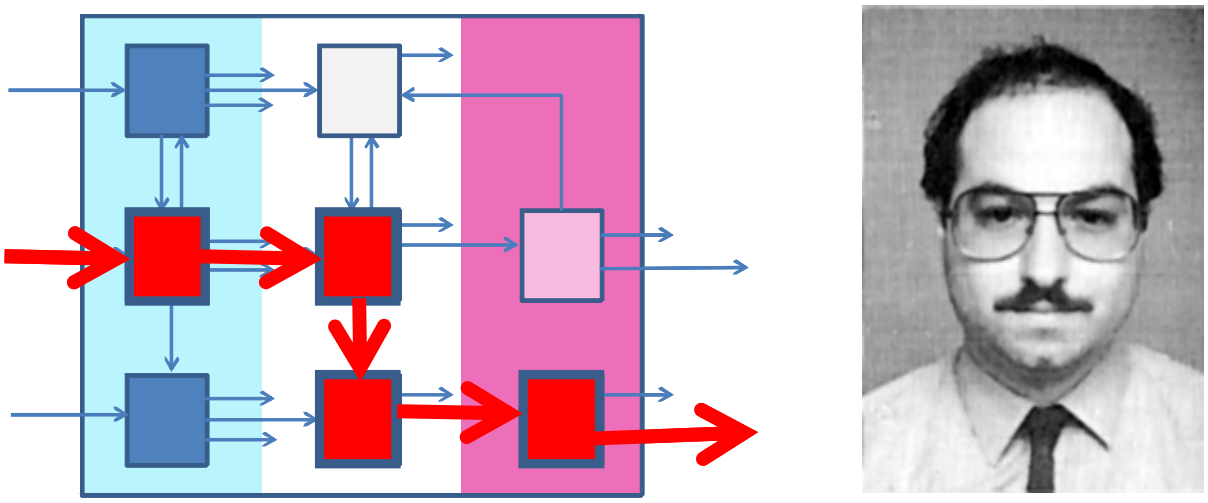


Figure 13. Tracking of Pollard through ELCM.

However, additional work remains for us to build on these initial model development efforts, creating a mature model suitable to support policy analysis:

- Concentrate on capturing system feedbacks

  The current version of the model provides a structural framework for tracking accumulations, but the flows and their dependencies are underdeveloped in this prototype version. We intend to expand upon our initial efforts to interact with a variety of security experts to elicit their observations regarding their experiences in implementing security policies to deal with the insider threat.

- Include dynamics associated with administration and control of the access to sensitive information

  Figure 14 provides a sketch representing our initial thinking. The workers viewed as trustworthy will accumulate access to protected information as needed to perform their jobs. Gaining legitimate information access can be minimized by enacting administrative controls that limit access to those workers with a legitimate need to know. However, taken too far, this may impact productivity. Conversely, relaxing these controls may enhance productivity, but at the expense of information access management. Accumulated information can be depleted by three mechanisms. First, over time the information can become outmoded. Likewise, at some rate forgetting will occur over time. Finally, as employees change jobs and their need-to-know goes away, their legitimate access should be terminated.

  There are two kinds of information – archival and employee memories. We lump paper and electronic information together as archival information. Particularly with regard to the three depletion mechanisms, there will be differences between archival information and information stored "between the ears" of the employees. Memories can be forgotten, but this doesn't happen with archival info. Conversely, access to archival information can be revoked, but this has no impact on memory retention. Both archival information and memory can become outmoded over time.

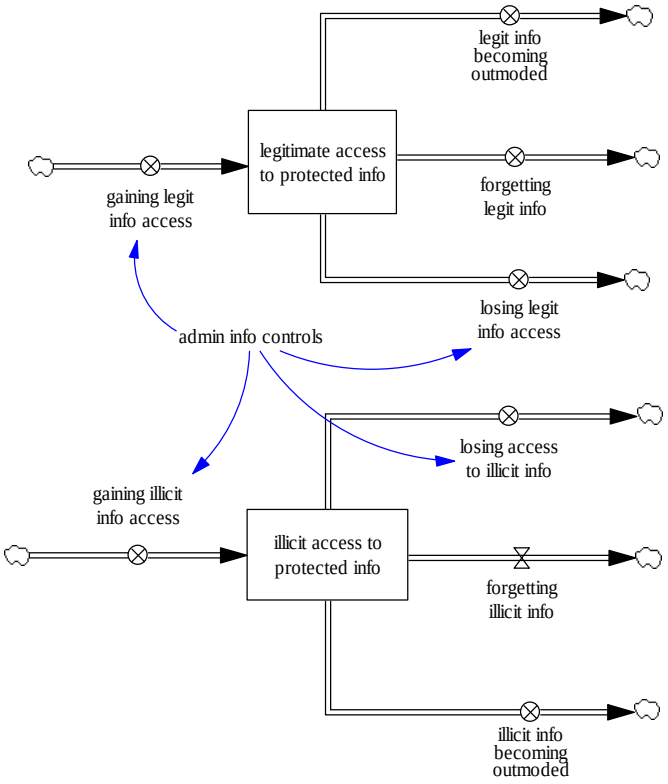
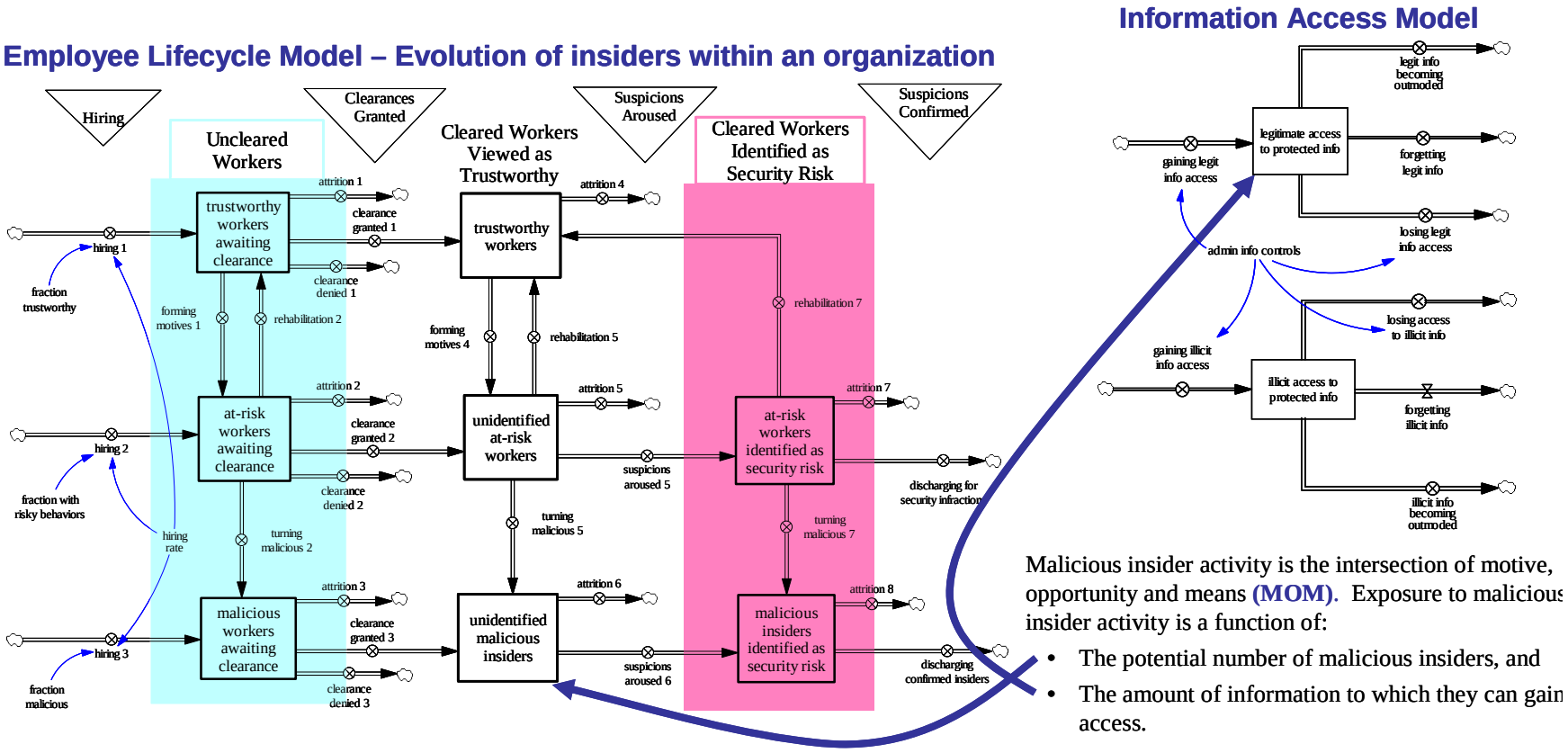


Figure 14. A stock-and-flow diagram representing the accumulation and depletion of access to protected information.

As one example, extraordinary work pressures may induce workers to illicitly cache information as a corner-cutting mechanism. Also, at-risk or malicious workers may probe the system attempting to gain access to information without authorization. Just as with the legitimate information access, the illicit information access can be depleted by either becoming outmoded, forgetting (for memory), and losing access (to archival info, such as by finding and patching a vulnerability).

Figure 15 overall illustrates overall how malicious insider activity is the intersection of MOM and how exposure of an organization to malicious insider activity is a function of the number of potential malicious insiders and the amount of information to which they can gain access.

These extensions of the prototype ELCM provide a framework to understand important interactions, interdependencies and gaps in insider protection strategies. The development of a systems-based approach will provide additional capabilities to incorporate and analyze a variety of insider security protection strategies to include formal security practices as well as operational procedures that comprise overall insider security. Additionally, insights from the system dynamics modeling provide the basis for identifying a preliminary set of objectives and principles for intrinsic insider security. Improved insider security should result by defining these key objectives and principles as part of an integrated systems-based process for designing, evaluating and operating effective insider security systems.



Malicious insider activity is the intersection of motive, opportunity and means **(MOM)**. Exposure to malicious insider activity is a function of:

- The potential number of malicious insiders, and
- The amount of information to which they can gain access.

Figure 15. Exposure to malicious insider activity – intersection of MOM and information access.

ACKNOWLEDGMENTS

This work was funded as a Laboratory Directed Research and Development (LDRD) project at Sandia National Laboratories (SNL). This work has benefited tremendously from the perspectives and significant expertise of the members of the Insider Team at Sandia National Laboratories, including Betty E. Biringer, John L. Russell, Consuelo J. Silva, Carla A. Ulibarrí and Gregory D. Wyss (Security Systems and Technology Center); and Roger A. Suppona (Cyber Monitoring and Policies Center).

REFERENCES

Andersen, David, Dawn M. Cappelli, Jose J. Gonzalez, Mohammad Mojtahedzadeh, Andrew P. Moore, and Eliot Rich. 2004. "Preliminary System Dynamics Maps of the Insider Cyber-threat Problem in *Proc. 22nd Int'l Conference of Sys Dynamics Society,* Albany NY: The System Dynamics Society.

Anderson, Robert H., Thomas Bozek, Tom Longstaff, Wayne Meitzler, Michael Skroch, and Ken Van Wyk. 2000. *Conference Proceedings – Research on Mitigating the Insider Threat to Information Systems – #2*, CF-163-DARPA, RAND National Defense Research Institute, Santa Monica CA: The RAND Corporation.

Band, Stephen R., Dawn M. Cappelli, Lynn F. Fischer, Andrew P. Moore, Eric D. Shaw, and Randall F. Trzeciak. 2006. *Comparing Insider IT Sabotage and Espionage: A Model-Based Analysis*, Technical Report CMU/SEI-2006-TR-026, ESC-TR-2006-091, Software Engineering Institute, Pittsburgh PA: Carnegie Mellon University.

Crayton, Christopher. 2003. *Security+ Exam Guide*, Boston MA: Charles River Media, Boston MA.

Gregg, Michael. 2007. "Network Security Threats and Answers, By Industry," Advice website: http://searchnetworking.techtarget.com/generic/0,295582,sid7_gcil238902,00.html

Herbig, Katherine L., and Martin F. Wiskoff. 2002. *Espionage Against the United States by American Citizens 1947-2001*, PERSEREC Technical Report 02-5, Monterey CA: Defense Personnel Security Research Center.

Hodel, Steve. 2004. *Black Dahlia Avenger: A Genius for Murder*, New York NY: HarperCollins, p. 36.

Hoffman, Bruce, Christina Meyer, Benjamin Schwarz, and Jennifer Duncan. 1990. *Insider Crime: The Threat to Nuclear Facilities and Programs*, R-3782-DOE, Santa Monica CA: The RAND Corporation.

Keeney, Michelle, Eileen Kowalski, Dawn Cappelli, Andrew Moore, Timothy Shimeall, and Stephanie Rogers. 2005. *Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors*, U.S. Secret Service and CERT Coordination Center, Software Engineering Institute, Pittsburgh PA: Carnegie Mellon University.

Martinez-Moyano, Ignacio J., Eliot H. Rich, Stephen H. Conrad, Thomas R. Stewart, and David F. Andersen. 2006a. "Integrating Judgment and Outcome Decomposition: Exploring Outcome-based Learning Dynamics," in *Proceedings of the 24th International Conference of the System Dynamics Society,* Albany NY: The System Dynamics Society.

Martinez-Moyano, Ignacio J., Eliot H. Rich, Stephen H. Conrad, and David F. Andersen. 2006b. "Modeling the Emergence of Insider Threat Vulnerabilities," in *Proceedings of the 2006*

Winter Simulation Conference, Piscataway NJ: Institute of Electrical and Electronics Engineers.

Martinez-Moyano, Ignacio J., Eliot H. Rich, Stephen Conrad, David F. Andersen, and Thomas R. Stewart. 2008. "A Behavioral Theory of Insider-Threat Risks: A System Dynamics Approach," *ACM Trans. on Mod. and Comp. Sim. (TOMACS)*, vol. 18, pp. 1-36.

Rich, Eliot, Ignacio J. Martinez-Moyano, Stephen Conrad, Dawn M. Cappelli, Andrew P. Moore, Timothy J. Shimeall, David F. Andersen, José J. Gonzalez, Robert J. Ellison, Howard F. Lipson, David Mundie, José Maria Sarriegui, Agat Sawicka, Thomas R. Stewart, José Manuel Torres, Elise A. Weaver, and Johannes Wiik. 2005. "Simulating Insider Cyber-Threat Risks: A Model-Based Case and a Case-Based Model," in *Proc. 23th Int'l Conference of Sys Dynamics Society*, Albany NY: The System Dynamics Society, p. 126.

Schneier, Bruce. 2000. *Secrets & Lies: Digital Security in a Networked World*, New York NY: John Wiley & Sons.

Turner, James T., and Michael G. Gelles. 2003. *Threat Assessment: A Risk Management Approach*, Binghamton NY: Haworth Press.