Software Engineering Institute

# Comparing Insider IT Sabotage and Espionage: A Model-Based Analysis

Stephen R. Band, Ph.D. (Counterintelligence Field Activity - Behavioral Science Directorate)
Dawn M. Cappelli (CERT)
Lynn F. Fischer, Ph.D. (DoD Personnel Security Research Center)
Andrew P. Moore (CERT)
Eric D. Shaw, Ph.D. (Consulting & Clinical Psychology, Ltd.)
Randall F. Trzeciak (CERT)

**December 2006**

**TECHNICAL REPORT**
CMU/SEI-2006-TR-026
ESC-TR-2006-091

**CERT® Program**


Carnegie Mellon

This report was prepared for the The Defense Personnel Security Research Center.

The ideas and findings in this report should not be construed as an official DoD position. It is published in the interest of scientific and technical information exchange.

This work is sponsored by the U.S. Department of Defense. The Software Engineering Institute is a federally funded research and development center sponsored by the U.S. Department of Defense.



For information about purchasing paper copies of SEI reports, please visit the publications portion of our Web site (http://www.sei.cmu.edu/publications/pubweb.html).

# Table of Contents

# List of Figures

# List of Tables

# Executive Summary

The purpose of this study is to examine psychological, technical, organizational, and contextual factors we believe contribute to at least two forms of insider trust betrayal: insider sabotage[1] against critical information technology (IT) systems, and espionage. Security professionals and policy leaders currently view espionage and insider threat as serious problems but often as separate issues that should be addressed by a different configuration of security countermeasures. In this study, our team of researchers investigated similarities and differences between insider IT sabotage and espionage cases to assess whether a single analytical framework based on system dynamics modeling could be developed to isolate the major factors or conditions leading to both categories of trust betrayal.

Based on the results, it is our position that insider IT sabotage and espionage share many contributing and facilitating system dynamics features. It follows that they might be detected and deterred by the same or similar administrative and technical safeguards. Research into countermeasures that address multiple threats should be of high priority so that organizations can adopt safeguards that counter both espionage and IT sabotage crimes. One outcome of this project is a description of research areas that are likely to identify such countermeasures.

Our modeling effort found definite parallels between the two categories of trust betrayal. The team created three models: one for IT sabotage, one for espionage, and one model, which we call the *abstracted common model*, representing a high-level view of the commonalities between the two domains. At present, these models are *descriptive* in nature, in that they attempt to describe the complex relationships among variables comprising the insider IT sabotage and espionage problem space. The models are based primarily on a combination of empirical trends observed in the cases examined and, secondarily, on the expert knowledge of the project team. In addition, the models were validated by comparing them against actual cases of sabotage and espionage available to the Insider Threat Team. Additional research and data collection regarding the relative impact of countermeasures on insider risk would be required to create *predictive* models, but this is beyond the scope of our current project.

### RESEARCH FINDINGS

Analysis of the system dynamics models leads to six major observations:

- *Observation #1:* Most saboteurs and spies had common personal predispositions that contributed to their risk of committing malicious acts.
- *Observation #2*: In most cases, stressful events, including organizational sanctions, contributed to the likelihood of insider IT sabotage and espionage.

[1] We define *insider IT sabotage* as malicious activity in which the insider's primary goal was to sabotage some aspect of an organization or to direct specific harm toward an individual or individuals. Definitions of other key terms used throughout the document are in Appendix I – Glossary.

- *Observation #3:* Concerning behaviors were often observable before and during insider IT sabotage and espionage.
- *Observation #4:* Technical actions by many insiders could have alerted the organization to planned or ongoing malicious acts.
- *Observation #5:* In many cases, organizations ignored or failed to detect rule violations.
- *Observation #6:* Lack of physical and electronic access controls facilitated both IT sabotage and espionage.

We support and explain each observation in terms of a portion of the abstracted common model. The description of each observation includes one espionage case example and one sabotage case example to further substantiate the observation and the associated model portion.

Although the original intention of this project was not to develop actionable conclusions, our findings led to recommendations for further research to support the mitigation of the risk of insider IT sabotage and espionage. These are summarized as follows:

- *Recommendation #1:* Develop a risk-indicator instrument for the assessment of behaviors and technical actions related to potential risk of insider IT sabotage or espionage.
- *Recommendation #2:* Acquire improved data on the relative distribution, interrelationships, and weight with respect to attack risk of concerning behaviors, stressful events, and personal predispositions across insider cases in IT sabotage and espionage.
- *Recommendation #3:* Acquire improved data related to technical actions that are and are not indicative of insider IT sabotage and espionage.
- *Recommendation #4:* Research policies, methods, and tools for auditing and monitoring behaviors and technical actions that are indicative of insider IT sabotage and espionage.
- *Recommendation #5:* Acquire improved data to assess the relationship between policy enforcement for behavioral and technical rule violations and the risk of insider IT sabotage and espionage.
- *Recommendation #6:* Analyze current access control policies and practices and identify and evaluate options to mitigate insider threat risk.
- *Recommendation #7:* Use the risk-indicator instrument noted in Recommendation #1 to acquire improved information on the base rates and baseline level of risk factors in proportion to actual insider activity.

Finally, based on its analysis, the team identified policy implications in the following areas:

- case data management
- management training
- security awareness training
- employee auditing and monitoring
- human resources policies
- access controls
- technical practices for prevention or detection of espionage and insider IT sabotage
- termination policies

## VALUE OF MODELING EFFORTS

A question of interest to the research team is to what extent the model-based approach contributed to greater understanding of the domains. It is likely that simply bringing together a group of people with such a broad range of experiences in insider threat and espionage would have produced positive results. However, we found that the system dynamics approach brought a number of positive benefits to the group analysis:

- The approach helped to structure and focus the team's discussion. This was particularly important since members of the team, by necessity, came from a variety of disciplines, including psychology, political science, history, counterintelligence, law enforcement, personnel security, and information security.
- The approach helped the team communicate more effectively. The rigorous notation involved helped identify commonalities to simplify the models and prevent misunderstandings that would have hindered progress.
- The models that we developed in group sessions provided a take-away for people that not only documented our progress, but also helped us pick up from where we left off after a period of downtime and reflect on what we had accomplished.
- The modeling approach facilitated the identification of commonalities between the insider IT sabotage and espionage domains.
- The models provided a concrete target for validation through mapping to observables exhibited by the real-world cases.

While this is the final report on our initial collaboration to compare the domains of insider IT sabotage and espionage, we hope that the collaboration continues. The team has assembled a database of areas that need further exploration to map out the problem domains more fully and understand their commonality. We believe that additional work is needed in both the analysis of case data and the elaboration of our system dynamics models. This report is a vital checkpoint regarding our current progress and future plans in this area. Feedback is critical to ensure the quality and direction of the work is consistent with the missions of the organizations involved.

# Acknowledgements

This project was sponsored and funded by the DoD Personnel Security Research Center (PERSEREC).

The project team consisted of the authors of this paper. The authors would also like to acknowledge contributions to the project by the following people whose expertise and participation were key to the project's success.

### PERSEREC

Dr. Katherine L. Herbig, Dr. Kent Crawford, and Dr. Eric Lang from PERSEREC contributed their expertise in the areas of espionage and insider threat.

### DEPARTMENT OF DEFENSE

Also in support of this effort Dr. Richard Ault, consultant to the Defense Intelligence Agency, provided unique insights into espionage cases that enhanced the quality of the model.

### UNITED STATES SECRET SERVICE NATIONAL THREAT ASSESSMENT CENTER

Our special thanks go to Dr. Marisa Reddy Randazzo, Dr. Michele Keeney, and Eileen Kowalski, behavioral psychologists and researchers in the U.S. Secret Service's National Threat Assessment Center, who served as the Secret Service's principal researchers on the *Insider Threat Study*. Their partnership with CERT in the study enabled us to establish the foundation of our insider threat research in CERT.

### CERT

Bradford Willke worked on both the *MERIT* and PERSEREC projects for some time before leaving the projects for new commitments. William Wilson and Joseph McLeod provided assistance and input throughout the project. In addition, Dr. Elise A. Weaver played a key role in development of the *MERIT* model by facilitating the group modeling effort and providing psychological expertise.

And finally we greatly appreciate the efforts of Ed Desautels, the editor of many of CERT's insider threat reports, who once again provided invaluable assistance in making this complex material comprehensible to the readers.

# Abstract

This report examines the psychological, technical, organizational, and contextual factors thought to contribute to at least two forms of insider trust betrayal: insider sabotage against critical information technology (IT) systems, and espionage. Security professionals and policy leaders currently view espionage and insider threat as serious problems but often as separate issues that should be each addressed by a different configuration of security countermeasures. In this study, researchers investigated similarities and differences between insider IT sabotage and espionage cases to isolate the major factors or conditions leading to both categories of trust betrayal. The team developed a descriptive model using the system dynamics methodology that represents the high-level commonalities between the two domains based on models of the individual domains.

The effort found definite parallels between the two categories of trust betrayal. Factors observed in both saboteurs and spies include

- the contribution of personal predispositions and stressful events to the risk of an insider committing malicious acts
- the exhibition of behaviors and technical actions of concern by the insider preceding or during an attack
- the failure of their organizations to detect or respond to rule violations
- the insufficiency of the organization's physical and electronic access controls.

Based on the study's findings and analysis, recommendations and policy implications are also presented.

# 1 Introduction

The literature on insider trust betrayal is rich in case studies with minimal attempts at systematic generalization or comparison. Several reports on contemporary espionage, however, have presented an analysis of aggregate information across cases, with the goal of revealing patterns and trends. The most successful effort in this regard was reported by the U.S. Department of Defense's Personnel Security Research Center (PERSEREC) in *Espionage Against the United States by American Citizens, 1947-2001*, which looks at distributions on key variables and cross-tabulations showing associations among variables [Herbig 2002].

Research efforts looking at trust betrayal have tended to be descriptive and policy oriented rather than explanatory or predictive. The infrequency of espionage makes it difficult to create random sampled behavioral data sets suitable for empirical research. However, some investigators believe the greater body of knowledge is enhanced and achieved by conducting interviews with incarcerated spies and saboteurs. Issues regarding predictive validity aside, understanding the individual psycho-social motivations and developmental histories of formerly trusted insiders lends insight into some security vulnerabilities and future investigative strategies.

There have been few efforts to map out a predictive model or framework for understanding this category of crime. These have tended to focus on the individual offender and his or her psychological predispositions or "issues." Thus, strategies for addressing the insider threat to valued assets in government or industry—whether they be classified information, trade secrets, or nuclear materials—lean heavily on vetting systems and background investigations to guarantee the reliability of each trusted employee. History has shown, however, that individuals deemed trustworthy when first hired years later committed some of the most damaging acts of espionage on record. For example, Robert Hanssen began espionage activity in 1979, three years after his background investigation; and Jonathan Pollard began his spying in 1984, five years after a periodic reinvestigation in 1979.[2]

The purpose of this study is to examine psychological, technical, organizational, and contextual factors we believe contribute to at least two forms of insider trust betrayal: insider sabotage against critical information technology (IT) systems, and espionage. We define insider IT sabotage as malicious activity in which the insider's primary goal was to sabotage some aspect of an organization or to direct specific harm toward an individual(s). Throughout this report, we use the term "spy" to refer to espionage and "saboteur" to refer to IT sabotage. The term "insider" encompasses both spies and saboteurs. Refer to Figure 1 for further clarification.

[2] These dates are derived from a query to the PERSEREC Espionage Database.

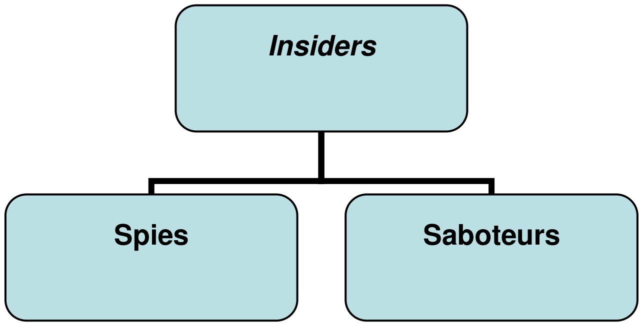


*Figure 1: Use of Terms: Spies, Saboteurs, and Insiders*

Security professionals and policy leaders currently view espionage and the insider threat as serious problems but often as separate issues that should be addressed by a different configuration of security countermeasures. In this study, researchers[3] investigated similarities and differences between insider IT sabotage and espionage cases to assess whether a single analytical framework based on system dynamics modeling could be developed to isolate the major factors or conditions leading to both categories of trust betrayal.

Based on the results, it is our position that insider IT sabotage and espionage are not distinct categories of crime, but variations on the same aberrant behavior. It follows that they might be detected and deterred by the same or similar administrative and technical safeguards. The argument for this convergence is strengthened by the fact that in several of the most recent damaging espionage cases (e.g., Aldrich Ames, 1994; Robert Hanssen, 2001; Ryan Anderson, 2004), the perpetrators have misused official information systems as a tool to search, retrieve, store, and contact or even transmit classified information to foreign agents. Conversely, several of the more serious cases of insider abuse of IT systems have had clear counterintelligence implications.[4]

Research into countermeasures that address multiple threats should be of high priority so that organizations can adopt safeguards that counter both espionage and insider IT sabotage crimes. One outcome of this project is a description of research areas that are likely to identify such countermeasures.

Note that our research for this project was based on open source information available for the espionage cases. Therefore, we feel comfortable using actual names of spies throughout this report. Appendix H contains brief descriptions of the espionage cases taken from the PERSEREC report ESPIONAGE CASES 1975-2004, Summaries and Sources [PERSEREC 2004].

However, our information for the sabotage cases was based on a variety of information sources, including case files from the *Insider Threat Study* that contain information not available to the public. Therefore, the use of saboteur names is avoided throughout this report.

---

3 The team includes researchers from the CERT Program in Carnegie Mellon University's Software Engineering Institute working closely with researchers at the Defense Personnel Security Research Center (PERSEREC).

4 Examples include the case of Eric Jenott of 1996 and attacks on the U.S. Army Enlisted Records and Evaluation System of 1999. These cases are summarized in a recent paper presented to the International Military Testing Association [Fischer 2003].

## 1.1 BACKGROUND

PERSEREC and the CERT Program (CERT) at Carnegie Mellon University's Software Engineering Institute initiated an ongoing partnership in 2001 to jointly research cyber insider threats in the military services and defense agencies. The work began in response to recommendations in the 2000 *DoD Insider Threat Mitigation report*.[5] The focus of that partnership was to identify characteristics of the environment surrounding insider cyber events evaluated for criminal prosecution by DoD investigative services. Since that time, both organizations have also conducted separate research in this area, publishing detailed results analyzing both the psychological and technical aspects of malicious technical activity by trusted insiders.[6] This section provides a brief overview of PERSEREC and CERT research in insider threat.

## 1.2 PERSEREC RESEARCH

From its establishment in 1986, PERSEREC has maintained a clear research focus on the question of the insider threat. Until recently, however, its researchers, who have attempted to define and understand the sources of that threat, have seen it almost exclusively in terms of the threat to classified and controlled government information and as an issue of trust betrayal for the cleared employee workforce. The DoD Personnel Security Program and the system for granting clearances (our substantive research concern) exists in large part to prevent espionage. Consequently, PERSEREC has undertaken a number of studies aimed specifically at helping the community understand how to recognize and prevent espionage-related behaviors.

One of PERSEREC's initial research efforts was the compilation of a database of information from publicly available sources on espionage. The Espionage Database now has coverage on 200 variables and describes over 150 criminal events.[7] In a parallel effort, PERSEREC has published, for educational and awareness purposes, a catalog of short case summaries on espionage events reported in the public media and in other open sources.[8]

While historically committed to a program of the study of espionage, PERSEREC researchers have come to recognize that other DoD assets, in addition to classified information, are vulnerable to adverse insider behavior and that our research resources should be devoted to the protection of critical information systems and the sensitive data they contain. As early as 1993, PERSEREC sponsored a conference on computer crime as a personnel security concern.[9] In addition, responding to a recommendation in the *DoD Insider Threat Mitigation* report [OSD 2000],

---

5 See http://www.dod.mil/nii/org/sio/iptreport4_26dbl.doc.

6 CERT insider threat research can be found at http://www.cert.org/insider_threat/. PERSEREC insider threat research is detailed in [Shaw 2005a] and Shaw and Fischer [Shaw 2005b].

7 Two reports on the analysis of that database have been issued: *Americans Who Spied Against their Country since World War II* [Wood 1992] and the report cited earlier by Katherine Herbig [Herbig 2002].

8 The most recent edition, *Espionage Cases: 1975-2004* [PERSEREC 2004], is regularly used as a training aid in the DoD, CIA, and other federal agencies. Other PERSEREC studies on espionage have resulted in technical reports such as *Temperament Constructs Related to Betrayal of Trust* [Parker 1991], *Assessment of Position Factors that Increase Vulnerability to Espionage* [Crawford 1993], and *Technological, Social, and Economic Trends that Are Increasing U.S. Vulnerability to Insider Espionage* [Kramer 2005].

9 The proceedings from that conference, *Computer Crime: A Peopleware Problem: Proceedings of a Conference Held October 25-26, 1993* [Sarbin 1996], contain a number of papers that focus on the human side of IT systems vulnerability.

PERSEREC designed and began to populate an Insider Events Database that now contains quantitative and descriptive information on over 80 cases of serious insider offenses that have occurred in Defense components and industry.[10]

More recently, PERSEREC has sponsored work undertaken by Dr. Eric Shaw, clinical psychologist and consultant to federal agencies on insider crime, that focuses on insider offenders in national critical infrastructure industries.[11] This recent study draws theoretical insight from ten in-depth case analyses. Shaw describes a critical pathway model for understanding insider attacks that begins with personal predispositions and personal and professional stressors that lead to maladaptive behavioral reactions and culminate in damaging attacks spurred by insufficient or inappropriate management intervention.[12]

In the authors' view, espionage and insider studies undertaken by PERSEREC since the mid-1980s have set the foundation for the current research effort. We have arrived at an understanding that no explanation or theory of insider trust betrayal is satisfactory unless it recognizes the significance of personal issues and psychology as well as organizational, social, and technical factors in the workplace. Significant variables include those that promote or permit crime as well as those that deter or mitigate it. Furthermore, conditions or factors change across time, and in changing they have effects (and sometimes unintended consequences) on other variables. The implied goal of this exercise is to identify where and what types of intervention will best prevent or discourage adverse insider behavior.

## 1.3 CERT RESEARCH

In 2002, CERT and the U.S. Secret Service (USSS) initiated the *Insider Threat Study*—a joint study of the psychological and technical issues surrounding actual insider threat cases.[13] The study combined the U.S. National Threat Assessment Center's (NTAC) expertise in behavioral psychology with CERT's technical security expertise to provide in-depth analysis of approximately 150 insider incidents that occurred in critical infrastructure sectors between 1996 and 2002. Analysis included the thorough review of case documentation and interviews of personnel involved in each incident.

Two reports have been published to date as part of the *Insider Threat Study*, one analyzing malicious insider incidents in the banking and finance sector [Randazzo 2004], and another

---

[10] A final report has not yet been issued on the analysis of these data, but two papers, prepared for professional conferences, provide initial findings from the data set, "A New Personnel Security Issue: Trustworthiness of Defense Information Systems Insiders" [Fischer 2000] and "Characterizing Information Systems Insider Offenders" [Fischer 2003].

[11] The resulting report, *Ten Tales of Betrayal: The Threat to Corporate Infrastructures by Information Technology Insiders* [Shaw 2005b] was released as a PERSEREC technical report.

[12] Dr. Shaw has continued his work for PERSEREC in a recent study on the insider threat: *A Survey of Innovative Approaches to IT Insider Prevention, Detection, and Management* [Shaw 2006b] and, of course, in the present study in which his expertise has been exceedingly helpful.

[13] The *Insider Threat Study* was funded by the USSS, as well as the Department of Homeland Security, Office of Science and Technology, which provided financial support for the study in fiscal years 2003 and 2004.

analyzing insider attacks across all critical infrastructure sectors where the insider's intent was to harm the organization, an individual, or the organization's data, information system, or network [Keeney 2005]. Two additional reports will be published in 2006: one specific to the IT and telecommunications sector, and one for the government sector.

The results of the *Insider Threat Study* show that to detect insider threats as early as possible, or to prevent them 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. The reports include statistical findings and implications regarding technical details of the incidents; detection and identification of the insiders; nature of harm; as well as insider planning, communication, behavior, and characteristics. The reports have been well received across several stakeholder domains, including the business community, government, technical experts, and security officers.

While the statistical information provided in those reports is immensely helpful to organizations, CERT next sought a method for conveying the "big picture" of the insider threat problem. We believe it is important that organizations understand the complex interactions, relative degree of risk, and unintended consequences of policies, practices, technology, insider psychological issues, and organizational culture over time.

In 2005, Carnegie Mellon CyLab funded the *MERIT* project—*Management and Education of the Risk of Insider Threat*.[14] The purpose of this CERT project was to create a descriptive model of insider IT sabotage and associated training assets based on the empirical data collected in the *Insider Threat Study*.

CERT researchers were not convinced that a single model could be developed to impart in sufficient detail the dynamic complexity of IT sabotage and other insider crimes like fraud and theft of confidential or proprietary information. Because a model of insider IT sabotage could be used for both the *MERIT* and PERSEREC projects, the CERT research team decided to focus *MERIT* on insider IT sabotage cases. As a result, a base model was developed for insider IT sabotage that can be used for both projects.

One unique aspect of the *Insider Threat Study* that was a key to its success was the equal attention it devoted to both the technical and psychological aspects of the problem. *MERIT* allowed the CERT team to realize unexpected benefits from the overlap with the PERSEREC project. CERT's technical security expertise was augmented with expertise from several organizations in the areas of psychology, insider threat, espionage, and cyber crime. Therefore, the system dynamics model for insider IT sabotage being developed for both *MERIT* and PERSEREC benefits from a broad range of experience regarding the technical, psychological, and organizational factors influencing insider threat risk.

[14] The CyLab *MERIT* project is supported by the Army Research Office through grant number DAAD19-02-1-0389 ("Perpetually Available and Secure Information Systems") to Carnegie Mellon University's CyLab.

# 2 Methodology

Our research uses system dynamics modeling to

- better understand and communicate common aspects of insider IT sabotage and espionage
- serve as a basis for policy and research recommendations
- facilitate identification of high-leverage countermeasures that would be effective in both domains

Our approach centered on a group modeling exercise combining the psychological and technical expertise of the various organizations involved to produce two models, one each for the insider IT sabotage and espionage domains.

## 2.1 MODELING TECHNIQUE

System dynamics is a method for modeling and analyzing the holistic behavior of complex problems as they evolve over time. System dynamics has been used to gain insight into some of the most challenging strategy questions facing businesses and government for several decades. The 2001 Franz Edelman Prize for excellence in management was given to a team at General Motors who used system dynamics to develop a successful strategy for launch of the OnStar System [Huber 2002].

System dynamics provides particularly useful insight into difficult management situations in which the best efforts to solve a problem actually make it worse. Examples of these apparently paradoxical effects include the following [Sterman 2000]:

- low-nicotine cigarettes, supposedly introduced to the benefit of smokers' health, that only result in people smoking more cigarettes and taking longer, deeper drags to meet their nicotine needs
- levees and dams constructed to control floods that only produce more severe flooding by preventing the natural dissipation of excess water in flood plains

The *Insider Threat Study* found that intuitive solutions to problems with employees often reduce the problem in the short term, but make it much worse in the long term. For example, employee termination might solve an immediate problem, but lead to long-term problems for the organization if the insider has the technical means to attack the system following termination. System dynamics is a valuable analysis tool for gaining insight into solutions that are effective over the long term and for demonstrating their benefits.

A powerful tenet of system dynamics is that the dynamic complexity of problematic behavior is captured by the underlying feedback structure of that behavior. So we decompose the causal structure of the problematic behavior into its feedback loops to understand which loop is strongest (i.e., which loop's influence on behavior dominates all others) at particular points through time. We can then thoroughly understand and communicate the nature of the problematic behavior and the benefits of alternative mitigations.

System dynamics model boundaries are drawn so that all the enterprise elements necessary to generate and understand problematic behavior are contained within them. This approach encourages the inclusion of soft (as well as hard) factors in the model, such as policy-related, procedural, administrative, or cultural factors. The exclusion of soft factors in other modeling techniques essentially treats their influence as negligible, which is often not the case. This endogenous viewpoint helps show the benefits of mitigations to the problematic behavior that are often overlooked, partly due to a narrow focus in resolving problems.

In this project we rely on system dynamics as a tool to help understand and communicate contributing factors to insider IT sabotage and espionage threats and implications for various mitigation strategies and tactics. It is tempting to try to use the simulation of the model to help predict the effect of mitigation strategies. But what is the nature of the types of predictions that system dynamics facilitates? Dennis Meadows offers a concise answer by categorizing outputs from models as follows [Meadows 1974]:

1. Absolute and precise predictions (Exactly when and where will the next cyber attack take place?)
2. Conditional precise predictions (If a cyber attack occurs, how much will it cost my organization?)
3. Conditional imprecise projections of dynamic behavior modes (If a bank mandates background checks for all new employees, will its damages from insider fraud be less than they would have been otherwise?)
4. Current trends that may influence future behavior (If the current trends in espionage continue, what effect will this have on national security in five years?)
5. Philosophical explorations of the consequences of a set of assumptions, without regard for the real-world accuracy or usefulness of those assumptions (If a foreign country succeeds in human cloning, how would this affect the United State's risk of espionage?)

The models we develop, and system dynamics models in general, provide information of the third sort. Meadows explains further that "this level of knowledge is less satisfactory than a perfect, precise prediction would be, but it is still a significant advance over the level of understanding permitted by current mental models."

## 2.2 MODELING PROCESS

As a basis for the modeling effort, we first determined the relevant cases for each of the domains. Although 49 insider IT sabotage cases were examined for the *Insider Threat Study*, not all of the case files contained enough information for this modeling effort. The *Insider Threat Study* focused on obtaining answers to hundreds of discrete questions regarding the psychological and technical aspects of the cases. On the other hand, the information needed for this modeling exercise was somewhat different, involving the dynamic nature of key variables. Such information was not readily available for all of the cases. Likewise, the PERSEREC insider threat case files had to be examined for the same criteria. In the end, 30 IT sabotage cases were selected for use in this project based on availability of pertinent information from both sources.

The selection process was somewhat different for the espionage cases. PERSEREC, as sponsor of the project and a center of expertise on espionage, selected nine espionage cases that involved use of IT resources and supplied the case information to the project team for use in the modeling effort.

Next, the team constructed separate databases to catalog relevant information for the cases. Case data drove the model scope and refinement. We gave preference to model variables that had strong links to observables in the data. The term *observables* in this report refers to specific events, conditions, or actions that could have been observed in the cases examined. This linkage ensures the ability to relate behaviors recognized as important for early detection with actions managers can take to better identify and understand an evolving insider threat. This approach helps to ensure that recommendations made as a result of the modeling effort are actionable.

At the outset, our intent was to develop two models—one for sabotage and one for espionage—and then compare them in a report. However, as the project progressed we realized that the high-level parallels between the models were so strong that it would be possible to create a third model to illustrate those parallels. Therefore, the abstracted common model was developed.

Figure 2 depicts the process used to develop the system dynamics models. The process used to refine the sabotage model is shown along the left side of the figure; that used to refine the espionage model is shown along the right side. The research recommendations flowing from the abstracted common model are shown along the bottom.

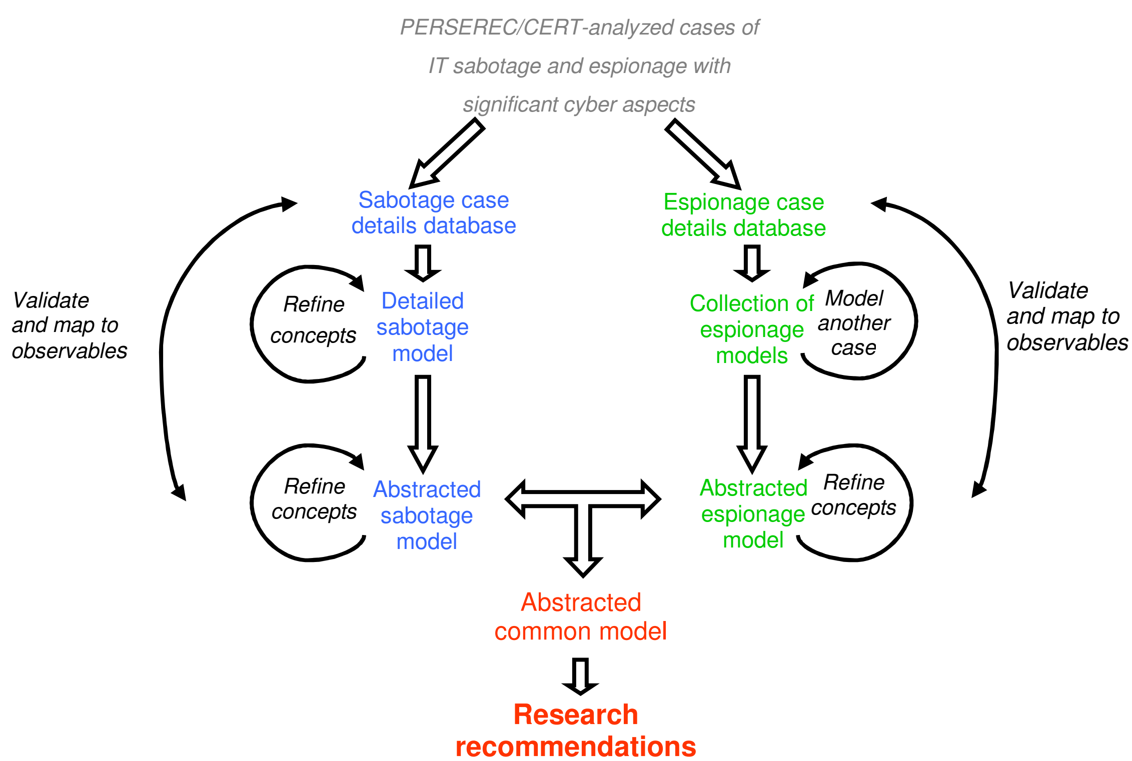


*Figure 2: Model-Based Analysis Approach*

We developed much of the initial sabotage model as part of the *MERIT* project. Consequently, the process used to refine the two models was somewhat different, due to the composition of the groups involved in the modeling effort. The group that developed the initial detailed sabotage model included CERT personnel with extensive knowledge of the IT sabotage cases from the *Insider Threat Study*. These team members had the same general understanding of the cases involved. A psychologist and experienced system dynamicist acted as facilitator for the group effort. Therefore, our initial modeling effort involved development of a very detailed model, then identification of the right abstractions or factors on which to base the model. We experimented with numerous formulations before identifying factors that coherently and simply conveyed the most important concepts from the sabotage cases we reviewed. The final product of this effort was an abstracted model that could be simulated. It was published in the proceedings of the International Conference of the System Dynamics Society [Cappelli 2006].

The espionage model development group was formed after much of the sabotage model was already developed. It included psychologists and other behavioral scientists, security personnel, and information technologists from PERSEREC, CERT, and other organizations. The meetings included four face-to-face group modeling meetings and two online meetings using an Internet-based virtual meeting application. The breadth of expertise was a welcome addition to the group modeling, but the participants had a range of familiarity with the system dynamics approach and the cases involved. This necessitated a different approach to the modeling effort: We decided to review and model several of the espionage cases individually. This approach allowed us to get a collective understanding of the modeling approach and the espionage cases of interest.

As explained earlier, while the team did not intend to build an abstracted common model at the outset of the project, it became evident after the sabotage and espionage models were completed that such a model could be created, and might be a useful mechanism for describing the similarities between the two models. Further, the team found that the differences between the models lay in the detailed observables related to the models, rather than in the structure of the models. Therefore, the abstracted common model could also be used as a basis for describing the differences found between insider IT sabotage and espionage.

Developing the abstracted sabotage and espionage models involved iterative refinement of the basic concepts by the group. The group's broader expertise allowed it to add the necessary behavioral and psychological constructs to the previously developed sabotage model. The group documented its collective understanding of the espionage cases in the form of an abstracted espionage model. During their formulation, the project team traced both the IT sabotage and espionage models back to the details of the actual cases to make sure they were representative of those cases.

Once the domain models stabilized, we extracted variables and feedback loops that constituted similar characteristics and behavior patterns in the two domains. These similarities formed the basis for the abstracted common model. At times, we had to abstract to a higher level than seen in either of the domains individually. To verify relevance, we traced all of the derived variables and feedback loops from the abstracted common model back to the individual models. Appendices A, B, and C depict the abstracted common model, the insider IT sabotage model, and the espionage model, respectively.

At times during the formulation of the models, the group had to make inferences regarding the underlying causes of observed behaviors in the cases, because of the lack of relevant data. We also postulated mechanisms to mitigate problematic behaviors, which were integrated into the model as balancing feedback loops. Based on the feedback loops and relationships of the abstracted common model, the research recommendations described in this paper suggest the collection of additional evidence of the validity of the model hypotheses.

## 2.3 MODELING NOTATION

In the portions of the system dynamics model presented in Section 3 (Figures 3 through 8), arrows represent the system interactions. These arrows are coded with an alphabetical label indicating the pair-wise influence of the variable at the source of the arrow on the variable at the target of the arrow:

- Roughly, an arrow labeled with an S indicates that the value of the source and target variables move in the same direction.[15]
- Roughly, an arrow labeled with an O indicates that the value of the source and target variables move in the opposite direction.[16]

As mentioned, dynamically complex problems can often be best understood in terms of the feedback loops underlying those problems. There are two types of feedback loops, balancing and reinforcing:

- Balancing loops (labeled *B#* in the figures) describe aspects of the system that oppose change, seeking to drive organizational variables to some goal state. In other words, balancing loops tend to move the system to a state of equilibrium even in the face of change. The behavior of a thermostat is an example of a balancing loop: it continually changes the air flow into a room based on the temperature of the room, with the goal of maintaining a consistent temperature.
- Reinforcing loops (labeled *R#* in the figures) describe system aspects that tend to drive variable values consistently upward or consistently downward. In other words, reinforcing loops can "spiral out of control." A flu epidemic is an example of a reinforcing loop: it spirals out of control as more and more people contract the flu.

The type of a feedback loop is determined by counting the number of *O*-influences along the path of the loop; an odd number of *O*'s indicates a balancing loop and an even (or zero) number of *O*'s indicates a reinforcing loop.

[15] More formally, an S-influence indicates that if the value of the source variable increases, then the value of the target variable increases above what it would otherwise have been, all other things being equal. And, if the value of the source variable decreases, then the value of the target variable decreases below what it would otherwise have been, all other things being equal.

[16] More formally, an O-influence indicates that if the value of the source variable increases, then the value of the target variable decreases below what it would otherwise have been, all other things being equal. And, if the value of the source variable decreases, then the value of the target variable increases above what it would otherwise have been, all other things being equal.

System dynamics models are described as a sequence of feedback loops that characterize how the problem unfolds over time. Each feedback loop describes a single aspect of the problem. Multiple feedback loops interact to capture the complexities of the problem domain.

# 3 Observations

Initially, some project participants felt it would be nearly impossible to develop one model representing most insider IT sabotage cases, and another representing most IT-related espionage cases. As the process evolved, however, the team discovered it was indeed quite possible to create such models. While each aspect of the models does not apply to every case, each has been validated to represent a significant percentage of the cases.[17]

The team also discovered that, in addition to its analytical usefulness, system dynamics modeling helps scientists from different disciplines (including psychologists, political scientists, historians, security specialists, and information security experts) communicate, collaborate, and view a problem with a new perspective. For example, by working together, the psychologists and technical experts on the team realized that some of the psychological and technical aspects of the problem could be modeled as one concept. These aspects include

- the prevalence of both behavioral and technical rule violations prior to attacks
- the important consequences of whether the rule violations were detected
- when they were detected, the critical nature of the manner in which they were handled by management
- the impact of auditing and monitoring, both technical and non-technical, on discovery and handling of behavioral and technical indicators

After the individual models were developed for sabotage and espionage, the team analyzed the two to determine if there were any parallels. It is important to point out that the models were deliberately developed as independent entities; the team consciously did not attempt to compare the two during the modeling process. Consequently, we are confident that no aspect of either model was overlooked due to the fact that it was not significant in *both* domains.

The results of our efforts surprised the team. Not only were there strong parallels between the models, but it was possible to create another model, the abstracted common model, which has the common elements of both. The abstracted common model successfully represents the issues surrounding saboteurs and spies in a single model. This does not imply that the team felt insider IT sabotage and espionage were identical phenomena carried out by similar types of people. There were significant differences in the observable variables within these theoretical concepts. Appendices D and G contain detailed lists of observables for many aspects of the models; we recommend that the reader reference these appendices frequently for a full understanding of the models and observations.

Analysis of the abstracted common model identified six issues the team feels should be explored further:

- *Observation #1:* Most saboteurs and spies had common personal predispositions that contributed to their risk of committing malicious acts.

[17] See Appendices E and Appendix F.

- *Observation #2*: In most cases, stressful events, including organizational sanctions, contributed to the likelihood of insider IT sabotage and espionage.
- *Observation #3:* Concerning behaviors were often observable before and during insider IT sabotage and espionage.
- *Observation #4:* Technical actions by many insiders could have alerted the organization to planned or ongoing malicious acts.
- *Observation #5:* In many cases, organizations ignored or failed to detect rule violations.
- *Observation #6:* Lack of physical and electronic access controls facilitated both insider IT sabotage and espionage.

This section of the report describes each of these observations based on overall trends and patterns observed in analysis of the cases. Each observation starts with a description of the common aspects of insider IT sabotage and espionage relevant to the observation. This description includes the applicable portion of the abstracted common model. Next, case examples from both espionage and IT sabotage clarify the stated observation. Finally, an analysis of the similarities and differences between insider IT sabotage and espionage draws from the team's collective experience and understanding of the domain. Specific statistics are not provided; rather, the observations are based on overall trends and patterns observed in analysis of the cases.

The combination of all model portions presented throughout the report comprises the whole of the abstracted common model (see Appendix A). Table 1 (also in Appendix A) enumerates the primary feedback loops of the model that form the basis for many of the observations. The loops described in Table 1 occur in all three of the models: abstracted common model, insider IT sabotage model, and espionage model.

The abstracted common model was validated against the case data. Appendix E contains a spreadsheet summarizing each insider IT sabotage case, noting whether it supports each observation. Case names have not been included to protect insider and organization confidentiality and cases are identified only by a sequential case number. Appendix F contains a similar spreadsheet mapping the espionage cases to the observations.

## 3.1 OBSERVATION #1

*Most saboteurs and spies had common personal predispositions that contributed to their risk of committing malicious acts.*

Most saboteurs and spies exhibited predispositions that produced personal and interpersonal needs that contributed directly to maladaptive workplace behaviors. These needs made them prone to undertake malicious acts or to betray trust or commitments. Personal predispositions refer to characteristics of the individual that can contribute to the risk of behaviors leading to espionage and sabotage, as well as to the form of these actions, their continuation, and escalation.

With regard to saboteurs, staff psychologists coded the presence or absence of these characteristics in case files containing taped insider interviews; notes from interviews with victim organizations, prosecutors, investigators, or insiders; direct observer reports; and personal and legal records. To be included, the insider had to display observables related to these characteristics prior to the incident under review. Appendix G describes the criteria for personal predispositions. In practice, personal predispositions have been related directly to maladaptive reactions to stress, financial and personal needs leading to personal conflicts and rule violations, chronic disgruntlement, strong reactions to organizational sanctions, concealment of rule violations, and a propensity for escalation during work-related conflicts.

The term “needs” denotes the manifestation of the personal predisposition in the workplace as it impacted the risk of sabotage or espionage. Examples include the following:

- One of several personal predispositions resulting in debt (alcoholism, impulse control problems, maladaptive personality attributes) could result in a *need* for money beyond expected income. This personal need for money can, in turn, create vulnerability for espionage.
- Anger—manifesting as a *need* for attention, revenge, or self-esteem reinforcement—resulting from a personal predisposition (such as sensitivity to criticism, poor social skills, a sense of entitlement) could increase the likelihood of conflict in the workplace, sanctions, and disgruntlement. The resulting situation can, in turn, create vulnerability to insider IT sabotage or espionage.
- An exaggerated need for ego satisfaction or to control others can overcome constraints against rule breaking with the same result.

Personal, versus interpersonal needs were defined as needs arising from an individual’s psychology that might not involve direct, observable interactions with others in the workplace. For example, an individual’s anxiety disorder (see “Serious Mental Health Disorders” in Appendix G) may produce workplace behaviors contributing to risk of insider threat or espionage independent of observable interactions with others of concern. One spy’s anxiety regarding public speaking was so extreme that it reportedly contributed to his decision to flee the workplace with classified information (see reference to Michael Peri in “Espionage” on page 16. However, his peers and supervisors were not aware of the extremity of his fears or discontent. Interpersonal needs were defined as arising as a result of, or in the context of, observable interactions with others. For example, ongoing conflict with a supervisor created a need for attention, revenge, or correction of a perceived injustice in several spies and saboteurs in our sample.

The observed personal predispositions were grouped into four categories, including

- Serious Mental Health Disorders
- Personality Problems
- Social Skills and Decision-making Biases
- A History of Rule Conflicts

Detailed definitions of these categories, their observables, and distribution among sabotage and espionage insiders are contained in Appendix G.

Personal predispositions appeared to play a role in both sabotage and espionage risk. Although data was only available for 60% of the IT sabotage cases in this study, all of the saboteurs for which data was available exhibited the influence of personal predispositions as depicted in Figure 3: Model Relationships Relevant to Observation #1, as well as all of the spies. As Figure 3 indicates, these predispositions created personal needs which, in turn, resulted in harmful actions (*B1*). Often, there were multiple harmful actions, including precursor activities to set up a sabotage attack (for example, creation of backdoor accounts or planting a logic bomb) and ongoing activities within an espionage case to set up, execute, conceal, and repeat the actions over time. As the figure also indicates, the impact of the expression of these needs in the form of the harmful actions often, albeit temporarily, fulfilled and reduced the personal need.

However, both sabotage and espionage insiders showed a predisposition to escalate conflicts and repeat rule violations, so this relief was often short lived. The seriousness of these personal needs also appeared to make their resurgence and additional harmful acts likely (R1), depending on the detection and management capabilities of the organization involved. Our observations of actual cases suggest that there are two factors that would escalate initial harmful or concerning behaviors to the point of committing serious damage: (1) sanctions directed at the offender intensify the need for revenge or getting even, or (2) perception of benefit or rewards, without sanctions or detection of rule violations, diminish anxieties about consequences and intensify the desire to commit even graver rule violations. The impacts of sanctions are discussed in detail in Observation #2.

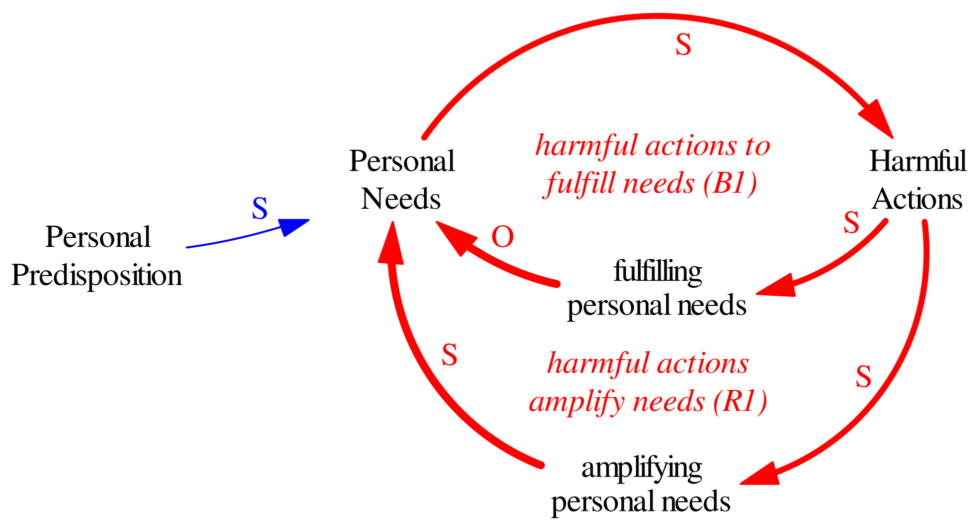


*Figure 3: Model Relationships Relevant to Observation #1*

## 3.1.1 Case Examples

### 3.1.1.1 Sabotage

A database administrator working for a U.S. government agency had a good reputation initially; she received letters of commendation for her work and was chosen for an executive training program. A few years later, however, she was diagnosed with a depressive disorder that included symptoms of insomnia, spontaneous periods of loss of emotional control (e.g., spontaneous crying), and difficulty in making decisions. She was placed on medication for this illness, which she was still taking at the time of the incident.

After being diagnosed, her performance went steadily downhill. She began to have conflicts with her male coworkers, as they were overriding her technical decisions and calling contractors for whom she was responsible without her knowledge. These conflicts escalated over several weeks leading her to file a complaint with her human resources department. However, no action was taken. Her performance continued to decline and tensions in the office grew, leading to a demotion by her supervisor.

Finally, the insider filed a complaint with the Equal Employment Opportunity (EEO) Commission for discrimination based on her national origin (India), race (Asian, Indian), and gender (female). In the meantime, the insider left the organization and took employment elsewhere. Eventually, her grievance was denied. On hearing of this decision, the insider accessed her former employer's database remotely and deleted critical system data. As a result of backup problems the organization was experiencing at the same time, it took 115 employees 1800 hours to restore the data.

This insider's serious mental health disorder was clearly a personal predisposition that resulted in a personal need for revenge.

#### 3.1.1.2 Espionage

Michael Peri, an electronic warfare signals specialist for the Army, fled to East Germany with a laptop computer and military secrets, then voluntarily returned less than two weeks later to plead guilty to espionage. Peri said he made an impulsive mistake, that he felt overworked and unappreciated in his job. His anxiety regarding public speaking was so extreme that it reportedly contributed to his decision to flee the workplace with classified information. This theft occurred the day before he was scheduled to make a presentation for the "Soldier of the Month" award. Rather than perceiving it as a reward, Peri suffered extreme anxiety in the face of the presentation. However, his peers and supervisors were not aware of the extremity of his fears.

In addition, Peri felt overworked and unappreciated, claiming that he had been working 100-hour weeks. However, he was unable to communicate his concerns regarding overwork due to his social anxiety. Because of his heavy workload, he was unable to accompany his unit on a survival training trip to Spain. He reportedly felt personally victimized by not being allowed to go on this trip. Together, his feelings of unjust exploitation, victimization and fear regarding the presentation, along with his inability to express his concerns, led to the decision to commit espionage. This example clearly illustrates how a spy's personal predisposition, in this case personality, social skills and decision-making problems, led to personal needs that resulted in harmful actions as depicted in Figure 3.

#### 3.1.1.3 Further Comparison of Espionage and Sabotage

In the sabotage cases, the interpersonal needs observed were frequently associated with disgruntlement and supervisor conflict. These needs derived from a combination of personal predispositions. Frequently, these were personality problems that also affected social skills and decision making. As the case database indicates, these saboteurs also had a significant history of rule violations, so that their pathway to harmful acts was previously established. Mental health problems were not prevalent for sabotage.

The interactions between personal predispositions and needs were somewhat more complex in the espionage cases. Personality issues and mental health problems also generated serious personal needs, which drove espionage activities. In addition to disgruntlement, as noted for the sabotage cases, personal predispositions often led to financial need in espionage cases. For example, Robert Hanssen, former FBI agent who spied for Russia for over 15 years, counted on his espionage activity to relieve his significant, ongoing personal debts. In addition, the payment he received for his espionage activities increased his spending beyond his immediate family needs and well beyond his means, creating an ongoing need for more funds, thereby escalating his espionage activity. In this regard, if the espionage was not detected or appropriately managed, its impact on the personal predisposition frequently reinforced (amplified) rather than reduced (fulfilled) the personal need, as shown by the O and S influences in the figure.

Another difference observed between sabotage and espionage cases involves the influence of external people or organizations. In sabotage cases, the insiders were rarely influenced by outsiders to commit their malicious acts. In some espionage cases, however, financial and personal relationships with outside agents and organizations heavily influenced the spy and contributed to a continuation of the harmful behaviors. For example, Hanssen’s correspondence with his Soviet handlers indicates the existence of a personal relationship and investment, as well as material assistance. There was only one example in the sabotage cases of such active involvement and assistance by outsiders. However, while these cases are rare, they may be under-represented in our sample of sabotage cases.

## 3.2 OBSERVATION #2

*In most cases, stressful events, including organizational sanctions, contributed to the likelihood of insider IT sabotage and espionage.*

Insider attacks are typically preceded by high rates of stressful events including work-related and personal events [Keeney 2005, Randazzo 2004, Shaw 2005b]. Stressful events are those events that cause concerning behaviors in individuals predisposed to malicious acts. Particularly noteworthy in the previous studies was the high incidence of work-related conflicts and sanctions prior to attacks (see Figure 4). The researchers found personal predispositions affected how an insider experienced and reacted to stress in multiple ways. For example, what insiders perceived as stressful, how they contributed to the occurrence of stress, and how they reacted to stress were viewed as influenced directly by personal predispositions.

Personal predispositions were noted to produce maladaptive behaviors, tensions, and often, conflict in the workplace (see “Behavioral and Technical Indicators or Violations [Actual]” in Figure 4). These behavioral indicators may produce stress in their own right. For example, personal predispositions often contribute to interpersonal conflicts which, in turn, create a sense of unfair victimization and a desire for revenge [Dupre 2006]. Personal predispositions can also contribute to a propensity for behavioral and technical rule violations that can also create interpersonal conflicts with coworkers and supervisors, generating further stress for the insider. These loops, including maladaptive behaviors, conflicts, and stress often take place independent of official notice and sanctions. However, Figure 4 illustrates the added impact of sanctions on personal needs through the stress these consequences produce for the insider.

With the addition of stressful events, the impact of personal predispositions as depicted in Figures 3 and 4 now becomes somewhat more complex. As noted, personal predispositions can result in harmful actions that can reduce personal needs (albeit temporarily), actually relieving the tension these needs produce in the workplace and in the mind of the potential offender. Or, these personal predispositions can increase personal needs by reinforcing these strivings, creating a need for even greater fulfillment in the absence of negative consequences as the offender continues to exhibit adverse behaviors. In addition, as shown in Figure 4, personal predispositions can lead to stress in the form of conflict, which further increases personal needs. Finally, should these conflicts be detected and result in sanctions, the insider may experience even greater aggravation of personal needs through the stress caused by these sanctions.

These pathways are consistent with observed patterns across both sabotage and espionage cases. For example, the finding that concerning behaviors were present prior to the employee attacks in all of the PERSEREC cases [Shaw 2005b, Shaw 2005a] and 80% of the *Insider Threat Study* IT sabotage cases [Keeney 2005, Randazzo 2004] is consistent with the manifestation of personal needs resulting in workplace conflict.

The finding noted by Shaw of significant delays in management discovery of insider disgruntlement also supports the potential for personal predispositions to cause stress and exacerbate insider needs independent of official sanctions [Shaw 2005b]. However, it was also clear that escalating conflict between insiders and management, including sanctions, was a major precipitant of insider attacks. One of the most consistent stressful events resulting from conflict that preceded attacks was termination of employment. All of the employees in the PERSEREC cases and the majority of insiders in the *Insider Threat Study* cases attacked after termination or suspension from duties.

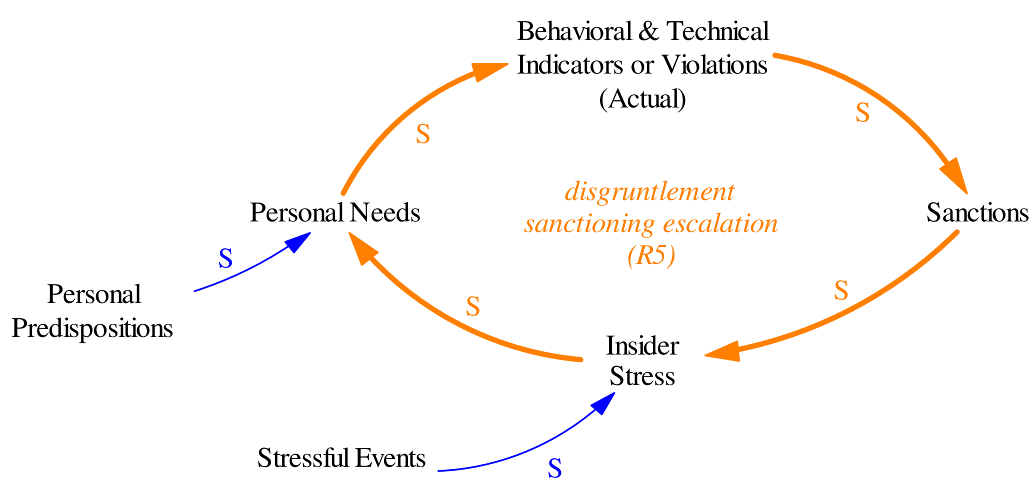


*Figure 4: Model Relationships Relevant to* Observation #2

### 3.2.1 Case Examples

#### 3.2.1.1 Sabotage

The case of the 20-year-old webmaster/systems administrator at a government facility demonstrates the synergistic effects of personal predispositions and stressful events on attack risk. Observables related to this saboteur's personal predispositions included

- deception on his security screening questionnaire (personality and decision-making problems)
- an arrest record related to drug abuse (serious mental health issues and rule violations)
- termination for misconduct at a previous employer (history of rule violations)
- non-disclosure or denial about drug use on the job (serious mental health issues, personality and decision-making problems, rule violations)

On-the-job observables related to personal predispositions included

- inappropriate racial and sexual comments
- late arrival at work
- early departure from work
- absence from the office area for extended periods
- failure to respond to system problems and customer requests
- sanctions for technical security violations prior to his attack

He also reportedly had frequent personal conflicts with his supervisor and other staff. These behavioral indicators were not formally addressed by his supervisor until a month after their occurrence.

Examples of stress related to sanctions included his behavior in a meeting with his supervisor regarding his history of behavioral and technical problems. The saboteur reportedly became hostile and was referred to the project manager, who advised the saboteur that any further behavioral problems or performance difficulties would result in dismissal. Illustrating the way personal predispositions can influence an insider's reaction to the stress of sanctions, he subsequently reported late for work seven times and had other personal conflicts. As a result, management decided to escalate its sanctions by limiting his work to a single, isolated server and curtailing his remote access to the system. Shortly after these sanctions, the saboteur had another dispute with a coworker and his immediate supervisor drafted a letter of dismissal and sent it to the project manager. He did not print the letter, give it to the saboteur, or advise him of its existence. However, the saboteur hacked into his supervisor's computer, discovered the letter, and decided to take action. He planted a logic bomb on the network and programmed it to go off in two different ways. At the same time, he framed his supervisor for the action and implemented a taunting electronic message to his supervisor when he logged into the system.

In an illustration of the idiosyncratic effects of personal predispositions on reactions to stress, the saboteur's project manager believes that his attack on the system was designed to intimidate staff into not firing him in exchange for disabling the logic bombs or into hiring him back to repair the damage—a move similar to one he reportedly attempted with a previous employer. The project manager believes that the insider's threatening message was an overt threat to prevent his termination. If he had wanted to destroy the system, he argues, he could have taken it down that evening or arranged for his time bomb to go off earlier. He believes that the saboteur underestimated the staff's ability to discover and disable the logic bomb and cites a number of clues about its implementation that the saboteur failed to erase. This case is a good example of the effect of interpersonal conflict, technical security violations, and, subsequently, sanctions on escalating risk.

#### 3.2.1.2 Espionage

Brian Patrick Regan, a former Air Force intelligence analyst turned defense contractor, faced retirement with $116,000 in consumer debt, four children, and severe resentment. Regan was arrested on August 23, 2001 at Dulles International Airport, on his way to Zurich with coded coordinates of missile sites in Iraq and China he had gleaned through authorized, but unneeded, access to a classified database. He reportedly complained frequently to coworkers and neighbors about his job, lack of recognition and status, and poor quality of life. In his pitch to sell classified documents to Iraq, China, and Libya, he also noted that he deserved more than his meager pension after so many years of service and protested the wages of movie stars and athletes who make so much money for much less contribution. His financial and personal stress was also reportedly aggravated by college tuition payments and family alcohol problems.

Regan's case is also interesting from the standpoint of personal predispositions as he reportedly had an active fantasy life about spying and told the judge in his case that he had been taking anti-depressant and anti-psychotic psychiatric medications. Coworkers and neighbors also described him as withdrawn and unsociable yet much more intelligent than the weight-lifting, lumbering persona he projected.

#### 3.2.1.3 Further Comparison of Espionage and Sabotage

The *Insider Threat Study* found that 92% of all insider saboteurs attacked following a negative event. All of the employees in the PERSEREC cases experienced work or personal stressful events prior to their attacks. These findings lend strong support to the role stressful events play in insider betrayal.

All but one of the sabotage cases in this study experienced significant stress prior to their attack. Among our limited espionage cases, stress affected six of nine insiders. These stressors were, specifically

- interpersonal conflicts or confrontations
- a sense of victimization
- mounting debt
- demotion or undesirable job transfer

According to our best available public data, only Montes, Aragoncillo, and Hoffman,[18] among espionage subjects, were not affected by stressful events in their decision to commit espionage. Based on available data it also appears that stressful events played a larger role in the risk of sabotage than espionage, since sabotage is more frequently associated with disgruntlement than is espionage. While it is difficult to explain this relative imbalance in the apparent contribution of stressful events to sabotage versus espionage using available data, these three spies differed from

[18] See Appendix H for case summaries.

other spies in a significant manner: Their ongoing relationships with, and the influence of, the foreign entities to whom they delivered stolen information may have been greater than their peers. For example, Aragoncillo may have been influenced by the former President of the Phillipines, Montes may have been effectively managed by her Cuban case officers, and Hoffman may have been inspired to sell secret proprietary information to foreign sources by lucrative financial incentives. Further research is required to ascertain the relative influence of outside organizations, personal predispositions, and stressful events on different types of insiders. While the PERSEREC data set includes a clear case of a saboteur motivated and aided directly by an outside group, the greater likelihood of such an influential outside presence may differentiate espionage from sabotage in general.

## 3.3 OBSERVATION #3

*Concerning behaviors were often observable before and during insider IT sabotage and espionage.*

As noted in Observation #2, stressful events were observable in the personal and work life of both saboteurs and spies prior to their attacks. In many cases, a series of stressful events later resulted in official intervention and sanctions against the employee, introducing additional stress. While stressful events include work-related conflicts and sanctions, there were also cases when significant stress and conflict emerged prior to official notice and sanctions. There is clearly a relationship between stressful events (Observation #2) and concerning behaviors (Observation #3), in that concerning behavior often follows stressful events. However, the presence of these concerning behaviors—often violations of the organization's personnel policies—was deemed of sufficient importance to merit a separate observation. In fact, one of the most important findings of this research has been the discovery that concerning behaviors, including personnel and security violations, were present in the vast majority of insider cases prior to their attacks. The presence of both stressful events and concerning behaviors also represents the escalating spiral of events that leads to many insider attacks. These observations are extremely important for the prevention and management of insider risk because they indicate the existence of a window of opportunity during which effective employer detection and intervention can reduce the risk of an attack.

According to Keeney, 80% of the IT saboteurs studied in the *Insider Threat Study* had drawn attention by displaying concerning behaviors prior to the act of sabotage [Keeney 2005]. These behaviors included

- tardiness, truancy
- arguments with coworkers
- poor job performance
- security violations
- attack preparations

Among the cases in which these behaviors were observed, 97% of the insider behavior came to the attention of supervisors, coworkers, or subordinates in the workplace. In addition, 31% of the insiders had prior histories of disciplinary action within their organizations. In 31%, of the cases, others had information about the insider's plans, intentions, and/or activities related to a planned attack. In this regard, 58% of insiders communicated negative feelings, grievances, and/or interest in causing harm to others and, in 20% of cases, the insider made a direct threat to harm the organization or an individual prior to attack.

All the PERSEREC insider threat cases studied include a significant number of personal stressors and personnel problems requiring company intervention prior to insider attacks. In nine cases of disgruntled insider behavior studied by Shaw, signs of disgruntlement appeared from 1 to 48 months before the attack [Shaw 2005b]. The period prior to the attack—during which there were active problems requiring company intervention—ranged from 12 days to 19 months. Similarly, in 6 of the cases examined, there were signs of significant problems meriting official attention prior to or during their activities.

Figure 5 depicts that part of the model that shows personal needs influencing the concerning behaviors, which are indicators of harmful actions to come. As discussed in Observation #1 personal needs include the need to act out disgruntlement, to satisfy ego, and to address personal insecurity. In summary, 90% of the insiders in the IT sabotage cases analyzed exhibited concerning behaviors prior to their attack, as did every one of the spies in the espionage cases included in the present study.

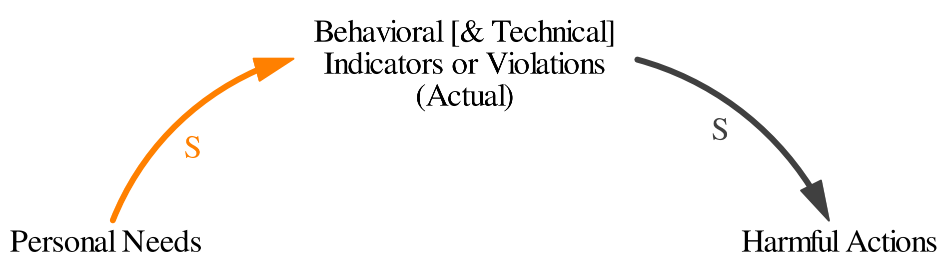


*Figure 5: Model Relationships Relevant to Observation #3*

### 3.3.1 Case Examples

#### 3.3.1.1 Sabotage

One case provides a good example of the presence of concerning behaviors prior to an insider attack. This saboteur was hired by a manufacturer as a network engineer on the basis of his networking certification and background checks by a reputable headhunter. Four months after he was hired, the saboteur was promoted to a management position after his supervisor quit. However, coworkers and supervisors became suspicious of the insider's actual technical ability and concerned about some of his behaviors. But these coworkers reported being afraid to complain to the insider's supervisor about him due to a recent spate of firings.

Following up on their suspicions, company personnel discovered that the saboteur had, and used, two Social Security numbers and seemed unable to obtain a passport to facilitate necessary foreign travel. The insider also installed a "webcam" in the computer room in order to observe his staff when he was not at work. He called and taunted the staff from home and referred to himself as the "President" and "King." The saboteur also missed a great deal of work when his supervisor was out of the office and bragged about performing side jobs for major corporations. Finally, the saboteur's supervisor attempted to verify his networking certification and learned that it was false. The saboteur was terminated and a security consulting firm was called in to assure that his access was revoked.

Security staff monitoring the company's network the day of the termination noticed the saboteur attempting to access the system and called him, ordering him to stop. The saboteur denied the activity. Coworkers also reported that, during the week after his termination, the saboteur had bragged about putting backdoors into the system and planning to use them to cause damage. Also during that period, the saboteur logged into the system using VPN accounts he had apparently created prior to termination for his supervisor, the CFO, and VP of Sales without their knowledge. Two weeks after his termination, the saboteur accessed one of the company's servers remotely using these VPN accounts and deleted crucial files. The security consulting firm had overlooked this server and the saboteur was the only company employee to ever have accessed it.

This case provides a good example of the presence of concerning behaviors as risk indicators before hiring, during employment, and even after termination. If at any point these concerning behaviors had been detected and acted on, the insider attack might have been prevented or managed differently.

#### 3.3.1.2 Espionage

Among those in our espionage sample, Aldrich Ames exhibited similar concerning behaviors prior to and during his espionage activity. Throughout his career at the CIA, Ames's alcoholism resulted in interpersonal problems, affected his job performance, and produced legal and security violations. According to Ames, his drinking problem and financial stress from debt contributed directly to his espionage. Ames reportedly was asked about an episode of drinking and joyriding in a stolen car during a polygraph exam when the Agency was considering hiring him. Ames was later arrested for alcohol-related reckless driving and speeding during his early years at the CIA. Alcoholism also reportedly contributed to his loss of classified information on a New York subway. Although Ames himself later reflected that the incident made him consider leaving the CIA, it appears that he received only a verbal reprimand. Several years later, in October 1980, Ames was cited for leaving TOP SECRET communications equipment unsecured in his office; but this, too, did not result in an official reprimand.

In an interview during a congressional investigation of his activities, Ames noted that he had a reputation for "regularly going out with a group of people, taking long lunches, and having too much to drink." He recalled one particular episode at a diplomatic reception at the American Embassy in Mexico City, where he had had too much to drink and became involved in a loud and boisterous argument with a Cuban official. On another occasion, Ames was involved in a traffic accident in Mexico City and was so drunk he could not answer police questions or recognize the U.S. Embassy officer sent to help him. According to Ames, the episode with the Cuban official "caused alarm" among his superiors. He was counseled by one superior, and another supervisor sent a message to CIA headquarters recommending that Ames undergo an assessment for alcohol abuse when he returned to the United States. On Ames's return from Mexico, he had one counseling session, but there was no follow-up program of treatment. Ames was administered blood tests, which proved normal, and he denied to the counselor that he had a drinking problem. The Inspector General's report indicates that the medical office was not aware of, and did not request, additional information about Ames's drinking habits, either from the Office of Security or the Directorate of Operations, prior to the counseling session.

Furthermore, although Ames's supervisor in Mexico City had recommended to CIA headquarters that Ames be counseled for his drinking problem, this was not made known at the time to his prospective supervisors in the South East Asia (SE) Division. In the summer of 1984 or 1985, after consuming several alcoholic drinks at a meeting with his Soviet contact, Ames continued to drink at a CIA-FBI softball game until he became seriously inebriated. Ames had to be driven home that night and left behind at the field his badge, cryptic notes, a wallet which included alias identification documents, and his jacket. Some recall that senior SE Division managers were either present or later made aware of this incident, but the record does not reflect that any action was taken.

Ames was involved in another breach of security in the fall of 1984, this time involving his fiancé Rosario. Ames had been temporarily detailed to work in New York. It had been arranged that Ames and two other officers would travel to New York and stay at Agency-provided housing. Ames showed up with Rosario. One of the other officers complained to a local CIA officer that Rosario's presence in the Agency housing compromised the cover of the other case officers as well as their activities. A second CIA officer confronted Ames and reported the matter to senior CIA management in New York. Ames says he complied with a management instruction to move to a hotel room. There is no record that any disciplinary action was taken against Ames in this matter, but both Ames and a Headquarters officer recall that Ames was told he had exercised bad judgment when he returned to Washington.

In the financial realm, the Inspector General report indicates that Ames believed his divorce settlement threatened to bankrupt him. At the same time, Ames acknowledged that his debt had grown since Rosario came to live with him in December 1983. He faced a new car loan, a signature loan, and mounting credit card payments. He later told congressional investigators that these financial difficulties led him to first contemplate espionage between December 1984 and February 1985. Following a long history of rule violations and stressful events in his personal and professional life, Ames finally sold out to adversarial interests, causing immeasurable damage to national security and the loss of life to U.S. intelligence sources.

#### 3.3.1.3 Further Comparison of Sabotage and Espionage

Concerning behaviors were present in all but three sabotage cases and all of the espionage cases in this study. As the examples above illustrate, concerning behaviors constitute a significant indicator of sabotage and espionage risk in both these groups.

## 3.4 OBSERVATION #4

*Technical actions by many insiders could have alerted the organization to planned or ongoing malicious acts.*

Figure 6 illustrates what can happen when organizations fail to recognize and act upon technical indicators exhibited by insiders prior to an act of sabotage or espionage, or while espionage is underway.

A technical indicator is a technical event, condition, or action that indicates increased risk. For instance, saboteurs sometimes created backdoor accounts—unauthorized accounts unknown to anyone except the person who created them—to facilitate system access following termination. In espionage cases, spies frequently exploited technical access to classified information to carry out their espionage. In both examples, these technical actions, if detected early, could have alerted the organization to the malicious activity in time to limit the damage. However, undetected, the technical indicators led to harmful actions in the cases examined.

Harmful actions are different in espionage and insider IT sabotage cases. In espionage cases, they involved information theft, such as printing documents or copying information to disks. These acts often continued repeatedly when not detected.

Although a few insider IT sabotage cases involved multiple attacks by the same insider, most acts of sabotage occurred only once. However, there were technical actions taken in the sabotage cases to set up the attack, which enabled the insiders to carry out their eventual sabotage when they went undetected. For example, logic bombs were constructed, tested, and planted on the system, and backdoor accounts were created that were used later for unauthorized access in order to commit the sabotage. These technical actions are referred to as “Harmful Actions” in the model.

The pivotal factor in Observation #4 is the “trust trap.” The trust trap is a reinforcing loop, meaning that the trust exhibited by an organization toward individuals tends to escalate over time, giving them a false sense of security because they let down their guard and thus discover fewer and fewer harmful actions, including technical indicators. As an organization’s perceived risk (of an act of IT sabotage or espionage) decreases, its trust of individuals in the organization tends to increase. As an organization trusts these individuals more, it tends to devote fewer resources to auditing and monitoring. As the level of auditing and monitoring decreases, the organization tends to discover fewer and fewer harmful actions. As an organization discovers fewer harmful actions, it tends to perceive less risk. Because the organization discovers fewer harmful actions, it may develop a false sense of security. The cycle continues, with the organization’s detection capability steadily deteriorating until a major compromise becomes obvious to all involved.

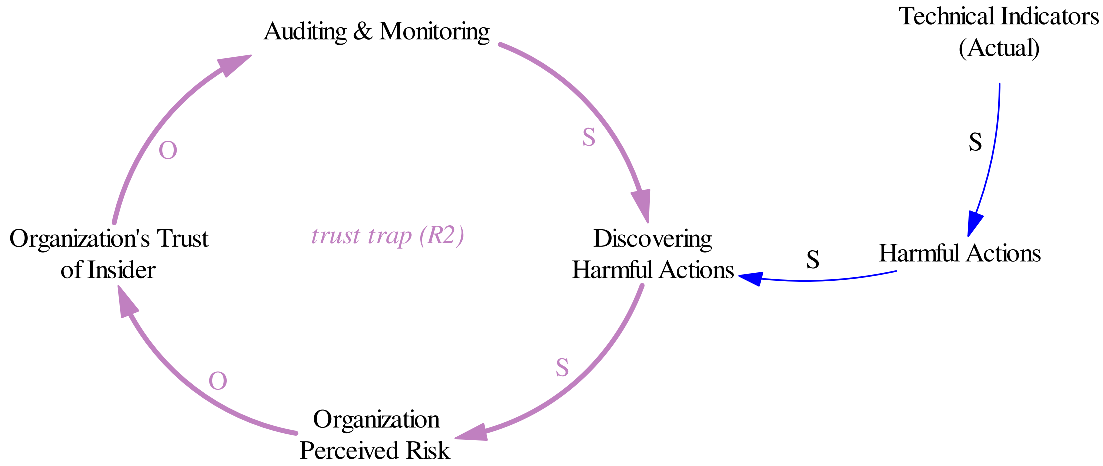


*Figure 6: Model Relationships Relevant to Observation #4*

In 27 of 28 IT sabotage cases in this study, there were undiscovered technical indicators of an impending attack due to inadequate monitoring and/or auditing (insufficient information was available for two of the cases). In every espionage case (insufficient information was available for one case) there was evidence of inappropriate access to classified information available prior to and during espionage activity that could have been discovered by auditing the spy's access.

The primary difference between the sabotage and espionage cases was the specific observable access path taken by the insider. In the espionage cases, the spy tended to use known, legitimate means to access the information to commit the crime, for example, physical access to a secure facility or electronic access to a system. The saboteurs tended to use access paths unknown to management, either because they forgot that they existed or because the saboteur created new, illegitimate access paths in preparation for the attack. For example, some saboteurs used inactive accounts that were overlooked in the termination process, while others created unauthorized backdoor accounts for use after termination. In both cases, had the organizations been paying attention through adequate auditing and monitoring, these acts may have been prevented or detected earlier, optimally as soon as the technical indicators were observable.

### 3.4.1 Case Examples

#### 3.4.1.1 Sabotage

In one case of IT sabotage, an insider prepared for the future release of a logic bomb by systematically centralizing the critical manufacturing programs for his organization onto a single server. He was able to accomplish this over the objections of his immediate supervisor by taking advantage of his long-term personal relationship with the owner of the company.

This insider had recently been demoted and transferred due to personnel conflicts, including a physical confrontation with a female coworker, and had ended up working for a former supervisee. Shortly before the attack, the organization was undergoing major expansion, opening up centers in other states and countries. Because of the complexity of the networking involved, the organization chose other employees with more technical expertise to lead the expansion effort. The insider, who had been with the organization for many years and had created the company's original network, became even more disgruntled. His immediate supervisor had previously attempted to terminate the insider but was overruled by company owners.

The saboteur had one final conflict with a member of human resources right before he was to be terminated. During the confrontation, the insider intimidated the HR employee into allowing him to take home the only system backup tapes even though the employee knew that the insider was to be fired. Having anticipated termination weeks earlier, the insider created the logic bomb noted above, tested it on the organization's system three times after working hours, set it to execute three weeks later, and released it. His action to centralize all of the files on a single server made the logic bomb much simpler to implement with more devastating impact.

The logic bomb deleted many crucial programs the organization depended on for its manufacturing process. The deleted software was never recovered and the saboteur maintained his innocence, even after the reformatted backup tapes and malicious programs were found in his possession.

Despite his supervisor's ongoing efforts to terminate this employee, management declined to monitor his technical activities. This inattention and the reluctance to terminate this employee were both related to his long tenure with the organization and his ongoing relationship with senior managers—a specific aspect of the trust trap. Diligent auditing and monitoring would have detected the creation and testing of the logic bomb. The attack severely derailed the company's growth, lead to layoffs of 80 employees, and resulted in damages valued over $10 million.

#### 3.4.1.2 Espionage

Robert Hanssen was a special agent for the FBI for 27 years when he was charged with spying for Russia for more than 15 years. He was charged with espionage and conspiracy to commit espionage.

For most of his FBI career, Hanssen had worked in counterintelligence. In order to perform his duties, he had full access to the FBI's Automated Case System (ACS). He was subject to minimal technical access control and monitoring and had complete access to the entire database. He was able to use that access to provide first the Soviet and, later, Russian governments with over 6,000 pages of classified documents and the identities of three Russian agents working for the United States. Two of these sources were tried in Russia and executed. According to court documents, Hanssen provided information on some of the most sensitive and highly compartmented projects in the U.S. intelligence community as well as details on U.S. nuclear war defenses. In return, the Russians paid him $1.4 million over the period of his espionage activities, including over $600,000 in cash and diamonds and $800,000 deposited in a Russian bank account.

It is believed that Hanssen became involved with the Soviets in 1979, broke off the relationship in 1980, but again volunteered to spy for them in 1985. Throughout this period, Hanssen frequently queried the ACS for his own name and for the addresses of the drop sites he used to determine if the FBI was suspicious and investigating him. In addition, once an investigation was initiated, he repeatedly queried the system for new information, becoming further emboldened by the fact that the FBI suspected and was investigating another individual in the CIA.

The ACS logged all system access, including all search criteria used by individual users. However, no one reviewed those logs until suspicion fell on Hanssen. In addition, the ACS had advanced security features for case owners to use in extremely sensitive cases. However, very few agents used those features because of their complexity and difficulty. Had the organization monitored employee information access, they may have noticed and investigated Hanssen's accesses beyond his need to know. With this knowledge, the organization may have been able to implement additional monitoring of the insider, possibly detecting the espionage activity earlier.

The lesson to be learned from the Hanssen case is that an overarching degree of trust awarded employees with access to highly classified information without a balance of auditing and monitoring presents a high degree of risk.

#### 3.4.1.3 Further Comparison of Espionage and Sabotage

In the majority of both sabotage and espionage cases, the organizations failed to recognize technical precursors before the attack. The sabotage cases typically were more technically sophisticated than the espionage cases. Most of the sabotage cases were one-time events resulting in the disruption of critical services. Most of the attacks and attack preparation were technical in nature; some were extremely sophisticated, but others only used fairly simple commands. In the latter cases, the technical sophistication came into play before the attack, when the insider created illegitimate access paths into the system for use later, often following termination. Had the organization been adequately auditing and monitoring, the technical precursors (for example, the development of logic bombs, the creation of backdoor accounts, the cracking of user passwords, and the downloading of malicious code) may have been observed and acted upon early enough to prevent the attack or minimize its impact.

The espionage cases typically were less technical than the sabotage cases. They tended to go on for longer periods and involve multiple acts of espionage. In these cases, the technical indicators typically occurred as part of the espionage acts. If these indicators had been detected, then the spy could potentially have been stopped before transferring the information, or at worst, before committing additional acts of espionage. Thus, the acts themselves were technical precursors to future acts of espionage.

The most common technical precursor exhibited by spies was the access of data outside their need to know. The violation of access level was typically not observed, because many of the systems managing the classified information were not equipped to separate authorization levels or enforce role-based access controls.[19] In the cases where the correct authorization levels could have been implemented (for example, Hanssen and Aragoncillo, who both used the ACS system), the systems were too complex. This tended to discourage users from taking the time to control and track who was accessing which information and alert management to access outside of the need to know.

---

[19] Role-based access control restricts each system function to specific roles, rather than individual users. Roles are created for various job functions, and each user is assigned one or more roles.

## 3.5 OBSERVATION #5

*In many cases, organizations ignored or failed to detect rule violations.*

Figure 7 depicts some of the relationships relevant to the detection of rule violations in IT sabotage and espionage. This observation is supported by 23 of 27 IT sabotage cases (insufficient information was available for three of the cases) and by all of the espionage cases. The three primary feedback loops, B3, R3, and B4, are discussed in order.

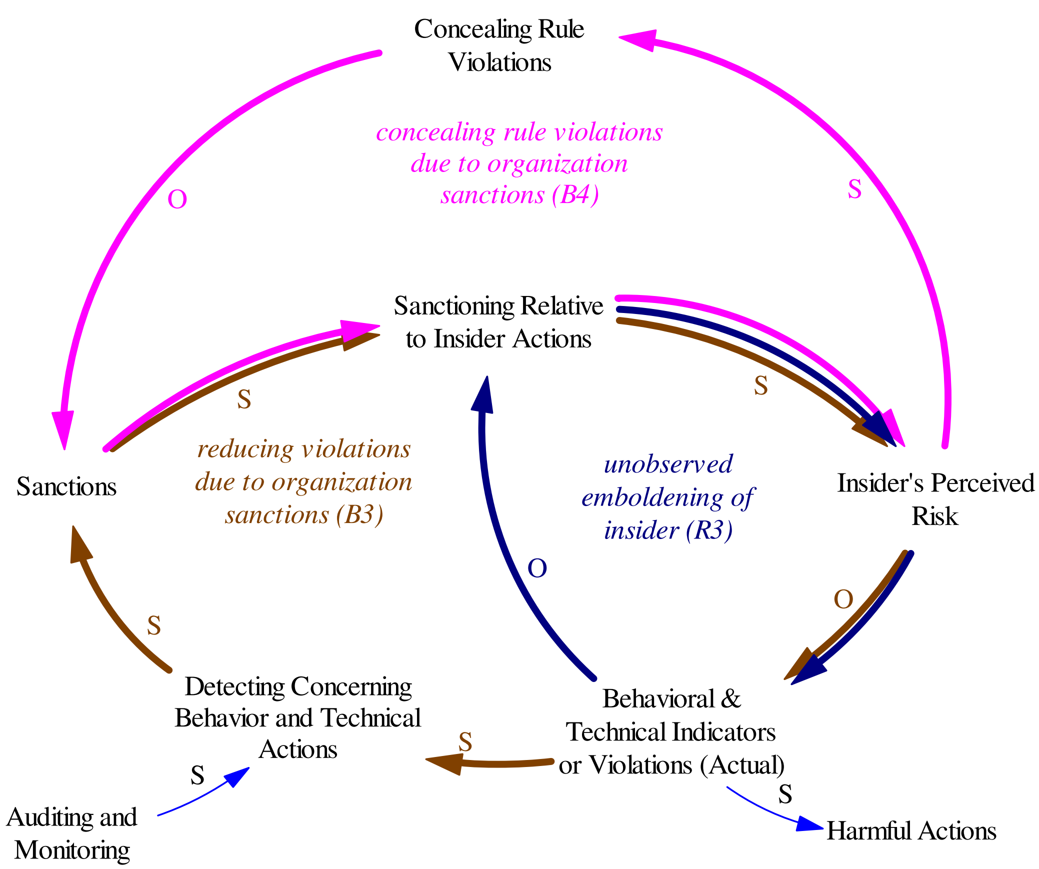


*Figure 7: Model Relationships Relevant to Observation #5*

Rule violations may be behavioral or technical in nature, as shown in the lower right portion of the figure. These rule violations may, in some cases, facilitate the harmful actions of insider IT sabotage or espionage. For instance, the act of downloading tools like password crackers for malicious use is a technical rule violation; the actual use of the password cracker to obtain passwords to others' accounts is the harmful action.

Going clockwise around the B3 (brown) feedback loop we see that, provided the organization has sufficient auditing and monitoring in place, detected behavioral and technical rule violations may lead to sanctioning of the insider. B3 reflects the intended effect of these sanctions, namely the reduction of future behavioral and technical rule violations by the insider. Rule violations may be reduced because, through the sanctions, the insider becomes aware that the organization is paying attention to his behavior and is willing to penalize the insider for that behavior. The variable *Sanctioning Relative to Insider Actions* indicates the extent to which the insider is aware that the organization is paying attention, that is, the extent to which the organization sanctions the insider for misbehavior. The insider's perceived risk of being held responsible for misconduct is heightened. The insider responds by curbing the rule violations to avoid further sanctions.

In the espionage and IT sabotage cases examined in this study, the organizations frequently ignored or failed to appreciate the significance of detected non-technical rule violations. On the other hand, they usually failed to detect technical rule violations in both domains. Feedback loop R3 (navy blue) shows what can happen if an organization ignores or does not detect rule violations. Unpunished or undetected misconduct causes a corresponding drop in the insider's perceived risk and an emboldening of the insider to engage in even more rule violations, possibly leading to harmful actions that the organization is trying to prevent. Note that this emboldening may occur even if the organization understands the implications of the rule violations but does not act on them. Inaction may at some times be warranted; for instance, to gather more evidence against an insider. But organizations need to be aware of the signals this inaction may send.

Rather than curbing their misconduct, insiders may respond to organizational sanctions by trying to conceal their behavior better. While this is not the intended effect of sanctions, it is a natural reaction by an insider already deeply involved in espionage activities or intent on committing IT sabotage. This particular response is exhibited by balancing feedback loop B4 (magenta/purple). As the insider's perceived risk increases due to sanctions, insiders conceal their misconduct better, resulting in fewer sanctions. Thus, the insiders do not cut back on their misconduct, they just "fly below the radar" of the organization's auditing and monitoring activity.

### 3.5.1 Case Examples

#### 3.5.1.1 Sabotage

One saboteur had extensive control over the source code of a mission-critical application being used by his organization. As lead developer of the software, he made sure that he possessed the only copy of the source code. In an effort to maintain "good working relationships," management did not request backups of the software because they thought it would show distrust of their employees. The insider refused to document and manage the configuration of the software according to the organization's own internal policies, even when explicitly requested by management.

After several years of development in this environment, the original manager of the project retired. New management demanded that the insider provide backup copies of the software and bring the software into conformance with the organization's policies. The insider refused to provide the backups or documentation of the source code. He claimed that the software needed to be documented continuously throughout the project, but was not because of a tight development schedule. According to the insider's coworker, the insider never intended to document the software and actually purposely tried to make the code difficult to understand. The insider's feelings of disgruntlement were apparent in his comments to coworkers, and he also intimidated colleagues who questioned his authority and decision making.

A month after learning of a pending demotion, he wiped[20] the hard drive of his laptop, deleting the only copy of the source code the organization possessed, and quit his job. It took more than two months to recover the source code—after it was located by law enforcement in encrypted form at the insider's home. Another four months elapsed before the insider provided the passphrase to decrypt the source code. During this time, the organization had to rely on the executable version of the application, with no ability to make any modifications. Management clearly ignored rule violations in this case, enabling the insider to set up his attack over a long period of time.

#### 3.5.1.2 Espionage

The Robert Hanssen case described in Observation #4 provides another good example of what can happen when management either ignores or fails to detect rule violations. The FBI detected, but did not effectively address, recurrent mishandling of classified information (e.g., attempts to take classified documents home from work) and physical aggression against a female employee. Ignored technical indicators included his use of a password cracker to obtain a system administrator password and probing of his supervisor's computer.

Hanssen installed a password cracking program on his computer while stationed at the State Department. When it was discovered, he claimed he needed it to install a color printer—he used it to obtain the system administrator password and used that account to install the printer. This explanation was accepted and Hanssen suffered no consequences, even though it was in flagrant violation of policy. He also was detected probing his supervisor's computer; his excuse was that he was attempting to demonstrate flaws in the FBI's system security. Once again, he suffered no consequences for his actions, and no increased monitoring of his technical actions.

The FBI did not detect much of Hanssen's other misconduct. Hanssen made many failed attempts to access information for which he did not have a need to know. He hacked into an FBI computer system to access the files of a high-level chief within the organization. He even successfully concealed his malicious intent to sell the information to the Russians by reporting the hacked access to his superiors.

#### 3.5.1.3 Further Comparison of Espionage and Sabotage

Many of the espionage cases examined occurred over long periods and required multiple, serious, ongoing technical rule violations. IT sabotage, although usually a one-time event, was still often preceded by serious technical rule violations.

In addition, sabotage attacks usually involved more technically sophisticated operations than espionage. For example, in the majority of the sabotage cases, the saboteur was angry after termination and attacked the organization remotely. Thus, more of the sabotage activity occurred online rather than physically. Such attacks require greater technical sophistication to set up and

---

[20] When data is deleted from a computer, the information is not actually deleted; rather, the disk space is simply marked as being available for use. Therefore, until it is overwritten, the original information is still intact and accessible. Wiping a hard drive, as this saboteur did, ensures that the information is overwritten several times, making the original data inaccessible.

execute. This modus operandi also highlights the lack of technology designed to detect such attacks. These attacks were usually not discovered until affected systems malfunctioned.

Espionage, on the other hand, typically did not require the spy to break technology-based system access controls to acquire the targeted information. Spies were able to use their own authorized accesses to obtain information for transfer to a foreign power, although often this access went beyond their need-to-know authorization level. Therefore, countermeasures for this activity would include better access controls to prevent the rule violations from happening in the first place, or, conversely, enhanced functionality for auditing and monitoring legitimacy of individuals' information access.

For an organization to improve its posture against insider IT sabotage and espionage, it must understand the potential implications of failing to detect rule violations or ignoring them altogether. Effective responses to acknowledged rule violations may require improving the organizational climate and managerial attitudes regarding rule violators. Effective detection of rule violations may require installing better detection and screening countermeasures. The differences noted above suggest that specific countermeasures effective for the espionage and sabotage domains may differ.

## 3.6 OBSERVATION #6

*Lack of physical and electronic access controls facilitated both IT sabotage and espionage.*

In 28 of the 30 IT sabotage and all of the espionage cases (information was not available for one case), lack of physical or electronic access controls—or both—facilitated the illicit acts. Physical access controls are restrictions on gaining access to organizational facilities, including buildings, rooms within a building, or equipment within a room. Electronic access controls are restrictions to computing and network resources that assume either a level of physical access to those resources or remote access. In most cases, either the insider was given a level of access without appropriate oversight and controls, enabling him to commit his crime, or the organization let its guard down, enabling the insider to escalate his physical or electronic access in order to commit his malicious activity.

Figure 8 illustrates the impact of physical and electronic access controls on insider IT sabotage and espionage. Consider feedback loop R2 (lavender/purple) close to the center of the diagram. This loop is a somewhat simplified version of the trust trap discussed in Observation #4. This reinforcing loop demonstrates that as an organization's perceived risk of insider threat decreases, it tends to devote fewer resources to auditing and monitoring. As a result, its ability to discover harmful actions decreases. As discovery of harmful actions declines, the organization develops the mistaken impression that such events are not happening, thereby lowering its perceived risk even more. Note that a similar dynamic is exhibited in the R3 loop (dark green) with one specific type of harmful activity: unauthorized access. The cycle continues, with the organization's detection capability steadily deteriorating.

Feedback loop B5 (black) characterizes how an organization changes the level of access control used to enforce users' authorization levels based on its perception of risk. The balancing nature of this feedback loop reflects the organization's setting the access controls at a level commensurate with perceived risk. If the trust trap drives perceived risk low then access controls deteriorate, and the insider can more easily commit both behavioral and technical rule violations. This leads to the harmful actions that the organization is trying to avoid. With low levels of perceived risk come low levels of auditing and monitoring, again because of the trust trap. This can result in delays of discovering the harmful actions which amplifies the harm to the organization.

The feedback loop B2 (light green) at the top left of the model reflects a similar dynamic as described above except that instead of the use of access controls to enforce an existing authorization level, the loop represents the organization's tightening of the authorization level itself. With low perceived risk eventually comes greater insider access and potentially more harm to the organization, if the insider is inclined to malicious intent. In both the loops B2 and B5, if an accurate perception of risk is maintained, the organization has a better chance of keeping authorization and access control at appropriate levels.

One question that arises from the above discussion is whether the model refers to enforcing the authorization level and restricting the authorized access level for an individual insider or for all employees of the organization. Better defense against attacks may come through stronger security across the organization, but this also may disrupt the organization from its mission unnecessarily. A strategy that combines proactive access controls and limited widespread monitoring with targeted restrictions on particularly suspicious insiders may be necessary to balance protection from compromise with mission fulfillment. If an organization can identify a member of a sub-group within the organization as the source of compromise, then they may be able to apply stricter security control only on that subgroup, at least until the culprit is identified and apprehended.

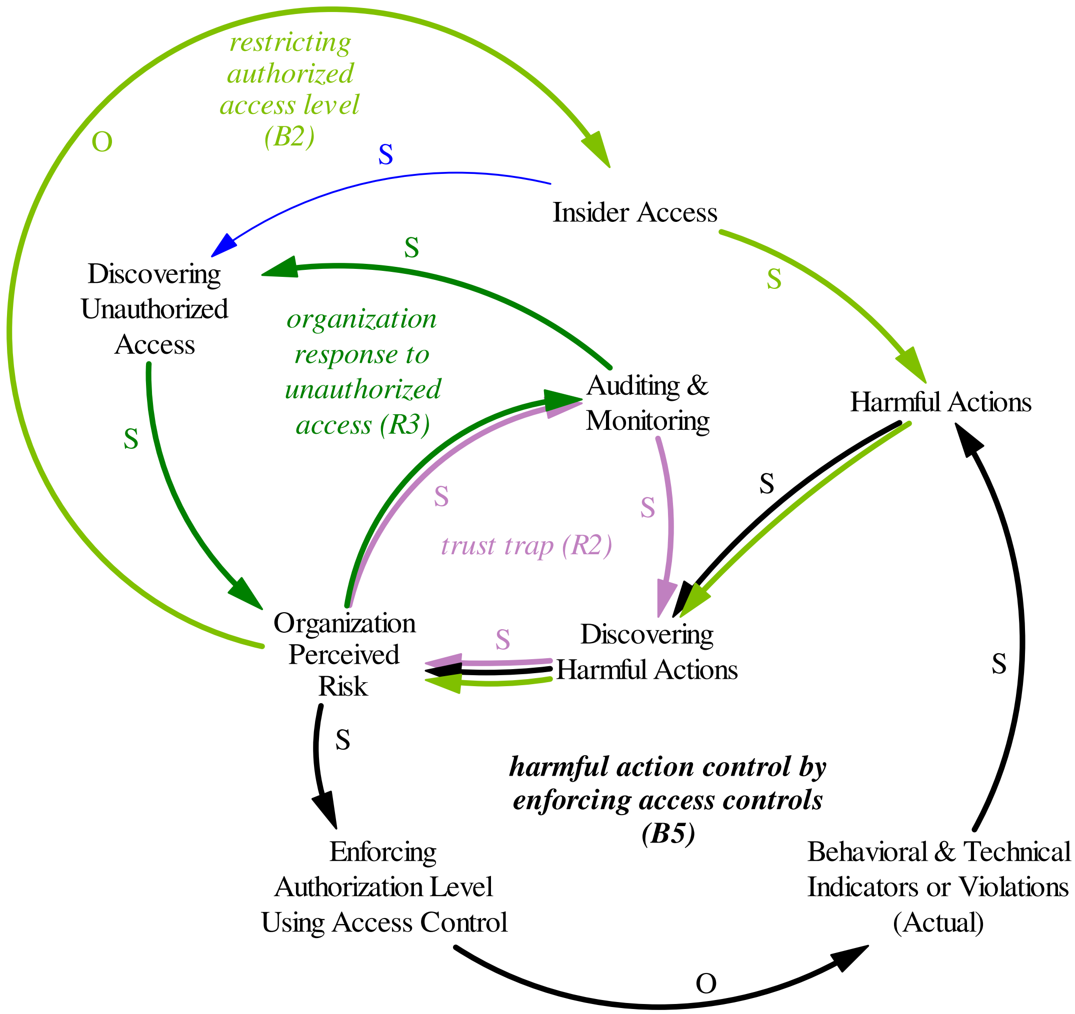


*Figure 8: Model Relationships Relevant to Observation #6*

### 3.6.1 Case Examples

#### 3.6.1.1 Sabotage

Ironically, the saboteur in this case was not disgruntled, but rather was hoping to impress his new supervisor, due to start working the next business day, by being the one to "save the day" after the systems failed. His organization was responsible for running the systems used to provide immediate address information to emergency services based on a caller's phone number for all 911 calls. The organization, apparently perceiving a low level of threat from insiders, protected its network operations center (NOC) solely through physical access controls. In other words, anyone who could gain physical access to the NOC had full access to all computers therein, since all computers were left logged in with system administrator access. Therefore, system authorizations were not well enforced by access controls.

Because of other lax controls, the saboteur was able to obtain a contractor's access card that provided access to the NOC. This behavioral rule violation enabled him to use the card to obtain access to the NOC late one Friday night (yet another behavioral rule violation). The access was not discovered, since there was little auditing and monitoring of either physical or electronic system access. The insider deleted the entire database and all software from all of the systems in the NOC, shut down every system, and stole every backup tape.

He then drove to the offsite backup storage location. There, due to lax access controls, he was able to commit another behavioral rule violation by once again using the contractor's access card to enter the building. He used this access to steal many of the offsite backup tapes.

If the organization had maintained a reasonable level of perceived risk of insider threat, it would not have allowed its access controls to degrade so badly. It would also have had sufficient monitoring and auditing in place to detect the insider's first rule violation. Instead, the entire region was without that critical 911 system function for many hours.

#### 3.6.1.2 Espionage

Leandro Aragoncillo, a naturalized citizen of Filipino descent, served as a military security official for the Vice President of the United States at the White House. Aragoncillo established a close relationship with the former President of the Philippines, Joseph Estrada, visiting the presidential palace with his wife and traveling to the Philippines to visit Estrada in the hospital. This behavior should have alerted his superiors, but it did not, presumably because they were not sufficiently monitoring and auditing behavioral indicators.

Aragoncillo was not authorized to view, access, download, or print information related to the Philippines—he had no need to know. However, this lack of authorization was not enforced via access controls. Therefore, he was able to search the FBI's ACS system for keywords related to the Philippines for at least seven months. Although his actions were logged, they were not reviewed during that period. As a result, he was able to use his access to print or download 101 classified documents pertaining to the Philippines from the ACS system and transmit the information to high-level officials in the Philippines via personal email accounts.

When Aragoncillo attempted to intervene on behalf of an accomplice who was arrested by Immigration and Customs Enforcement (ICE) agents for exceeding his tourist visa, his behavior exceeded a threshold that finally raised his superiors' perceived risk of espionage. They increased auditing and monitoring and discovered his illicit activity. Specifically, they caught him copying classified information to a disk and taking the disk home in his personal bag.

This case illustrates how easy it can be for a spy to commit acts of espionage if access controls are not used to enforce authorization levels. In addition, it shows how insufficient monitoring and auditing enabled a spy to perform actions over a long period that, even at a cursory glance, would have been obviously unauthorized and suspicious.

#### 3.6.1.3 Further Comparison of Espionage and Sabotage

There are several differences between insider IT sabotage and espionage related to this portion of the model. In the espionage cases examined, organizations heavily relied on security clearances to protect their information. Once a clearance had been granted for an employee or contractor, a level of trust was established that trumped all other controls. Therefore, while stringent physical and electronic access controls were implemented to restrict access to facilities and systems only to cleared personnel, lower level access controls or auditing and monitoring were absent or overlooked. Examples include the following:

- Role-based access control was not implemented in technical systems at the data or function level to enforce "need to know."
- Monitoring and auditing were insufficient to detect illegitimate access.
- Physical searches of individuals were not done when leaving a secure facility.

Many of the spies in the espionage cases examined took advantage of these lapses in controls.

On the other hand, in insider IT sabotage cases, the saboteurs were typically system administrators or privileged users. It is much more difficult to control access for these users than for unprivileged users; by definition, they have total access to at least some portion of the organization's system or network. The circumstances were different from the espionage cases; however, the system administrators were granted ultimate trust much in the same way as spies holding security clearances in the espionage cases. In the sabotage cases examined, the organizations did not implement extra controls to restrict and monitor what these "superusers" did. Therefore, the insiders were able to take technical steps to provide themselves with additional access paths to the systems and networks that were very difficult to detect.

Finally, we discovered differences between espionage and IT sabotage concerning the impact of detection. In the cases examined, the organizations usually identified the spy once they acquired information regarding suspicious outside activities and increased auditing and monitoring. However, in the IT sabotage cases, by the time the organizations became aware of a problem with the insider and took action such as demotion or termination, they were usually too late or it was much more difficult to stop the sabotage from happening. By that time, the insider had already taken steps to create new, illegitimate access paths to the organization's systems and data. In these cases, the organization most frequently learned of the attacks after discovering system damage.

# 4 Possible Policy Implications of This Research

While the purpose of this project was not to produce policy recommendations, some of the findings throughout the course of this work are too important to overlook. Therefore, we have decided to include a section in the report discussing policy issues that should be considered at this time. Definite recommendations will not be made until the additional research, detailed in the next section of this report, is completed.

## 4.1 CASE DATA MANAGEMENT

One important implication of this report is that industry and government could benefit greatly from the improved exchange of case data, research, policies, and methods with regard to insider risk mitigation. This is particularly the case given recent innovations in industry following the significant increase in legal and regulatory requirements related to the detection of insider activities [Shaw 2006b]. The significant similarities between IT sabotage and espionage, despite specific differences in some of the concrete behaviors associated with these acts, offers opportunities for those interested in preventing, deterring, and investigating these actions. Both activities appear to offer significant challenges in the areas of personnel screening and selection, detection of at-risk behaviors, and effective investigation of, and, intervention with, persons at risk.

## 4.2 MANAGEMENT TRAINING

Personal predispositions, stressful events and sanctions played a key role in both IT sabotage and espionage cases. This report identifies observable behaviors that can serve as possible indicators of such predispositions, as well as stressful events and sanctions that triggered malicious acts in the case studied. Therefore, mandatory training should be considered to instruct managers how to thoroughly and aggressively evaluate persons at-risk for insider activities. Particular attention should be given to helping managers

- recognize evidence of personal predispositions in their employees that might make them inclined to respond to stressful events inappropriately
- recognize and respond to concerning behaviors and concerning technical actions in their employees
- recognize stressful events that were consequential in the cases studied and take mitigating actions
- impose sanctions appropriately
- monitor sanctioned employees for inappropriate reactions
- understand when they may need to request assistance from qualified outsiders, including security and IT specialists, employee assistance officers, and mental health professionals, to fully evaluate risk

## 4.3 SECURITY AWARENESS TRAINING

In addition to management training, organizations should consider the benefits of periodic security awareness training for all employees. Both the spies and the saboteurs in this study exhibited observable behavior and technical actions detailed in this report that could have alerted their organizations to severe disgruntlement and potential malicious intent. Managers are not always the first to observe these behaviors; therefore, it could be beneficial for all employees to recognize their responsibility for reporting concerning behaviors and concerning technical actions to management for follow up.

## 4.4 EMPLOYEE AUDITING AND MONITORING

Both saboteurs and spies exhibited concerning behaviors following a stressful event, and performed technical actions that could have raised alerts to their malicious intent. Therefore, organizations might consider enhanced monitoring and auditing of individual employee technical activity when concerning behaviors are noted following some stressful event. Associated legal and privacy issues must also be addressed; however, it is not anticipated that this would pose a problem for DoD organizations.

## 4.5 HUMAN RESOURCES POLICIES

Because of the prevalence of serious mental health disorders, personality problems, social skills and decision-making biases, and history of rule conflicts in both the espionage and IT sabotage cases studied, DoD human resources departments should consider creation of policies dictating how observable signs of these problems should be handled. The presence of a history of rule violations in these insiders argues for the expansion of basic background checks where they are not presently used in critical infrastructure organizations. While it is not technically or financially practical to conduct psychological assessment of all new employees, the use of more aggressive employee evaluation methods for persons at risk, including psychological assessments, should be considered when risk factors first appear or when employees are being considered for critical and sensitive positions.

## 4.6 ACCESS CONTROLS

Relying solely on security clearances for physical and electronic access controls can be a dangerous condition, as exhibited in the espionage cases in this study. While DoD policy mandates “need to know” for information access, that policy is not enforced through technical controls. All but one of the spies we studied exploited access control gaps to steal classified information. The DoD might consider enhancing the existing policy to require technical controls (for example, role-based access controls), for enforcing need-to-know access. In addition, more stringent physical security measures might be considered to detect physical evidence of stolen information.

Likewise, granting system administrator or privileged access to employees without procedural and technical controls makes insider IT sabotage easier to carry out. Such elevated access level gives insiders the ability to cause catastrophic system failure or gradually compromise system or data confidentiality, integrity, or availability over time.

It is in the best interest of organizations to devote resources to investigating optimal methods for configuring their systems for controlling and monitoring system administrator and privileged user access. For example, following the institution of the security measures associated with the Health Information Portability and Accountability Act (HIPAA), the healthcare industry has created and enforced new policies and monitoring and auditing practices for detection of suspicious access of medical information without a need to know. Healthcare workers are now routinely fired on the spot for accessing or discussing confidential medical information. Other companies are also testing specific monitoring systems designed to detect insider technical and behavioral risk factors. The research by Shaw details other examples of the migration of such methods from industry to government [Shaw 2006b].

## 4.7 TECHNICAL PRACTICES FOR PREVENTION OR DETECTION OF ESPIONAGE AND INSIDER IT SABOTAGE

Most of the saboteurs took technical actions to set up their attack, and most of the spies accessed information outside of their need to know. Therefore, actions to monitor or audit information access could detect suspicious accesses in time to detect ongoing espionage activity. Likewise, IT practices such as account audits, configuration management, and characterization practices could enable organizations to detect precursors to IT sabotage in time to prevent the actual destruction from happening.

## 4.8 TERMINATION POLICIES

A significant number of insider IT sabotage attacks occurred following termination. Therefore, organizations should establish formal policies and procedures for disabling access immediately upon an employee's termination or resignation. These procedures should include

- deactivating computer accounts
- revoking system authorizations
- disabling remote access
- disabling access to shared accounts
- requiring all coworkers of the departed employee to change their passwords if there is the slightest chance they may have shared their passwords
- terminating physical access
- notifying other employees
- enhancing system access monitoring and system audits immediately following the termination or resignation of a disgruntled employee

However, when it comes to technically sophisticated individuals, even the most scrupulous technical investigations for possible remote access points may not be sufficient. Therefore, more thorough investigation and assessment of individuals at risk prior to their termination should help determine the most appropriate termination tactics, including creative human resource interventions.

# 5 Directions for Immediate Future Research

This report presented six observations resulting from the analysis of the three system dynamics models created for this project (insider IT sabotage model, espionage model, and the abstracted common model). This section describes implications of those observations for future research to support the mitigation of the risk of insider IT sabotage and espionage. These are summarized as follows:

- Recommendation #1: Develop a risk-indicator instrument for the assessment of behaviors and technical actions related to potential risk of insider IT sabotage or espionage.
- Recommendation #2: Acquire improved data on the relative distribution, interrelationships, and weight with respect to attack risk of concerning behaviors, stressful events, and personal predispositions across insider cases in IT sabotage and espionage.
- Recommendation #3: Acquire improved data related to technical actions that are indicative of insider IT sabotage and espionage.
- Recommendation #4: Research policies, methods, and tools for auditing and monitoring behaviors and technical actions that are indicative of insider IT sabotage and espionage.
- Recommendation #5: Acquire improved data to assess the relationship between policy enforcement for technical and non-technical rule violations and the risk of insider IT sabotage and espionage.
- Recommendation #6: Analyze current access control policies and practices and identify and evaluate options to mitigate insider threat risk.
- Recommendation #7: Use the risk-indicator instrument noted in Recommendation #1 to acquire improved information on the base rates and baseline level of risk factors in proportion to actual insider activity.

## 5.1 RECOMMENDATION #1

*Develop a risk-indicator instrument for the assessment of behaviors and technical actions related to potential risk of insider IT sabotage or espionage.*

The effectiveness of this instrument would be tested in controlled, prospective trials involving investigation and assessment of persons with identified risk factors. Our findings indicate that the most productive future research should be directed toward earlier detection of risk indicators and more aggressive and in-depth evaluation of risk in individuals once these signs are discovered. Results of this and earlier research should be used to construct a simple risk-indicator instrument or audit guide that integrates information on personal and organizational predispositions, concerning insider behavior stressful events, and technical risks and rule violations in a simple cumulative checklist. The term organizational predispositions refers to characteristics of the organization which make it vulnerable to insider activity by impacting the organization’s ability to prevent, detect, and successfully manage individuals at risk. This instrument could then be applied in additional post hoc studies of persons with a history of insider rule violations across a range of seriousness.

In this post hoc format, researchers could learn the extent to which past rule violations predict future acts and the extent to which different forms of rule violations co-occur. We could also examine the relative weight or importance of different types of concerning behaviors as they predict the risk of retaining an individual in a position of trust.

In order to address the predictive utility of the list, it could also be applied to the personnel records of a general employee population (including persons with and without a history of risk) to determine the extent to which these indicators occur with and without additional risk behaviors.

In a prospective format, the risk indices could be used to facilitate and test the effectiveness of more aggressive detection, risk investigation, and intervention methods. For example, within the population under study, the occurrence of any individual risk behavior on the indices could mandate a more aggressive and in-depth review of the insider. This might involve psychological evaluation and testing for personal predispositions, technical audits of his electronic access and use, supervisor and peer interviews, financial and travel reviews, and so forth.

This indicator-driven approach could then be compared to conventional evaluation methods in use at the organization to determine whether it results in the more frequent discovery of risk factors and more effective interventions with persons at risk. Employee assistance and other intervention programs could also use this inventory to encourage or mandate referrals and guide specific interventions based on risk. For example, a person with greater levels of personal predispositions and stressful events might be removed from the workplace during investigation while an individual with fewer indicators might be allowed to continue on the job.

## 5.2 RECOMMENDATION #2

*Acquire improved data on the relative distribution, interrelationships, and weight with respect to attack risk of concerning behaviors, stressful events, and personal predispositions across insider cases in IT sabotage and espionage.*

The research literature on insider risk can benefit from larger sample sizes as well as more in-depth information on individual and organizational factors and the use of actual personnel files involving both positive and negative outcomes. The inclusion of persons with identified risk factors who do not commit rule violations is vital to better understanding how to prevent and deter insider acts.

The presence of many of the insiders in this study on the security and human resource “radar” prior to their attacks raises numerous research questions:

- What is the relative distribution of concerning behaviors, stressful events, and personal predispositions across insider cases in sabotage and espionage?
- What are their relative weights with respect to attack risk?
- What is the relative distribution of these factors in general employment populations and, in prospective studies, how often do they signal the presence of a security risk?
- To what extent are all three present in espionage and sabotage cases, consistent with an escalating cycle of risk?

In the combined sample of cases, data on personal predispositions was limited. When insiders were not available for interview, information on medical and psychological history was obtained from records and peer and supervisor reports. Data on decision-making biases, social skills problems, and previous rule violations was more readily available from workplace interviews.

Future research should aim to acquire improved data on personal predispositions so that the distribution of different types of medical and psychological issues in these individuals can be better assessed. We may also then be able to associate different forms of decision-making biases and rule violations with different medical and personality issues.

For example, are shy and withdrawn individuals at greater risk for seduction by outside groups when they become disgruntled? Are persons with anti-social personalities and substance abuse issues at greater risk for impulsive and destructive acts? This research could greatly assist managers and security personnel assess risk in individuals who have come to their attention because of problems in one of these areas.

The equal contribution of personal predispositions in the sabotage and espionage cases has significant implications for future research designed to prevent insider attacks. Many of our spies had gone through significant pre-employment screening, including investigator assessments designed to detect these personal predispositions. In addition, the unknown effectiveness (false positive problem) and financial and legal limitations on general pre-employment psychological testing to detect these personal predispositions prohibit this general approach. Limiting psychological screening prior to assignment to high-risk environments (e.g., systems administration, special weapons access, human intelligence sources, and methods access) might reduce the costs associated with such screening. However, there would still likely be a high number of persons with personal predispositions that would not result in harmful actions (false positives). In this regard, the case data indicate that these personal predispositions become problematic in the context of stressful events and interpersonal conflicts and setbacks.

The occurrence of stressful events prior to insider attacks in both espionage and sabotage insiders indicates the importance of future research on their relative contribution to risk, in combination with personal predispositions and other risk variables. Within the post hoc and prospective research designs proposed above, it will be important to construct an inventory of stressful events with potential insider impacts for use by researchers and managers. As the Peri case demonstrates, because stress is related to insider perceptions and predispositions, this may prove particularly challenging. In this regard, it will also be important to determine whether specific types of stress are associated with different personal predispositions and what types of stress appear to provoke different levels of risk in insiders with different personal predispositions. This information could be extremely important to managers and employee assistance program personnel trying to formulate intervention plans for at-risk individuals.

The high rate of stressful events in these post hoc case studies also reinforces the need to expand the insider pool to include a broader employee base and prospective approaches. For example, the work of Dupre and Barling indicates that employee feelings of victimization by supervisors, often accompanied by a desire for revenge, is relatively common in the workplace [Dupre 2006]. However, these authors found that inhibitory cognitive functions, such as fear of consequences, limit the frequency of employee retaliation. Their findings reinforce the importance of examining the role of personal predispositions in inhibiting the desire for revenge following perceived victimization. This should be a critical focus in prospective studies of employees selected for evaluation after the occurrence of risk items on the inventory proposed above—especially stressful events. Their work also provides a model for studies on a broader range of subjects. If feelings of victimization following workplace stressful events are as common as this work indicates, it may be possible to examine many of the risk factors and dynamics described in this paper without the burden of such low probability events as insider attacks.

In addition, the relative lack of stressful events in the three espionage cases cited earlier raises questions about the role and influence of outside organizations on insider risk. A subset of espionage and sabotage cases should be examined to try to determine the relative influence of outside organizations and/or individuals. A hypothesis to be tested could include the prediction that outside organizations take effective advantage of specific personal predispositions, with and without the presence of stressful events.

Both the *Insider Threat Study* and PERSEREC case files revealed high rates of personnel and technical risk behaviors and clues prior to the studied attacks. The findings regarding the presence of concerning behaviors point squarely to organizational issues affecting the group's ability to detect and intervene with at-risk employees. They raise significant questions regarding the depth of management's understanding of the risk involved in these cases and the effectiveness of the interventions undertaken.

Consistent with the possible presence of an escalating risk cycle, Shaw concluded that many management interventions actually made matters worse [Shaw 2005a]. The high frequency of attacks after termination indicates that these termination procedures have been relatively ineffective in reducing attack risk. Future research might therefore focus on identifying management errors of omission and commission that amplify rather than resolve insider risk.

It will be necessary to analyze these vulnerabilities to determine whether they are also indicators of underlying organizational culture. For example, there are multiple cases from both the sabotage and espionage files in which concerning behaviors appear to have been tolerated and overlooked due to personal connections within the organization, organizational tolerance of particular forms of risk behavior versus others, and over-reliance on ineffective forms of personal screening that could not account for future risk.

Conversely, it may be extremely important to survey the evaluation criteria and procedures used by government and corporate organizations to investigate and evaluate insider risk when behaviors of concern are noted.

- How do these groups balance the relative weight of these different risk factors in security decision making?
- How effective are these approaches in avoiding risk escalation?
- How often do they lead to "rehabilitation" versus loss of an at-risk employee?
- What termination procedures do different groups follow when an employee unusually capable of hurting the organization is terminated in a disgruntled state?

Research suggests that security awareness training could assist all employees in identifying suspicious behaviors that could be indicators of either insider IT sabotage or espionage. Questions for researchers investigating effective security awareness training include

- What constitutes effective security awareness training? Content, frequency, delivery method, others to be determined?
- Has security awareness training been effective in preventing or detecting insider IT sabotage or espionage?

Potential research methods include

- Review prior studies of security awareness training and its effectiveness; determine effective content, audience, frequency of offerings, policy for mandatory training, delivery methods, and so forth.
- Collaborate with private and public sector organizations to collect data on effective and ineffective security awareness training.
- Publish recommendations for security awareness training: content, audience, frequency of offerings, policy for mandatory training, and delivery methods. Recommendations will be based on research described above, as well as expert opinion from researchers in the areas of insider threat and espionage.

## 5.3 RECOMMENDATION #3

*Acquire improved data related to technical actions that are and are not indicative of insider IT sabotage and espionage.*

Observation #4 indicated that if organizations had been paying closer attention to the technical actions of its employees they could have seen insider IT sabotage coming or stopped espionage in its early stages. But what technical actions should the organization view as indicative of pending or ongoing attack? Some actions are obvious indications (e.g., the installation of a logic bomb), whereas the relevance of other actions is not so clear (e.g., accessing information outside the employee's immediate domain of responsibility). We currently have a general understanding of some important indicators and their relationship to a pending attack, but much more targeted research is needed in this area.

Additional analysis of existing data sets is a good starting point, but improved data is needed in the form of additional cases and more extensive field work on cases in our current database. The *Insider Threat Study* cases only cover the period from 1996 through 2002. Due to enormous technological advances since then, it is important that more recent cases be studied in order to update the list of technical indicators. While the observation regarding the technical actions is not likely to change, most likely the actual indicators will. In addition, sufficient details regarding technical actions were not available for the espionage cases studied. Open source information provided a high-level description of technical actions, but more details would have to be gathered in order to develop a valid list of technical indicators of pending or ongoing espionage.

Once a comprehensive list of technical actions has been developed, they should be ranked based on prevalence and impact in the cases studied, and a prioritized list should be produced for use in additional research described below. Finally, those technical actions should be further researched to determine the risk of false positives if they are used as alerts to potential malicious insider activity. While these actions would have been shown to be observable in the insider threat cases, it is possible that some of them might also occur as a matter of course by non-malicious insiders.

## 5.4 RECOMMENDATION #4

*Research policies, methods, and tools for auditing and monitoring behaviors and technical actions that are indicative of insider IT sabotage and espionage.*

Considerations surrounding auditing and monitoring of employee technical actions include technology, process, financial, and employee privacy/legal issues. Technology issues require research into available tools, comparison of their functionality versus requirements from the research described above, and analysis of implementation details. A financial analysis would assess the cost of various implementation options, including cost of the tools, infrastructure enhancements, and staffing required. Collaboration with experts in the information security field as well as practitioners in government and industry should be used to gather information based on practical experience as well as expert opinion.

Privacy/legal restrictions surrounding use of the tools must also be considered. The research also suggests that targeted auditing and monitoring of suspected insiders due to concerning behavior or concerning technical actions could result in detection of pending sabotage or espionage before it happens, as well as ongoing espionage. However, the extent to which organizations can audit and monitor the behaviors of its employees without it being viewed as an infringement on employee privacy depends, to a large extent, on the type of organization. Employees in U.S. government organizations are accustomed to fairly stringent terms of oversight of their behaviors, and need to accept these terms prior to and as a condition for continuing employment. Employees in commercial firms can be much less amenable to strict oversight. However, regardless of the type of organization, employees or employee groups will have general limits on auditing and monitoring beyond which they will view those actions as intrusive and infringing on their privacy. When these limits are exceeded, feelings of trust between management and other staff can suffer possibly leading to decreased morale and productivity and increased disgruntlement.

Organizations and managers have good reason to maintain positive trust relationships with their employees. As noted in Observation #4, however, excessive trust can be self-reinforcing, leading to the progressive dismantling of its auditing and monitoring measures and increasing risk of successful insider attack. Consequently, a proper balance must be struck between the level of trust and the level of auditing and monitoring necessary for different classes of organizations. We recommend research to develop guidance for organizations on how to strike this balance. This research would entail collaboration with legal experts, as well as government and industry organizations that may have already addressed this issue.

## 5.5 RECOMMENDATION #5

*Acquire improved data to assess the relationship between the application of sanctions for rule violations and the risk of insider IT sabotage and espionage.*

Organizations are in a difficult position when faced with an employee who is causing problems—violating technical or non-technical rules—in the workplace and has the potential to commit sabotage or espionage (the extent to which is usually unknown). As noted in Observations #2 and #3, sanctioning due to rule violations can disgruntle an insider to the point of committing harmful acts. Observation #5, on the other hand, indicates that taking no action against rule violations carries its own risk of emboldening the insider. Sanctioning can also push an already committed spy or saboteur to take greater care in concealing harmful acts, thus pushing them further underground and making it harder to detect the crime. Finally, some insiders became disgruntled when rules of behavior were suddenly enforced after a period of exemption from those same rules.

Data are needed to determine the effect of organizational enforcement of rules on different classes of insider saboteurs and spies. We recommend research to collect and analyze such data by surveying and reviewing practices in technical and non-technical policy and rule enforcement and evaluating their impact on the risk of insider IT sabotage and espionage.

## 5.6 RECOMMENDATION #6

*Analyze current access control policies and practices and identify and evaluate options to mitigate insider threat risk.*

Observation #6 indicates the critical role that inadequate physical and electronic access control plays in both insider IT sabotage and espionage. But what reasons underlie an organization's lack of sufficient access controls? Often, organizational performance concerns, such as productivity or growth, compete with managers' attention and good faith attempts to sustain the access controls they have in place. In other cases, organizations never adopt sufficient access controls. Since 9/11, there have been many attempts to increase information sharing within the government. While there are good reasons for improved information sharing, we need to better understand the risks associated with these movements and their potential effects, particularly with regard to espionage.

Research is needed to evaluate optional access control policies and practices that could help organizations deal with competing concerns while still providing adequate mitigation of the insider threat risk. As noted in Observation #6, while access control gaps facilitated the malicious insider activity for both espionage and IT sabotage, the types of vulnerabilities exploited were quite different between the two domains. Therefore, the requirements and solutions will most likely be different. However, it is important that a comprehensive solution be produced as a result of the research that is effective against both types of threat.

This research will require

- determination of access control requirements

- collaboration with government and industry to survey and review operational access control policies and practices
- evaluation of their impact on insider threat risk

## 5.7 RECOMMENDATION #7

*Use the risk-indicator instrument noted in Recommendation #1 to acquire improved information on the base rates and baseline level of risk factors in proportion to actual insider activity.*

Our methods and results indicate that the frequency of IT sabotage and espionage may be greatly underestimated. However, there is little research on the base rates of these phenomena. More thorough and aggressive evaluation of persons at risk may shed light on the ratio of risk factors to actual insider rule violations.

Several factors suggest the above hypothesis. The E-Crime Watch Survey™ was conducted by the U.S. Secret Service, CERT, and *CSO Magazine* in summer 2006 [CSO 2006]. The survey elicited responses from 434 security and law enforcement executives on issues related to electronic crimes. Fifty-five percent of the organizations that were the victim of electronic crime reported one or more insider attacks or intrusions, up from only 39% in 2005. Fifty-eight percent of all attacks were known or suspected to have come from outsiders and 27% from insiders—the rest were unknown. Among organizations experiencing insider attacks, 72% report that one or more cases were handled internally without involving legal action or law enforcement.

Our sabotage sample includes mainly cases in which the damage to systems was discovered only after the systems malfunctioned. As in our espionage cases, this leaves the possibility of insider espionage and sabotage that remains undiscovered due to the lack of observed system damage. These factors make it highly likely that our measures of insider activity—both sabotage and espionage in the private sector—are biased toward under-reporting.

The current research indicates that there are considerable organizational road blocks to the discovery of espionage and that spies often carry out their malicious activity for years before their discovery. Our findings that spies committed their acts using authorized access, and that organizations frequently missed both behavioral and technical indicators of rule violations, support this conclusion. While the circumstances surrounding the discovery of espionage activity are not always clear cut, it appears that many cases are discovered after impacts outside the organization are noted. Only then are internal investigations launched. While organizations are proactively looking for insider violations, the U.S. government reportedly spends less per employee than organizations in the private sector [Gordon 2006]. These findings argue the need for basic research within an array of sample populations to determine the baseline level of risk factors in proportion to actual insider activity. Such research on actual base rates grows more critical as social and political conflicts fuel the potential for insider activity in our society.

# 6 Conclusion

The project described in this report investigated similarities and differences between insider IT sabotage and espionage cases to assess whether a single analytical framework based on system dynamics modeling could be developed to isolate the predictors or conditions leading to both categories of trust betrayal. The research team created three descriptive models: one for IT sabotage, one for espionage, and one called the abstracted common model that represents a high-level view of the commonalities between the two domains.

## 6.1 SUMMARY OF RESULTS

This research represents the analysis of the largest in-depth, unclassified insider case database including psychological, organizational, and technical information, in the literature thus far [Shaw 2006a]. While we await improvements in research methods in this area, the exploration of these data through system dynamics modeling may represent the best available means to apply empirical insider research to practical issues of prevention, detection, and management. This research approach can now be used to test the impact of proposed policy changes, detection technologies, and intervention techniques before they are implemented in the field. Additional research that bolsters the database with successfully prevented, detected, and managed cases would further increase the utility of this approach.

Our research found definite parallels between the two categories of trust betrayal. This provides evidence that insider sabotage and espionage share critical predictors and facilitating conditions. It follows that they could be detected and deterred by the same or similar administrative and technical safeguards and prevented by similar configurations of security countermeasures. Organizations adopting safeguards that counter both espionage and IT sabotage crimes get added return on their investment. Therefore, research into countermeasures that address multiple threats should be of high priority. We have identified areas of research that our study suggests would be most fruitful for combating both IT sabotage and espionage.

In the process of executing this study, we combined case information from two databases with distinctive and overlapping characteristics. CERT's *Insider Threat Study* database emphasized technical aspects of the insider threat, while the smaller PERSEREC database emphasized more in-depth insider and organization psychological characteristics. Together, these data represented one of the largest and in-depth unclassified databases on insider activity currently available. It was interesting from a theoretical standpoint that the models produced by this process tended to support emerging theoretical concepts regarding the key components of insider risk. For example, the importance of predisposing characteristics and stressful events in contributing to insider motivation was supported. The presence of concerning behavior and concerning technical actions prior to the incident was also consistent with previous research. Support for these findings provides the confirmation for some rudimentary guidelines for detecting persons at risk and for the identification of organizations and systems where risk of insider betrayal is higher. At the same time, the current study also confirmed the role and contribution of organizational problems to emerging insider risk. As in previous studies, organizations proved handicapped in detecting persons at risk and managing them effectively once they were identified. In this regard, the finding from earlier studies that most IT saboteurs attacked after termination also was confirmed.

## 6.2 VALUE OF MODELING EFFORTS

A question of interest to the research team is to what extent the model-based approach contributed to greater understanding of the domains. Would similar, or better, results have been obtained without the development of the system dynamics models? Are further modeling efforts warranted in these domains to develop greater understanding, to refine the recommendations, or to gain greater confidence in the results?

It is difficult, in retrospect, to assess how productive the team would have been without the use of the system dynamics modeling approach. It is possible that simply bringing together a group of people with such a broad range of experiences in insider threat would have produced positive results. However, we found that the system dynamics approach helped to structure and focus the team's discussion. This was particularly important since members of the team, by necessity, came from a variety of disciplines, including psychology, political science, history, and information security.

By identifying the primary variables of interest, the influences between these variables, and the feedback loops that are so important for understanding complex behavior, the team found itself able to communicate much more effectively. The group modeling process enabled the team to step back and consider the "big picture" at times, and focus on individual concepts at other times. The rigorous notation helped identify commonalities to simplify the models and prevent misunderstandings that could have hindered progress otherwise. In addition, it was immensely valuable for each team member to be able to come away with the models that we developed after our group sessions and devote individual thought to each. It not only documented our progress but helped us pick up from where we left off after a period of downtime and reflection on what we had accomplished. The models also provided a concrete target for validation through mapping to observables exhibited by the real-world cases.

The modeling approach was particularly useful for the identification of commonalities between insider IT sabotage and espionage. Modeling each of the domains separately allowed a much more structured comparison of important dynamic aspects of each than would have been otherwise possible. The system dynamics models documented the feedback structure important to understanding each domain. By focusing the comparison on the feedback structure shared by both models, the abstracted common model elaborated the most critical elements of commonality: the feedback loops that underlie the problematic behavior shared by both IT sabotage and espionage.

We cannot overestimate the importance of looking at the total context of adverse insider behavior for understanding why these events happened and how they might be prevented in the future. Too often research on espionage or cyber crime focuses on the individual offender and his or her personal history, psychological defects, or external inducements for understanding the crime or offense. By employing the system dynamics approach we attempt to assess the weight and interrelatedness of personal, organizational, social, and technical factors as well as the effectiveness of deterrent measures in the workplace.

As noted in our research recommendations, there are significant methodological and data challenges to be solved before research on insider activity can be soundly prescriptive for policies, practices, and technology. Prospective studies of these phenomena will always be challenging because of apparently low base rates, particularly for the rare but extremely damaging crime of espionage. In the meantime, system dynamics modeling using available empirical data can plug this methodological gap and translate the best available data into implications for insider policies and practices.

## 6.3 RECOMMENDATIONS FOR FOLLOW-ON WORK

The primary outputs of this initial effort are

- a comparison of the IT sabotage and espionage domains using the abstracted common model
- policy implications
- research recommendations

We view the development of individual system dynamics models for IT sabotage and espionage to be a means to an end—comparing the domains of sabotage and espionage—rather than an end in itself. The abstracted common model, as shown in Appendix A, served as the link between the detailed group modeling efforts and the implications and recommendations. Its central role is exhibited by its use throughout this report to formally represent the observations on which the recommendations and implications were based.

The detailed IT sabotage and espionage models, as shown in Appendices B and C, are still works in progress.[21] In general, these were developed by comparing events in each of the two domains as distinct categories of trust betrayal. While they were instrumental in our initial efforts to understand the two domains as if they encompassed unrelated phenomena, the focus eventually shifted to a higher, abstracted level, at which time development of the individual models was halted. Nevertheless, we believe that there is value in documenting the IT sabotage and espionage models as a basis for further insight and continued research in the area. We therefore, propose additional work to simplify, modularize, and unify the existing IT sabotage and espionage models to improve their comprehensibility, extensibility, and analyzability.

In addition, we hope that the collaboration among the organizations participating in this work continues. We believe that additional work is needed in both the analysis of case data and the elaboration of our system dynamics models. The team has assembled a database of areas that need further exploration to map out the problem domains more fully and understand their commonality. Specifically, our models could be refined as follows:

- Enhance the models to accommodate simulation to improve the accuracy and validate the recommendations made.
- Expand the coverage of personal predispositions, organizational predispositions, and vulnerabilities, co-opting organization influences and feedbacks.

[21] This report does not describe these two models sufficiently so that an independent party could understand or evaluate their validity. We include them in this report only to record their state at the conclusion of our initial efforts.

- More accurately reflect the effect of sanctions and employee intervention on insider disgruntlement and the risk of insider attack based on insider predispositions.
- Include indication of the strength of influence between variables in the model.
- Characterize the effect of screening on prevalence of insider attributes.
- Reflect changing motivations over time (e.g., the motivation driving espionage activity may be different before starting espionage and after first engagement).
- Include effects of fantasies about spying as a motivator.
- Characterize the short-term and long-term effects of overreaction of organization to suspected insider attack.
- Represent the effect of widespread, open communication of technical security measures by the organization on insider’s perceived risk.
- Reflect on how organizational reactions deter or promote others to engage in insider IT sabotage or espionage.

This work would support refining our recommendations in the areas of organizational policies, practices, and technologies that would help mitigate insider threat risk. This report is a vital checkpoint on our current progress and future plans in this area. Feedback is critical to ensure the quality and direction of the work is consistent with the missions of the organizations involved.

# 7 References


**[APA 1994]**
American Psychiatric Association. *Diagnostic and Statistical Manual of Mental Disorders, Fourth Edition.* Washington, DC: American Psychiatric Association, May 1994.

**[Anderson 2004]**
Anderson, D. F.; Cappelli, D. M.; Gonzalez, J. J.; Mojtahedzadeh, M.; Moore, A. P.; Rich, E.; Sarriegui, J. M.; Shimeall, T. J.; Stanton, J. M.; Weaver, E.; & Zagonel, A. "Preliminary System Dynamics Maps of the Insider Cyber-Threat Problem." *Proceedings of the 22nd International Conference of the System Dynamics Society.* Oxford, UK, July 2004. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2004.
http://www.cert.org/archive/pdf/InsiderThreatSystemDynamics.pdf.

**[Cappelli 2006]**
Cappelli, D. M.; Desai, A. G.; Moore, A. P.; Shimeall, T. J.; Weaver, E. A.; & Willke, B. J. "Management and Education of the Risk of Insider Threat (MERIT): Mitigating the Risk of Sabotage to Employers' Information, Systems, or Networks." *Proceedings of the 24th International System Dynamics Conference.* Nijmegen, Netherlands, July 2006.
http://www.albany.edu/cpr/sds/conf2006/proceed/proceed.pdf.

**[Crawford 1993]**
Crawford, Kent S. & Bosshardt, Michael J. *Assessment of Position Factors that Increase Vulnerability to Espionage.* Monterey, CA: Defense Personnel Security Research Center, 1993.

**[CSO 2006]**
*CSO magazine* in cooperation with the U.S. Secret Service & CERT® Coordination Center. 2006 eCrime Watch™ Survey. http://www.cert.org/archive/pdf/ecrimesurvey06.pdf.

**[Dupre 2006]**
Dupre, K. E. & Barling, J. "Predicting and Preventing Supervisory Workplace Aggression." *Journal of Occupational Health Psychology 11,* 1 (2006): 13–26.

**[Fischer 2003]**
Fischer, L. F. "Characterizing Information Systems Insider Offenders." *Proceedings of the International Military Testing Association Conference*, Pensacola, FL, November 2003.
http://www.internationalmta.org.

**[Fischer 2002]**
Fischer, L.F.; Riedel, J.A.; & Wiskoff, M.F. (2000) *A New Personnel Security Issue: Trustworthiness of Defense Information Systems Insiders*, November 2002. http://www.internationalmta.org.

**[Gordon 2006]**
Gordon, Lawrence A.; Loeb, Martin P.; Lucyshyn, William; & Richardson, Robert. *2006 CSI/FBI Computer Crime and Security Survey*. San Francisco, CA: Computer Security Institute, 2006.

**[Herbig 2002]**
Herbig, Katherine L. & Wiskoff, Martin F. "Espionage Against the United States by American Citizens, 1947–2001." *PERSEREC Technical Report 02-5.* July 2002. http://www.fas.org/sgp/library/spies.pdf.

**[Huber 2002]**
Huber, C.; Cooke, F.; Smith, J.; Paich, M.; Pudar, N.; & Barabba, V. "A Multimethod Approach for Creating New Business Models: The General Motors OnStar Project," *Interfaces 32,* 1 (2002): 20–34.

**[Keeney 2005]**
Keeney, M. M.; Kowalski, E. F.; Cappelli, D. M.; Moore, A. P.; Shimeall, T. J.; & Rogers, S. N. "Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors." *Joint SEI and U.S. Secret Service Report*. May 2005. http://www.cert.org/archive/pdf/insidercross051105.pdf.

**[Kramer 2005]**
Kramer, L.; Heuer, R.; & Crawford, K. *Technological, Social, and Economic Trends that Are Increasing U.S. Vulnerability to Insider Espionage* (TR05-10). Monterey, CA: PERSEREC, 2005. http://www.fas.org/sgp/othergov/dod/insider.pdf.

**[Meadows 1974]**
Meadows, D. L.; Behrens, W. W.; Meadows D. H.; Naill, R. F.; Randers, J.; & Zahn, E. K. O. *Dynamics of Growth in a Finite World*. Cambridge, MA: Wright-Allen Press, Inc., 1974.

**[Melara 2003]**
Melara, C.; Sarriegui, J. M.; Gonzalez, J. J.; Sawicka, A.; & Cooke, D. L. "A system dynamics model of an insider attack on an information system." *Proceedings of the 21st International Conference of the System Dynamics Society.* New York, NY, July 20–24, 2003. Albany, NY: Systems Dynamics Society, 2003. Available through http://www.systemdynamics.org/publications.htm.

**[Moore 2005]**
Moore, A. P. & Cappelli, D. M. "Analyzing Organizational Cyber Threat Dynamics." *Proceedings of the Workshop on System Dynamics of Physical and Social Systems for National Security*. Chantilly, VA: April 21–22, 2005. Available through the author: apm@sei.cmu.edu.

**[OSD 2000]**
Office of the Secretary of Defense. *DoD Insider Mitigation, Final Report of the Insider Threat Integrated Process Team*. 2000. https://dssacdsws.dss.mil/is201docs/DoD_Insider_Threat_Mitigation.pdf.

**[Parker 1991]**
Parker, Joseph P. & Wiscoff, Martin F. *Temperament Constructs Related to Betrayal of Trust.* Monterey, CA: Defense Personnel Security Research Center, 1994.

**[PERSEREC 2004]**
PERSEREC. *Espionage Cases: 1975–2004, Summaries and Sources.* Monterey, CA: Defense Personnel Security Research Center, 2004.

**[Randazzo 2004]**
Randazzo, M. R.; Keeney, M. M.; Kowalski, E. F.; Cappelli, D. M.; & Moore, A. P. "Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector." *Joint SEI and U.S. Secret Service Report*, August 2004. http://www.cert.org/archive/pdf/bankfin040820.pdf.

**[Rich 2005]**
Rich, E.; Martinez-Moyano, I. J.; Conrad, S.; Cappelli, D. M.; Moore, A. P.; Shimeall, T. J.; Andersen, D. F.; Gonzalez, J. J.; Ellison, R. J.; Lipson, H. F.; Mundie, D. A.; Sarriegui, J. M.; Sawicka, A.; Stewart, T. R.; Torres, J. M.; Weaver, E. A.; & Wiik, J. "Simulating Insider Cyber-Threat Risks: A Model-Based Case and a Case-Based Model." *Proceedings of the 23rd International Conference of the System Dynamics Society.* Boston, MA, July 2005. Albany, NY: Systems Dynamics Society, 2005.

**[Sarbin 1996]**
Sarbin, T.R. *Computer Crime: A Peopleware Problem. Proceedings of a Conference Held in Monterey, California on October 25 - 26, 1993*. Monterey CA: Defense Personnel Security Research and Education Center, 1993.

**[Shaw 2005a]**
Shaw, E. D. "Ten Tales of Betrayal: The Threat to Corporate Infrastructures by Information Technology Insiders," Report 2—Case Studies. *Technical Report 05-05* (FOUO). Monterey, CA: Defense Personnel Security Research Center, 2005.

**[Shaw 2005b]**
Shaw, E. D. & Fischer, L. "Ten Tales of Betrayal: An Analysis of Attacks on Corporate Infrastructure by Information Technology Insiders," Report 1—Overview and General Observations, *Technical Report 05-13* (FOUO). Monterrey, CA.: Defense Personnel Security Research Center, 2005.

**[Shaw 2006a]**
Shaw, E. D. "The Role of Behavioral Research and Profiling in Malicious Cyber Insider Investigations," 20–31. *Digital Investigation, The International Journal of Digital Forensics and Incident Response, Vol. 3.* Exeter, UK: Elsevier Publications, 2006.

**[Shaw 2006b]**
Shaw, Eric D. & Wirth-Beaumont, Erin. *A Survey of Innovative Approaches to IT Insider Prevention, Detection, and Management*. Washington DC: Consulting & Clinical Psychology, Ltd., March 2006.

**[Sterman 2000]**
Sterman, John D. *Business Dynamics: Systems Thinking and Modeling for a Complex World*. New York, NY: McGraw-Hill, 2000.

**[Wood 1992]**
Wood, S.& Wiskoff, M. *Americans who Spied Against Their Country since World War II* (PERS-TR-92-005). Monterey, CA: PERSEREC, 1992. http://www.dss.mil/training/tr92005.pdf.

# Appendix A: Abstracted Common Model

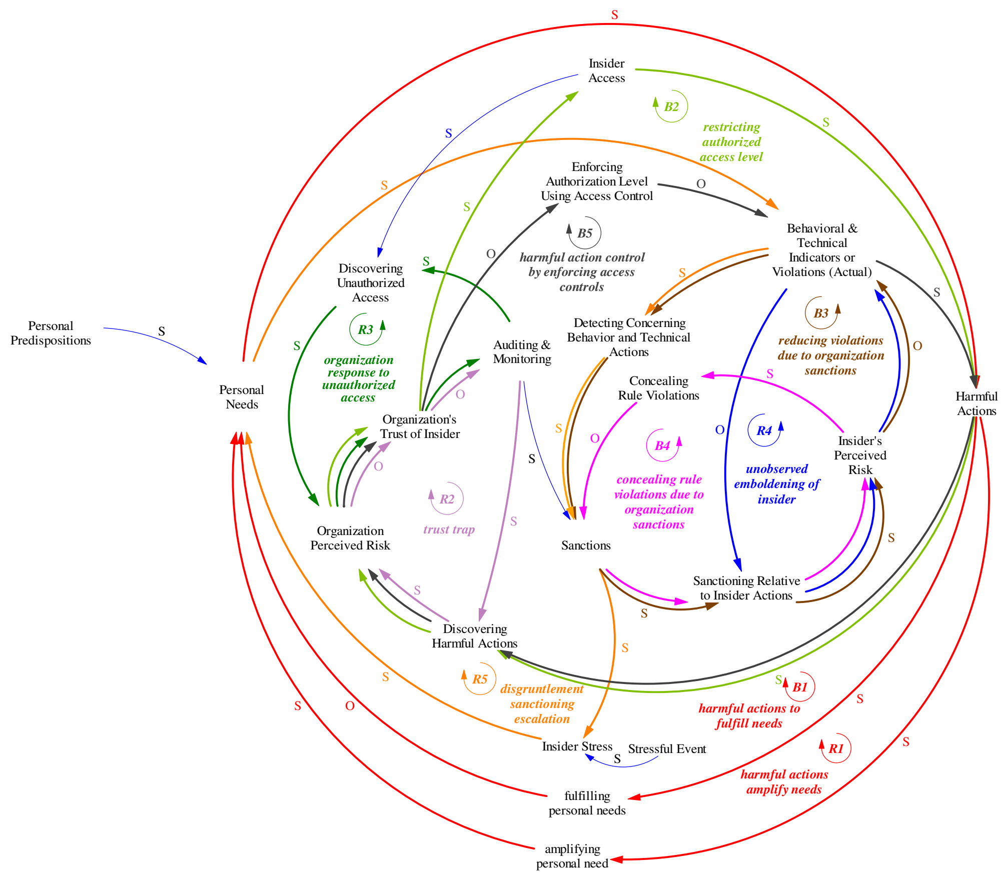


*Figure 9: Abstracted Common Model*

*Table 1: Model Feedback Loops*

| Loop Num | Loop Label | Aspect Characterized |
|---|---|---|
| B1 | harmful acts to fulfill needs | Motivation driving insider's harmful activity (i.e., sabotage or espionage), especially the initial act of harm. |
| R1 | harmful acts amplify needs | Once the insider's harmful acts start, this keeps the insider engaged in the activity—either committing espionage, or taking technical actions to prepare for IT sabotage. |
| R2 | trust trap | Over time, excessive trust of employees can lead gradually to decreases in an organization's auditing and monitoring activity, leading to fewer detected compromises. This, in turn, reduces the organization's perception of risk and leads to more trust in employees |
| B2 | restricting authorized access level | Based on perceived risk of insider attack, an organization can restrict an insider's authorized access to information and thus limit an insider's ability to commit harmful acts. |
| R3 | org. response to unauthorized access | Heightened perceived risk of insider threat leads to increased auditing/monitoring and the discovery of unauthorized insider accesses, which further increases risk perception. Subject to the *trust trap* above. |
| B3 | reducing violations due to org. sanctions | An increase in sanctions can increase the insider's perceived risk of being caught, which may cause the insider to reduce espionage activities or technical actions to set up IT sabotage. This is the desired effect of sanctions and may cause the organization to perceive less risk and think that the sanctions worked. |
| R4 | unobserved emboldening of insider | Left undetected or ignored, rule violations reduce the insider's perception of risk of being caught. In turn, reduced perception of risk leads to additional rule violations. This reinforcing cycle of emboldening can remain unobserved by management (absent sufficient enforcement, auditing, and monitoring by the organization, perhaps due to organization's misplaced trust). |
| B4 | concealing rule violations due to org. sanctions | An increase in sanctions can increase the insider's perceived risk of being caught, which may cause the insider to increase concealment of his espionage activities or technical actions to set up IT sabotage. This is not the desired effect of sanctions but may cause the organization to perceive less risk and think that the sanctions worked. |
| R5 | disgruntlement sanctioning escalation | Depending on insider predispositions, sanctions may increase the interpersonal needs of the insider, leading to more rule violations and an escalation of sanctioning. |
| B5 | harmful action control by enforcing access controls | Based on perceived risk of insider attack, an organization can increase enforcement of access controls (physical and electronic) and reduce the insider's unauthorized access to information. |

# Appendix B: Insider IT Sabotage Model

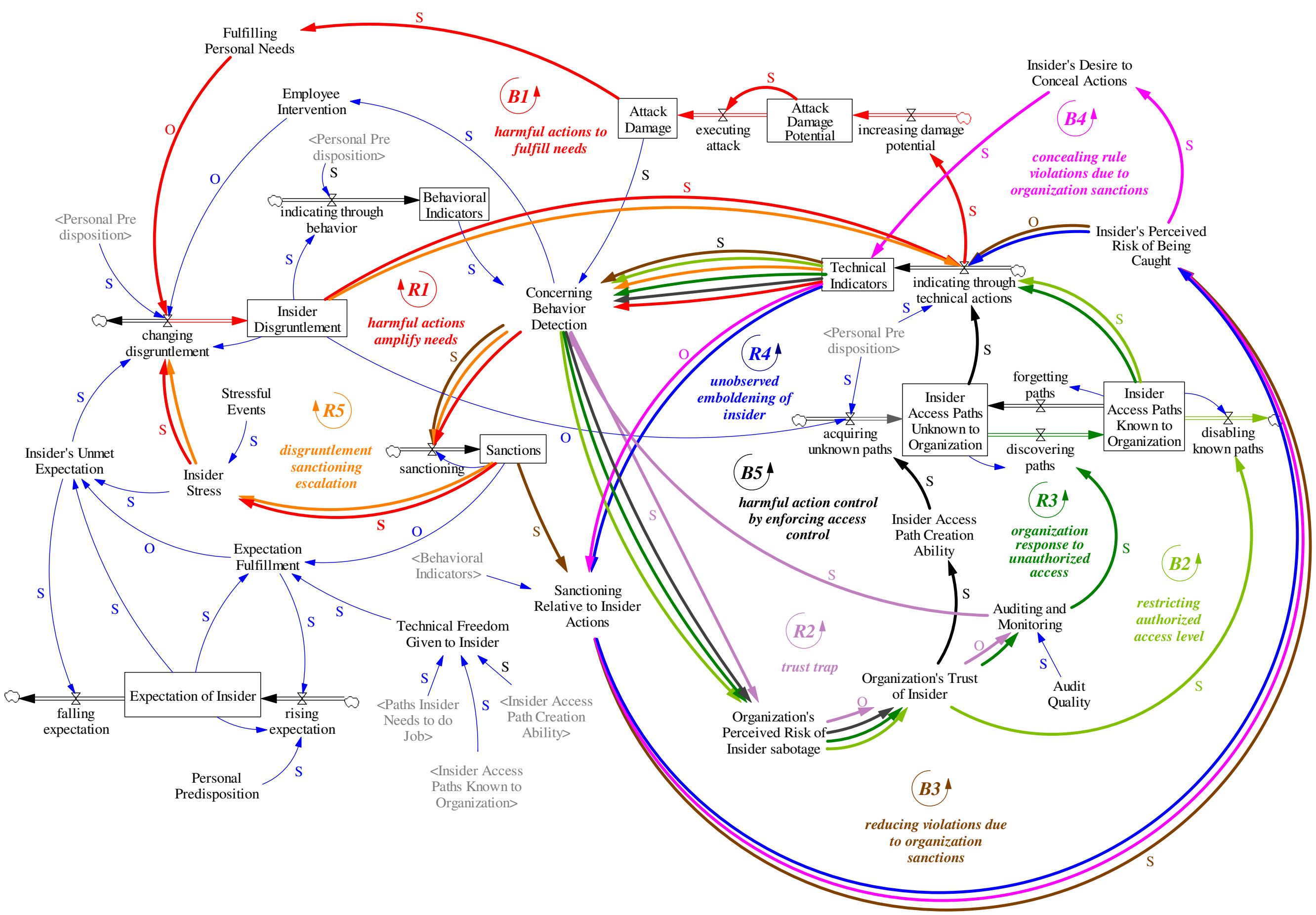


*Figure 10: Insider IT Sabotage Model*

# Appendix C: Espionage Model

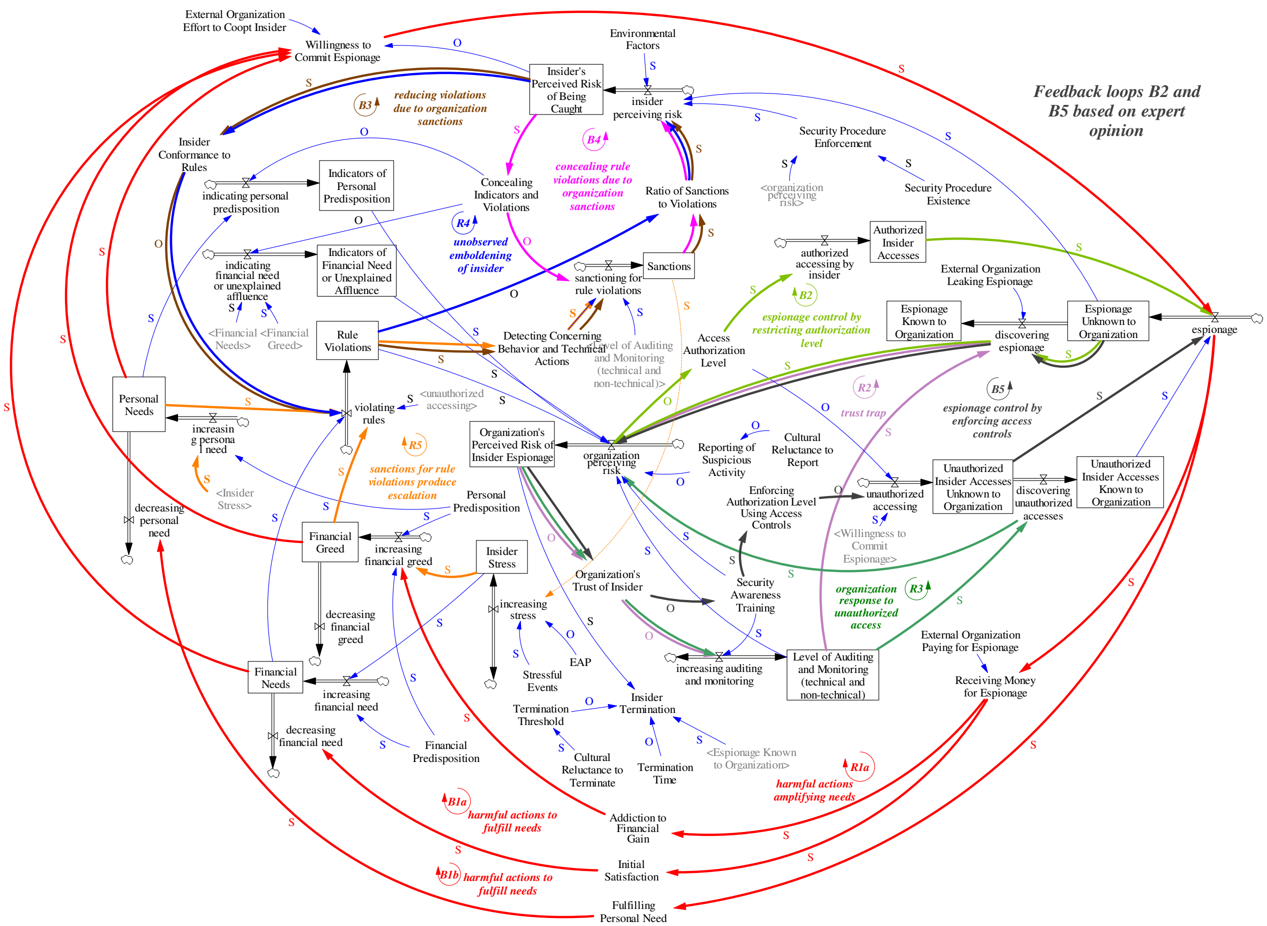


*Figure 11: Espionage Model*

# Appendix D: Technical Observables

## TECHNICAL ACTIONS AND INDICATORS

| |
|---|
| **Espionage Cases** |
| Access of information outside of need to know |
| Concealment strategies |
| Download and installation of malicious code and tools |
| Hacking |
| Unauthorized encryption of information |
| Unauthorized information transfer |
| Violation of acceptable use policy |
| Violation of password management policy |
| **Sabotage Cases** |
| Creation of backdoor account |
| Download and installation of malicious code and tools (e.g., password cracker or virus) |
| Failure to comply with configuration management policy |
| Unauthorized information transfer |
| Access from new employer’s system |
| Installation of an unauthorized modem (hardware backdoor) for later access |
| Disabling of anti-virus on insider’s computer to test virus for later use in sabotage |
| Network probing |

## HARMFUL TECHNICAL ACTIONS

| Espionage Cases |
| --- |
| Printing documents |
| Copying information to disks |
| Relabeling of disks |
| **Sabotage Cases** |
| Denial of service by changing passwords or disabling access |
| Deletion of files, databases, or systems—including system history files |
| Constructing, downloading, testing, or planting logic bombs |
| Stealing or sabotaging backups |
| Terminating programs or shutting down computers or equipment |
| Cutting cables |
| Reformatting disks |
| Downloading a virus onto customers' computers |
| Turning off system logging |
| Web site defacement |
| Use of organization's system following termination to send derogatory email to customers |
| Modification of ISP's system logs to frame someone else for actions |
| Accessing confidential information and making it available to customers, employees, or the public |
| Theft of hardware, software, and documentation |

## TECHNICAL RULE VIOLATIONS

| |
|---|
| **Espionage Cases** |
| Violation of need to know |
| Violation of SCIF physical security policies and procedures |
| Download and use of password cracker |
| Unauthorized encryption of information |
| Compromise of supervisor’s computer |
| Unauthorized “web surfing” and watching videos on office computer in violation of acceptable use policy |
| **Sabotage Cases** |
| Downloading and use of “hacker tools” such as rootkits, password sniffers, or password crackers |
| Failure to create backups as required |
| Failure to document systems or software as required |
| Unauthorized access of customers’ systems |
| Unauthorized use of coworkers machines left logged in |
| Sharing passwords with others |
| System access following termination |
| Refusal to swipe badge to record physical access |
| Access of web sites prohibited by acceptable use policy |
| Refusal to return laptop upon termination |
| Use of backdoor accounts |
| Use of organization’s system for game playing, violating acceptable use policy |

# Appendix E: Mapping IT Sabotage Cases to Observations

(**X**—Observation Exhibited; **N**—Observation Not Exhibited; **U**—Unknown if Observation was Exhibited)

| CERT Tracking Number | Obs. #1 Personal Predispositions | Obs. #2 Stressful Events | Obs. #3 Concerning Behavior (Non-Technical) | Obs. #4 Technical Actions | Obs. #5 Ignoring or Lack of Detection of Rule Violations | Obs. #6 Lack of Physical and Electronic Access Control |
|---|---|---|---|---|---|---|
| 1 | **U** | **X** | **X** | **X** | **X** | **X** |
| 2 | **X** | **X** | **X** | **X** | **X** | **X** |
| 3 | **X** | **X** | **X** | **X** | **X** | **X** |
| 4 | **X** | **X** | **X** | **X** | **X** | **X** |
| 5 | **U** | **X** | **X** | **X** | **U** | **X** |
| 6 | **X** | **X** | **X** | **X** | **X** | **X** |
| 7 | **U** | **X** | **N** | **X** | **X** | **X** |
| 8 | **X** | **X** | **X** | **X** | **N** | **X** |
| 9 | **U** | **X** | **N** | **X** | **N** | **X** |
| 10 | **U** | **X** | **X** | **X** | **X** | **X** |
| 11 | **X** | **X** | **X** | **X** | **X** | **X** |
| 12 | **U** | **U** | **X** | **X** | **N** | **X** |
| 13 | **X** | **X** | **X** | **X** | **X** | **X** |
| 14 | **U** | **X** | **X** | **X** | **X** | **X** |
| 15 | **U** | **X** | **X** | **X** | **X** | **X** |
| 16 | **U** | **X** | **X** | **X** | **X** | **N** |

| | | | | | | |
|---|---|---|---|---|---|---|
| 17 | **U** | **X** | **X** | **X** | **X** | **N** |
| 18 | **X** | **X** | **X** | **X** | **X** | **X** |
| 19 | **X** | **X** | **X** | **X** | **X** | **X** |
| 20 | **X** | **X** | **N** | **X** | **X** | **X** |
| 21 | **X** | **X** | **X** | **X** | **U** | **X** |
| 22 | **X** | **X** | **X** | **U** | **X** | **X** |
| 23 | **X** | **X** | **X** | **U** | **U** | **X** |
| 24 | **X** | **X** | **X** | **X** | **X** | **X** |
| 25 | **X** | **X** | **X** | **X** | **X** | **X** |
| 26 | **X** | **X** | **X** | **X** | **X** | **X** |
| 27 | **X** | **X** | **X** | **X** | **X** | **X** |
| 28 | **U** | **X** | **X** | **N** | **N** | **X** |
| 29 | **X** | **X** | **X** | **X** | **X** | **X** |
| 30 | **U** | **X** | **X** | **X** | **X** | **X** |

## Appendix F: Mapping Espionage Cases to Observations

(**X**—Observation Exhibited; **N**—Observation Not Exhibited; **U**—Unknown if Observation was Exhibited)

| Case Name | Obs. #1 Personal Predispositions | Obs. #2 Stressful Events | Obs. #3 Concerning Behavior (Non-Technical) | Obs. #4 Technical Actions | Obs. #5 Ignoring or Lack of Detection of Rule Violations | Obs. #6 Lack of Physical and Electronic Access Control |
|---|---|---|---|---|---|---|
| Ames | X | X | X | X | X | X |
| Anderson | X | U | X | X | X | X |
| Aragoncillo | X | X | X | X | X | X |
| Hanssen | X | X | X | X | X | X |
| Hoffman | X | X | X | U | X | U |
| Montes | X | U | X | X | X | X |
| Peri | X | X | X | X | X | X |
| Regan | X | X | X | X | X | X |
| Smith | X | U | X | X | X | X |

# Appendix G: Criteria for Personal Predispositions

## SERIOUS MENTAL HEALTH DISORDERS

Serious mental health disorders involved evidence of Axis I Psychiatric Diagnoses derived from the American Psychiatric Association's (APA) *Diagnostic Manual* [APA 1994]. This level of psychological difficulty often threatened the insiders' ability to function successfully in their job and in personal relationships at work in both IT sabotage and espionage cases (versus Axis II personality disorders below). Several saboteurs in the combined database on IT sabotage appear to have suffered from such serious mental health disorders (some requiring medical treatment) prior to their attacks and legal problems [Randazzo 2004, Keeney 2005, Shaw 2005a]. For example, one or more insiders

- were being treated with anti-anxiety and anti-depressant medications
- suffered from alcohol and drug addiction
- suffered from panic attacks
- were forced to leave a business partnership due to drug addiction
- reported seeing a psychologist for stress-related treatment
- had a history of physical spouse abuse

The presence of these serious mental health problems has frequently been thought to play less of a role in espionage cases because of the significant levels of emotional and cognitive control required to execute and maintain covert activities while committing these acts. The serious emotional and cognitive symptoms associated with these disorders would, it has been argued, "screen-out" candidates for this stressful activity and lifestyle. However, the espionage cases included in our sample indicate that that these disorders may play a role in a limited number of cases, especially if addictive disorders are included in this category of personal predisposition. Examples of evidence of the presence of serious mental health disorders from our espionage sample included Ames's and Walker's alcoholism; Regan's reported prescriptions for anti-psychotics, Prozac, and his alcohol abuse; and Smith's reported alcoholism and need for mental health treatment. It should be noted that the use of information technology by many of these spies may have simplified the processes and requirements to commit these acts. In addition, whether the presence of a major mental health disorder impacts discovery of espionage is also an independent function of the sensitivity of the organization involved to the insider's behavior.

## PERSONALITY PROBLEMS

This category includes self-esteem deficits and patterns of biased perceptions of self and others that impact personal and professional decision making in consistently maladaptive ways for the individual. This includes classic Axis II personality disorders [APA 1994], problems with self-esteem that produce compensatory behaviors and reactivity, problems with impulse control, a sense of entitlement, and other personal characteristics that result in consistent maladaptive judgment and behavior. Specific observables of these characteristics in our sabotage and espionage samples have included

- extreme sensitivity to criticism
- unusual needs for attention
- chronic frustration and feeling unappreciated
- difficulties controlling anger with bursts of inappropriate temper
- chronic sense of victimization or mistreatment
- chronic grudges against others
- belief, and conduct, reflecting the sense that the insider is above the rules applicable to others due to special characteristics or suffering
- chronic interpersonal problems and conflicts (including physical conflicts) such that the insider is avoided by others or they “walk on eggshells” around him or her
- compensatory behaviors reflecting underlying self-esteem problems such as bragging, bullying, spending on fantasy-related items
- chronic difficulties dealing with life challenges indicating an inability to realistically assess his or her strengths, limitations, resources—overspending, overestimating his abilities and underestimating others, attempting to gain positions for which he or she clearly lacks training or qualifications
- use of compartmentalization such that the insider has no problems living with contradictions between his maladaptive behavior and espoused beliefs (an allegedly religious individual who cheats on his wife or expenses)
- lack of inhibitory capabilities such as a conscience, impulse control, empathy for others, comprehension of the impact of actions on others, or any regard for the feelings of others such that the insider is chronically offending or exploiting those around him or her

Specific examples of personality-related observable behaviors exhibited by IT saboteurs included

- bullying
- chronic insecurity
- intimidation of others
- refusal to conform to rules
- chronic complaining
- chronic disregard for, and manipulation of, the office policies and practices
- threatening the life of those opposing him
- stealing items from work
- admitted theft of computer equipment
- access from a new employer’s system without displaying remorse
- withholding of information from team members
- intimidation of team members to the extent they were fearful for their safety

Examples of such individuals from the espionage cases include Ames, who according to a consulting psychologist familiar with the case, suffered from a narcissistic personality disorder that lead him to “believe he was bulletproof”; Hanssen, who was socially isolated and had personality and physical conflicts with others and lacked a conscience; and Hoffman, who felt above the rules regarding conflicts of interest and use of company property and intellectual property.

### SOCIAL SKILLS AND DECISION-MAKING DEFICITS

This refers to chronic problems getting along and working with others, due to active social tension or conflict attributable to the insider or active withdrawal from contact on the insider’s part. While social skills deficits are often associated with mental health and personality problems (see sections above), there were cases in which evidence of the presence of these disorders was not available while data on the social skills and decision-making deficits appeared. For example, there were insiders who displayed social skills deficits without displaying these more serious underlying personality issues (for example, outwardly charming but manipulative sociopaths who appeared “normal”). In addition, there were insiders with mental health and personality problems that did not manifest social skills or decision-making problems due to the isolated nature of their work environment or the extreme tolerance of supervisors and/or peers. Risk-related behaviors by insiders in this category ranged from extreme shyness and avoidance of others to bullying, exploitation, and ruthless manipulation of others.

Example behaviors from the sabotage case files included

- chronic conflicts with fellow workers, supervisors, and security personnel
- bullying and intimidation of fellow workers
- refusal to confront supervisors with legitimate work-related complaints due to shyness while complaining to competitors
- serious personality conflicts
- unprofessional behavior
- personal hygiene problems
- inability to conform to rules

From the espionage cases, Hanssen, Ames, Regan, and Peri all displayed social skills deficits ranging from withdrawal to bullying.

### HISTORY OF RULE VIOLATIONS

Insiders in both domains (IT sabotage and espionage) had a record of breaking rules ranging from prosecuted legal violations and convictions to violations of security regulations to participation in financial conflicts of interest. Within this range, a history of hacking, petty theft, misuse of organization property or resources, falsifying official information, or violation of policies or practices was included. For example, 30% of the IT sabotage insiders in the *Insider Threat Study* had prior criminal violations. Among espionage cases, Ames (loss of classified documents, alcohol use), Hanssen (misuse of government funds on travel), and Hoffman (misuse of company resources) violated legal and security guidelines prior to (and during) their espionage activities.

| **Insider Personal Predisposition** | **Definition** | **Observables** | **Sabotage Cases (Case Numbers)** | **Espionage Cases** |
|---|---|---|---|---|
| Serious mental health disorder | A diagnosed mental health problem for which treatment was recommended prior to legal proceedings or for which symptoms and the need for treatment were noticed by multiple peers, supervisors, or others with first-hand knowledge; determination made by clinical psychologist trained in remote assessment. | Addiction or behaviors that impair professional abilities resulting in intervention or sanctions; psychiatric medications are being taken; psychological treatment is recommended or administered; insider complains to others of psychological symptoms, symptoms are noticeable by peers (absenteeism, mood, concentration problems); legal problems related to disorder (driving while intoxicated, arrests, debt). | 11<br>3<br>22<br>23 | Ames<br>Smith<br>Regan<br>Anderson |
| Personality problems that result in biased perceptions of self and others | There are consistent interpersonal problems generated mainly by insider's perceptions of self and others; insider displays consistent sensitivity to criticism, frustration, propensity for impulsive behaviors, vulnerability to feeling victimized and/or entitled to special treatment; peers and supervisors walk on eggshells, avoid him or her. Defenses may include dangerous compensatory fantasies like revenge, spying. | Unusual needs for attention, sense of entitlement such that he is above the rules, chronic dissatisfaction with aspects of job or personal feedback, forms grudges, feels unappreciated, unrealistic expectations of others, arrogance, personal conflicts, fearful of usually routine experiences, compensatory behaviors designed to enhance self-esteem (spending, bragging, bullying). May or may not manifest in flagrant social skills problems (vs. withdrawal). | 27<br>25<br>26<br>11<br>3<br>22<br>23 | Regan<br>Hanssen<br>Ames<br>Smith<br>Hanssen<br>Anderson<br>Hoffman |

| | | | | |
|---|---|---|---|---|
| Social skills and decision-making deficits | Problems relating to others, especially appreciating interpersonal consequences of actions, controlling actions that lead to social exclusion, alienation or intimidation of others; lack of assertiveness that results in non-adaptive reactions to professional stress or setbacks, emotional and/or physical conflicts with others, rule violations. Lack of conscience, common sense judgment, empathy for others, control of impulses, loyalty or other “brakes” on behavior damaging to self and others. | Isolation from the group, propensity for interpersonal conflicts with supervisors, lack of expected professional advancement, frequent transfers, avoidance by peers, stereotyping (geek, loser, weird), scapegoating/bullying, misinterpretation of social cues. With lack of impulse control and/or conscience, chronic rule violations as in sociopathy. | 11<br>3<br>22<br>23<br>27<br>25<br>26 | Regan<br>Peri<br>Hanssen<br>Ames<br>Smith<br>Anderson |
| History of legal, security or procedural rule violations prior to attack | Prior criminal offenses, hacking, security violations, self-serving conflicts of interest or activities indicating a serious disregard for important social rules and expectations. | Arrests, hacking, security violations, harassment or conflicts resulting in official sanctions or complaints, misuse of travel, time, expenses. | 11<br>3<br>22<br>23<br>27<br>25<br>26 | Ames<br>Hanssen<br>Hoffman<br>Aragoncillo |

# Appendix H: Espionage Case Summaries

With the exception of the Aragoncillo case, the following summaries were taken directly from the PERSEREC report *ESPIONAGE CASES 1975-2004, Summaries and Sources* [PERSEREC 2004].

**AMES**, **ALDRICH HAZEN**, CIA intelligence officer and his Colombian-born wife **MARIA DEL ROSARIO CASAS AMES**, were arrested 21 February 1994, after various attempts since 1985 to identify a mole in the CIA. The arrests followed a ten-month investigation that focused on Rick Ames. He was charged with providing highly classified information to the Soviet KGB and later, to its successor, the Russian SVR, over a nine-year period. From 1983 to 1985, Ames had been assigned to the counterintelligence unit in the agency's Soviet/East European Division, where he was responsible for directing the analysis of Soviet intelligence operations. In this capacity he would have known about any penetration of the Soviet military or the KGB. According to press reports, the trail that led to the arrest of Ames and his wife began in 1987 after the unexplained disappearance or deaths of numerous U.S. intelligence sources overseas. According to court documents, Ames's information allowed the Russians to close down at least 100 intelligence operations and led to the execution of the agents in Russia that he betrayed. Despite reports of alcohol abuse, sexual misconduct, and repeated security violations, Ames was promoted into positions at the CIA that allowed him to steal increasingly sensitive information while he was spying for the Soviets. Facing alimony payments and the financial demands of his new wife, Rosario, in April 1985 Ames decided to get money by volunteering to spy for the Russians. He first contacted the KGB by dropping a note at the Soviet Embassy. Over his nine years of espionage activity, he removed bags of documents from CIA facilities, without challenge, and deposited them at dead drops around Washington or met his handlers at meetings around the world. Ames reportedly received up to $2.5 million from the Russians over this period of time. Reports of the couple's high-rolling life style included the cash purchase of a half-million dollar home, credit card bills of $455,000, and a new Jaguar sports car. But despite his unexplained affluence, Ames's story that his wife had wealthy relatives in Colombia satisfied doubts about his income for years, until a CIA counterintelligence investigator finally checked the cover story with sources in Colombia. A search of Ames's office uncovered 144 classified intelligence reports not related to his current assignment in CIA's Counternarcotics Center. The Director of Central Intelligence reported to Congress that Ames's espionage caused "severe, wide-ranging, and continuing damage to U.S. national security interests," making Ames one of the most damaging spies in U.S. history. He provided the Soviets, and later the Russians, with the identities of ten US clandestine agents (at least nine of whom were executed), the identities of many U.S. agents run against the Russians, methods of double agent operations and communications, details on U.S. counterintelligence operations, identities of CIA and other intelligence personnel, technical collection activities, analytic techniques, and intelligence reports, arms control papers, and the cable traffic of several federal departments. On 28 April 1994, Aldrich Ames and his wife pleaded guilty to conspiring to commit espionage and to evading taxes. Ames was immediately sentenced to life imprisonment without parole. Under a plea agreement, Maria Rosario Ames was sentenced to five years and three months in prison for conspiring to commit espionage and evading taxes on $2.5 million obtained by her husband for his illegal activities.

*New York Times* 22 Feb 1994, “Ex-Branch Leader of C.I.A. is Charged as a Russian Agent”

*Washington Post* 23 Feb 1994, “CIA Officer Charged With Selling Secrets”

25 Feb 1994, “Accused Couple Came From Different Worlds”

27 Dec 1994, “Ames says CIA Does Not Believe He Has Told All”

11 Jun 1995, “The Man Who Sold the Secrets”

*Los Angeles Times* 22 Oct 1994, "Wife of CIA Double Agent Sentenced to 5 Years in Prison"

U.S. Senate Select Committee on Intelligence, 1 Nov 1994, “An Assessment of the Aldrich H. Ames Espionage Case and Its Implications for U.S. Intelligence”

**ANDERSON, RYAN GILBERT,** 26, a Specialist and tank crewman in the Washington National Guard, was arrested on 12 February 2004, and charged with five counts of attempting to provide aid and information to the enemy, Al Qaeda. Anderson converted from his Lutheran upbringing to Islam while attending Washington State University where he studied Middle Eastern military history and graduated with a B.A. in 2002. In late 2003, as his National Guard unit was preparing to deploy to the war in Iraq, Anderson went onto Internet chat rooms and sent emails trying to make contact with Al Qaeda cells in the United States. His emails were noticed by an amateur anti-terrorist Internet monitor, Shannen Rossmiller, a city judge in Montana who had begun monitoring Islamist Jihad websites in an effort to contribute to homeland defense after the 9/11 attacks. After she identified him by tracing his Arab pseudonym, Amir Abdul Rashid, Rossmiller passed along to the FBI her suspicions about Anderson. In a joint DOJ and FBI sting operation conducted in late January 2004, Anderson was videotaped offering to persons he thought were Al Qaeda operatives, sketches of M1A1 and M1A2 tanks, a computer disk with his identifying information and photo, and information about Army weapons systems, including "the exact caliber of round needed to penetrate the windshield and kill the driver of an up-armored Humvee." At his Army court martial the defense argued that Anderson suffered from various mental conditions including bipolar disorder and a high-performing type of autism, which led to role playing, exaggeration of his abilities, and repeated attempts to gain social acceptance. The prosecution argued that what he did constituted treason. The court martial convicted Anderson on all five counts and on 3 September 2004, sentenced him to life in prison with the possibility of parole, demotion to the rank of private, and a dishonorable discharge.

---

*New York Times* 13 Feb 2004, "Guardsman Taken Into Custody and Examined for Qaeda Tie" 4 Sep 2004, "Guardsman Given Life in Prison for Trying to Help Al Qaeda"

*New York Post* 12 Jul 2004, "Lady Who 'Nets Spies'"

*Seattle Times* 31 Aug 2004, "Guardsman Anderson Accused of 'Betrayal' as Court Martial Begins"

*Seattle Post Intelligencer* 2 Sep 2004, "Accused GI Called Bipolar, 'Social Misfit'"

---

**ARAGONCILLO, LEANDRO,** a naturalized citizen of Filipino descent, served as a military security official for the Vice President of the United States at the White House. Aragoncillo established a close relationship with the former President of the Philippines, Joseph Estrada, visiting the presidential palace with his wife and traveling to the Philippines to visit Estrada in the hospital. This behavior should have alerted his superiors, but it did not, presumably because they were not sufficiently monitoring and auditing behavioral indicators.

Aragoncillo was not authorized to view, access, download, or print information related to the Philippines—he had no need to know. However, this lack of authorization was not enforced via access controls. Therefore, he was able to search the FBI's Automated Case Support (ACS) system for keywords related to the Philippines for at least seven months. Although his actions were logged, they were not reviewed during that period. As a result, he was able to use his access to print or download 101 classified documents pertaining to the Philippines from the ACS system and transmit the information to high-level officials in the Philippines via personal email accounts.

When Aragoncillo attempted to intervene on behalf of an accomplice who was arrested by Immigration and Customs Enforcement (ICE) agents for exceeding his tourist visa, his behavior exceeded a threshold that finally raised his superiors' perceived risk of espionage. They increased auditing and monitoring and discovered his illicit activity. Specifically, they caught him copying classified information to a disk and taking the disk home in his personal bag.

This case illustrates how easy it can be for a spy to commit acts of espionage if access controls are not used to enforce authorization levels. In addition, it shows how insufficient monitoring and auditing enabled a spy to perform actions over a long period that, even at a cursory glance, would have been obviously unauthorized and suspicious.

**HANSSEN**, **ROBERT PHILIP**, an agent for the FBI for 27 years, was charged on 20 February 2001 with spying for Russia for more than 15 years. He was arrested in a park near his home in Vienna, Virginia, as he dropped off a bag containing seven Secret documents at a covert location. For most of his FBI career, Hanssen had worked in counterintelligence, and he made use of what he learned in his own espionage career. He was charged with espionage and conspiracy to commit espionage. Specifically, Hanssen provided first the Soviets and then the Russian government over 6,000 pages of classified documents and the identities of three Russian agents working for the United States. Two of these sources were tried in Russia and executed. According to court documents, the FBI employee provided information on "some of the most sensitive and highly compartmented projects in the U.S. intelligence community" as well as details on U.S. nuclear war defenses. In return, the Russians paid him $1.4 million over the period of his espionage activities, including over $600,000 in cash and diamonds and $800,000 deposited in a Russian bank account. Hanssen was identified after the United States obtained his file from a covert source in the Russian intelligence service. However, the Russians never knew Hanssen's true name. To them, he was known only as "Ramon" or "Garcia." It is believed that Hanssen was involved with the Soviets beginning in 1979, broke off the relationship in 1980, but again volunteered to engage in espionage in 1985 by sending an unsigned letter to a KGB officer in the Soviet Embassy in Washington. The letter included the names of the three Soviet double-agents working in the United States. Although Hanssen's motives are unclear, they seem to have included ego gratification, disgruntlement with his job at the FBI, and a need for money. He and his wife struggled to provide for his large family on an agent's salary and by 1992 had incurred debts of over $275,000. Hanssen exploited the FBI's computer systems for classified information to sell and kept tabs on possible investigations of himself by accessing FBI computer files. Friends and coworkers were at a loss to explain how this supposedly deeply religious father of six and ardent anti-communist could have been leading a double life. A large part of his illegal income is believed to have been used to buy expensive gifts and a car for a local stripper. In July 2001, a plea agreement was reached by which Hanssen would plead guilty to espionage, fully cooperate with investigators, but avoid the death penalty. On 11 May 2002, the former FBI agent was sentenced to life in prison.

---

*New York Times* 21 Feb 2001, "F.B.I. Agent Charged as Spy Who Aided Russia for 15 Years"

*Washington Post* 25 Feb 2001, "A Question of Why," Contradictory Portrait Emerges of Spying Suspect"

*Washington Post* 6 Jan 2002, "From Russia With Love"

*Los Angeles Times* 7 May 2002, "U.S. Authorities Question FBI Spy's Candor"

---

**HOFFMAN**, **RONALD**, was working as a general manager at Science Applications International Corporation (SAIC), in Century City, California, when his dissatisfaction with his salary led him to create a sideline business called "Plume Technology" at home. Hoffman had worked on a software program called CONTAM, developed at SAIC under classified contract for the Air Force, which could classify rockets upon launch from their exhaust contrails and respond with appropriate countermeasures. The software also had application for the design of spacecraft, guided missiles, and launch vehicles. In 1986 he contacted Japanese companies working with Japan's space program and offered to sell them entire CONTAM modules—"data, components and systems, expertise in the field, and training for employees in use of the system." Four Japanese companies, including Nissan and Mitsubishi, bought the classified software from Hoffman for undercover payments that totaled over $750,000. Hoffman also tried to develop customers in Germany, Italy, Israel, and South Africa. Late in 1989, his secretary at SAIC noticed a fax addressed to Hoffman from Mitsubishi that asked for confirmation that their payment into his account had been received. Adding this to her knowledge of Hoffman's lavish lifestyle, she took her suspicions and a copy of the fax to SAIC's chief counsel. Confronted, Hoffman resigned on the spot and left, but returned to his office during the night when a security video camera captured him carrying out boxes of CONTAM documents. In a joint Customs and Air Force sting operation, investigators posed as South African buyers and documented Hoffman trying to sell them CONTAM modules without an export license. Hoffman was arrested 14 June 1990 and convicted early in 1992 of violations of the Arms Export Control Act and the Comprehensive Anti-Apartheid Act. He was sentenced on 20 April 1992 to 30 months in prison and fined $250,000.

---

Steven J. Bosseler Affidavit, U.S. District Court, "U.S. v. Ronald Hoffman," June 15, 1990.

U.S. v. Hoffman 10 F 3d 808 (9th Cir. 1993).

Chicago Tribune 22 Apr 1992, "U.S. Scientist Faces Jail in Sale of Star Wars Software"

---

**MONTES**, **ANA BELEN**, a senior intelligence analyst at the Defense Intelligence Agency, transmitted sensitive and classified military and intelligence information to Cuba for at least 16 years before she was arrested on 21 September 2001. Surveillance on her activities was curtailed in response to the terrorist attacks of 11 September 2001 and concern that Cuba could pass on intelligence to other nations. Montes was 44, unmarried, and a U.S. citizen of Puerto Rican descent. She was employed by the Justice Department when sometime before 1985 she began working with the Cuban Directorate of Intelligence—it has not been revealed whether she volunteered or was recruited by them. They encouraged her to seek a position with better access to information, and in 1985 she transferred to a job at DIA. From her office at Bolling AFB in Washington, DC, she focused on Latin American military intelligence. In 1992, she shifted from her initial work on Nicaragua and became the senior DIA analyst for Cuba. She passed at least one polygraph test while engaged in espionage. Montes met her Cuban handlers every three or four months either in the United States or in Cuba to exchange encrypted disks of information or instructions. The Cubans also kept in contact through encrypted high-frequency radio bursts that she received on a short-wave radio. She would enter the sequences of coded numbers coming from the radio into her laptop computer, and then apply a decryption disk to them to read the messages. She used pay phones on Washington street corners to send back encrypted number sequences to pager numbers answered by Cuban officials at the United Nations. By not following their strict instructions on how to remove all traces of the messages from her computer hard disk, Montes left behind evidence of her activities. Over her years of espionage, she gave the Cubans the names of four U.S. military intelligence agents (they escaped harm), details on at least one special access program, defense contingency planning for Cuba, and aerial surveillance photos. She had access to Intelink and the information contributed to that network by 60 agencies and departments of the Federal government. Montes cooperated in debriefings by various intelligence agencies in a plea agreement to reduce her sentence. Her lawyers claimed she spied from sympathy toward Cuba and that she received no money for her espionage other than travel expenses and the cost of her laptop. She was sentenced on 16 October 2002 to 25 years in prison and five years' probation. At the sentencing hearing she made a defiantly unrepentant statement condemning U.S. policy towards Cuba. The judge responded that she had betrayed her family and her country and told her "If you cannot love your country, you should at least do it no harm."

---

*New York Times* 30 Sep 2001, "Intelligence Analyst Charged With Spying for Cuba"

*Miami Herald* 21 Mar 2001, "To Catch a Spy"

*Miami Herald* 28 Mar 2001, "Cuban Spy Passed Polygraph at Least Once"

*Miami Herald* 16 Jun 2002, "She Led Two Lives—Dutiful Analyst, and Spy for Cuba"

*New York Times* 17 Oct 2002, "Ex-U.S. Aide Sentenced to 25 Years for Spying for Cuba"

---

**PERI**, **MICHAEL A**., 22, an electronic warfare signals specialist for the Army, fled to East Germany with a laptop computer and military secrets on 20 February and voluntarily returned 4 March 1989 to plead guilty to espionage. He was sentenced to 30 years in a military prison. Even after his court-martial, authorities were at a loss to explain what had happened. Peri said he made an impulsive mistake, that he felt overworked and unappreciated in his job for the 11th Armored Cavalry Regiment in Fulda, West Germany. His work involved operating equipment that detects enemy radar and other signals. Peri had been described as "a good, clean-cut soldier" with a "perfect record." During his tour of duty in Germany he had been promoted and twice was nominated for a soldier of the month award.

---

*Los Angeles Times* 29 Jun 1989, "From Soldier to Spy; A Baffling About-Face"

*St. Louis Post-Dispatch* 25 Jun 1989, "U.S. Soldier Given 30 Years"

---

**REGAN**, **BRIAN PATRICK**, a former Air Force intelligence analyst, was arrested on 3 August 2001 at Dulles International Airport as he was boarding a flight for Switzerland. On his person he was carrying missile site information on Iraq and contact information for embassies in Switzerland. Regan, who had enlisted in the Air Force at 17, began working for the National Reconnaissance Office (NRO) in 1995 where he administered the Intelink, a classified Web network for the intelligence community. Following his retirement from the military as a Master Sergeant in 2001, he was employed by defense contractor TRW and resumed work at NRO where he was employed at the time of his arrest. Regan had held a Top Secret clearance since 1980. Computers searched in Regan's home led to the discovery of letters offering to sell secrets to Libya, Iraq, and China. In the Iraq case, he asked Saddam Hussein for $13 million. At his arraignment on 5 November 2001, he pleaded not guilty to three counts of attempting to market highly classified documents and one count of gathering national defense information. The documents, classified at the Top Secret SCI level, concerned the U.S. satellite program, early warning systems, and communications intelligence information. Regan is thought to have been motivated not only by money (he had very heavy personal debts), but also by a sense of disgruntlement, complaining frequently to former coworkers and neighbors about his job and station in life. On 20 February 2003, Regan was convicted of all charges except attempting to sell secrets to Libya, and on 21 March, under a sentencing agreement, he was sentenced to life imprisonment without parole. Information provided by Regan after sentencing led FBI and NRO investigators to 19 sites in rural Virginia and Maryland where he had buried over 20,000 pages of classified documents, five CDs, and five videotapes that he had stashed presumably for future sales.

---

Washington Post 24 Aug 2001, "Retired Air Force Sgt. Charged With Espionage"

*Washington Post* 21 Feb 2003, "Analyst Convicted in Spy Case; Regan Jury Yet to Decide if Death Penalty Applies"

*New York Times* 21 Mar 2003, "Life Sentence for Bid to Sell Secrets to Iraq"

*Los Angeles Times* 31 Jul 2003, "Arduous Dig to Find Spy's Buried Stash; Agents Search Virginia, Maryland Park Sites Under Rough Conditions, Recover All Documents"

---

**SMITH**, **TIMOTHY STEVEN**, 37, was a civilian serving as an ordinary seaman on the *USS Kilauea*, an ammunition and supply vessel attached to the Pacific Fleet. On 1 April 2000, while the ship was moored at the Bremerton Naval Station in Bremerton, Washington, Smith was surprised by an officer when removing computer disks from a desk drawer. After a scuffle, Smith was subdued and 17 disks were retrieved from his clothing. A search of his quarters found five stolen documents marked “Confidential,” including one describing the transfer of ammunition and handling of torpedoes on U.S. Navy vessels. Charged initially in U.S. District Court in Tacoma, WA, with two counts of espionage and two counts of theft and resisting arrest, investigation showed that Smith needed mental treatment and had a severe alcohol problem. He told FBI agents that he “wanted to get back at the crew” for their mistreatment of him and that, in order to get revenge, he had tried to steal “valuable classified materials” because “if I got something valuable, then I could turn my life around.” To sell his cache, he thought he might “go online and solicit buyers from terrorist groups.” Smith pled guilty after prosecutors dropped espionage charges. In a plea agreement reached in August 2000, he pleaded guilty to one count of stealing government property and one count of assaulting an officer. He was sentenced in December 2000 to 260 days’ confinement (to include time served) and was released on 22 December 2000.

---

*Seattle Post-Intelligencer* 14 Apr 2000, “Seaman Admits Stealing Defense Secrets, FBI Says”

*National Counter Intelligence Executive - News and Developments*, Vol. 1, March 2001

---

# Appendix I: Glossary

Terms are grouped and ordered so that their definitions flow logically, rather than alphabetically.

**Insider IT Sabotage**
Malicious activity in which the insider's primary goal was to sabotage some aspect of an organization or to direct specific harm toward an individual(s).

**Spy**
Insider who commits or attempts to commit espionage.

**Saboteur**
Insider who commits or attempts to commit IT sabotage.

**Insiders**
Spies and saboteurs.

**Behavioral**
Involves personal or interpersonal behaviors.

**Technical**
Involves the use of a computer or electronic media.

**Concerning behavior**
Behavior that should raise concern about an individual's reliability or trustworthiness (e.g., excessive drinking during lunch).

**Concerning technical action**
Technical action that should raise concern about an individual's reliability or trustworthiness. All concerning technical actions are technical indicators (e.g., creating backdoor account).

**Indicator**
An event, condition, or action that indicates increased risk.

**Behavioral Indicator**
A behavioral event, condition, or action that indicates increased risk (e.g., intoxication during working hours).

**Technical Indicator**
A technical event, condition, or action that indicates increased risk (e.g., account audit reveals unauthorized account).

**Harmful Action**
An action taken that harms an organization.

**Harmful Behavioral Action**
A behavior that harms an organization or person (e.g., inappropriate transferring of classified information).

**Harmful Technical Action**
A technical action taken that harms an organization or person (e.g., deleting files and sabotaging backups).

**Rule Violation**
An action that violates a law or organizational policy.

**Behavioral Rule Violation**
A behavior that violates a law or organizational policy (e.g., frequent unexplained absence from work).

**Technical Rule Violation**
A technical action that violates a law or organizational policy (e.g., violation of acceptable computer use policy).

**Observables**
Specific events, conditions, or actions that could have been observed in the cases examined.

# REPORT DOCUMENTATION PAGE

*Form Approved*
*OMB No. 0704-0188*



| | | |
|---|---|---|
| 1. **AGENCY USE ONLY**<br>(Leave Blank) | 2. **REPORT DATE**<br>December 2006 | 3. **REPORT TYPE AND DATES COVERED**<br>Final |

4. **TITLE AND SUBTITLE**
Comparing Insider IT Sabotage and Espionage: A Model-Based Analysis

5. **FUNDING NUMBERS**
FA8721-05-C-0003

6. **AUTHOR(S)**
Stephen R. Band, Ph.D; Dawn M. Cappelli; Lynn F. Fischer, Ph.D; Andrew P. Moore; Eric D. Shaw, Ph.D., Randall F. Trzeciak

7. **PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)**
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

8. **PERFORMING ORGANIZATION REPORT NUMBER**
CMU/SEI-2006-TR-026

9. **SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)**
HQ ESC/XPK
5 Eglin Street
Hanscom AFB, MA 01731-2116

10. **SPONSORING/MONITORING AGENCY REPORT NUMBER**
ESC-TR-2006-091

11. **SUPPLEMENTARY NOTES**

12A **DISTRIBUTION/AVAILABILITY STATEMENT**
Unclassified/Unlimited, DTIC, NTIS

12B **DISTRIBUTION CODE**

13. **ABSTRACT (MAXIMUM 200 WORDS)**

This report examines the psychological, technical, organizational, and contextual factors thought to contribute to at least two forms of insider trust betrayal: insider sabotage against critical information technology (IT) systems, and espionage. Security professionals and policy leaders currently view espionage and insider threat as serious problems but often as separate issues that should be each addressed by a different configuration of security countermeasures. In this study, researchers investigated similarities and differences between insider IT sabotage and espionage cases to isolate the major factors or conditions leading to both categories of trust betrayal. The team developed a descriptive model using the system dynamics methodology that represents the high-level commonalities between the two domains based on models of the individual domains.

The effort found definite parallels between the two categories of trust betrayal. Factors observed in both saboteurs and spies include the contribution of personal predispositions and stressful events to the risk of an insider committing malicious acts; the exhibition of behaviors and technical actions of concern by the insider preceding or during an attack; the failure of their organizations to detect or respond to rule violations; and the insufficiency of the organization's physical and electronic access controls. Based on the study's findings and analysis, recommendations and policy implications are also presented.

14. **SUBJECT TERMS**
espionage, insider IT sabotage, employee auditing, employee monitoring, espionage model, sabotage model, technical observables, personal predispositions, malicious acts

15. **NUMBER OF PAGES**
110

16. **PRICE CODE**

| | | | |
|---|---|---|---|
| 17. **SECURITY CLASSIFICATION OF REPORT**<br>Unclassified | 18. **SECURITY CLASSIFICATION OF THIS PAGE**<br>Unclassified | 19. **SECURITY CLASSIFICATION OF ABSTRACT**<br>Unclassified | 20. **LIMITATION OF ABSTRACT**<br>UL |

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89) Prescribed by ANSI Std. Z39-18
298-102