



# **UNIVERSITY OF NAIROBI**

## **SCHOOL OF COMPUTING AND INFORMATICS**

### **MODELING AND SIMULATING INSIDER CYBER SECURITY THREATS USING PSYCHOSOCIAL FACTORS**

By

MARK MBOCK OGONJI

REG.NO. P58/63163/2011

SUPERVISOR

PROF. WILLIAM OKELO ODONGO

*Submitted in partial fulfillment for the requirements of Master of Science in Computer Science of  
the University of Nairobi*

**OCTOBER, 2013**

## Declaration

This is to certify that this report which is submitted by me to the University of Nairobi School of Computing and Informatics, Chiromo Campus in partial fulfillment of the requirement for the award of degree of Master of Science in Computer Science comprises only my original work and due acknowledgement has been made in the text to all other material used.

Date:.....

Student Sign:.....

**Name: Ogonji Mark Mbock**

**Registration Number: P58/63163/2011**

This is to certify that this report which is submitted by **Mr. Ogonji Mark Mbock** in partial fulfillment of the requirement for the award of degree in Master of Science in Computer Science of the University of Nairobi School of Computing and Informatics, Chiromo campus is a record of the candidate's own work carried out by him under my supervision. The matter embodied in this research is original and has not been submitted for the award of any other degree.

Date:.....

Supervisor Sign:.....

**Name: Prof. William Okelo Odongo**

## **Abstract**

Insider threat is rapidly becoming the largest information security problem that organizations face. The Government and the private sector have made technology adoption their central focus over the last couple of years. The investment in technology as well as improvement in the telecommunications infrastructure has led to tremendous growth in Internet usage, but with insufficient attention being given to securing the cyberspace. With granted access to internal systems, it is becoming increasingly harder to protect organizations from malicious insiders. The typical methods of mitigating insider threat are simply not working, primarily because insider threat is a people problem and most mitigation strategies are geared towards profiling and anomaly detection which are problematic at best. As a result, a new type of model is proposed here, one that incorporates risk management with human behavioral science.

The new insider threat prediction model focuses on observable influences that affect employees and identifies employees with increased risk of becoming malicious insiders. This research details the need for the model, the model's components and how it works. The model is tested using psychosocial factors as derived from case studies that indicate an individual's predisposition to malicious activities.

The model's main purpose is the differentiation of malicious and non-malicious employees. Implemented with the right tool, the new model has great potential for use by security personnel in their efforts to mitigate insider threat damage. It can also be used by HR personnel in their desire to monitor and track employee behavior that is likely to lead to harm to organization systems.

The researcher reviewed literature on insider cyber threats by covering the insider cyber security threat concept. The concept addressed who an insider is with emphasis given to trusted employees with legitimate access. Through literature review, the researcher was able to identify existing approaches that have been developed to address insider threat issues. Some of the approaches include Counter-productive Work Behavior (CWB), Schematic Protection Model and agent-based user profiling model.

The researcher then developed a conceptual framework to guide the study. The Model-Based Predictive Conceptual Framework comprises a knowledge base of indicators which has processes ranging from data to observations and finally behaviors. The framework requires data which is processed to infer observations, while observations are processed to infer indicators and finally indicators are processed to infer behavior.

The researcher used a hybrid of the system dynamics and agent-based modeling technique to simulate insider cyber threats. The psychosocial indicators identified during literature review were the input variables that were given weights based on their influence on human behavior.

The study underscored the fact that employee disgruntlement was a recurring factor in all the cases. For example, one's previous behavior had an effect on their current behavior, while expectations of recognition would affect where an individual if they are denied promotion or some perceived entitlement.

The evaluation of the data collected showed that men contributed approximately 67.65% of the insider cyber threat cases with women standing at 32.35% of the total sampled data.

From the study, it can be stated that the Insider Threat Prediction Model (ITPM) is a useful tool for any security practitioner and HR or management personnel for identifying at risk employees and making useful remedial action before the concerning behavior becomes a threat to security.

The research provides a foundation for learning behavioral characteristics when hiring employees but also being able to continuously monitor employee behavior in order to stem possible disgruntlement or other concerning behaviors.

*Key Words:* **insider threats, system dynamics, psychosocial factors**

## **Dedication**

I dedicate this work to my late mum Mrs. Elizabeth Akinyi and my dad Mr. Pius Ogonji for their nurturing and support as well as inculcation of the need to acquire knowledge through education. I also dedicate this work to my wife Gladys, my son Ernie and daughter Flevian for their invaluable support during the entire course when I would be away for long hours.

## **Acknowledgement**

First and foremost, I would like to thank my supervisor Prof. Okello Odongo for his guidance, support and dedication during the period I undertook the project. He was insightful and thorough in his assessment of my work and provided direction throughout the research period. I would also like to thank members of my panel led by Mr. Erick Ayienga, Dr. Muthoni Masinde and Dr. Elisha Abade for giving feedback and direction during the presentation of each milestone.

I would especially like to thank Dr. Elisha Opiyo for taking time out of his busy schedule to provide valuable input during the initial stages of my research particularly his knowledge in agent modeling was quite useful.

Last but not least, I wish to thank my family for their support and patience whenever I would be engaged in the research.

## Table of Contents

Abstract.....	iii
Dedication.....	v
Acknowledgement.....	vi
Table of Contents.....	vii
List of Figures.....	x
List of Tables.....	x
List of Abbreviations.....	xi
CHAPTER ONE: INTRODUCTION.....	1
1.0    Background.....	1
1.1    Problem Statement.....	2
1.2    Purpose.....	3
1.3    Research Objectives.....	3
1.4    Research Question.....	4
1.5    Scope.....	4
1.6    Significance of Study.....	4
1.7    Assumptions and Limitations.....	5
1.8    Project Deliverables.....	5
1.9    Chapter Summary.....	6
CHAPTER TWO: LITERATURE REVIEW.....	7
2.0    Introduction.....	7
2.1    Insider Cyber Security Threat Concept.....	7
2.2    Insider Threat Approaches.....	8
2.3    Conceptual Model.....	11
2.4    The Gap.....	13

2.5	Chapter Summary .....	13
CHAPTER THREE: RESEARCH METHODOLOGY.....		14
3.1	Introduction.....	14
3.2	Target Population and Sampling Technique .....	14
3.3	Sampling Design.....	15
3.4	Research Instruments .....	15
3.4.1	Questionnaires.....	15
3.4.2	Personal Interviews.....	16
3.4.3	Case Study Methodology.....	16
3.5	Coding Methodology .....	16
3.6	Modeling Technique .....	17
3.6.1	Agent Based Model.....	17
3.6.2	System Dynamics Model .....	20
3.6.3	Psychosocial Model .....	24
3.7	Modeling Process.....	27
3.8	Modeling Notation .....	28
3.9	Modeling Tool .....	30
3.10	Chapter Summary .....	31
CHAPTER 4: RESULTS AND DISCUSSION.....		32
4.1	Research Demographics.....	32
4.2	Insider Threat Prediction Model .....	35
4.3	Observation 1: Insider’s Intention.....	36
4.4	Observation 2: Insider’s Expectation of Freedom .....	40
4.5	Observation 3: Escalation of Disgruntlement and Sanctioning .....	42
4.6	Observation 4: Organizations Ignored or Failed to Detect Rule Violations .....	45



4.7	Validation of Predictive Model.....	48
4.8	Application.....	49
CHAPTER FIVE: CONCLUSIONS AND RECOMMENDATIONS .....		52
5.1	Achievements.....	52
5.2	Research Contribution.....	55
5.2.1	Model framework.....	55
5.2.2	Data sharing .....	57
5.2.3	Employee vetting, auditing and monitoring.....	57
5.2.4	Management training and awareness programs .....	58
5.3	Limitations of the Research .....	59
5.3.1	Lack of sufficient real-world data.....	59
5.3.2	Differences in expert judgment.....	59
5.3.3	False alerts .....	60
5.4	Research Conclusions .....	60
5.5	Further research .....	61
REFERENCES .....		63
APPENDIX I: STRUCTURE OF INSIDER THREAT DATABASE .....		66
APPENDIX II: QUESTIONNAIRE.....		71
APPENDIX III: MAPPING INSIDER CASES TO OBSERVATIONS.....		78
APPENDIX IV: CRITERIA FOR PERSONAL PREDISPOSITIONS.....		80
APPENDIX V: CASE SUMMARIES.....		87
APPENDIX VI: INSIDER THREAT PREDICTION MODEL.....		100

## List of Figures

<i>Figure 1: Multidisciplinary approach framework for mitigating insider threats (Butts, 2006)</i> .....	9
<i>Figure 2: Authentication system and agents interaction (Ali et al. ,2008)</i> .....	10
<i>Figure 3: Model-Based Predictive Conceptual Framework</i> .....	12
<i>Figure 4: Agent interaction</i> .....	18
<i>Figure 5: Model showing relationship within an organization</i> .....	19
<i>Figure 6: System Dynamics modeling principle</i> .....	21
<i>Figure 7: Insider Model Evolution Framework</i> .....	28
<i>Figure 8: System Dynamics Notation</i> .....	30
<i>Figure 9: Insider Intention Model</i> .....	38
<i>Figure 10: Agent based model</i> .....	39
<i>Figure 11: Expected freedom by Insider</i> .....	41
<i>Figure 12: Expectation escalation</i> .....	41
<i>Figure 13: Escalation of Disgruntlement and Sanctioning</i> .....	44
<i>Figure 14: Simulated escalation of disgruntlement and sanctioning</i> .....	44
<i>Figure 15: Organizations Ignored or Failed to Detect Rule Violations</i> .....	46
<i>Figure 16: Failure to recognize rule violations</i> .....	47
<i>Figure 17: Parameter variation experiment</i> .....	49
<i>Figure 18: High-level Structure of Insider Threat Database</i> .....	66
<i>Figure 19: Causal loop of the Insider Threat Prediction Model</i> .....	100

## List of Tables

<i>Table 1: Psychosocial indicators</i> .....	26
<i>Table 2: Distribution of research questions to respondents</i> .....	33
<i>Table 3: Sample demographics</i> .....	33
<i>Table 4: Components of an Incident</i> .....	34
<i>Table 5: Occurrence and weights of the psychosocial model</i> .....	36
<i>Table 6: Insider behavior distribution</i> .....	37
<i>Table 7: Organization information collected</i> .....	67
<i>Table 8: Subject information collected</i> .....	69
<i>Table 9: Incident Information Collected</i> .....	70
<i>Table 10: Observables mapped to cases</i> .....	79
<i>Table 11: Personal predispositions</i> .....	86
<i>Table 12: Summary of the Insider Cases</i> .....	99
<i>Table 13: Model Feedback Loops</i> .....	102

## List of Abbreviations

CCK.....	Communication Commission of Kenya
FBI.....	Federal Bureau of Investigation
HR.....	Human Resource
ICT.....	Information and Communications Technology
ITPM .....	Insider Threat Prediction Model
JWICS.....	Joint Worldwide Intelligence Communications System
KRA.....	Kenya Revenue Authority
MAMIT .....	Multidisciplinary Approach to Mitigating the Insider Threat
MERIT.....	Management and Education of the Risk of Insider Threat
SIPRNet .....	Secret Internet Protocol Router Network

## **CHAPTER ONE: INTRODUCTION**

### **1.0 Background**

Insiders by virtue of enjoying privileged access to organization information, and critical infrastructure pose the greatest danger to businesses. This has been accelerated by the use of and dependence on Information Technology which has exposed a number of organizations to premeditated attacks that are either externally or internally induced.

Globally, governments and organizations rely on networked information systems critical to their business operations, but which make them vulnerable to threats from employees (current and former), contractors, consultants and clients alike. This state of affairs is prevalent locally where organizations have automated their processes with focus being on technical security controls at the expense of other forms of controls to deter insider or external attacks.

While global trends indicate an increase in level of sophistication of attacks, the local conditions in Kenya are difficult to ascertain as there have been few studies on information security threats, attacks and mitigation measures. This means that attacks targeting organizations go undetected due to inadequate detection and prevention methods and tools.

Espionage and sabotage involving computer networks are among the most pressing cyber security challenges that threaten government and private sector information infrastructures. The insider threat is manifested when individuals fail to observe and comply with established policies. The types of crimes and abuse associated with insider threats include espionage, sabotage, terrorism, embezzlement, extortion, bribery, and corruption. However, malicious activities include an even broader range of exploits, such as copyright violations, negligent use of classified data, fraud, unauthorized access to sensitive information, and illicit communications with unauthorized recipients.

According to the Communication Commission of Kenya (CCK), the country had an estimated 17.38 million Internet users as at December 2011 representing an increase of 95.63% from 8.8 million users in December 2010. This has seen a rise in Internet security incidents with most

organizations being targets of insider attacks (Kenya Cyber Security Report, 2012). Compounding this state of affairs is the ready availability of sophisticated attacker tools which make it easy for even inexperienced individuals to mount sophisticated attacks. Notable threats to government or corporate organization information assets include information leakage, fraud, espionage and sabotage that involve the use of computers and computer networks.

Several attempts have been made towards developing a framework for understanding and predicting insider threats. However, the lack of adequate real-world data about the insider threat (C. P. Pfleeger, 2008), has remained a challenge to most security practitioners, yet this is a serious problem in cyber and organizational security in general. It is also considered the most difficult problem to deal with because insiders often have information and capabilities not known to external attackers, and as a consequence can cause serious harm.

The motivation behind this project is based on the fact that as the growth in Internet and other technologies increase, there is insufficient information on how insider behavior precipitates insider cyber-attacks whereas this phenomenon affects many organizations with serious consequences. This is aggravated by the limited understanding of the insider threat, due to the fact that organizations have not given this area due attention or have failed to recognize the threat insiders pose to systems.

## **1.1 Problem Statement**

As a number of key business functions continue being moved to Internet-based operations, organizations need to understand the security challenges posed by insiders who normally have legitimate access to systems. This is because the numbers of incidents where organizations have made huge losses as a result of insider malicious activities continue to rise while the activities may have been detected and prevented. The problem is worsened by the inability of HR personnel and security practitioners to predict malicious behavior before a compromise or attack occurs. Currently, there are no simple and agreed approaches for predicting insider threats before attacks begin, and no simple profiles on potential attackers (Randazzo et al., op. cit.). The

primary focus for most researchers has been improving anomaly detection efficiency without first determining how the insiders trigger anomalous actions (Brancik et al.).

The problem this research undertakes to investigate involves simulation of the problem of insider cyber threats by proposing a new model that applies the human behavior element to predict an employee's predisposition to being a malicious insider.

## **1.2 Purpose**

The goal of this study is to simulate the insider cyber security threats by examining whether human behavior influences or motivates malicious insiders to attack systems.

## **1.3 Research Objectives**

The objective of this project is to provide information security professionals, security agents and other law enforcement agencies with relevant knowledge and insight into psychosocial factors that influence individuals to attack systems, the internal checks and the interventions and mitigation measures employed. Through elaborate literature review and case study, this insight will contribute further to information systems security research.

The research project will therefore seek:

1. To identify psychosocial factors and determine their influence on human behavior. This will help determine the occurrence and weights associated with each indicator.
2. To create a model based on human behavior that provides indicators for potential risk for insider cyber threats. The simulation of the model will be done by inserting factors that influence and events that affect human behavior to identify employees with high risk of malicious attack.
3. To show that the model can differentiate between normal and malicious employee who has caused harm to an organization. The model together with an appropriate tool can be used to implement measures to mitigate insider cyber threats so as to reduce amount of damage done to critical systems.

## **1.4 Research Question**

The research questions below support the research problem and objective by acquiring knowledge from both scientific literature and case study. The scientific literature provides insight into the factors that motivate or trigger individuals to undertake insider attacks while the case study gives insight into the occurrence of the insider threat problem in practice.

Research Question 1: Which human behavioral factors have the most influence on the insider cyber threats to organization's systems? What is their level of influence?

Research Question 2: Is it possible to come up with a simulation model that can predict the insider cyber threat and differentiate normal from malicious behavior?

Research Question 3: How effective would the model be in predicting cyber threats?

## **1.5 Scope**

The scope of this study focuses on threats posed by insiders. This is because threats can be posed by different sources (threat agents). For example, threats can result from nature, the environment and humans. Therefore, in this context, focus is on threats caused by humans especially those considered insiders.

## **1.6 Significance of Study**

This study provides information security professionals with relevant information that will be used to determine how to deal with the insider cyber security threats. It will contribute to Information System security research by addressing gaps in insider threat prediction model based on human behavioral influences.

The study will also contribute to cyber security research as it delves into deficiencies identified from the simulation analysis and provides mitigation strategies against malicious insiders. The insight may be useful to individuals employed in critical infrastructure areas as well as security

agencies charged with protecting critical assets to assist them build or improve defenses against insider threats.

### **1.7 Assumptions and Limitations**

The insider threat perspective being investigated assumes that the insider has the level of knowledge and skill of the systems required for successful attack. The insider threat is a big problem, and no single research effort is going to solve the problem. Every research undertaken only hopes to help in some way by targeting a specific area. This research will focus mainly on employees with legitimate rights of access and who originally had no intention of causing harm. It therefore ignores those hired with the secret intention of attacking systems or those paid by outsiders to cause damage. This will provide a basis for identifying high risk employees from those exhibiting normal behavior.

It is also assumed that the insider will be acting alone to attack or compromise a system in order to achieve some personal goal. However, the insider may co-opt a colleague into enabling an attack without that person's knowledge.

Research into insider threats face certain limitations which involve inadequate reporting of incidents and lack of real-world data on insider attacks. This is mainly attributed to reluctance by many organizations to disclose incidents of insider attacks for fear of damaging reputation.

### **1.8 Project Deliverables**

The overall deliverable in this research project includes;

- A model of the insider cyber threat using psychosocial factors.
- Simulation of the model
- A detailed report of the research project



## **1.9 Chapter Summary**

This chapter has provided a background to the study and the statement of the problem. It also outlines the general and specific objectives, and significance of the study. The chapter looks at the scope, and the assumptions and limitations of the study.

## **CHAPTER TWO: LITERATURE REVIEW**

### **2.0 Introduction**

This chapter reviews past and current research about insider cyber threat and also satisfies the first objective of this research by identifying the psychosocial factors that influence individuals to maliciously attack systems. It is also used to determine the need for a new model that uses influences on human behavior rather than computer logs and email mining to mitigate insider threat.

It has been divided into two areas; 1) insider cyber security threat concept, 2) Insider Threat Approaches.

### **2.1 Insider Cyber Security Threat Concept**

Threats to valuable information are posed by so called threat agents that could originate from both the outside and inside. Research shows that although attacks originating from the outside, such as hacking attempts or viruses, have gained a lot of publicity, insider threats pose a significantly greater level of risk (Schultz, 2002; Baker et al., 2008).

Predd et al., (2008) defines an insider as someone with legitimate access to an organization's computers and networks. It means that an insider is a person that has been legitimately empowered with the right to access, represent, and has knowledge about security measures that protect information within an organization. Insider threat is the potential for an insider to perform an attack either intentionally or unintentionally by exploiting vulnerabilities (Bishop, 2005; Carroll, 2006). It is the potential for trusted employees, contractors or consultants who have legitimate access, to exploit vulnerabilities and who in doing so violate the organization's security policy.

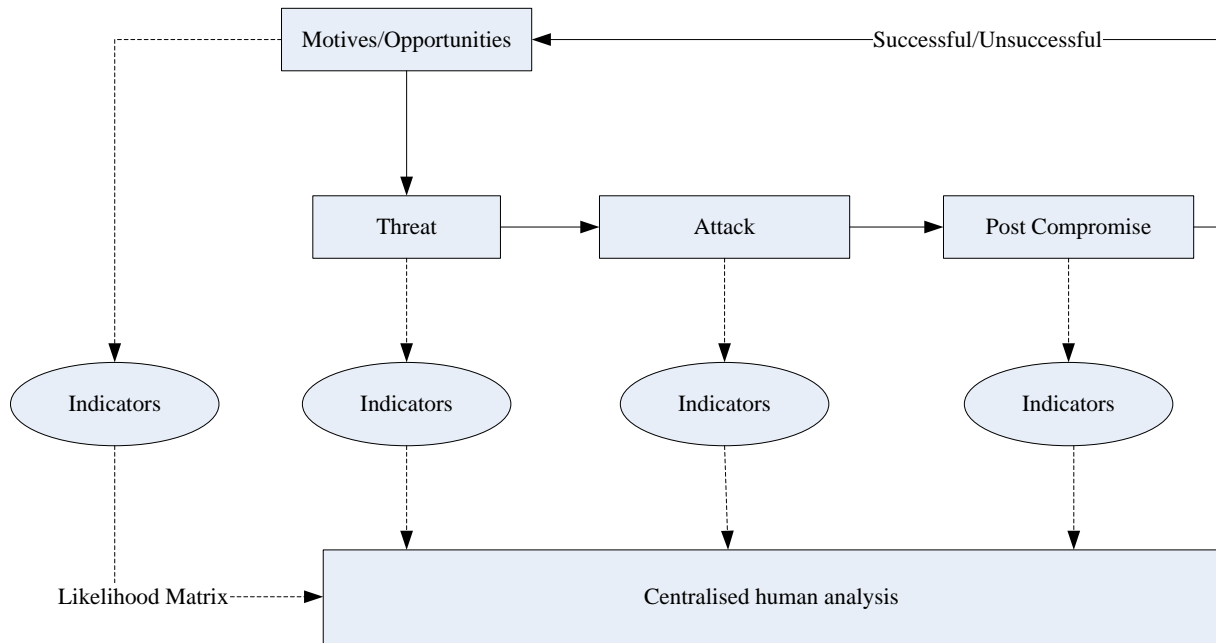
Insider threat may occur as a result of accidental access due to ignorance of security policy and practices or carelessness. It may also result from contempt for security practices, which includes inappropriate display or storage of classified or proprietary materials, poor protection of materials such as an unattended laptop that contains vital information or the unauthorized

destruction of classified or proprietary data. The worst form of insider damage comes from malicious intent which is purposeful compromise performed by individuals with the intent to harm and often results in the compromise or destruction of information or disruption of services to other insiders. There are several ways in which an insider may attack systems. Some of these include IT sabotage, espionage, theft of intellectual property and fraud among others.

## **2.2 Insider Threat Approaches**

There is a vast literature on counter-productive work behavior (CWB), which is defined as “any intentional behavior on the part of an organizational member viewed by the organization as contrary to its legitimate interests” [Sackett 2002]. This includes a wide variety of both self-destructive and retaliatory behaviors, but specifically encompasses, sabotage, stealing, fraud, and vandalism. Sackett and DeVore provide a thorough literature review and group the antecedents into personality variables, job characteristics, work group characteristics, organizational culture, control systems, and injustice [Sackett 2001]. This work is useful for the investigation into personal predispositions and organizational and individual stressors as antecedents of a range of malicious insider activity.

Butts (2006) expands the Schematic Protection Model to come up with a comprehensive security model capable of analyzing the safety of a system against the insider threat. The goal of the Multidisciplinary Approach to Mitigating the Insider Threat (MAMIT) is identification of suspicious individuals within an organization that display a credible amount of threat so follow-up action can be taken. The Multidisciplinary Approach to Mitigating the Insider Threat (MAMIT) is the framework designed to perform risk analysis for the insider threat. Figure 1 illustrates the process for countering malicious insider.



*Figure 1: Multidisciplinary approach framework for mitigating insider threats (Butts, 2006)*

Eberle et al. have proposed a graph-based approach for insider threat detection. This approach models the normal workflows as a graph and detects insider threats as anomalies in the graph. Brancik et al. proposed a data-intensive architecture comprising “event and anomaly collection”, “data analysis and correlation”, and “e-discovery tools” for detection of and protection from insider threats.

Ali et al. (2008) presented an Agent-based User-Profiling model shown in Figure 2 which builds and maintains the profile of all the insiders. The profile is dynamic in nature such that it is being updated continuously while monitoring the behavior of an insider. The presented model also monitors the behavior of the authorized users in an organization to avoid risk. McCormick (2008) assesses the threat of confidential data leakage, focusing on its most dangerous insider data theft attacks. He describes a comprehensive strategy which can mitigate inadvertent leakage as well as intentional data theft and reduce the risk of a large or embarrassing “data spill” in most modern automated enterprises.

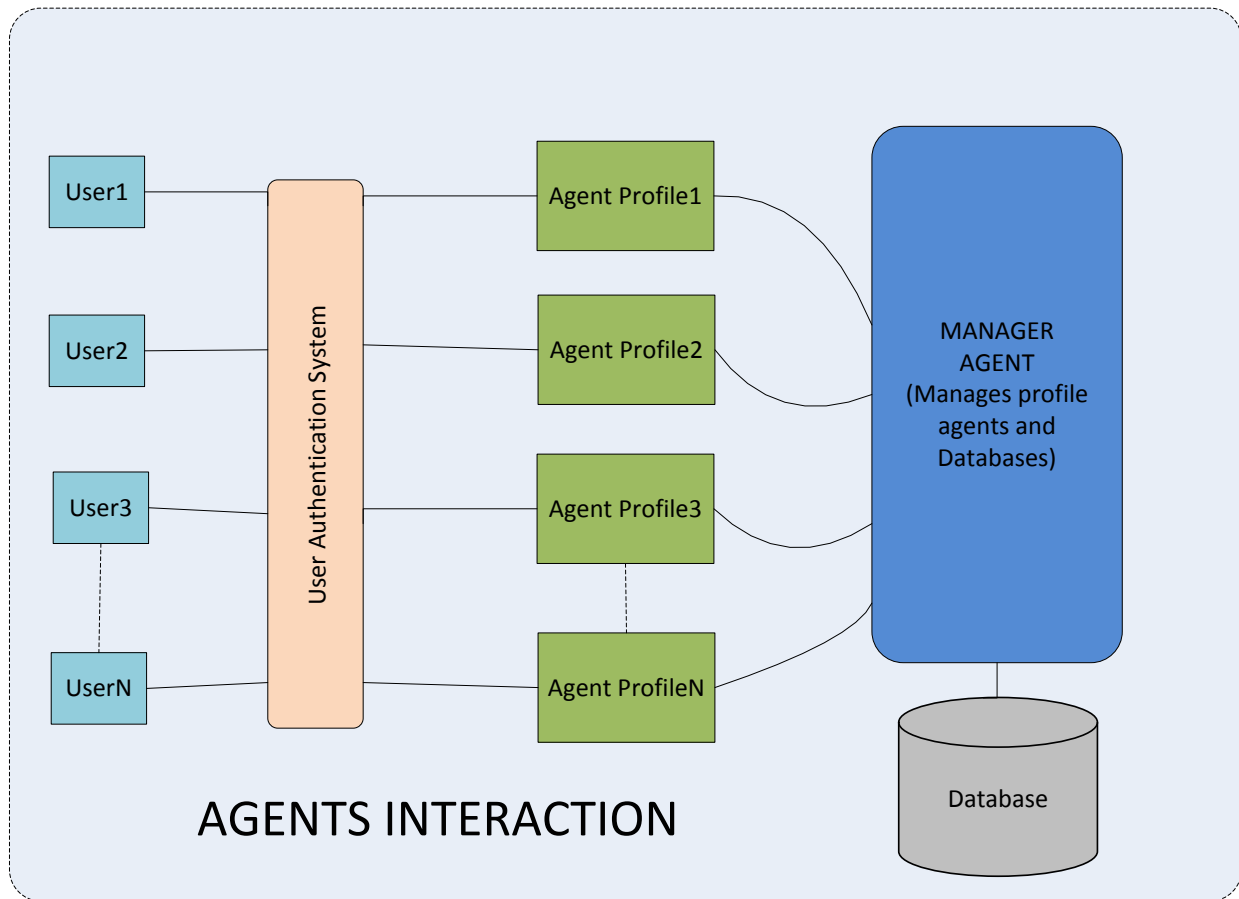


Figure 2: Authentication system and agents interaction (Ali et al. ,2008)

Greitzer et al. proposed a predictive risk model for insider threat mitigation. This model uses psychological indicators such as disgruntlement, accepting feedback, anger management, disengagement, disregard for authority, performance issues, stress, personal issues, self-centered, absenteeism, confrontational and dependability. The model then calculates risks using Bayesian network of the indicators. Cappelli and Moore et al. have proposed Management and Education of the Risk of Insider Threat (MERIT) for analyzing insider threats. MERIT analyzes insider activities using system dynamics framework for detecting insider threats as early as possible.

Another insider threat prediction model is proposed by Kandias (2010). This model uses an approach, techniques and tool that utilizes both soft and hard computing to monitor, capture

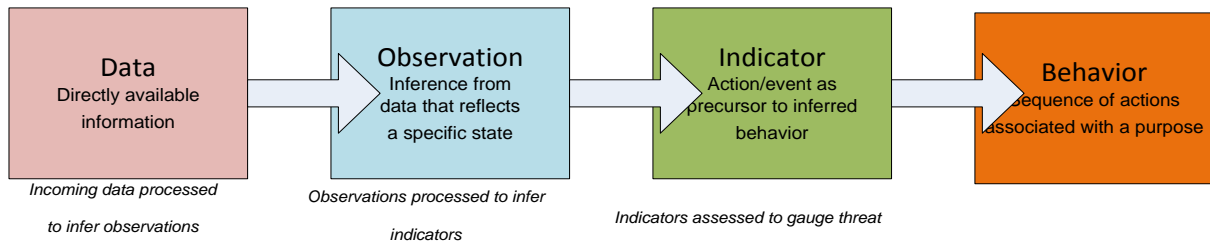
user's technological traits and analyzes it for misbehavior in a parallel environment. This model is categorized as a hybrid model. It is claimed that the proposed hybrid models could predict more accurately most of the time than all the techniques when applied individually.

The studies mentioned have focused more on technology as a means of preventing malicious insider activities. Some of the research also aims to improve anomaly detection efficiency but not what can trigger anomalous actions of the malicious insiders. Thus, the studies have neglected the people who are central in the insider threat study. Keeney (2005), Cappelli (2006-2007), Band (2006), Greitzer (2008), and Moore et al. (2008) have all used system dynamics to prevent insider threat. Apart from technology, the method includes process and people. This study will use a combination of agent based and system dynamics to determine the motives or opportunities that induce individuals into committing insider attacks by using behavioral factors.

### **2.3 Conceptual Model**

Most methods used in insider threat detection have focused on learning from an event/attack that has already taken place which is not useful in predicting the likelihood of a threat posed by an individual prior to an attack. This model is expected to be proactive and assist in predicting insider threats before they occur by analyzing individual behavior.

The model comprises a knowledge base of indicators and heuristic models of insider behavior. Indicators are essentially the semantics of insider behavior and characteristics—interpretations of intentions and actions based on observations. This knowledge base informs all of the components of the insider threat model, and is in turn updated or modified by outputs from components that perform functions such as data collection, data fusion, and analysis. The process can be thought of as a multi-layered analysis/inference processes that progress from Data to Observations to Indicators to Behaviors, as depicted in Figure 3.



*Figure 3: Model-Based Predictive Conceptual Framework*

*Observations* are processed from psychosocial data to infer *indicators* such as “excessive attempts to access a privileged database” or “presence of automated scripts.” In terms of psychosocial, one may infer an indicator such as “anger management” or “disgruntlement” based on observations such as entries in an HR database relating to arguments with supervisors. Employees may exhibit indicators to varying degrees: someone who has difficulty recalling a recently changed password might appear on a security log as making excessive attempts to access a protected database, but someone running password-cracking software exhibits the indicator to a higher degree.

Indicators are processed to infer *behaviors* as they are used to gauge the threat. Behaviors are sequences of activities for achieving some specific purpose, whether malicious or benign; the objective is to warn analysts about inferred behaviors consistent with established patterns of insider exploits. For example, if there are multiple policy violations which indicate attempts to run unauthorized computer programs, and which occur after normal working hours then a malicious activity is possibly underway. Therefore, isolated psychosocial indicators would not point to espionage by themselves, but when issues like anger, stress, and disgruntlement are observed along with trust/risk factors such as the employee’s access to sensitive information, that pattern increases risk.

## **2.4 The Gap**

The review conducted under this section reveal significant deficiencies on the approaches employed in mitigating insider cyber threats. The focus is mainly on technology and processes which leaves out people which is a crucial component in the insider threat study. Individual behavior has not been explicitly tested to determine its effectiveness in predicting insider malicious activities. Most of the studies also focus on detecting malicious activities and not on prediction to allow for preemptive action.

## **2.5 Chapter Summary**

This chapter has shown that first, it is important to study insider threat because it continues to evolve and most of the studies conducted have not been fully implemented. The insider threat study is also a hard problem that lacks good mitigation strategies. Second, insider threat is a people problem, where profiling and anomaly detection seem to show the best results, though are often unsuccessful or too late. As a result, since insiders have proven to come from all walks of life with differing skill sets and a vast range of motivations, it is clear that a new form of model is needed.

Third, this model needs to incorporate psychosocial factors or more specifically, the influences that govern human behavior. By monitoring how influences affect human behavior, it becomes possible to insert influences into a model and present an assessment of an employee's risk for becoming a malicious insider. As a result, the first objective of this research has been met, by identifying the need for a new model, the Insider Threat Prediction Model (ITPM), which uses the psychosocial factors to predict the predisposition of an individual to becoming a malicious insider. Chapter Three details the methodology used in developing the model and Chapter Four presents the results and discussion of how they relate to the problem, research framework and methodology.



## **CHAPTER THREE: RESEARCH METHODOLOGY**

### **3.1 Introduction**

In Chapter Two, material was presented outlining the need for a new and different kind of model to predict insider cyber threat. This chapter focuses on the methodology for building an Insider Threat Prediction Model (ITPM) using psychosocial factors. The approach in this study involves identification of key psychosocial factors that influence individuals to engage in malicious actions. To undertake the study of insider behavioral intention, we first interviewed insiders from at least two organizations to determine what their intentions were, their previous behavior and how they influence the current behavior.

The information obtained from the interview was used in the agent-based modeling stage of insider problem. This was designed to identify from a given population those who are susceptible to malicious activities.

The core of the study involved identification of cases relevant to the insider threat study. These cases were used to identify the various psychosocial factors that predispose individuals to commit insider crime. This research is based on information extracted from 11 cases of insider attacks

### **3.2 Target Population and Sampling Technique**

The insider as defined in 2.1 above is *a person that has been legitimately empowered with the right to access, represent, and has knowledge about security measures that protect information within an organization*. The target population for this research study was insiders within a few selected Government departments who have access to information or data considered confidential. The three departments/ministries identified were based in Nairobi for ease of access and cost for the researcher. We used a stratified random sampling technique in selecting respondents from the population.

### **3.3 Sampling Design**

The study adopted the stratified sampling technique as it was targeting a specific group of respondents within the population. According to C.R Kothari, 2004, if a population from which a sample is to be drawn does not constitute a homogenous group, stratified sampling technique is generally applied in order to obtain a representative sample.

A sample design therefore is a definite plan for obtaining a sample from a given population. When time and resources allow, the sample size should be taken as big as possible, since this would ensure reliability of the results. The danger with smaller samples therefore is that they do not reproduce the salient characteristics of the accessible population to an acceptable degree, Mugenda & Mugenda (2003).

### **3.4 Research Instruments**

The study used different data collection methods to capture data relevant to the insider threat. This study employed primary and secondary sources of data. Primary data are collected by the investigator conducting the research, whereas secondary data is data collected by someone other than the user. For primary data we used interviews, questionnaires while secondary data collection involved document reviews. The methods used to collect primary data were by dispensing the questionnaire, interviews and case studies. Secondary data is data collected by someone other than the user through documentation reviews.

#### **3.4.1 Questionnaires**

The questionnaire developed as shown in Appendix I was dispensed to personnel in two departments namely Kenya Revenue Authority, and Immigration. The questionnaire touched on the organization, subject and incident to determine the various elements that predispose individuals to commit malicious acts.

### **3.4.2 Personal Interviews**

While questionnaires were distributed to officers within the departments mentioned, personal interviews were conducted for heads of ICT and HR. Those interviewed were the Senior Deputy Director in-charge of HR and Deputy Director in-charge of ICT, Ministry of State for Immigration and Registration of Persons; Director in charge of Shared Services, e-Government; and KRA's Senior Assistant Commissioner Information & Communication Technology.

This methodology assisted in obtaining further information on insiders from the perspective of the HR and the technical staff as the manifestation of malicious activities can be detected through performance reviews and log analysis.

### **3.4.3 Case Study Methodology**

The methodology employed is a multiple case study approach, which focuses on psychosocial or behavioral elements of the insider threat. As described in Yin, 2009, a case study inquiry is defined as, "an empirical inquiry that investigates a contemporary phenomenon within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident."

This research methodology was employed to study existing insider cyber threat cases which have been documented. It was meant to discover factors that predispose individuals to perpetrate malicious activities.

### **3.5 Coding Methodology**

The data used for the study was taken from a large database of actual cases of insider activity, covering the crimes of fraud, intellectual property theft, espionage and sabotage. Case information was collected from both public sources such as court documents and non-public sources such as law enforcement investigations and interviews with insiders. Information was collected about the organizations involved, the perpetrator, and other details of the incident. With respect to the organizational data, information was collected such as the industry sector, work

environment, and opportunity provided to the insider by the organizational action or inaction. The information collected on an insider included demographic information, potential motives, concerning behavior, and violation history. The section of the database that is most relevant for this study is the psychosocial factors. Each factor provides elements which may instigate change in behavior from normal to abnormal for any one insider, thus becoming a threat to the organization.

11 cases of insider threats were selected from over 100 previously collected cases in the insider threat study. The cases were selected based on factors such as concerning behavior,

The research uses system dynamics modeling to better understand and communicate common aspects of insider threats. This methodology is based on the psychosocial factors that we use to map each case to the observables.

### **3.6 Modeling Technique**

The study employs agent based and system dynamics to model insider behavior. Agent based model is used to determine the interactions insiders have within a given organization. In the agent based scenario, we have two types of insiders within the population to consider; normal and malicious insiders.

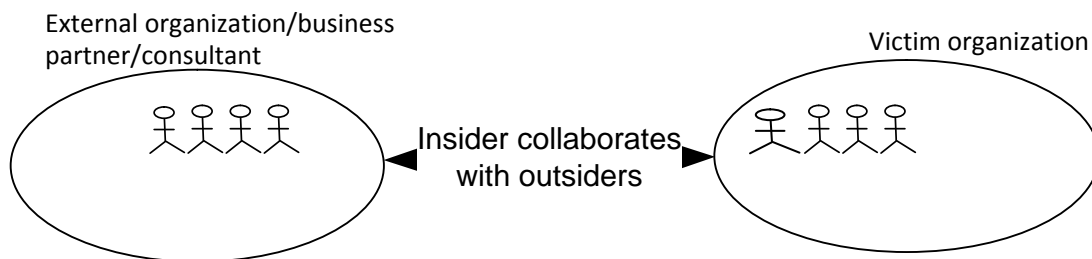
System dynamics is a method for modeling and analyzing the holistic behavior of complex problems as they evolve over time. System dynamics has been used to gain insight into some of the most challenging strategy questions facing businesses and government for several decades.

#### **3.6.1 Agent Based Model**

The data collected on insider intention or motive during the interview and questionnaire stage was used to model agent (insider) behavior within an organization. According to Russell & Norvig (1995), agents are objects in the environment that perceive and react to states in the environment.

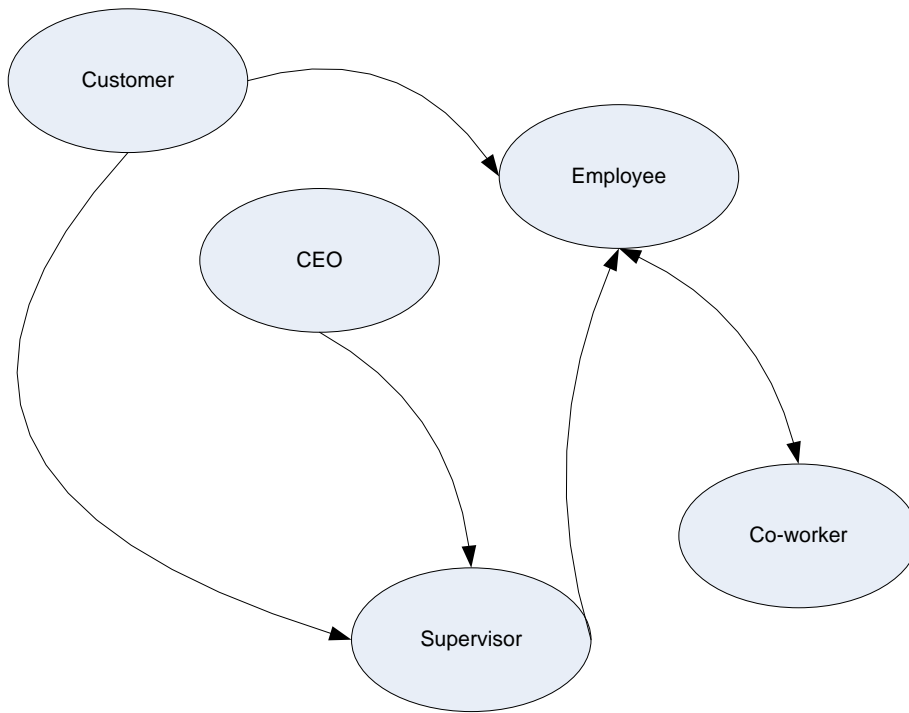
The insiders (agents) are individuals granted any level of trust in an information system and have access privileges or knowledge of the system (Butts et al., 2005, Bishop, 2005).

The agent-based model was used to profile the behavior of the malicious insider that is useful in predicting the possible indicators for attack. The insider is assumed to act alone when committing malicious acts. Therefore, the interaction between insiders may be deemed to be negligible in the insider threat study. Figure 4 provides a general agent interaction with the organization.



*Figure 4: Agent interaction*

The interaction and discussion with HR managers resulted in a relational diagram of an organization where the individuals in the organization interact and influence each other as shown in Figure 5.



*Figure 5: Model showing relationship within an organization*

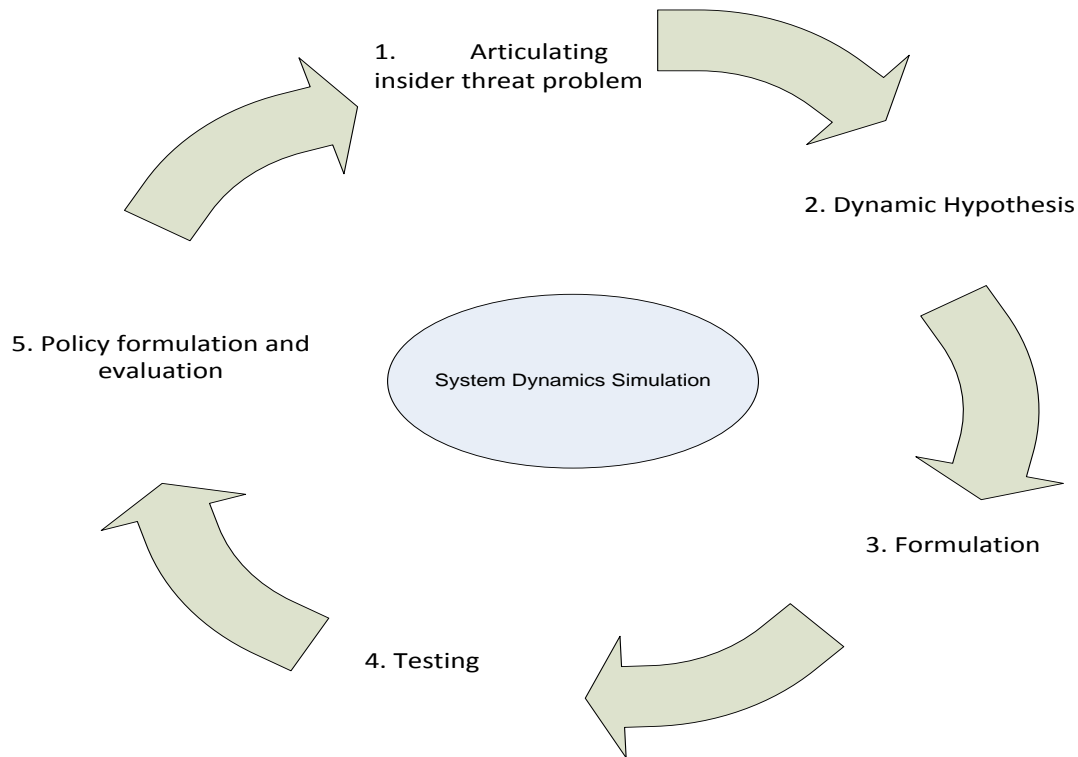
This model demonstrates the importance of relationships between the members of an organization. It is significant to note that some members hold more influence over other members in the organization. This is important because organizations have their own inherent culture which defines the relationship between its members. There are instances when an individual is either acting alone or is under the influence of a third party. Even though most of the insiders interviewed did not wish to state whether they at any one time had the intention of harming their organizations, the reports from HR personnel provided an insight into cases of misconduct that were indicative of possible malicious acts.

### **3.6.2 System Dynamics Model**

System dynamics is a computer-aided approach that can define problems dynamically and build confidence in the model. It applies interdependence, mutual interaction, information feedback, and circular causality to dynamic problems arising in complex social systems.

One of the fundamental principles of system dynamics is the hypothesis that a model predicts behavior. The importance of the connection between model and behavior is easily seen in Forrester's introduction to *Industrial Dynamics*.

System dynamics models can also be stand-alone. It formulates the problem of representing behavior over time as the problems of distinguishing the key variables in the situation, graphing the behavior of those variables over time. The modeling principle of system dynamics is as shown in Figure 6. It seeks to identify feedback mechanisms within a system to explain the system's behavior, (J.D. Sterman, 2000).



*Figure 6: System Dynamics modeling principle*

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.

System dynamics models consist of variables connected by causal relationships. Every relationship represents either a positive or negative influence of one variable on another. A positive influence (shown as a solid arrow between two variables) indicates that the values of the



variables move in the same direction, and a negative influence (shown as a dotted arrow between two variables) indicates that they move in opposite directions.

System dynamics is grounded in the theory of nonlinear dynamics and feedback control developed in mathematics, physics, and engineering (Sterman [2000], pp. 4–5). Mathematically, “the basic structure of a system dynamics model is a system of coupled, nonlinear, first-order differential (or integral) equations,” (Richardson [1996], p. 657) that can be written in the form:

$$dx/dt = \dot{x}(t) = f[x(t), u(t)]; x(t_0)$$

given

$x(t)$  = nth-order vector of system states (or levels)

$u(t)$  = vector of exogenous inputs

$x(t_0)$  = initial value for state vector at  $t = t_0$

$f$  = nonlinear vector-valued function

$dx/dt = \dot{x}(t)$  = time derivative of the state vector.

From the above equation, the system dynamics applies an The aim of a system dynamics modeling effort is to produce a structurally based explanation of the behavioral evolution of the system under investigation to generate insights that will identify leverage points of intervention.

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.

The systems dynamics approach may be used to analyze managerial or organizational problems in three steps:

1. Creating a model to represent the real-world structure. According to Forrester, system dynamics models are formulated to unite “the structure of the real system, the behavior of the real system, the model, the behavior of the model, and the model builder’s purpose” (Forrester, 1979, p.15). Such dynamic structure serves as hypotheses that characterize the interdependency, interaction, feedback, and causality of endogenous factors within the systems being studied (Matinez-Moyano, 2003).
2. Establishing the functional relationships among the variables in the dynamic structure, and the “dynamics” of the variables. These relationships can be analytical, empirical, or numerical in nature.
3. From a set of initial values, iterating (1) and (2) for all variables simultaneously to either reach a steady state or for a set period of time. This is done often with the aid of computer simulation programs.

The results of the computer simulation (Step 3) will give a dynamic picture of the behavior of the system under study. However, a rigorous and stable model (Step 1) and the variable relationships therein (Step 2) are crucial to the usefulness of the system dynamics approach, because “the most important and difficult step in system dynamics is perception of a model structure appropriate to the chosen purpose” (Forrester, 1979, p. 14). Although “trial and error” is often used to improve the modeling, techniques such as boundary scenarios and sensitivity analysis can be employed to ensure the stability and robustness of the system dynamics models. Other internal and external verification and validation methods are often necessary to make certain the model’s functional integrity, structural integrity, completeness, and relevance.

In this study we rely on system dynamics as a tool to help understand and communicate contributing factors to insider 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 this will 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 inhuman cloning, how this would affect the country's risk of espionage?)

The models we develop and system dynamics models in general, provide information of the third sort. Meadows explain 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.”

### **3.6.3 Psychosocial Model**

The implementation of the psychosocial model used personnel data that is likely available within organizations, court records as well as in public domain. The indicators used in the model, such as disgruntlement, anger management issues, and disregard for authority, are defined in Table 1. As discussed in F. L. Greitzer, et al., the selection of these indicators reflects an approach that (a) acknowledges privacy considerations that limit access to private information that has been associated with insider crime (such as financial and medical records) and (b) relies on observable behaviors rather than psychological personality predispositions that would otherwise have to be determined through personnel evaluations. We developed the list of indicators based on

examination of published case studies. The psychosocial model outputs indicators which are the inputs to the Insider Threat Prediction Model (ITPM).

We identified some data sources that appear to show promise in assessing relevant psychosocial factors and that also seem to be reasonable candidates to be considered from a legal or privacy ethics perspective. These are: staff performance evaluations; competency tracking; disciplinary tracking; timecard records; proximity card records; and pre-employment background checks (vetting). These sources, by themselves, do not constitute the psychosocial factors directly, but they do inform such factors.

Use of these indicators assumes an observational/management reporting approach that would rely on personnel data and judgments that are likely to be available from management and HR staff. Also, it assumes some manner of quality control and possibly employee appeal and review, to reduce likelihood of misuse.

The psychosocial indicators shown in Table 1 were developed by obtaining judgments from available HR experts on the prevalence and severity of different combinations of indicators that reflect different scenario cases. From the knowledge of experts, these psychosocial indicators contribute differentially to the judged level of psychosocial risk—*disgruntlement*, *difficulty accepting feedback*, *anger management issues*, *disengagement*, and *disregard for authority* have higher weights than other indicators, for example.

<b>Indicator</b>	<b>Description</b>
Disgruntlement	Employee observed to be dissatisfied in current position; chronic indications of discontent, such as strong negative feelings about being passed over for a promotion or being underpaid, undervalued; may have a poor fit with current job.
Not Accepting Feedback	The employee is observed to have a difficult time accepting criticism, tends to take criticism personally or becomes defensive when message is delivered. Employee has been observed being unwilling to acknowledge

	errors; or admitting to mistakes; may attempt to cover up errors through lying or deceit.
Anger Management Issues	The employee often allows anger to get pent up inside; employee has trouble managing lingering emotional feelings of anger or rage. Holds strong grudges.
Disengagement	The employee keeps to self, is detached, withdrawn and tends not to interact with individuals or groups; avoids meetings.
Disregard for Authority	The employee disregards rules, authority or policies. Employee feels above the rules or that they only apply to others.
Performance	The employee has received a corrective action (below expectation performance review, verbal warning, written reprimand, suspension, termination) based on poor performance.
Stress	The employee appears to be under physical, mental, or emotional strain or tension that he/she has difficulty handling.
Confrontational Behavior	Employee exhibits argumentative or aggressive behavior or is involved in bullying or intimidation.
Personal Issues	Employee has difficulty keeping personal issues separate from work, and these issues interfere with work.
Self-Centeredness	The employee disregards needs or wishes of others, concerned primarily with own interests and welfare.
Lack of Dependability	Employee is unable to keep commitments /promises; unworthy of trust.
Absenteeism	Employee has exhibited chronic unexplained absenteeism.

*Table 1: Psychosocial indicators*

From the observations and judgments of experts, it is expected that management and HR personnel would use the information obtained to better understand the nature of the threat and the likely precursors or threat indicators that may be usefully reported to cyber security officers.

Therefore, the predictive modeling approach provides leads for cyber security officers to pursue in advance actual crimes, without which they would likely have little or no insight from which to select individuals showing malicious intent as a focus for further analyses.

### **3.7 Modeling Process**

The modeling effort began with identification of cases to be used in determining an insider's behavioral or psychosocial characteristics. While at least 20 cases were examined, only 11 cases contained relevant information for this modeling effort. The information needed for this modeling exercise involved the dynamic nature of key variables. However, such information was not readily available for all of the cases. Therefore, the cases were selected based on their relevance to the research and the availability of pertinent information.

Separate databases were then constructed to catalog relevant information for the cases. Case data drove the model scope and refinement. We gave preference to model variables that headstrong links to observables in the data. The term *observables* in this report refer 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.

Figure 7 depicts the process used to develop the Insider Threat Prediction Model (ITPM). The source of information for the modeling was the set of 11 insider cases (shown in the center of Figure 7). We captured information relevant to the modeling effort in the *Insider Case Details Database* (stage 1). The modeling efforts (stage 2) took the process to a *Detailed Concept Model*. The data was submitted to a psychologist who provided expert opinion as well as identification of the various psychosocial factors in each case.

The notation used to present the model was simplified as it focused on the feedback relationships between model variables. The resulting model is the Insider Simulation Model (stage 3). Then, all model variables were linked to case observables (stage 6).

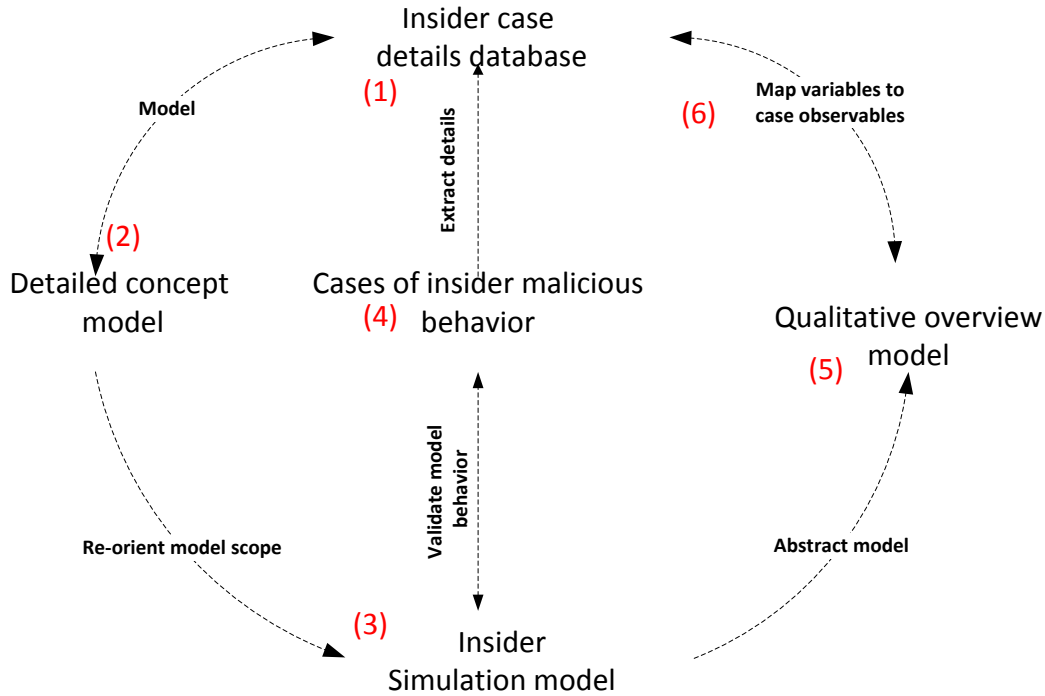


Figure 7: Insider Model Evolution Framework

### 3.8 Modeling Notation

In the portions of the system dynamics model presented below, arrows represent the system interactions. These arrows are coded with either positive (+) or negative (-) value 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 a+ (positive) indicates that the value of the source and target variables move in the same direction.
- Roughly, an arrow labeled with a- (negative) indicates that the value of the source and target variables move in the opposite direction.

The dynamically complex problems are 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.

- 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.”

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

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.

Figure 8 summarizes the notation used in this report. Models using this notation are often referred to as *qualitative system dynamics models* or *causal loop diagrams*.







Var	<b>Variable</b> – anything of interest in the problem being modeled
Var1  Var2	<b>Positive Influence (solid arrow)</b> – values of variables move in the same direction (e.g., source increases, target increases)
Var1  Var2	<b>Negative Influence (dotted arrow)</b> – values of variables move in the opposite direction (e.g., source increases, the target decreases)
	<b>Balancing Loop</b> – a feedback loop that moves variable values to a goal state; color loop identifies circular influence path
	<b>Reinforcing Loop</b> – a feedback loop that moves variable values consistently upward or downward; loop color identifies circular influence path

Figure 8: System Dynamics Notation

### 3.9 Modeling Tool

The research applies the AnyLogic program, a multi-method simulation modeling tool that supports all three well-known modeling approaches:

- System dynamics,
- Discrete event simulation,
- Agent-based modeling.

The system dynamics approach deals mostly with continuous processes whereas "discrete event" and agent based models work mostly in discrete time that is jump from one event to another.

System dynamics dealing with aggregates is obviously used at the highest abstraction level. Discrete event modeling is used at low to middle abstraction while agent based modeling technology is used across all abstraction levels, and agent may model objects of very diverse nature and scale. For example at the "physical" level agents may be pedestrians or cars or robots; at the middle level they may be customers and at the highest level they may be competing companies.

The AnyLogic simulation language consists of the following items:

- Stock & Flow Diagrams are used for System Dynamics modeling.
- State charts are used mostly in Agent Based modeling to define agent behavior. They are also often used in Discrete Event modeling, e.g. to simulate machine failure.
- Action charts are used to define algorithms. They may be used in Discrete Event modeling, e.g. for call routing, or in Agent Based modeling, e.g. for agent decision logic.
- Process flowcharts are the basic construction used to define process in Discrete Event modeling. Looking at this flowchart you may see why Discrete Event style is often called Process Centric.

AnyLogic includes a graphical modeling language and also allows the user to extend simulation models with Java code. The Java nature of AnyLogic lends itself to custom model extensions via Java coding as well as the creation of Java applets which can be opened with any standard browser.

### **3.10 Chapter Summary**

This chapter has provided a description the Agent based and System Dynamics approaches to modeling the insider cyber threats. We have also explained the data collection methods used and identified the psychosocial indicators that are the input variables in the model.

## **CHAPTER 4: RESULTS AND DISCUSSION**

This chapter describes the methods used to analyze the data collected for this study and the results obtained from the analysis. We first collected data about insider incident activities and tabulated the results. Thereafter, we used the case studies to model and simulate insider cyber threats.

Employee disgruntlement was a recurring factor in the insider cases, predominately due to some unmet expectation by the insider. This is evident in the examples below:

1. Insider intention and previous behavior was found to have an effect on their current behavior. In some cases, individuals may exhibit normal intention or motive while others may show threatening or malicious intent which may lead to harm to organization information.
2. The insider expected certain technical freedoms in his use of the organization's computer and network systems, such as storing personal files, but was reprimanded by management for exercising those freedoms.
3. The insider expected to have control over the organization's computer and network system, but that control was revoked or never initially granted.
4. The insider expected recognition or prestige from management, but was disturbed upon some event in the workplace, such as being passed over for a promotion.

The models developed address the main areas of insider threats that use behavioral factors as a catalyst to attack of systems. Insider freedom represents freedom for the insider to use or control the system. Expected freedoms could be measured either by the number or extent of privileges or on a continuous scale from none to root access.

### **4.1 Research Demographics**

Data on the two institutions on insider threats was obtained by use of questionnaires, interview notes, case studies, policy document reviews and online documentary repository reviews. The data so obtained was therefore cleaned and then grouped as per research questions before analysis. Table 2 below shows the breakdown of how the various strategies were applied to aid in data collection. The targeted population was 200 respondents, however, a total of 350

respondents were distributed. This was designed to take care of possible non-response as well as incorrectly filled in questionnaires.

From the 350 questionnaires dispensed using different methodologies, a total of 275 questionnaires were found to be valid after doing data cleaning and validation. Table 3 summarizes the demographics for the sample.

<b>Method</b>	<b>Sent</b>	<b>Received</b>	<b>Cleaned</b>
Electronic (online)	220	190	175
Hard copy	95	70	60
Phone	20	20	20
Face to face interview	15	20	20
<b>Total</b>	<b>350</b>	<b>300</b>	<b>275</b>

*Table 2: Distribution of research questions to respondents*

<b>Gender</b>	<b>Total</b>	<b>Percentage (%)</b>
Male	183	66.7
Female	92	33.3
<b>Current position within organization</b>		
Management	25	9.1
Administrative or support staff	183	66.7
Other	67	24.2
<b>Total length of time in organization</b>		
Less than 1 year	10	3.6
1 year to less than 5 years	180	65.4
5 years to less than 10 years	15	5.5
10 years to less than 15 years	45	16.4
15 years to less than 20 years	15	5.5
More than 20 years	10	3.6

*Table 3: Sample demographics*

<b>Components of incidents</b>	<b>Total</b>	<b>Percentage (%)</b>
Work related violations	30	10.9
Threatening behavior	50	18.2
Financial difficulties	60	21.8
Technical violations	20	7.3
Disloyalty	30	10.9
Social skills and decision making deficits	20	7.3
Unusual needs for attention	15	5.5
History of legal, security or procedural rule violations prior to attack	50	18.2
<b>Potential Motives</b>		
Financial	50	18.2
Revenge	30	10.9
Recognition	40	14.5
Disgruntlement	125	45.5
Disloyalty	35	12.7
<b>Personal characteristics</b>		
Drug involvement	15	5.5
Alcohol abuse	15	5.5
Sexual behavior	15	5.5
Personal conduct	90	32.7
Foreign influence	25	9.1
Emotional, mental and personality disorder	50	18.2
Criminal conduct	50	18.2
Security violations	15	5.5

*Table 4: Components of an Incident*

From the data and analysis given above, majority of insiders were men contributing to 66.7% while women stood at 33.3% as shown in Table 3. From the same table, most insiders were employed in administrative and support positions that required limited technical skills. In terms of duration of stay in an organization, those with between one year (1 year) and five years (5 years) service had a chance of 65.4% of being malicious compared to those with over 20 (twenty) years who were at 3.6% likelihood.

Nearly half of the insiders exhibited some inappropriate or concerning behavior prior to the incidents, but had no recorded incidents of violating organizational policies. However, financial gain was both the motive for, and objective of, most insiders' malicious activities.

#### **4.2 Insider Threat Prediction Model**

The predictive model is based on the relative influence each indicator variable in the psychosocial model has on individual behavior. The model depicts the weights of the various indicators as observed by two HR experts. Table 5 lists the psychosocial indicators with the relative weights and occurrences in a given organization.

<b>Indicator</b>	<b>Influence</b>	<b>Weight</b>
Disgruntlement	0.025	0.400
Not Accepting Feedback	0.060	0.280
Anger Management Issues	0.019	0.260
Disengagement	0.040	0.310
Disregard for Authority	0.075	0.340
Performance	0.020	0.160
Stress	0.030	0.200

Confrontational Behavior	0.063	0.120
Personal Issues	0.080	0.140
Self-Centeredness	0.100	0.180
Lack of Dependability	0.038	0.060
Absenteeism	0.010	0.060

*Table 5: Occurrence and weights of the psychosocial model*

From Table 5, it can be seen that disgruntlement occurs seldom (0.025) but has a higher influence on insider risk behavior (0.400) while self-centeredness occurs quite often (0.100) but has relatively low influence (0.180). It therefore means that if self-centeredness is observed independently in at least 10% of employees, it should not cause any alarm. However, if it is combined with another variable indicator, it may be worth considering.

#### **4.3 Observation 1: Insider’s Intention**

To understand the behavioral aspects influencing an insider to commit malicious acts, a number of insiders from at least three organizations were interviewed for this study. The insiders ranged from support staff to management.

It was determined that when individuals join an organization, they are presumed to have no motive to cause harm to the organization, that is, they are of normal behavior. However, data collected indicates that at least 1% of those who seek employment always have prior intention to steal corporate information, sabotage systems or commit fraud while the remaining 99% have no malicious intention. For example, an employee being sent by a competitor to seek employment would be predisposed to commit malicious acts through espionage and under the direction and control of the sponsor.

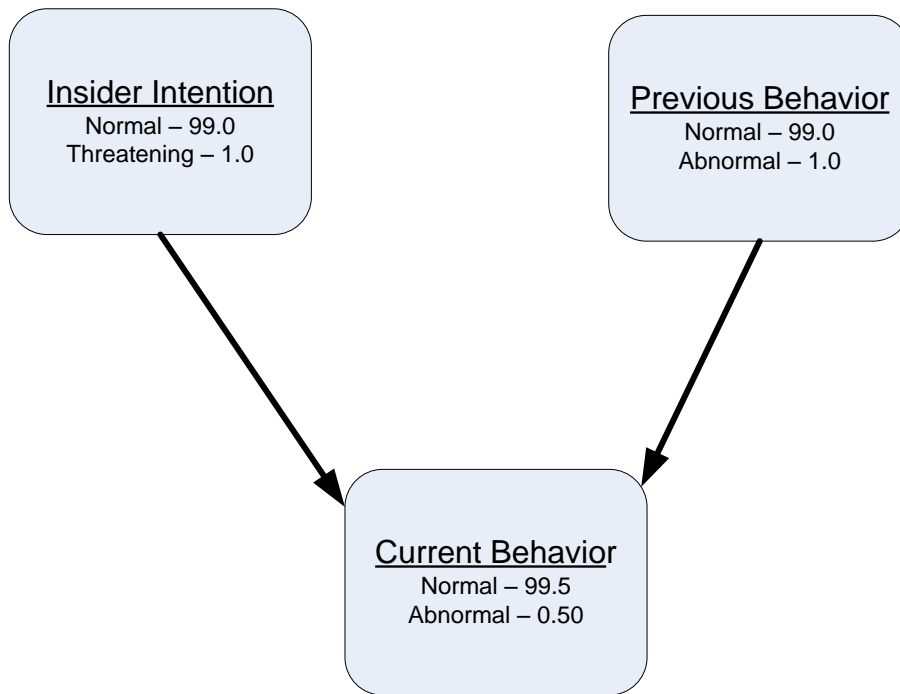
Insider’s previous behavior was found to have a direct influence on the insider’s current behavior. Therefore, if an insider’s behavior in previous session was Normal, then there is a 90%

chance it will be Normal in current session and 10% chance it will be Abnormal. But if it was Abnormal in the previous session then there is an 80% chance it will be Normal in current session and 20% Abnormal. The probabilities mean Abnormal behavior in previous session results in Abnormal behavior in current session 2 times (0.2/0.1) than if it was Normal. The insider behavior distribution according to gender is shown in Table 6 below. Figure 9 below models the insider motive while Figure 10 is the agent based model version of the same.

<b>Gender</b>	<b>Previous behavior</b>		<b>Current behavior</b>	
	<b>malicious</b>	<b>normal</b>	<b>malicious</b>	<b>normal</b>
Male	3	180	1	182
Female	0	92	0	92
Total	3	272	1	275
% of Total	1	99	0.5	99.5

*Table 6: Insider behavior distribution*





*Figure 9: Insider Intention Model*

The intention model became the basis for the agent based modeling of the insider interaction to determine how their previous behavior influence their current behavior based on their intention.

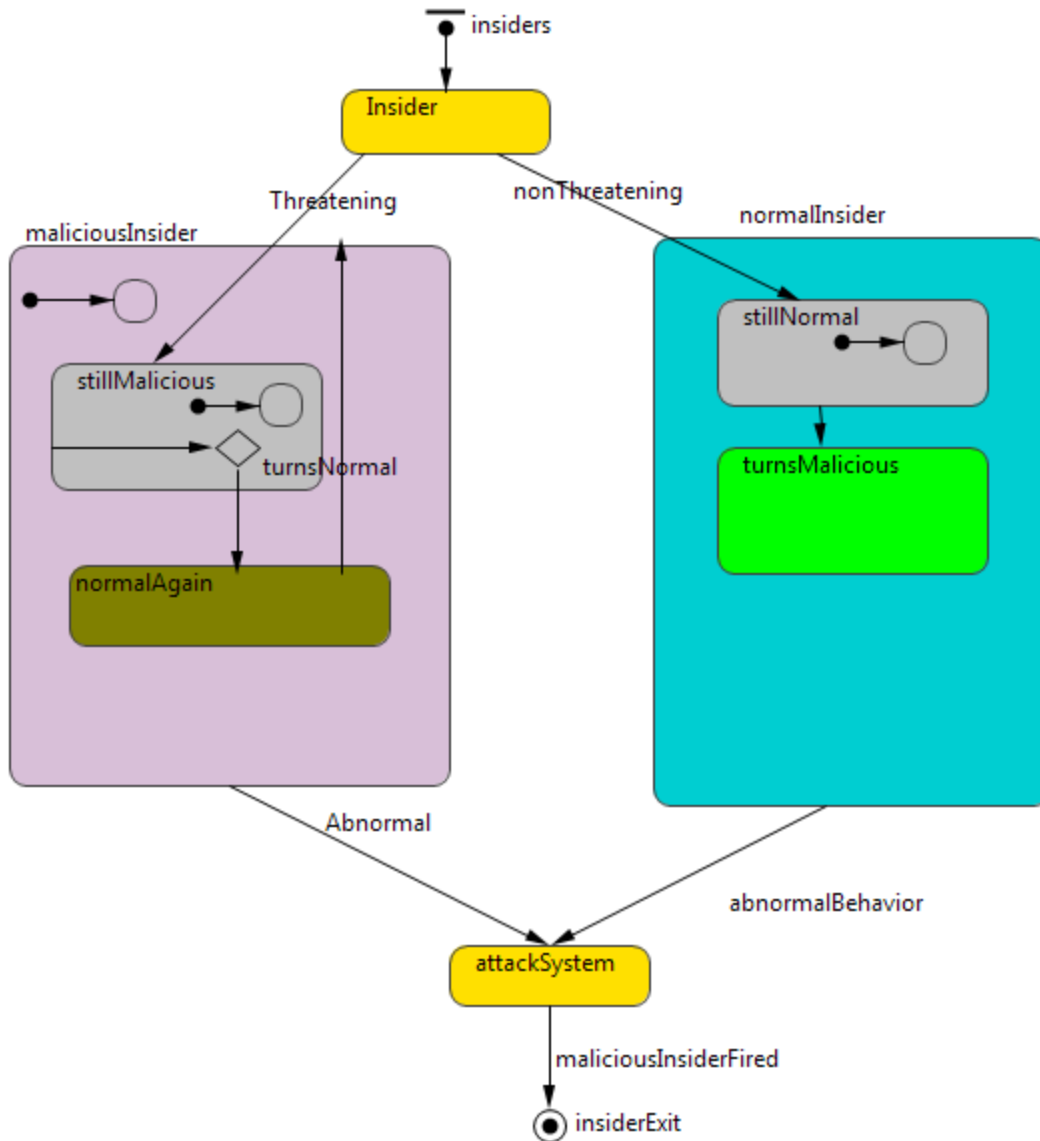


Figure 10: Agent based model

The model creates a simulated insider whose level of acculturation to the broader population of which it is a part dynamically varies according to individual behavior. The modeling technique used draws on both System Dynamic and Agent based paradigms. Within an organization, each agent makes choices stochastically as modulated by its current state and the outside environment that it operates in.

The model in Figure 10 starts with the identification of the insider's intention or motive. If the insider's motive is malicious and is likely to harm the organization, then the model determines the individual as having a motive. Then if the insider has motive and is threatening, he is perceived to have the potential to attack a system

The model was able to draw from both the agent's state as well as the System Dynamics concepts of modeling variables to represent the accumulation and decay of behavioral factors within an agent. Also in the System Dynamics tradition the global level feedback structures that shape agent level behavior are identified.

The model helps to find that dynamically complex behavior endogenously emerges in the insider study population.

#### **4.4 Observation 2: Insider's Expectation of Freedom**

Figure 11 depicts changes in the insider's expectations over time based on his actual freedom as well as the insider's predisposition to disgruntlement. This predisposition differs from one person to the next, and influences the rate at which expectations rise and fall. The rise of expectations is influenced heavily by the actual freedom given insider. As illustrated in reinforcing loop R1, with lax management controls actual freedom grows commensurately with expected freedoms. As more freedom is allowed, more freedom is taken; as more freedom is taken, more is allowed. In the model, it is assumed that even lax management sets an upper bound on the extent of freedoms allowed to any employee.

Lack of supervision and controls encourages escalation of expectation. Expectation escalation is seen in the simulation results in Figure 12. The simulation starts off with expected and actual freedom at an equal value of 10 on a scale of relative freedom. This is an arbitrary measure of the relative freedom allowed any employee of an organization according to the organization's appropriate systems usage policy. Laxity in supervision may entice employees to abuse their privileges. This is especially true for insiders with a strong sense of entitlement.

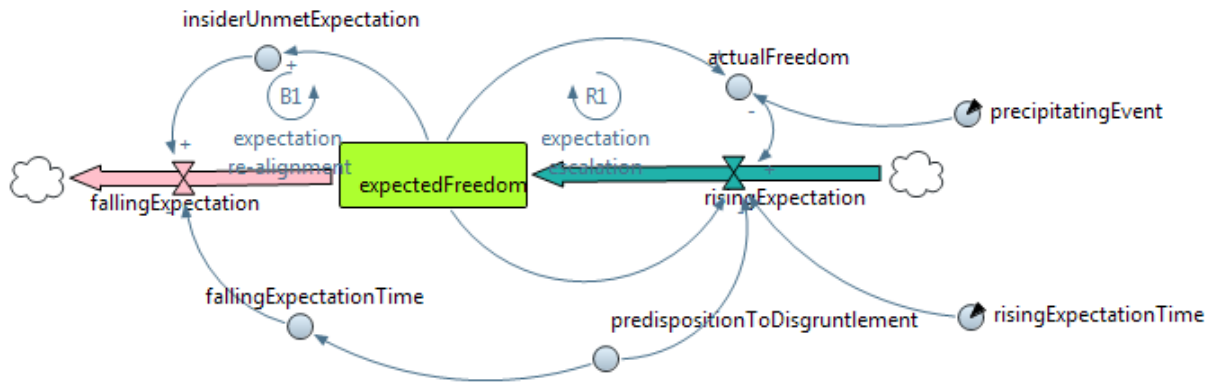


Figure 11: Expected freedom by Insider

As management allows the insider’s actual freedom to increase beyond that permitted by policy, the insider’s expectation also rises. As shown in the figure, expected and actual freedom continue to increase at an equal rate until when freedom reaches a point that even lax management will not permit—more than twice the freedom allowed by policy. At this point, the insider expects slightly more than is permitted; this situation creates an equilibrium condition where unmet expectation stays fairly constant over time.

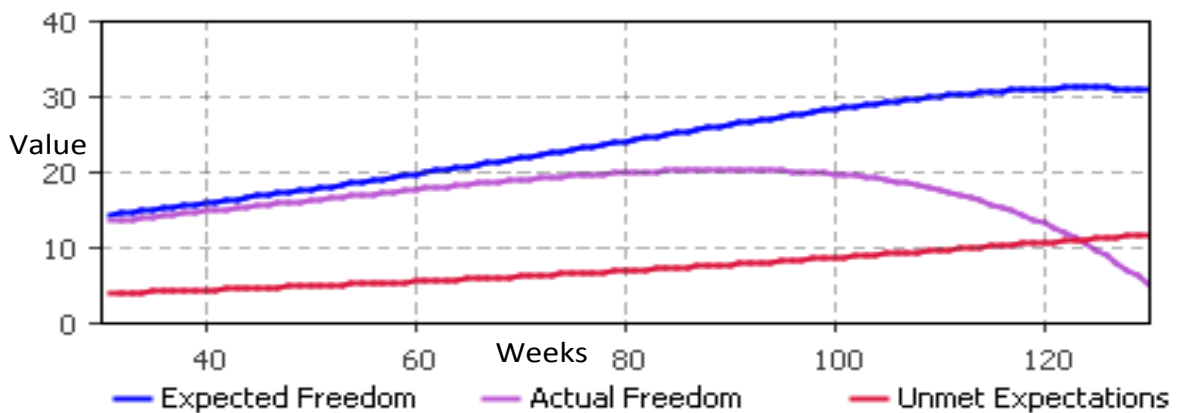


Figure 12: Expectation escalation

This simulation shows that where management permits increasing freedom for the insider it can cause major problems later on, especially if that insider has a predisposition for disgruntlement. The trigger for the major problems, which are called, precipitating event, tends to be anything that removes or restricts the freedom to which the insider has become accustomed.

For example, Michael Peri, an electronic warfare signals specialist for the Army, felt overworked and unappreciated in his job and also had anxiety regarding public speaking that was so extreme that it reportedly contributed to his decision to flee the workplace with classified information.

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 was an indication that the work environment did not provide appropriate safeguards for his fears.

In the Bradley Manning case for example, he was deployed to Forward Operating Base Hammer, near Baghdad, arriving in October 2009. From his workstation there, he had access to SIPRNet (the Secret Internet Protocol Router Network) and JWICS (the Joint Worldwide Intelligence Communications System). Two of his superiors had discussed not taking him to Iraq – it was felt he was "a risk to himself and possibly others," according to a statement later issued by the army – but again the shortage of intelligence analysts held sway.

#### **4.5 Observation 3: Escalation of Disgruntlement and Sanctioning**

Figure 13 depicts part of the model which refers to the influences of *unmet expectation* on the insider's offline<sup>1</sup> behavior, and the organization's response. Three additional stocks are introduced:

---

<sup>1</sup> In this report, *online behavior* refers to actions taken using the computer, while *offline behavior* refers to social behaviors that are not taken on the computer.

1. *Insider disgruntlement*: the insider's internal feelings of discontent due to demands or restrictions by the organization that he perceives as unacceptable or unfair.
2. *Behavioral precursors*: observable aspects of the insider's offline/social behavior inside or outside the workplace that might be deemed inappropriate or disruptive in some way.
3. *Sanctions*: the organization's punitive response to inappropriate behaviors. Sanctions can be technical, such as restricting system privileges or right to use the organization's equipment at home, or non-technical, such as demotion or formal reprimand.

A generic measure of *relative severity* is used to measure behavioral precursors, damage, and disgruntlement.

Reinforcing loop R2 in Figure 13 characterizes escalation of disgruntlement in response to sanctions for inappropriate social behaviors. As the *insider's unmet expectations* increase, *Insider disgruntlement* increases. Insiders exhibit disgruntlement by *acting inappropriately offline*. Observable inappropriate offline behaviors vary; some insiders take revenge primarily online, exhibiting fewer offline precursors. We assume that the insider's *predisposition to disgruntlement* indicates his tendency to engage in inappropriate offline behavior before an attack.

Continuing around loop R2 of Figure 13, notice that *Severity of the actions perceived by org* is affected by *time to realize insider responsible*. Severity of actions influences the extent of sanctioning, which further limits the *actual freedom given insider*.

Instead of (or in addition to) punitive measures, organizations may take positive actions to address an insider's disgruntlement. Such actions, represented as *employee intervention*, include referral to an employee assistance program or counseling. Balancing loop B2 in Figure 13 reflects use of *employee intervention* to address disgruntlement. The organization's perception of the severity of the *Behavioral precursors*, the observable manifestation of the insider's disgruntlement, and organizational policies determine whether positive intervention or sanctions are warranted.

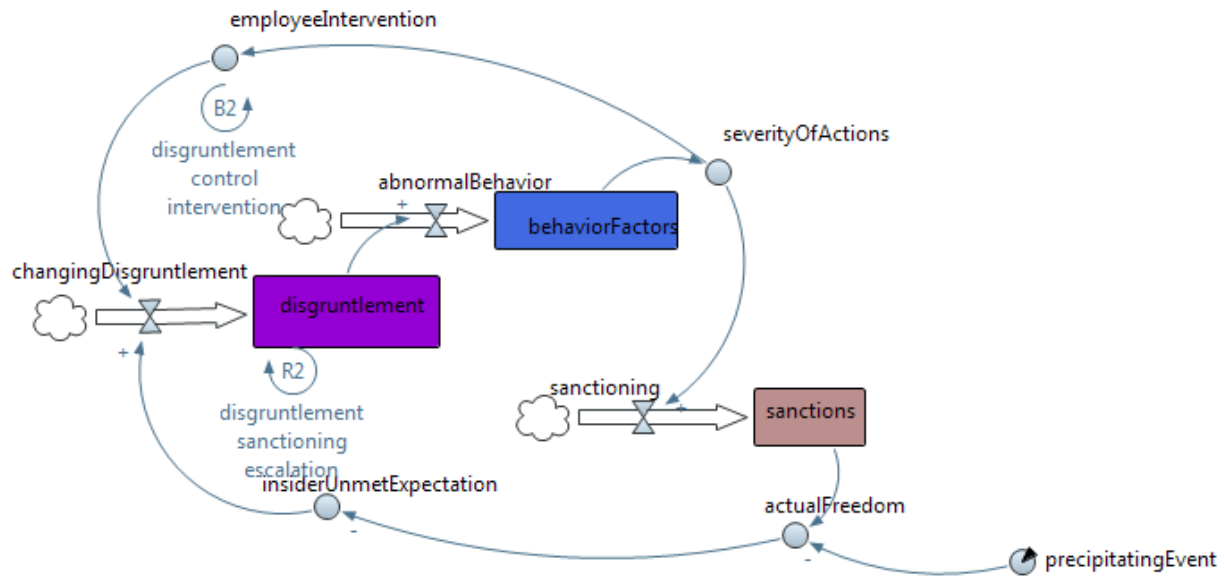


Figure 13: Escalation of Disgruntlement and Sanctioning

Figure 14 below provides a general view of how proactive employee intervention can be used to decrease both disgruntlement and the sanctions needed to address inappropriate behavior arising from that disgruntlement. The positive aspect of employee intervention is that by treating disgruntlement directly, there is less need for punishment and corresponding less disgruntlement caused by the punishment.

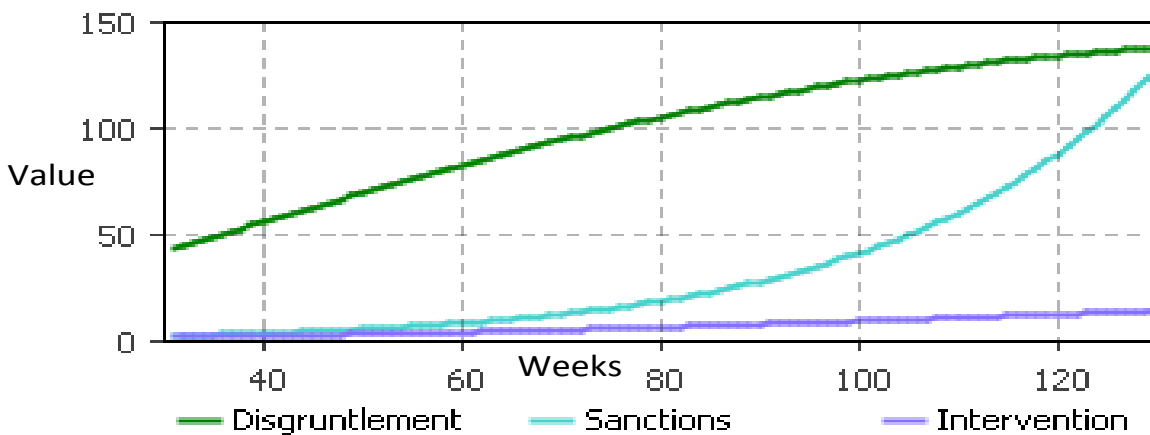


Figure 14: Simulated escalation of disgruntlement and sanctioning

#### **4.6 Observation 4: Organizations Ignored or Failed to Detect Rule Violations**

Figure 15 depicts some of the relationships relevant to the detection of rule violations in most of the cases. 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. 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 cases examined in this study, the organizations frequently ignored or failed to appreciate the significance of detected non-technical rule violations. Feedback loopR3 (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 malicious activities. 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.

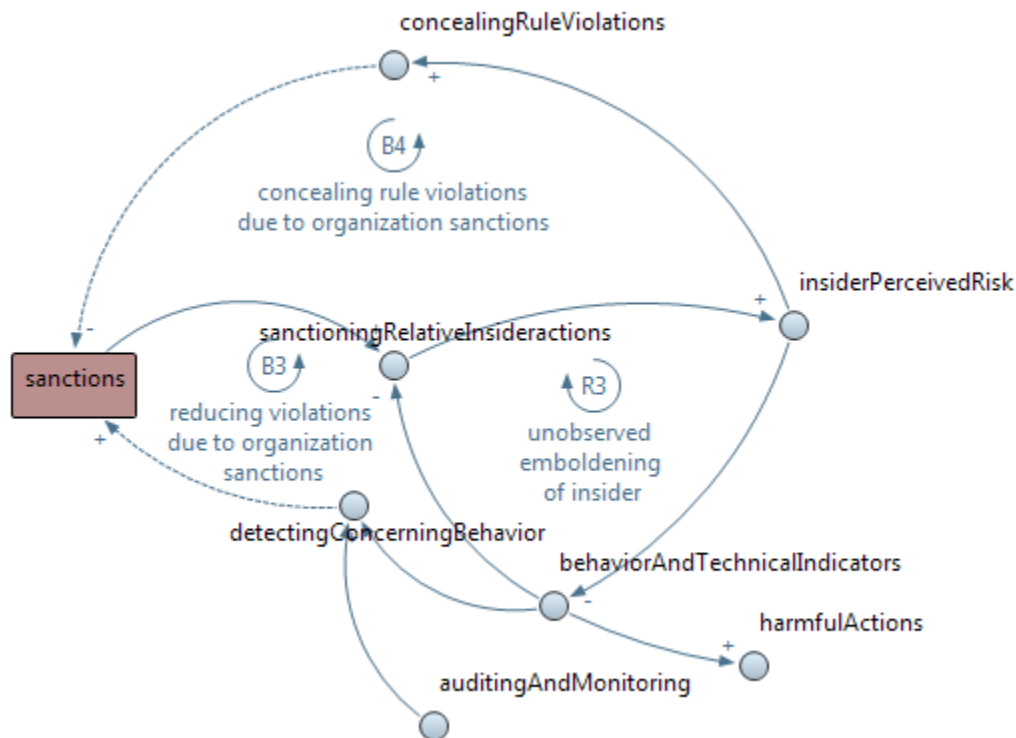


Figure 15: Organizations Ignored or Failed to Detect Rule Violations

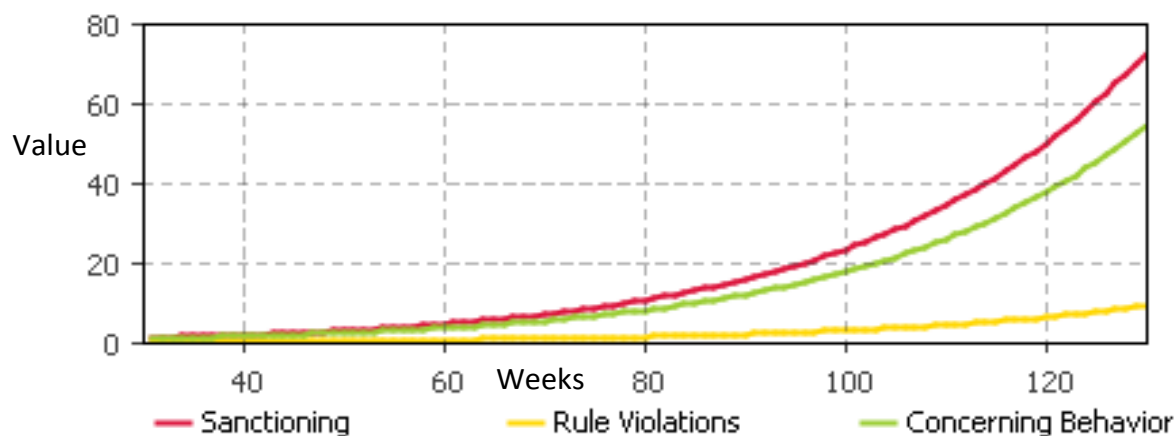


Figure 16: Failure to recognize rule violations

For example, the Robert Hanssen case provides a 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.

#### **4.7 Validation of Predictive Model**

The most rigorous form of evaluation of a predictive model is to test the predictions against a set of real cases as indicated in the 11 case studies shown in appendices III, IV and V. Appendix III is a mapping of insider cases to observables. This information is used to model the insider threats

The objective in validating the psychosocial component of the model was to demonstrate agreement between the model and expert judgments. This requires the following steps:

- Obtain expert judgments on what constitutes a valid threat, what constitutes valid indicators for that threat, and how to tie indicators to observables.
- Develop test scenarios with experts' help—scenarios must be specified in detail with appropriate data and observables that will drive the model.
- Obtain expert judgments on the scenarios that will be used to test the model.
- Operate the model on the data or observables associated with a scenario. The model must characterize the extent to which the observables match a scenario.

As part of validation, the researcher performed parameter variation to determine the effect of varying precipitating event, relative freedom and rising expectation on the model outputs as shown in Figure 17.

While rising expectation is held constant at a value of 1, the precipitating event acts like a trigger that either increases or reduces the relative freedom an individual enjoys. This effect is shown in how the three variables influence expected freedom, escalation of disgruntlement and indications that organizations ignore or fail to detect rule violations.

## Insider\_Threat\_Prediction\_Model : Parameters Variation

Parameter Variation Experiment in which three variables; precipitating event, relative freedom and rising expectation time are compared. The experiment goes through a number of iterations.

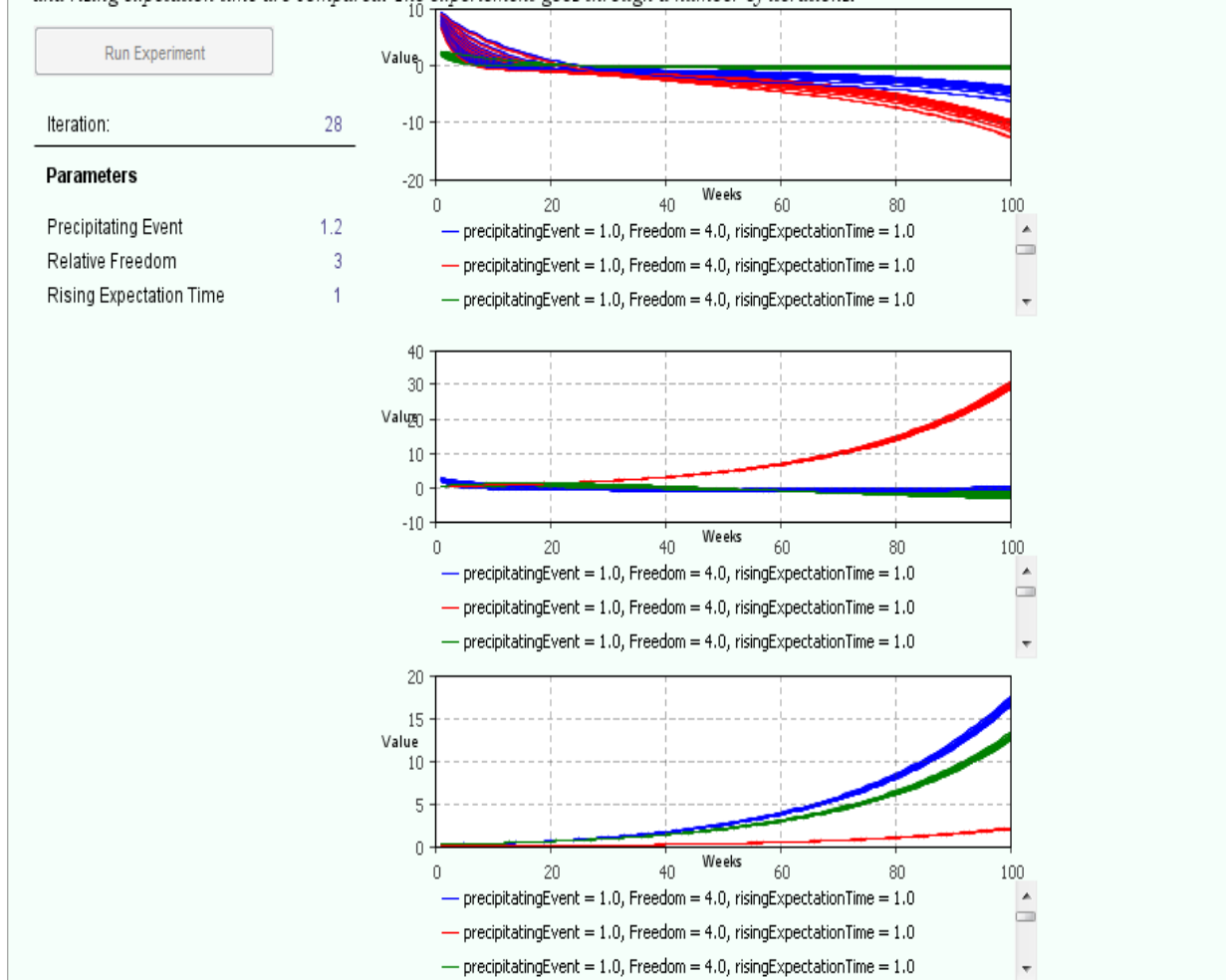


Figure 17: Parameter variation experiment

### 4.8 Application

The insider cyber threat is hard to detect and an even harder to predict. The research described so far suggests that any attempt to seriously address the insider threat, particularly through proactive means, must consider behavioral indicators in the workplace in addition to the more traditional workstation monitoring methods.

Identifying behavioral indicators is difficult and requires training, which requires that managers' and HR staff's awareness and skills is continuously increased to help them recognize potential risks and to assist in dealing with severe insider threat risks. It may not be feasible to employ

many experts in a large organization, but doing so in a computer-based decision aid will help ensure that the “system” is applied consistently and fairly. The model automates this process, given that the organization implements employee performance management system that deposit behavioral assessments in a database of personnel files at regular intervals during the course of the evaluation period.

Managers and HR staff do understand incidents and issues relating to “concerning behaviors” such as increasing complaints to supervisors regarding salary, refusal to work with new supervisors, increased outbursts directed at coworkers, and isolation from coworkers (E. Cole and S. Ring, 2006). In most cases, management is aware of the most serious behaviors as well as indicators of concerning behaviors which may appear 1 to 48 months before the attack (E. D. Shaw and L. F. Fischer, 2005). This provides a window of opportunity during which employers’ awareness of risk linked to effective interventions could reduce the threat of an attack. Randazzo et al. reported that eighty percent of insider cases in their study raised official attention for concerning behaviors such as tardiness, truancy, arguments with coworkers, and poor job performance; and in 97% of those cases, supervisors, coworkers, and subordinates were aware of these issues. However, typically there is no formal infrastructure for recording and tracking such behaviors, except when they become critical to the point where disciplinary action is taken.

Within organizations, a system for collecting and tracking reported concerning behaviors will enable objective examination of these data and their integration with physical and cyber monitoring data to derive a complete picture of potential malicious employees and insider threats.

It has been argued that insider threat assessment based on screening of personal characteristics will be imperfect because malicious insiders do not share a common profile and that characteristics of bad actors are shared by good actors; and “Because the set of malicious insiders is small and diverse, no single personal characteristic or set of characteristics can act as a reliable predictor of future misbehavior,” (S. L. Pfleeger, et al, 2010). We do not advocate a model based only on personal characteristics, but rather a model that integrates multiple sources of data—consistent with Schultz advocacy for systems that monitor and analyze numerous clues of diverse types, including personal characteristics and suspicious cyber activities.

Analysis of outputs from a psychosocial model and other more conventional workstation activity monitoring would be used in informed decisions of a multidisciplinary team comprising management, HR, security, cyber-security personnel, as well as a counterintelligence officer for the most serious transgressions. Most importantly, the automated decision aid would be used only to inform and advise—not to invoke unilateral sanctions.

## **CHAPTER FIVE: CONCLUSIONS AND RECOMMENDATIONS**

This chapter presents project achievements, challenges, limitations, conclusion, recommendations and a brief description of potential future works.

### **5.1 Achievements**

The research began with identification of the problem and the formulation of research objectives intended to address the insider threat problem. From the literature reviewed, no research has been undertaken locally to address the insider threat, more so the factors that predispose individuals to commit insider attacks on critical systems.

This report presents a predictive model based on human behavior that determines the individual's predisposition to malicious activities. To address the problem, the researcher developed three research questions for each of the research objectives which are 1). Which human behavioral factors influence the insider cyber threats to organization's systems? 2). Is it possible to come up with a simulation model that can predict the insider cyber threat and differentiate normal from malicious behavior? 3). How effective would the model be in predicting cyber threats?

The researcher was able to review literature on modeling, simulation, system dynamics and agent based development to better understand studies already conducted in the area of insider threats. The review led to the identification of psychosocial factors that predispose individuals to cause harm to organization's information systems.

From the factors identified, the researcher was able to develop a conceptual model that was eventually developed into Insider Threat Predictive Model (ITPM) that used a hybrid of the agent-based modeling and system dynamics.

The researcher used the System Dynamics modeling technique which is employed in causal relationships to understand the behavior of complex systems by employing feedback loops and the stocks and flows. Thus, the causal loop diagrams are used to visualize the systems structure

and behavior as well as qualitatively analyzing the system. To perform more quantitative analysis, the causal loop is transformed into a stock and flow diagram. The stock and flow model is built and simulated using the AnyLogic program.

In the local context, research has been lacking in the field of insider cyber threats while most organizations have had experiences with breaches of security, fraud, espionage as well as sabotage of operations as shown in the results of insider interviews.

The lack of data on insider threat and unwillingness to disclose material on insider attacks has hampered survey in insider threats. The overall objective of this research was to create a model to predict insider cyber threats and determine through simulation whether human behavior plays an important role in influencing insiders to commit malicious acts. This model is supposed to identify and differentiate normal individuals from abnormal ones as a way of providing management with a holistic approach towards monitoring the activities of a few individuals whose activities tend towards malicious acts.

Objectives to address the problem were defined and research questions for each formulated to assist in achieving them.

***Objective 1: To identify psychosocial factors and determine their influence on human behavior.***

This objective set out to identify the psychosocial factors that predispose individuals to malicious activities. To achieve the above objective, the researcher developed the following question: Which human behavioral factors have the most influence on the insider cyber threats to organization's systems?

From literature review, a number of psychosocial factors were identified. The indicators range from disgruntlement, not accepting feedback, anger management, disengagement among others. For each indicator, its frequency of occurrence and weight was obtained from the judgments of two HR experts. This is shown in Table 1 and Table 5 respectively.



***Objective 2: To create a model based on human behavior that provides indicators for potential risk for insider cyber threats.***

In order to achieve the above object, the following question was developed: Is it possible to come up with a simulation model that can predict the insider cyber threat and differentiate normal from malicious behavior?

From the literature review, we determined there was a need for a new model to predict insider cyber threats. In most of the cases, insider threat study focused on processes and technology, leaving out the human element. In situations where prediction was employed, it relied on logs and technical controls unlike this study which focuses on human behavior as a basis for predicting malicious behavior.

***Objective 3: To show that the model can differentiate between normal and malicious employee who has caused harm to an organization.***

The research question which assisted in answering this objective was: How effective would the model be in predicting cyber threats?

To answer the question, we verified and validated the model through simulation in which a group of agents were subjected to the behavioral factors. Through simulation, agents who expressed some of the factors turned red showing abnormal behavior while those not predisposed remained blue. This confirmed that the model could differentiate normal individuals from abnormal ones.

As individuals join organizations, their behavior is recorded through various instruments such as performance management systems and disciplinary processes where applicable. Thus, in situations where the HR or security personnel suspect or come across any unbecoming behavior, such incidents are recorded and fed into the system.

The model was able to differentiate normal and malicious insider through the agent based modeling process. Additionally, the model is robust, and can be adopted to include technical as well as organizational factors that influence individuals to commit malicious acts.

If implemented, the Insider Threat Prediction Model would aid security personnel by generating clear indicators for flagging employees with increased risk for performing insider threat damage.

The model has also shown that these indicators are available early in a malicious insider's career, which could directly lead to measures that reduce insider threat damage.

While an empirical test is the ultimate aim, other evaluation approaches can be used to test aspects of the model. An objective in validating the psychosocial component of the model was to demonstrate agreement between the model and observables.

Verification has been accomplished by using expert views in examining the observables used by the model. Evaluations used case studies, of reported and documented cases.

## **5.2 Research Contribution**

This research recognizes that behavioral indicators are difficult to understand and require that management and HR personnel are well trained to identify concerning behaviors. It is critical that management and HR staff is given awareness and skills to recognize potential risks to enable them monitor employee behavior. However, for a large organization, training large numbers of experts is not feasible. Therefore, the expertise can be used in a computer based system to help ensure the system is standardized and employed more efficiently in assessing employee behavior.

### **5.2.1 Model framework**

The researcher looked at the extent to which the model-based approach contributed to greater understanding of the insider cyber threats. In this case we asked whether similar or better

results would have been obtained without the development of the system dynamics models. The system dynamics approach helped to structure and focuses the research where the researcher identified the primary variables of interest, the influences between these variables, and the feedback loops that are so important for understanding complex behavior.

By looking at the total context of adverse insider behavior we were able to understand why such incidents happened and how they might be prevented in the future. In most instances research on insider threats especially espionage, sabotage, theft or cybercrime focused on the individual offender and his or her personal history, psychological defects, or external inducements a way of understanding the crime or offense. By employing the system dynamics approach we attempt to assess the weight and interrelatedness of personal, organizational, and social factors as well as the effectiveness of deterrent measures in the workplace.

The model addresses two strategies for mitigating insider threat. First, all employees have been granted access to organization assets and therefore introduce vulnerabilities. By recognizing that all employees are insiders, and therefore threats to the organization, the model considers the relationship between individuals within an organization (See Figure 5). An organization that implements the model learns who is trustworthy, but its employees learn as well, because they are assured that anyone causing harm is removed.

The model is a valuable tool to add to the suite of tools available to the organization's security personnel as well as more deterrence to keep employees in line. The model assists management and security personnel by identifying employees with the highest potential of causing harm, as well as correcting unacceptable behavior and holding employees accountable for their actions as soon as they cross the line or possibly before by providing sufficient records of observable behavior leading up to a potential incident of insider damage.

It is not possible to completely eliminate insider threat, but the objective of this study is to ensure the threat to organization information or information systems is minimized as much as

possible by significantly reducing information system vulnerabilities to a wide range of misuse and abuse.

### **5.2.2 Data sharing**

This study shows to be able to effectively deal with insider cyber threats, that the industry and government must share case data, research, policies, and methods with regard to insider risk mitigation. There is always a challenge in the areas of personnel screening and selection, detection of at-risk behaviors, and effective investigation of, and, intervention with, persons at risk.

With emphasis on individual accountability using personnel policies such as performance management tools and deployed technology, organizations must rely on existing protection technologies and publicized deterrence policies to stem the tide of insider damage. Even with maximum employment of data mining technologies “to detect anomalous behavior and thus provide advanced warning of an increased security risk” insiders are typically caught only after causing significant damage. Even by improving deterrence visibly, organizations still need more effective “methods and tools that improve deterrence. The Insider Threat Prediction Model augments all of these activities, first by identifying and recognizing psychosocial factors that predispose individuals to cause harm, then by pre-loading data mining activities with data regarding individual employee risk levels and finally by serving as an effective method of deterrence.

### **5.2.3 Employee vetting, auditing and monitoring**

Individuals who attacked systems 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 vetting, monitoring and auditing of individual employee technical activity when concerning behaviors are noted following some stressful event.

The research may be useful in personnel management by establishing “Employee Assistance Programs for those who, through no fault of their own, encounter personal problems for which they are unable to cope without assistance” and requiring that “managers and supervisors must live up to the expectation that they evaluate personnel effectiveness daily, develop the skills to recognize individuals who require special assistance and provide the avenue for them to acquire that assistance. The model assists supervisors in recognizing which employees are in need of assistance, and produces a record of events and heightened risk level. The fact that supervisors evaluate employees regularly ensures the model works to its fullest potential.

#### **5.2.4 Management training and awareness programs**

Personal predispositions, stressful events and sanctions played a key role in insider cases used in the study. 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 cases 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

Organizations would be better placed to consider the benefits of periodic security awareness training for all employees in addition to the management training programs. The cases studied show the individuals exhibited observable behavior and technical actions detailed that could have alerted their organizations to severe disgruntlement and potential malicious intent. The first people to notice changes in behavior are fellow employees, as such; it could be beneficial for all employees to recognize their responsibility for reporting concerning behaviors and concerning technical actions to management for follow up.

The Insider Threat Prediction Model places emphasis on security awareness, improving personnel security practices, and continued research in Information Technology (IT) systems and personnel management. This activity tries to place the focus on heightening security awareness, rather than on mitigating insider threat with IT, which is an essential aid, but not a solution. The model clearly heightens security awareness by identifying the personnel within an organization that have increased risk of causing insider damage. It therefore indicates that for an organization to establish good personnel security practices to mitigate insider threat, it must begin with personnel selection and determination of suitability for service.

### **5.3 Limitations of the Research**

While the study produced useful results, it also has some limitations.

#### **5.3.1 Lack of sufficient real-world data**

Locally, no empirical studies have been conducted on insider threats and its mitigating factors. Data used in the study are from records of cases that have been conducted in USA. This results in inadequate data for scientific verification and validation of the proposed model.

#### **5.3.2 Differences in expert judgment**

Further difficulties arise from the fact that data are collected over long time spans, making it difficult for experts to comprehend and reason about large volumes of data. Experts also may vary in their assessments of risk for a given set of indicators, depending on their background

and experiences. In addition, while it is reasonable for experts to validate the findings of the system to perceived matches to insider threats; it is not practical for experts to examine all the observables for monitored subjects to determine which of them should be flagged. A confounding problem is that experts could find evidence of a threat that is not modeled by the system, causing difficulties in the interpretation of test results.

### **5.3.3 False alerts**

The data collected as well as cases used in the study provided useful information for identifying persons whose behavior may lead to a breach of security on critical systems. While the concerning behaviors could be easily identified, it was not easy to differentiate malicious individuals from non-malicious ones as some of the factors may be exhibited even by those who mean no harm to organizations. Therefore, the possibility of ignoring individuals with higher risk of harm while focusing on those without as a result of false negative alarm and vice versa is real.

## **5.4 Research Conclusions**

This section highlights the key findings in form of conclusions from the work done during the study.

The Insider Threat Prediction Model (ITPM) is a useful tool that can be applied in many organizations to identify employees whose behavior may compromise security of information assets. This predictive modeling approach to insider threat that use psychosocial data automates the various factors with a focus on insider's expectation of freedom, disgruntlement and escalation of the same with severe sanctions initiated.

While the research shows that men exhibited malicious behavior more than women, there is need to continue monitoring and evaluating behavior of all personnel at the work place. This will assist in identifying employees who are more at risk as well as those who are likely tube coerced into malicious acts.

The insider cyber threat, especially espionage and sabotage is among the most pressing cyber security challenges that threaten government and industry information infrastructures. However, lack of real world data and the sensitivity with which organizations handle security issues makes progress in this area difficult. The current practice tends to be reactive as it focuses on detecting malicious acts after they occur with the aim of identifying and disciplining the perpetrator. The objective of this research is to develop a predictive that uses psychosocial indicators of potential abuse of network resources or systems to predict possible malicious exploits. Some indicators may be observed directly, while others are inferred or derived from observed data. Defining possible precursors in terms of behavioral observable cyber and psychosocial indicators is a major challenge in developing a predictive methodology.

An informed and enlightened organization requires that management and HR staff be equipped with tools to maintain awareness of worker satisfaction and well-being—but not overstepping ethical and privacy boundaries—that enables thoughtful, proactive responses to situations that increase the risk of insider threat activity.

The research is used to determine whether or not an effective interactive learning environment could be developed to teach executives, managers, technical staff, human resource staff, and security officers the complex dynamics of the insider threat problem.

At this point, we feel confident that an effective model that conveys important lessons regarding insider threat has been created. The simulations accurately mimic the patterns and trends in the majority of the cases in this study.

### **5.5 Further research**

The Insider Threat Prediction Model (ITPM) uses human behavior concepts to mitigate insider threat by predicting which employees are higher risks for becoming malicious insiders. Research in this area is still in the formative stages and the model serves as a basis for further research involving human influences and modeling.



The results from this study could be used as a baseline for the construction of a risk indicator instrument to assess individual behavior and technical actions that may be a threat to organization's systems. 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.

Researchers could use this tool to 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.

There will be need to identify and better understand effective risk mitigations by collecting data on what policies, practices and technologies are being successfully implemented for insider threat prevention and detection.

Some of the areas for possible future research include:

- Behavioral Profiling - there is need to further develop and update predictive behavioral indicators of malicious insider threats; the research need is focused on refinement of a taxonomy or characterization that captures insiders—behaviors, motives, methods, and psychological factors.
- Intrusion Detection - increased focus should be on host-based insider detection and centralized situation awareness of distributed sensor data.
- The development of methods and tools for prediction to prevent or limit impact of insider exploits.
- Effective frameworks or methods for testing and evaluating the performance of predictive insider threat models. Major problems concern the lack of appropriate data sets, lack of ground truth, and challenges surrounding the acquisition and storage of test data because of organizational constraints.

Finally, the purpose of this research was to show the need for and present a model useful to security personnel in mitigating insider threat.

## REFERENCES

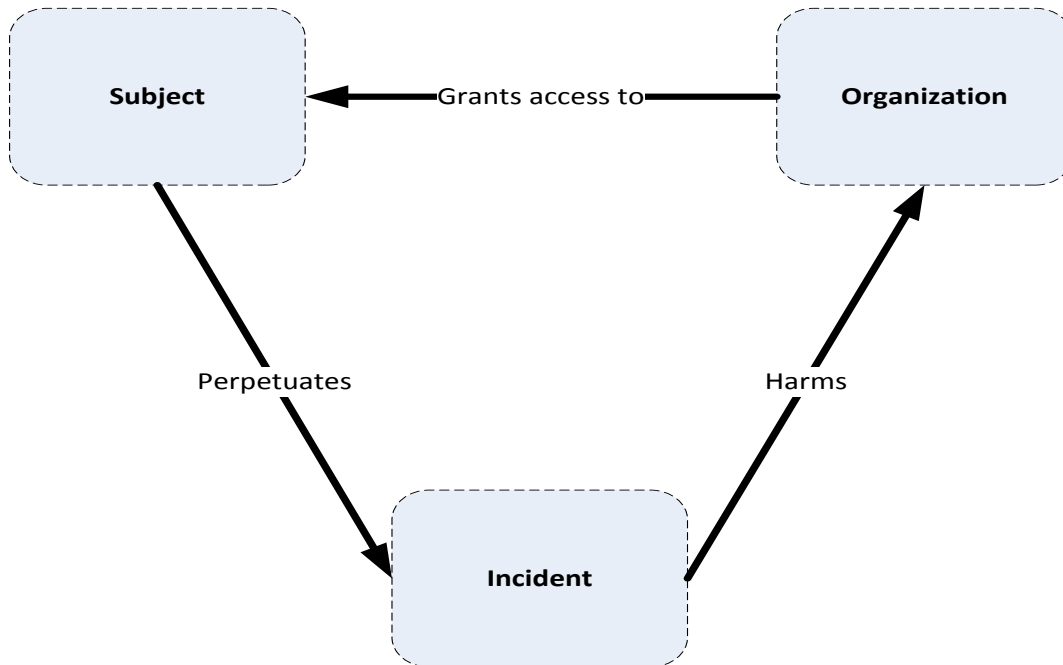
1. Andersen, D. F., D. Cappelli, et al., Preliminary System Dynamics Maps of the Insider Cyber-threat Problem. 22nd International Conference of the System Dynamics Society, Oxford, UK, 2004.
2. Baker, W.H., Hylender, C.D. & Valentine, J.A., Data Breach Investigations Report, 2008. Obtained from [www.verizonbusiness.com](http://www.verizonbusiness.com), October 2008.
3. Butts, J.W., Mills, R.F. & Baldwin, R.O., Developing an Insider Threat Model Using Functional Decomposition. In Proceedings of the Third international workshop on mathematical methods, models, and architectures for computer network security (St. Petersburg, Russia, September 25-27), pp. 412-417, 2005.
4. C. P. Pfleeger, *Reflections on the Insider Threat*. Springer, 2008, Ch. in [71].
5. E. Cole and S. Ring, *Insider Threat: Protecting the Enterprise from Sabotage, Spying and Theft*. Rockland, MA: Syngress Publishing, 2006.
6. E. D. Shaw and L. F. Fischer, "Ten tales of betrayal: the threat to corporate infrastructures by information technology insiders. Report 1 - overview and general observations," Defense Personnel Security Research Center, Monterey, CA TR 05-04, 2005.
7. E. Eugene Schultz, "A framework for understanding and predicting insider attacks," *Computers and Security*, vol. 21, pp. 526-531, Oct. 2002.
8. F.L. Greitzer, A.P. Moore, D.M. Cappelli, D.H. Andrews, L. Carroll, T.D. Hull, Combating the Insider Cyber Threat. *IEEE Security & Privacy* 6(1):61-64, 2008.
9. Forrester, J.W. *Principles of Systems*. Cambridge, MA: Wright-Allen Press, 1968.
10. G. Ali, N.A. Shaikh, Z.A. Shaikh, Towards An Automated Multiagent System to Monitor User Activities Against Insider Threat. Proceedings of the International Symposium on Biometrics and Security Technologies, IEEE-ISBAST 2008, Islamabad, Pakistan, pp. 1-5, 2008. [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=312685](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=312685).
11. J. Predd, S. L. Pfleeger, J. Hunker, and C. Bulford, "Insiders behaving badly," *IEEE Security and Privacy*, vol. 6, pp. 66-70, July 2008. [Online]. Available: <http://portal.acm.org/citation.cfm?id=1441365.1441416>

12. J.D. Sterman, *Business Dynamics: Systems Thinking and Modeling for a Complex World*. McGraw-Hill/Irwin: New York, 2000.
13. Jay W. Forrester, *Industrial Dynamics*. Pegasus Communications. ISBN 1883823366, 1961.
14. K. Brancik and G. Ghinita, "The optimization of situational awareness for insider threat detection," in *Proc. of the 2011 ACM conference on Data and application security and privacy (CODASPY'11)*, San Antonio, Texas, USA. ACM, February 2011, pp. 231–236.
15. Kandias , Miltiadis, Alexios Mylonas, Nikos Virvilis, Marianthi Theoharidou, and Dimitris Gritzalis, "An Insider Threat Prediction Model", *Lecture Notes in Computer Science, 2010, Volume 6264, Trust, Privacy and Security in Digital Business*, pp. 26-37
16. M. Bishop, "The insider problem revisited," in *Proc. of New Security Paradigms Workshop 2005 (NSPW'05)*, Lake Arrowhead, California, USA. ACM Press, September 2005, pp. 75–76.
17. M. McCormick, *Data Theft: A Prototypical Insider Threat*. In *Advances in Information Security*, 2008.
18. M.M. Keeney, E.F. Kowalski, D.M. Cappelli, A.P. Moore, T.J. Shimeall, S.N. Rogers et al, *Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors*. Joint SEI and U.S. Secret Service Report, Pittsburgh, PA, 1-45, 2005.
19. Martínez-Moyano, I.J. "Structure as Behavior: Exploring Elements of the System Dynamics Modeling Process," *Proceedings of the 21st International Conference of the System Society*, New York, New York, 2003
20. Moore, A. P., D. M. Cappelli, & R. F. Trzeciak (2008). *The "Big Picture" of Insider IT Sabotage Across U.S. Critical Infrastructures*. Software Engineering Institute, Carnegie Mellon University, May 2008.
21. Pare, G., *Investigating Information Systems with positivist case study research*, *Communications of the Association for Information Systems* 13, pp. 233-264, 2004.
22. R.K. Yin. *Case Study Research: Design and Methods*. Sage, 4th edition, 2009.
23. Randazzo, M. R., M. M. Keeney, et al., *Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector*, U.S. Secret Service and CERT Coordination Center / Software Engineering Institute: 25, 2004.

24. Richardson, G. P.. Definition of system dynamics. In *Encyclopedia of Operations Research and Management Science*, S. I. Gass and C. M. Harris, Eds. Kluwer Academic Publishers, Boston, MA, 656–660, 1996.
25. S. L. Pfleeger, et al., "Insiders behaving badly: addressing bad actors and their actions," *IEEE Transactions on Information Forensics and Security*, vol. 5, pp. 169-179, 2010.
26. S. R. Band, Lynn F. Fischer, Andrew P. Moore, Eric D. Shaw, Randall F. Trzeciak, Comparing Insider IT sabotage and espionage: A Model based Analysis., CMU/SEI-2006-TR-026, 2006.
27. Sackett, Paul R. & DeVore, Cynthia J. Ch. 5, "Counterproductive Behaviors at Work," 145-164. *Handbook of Industrial, Work and Organizational Psychology*, Sage, 2001.
28. Sackett, Paul R. "The Structure of Counterproductive Work Behaviors: Dimensionality and Relationships with Facets of Job Performance." *International Journal of Selection and Assessment* 10 (2002): 5-11.
29. Serianu, Kenya Cyber Security Report, 2012.
30. Sterman, J. D.. *Business Dynamics: Systems Thinking and Modeling for a Complex World*. Irwin McGraw-Hill, Boston, MA, 2000.
31. W. Eberle and L. Holder, "Graph-based approaches to insider threat detection," in *Proc. of the 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies (CSIIRW'09)*, Knoxville, TN, USA. ACM, April 2009.

## APPENDIX I: STRUCTURE OF INSIDER THREAT DATABASE

At higher levels, the insider threat database consists of three entities: organization(s) involved; the subject (insider); and the details of the incident. Figure 18 below shows the relationship among the three entities.



*Figure 18: High-level Structure of Insider Threat Database*

### **Organization Data**

Multiple organizations can be involved in a single incident. An organization that is negatively impacted by an incident is designated as a victim organization. Incidents may also involve the victim organization's trusted business partner. In these incidents, the malicious insider is not directly employed by the victim organization, but is able to attack the victim organization via access authorized by a contractual relationship with the insider's employer.

Incidents, particularly those involving theft of IP, may also involve a beneficiary organization—an organization that knowingly or unknowingly benefits from the incident to the detriment of the victim organization. When entering case data into the insider threat database, we identify the organization and any organizational issues relevant to the case, as shown in Table 7.

<b>Organization Category</b>	<b>Information Collected in the Database</b>
Organization Identity	name, address, relation to insider
Organization Type	victim, beneficiary, trusted business partner, other
Organization Description	description of the organization
Industry	critical infrastructure sector of the organization
Location	location of the organization
Organization issues	work environment, such as hostile work environment or culture of mistrust, and layoffs, mergers, and acquisitions, reorganizations, and other workplace events that may have contributed to an insider’s decision to act
Opportunity Provided to Insider	actions taken by an organization that may have contributed to the insider’s decision to take action (such as demotions or transfers of employees); failure on the part of the organization to take action based on concerning behaviors or other events, actions, or conditions; or vulnerabilities, for example, insufficient monitoring of external access

*Table 7: Organization information collected*

## Subject Data

We collect as many details as possible about the insider, including details regarding planning activities.

These details are generally discovered after an incident has already occurred, but they are essential to preventing future insider threats. We also collect information about the insider's accomplices, including demographic data, the accomplice's relationship to the insider and the victim organization, and the accomplice's role in the incident.

We do not make any judgments about the insider or attempt to diagnose his or her behavior; we code exactly what we find in the source materials.

<b>Subject Category</b>	<b>Information Collected in the Database</b>
Subject Identity	name, gender, age, citizenship, residence, education, employee title/type/status, departure date, tenure, access, position
Motives and Unmet Expectations	motives (financial, curiosity, ideology, recognition, external benefit), unmet expectations (promotion, workload, financial, usage)
Concerning Behaviors	tardiness, insubordination, absences, complaints, drug/alcohol abuse, disgruntlement, coworker/ supervisor conflict, violence, harassment, poor performance, poor hygiene, etc.
Violation History	security violations, resource misuse, complaints, deception about background
Consequences	reprimands, transfers, demotion, HR reports, termination, suspension, access revocation, counseling

Substance Abuse	alcohol, hallucinogens, marijuana, amphetamines, cocaine, sedatives, heroin, inhalants
Planning and Deception	prior planning activities, explicit deceptions

Table 8: Subject information collected

**Incident Data**

The information we collect about an incident includes individual actions taken to set up the attack, vulnerabilities exploited during the attack, steps taken to conceal it, the way the incident was detected, and the impact on the victim organization. In addition, we also collect data on the victim organization’s response to the incident and events and conditions that may have contributed to an insider’s decision to attack. Table 9 describes the incident attributes in more detail.

<b>Incident Category</b>	<b>Information Collected in the Database</b>
Case summary	incident dates, duration, prosecution
Conspirators	accomplices, type of collusion, relationships to insider
Information Sources	origin type
Incident Chronology	sequence, date, place, event
Investigation and Capture	how the insider was identified and caught
Prosecution Result	indictment, subject’s story, sentence, case outcome
Recruitment	outside/competitor induced, insider collusion, outsider collusion, acted alone, reasons for collusion
IT Accounts Used	subject’s, organization’s, system administrator’s, database administrator’s, co-



	worker's, authorized third parties, shared, back door
Outcome	data copied/deleted/read/modified/created/disclosed, identity theft, creation of unauthorized document, denial of service
Impact	description, financial
How Detected	software, information system, audit, non-technical, system failure
Who Detected	self-reported, it staff, other internal; customer, law enforcement, competitor, other external

*Table 9: Incident Information Collected*

## APPENDIX II: QUESTIONNAIRE

### QUANTITATIVE QUESTIONNAIRE

Date:

Serial Number:

Dear Sir/Madam,

*You are invited to participate in a research study investigating the influence human behavior plays in insider cyber-attack. You are selected because of your role as a user of technology resources within your organization, and thus being an insider. This questionnaire is therefore designed to collect data to help determine the psychosocial factors that influence malicious insiders to attack systems. Through this study, an attempt will be made to model and simulate the insider cyber security threats by examining whether human behavior plays an important role in influencing insiders to attack systems.*

*If you agree to participate, you will be required to fill out a simple survey that takes approximately 10-15 minutes of your time to complete. The information gathered from this study will help future researchers and security personnel in organizations dealing with information resources.*

*The information collected through your participation will be used to fulfill an educational requirement and may be published in a professional journal or presented at a professional meeting.*

*Thank you.*

*Ogonji Mark.*

*e-mail: [mmogonji@yahoo.com](mailto:mmogonji@yahoo.com)*

*Student University of Nairobi.*

<b>PART I: DEMOGRAPHICS</b>		
Your Name: {optional}		
Contact details: (Phone, e-mail)		
Gender	Male Female	<input type="checkbox"/> <input type="checkbox"/>
Which of the following best describes your current position within the organization?	Management  Administrative or Support Staff  Other	<input type="checkbox"/>  <input type="checkbox"/>  <input type="checkbox"/>
The total length of time you have been a member of the organization	Less than 1 year  1 year to less than 5 years  5 years to less than 10 years  10 years to less than 15 years  15 years to less than 20 years  More than 20 years	<input type="checkbox"/>  <input type="checkbox"/>  <input type="checkbox"/>  <input type="checkbox"/>  <input type="checkbox"/>

<b>PART II: COMPONENTS OF THE INCIDENT</b>		
Behaviors of Concern that Prompted investigation (Tick whichever applies)	<p>Work-related violations <input type="checkbox"/></p> <p>Threatening behavior <input type="checkbox"/></p> <p>Financial difficulties <input type="checkbox"/></p> <p>Technical violations <input type="checkbox"/></p> <p>Disloyalty <input type="checkbox"/></p> <p>Social skills and decision making deficits <input type="checkbox"/></p> <p>Unusual needs for attention, sense of entitlement <input type="checkbox"/></p> <p>History of legal, security or procedural rule violations prior to attack <input type="checkbox"/></p>	
Subject Factors:	<p>Is the subject or suspect identified? (Yes/No)</p> <p>Are there other potential accomplices? (Yes/No)</p>	

	<p>What are the potential motives for the behaviors of concern?</p> <ul style="list-style-type: none"> <li>- Financial <input type="checkbox"/></li> <li>- Revenge <input type="checkbox"/></li> <li>- Recognition <input type="checkbox"/></li> <li>- Disgruntlement <input type="checkbox"/></li> <li>- disloyalty <input type="checkbox"/></li> </ul> <p>What personal characteristics of subject enhance and/or mitigate the threat?</p> <ul style="list-style-type: none"> <li>- Drug involvement <input type="checkbox"/></li> <li>- Alcohol abuse <input type="checkbox"/></li> <li>- Sexual behavior <input type="checkbox"/></li> <li>- Personal conduct <input type="checkbox"/></li> <li>- Foreign influence (allegiance) <input type="checkbox"/></li> <li>- Emotional, mental and personality disorders. <input type="checkbox"/></li> </ul>	
--	---	--

	<ul style="list-style-type: none"> <li>- Criminal conduct <input type="checkbox"/></li>   <li>- Security violations <input type="checkbox"/></li>   <li>How capable is the subject in carrying out the threat (e.g. access, expertise)?</li> <li>- Very capable <input type="checkbox"/></li>   <li>- Capable <input type="checkbox"/></li>   <li>- Moderately capable <input type="checkbox"/></li>   <li>- Not capable <input type="checkbox"/></li>   <li>What is the subject's personal situation?</li> <li>- Indebted <input type="checkbox"/></li>   <li>- Stressed <input type="checkbox"/></li>   <li>- Family issues <input type="checkbox"/></li>   <li>- Medical issue <input type="checkbox"/></li> </ul>	
Insider's behavior	Did insider's previous behavior have an effect on current behavior? Yes/No.	
Protective Factors	What are the human, technical and physical security measures in place?	

	<p>What protective resources may have been compromised?</p> <p>What was necessary to compromise protective factors?</p> <ul style="list-style-type: none"> <li>- behavior</li> <li>- technical expertise</li> <li>- level of access</li> </ul>	<p>[ ]</p> <p>[ ]</p> <p>[ ]</p>
<p>Organizational</p>	<p>Is there an organizational culture and climate for security and reporting? Yes/No</p> <p>Has there been a reported case of security compromise? Yes/No</p> <p>Are there recent events that could affect security and/or risk? (Yes/No)</p> <p>What is the nature of the asset being targeted within the organization?</p> <ul style="list-style-type: none"> <li>- Personnel data</li> <li>- Proprietary company information</li> <li>- designs</li> </ul> <p>What situational or contextual factors relate to the breach or attempted breach?</p> <ul style="list-style-type: none"> <li>- Political</li> </ul>	<p>[ ]</p> <p>[ ]</p> <p>[ ]</p> <p>[ ]</p> <p>[ ]</p>

	- Media	[ ]
	- social	[ ]



### APPENDIX III: MAPPING INSIDER CASES TO OBSERVATIONS

(X- Observation Exhibited, N-Observation Not Exhibited, U-Unknown if Observation was Exhibited)

Indicator	Cases										
	Am es	Ander son	Aragonc illo	Hanss en	Hoff man	Mont es	Pe ri	Reg an	Smi th	Manni ng	Chu ng
Disgruntle ment	X	X	X	X	X	X	X	X	X	X	X
Not Accepting Feedback	X	X	X	X	X	X	X	X	X	X	X
Anger Manageme nt Issues	X	X	X	X	X	X	X	X	X	X	X
Disengage ment	X	X	X	X	X	X	X	X	X	X	X
Disregard for Authority	X	X	X	X	X	X	X	X	X	X	X
Performan ce	X	X	X	X	X	X	X	X	X	X	X
Stress	X	U	X	X	X	U	X	X	U	X	X
Confrontat ional Behavior	X	X	X	X	X	X	X	X	X	X	X
Personal Issues	X	X	X	X	X	X	X	X	X	X	X

Self-Centeredness	X	X	X	X	X	X	X	X	X	X	X
Lack of Dependability	X	X	X	X	X	X	X	X	X	X	X
Absenteeism	X	X	X	X	X	X	X	X	X	X	X

Table 10: Observables mapped to cases

## **APPENDIX IV: CRITERIA FOR PERSONAL PREDISPOSITIONS**

### **SERIOUS MENTAL HEALTH DISORDERS**

In some cases insiders were found to have suffered from 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:

- we're 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

Examples of evidence of the presence of serious mental health disorders from the sample included Ames's and Walker's alcoholism; Regan's reported prescriptions for antipsychotics, Prozac, and his alcohol abuse; and Smith's reported alcoholism and need for mental health treatment.

### **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 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 the samples 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

Examples of individuals exhibiting such behaviors from the 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 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 cases, Hanssen, Ames, Regan, and Peri all displayed social skills deficits ranging from withdrawal to bullying.

#### HISTORY OF RULE VIOLATIONS

Insiders sampled 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. Among the identified 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 malicious activities. Table 11 provides the personal predisposition for each case.

Insider	Definition	Observables	Cases
Personal			

<b>Predisposition</b>			
<p>Serious mental health disorder</p>	<p>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.</p>	<p>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).</p>	<p>Ames Smith Regan Anderson</p>
<p>Personality</p>	<p>There are consistent</p>	<p>Unusual needs for</p>	<p>Regan</p>

<p>problems that result in biased perceptions of self and others</p>	<p>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.</p>	<p>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</p>	<p>Hanssen Ames Smith Anderson Hoffman</p>
<p>Social skills and decision making deficits</p>	<p>Problems relating to others, especially appreciating</p>	<p>Isolation from the group, propensity for interpersonal conflicts</p>	<p>Regan Peri</p>

	<p>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.</p>	<p>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 sociopath.</p>	<p>Hanssen  Ames  Smith  Anderson</p>
<p>History of legal, security or procedural</p>	<p>Prior criminal offenses, hacking, security violations,</p>	<p>Arrests, hacking, security violations, harassment</p>	<p>Ames  Hanssen</p>



<p>rule violations prior to attack</p>	<p>self-serving conflicts of interest or activities indicating a serious disregard for important social rules and expectations.</p>	<p>or conflicts resulting in official sanctions or complaints, misuse of travel, time, expenses.</p>	<p>Hoffman  Aragoncillo  Manning</p>
--	---	--	--

*Table 11: Personal predispositions*

## **APPENDIX V: CASE SUMMARIES**

**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<sup>2</sup>. 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

---

<sup>2</sup>*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"

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 Counter-narcotics 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.

**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<sup>3</sup>. 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.

**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

---

<sup>3</sup>*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’”

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.

**HANSEN, 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<sup>4</sup>. He was arrested in a park near his home in

---

<sup>4</sup>*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”

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 against him 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.

**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<sup>5</sup>. 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.

---

<sup>5</sup>*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<sup>6</sup>. 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.

---

<sup>6</sup>*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”



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."

**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<sup>7</sup>. 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.

**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<sup>8</sup>. On his person

---

<sup>7</sup>*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"

<sup>8</sup>*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"

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.

**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<sup>9</sup>. 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,

---

<sup>9</sup>*Seattle Post-Intelligencer* 14 Apr 2000, "Seaman Admits Stealing Defense Secrets, FBI Says"

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

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.

**CHUNG, GREG**, a former Rockwell and Boeing engineer was in February 2010, sentenced to more than 15 years’ imprisonment for acting as an agent of the PRC and stealing trade secrets about the Space Shuttle, the Delta IV rocket, and the C-17 military cargo jet for the benefit of the Chinese government. In a September 2006 search of Chung’s residence, FBI and NASA agents found more than 250,000 pages of documents from Boeing, Rockwell, and other defense contractors inside the house and in a crawl space underneath the house. Among the documents were scores of binders containing decades’ worth of stress analysis reports, test results, and design information for the Space Shuttle. Chung also sent numerous engineering manuals to the PRC, including 24 manuals relating to the B-1 bomber that Rockwell had prohibited from disclosure outside the company and select federal agencies.

**MANNING, BRADLEY EDWARD** (born December 17, 1987) is a United States Army soldier who was arrested in May 2010 in Iraq on suspicion of having passed classified material to the whistleblower website WikiLeaks. He was charged with a number of offenses, including communicating national defense information to an unauthorized source and aiding the enemy,

a capital offense, though prosecutors said they would not seek the death penalty. He was arraigned in February 2012 at Fort Meade, Maryland, where he declined to enter a plea. The trial is expected to begin in June 2013.

Assigned to an army unit based near Baghdad, Manning had access to databases used by the United States government to transmit classified information. He was arrested after Adrian Lamo, a computer hacker, co-operated with the Department of Defense, stating Manning had confided during online chats that he had downloaded material from these databases and passed it to WikiLeaks. The material included videos of the July 12, 2007 Baghdad airstrike and the 2009 Granai airstrike in Afghanistan; 250,000 United States diplomatic cables; and 500,000 army reports that came to be known as the Iraq War logs and Afghan War logs. It was the largest set of restricted documents ever leaked to the public. Much of it was published by WikiLeaks or its media partners between April and November 2010.

Manning was held from July 2010 in the Marine Corps Brig, Quantico, Virginia, under Prevention of Injury status, which entailed de facto solitary confinement and other restrictions that caused international concern. In April 2011, 295 academics – many of them prominent American legal scholars – signed a letter arguing that the detention conditions violated the United States Constitution. Later that month, the Pentagon transferred him to Fort Leavenworth, allowing him to interact with other detainees.

Reaction to his arrest was mixed. Denver Nicks, one of Manning's biographers, writes that the leaked material, particularly the diplomatic cables, was widely seen as a catalyst for the Arab Spring that began in December 2010, and that Manning was viewed as both a 21st-century Tiananmen Square Tank Man and an embittered traitor. Several commentators focused on why an apparently very unhappy Army private had access to classified material, and why no security measures were in place to prevent unauthorized downloads.

<b>Case</b>	<b>Action</b>	<b>Motive</b>	<b>Precursors</b>	<b>Opportunity</b>	<b>Period</b>
Ames	Espionage – theft of classified information	Financial gain(taking care of his wife)	- Alcoholism - Sexual misconduct	Privileged access	Life

			- Security violations		
Anderson	Espionage	Grudge	- Lack of social acceptance - Bipolar disorder	Privileged access	Life
Aragoncillo	Espionage	Grudge	- No controls	Absence of management control	
Hanssen	Espionage	Ego gratification disgruntlement	Lifestyle	Privileged access	Life
Hoffman	Espionage	Dissatisfaction	- Security violations	Lack of controls	30 years
Montes	Espionage	Grudge	Concerning behavior	- Privileged access - Lack of controls	25 years
Peri	Espionage	Lack of appreciation	- Concerning behavior	Lack of controls	30 years
Regan	Espionage	- Financial - Disgruntlement	- Concerning behavior	Lack of controls	Life
Smith	Espionage	- Felt mistreated - Revenge	- Alcoholism - Mental problems	Lack of controls	260 days
Manning	Espionage	Grudge	- Concerning behavior	Privileged access	

			<ul style="list-style-type: none"> <li>- Disgruntled</li> <li>- Sexual orientation</li> <li>- Family issues</li> </ul>		
Chung	Theft of trade secrets	Financial gain	<ul style="list-style-type: none"> <li>- Work environment discontent</li> </ul>	Privileged access	

*Table 12: Summary of the Insider Cases*

## APPENDIX VI: INSIDER THREAT PREDICTION MODEL

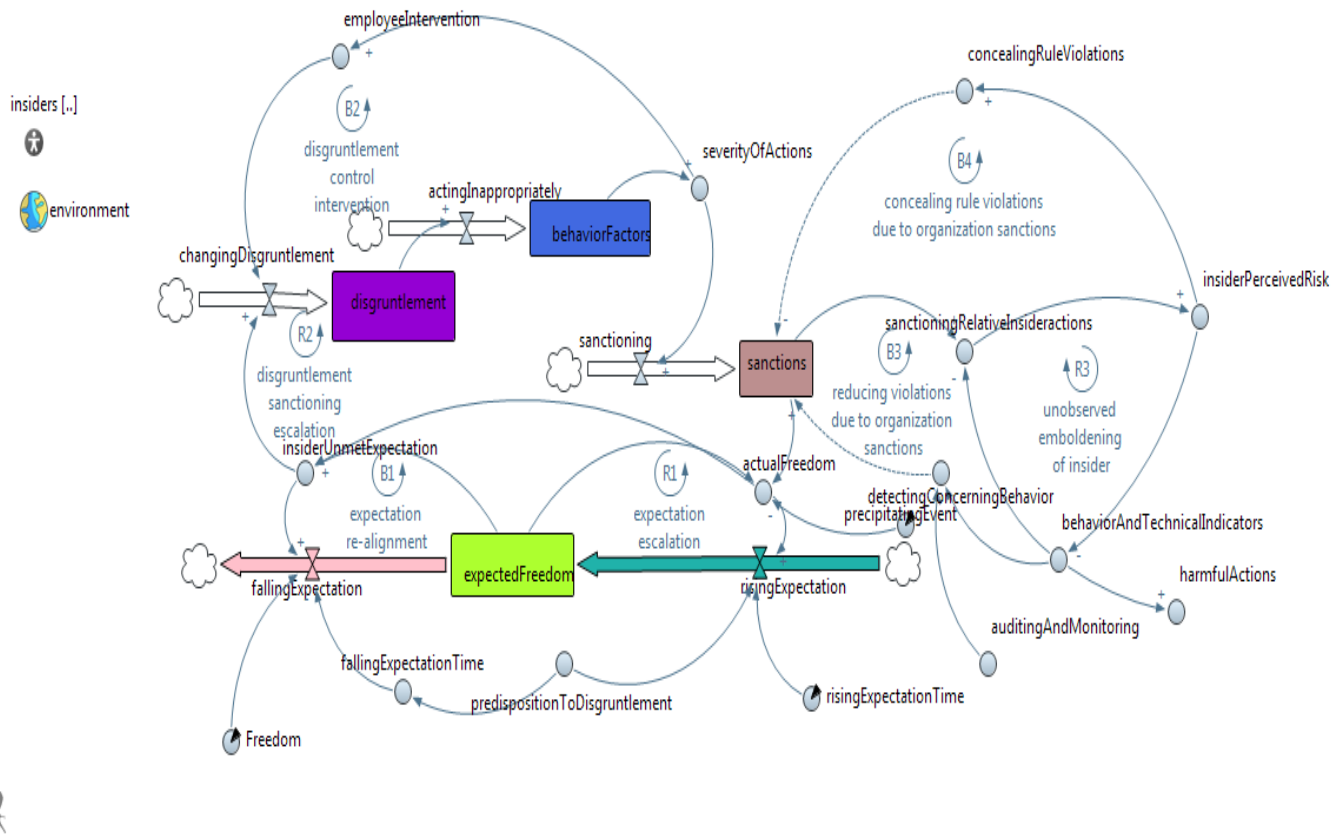


Figure 19: Causal loop of the Insider Threat Prediction Model

Loop Number	Loop Label	Aspect Characterized
B1	Expectation re-alignment	Individual's expectation is based on his actual freedom as well as the predisposition to disgruntlement.
R1	Expectation escalation	With lax management controls actual freedom grows commensurately with expected freedoms. Lack of

		supervision and controls encourages escalation of expectation
<b>B2</b>	Disgruntlement control interventions	The organization's perception of the severity of the <i>Behavioral precursors</i> , determines whether positive intervention or sanctions are warranted.
<b>R2</b>	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.
<b>B3</b>	Reducing violations due to organization 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.
<b>R3</b>	<b>Unobserved emboldening of insider</b>	Left undetected or ignored, rule violations reduce the



		<p>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).</p>
<p><b>B4</b></p>	<p>Concealing rule violations due to organization sanctions</p>	<p>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.</p>

Table 13: Model Feedback Loops