MITIGATING INSIDER THREAT USING HUMAN BEHAVIOR INFLUENCE MODELS

THESIS

Anthony J. Puleo, Captain, USAF

AFIT/GCE/ENG/06-04

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

AFIT/GCE/ENG/06-04

MITIGATING INSIDER THREAT USING HUMAN BEHAVIOR INFLUENCE MODELS

THESIS

Presented to the Faculty

Department of Electrical and Computer Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Computer Engineering

Anthony J. Puleo, BS

Captain, USAF

June 2006

AFIT/GCE/ENG/06-04

MITIGATING INSIDER THREAT USING HUMAN BEHAVIOR INFLUENCE MODELS

Anthony J. Puleo, BS
Captain, USAF

Approved:

/signed/

Robert F. Mills, PhD (Chairman)	Date

/signed/

Gilbert L. Peterson, PhD (Member)	Date

/signed/

Michael R. Grimaila, PhD (Member)	Date

AFIT/GCE/ENG/06-04

Abstract

Insider threat is rapidly becoming the largest information security problem that organizations face. 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 risk-based 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 an in-depth case study on Robert Hanssen, the FBI's double agent who sold the Soviets secrets for more than twenty years.

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.

Acknowledgements

First and foremost, I would like to thank my lovely wife, for her patience and support. There were far too many times when I was present physically, but not mentally. At times, she was a single mom and never once complained. To my children, thank you for understanding.

Next, I would like to thank my Thesis advisor, Dr. Mills, for sticking with me during the long period when I couldn't find my niche, and then for keeping me on track when I finally found my way. I would also like to thank the members of my committee, Dr. Peterson and Dr. Grimaila for accepting my research so late in the game.

I would especially like to thank Dr. Patrick McGrath for taking time out of his busy schedule to serve as a subject matter expert and lend credibility to my research.

Anthony J. Puleo

Table of Contents

Page

List of Figures

Page

Page

MITIGATING INSIDER THREAT USING

HUMAN BEHAVIOR INFLUENCE MODELS

I. Introduction

This chapter introduces the reader to the research areas of insider threat mitigation and human behavior modeling. The problem is clearly defined and scoped, a proposal for a new model is introduced, the research objectives are identified, and finally, an overview of the thesis is presented.

1.1 Mitigating Insider Threat

The concept of mitigating insider threat is often used loosely and is frequently misunderstood. Many imagine mitigating insider threat is a solution to the problem, one that detects or catches insiders and eliminates the threat of damage. Realistically, however, insider threat is a much bigger problem and mitigating insider threat does not imply fixing or removing the threat. People define mitigating insider threat numerous ways, but the simplest way is to define the words separately and then combine them.

1.1.1 Mitigate.

To mitigate is to make milder, less harsh, less severe, or to moderate [1]. The definition makes no implication of eliminating, controlling, or even minimizing; it simply means to reduce. When an organization attempts to mitigate something, it is simply trying

to implement a practice that helps reduce the problem in question, in the case of this research, insider threat.

1.1.2 Insider.

An insider is any current or former employee, to include contractors, of an organization who is or was inside and as a result, has special information or advantages and has authorized physical or electronic access to organizational information and infrastructure resources [2-4]. Basically, an insider is anyone who has been given the right to access organization information and assets.

1.1.3 Threat.

Threat is a menace or danger of any sort, which includes situations in which an insider intentionally exceeds, misuses or abuses their authorized level of system access in a manner that adversely affects the organization's data, daily business operations, or system security [2-4]. In other words, threat is the consequence that happens when insiders misuse their granted rights.

1.1.4 Pulling it All Together.

Insider threat is summed up as the damage done to an organization by its own authorized employees, and mitigating insider threat is generating tools or research of any kind that reduces damage done to an organization by its authorized employees.

Most mitigation approaches focus on methods of detecting insiders or more likely detecting indicators that a problem exists. Although this is necessary research, these detections often result in catching the insider after the damage is already done. However, a fundamental approach to mitigating a problem is through deterrence, and insider threat

is no different. By learning exactly what influences the behavior of potential malicious insiders, it is possible for organizations and security personnel to reduce insider threat damage.

Computer security is a people problem [5], as it is people that are ultimately responsible for attacks against a system. This serves as the foundation for this research. Much research has been done on human behavior, but little has been done to tie it in with computer engineering models used to mitigate insider threat. It is possible to show that observing certain influences that affect human behavior are beneficial in computer modeling to identify the potential for insider damage, thus enabling security personnel to implement appropriate measures that mitigate the threat and reduce the amount of damage that occurs.

1.2 Human Behavior

Human Behavior is defined as a "collection of activities performed by human beings and influenced by culture, attitudes, emotions, values, ethics, authority, rapport, hypnosis, persuasion, and/or coercion." [6] The theory behind human behavior is humans react to "definite objective stimuli or situations and not to subjective factors." [2] Each of these statements yields key words important to this research. From the first sentence, influence, which is a fundamental concept used throughout this research, is defined below. The second sentence yields "objective stimuli or situations", which are simply events. In other words, human behavior is simply the actions or reactions made by human beings as a result of influences and events. This is discussed further in Chapter III.

1.3 Influence Models

Influence is defined as "the ability to indirectly control or affect the actions of…people," [7] or "the power…of producing an effect on a person." [2] Here, the key words are "indirectly control" and "produce an effect" on individuals. The model proposed by this research is based on the concept that human behavior is indirectly "controlled" by the influences that "produce an effect" on people. If human behavior is affected by influences, then monitoring the influences and degree of effect they have over employees within an organization provides insight into the potential behavior the organization expects the employee to exhibit.

A model is a "conceptual object used in the creation of a predictive formula." [8] A model provides a "framework for applying logic and mathematics that can be independently evaluated." [9] They are common in the natural and social sciences where logical principles apply, but are not always completely mathematical. "Models can be used to implement computer simulations that illustrate behavior…over time." [9] The influence model proposed here is intended to predict the potential for increased risk of becoming an insider threat based on the observation of influences that affect human behavior over time.

1.4 Problem Statement

The purpose of this research is to mitigate the problem of insider threat by proposing a new model that uses the influences that affect human behavior to predict employees' potential risk of becoming malicious insiders.

1.5 Research Objectives

The research objectives for this thesis are three-fold. The first objective is the establishment that human behavior plays an important role in mitigating insider threat. By considering human behavior, security personnel are able to combat insider threat just as readily and possibly with better success, than by only taking technical approaches, such as data mining email accounts or tracking logins. Additionally, by relating how influences affect people and the inherent risk involved from their exposure to computer systems containing sensitive information, it is possible to flag or generate indicators of an employee's potential risk for causing insider damage.

The second objective of this research is the creation of the Risk Predictor Model (RPM), a human behavior model that uses known influences on people to generate indicators of potential risk for insider threat. It is possible to mitigate insider threat by inserting specific influences and events that affect human behavior into a model that organizations use to identify employees with a higher risk of becoming a malicious insider, thus reducing the amount damage done.

The third and final objective of this research is to show that the RPM is able to successfully differentiate between a normal employee and malicious one who has caused harm. The model, coupled with an appropriate tool, allow security personnel to implement appropriate measures to mitigate insider threat and reduce the amount of damage that occurs.

1.6 Scope

Insider threat is a big problem, and no single research effort is going to solve the problem. Each only hopes to help in some way by targeting a specific area. This research focuses on the normally ethical employee who originally has no intentions of causing damage. This ignores employees hired with the secret intention of doing harm, as well as those paid by outsiders to enter an organization and do harm. By excluding people that already have the intent to do harm from this research, it is possible to get an idea of what behavioral scientists might consider the "normal" behavior of a typical employee. Using this as a baseline, it is possible to differentiate between employees with higher risk for causing damage and normal insiders.

1.7 Preview

This chapter defined insider threat mitigation, human behavior, influence models, and why it is important to study these areas. Next, a specific problem was identified and the three-fold research objectives to solve this problem were introduced along with the overall scope of the research. A new model is needed to mitigate insider threat and by observing influences that affect human behavior it is possible for organizations to predict which employees pose a higher risk for becoming a malicious insider.

Chapter II reviews the ongoing research in the area of insider threat and identifies the need for a new model based on influences and human behavior (the first objective of this research). Chapter III outlines the research methodology used to build the Risk Predictor Model, starting with a solid foundation for the model and building up to the outputs the model produces to mitigate insider threat (the second objective of this

research). Chapter IV gives a detailed description of how the RPM is tested, starting with how the model is populated, continuing with an in-depth case study on a known malicious insider, and culminating in an analysis of the results produced by the model and how well the model differentiates between a malicious insider and a normal insider (the third objective of this research). Finally, Chapter V identifies the relevance of the model and the data obtained from it, as well as future work considerations, and some concluding remarks.

II. Literature Review

This chapter not only reviews past and current research about insider threat and mitigation strategies available, but more importantly, satisfies the first objective of this research by identifying the need for a new model that uses influences on human behavior rather than computer logs and email mining to mitigate insider threat. After an initial discussion about why it is important to study insider threat, some relevant statistics about insiders are presented, followed by a discussion of mitigation strategies, with specific focus on risk management, which is vital to this research. Then a brief indication of the model format is presented, followed by a short summary.

2.1 Why Study Insider Threat?

Insider threat is a big problem for any organization large enough to use a computer network. When proprietary information is transferred across or stored on a network, the organization becomes susceptible to attack. Significant research has been conducted on finding ways to protect, react, and otherwise mitigate attack from outside sources, but much work is necessary to protect organizations from damage done by employees with legitimate access to the network. A recent Department of Defense (DoD) Inspector General report indicated that 87 percent of identified intruders of DoD information systems were insiders. The insider is different from an outsider, because they have been granted certain authorities and trust, and they have superior knowledge of asset value [3].

Insider threat is a vast problem and occurs on many levels starting with accidental access due to ignorance of security policy and practices or carelessness. More harmful is disdain 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 people with the intent to do harm and often results in the compromise or destruction of information, or disruption of services to other insiders [3]. The damage, intentional or not, is staggering to an organization's finances, reputation, and its people, especially if the organization has field operatives such as the United States (US) military, Federal Bureau of Investigations (FBI), Secret Service, etc. Insiders do much more, however, such as disrupt interconnected information systems, deny the use of information systems and data to authorized users, and remove, alter or destroy information. They may even use outside help to significantly increase the severity of their malicious activity [3].

"Common wisdom in the cyber security community holds that over 80% of recorded intrusion cases are attributed to trusted insiders, and the threat is rising." [10] Insider threat is on the rise for several reasons. Espionage, specifically Post Cold War era-type espionage, has increased with the collection and sale of technical weapons system information made easier through foreign visits to US facilities, joint ventures, conventions, and seminars, coupled with access to DoD information systems. Also, mindset has changed, as individuals look at selling secrets as business affairs rather than

acts of national betrayal or treason. Furthermore, the US Government is no longer isolated from the public. Cleared Defense Contractor activities were traditionally isolated from the general population, but are now increasingly vulnerable to exploitation. Moreover, commercial off-the-shelf (COTS) products have become ubiquitous to the point that even the DoD acquires most of its information systems from vendors but has little or no knowledge of who developed the systems and, therefore, has no measure of the trustworthiness, reliability or loyalties of those individuals. With little or no influence over the development of COTS products, many organizations are in danger of deploying their security systems with exploitable errors or security breeches. Additionally, the rate at which attackers exploit holes in security has increased to the point that detection of malicious code has become extraordinarily difficult. Network security personnel have been unable to convincingly demonstrate that an information system is secure; rather they are only able to demonstrate the many ways it is not [3].

2.2 Insider Threat Statistics

There have been several studies done that have pointed to the nature of the typical insider. These studies focus on identifying common characteristics among apprehended insiders and the damage they caused. What follows here is a brief synopsis.

In August of 2004, the Computer Emergency Response Team (CERT) Coordination Center at Carnegie Melon University's Software Engineering Institute and the United States (US) Secret Service National Threat Assessment Center conducted a study of 23 incidents carried out by 26 insiders in the banking and finance sector between 1996 and 2002. "Efforts to estimate how often companies face attacks from within are

difficult to make. Many believe that insider attacks are under-reported to law enforcement agencies or prosecutors. Companies fear the negative publicity or increased liability that arises because of the incidents. Or, they believe that the harm suffered is not sufficient to warrant criminal charges." [11] This is interesting, because many insiders do not equate their actions or the damages they cause to illegal activities or betrayal of country or organization. Most studies done on insider threat are reported from a purely technical perspective, relaying how the insiders accomplished their deeds, the vulnerabilities exploited, and possible solutions to prevent it from happening again. Although valuable, the significance of this study exists in the fact that it examines the threat from two perspectives, behavioral and technical, simultaneously; an industry first. Below are the seven findings the study produced.

Finding 1: Most Incidents Required Little Technical Sophistication. Most attacks were not directed at information systems or network vulnerabilities, but rather against business rules or organization policies, and individuals had little or no technical expertise or made no attempts to scan for vulnerabilities prior to the incident [11]. Based on the statistics produced in the report (Figure 1), it is apparent that organizations are susceptible to insider attack from employees of all skill levels, not just computer savvy hackers.

87% employed simple user commands
70% exploited business rules such as authorized overrides
61% exploited vulnerabilities
78% were authorized users with active computer accounts
43% used his or her own username and password
26% used someone else's computer account,
23% were employed in technical positions
17% possessed system administrator/root access
39% were unaware of technical security measures

Figure 1. Secret Service/CERT 2004 Insider Threat Study Finding 1 Statistics [11]

Finding 2: Perpetrators Planned Their Actions. "Most of the incidents were thought out and planned in advance, and often included others with knowledge of the insider's intentions, plans, and/or activities." [11] Based on the statistics for this finding (Figure 2), it is clear that events leading up to the incidents are observable, which given the proper monitoring tool, makes it easier to catch insiders earlier or even before they attack. Additionally, increased awareness of reporting requirements could reduce the number of insider transgressions.

81% planned their actions in advance
85% let others have partial or full knowledge
    74% of whom stood to benefit from the activity
    26% of whom knew about it and stood to gain nothing from it!
31% of activities or plans were noticeable
65% did not consider the negative consequences associated with their actions

Figure 2. Secret Service/CERT 2004 Insider Threat Study Finding 2 Statistics [11]

Finding 3: Financial Gain Motivated Most Perpetrators. Although this study was done in the financial sector, there were still significant motivations (Figure 3) for causing harm, other than financial reasons. Some insiders are motivated by a desire to harm the company or information system. Still, with greed being the overwhelming reason for causing harm, sudden unexplained affluence is an obvious cue to possible employees causing damage.

81%	motivated by financial gain
27%	tried to sabotage business operations
23%	motivated by revenge
19%	attempted to steal proprietary information
15%	motivated by dissatisfaction with company
15%	motivated by a desire for respect
27%	had multiple motives

Figure 3. Secret Service/CERT 2004 Insider Threat Study Finding 3 Statistics [11]

Finding 4: Perpetrators did not Share a Common Profile. There was a wide variety of employees involved in the cases represented in the report. The statistics showed that demographics was not the prevalent data to look at to find the insiders, behavior was (Figure 4). Most did not hold technical positions, with only a few technically savvy enough to consider themselves hackers. They were employed in various roles including service, clerical, professional, and technical. They ranged in age from 18 to 59, were married, single, male, female and came from a variety of racial and ethnic backgrounds. Given that the employees that caused damage came from all walks of life makes it difficult to pinpoint where to look, but their behavior gave some insiders away.

27%	exhibited concerning behavior
19%	were disgruntled employees
15%	were considered difficult to manage
4%	were considered untrustworthy
9%	had a history of electronic abuses or violations
13%	had shown an interest in hacking
27%	had prior arrests

Figure 4. Secret Service/CERT 2004 Insider Threat Study Finding 4 Statistics [11]

Finding 5: Incidents were Detected by Various Methods and People. Surprisingly, the majority of insiders were not caught by security personnel or by electronic means. As the statistics show, they were caught by a variety of sources, both internal and external to the organization and through both manual and electronic means (Figure 5). The major underpinning here is that most insiders were not stopped via monitoring their email accounts or network logins, but through interaction with people.

61% detected by non security personnel
- customers (35%)
- supervisors (13%)
- other non-security personnel (13%)

39% detected by security staff
- corporate security department staff (4%)
- security staff or system administrators (13%)
- staff responsible for info systems/data (17%)

61% caught through manual procedures
- inability to log in
- customer complaints
- manual account audits
- notification by outsiders

26% caught through system failure or irregularities

22% were caught through auditing or monitoring procedures

74% of insiders' identities were obtained using system logs

30% required examination of the network, system, or data to help identify the insider

Figure 5. Secret Service/CERT 2004 Insider Threat Study Finding 5 Statistics [11]

Finding 6: Victim Organizations Suffered Financial Loss. Given the study on the financial sector, it is not surprising that an overwhelming majority of organizations suffered a financial loss due to insider actions. However, as statistics show, even financial institutions suffered other losses, such as proprietary information or defamation of reputation (Figure 6). Accordingly, organizations outside the financial realm have their

share of financial loss due to insider damage, but stand to lose more when insiders sell secrets and betray national security.

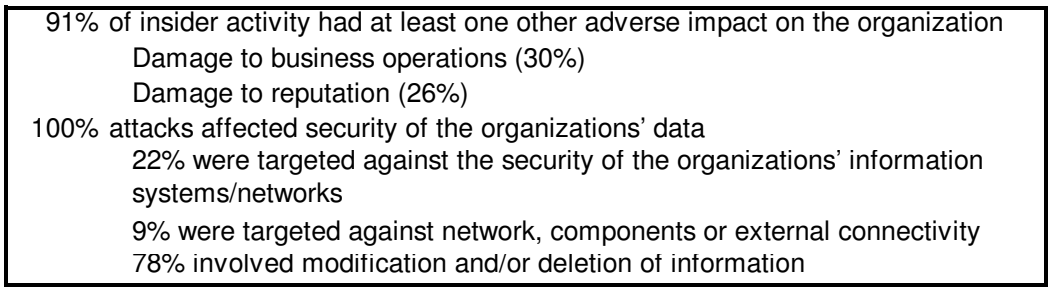

Figure 6. Secret Service/CERT 2004 Insider Threat Study Finding 6 Statistics [11]

Finding 7: Perpetrators Committed Acts While on the Job. This refutes the notion that spies and embezzlers sneak into the work place late at night when no one is looking in order to carry out their crimes. The statistics show quite the contrary, as most employees have little trouble causing damage right from their desks at work during duty hours (Figure 7). It appears that employees feel safe enough to perform illicit acts without fear of reprisal.

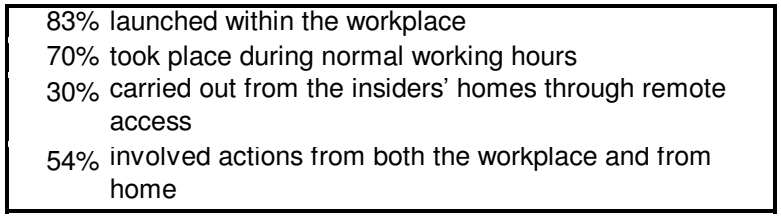

Figure 7. Secret Service/CERT 2004 Insider Threat Study Finding 7 Statistics [11]

This was a powerful study because it is recent (2004) and because it considered both technical and behavioral implications for the first time. It produced several key insights into the nature of the insider as well. Most attackers exhibit one or more of the following observable behaviors. They

- have a wide range of skills, often not technical in nature,
- plan their attacks, share their intents with others, maybe even coworkers,
- are motivated by financial gain, but usually have multiple motives,
- do not share a common profile, but rather a common set of observable behaviors,
- are caught not by security personnel and fancy software, but by people, manually,
- cause organizations loss of data and reputation as well as financial loss,
- attack at the office during normal duty hours, in the face of security, and feel safe.

The underlying theme to these findings is that insiders throw behavioral signals that supervisors and security personnel need to watch for. Organizations need to instill the importance of proper reporting procedures, lest anyone in the organization feels the need to report someone acting out of the ordinary. Proper reporting of observable behavior provides leverage to security personnel.

2.3 Mitigation Strategies

Mitigation strategies for insider threat are rare for several reasons. First, it is a hard problem, that deals with people and people are not easily categorized, or lumped into good and bad groups from which to select. The simple fact that no two people are alike makes it difficult to introduce sound mitigation strategies, and as a result, few exist.

Second, “among the approaches for detecting insider abuse, profiling is the favored technology, and its preferred implementation mechanism, especially given a goal of detecting novel attacks or abuses, is anomaly detection.” [10] Unfortunately, profiling yields few conclusive factors, except for the fact that insiders come from all walks of life, with vastly different skill sets (some technical and some non-technical), are hard working, dedicated individuals, loyal US citizens, and often have security clearances. Since it is difficult to identify a single profile, or even a broad one that successfully identifies malicious insiders, it is clear that profiling is not the best solution to mitigating insider threat. However, one fact remains; all insiders that caused damage were human and as a result are susceptible to influences that affect human behavior. Rather than generating a single profile that attempts to capture the nebulous essence of malicious insiders, concentrating on the influences that affect the behavior of employees yields interesting results.

Third, and most significantly, most mitigation strategies focus on how incidents are executed, detected, and the insider identified. This is mostly effective in stopping insiders after significant damage has already occurred. By monitoring networks, email accounts, logins, building accesses, etc., security personnel watch employees’ normal everyday work pattern, identifying an anomaly here or there, without raising suspicion. However, when anomalies begin to add up, it is time to act, but by then, it is often too late because the damage is done. Although these are still valuable techniques that require more research, there is little research in identifying the physical and observable behaviors and interactions that insiders engage in before the incidents occur. By identifying

employees with a higher risk for causing damage, indicators identified by existing sources hold more value, meaning less are required to occur before security personnel engage, thus reducing the amount of damage the insider causes.

There are, however, some strategies that show promise, such as anomaly detection. However, most anomaly detection techniques are not preemptive and often require multiple anomalies to occur before action is taken. For example, detecting unauthorized access to classified information is useful, but late. Additionally, by definition, an anomaly is an outlier, and security personnel ignore one, two, or even three anomalies before acting on a trend four or more anomalies. As a result, by the time action is taken, significant damage has already been done.

2.4 Risk Management

A good insider threat mitigation strategy is risk based. Risk is defined as the probability or chance of encountering harm or loss [1, 3]. Risk management is the act or manner of managing, controlling or regulating risk [1]. The DoD definition states that risk management is a decision making process involving relevant risk assessments based on a function of three variables; criticality, vulnerability, and threat. Criticality represents how important the asset is to the mission, vulnerability suggests the ways to compromise, exploit, damage or destroy the asset, and threat characterizes who intends to exploit a vulnerability, against what, and what capabilities they possess to do so [3]. The DoD has adopted a 7-segment model where risk occurs at the intersection of criticality, vulnerability, and threat (Figure 8). Each segment is defined in a legend (Figure 9).

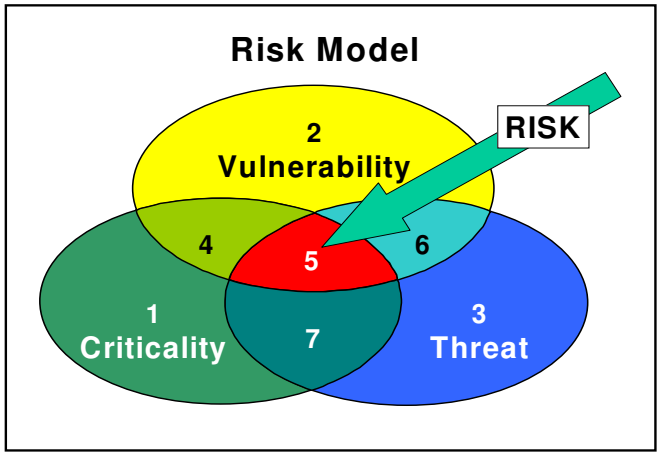

Figure 8. DoD Risk Model [3]

1 -	Critical assets (information, systems, programs, people, equipment or facilities) for which there is no known vulnerability and no known threat
2 -	Vulnerabilities in systems, programs, people, equipment or facilities that are not associated with critical assets and for which there is no known threat
3 -	Threat environment for which there is no known threat to critical assets or access to vulnerabilities (or vulnerability information).
4 -	Critical assets for which there are known vulnerabilities, but no known threat exposure.
5 -	Critical assets for which there are known vulnerabilities and threat exposure.
6 -	Threat has acquired specific knowledge and/or capability to exploit a vulnerability although not a critical asset vulnerability.
7 -	Critical asset for which there are no known vulnerabilities, but there is exposure to a specific threat.

Figure 9. Legend for Numbered Segments of DoD Risk Model [3]

The segments of interest appear where the three variables criticality, vulnerability, and threat intersect. For purposes of this research, segment 7 is ignored because in theory, even a highly critical asset that is invulnerable (improbable) is unlikely to sustain damage even under severe threat. Likewise, segment 4 is ignored because in the face of no threats (also improbable), even a critical system with vulnerabilities is unlikely to sustain

damage, at least until a perceived threat surfaces. This leaves segments 6 and 5, where in the former, a threat to a non-critical but vulnerable system is potentially harmful, and in the latter, all three variables collide representing the highest risk possible. Segment 6 remains a concern for this research because insider damage comes in many forms, including organization reputation, for example, which potentially suffers at the hand of insiders without access to critical information.

The next step is to categorize insiders into the model. Since this is a risk model, not a police blotter, it is not an insult to employees if all employees are considered threats, since it is true that each employee in an organization, from top to bottom, is a potential threat to the organization.

Next, all organization assets, critical or otherwise, are considered vulnerable, because employees are granted rights and privileges to use company assets as a condition of their employment, that is what makes them insiders. This falls under segment 6, and by entering critical assets into the equation, segment 5, extreme risk is reached. The criticality of organization assets is constant here; it does not change based on the organizations employees. Likewise, the vulnerabilities created by giving those employees jobs does not change either (this is separate from inherent vulnerabilities not associated with employees, such as unsecured vaults, faulty programming, etc.). This indicates an important fact; the amount of risk an organization undertakes is directly proportional to the risk each of its employees poses to the organization. By determining which employees pose the highest threat to an organization, security personnel are able to act accordingly to mitigate the potential for damage.

In summary, mitigating insider threat is a hard problem that requires knowledge of human behavior. Strategies structured around mitigating risks inherent in an organization's employees are necessary, but there is a lack of good models that show increased risk. Coupled with the fact that most mitigation strategies focus on insiders' current actions, which are looked at in a vacuum, rather than attempting to ascertain the potential risk an employee has for causing harm in the first place, it becomes clear that a new type of model involving human behavior is in order. Because humans are so vastly different, it becomes necessary to study human behavior to help with mitigation strategies. By learning which indicators are not only important, but also observable, it is possible to put them into a model useful in mitigating insider threat.

2.5 Model Format

The first thing to determine before developing a model using human behavior characteristics to mitigate insider threat is to model. Based on the following research done on insider threat, it becomes clear how to build a new model using human behavior as its inputs.

The Air Force Office of Special Investigations conducted a recent study (2005) of 154 cases of insider espionage from 1945 to 2004. They defined espionage as "the process of obtaining military, political, commercial, or other secret information by means of spies, secret agents, or illegal monitoring devices." [12] This is important because it twists the usual notion that insiders only cause damage by transmitting information over the computer where some high tech security software might catch it, but rather implies that it is not always a computer issue; it is a human one. The study found that in 68% of

the cases the insider volunteered the information, 12% were recruited by friends or family, and only 20% were actually recruited by foreign intelligence and that the motivations for spying were greed, revenge, ideological, sympathy for cause, and recognition or power [12]. This is significant because a vast majority of insiders are not coerced into betraying their country or government, yet their motivations stem from human emotions. As a result, the study produced a key set of indicators for organizations to look for to detect espionage activity (Figure 10). These indicators are important because they represent the observable behaviors that are used to build a model that is useful in mitigating insider threat.

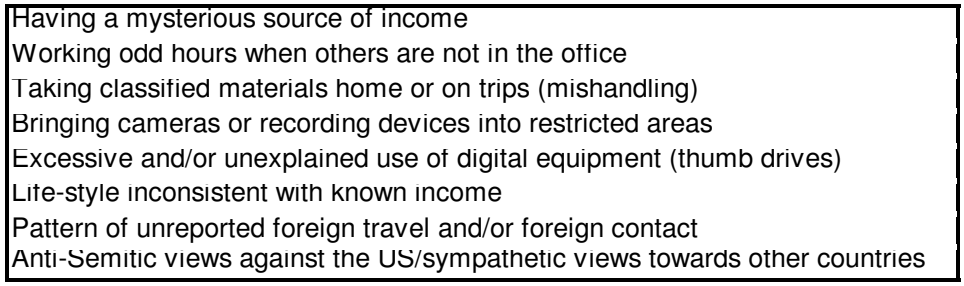

Figure 10. AFOSI Key Indicators of Espionage Activity [12]

2.6 Summary

This chapter has shown that first, it is important to study insider threat because it is 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, but unfortunately 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 the principles of risk management, which provides a good framework for mitigating insider threat, and human behavior analysis, 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 thesis has been met, by identifying the need for a new model, the Risk Predictor Model (RPM), which uses the influences that affect employees to determine an employee's level of risk for becoming an insider threat to the organization. Chapter III details the development of the model and Chapter IV tests the model to show that is capable of differentiating between malicious and non-malicious insiders.

III. Methodology

Chapter II presented material outlining the need for a new and different kind of model to mitigate insider threat. This chapter focuses on the methodology of building the Risk Predictor Model, starting with a thorough review of the concepts that are fundamental to the model's construction. Then a formal definition of the model and mathematics involved is presented. Finally, a detailed description of the model's inputs, mathematics, and outputs, along with their usefulness is presented, prior to a short summary about the model.

3.1 Model Inception

Early discussion with the research sponsor [13] resulted in a relational diagram of an organization where the individuals in the organization have certain influences over each other (Figure 11).

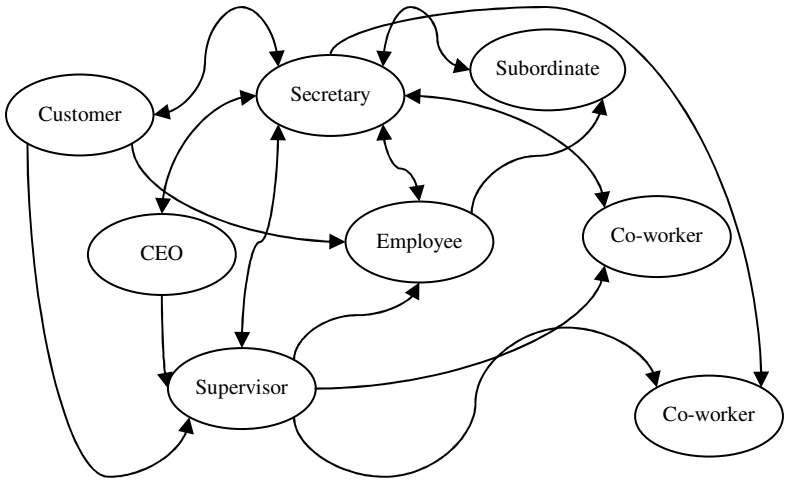

Figure 11. Model Showing Relationships Between Members of an Organization [13]

This model demonstrates the importance of relationships between the members of an organization. More importantly, it shows that certain members of the organization hold more influence over other members in the organization. For example, although the Chief Executive Officer (CEO) of an organization resides at the top of the organizational chart, it is the CEO's secretary that is tied into all aspects of the organization, not the CEO. Likewise, the secretaries' influence over other employees is perceived great, due to the single influence the CEO has over the secretary. In other words, employees accept that correspondence from the secretary is the result of action taken by the CEO and therefore value the secretaries' influence as if it were from the CEO. As a result, it is clear that a model based on relationships and the influences these relationships have on each of the entities within the model is helpful in mitigating the insider threat problem.

The model in Figure 11 is just the foundation for the model developed in this research. For an effective model, it is important to look at a number of business dynamics principles [14]. First, develop the model to solve a particular problem, not to model the system, (in this case, to alert security personnel of employees with higher risk of performing insider damage). Second, a good model does not stand alone, and although the model proposed here provides interesting insight into the risk an employee displays, the model outputs are indicators to evaluate with other indicators before action is taken. Lastly, modeling works best as an iterative process, so the model is developed in a way such that additional future inputs are made available to the model for evaluation. The model is capable of evaluating the data over time, not just as a one-time snapshot of the situation. Given enough time, the model is capable of trend analysis as well.

Next, it is important to develop how to model the relationships and how the links between relationships are quantified. Since it is relationships between people, or more precisely, the influences that effect people that are modeled, a causal relationship is used. In this type of modeling, relationships are linked together when one entity has some effect over another entity. Likewise, the link between them is quantified, and in this case is the amount of effect, either positive or negative, one entity has over the other. It is also important to note that "social dynamics are fraught with counterintuitive behavior" [15]. Figure 12 illustrates this; smoking, arteries, weight, anxiety, lungs, and heart are entities linked together by causal relationships. Directionality, also required to evaluate causal relationships is also illustrated.

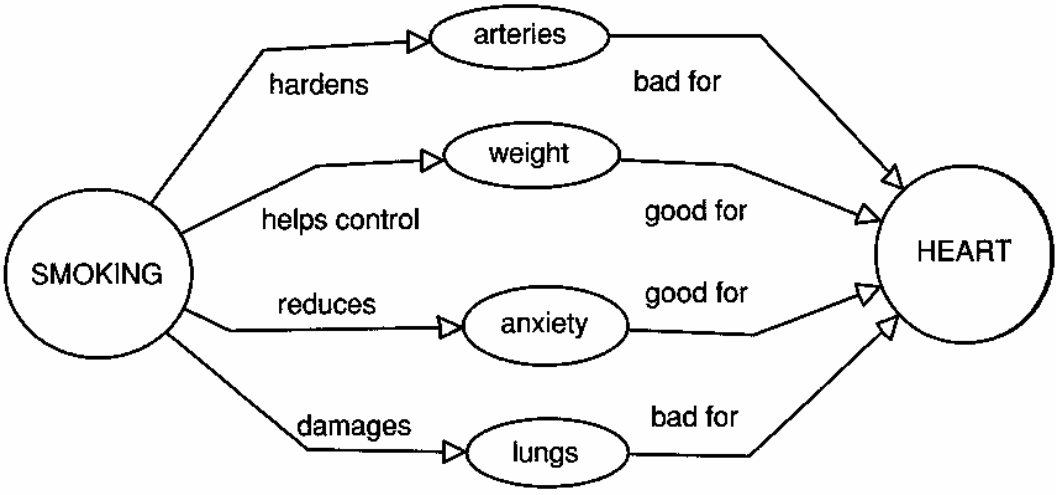

Figure 12. Model Showing Counterintuitive Behavior [15]

In this example, it is possible to derive several relationships between the entities. Smoking hardens the arteries and damages the lungs, which is bad for your heart;

however, smoking also helps control weight and acts as an anxiety reducer for smokers, which has a positive effect on the heart [15]. So, the act of smoking has both positive and negative effects on the heart. It is the idea that multiple entities, or in the case of the Risk Predictor Model, influences, effect other entities in both positive and negative ways that becomes the foundation for the model.

It is established that the model has entities that represent relationships, or more specifically, influences, and these entities are connected together by links that hold certain weights. For the purposes of this research, the model is loosely designed as a polytomous Rasch model. "The polytomous Rasch model is a measurement model that has potential application in any context in which the objective is to measure a trait or ability through a process in which responses to items are scored with successive integers." [16] Developed in 1978 by Andrich, the relevant terms of Rasch's 1961 derivations are resolved into threshold and discrimination parameters. "Rasch models provide a foundation for the measurement of quantitative attributes and traits on a continuum, based on categorical data derived from interactions between persons and items. In principle, Rasch models are applied in any experimental context in which persons interact with assessment questions or items in a manner that provides for comparisons between persons with respect to the magnitude of some attribute or trait." [17] This leads to a model that contains human influences as entities and uses integers to represent the magnitude each influence has over the others.

The magnitudes of the links are represented by integers, but the degree they are computed to is still undetermined. When Andrich developed the polytomous Rasch

model, he used the Likert scale [16]. The Likert scale, invented in 1932 by Rensis Likert, is a type of psychometric scale often used in questionnaires, where respondents specify their level of agreement to each of a list of statements [18]. ”Psychometrics is the field of study concerned with the theory and technique of psychological measurement, which includes the measurement of knowledge, abilities, attitudes, and personality traits.” [19] A traditional Likert scale uses a five-point bipolar measurement to indicate the degree of agreement with a statement and being bipolar, the measurement considers both positive and negative slants. For example, when asked if smoking is bad for your health, respondents are given the following choices: strongly agree, agree, neither agree nor disagree, disagree, and strongly disagree. This scale has degree, evidenced by the difference between agree and strongly agree, and is bipolar, by showing both a positive and negative attitude. Similarly, the question, rate your level of stress as highly stressed, moderately stressed, average stress, fairly unstressed, or not stressed at all, also has a scale that shows degree, evidenced by the difference between highly and moderately stressed, and has bipolarity by showing above average levels of stress as well as below average levels of stress. Converting the Likert scale into integers from 2 to -2 allows for easy incorporation into a Rasch type model. As a result, the model contains human influences as entities and integers from 2 to -2 represent the magnitude each influence has over the others.

Next, using the DoD’s 7-segment risk model [3], and the desire to model human behavior, potential insiders are identified using a model built to determine employee risk for insider damage based on the influences over them. Using the Lowenstein Life Stress

Test [20] as the foundation for the influences included in the model is a reasonable place to start (Figure 13). The Life Stress Test is widely used by mental health professionals to

In the past 12 to 24 months, which of the following major life events have taken place in your life? Make down the points for each event that you have experienced this year. When you're done looking at the whole list, add up the points for each event. Check your score at the bottom.

_____ 100 Death of Spouse	_____ 29Change in work responsibilities
_____ 73 Divorce	_____ 29 Trouble with in-laws
_____ 65 Marital Separation	_____ 28 Outstanding personal achievement
_____ 63 Jail Term	_____ 26 Spouse begins or stops work
_____ 63 Death of close family member	_____ 26 Starting or finishing school
_____ 53 Personal injury or illness	_____ 25 Change in living conditions
_____ 50 Marriage	_____ 24 Revision of personal habits
_____ 47 Fired from work	_____ 23 Trouble with boss
_____ 45 Marital reconciliation	_____ 20 Change in work hours, conditions
_____ 45 Retirement	_____ 20 Change in residence
_____ 44 Change in family member's health	_____ 20 Change in schools
_____ 40 Pregnancy	_____ 19 Change in recreational habits
_____ 39 Sex difficulties	_____ 19 Change in church activities
_____ 39 Addition to family	_____ 18 Change in social activities
_____ 39 Business readjustment	_____ 17 Mortgage or loan under $20,000
_____ 38 Change in financial status	_____ 16 Change in sleeping habits
_____ 37 Death of close friend	_____ 15 Change in number of family gatherings
_____ 36 Change to a different line of work	_____ 15 Change in eating habits
_____ 35 Change in number of marital arguments	_____ 13 Vacation
_____ 31 Mortgage or loan over $30,000	_____ 12 Christmas season
_____ 30 Foreclosure of mortgage or loan	_____ 11 Minor violations of the law

_____ Your Total Score

This scale shows the kind of life pressure that you are facing. Depending on your coping skills or the lack thereof, this scale can predict the likelihood that you will fall victim to a stress related illness. The illness could be mild - frequent tension headaches, acid indigestion, loss of sleep to very serious illness like ulcers, cancer, migraines and the like.

LIFE STRESS SCORES
0-149 Low susceptibility to stress-related illness
150-299 Medium susceptibility to stress-related illness.
300 and over High susceptibility to stress-related illness

Figure 13. Sample Lowenstein Life Stress Test [20]

determine the levels of stress an individual suffers from. The test is administered in a questionnaire format where the respondent identifies events that have occurred within the last twelve to twenty-four months. Each event has a score associated with it and the sum of the scores relevant to the individual yields a total stress level, which is then checked against a susceptibility to illness gauge.

For example, a personal injury, change in financial status, addition to the family and the foreclosure of a mortgage yields a score of 160, which puts an individual in the medium susceptibility to stress-related illness category. Similarly, these same influences indicate a higher potential for an individual to cause insider damage, given the financial hardships the individual appears to face. Examination of the events used in the Life Stress Test reveals another relevant point; even events that are considered good are found on the test, which negatively contributes to the overall stress level. This is important when considering the positive and negative representation used in the Likert Scale mentioned earlier. In other words, any influence, whether positive or negative, affects an individual's risk level for causing insider damage. For purposes of this research, influences similar to the events used in the Life Stress Test are used, each cross-referenced against the others for effect using the Likert scale, resulting in a matrix of human influences. The model also includes a similar matrix of events, in keeping with the Life Stress Test, used in conjunction with the influence matrix to generate scores representing an employees potential for causing insider damage.

3.2 Formal Description

This section provides a formal description of the Risk Predictor Model, including variable definitions and formulae the RPM uses to produce the outputs. Note, *m* represents the number of influences, *n* represents the number of events, and x represents the current iteration through the model.

3.2.1 RPM Variable Definitions.

Inputs

- I = Influence Matrix — $m \times m$
- E = Event Matrix — $n \times m$
- R_x = Response Vector (either Initial or Current) — $1 \times m$
- S_x = Stimulus Vector (either Initial or standard) — $1 \times n$

Interim variables

- x_x = Interim Response Vector — $1 \times m$
- y_x = Interim Stimulus Vector — $1 \times m$
- z_x = Interim Stimulus Response Vector — $1 \times m$

Outputs

- R_{x+1} = new Current Response Vector — $1 \times m$
- $Initial\ Score_x$ = numerical representation of the employees' initial risk
- $Current\ Score_{x+1}$ = numerical representation of the employees' current risk
- $time\_y$ = time period of interest
- $Slope_{time\_y}$ = slope of scores versus time period of interest

3.2.2 Formulae – In Step-by-Step Order.

$$R_x * I = x_x$$

$$S_x * E = y_x$$

$$x_x + y_x = z_x$$

$$z_x * I = R_{x+1}$$

$$\sum_{i=1}^{m} R_{x+1} = \text{Score}_{x+1}$$

$$\frac{\text{Score}_{x+1} - \text{Score}_x}{\text{time\_y}} = \text{Slope}_{\text{time\_y}}$$

3.3 Risk Predictor Model

Given the foundation for the Risk Predictor Model, and its formal definition, it is now possible to cover specifics about the model, such as its inputs and outputs and what the model actually does. The next few sections look into each aspect of the model in detail, while Chapter IV is reserved for testing the model. The RPM takes four separate inputs: the influence matrix, the event matrix, the response vector, and the stimulus vector. Each is described below:

3.4 The Influence Matrix

The influence matrix contains all the influences an organization considers pertinent to its operation. The organization must decide which influences are important and how the influences affect each other. For example, having a Secret or Top Secret security clearance is certainly an influence to include in the DoD influence matrix, but is

probably not a concern for a department store. Similarly, an airline company's interest in the influence of noise on its employees differs from the city library's interest. Once an organization decides which influences are important, they are added to the matrix by listing them in a column on the left and again in a row across the top (Figure 14 below). Although the number of influences in this example is small, Figure 14 shows an influence matrix where the organization has selected six influences of concern. The next step is to cross-reference each influence in the first column against each of the influences in the top row. As before, this is organization specific since each organization feels differently about how one influence affects another. For example, a coffee house treats the influence caffeine has over a medical condition differently physician's office treats it. So, the organization takes the desired influences, determines how each affects the others, and completes the matrix.

Influence Matrix	Influence A	Influence B	Influence C	Influence D	Influence E	Influence F
Influence A						
Influence B						
Influence C						
Influence D						
Influence E						
Influence F						

Figure 14. Example of Influence Matrix

3.4.1 Scoring

There are a few important details to note about scoring in the RPM. First, a higher overall score equates to higher overall risk. As a result, a -2 lowers the overall score and a 2 raises the score (actually, it is more likely that a -2 simply raises the overall score by less than a 2 does). For example, stress has a negative effect on the relationship with family, which is represented by a positive 2, because the implication is that the score (risk) goes up because of the negative influence of stress. Likewise, a pay raise at work positively effects family financial stability, but is represented by a -2, resulting in a lower overall score (risk) based on the positive influence of additional pay.

Second, the model is only as good as its inputs, which are derived by the organization. As a result, it is critical that a subject matter expert (or team of them) within the organization is the individual which determines which influences (and later events) are used to build the matrices used for the model inputs. Furthermore, because the model deals with human influences, it is equally important that the individual (or team) that scores how each influence (or event) affects the others in the matrix is not only a subject mater expert, but also has human behavior experience. This ensures that the model is properly populated with pertinent organization information as well as relevant human behavior data.

Third, it is important to realize that the relationship between two influences (or event and influence) is not necessarily reciprocal. For example, a pay raise has a positive effect on the family financial situation, but the reverse is not true; family financial situation has no bearing on receiving a pay raise.

Fourth, to avoid circular feedback where the result is a spiraling score with no limit, the RPM does not consider the affects of an influence over itself. For example, having a certain level of stress is, by itself, stressful. If an organization were to evaluate the affect stress has over stress, the resulting value spirals out of control as stress begets more stress, which begets more stress, etc.

3.4.2 Influence Matrix Revisited

Now that matrix scoring is established, it is helpful to look at a small example of populating an influence matrix, or similarly, an event matrix (Figure 15). This figure illustrates an example where the organization has chosen stress, pay cut, relationship with family, and family financial status as the applicable influences.

Influence Matrix	Stress	Pay Raise	Relationship with Family	Family Financial Status
Stress	0			
Pay Cut		0		
Relationship with Family			0	
Family Financial Status				0

Figure 15. Populating an Influence Matrix, part 1

Notice that the diagonal elements in the matrix that correspond to influences cross-referenced with themselves are filled with zeros, to avoid feedback. Next, the subject matter expert completes the matrix by examining the influence in each row and determining how it affects each of the influences in the columns. Essentially, they take

the first influence, stress, and determine how they believe stress affects a pay cut, the relationship with family and the family financial status influences. For example, they decide that stress negatively effects the relationship with family (and receives a 1), but has no effect on receiving a pay cut or the current family financial situation (both receive 0s). Additionally, a pay cut negatively effects stress, relationship with family, and family financial situation (all three receiving 1s). This process continues until the entire matrix is populated (Figure 16). Notice how the relationship between stress and family financial status differs from the relationship between family financial status and stress.

Influence Matrix	Stress	Pay Raise	Relationship with Family	Family Financial Status
Stress	0	0	1	0
Pay Cut	1	0	1	1
Relationship with Family	1	0	0	0
Family Financial Status	1	0	1	0

Figure 16. Populating an Influence Matrix, part 2

Lastly, once created, the matrix is static for purposes of the model. Although the organization has the ability to change the matrices (influence or event) at any time, the RPM has no capability to change the matrices, hence they are considered static.

3.5 The Event Matrix

The event matrix is formed exactly like the influence matrix. It is similarly organization specific, where a subject matter expert within the organization decides

which events are important and how they affect the influences used in the influence matrix. It is here that it becomes increasingly clear that cross-referenced relationships are not reciprocal. In the case of the event matrix, the chosen events are listed in the first column and the exact same influences used in the influence matrix are listed in the row across the top (Figure 17).

Event Matrix	Influence A	Influence B	Influence C	Influence D	Influence E	Influence F
Event A						
Event B						
Event C						
Event D						

Figure 17. Example Event Matrix

There are two major differences between the event matrix and the influence matrix. First, the event matrix is not always square. Figure 17 above illustrates this, as there are four events and six influences. The number of events varies (more than, equal to or less than the number of influences), but the influences used must exactly match the ones used in the influence matrix in number, name and location in the matrix. Secondly, because of the first difference, there are no possibilities for circular relationships and therefore every event is evaluated against every influence.

Aside from these differences, population of the event matrix is performed in the same manner as the influence matrix (see Section 3.4.2 above) and is likewise static, once created (Figure 18). In this example, Event A increases stress and negatively affects the

employee's relationship with family, Event B increases stress and negatively affects the employee's family financial status and Event C significantly increases stress while negatively affecting both the employee's relationship with family and family financial status.

Event Matrix	Stress	Pay Raise	Relationship with Family	Family Financial Status
Event A	1	0	1	0
Event B	1	0	0	1
Event C	2	0	1	1

Figure 18. Example of a Populated Event Matrix

3.6 Response Vector

The third input to the RPM is the employee's Response Vector. The Response Vector is a one-dimensional (hence a vector and not a matrix) input that consists of a list of influences and a number (between -2 and 2) representing the level of effect each has over the particular employee (Figure 19). Each employee has one, and it is important that the list of influences in the Response Vector exactly match the influences used in the influence matrix in number, name, and ordering within the matrix.

Response Vector	John Smith
Stress	2
Pay Raise	0
Relationship with Family	1
Family Financial Status	0

Figure 19. Sample Response Vector for Employee John Smith

In this example, employee John Smith suffers from a heavy stress level, is uninfluenced by a pay cut or family financial status, and has some strain in his relationship with his family. Note the same Likert Scaling is used and the influences used are identical to the ones used in the previous example (see Section 3.4.2 above). Described below are three different types of Response Vectors, all having the exact same form, with slightly varying function.

3.6.1 Initial Response Vector

The Initial Response Vector is the initial vector that represents the influences over an employee at the beginning, whether it is at job inception, upon implementation of the RPM by security personnel, simply the results of a survey, or some amalgamation of the three. Organizations determine the exact method for attaining these Initial Response Vectors and recognize the fact that accurately establishing a baseline of the influences that affect their employees is a difficult one. At initial employment, not much is known about an employee, but diligent review of past work experience and references usually sheds some light on employees. A security clearance goes a long way towards starting an Initial Response Vector. Conversely, employee surveys are problematic because

individuals tend to inaccurately evaluate the severity or even existence of influences over themselves. One way to help generate Initial Response Vectors is through supervisor involvement. There is no substitute for good supervisor involvement, because supervisors know their employees better than anyone in the organization does. Whether a survey is administered, or a supervisor makes an informed opinion based on careful observation and interaction with the employee, it is crucial that an Initial Response Vector is created for every employee. The Initial Response Vector is used only once, as an input to the RPM to determine each employee's initial score.

3.6.2 Interim Response Vector

The second type Response Vector is the Interim Response Vector. This vector is only the result of an intermediate step in the RPM mathematics. It is referred to later in this chapter, but serves no other purpose outside the model mathematics.

3.6.3 Current Response Vector

The last type of Response Vector is the Current Response Vector, which is the standard Response Vector. This vector is identical in all respects to the Initial Response Vector except for the updated influence values in the vector. It is actually an output of the model, which then serves as the next Response Vector input to the RMP when another stimulus is introduced. So, the first time the model is used on an employee, it takes the Initial Response Vector as one of the inputs, produces an Interim Response Vector during an intermediary math step, which is used during the final mathematics calculations to produce one of the outputs, the Current Response Vector. Then, each time a new iteration

of the model is needed, the Current Response Vector is used as the input in place of the Initial Response Vector.

3.7 Stimulus Vector

The fourth and final input to the RPM is the Stimulus Vector. Like the Response Vector, it is a one-dimensional (hence a vector and not a matrix) input that consists of a list of all events found in the Event Matrix evaluated with a zero or one (Figure 20).

Stimulus Vector	John Smith
Event A	0
Event B	1
Event C	0

Figure 20. Sample Stimulus Vector for Employee John Smith

The Stimulus Vector is used to "turn on" events as they occur during an employee's career and, like the Response Vector, it is crucial that the list of events in the Stimulus Vector exactly match the events used in the event matrix in number, name and ordering within the matrix. The Stimulus Vector is a list of all possible events with a "1" representing an event that has occurred and a "0" representing events that have not occurred. In this example, only Event B has occurred. The model accepts multiple events in the Stimulus Vector, but traditionally, each time an event occurs, the Stimulus Vector is reset and updated accordingly, before being input into the RPM. Like the Response

Vector, there are several types of Stimulus Vectors, all having the same form, differing only in function.

3.7.1 Initial Stimulus Vector

The Initial Stimulus Vector is used during the first calculations made by the RPM, prior to any events being applied to the employee, in order to calculate the employee's initial score (see Outputs in Section 3.9 below). It is simply a Stimulus Vector with all events "turned off", shown with zero values.

3.7.2 Interim Stimulus Vector

Like the Interim Response Vector, the Interim Stimulus Vector is only the result of an intermediate step in the RPM mathematics. It is important to note that due to the mathematics explained in Section 3.8 below, the Interim Stimulus Vector is actually the length of the number of influences, not the number of events. It is referred to later in this chapter, but serves no purpose outside the model mathematics.

3.7.3 Interim Stimulus Response Vector

Like the other interim vectors, the Interim Stimulus Response Vector is a temporary vector created during the model mathematics. It is actually the sum of the Interim Response Vector and the Interim Stimulus Vector, which makes it the length of the number of influences, not the number of events. It is referred to later in this chapter, but serves no purpose outside the model mathematics.

3.7.4 Standard Stimulus Vector

The fourth and final type is the standard Stimulus Vector or just Stimulus Vector. It is used each time an event occurs during an employee's career by "turning on" the

event by setting it to a 1 in the vector. It is used in all RPM calculations except for determining initial employee scores, when the Initial Stimulus Vector is used.

3.8 Interaction of the Inputs

Now that each of the inputs is defined, both in use and shape (matrix or vector), it is necessary to determine how these inputs interact. The formal description of the model was given in Section 3.2 above. The section defined the way the RPM uses the inputs to produce outputs, for example, *multiply* the Response Vector by the Influence Matrix or *add* the Interim Stimulus Vector to the Interim Response Vector. This is the step-by-step process of using the inputs mathematically to yield a usable output that mitigates insider threat, the primary goal of this research. These operations are accomplished using basic matrix mathematics.

3.8.1 Notes on Matrix Representation.

It is important to note, that for purposes of display appealing to the human eye, the Response and Stimulus Vectors have been transposed and displayed in multi-row, single column or *m x* 1 format (see Figures 19 and 20 above). This is how one expects to look at a list of influences or events and whether or not they apply to an employee. However, for mathematical reasons, they are represented as 1 *x m* and 1 *x n* vectors, respectively.

It is also important to understand that maintaining the quantity, order and naming of the text portion of the matrices and vectors is necessary to perform the operations only on the numerical portion of the input matrices and vectors. In other words, the mathematics involved only works on the numerical data (initial values between -2 and 2) contained within the matrices and vectors, and the data becomes useless if the text portion

(the lists of influences or events) of the matrices and vectors is not rigidly maintained. With that in mind, the next section describes the steps the RPM performs, using the following notation: *m* represents the number of influences and *n* represents the number of events. Therefore, the influence matrix is *m x m*, the response vector is 1 *x m*, the event matrix is *n x m* and the stimulus vector is 1 *x n*.

3.8.2 Description of the Risk Predictor Model Mathematics

First, multiply the Current Response Vector (or during the first calculation, the Initial Response Vector) by the Influence Matrix, yielding the Interim Response Vector. This is represented as 1 *x m* * *m x m* which yields a 1 *x m* vector, and effectively computes the effect the influences over the employee actually have on the employee. In other words, the Response Vector identifies which influences affect the employee, but not how they affect each other as defined by the influence matrix. The Interim Response Vector holds this information. To continue the example from before, Figures 16, 18, 19, and 20 represent the inputs to the RPM. This step produces the mathematics in Equation 1, resulting in the Interim Response Vector on the right.

$$\begin{bmatrix}2 & 0 & 1 & 0\end{bmatrix} * \begin{bmatrix}0 & 0 & 1 & 0\\ 1 & 0 & 1 & 1\\ 1 & 0 & 0 & 0\\ 1 & 0 & 1 & 0\end{bmatrix} = \begin{bmatrix}1 & 3 & 2 & 3\end{bmatrix} \qquad (1)$$

Next, multiply the Stimulus Vector (or during the first calculation, the Initial Stimulus Vector) by the Event Matrix yielding the Interim Stimulus Vector. This is

represented as 1 *x n* * *n x m* which yields a 1 *x m* vector, and effectively determines the new influences that affect the employee as a result of the event. That is the reason the Interim Stimulus Vector is equal in length to the response vector, as it holds data about influences, not events. These new influences are added to the existing influences that affect the employee to determine the total effect of the influences over an employee after the event has occurred. In the continuing example, this step produces the mathematics in Equation 2, resulting in the Interim Stimulus Vector on the right.

$$\begin{bmatrix}0 & 1 & 0\end{bmatrix} * \begin{bmatrix}1 & 0 & 1 & 0\\ 1 & 0 & 0 & 1\\ 2 & 0 & 1 & 1\end{bmatrix} = \begin{bmatrix}1 & 0 & 0 & 1\end{bmatrix} \qquad (2)$$

As a result, the model adds the interim stimulus vector to the interim response vector yielding the interim stimulus response vector. This is represented as 1 *x m* + 1 *x m*, which yields a 1 *x m* vector that effectively computes the magnitude that each influence has over the employee. However, as with the Response Vector, the interim stimulus response vector reflects which influences affect the employee, but not how they affect each other as defined by the influence matrix. Our example continues in Equation 3, with the Interim Stimulus Response Vector being the final result on the right.

$$\begin{bmatrix}1 & 3 & 2 & 3\end{bmatrix} + \begin{bmatrix}1 & 0 & 0 & 1\end{bmatrix} = \begin{bmatrix}2 & 3 & 2 & 4\end{bmatrix} \qquad (3)$$

In the final mathematical step, the model multiplies the interim stimulus response vector by the Influence Matrix to produce a new Current Response Vector. This is 1 *x m* * *m x m* which yields a 1 *x m* vector, and effectively computes the effect of all influences (including influences raised by the event) over the employee, to include influence matrix affects. In the example, Equation 3 is multiplied by the Influence Matrix (Figure 16), with the new Current Response Vector being the final result on the right (Equation 4).

$$\begin{bmatrix}2 & 3 & 2 & 4\end{bmatrix} * \begin{bmatrix}0 & 0 & 1 & 0\\ 1 & 0 & 1 & 1\\ 1 & 0 & 0 & 0\\ 1 & 0 & 1 & 0\end{bmatrix} = \begin{bmatrix}10 & 0 & 9 & 3\end{bmatrix} \qquad (4)$$

3.9 Outputs

The RPM produces four outputs: the Current Response Vector, the Current Score (also the initial score as a result of the first iteration with no stimulus), a linear regression, and the change in scores versus time. Each is described below:

3.9.1 Current Response Vector.

Transposing the new Current Response Vector from Equation 4 yields an *m x* 1 vector, which represents a list of all the influences that currently affect the employee and to what magnitude (Figure 21). In the situation where another event occurs, this vector is fed back into the RPM as the Response Vector input. Note that in John Smith's Initial Response Vector (see Figure 19 above), he had no influence from family financial status, but now does because Event B has added the influence. Although produced as an output

of the RPM, it is more valuable as a new input to the next iteration of the RPM, and is not considered an output for purposes of the model test in Chapter IV.

Response Vector	John Smith
Stress	10
Pay Raise	0
Relationship with Family	9
Family Financial Status	3

Figure 21. Response Vector for Employee John Smith AFTER Event B has Occurred

3.9.2 Current Score.

The Current Response Vector presents the important ability to track the current state of influences over an employee. It serves as a snapshot of the employee's current situation, but is also the fundamental method of continued monitoring of an employee by returning it to the RPM during the next iteration performed on another event. However, the vector is still a list of influences and every employee has a different list with different magnitudes. In order to better predict the risk an employee poses to the organization, another metric is needed. The sum of the elements of the Current Response Vector yields a Current Score (Figure 22), or in the case of the first iteration, the Initial Score. This score is used to compare employees to each other or more importantly, against an organization's established norm.

Response Vector	John Smith
Stress	10
Pay Raise	0
Relationship with Family	9
Family Financial Status	3
Current Score	**22**

Figure 22. Current Score for Employee John Smith (Sum of Response Vector)

There are numerous ways for an organization to use the Current Score, but just like choosing the influences and events to use in the RPM and populating the Influence and Event Matrices, the method of analysis is left to each organization. While some organizations set thresholds, others establish scores representing the norm and look for scores that greatly deviate from the norm, and still others look at the amount of change over time as an indicator of risk.

3.9.3 Linear Regression (Trend Lines).

The third output available from the RPM is a linear regression of the scores. "Linear regression is a mathematical process that determines the best linear fit through a set of data points." [21] "Linear regression is widely used in biological and behavioral sciences to describe relationships between variables. It ranks as one of the most important tools used in these disciplines." [22] By taking the linear regression of a set of scores, the organization establishes trends, comparable to slopes, on each of their employees. As before, it is left to the organization to determine how to use the information, but establishing a baseline regression, and then looking for large degrees or angles of

separation between employees' regressions and the baseline regression is a good example (see Chapter IV). Other options are setting a threshold slope and looking for slopes that exceed the threshold, or establishing a "normal" slope and looking for slopes that significantly deviate from "normal". These are indicators of heightened risk that security personnel use to stop insider damage before it occurs. Another way to look at the slopes or regression is to watch employees' regression lines grow over time and pay close attention to the ones that grow faster than normal. The example used so far in this chapter has only inserted one event, and although enough to show a slope, Chapter IV provides a much better example of this capability.

3.9.4 Change in Scores Versus Time.

The final output of the RPM is useful to organizations interested in the amount of Change in Scores Versus Time. By plotting scores over certain time periods, organizations observe the periods of heightened activity, which, like scores, are used in any number of ways and is left to the organization to decide how to make them useful. Examples are interest in seeing the change in scores over a three-year window or watching the change quarterly.

Another significance of the Change in Scores Versus Time metric is that organizations choose the time period of interest. By setting the time period small enough, changes in score for each event in an employee's history are seen, conversely by selecting a longer the time period, the change in score by quarter, year, or assignment are available which provide organizations with a bigger picture of employee risk. Again, the example

used in this chapter has only produced two scores (one change), but a more interesting example is provided in Chapter IV.

3.10 Summary

This chapter presented the concepts behind the Risk Predictor Model, starting with a firm modeling foundation, continuing with a formal description of the model and mathematics involved, and finishing with in-depth details about the model itself, both in what it does and how it does it. The model as described is intended to identify employees with a higher risk of performing insider damage against an organization. It is in no way an "insider detector", but rather a security tool that identifies another indicator, in this case risk, which assists in mitigating insider threat. However, before the model is implemented, it is necessary to verify that it does what is intended. Chapter IV provides an in-depth case study as well as rigorous testing necessary to exercise the model properly.

IV. Application and Case Study

Chapter III gave a detailed description of the Risk Predictor Model, from model inception to usefulness of it outputs. The example presented throughout the chapter was sufficient to illustrate the steps involved in creating the model, but was too limited to serve as a full operations check of the model. This chapter describes the method of testing the model, including how it is populated as well as tested using a detailed case study. Also included, is a thorough account of the model outputs following the test.

4.1 Adjudicative Guidelines

Now that the model design is complete, it is necessary to populate and test it. For purposes of testing the model in this research, the static Influence and Event matrices in the model are populated using the Thirteen Adjudicative Guidelines for Determining Eligibility for Access to Classified Information (Figure 23).

(1) GUIDELINE A: Allegiance to the United States;
(2) GUIDELINE B: Foreign influence;
(3) GUIDELINE C: Foreign preference;
(4) GUIDELINE D: Sexual behavior;
(5) GUIDELINE E: Personal conduct;
(6) GUIDELINE F: Financial considerations;
(7) GUIDELINE G: Alcohol consumption;
(8) GUIDELINE H: Drug involvement;
(9) GUIDELINE I: Emotional, mental, and personality disorders;
(10) GUIDELINE J: Criminal conduct;
(11) GUIDELINE K: Security violations;
(12) GUIDELINE L: Outside activities;
(13) GUIDELINE M: Misuse of Information Technology Systems

Figure 23. Adjudicative Guidelines for Determining Eligibility For Access To Classified Information [23]

In 1997, these guidelines were approved by the President of the United States for use by "all U.S. government civilian and military personnel, consultants, contractors, employees of contractors, licensees, certificate holders or grantees and their employees and other individuals who require access to classified information" and for "initial or continued eligibility for access to classified information, to include sensitive compartmented information and special access programs, and are to be used by government departments and agencies in all final clearance determinations." [23] Below is a short description of each guideline.

4.1.1 Guideline A: Allegiance to the United States.

Key words – "Individuals must be of unquestioned allegiance to the United States…or the safety of classified information is in doubt." [23]

4.1.2 Guideline B: Foreign Influence.

Key words – A security risk from potential foreign influence exists when an individual's immediate family or someone he or she is bound by influence are not citizens of the United States, which potentially results in the compromise of classified information. "Contacts with citizens of other countries or financial interests in other countries…make an individual potentially vulnerable to coercion, exploitation, or pressure." [23]

4.1.3 Guideline C: Foreign Preference.

Key words – "When an individual acts in such a way as to indicate a preference for a foreign country over the United States, then he or she is prone to provide information or make decisions that are harmful to the interests of the United States." [23]

4.1.4 Guideline D: Sexual Behavior.

Key words – "Sexual behavior is a security concern if it involves a criminal offense, indicates a personality or emotional disorder…or reflects lack of judgment or discretion." [23]

4.1.5 Guideline E: Personal Conduct.

Key words – "Conduct involving questionable judgment, untrustworthiness, unreliability, lack of candor, or unwillingness to comply with rules and regulations could indicate that the person may not properly safeguard classified information." [23]

4.1.6 Guideline F: Financial Considerations.

Key words – "An individual who is financially overextended is at risk of having to engage in illegal acts to generate funds. Unexplained affluence is often linked to proceeds from financially profitable criminal acts." [23]

4.1.7 Guideline G: Alcohol Consumption.

Key words – "Excessive alcohol consumption often leads to the exercise of questionable judgment, unreliability, failure to control impulses, and increases the risk of unauthorized disclosure of classified information due to carelessness." [23]

4.1.8 Guideline H: Drug Involvement.

Key words – "Illegal involvement with drugs raises questions regarding an individual's willingness or ability to protect classified information. Drug abuse or dependence may impair social or occupational functioning, increasing the risk of an unauthorized disclosure of classified information." [23]

4.1.9 Guideline I: Emotional, Mental, and Personality Disorders.

Key words – Mental Health "disorders can cause a significant deficit in an individual's psychological, social and occupational functioning…[which] may indicate a defect in judgment, reliability or stability." [23]

4.1.10 Guideline J: Criminal Conduct.

Key words – "A history or pattern of criminal activity creates doubt about a person's judgment, reliability and trustworthiness." [23]

4.1.11 Guideline K: Security Violations.

Key words – "Noncompliance with security regulations raises doubt about [a person's] trustworthiness, willingness, and ability to safeguard classified information." [23]

4.1.12 Guideline L: Outside Activities.

Key words – "Involvement in certain types of outside employment or activities is of security concern if it poses a conflict with an individual's security responsibilities and could create an increased risk of unauthorized disclosure of classified information." [23]

4.1.13 Guideline M: Misuse of Information Technology Systems.

Key words – "Noncompliance with…regulations pertaining to information technology systems may raise security concerns about an individual's trustworthiness…and ability to properly protect classified systems, networks, and information." [23]

4.1.14 Adjudicative Process.

"The adjudicative process is an examination of a sufficient period of a person's life to make an affirmative determination that the person is an acceptable security risk. Eligibility for access to classified information is predicated upon the individual meeting these personnel security guidelines. The adjudication process is the careful weighing of a number of variables known as the whole person concept. Available, reliable information about the person, past and present, favorable and unfavorable, should be considered in reaching a determination." [23]

4.2 Populating the Model

As discussed during model development (Chapter III), the actual influences and events used in the model are organization specific and populated by an organization expert, someone familiar with the organization's wants and needs. The Adjudicative Guidelines are used by all government agencies to grant security clearances and for this reason, the model is populated with influences and events that stem from the guidelines. Thus, as the model tracks employees throughout their careers, it is as if they are constantly being checked against the guidelines that granted them clearance in the first place.

4.2.1 Influences and Descriptions.

The Sample Influence Matrix is populated with thirty influences based on the Adjudicative Guidelines (Figure 24). Each guideline is represented at least once and some are represented more than once. Guidelines E and F are represented several times each

because they signify events that are most common and observable in employees' behavior.

Influence	Guideline
Stress	I
Have Criminal record	J
Self Esteem	I
Use of legal substances (Caffeine, Nicotine, Social drinking)	G
Use of Narcotics/Addictions (alcoholism, gambling)	H
S/TS clearance	K
High profile job	F
Satisfaction with company/organization	F
Expectations for advancements (promotion/pay raise)	F
Job security/stability	F
Workload, quantity/ability to meet deadlines	F
Amount of and ability to deal with complex technology	M
Experience required for job	F
Community involvement	L
Relationship with family	B
Social commitments (relationship w/friends or foreign influence)	B
Involved in illicit/illegal relationships	D
Religious practices	L
Satisfaction with salary	F
Family financial stability/security (debt, savings, retirement, etc.)	F
Relationship with Co-workers	E
Desire to cover for inadequacies	E
Greed	F
Feeling of invincibility - can't get caught	E
Name recognition (narcissism)	E
Experienced rejection	I
Opportunity (lack of Organized Defense)	E
Satisfaction with country/politics (patriotism)	A
State of the Economy	F
Concern for world condition (foreign preference)	C

Figure 24. Influences Used in the Sample Influence Matrix

The influences chosen have general names to make them wieldy in the matrices and vectors, but require short definitions to help categorize various influences in employee's lives. Each organization not only chooses the influences it wants to use and

the degrees to which they affect each other, but also defines each influence so they are clearly distinct from one other. The influences used in this test of the RPM are defined as follows, with low (or positive) amount of influence being represented by -2 on the Likert Scale and high (or negative) amount of influence represented by 2 on the Likert Scale. Additionally, each influence is considered to affect the employee if someone observes it and reports it to the organization or the employee admits to it.

Stress refers to any external stimulus that causes a physiological response in the employee. *Have Criminal Record* refers to the effects of current or past criminal activities in the employee's life, for example, a past mistake is forgotten by the employee, but not necessarily by disgruntled accomplices. *Self Esteem* refers to the current level of self-esteem the employee displays. *Use of Legal Substances* such as caffeine, nicotine, or social drinking refers to the number of and amount of legal substances the employee uses. *Use of Narcotics or Addictions* such as alcoholism or gambling refers to the number of and amount of illegal substances the employee uses.

Secret or Top Secret Clearance refers to the current level of clearance the employee has. *High Profile Job* refers to the type of position the employee holds within the organization, such as political office, high rank official, or coveted job in public service such as police officer, fire fighter, or FBI agent. *Satisfaction with Organization* refers to the employee's apparent happiness with the organization as a whole. *Expectations for Advancements* refers to the employee's satisfaction with expectation for promotion or pay raises within the organization. *Job Secu*rity refers to climate within the organization regarding the stability of each employee's position.

Workload or Ability to Meet Deadlines refers to the amount of work the employee has, whether deadlines are reasonable, and whether the employee has the ability and appropriate materials available to meet deadlines. *Amount of and Ability to Deal with Complex Technology* refers to the amount of complex technology within the organization, the employees' ability to use it, the training offered by the organization and the conditions for employees unable to adjust to the complex technologies. *Experience Required for the Job* refers to the amount of experience required for the job, the employee's level of experience and its correlation to the experience needed for the job. *Community Involvement* refers to the opportunity (time) for and the employee's satisfaction with involvement in the employee's community. *Relationship with Family* refers to the time for and quality of the employee's relationship with family.

Social Commitments refers opportunity (time) for and the employee's satisfaction with social commitments to include relationships wit friends or foreign influences. *Involved in Illicit or Illegal Relationships* refers to the employee's involvement in relationships with extramarital partners, prostitution, or other characters who partake in illegal activities such as drug dealers. *Religious Practices* refers to the level of influence religious faith holds over the employee. *Satisfaction with Salary* refers to the employee's satisfaction with his or her salary and belief that he or she is being paid fairly. *Family Financial Security* refers to the employee's apparent satisfaction with his or her income, debt, savings, insurance, and retirement plan.

Relationship with Co-workers refers to how the employee gets along with co-workers, subordinates and supervisors, as well as how they get along with the employee

and whether the employee is a loner. *Desire to Cover for Inadequacies* refers to the employee's need to cover up any inadequacy, self imposed or otherwise. *Greed* refers the employee's need to build financial wealth and to what lengths the employee goes to achieve such wealth. *Feeling of Invincibility* refers to the employee's apparent belief that he or she cannot or will not get caught doing something unauthorized. *Name Recognition or Narcissism* refers to the degree the employee wished to make a name for himself or herself and to what ends the employee goes to achieve such recognition.

Experienced Rejection refers to the number of times, the severity of, and the employee's perceived ability to handle rejection, whether it is from employers, potential mates, etc. *Opportunity* refers to the employee's perceived opportunity to cause damage due to known lack of organized defense within the organization. *Satisfaction with Country and Politics* refers to the employee's commitment to the US, perceived happiness with politics (party in office) and overall patriotism towards the US. *State of the Economy* refers to the employee's current satisfaction with the state of the economy and expectations that such state has a negative impact on the employee (e.g., high gas prices). *Concern for World Condition* refers to the employee's predilection for foreign preference or the degree to which the employee values the opinions of foreign nations, especially with respect to American foreign policy.

4.2.2 Influence Matrix.

Next, the influences are entered into the influence matrix where each influence is systematically analyzed against each of the other influences to determine its effect on them. Again, as discussed during model development, this process is accomplished by a

subject matter expert, preferably someone with human behavior experience. Patrick B. McGrath, Ph.D., is the Clinical Manager of Anxiety Services at Linden Oaks Hospital at Edward. Dr. McGrath is a clinical psychologist and holds a Bachelor's Degree in Psychology from Illinois Wesleyan University, a Master's Degree in Clinical Psychology from Mississippi State University, and a Doctoral Degree in Clinical Psychology from Northern Illinois University. Further, he completed a two-year Postdoctoral Fellowship through the St. Louis University School of Medicine at the St. Louis Behavioral Medicine Institute. Dr. McGrath served as subject matter expert for purposes of this research [24], and with his help, each of the 900 cells in the influence matrix was analyzed to produce the populated influence matrix shown in Appendix A.

4.2.3 Events and Descriptions.

The Sample Event Matrix is populated with twenty-seven events, also based on the Adjudicative Guidelines (Figure 25 below).

Like the influences above, the events chosen also have general names, but require definitions to help categorize occurrences in employee's lives into the correct event name. They are defined below.

Event	Guidelines
Alarming Statement	B, C, D, E
Reported insider transgression	K, M
Action out of Character	E, I
Salary anomaly	F
Excessive Interest	B, C
Scrupulosity (Religious Fanaticism)	A, E, I
Personality Quirk	I
Unexplained affluence	F
Legal Activity (Minor)	D, E, J
Legal Activity (Moderate)	D, E, J
Legal Activity (Major)	D, E, J
Reprimanded	D, E, J
Increased Absenteeism/Tardiness	E
Change in Mental Health (positive)	I
Change in Mental Health (negative)	I
Change in Physical Health (positive)	I
Change in Physical Health (negative)	I
Change in work environment (positive)	E, F, J
Change in work environment (negative)	E, F, J
Recently fired	D, E, J
Recently retired/quit	F, I
Catastrophic event	F, I
Change in family status (positive)	B, F
Change in family status (negative)	B, F
Financial impact	F
Foreign interaction	B, C
Hostile environment	A, B, C

Figure 25. Events Used in the Sample Event Matrix and Stimulus Vector

An *Alarming Statement* is a public statement made by an employee or about an employee that indicated a potential security risk to those that heard it. A *Reported Insider Transgression* occurs when an employee is reported, through word of mouth or through official channels, to have caused actual insider damage. An *Action out of Character* occurs when an employee is witnessed acting out his/her normal behavior range. A *Salary Anomaly* occurs when an employee has experienced an oddity with respect to their current employment and their wages/benefits, such as salary not commiserate with job or

workload. *Excessive Interest* occurs when an employee is witnessed showing an odd amount of interest in a subject not normally within their sphere of interest, such as "need to know" violations.

Scrupulosity, or religious fanaticism, occurs when an employee is witnessed showing or having extreme religious beliefs, such as occultism. A *Personality Quirk* occurs when an employee is witnessed having or showing abnormal behavior. *Unexplained Affluence* occurs when an employee is witnessed showing or having excess resources with respect to their economic status or class, such as having excessive cash or buying expensive items on a limited salary. *Minor Legal Activity* occurs when an employee experiences minor legal actions such as traffic tickets or small claims court. *Moderate Legal Activity* occurs when an employee experiences moderate legal actions such as misdemeanors, lawsuits, divorce proceedings, or child custody suits. *Major Legal Activity* occurs when an employee experiences major legal actions such as felonies or court martial proceedings.

Reprimanded occurs when an employee receives punishment for an infraction at work to include leave without pay or suspension. *Increased Absenteeism/Tardiness* occurs when an employee is witnessed skipping work, calling in sick or coming in late more frequently than usual. *Change in Mental Health* occurs when an employee is has a change in mental health such as increased irritability, depression, anxiety, panic attacks or losing touch with reality (negative) or shows recovery from mental illness (positive). *Change in Physical Health* occurs when an employee has a change in physical health

such as injury, sickness, increased fatigue, or frequent visits to the doctor (negative) or shows a recovery from physical maladies (positive).

Change in Work Environment occurs when an employee experiences a change in employer, supervisor, job location, job title, position (promotion), pay scale (raise) or rank (positive) or a change in employer, supervisor, job location, job title, rank, position (demotion), pay scale (pay cut), or is the victim or perpetrator of sexual harassment or racism (negative). *Recently Fired* occurs when an employee has recently involuntarily left the organization such as being let go, fired, downsized, involuntary separated or dishonorably discharged. *Recently Retired or Quit* occurs when an employee has recently voluntarily left the organization. A *Catastrophic Event* occurs when an employee experiences terrorism, natural disaster such as fire, flood, earthquake, tornado, or hurricane, man-made disaster such as criminal activity, including arson, murder, kidnapping, rape, assault, theft, or personal loss such as loss of home.

A *Change in Family Status* (also includes close friends) occurs when an employee experiences a gain of family member, to include pregnancy or a change in relationship status such as marriage or marital reconciliation (positive) or the loss of family member, to include loss of pregnancy or a change in relationship status such as divorce or separation (negative). *Financial impact* occurs when an employee experiences a large financial change such as bankruptcy or a large purchase such as car, home, or boat. *Foreign Interaction* occurs when an employee is deployed, attached, assigned, or vacationing to a foreign location. *Hostile Environment* occurs when an employee is

inserted into a hostile, dangerous, or life-threatening environment, experiences combat, reunion stress, battle fatigue, or Post Traumatic Stress Disorder.

4.2.4 Event Matrix.

Next, the events are entered into the event matrix where each event is systematically analyzed against each of the influences (from the influence matrix) to determine its effect on the influences. As before, this process is accomplished by a subject matter expert, and Dr. McGrath helped analyze each of the 810 cells in the event matrix [24], producing the resulting populated event matrix shown in Appendix B.

4.2.5 Initial Stimulus Vector.

The Initial Stimulus Vector contains all zeros, as the initial employee evaluation occurs with no events. Figure 26 below represents the Initial Stimulus Vector used during the testing of the model.

4.2.6 Response Vectors.

The last model input populated before testing is the Response Vector. However, before the model differentiates between a normal employee and a malicious one, it is first necessary to consider the employee used to represent “normal”. The employee is subject to the same influence and event matrices as well as the initial stimulus vector. The exact nature of the normal employee is also left to the organization and its experts on the subject, as different organizations have vastly different ideas of normal. For some organizations, comparing all of their employees by using the model to generate an average is considered “normal”. Other organizations with specific needs precisely pick what they wish to consider normal. For purposes of this research, normal is being defined

as a "typical employee" who has initial responses and career events defined in the next sections.

Event	Stimulus Vector
Alarming Statement	0
Reported insider transgression	0
Action out of Character	0
Salary anomaly	0
Excessive Interest	0
Scrupulosity (Religious Fanaticism)	0
Personality Quirk	0
Unexplained affluence	0
Legal Activity (Minor)	0
Legal Activity (Moderate)	0
Legal Activity (Major)	0
Reprimanded	0
Increased Absenteeism/Tardiness	0
Change in Mental Health (positive)	0
Change in Mental Health (negative)	0
Change in Physical Health (positive)	0
Change in Physical Health (negative)	0
Change in work environment (positive)	0
Change in work environment (negative)	0
Recently fired	0
Recently retired/quit	0
Catastrophic event	0
Change in family status (positive)	0
Change in family status (negative)	0
Financial impact	0
Foreign interaction	0
Hostile environment	0

Figure 26. Initial Stimulus Vector

4.2.7 Typical Employee's Initial Response Vector.

The Typical Employee's Initial Response Vector used here shows the employee at career inception (Figure 27). The employee exhibits a moderate level of stress, has just received a Secret security clearance, and is optimistic about the organization, expectations for advancement and job security. Being new to the organization and young, the

employee is somewhat dissatisfied with salary, family financial stability, and the current state of the economy. On the other hand, the employee is patriotic and loyal to the United States.

Influence	Response Vector
Stress	1
Have Criminal record	0
Self Esteem	0
Use of legal substances (Caffeine, Nicotine, Social drinking)	0
Use of Narcotics/Addictions (alcoholism, gambling)	0
S/TS clearance	1
High profile job	0
Satisfaction with company/organization	-1
Expectations for advancements (promotion/pay raise)	-1
Job security/stability	-1
Workload, quantity/ability to meet deadlines	0
Amount of and ability to deal with complex technology	0
Experience required for job	0
Community involvement	0
Relationship with family	0
Social commitments (relationship w/friends or foreign influence)	0
Involved in illicit/illegal relationships	0
Religious practices	0
Satisfaction with salary	1
Family financial stability/security (debt, savings, retirement, etc.)	1
Relationship with Co-workers	0
Desire to cover for inadequacies	0
Greed	0
Feeling of invincibility - can't get caught	0
Name recognition (narcissism)	0
Experienced rejection	0
Opportunity (lack of Organized Defense)	0
Satisfaction with country/politics (patriotism)	-1
State of the Economy	1
Concern for world condition (foreign preference)	0

Figure 27. Typical Employee's Initial Response Vector

4.2.8 Typical Employee's Career Stimuli.

Next, the Typical Employee's Career Stimuli are generated. For purposes of this research, the employee is considered to have 13 years with a government organization (from 1993 to present), has had several promotions and multiple assignments. Along the way, the employee has had several additions to the family and some short family separations due to work. In addition, there have been short periods of financial difficulty, as well as some minor legal action due to a traffic ticket and an automobile accident. Finally, in recent times, the employee has had some trouble with family and health. All total, there are 53 stimuli from the employee's 13-year career (Figure 28). Note, the Typical Employee's Initial Score is shown in 1992, just prior the employee's acceptance into the government organization.

This is a reasonable representation of a typical employee. No one goes through life without obstacles and including several events near the end of the stimulus list helps test the ability of the model to differentiate between normal and malicious while still showing increased risk. Also, none of the 53 events has anything to do with malicious insider intent to cause damage.

Year	Description	Stimulus
1993	Career Inception	Change in work environment (positive)
1993	Assignment	Change in work environment (positive)
1993	Assignment	Change in work environment (positive)
1993	Assignment	Change in work environment (positive)
1993	Reunited with family after short separation	Change in Family (positive)
1993	Financial problems	Financial Impact
1993	Assignment	Change in work environment (positive)
1993	Assignment	Change in work environment (positive)
1993	Assignment	Change in work environment (positive)
1993	Assignment	Change in work environment (positive)
1994	Reunited with family after short separation	Change in Family (positive)
1994	Child born	Change in Family (positive)
1995	Pay Raise	Change in work environment (positive)
1995	Promotion	Change in work environment (positive)
1996	Assignment	Change in work environment (positive)
1996	Car Accident and lawsuit	Legal Activity (minor)
1997	Child born	Change in Family (positive)
1997	Pay Raise	Change in work environment (positive)
1998	Assignment	Change in work environment (positive)
1998	Assignment	Change in work environment (positive)
1998	Assignment	Change in work environment (positive)
1998	Assignment	Change in work environment (positive)
1998	Assignment	Change in work environment (positive)
1998	Promotion	Change in work environment (positive)
1999	Pay Raise	Change in work environment (positive)
1999	Child born	Change in Family (positive)
2000	Financial problems	Financial Impact
2001	Pay Raise	Change in work environment (positive)
2001	Speeding ticket	Legal Activity (minor)
2001	Assignment	Change in work environment (positive)
2002	Assignment	Change in work environment (positive)
2002	Financial problems	Financial Impact
2002	Assignment	Change in work environment (positive)
2002	Assignment	Change in work environment (positive)
2002	Promotion	Change in work environment (positive)
2002	Assignment	Change in work environment (positive)
2002	Assignment	Change in work environment (positive)
2002	Assignment	Change in work environment (positive)
2002	Family trouble	Change in Family (negative)
2002	Health Problem	Change in Mental Health (negative)
2002	Health Problem resolved	Change in Mental Health (positive)
2003	Pay Raise	Change in work environment (positive)
2003	Family trouble	Change in Family (negative)
2003	Health Problem	Change in Mental Health (negative)
2004	Promotion	Change in work environment (positive)
2004	Health Problem resolved	Change in Mental Health (positive)
2004	Family trouble resolved	Change in Family (positive)
2004	Assignment	Change in work environment (positive)
2005	Pay Raise	Change in work environment (positive)
2005	Health problem	Change in physical health (negative)
2005	Health Problem resolved	Change in physical health (positive)
2005	Financial problems	Financial Impact
2006	Promotion	Change in work environment (positive)

Figure 28. Typical Employee's Career Stimuli

4.3 Case Study

Making up the typical employee for the model test is acceptable, primarily because each organization creates its own version of a typical employee to peg its employees against during operational use of the model. However, to test that the model can, in fact, differentiate between a normal employee and a malicious one, it is necessary to use a real perpetrator of insider damage. To test the model, a case study on Robert Phillip Hanssen, the Federal Bureau of Investigation's (FBI) agent turned spy was performed.

4.3.1 Why choose Robert Hanssen?

There are several reasons for testing the RPM using the Hanssen case study for the malicious insider. For starters, he was caught in February 2001 after 25 years of selling secrets to the Soviet Union and Russia. This provides a long history of transgressions, which yields an ample supply of observable and recordable behaviors that are typical of malicious insiders. Second, his apprehension was purely accidental; the FBI had no clue what was going on until a Russian agent turned over boxes of FBI information that Hanssen had secretly turned over to his handlers during the previous 25 years. Even after receiving all the contraband, FBI operatives had no clue who the culprit was and claimed it could take years to find out; until they found Hanssen's fingerprints on the plastic garbage bags he had wrapped his illegal packages in. This is significant because it gives the model an opportunity to flag Hanssen as a high risk for causing insider damage long before his accidental capture occurred. The model is not designed to only identify high-risk employees, but also identify them early, thus reducing the amount of damage that

occurs. Finally, although Hanssen's case is considered one of the most damaging cases of espionage in history, the fact that he led two separate lives is significant because it makes him just like all the other insiders that have caused damage. On the outside, he was a seemingly patriotic, deeply religious family man, but on the inside, he was a cold calculating spy, capable of giving the Soviets the names of three Russians (who were later executed or imprisoned) who were spying for the US. This makes even Hanssen's high profile case, complete with accidental capture and extreme length of maliciousness, susceptible to anomaly detection. A person that lives two lives is going to make mistakes, and that is where the Risk Predictor Model comes in.

4.3.2 Brief Historical View of Hanssen.

It is important to begin with a brief history of Hanssen's career with the FBI before creating his Initial Response Vector and career stimuli. Prior to establishing initial influences for Hanssen, it is necessary to get to know him in detail. Similarly, it is important to research the details of Hanssen's life in order to properly assess which events in his life were observable and reportable, or were matters of public record, and which were not. For example, there were five separate incidents prior to Hanssen's arrest where he was either directly implicated in causing insider damage or even admitted to it, however only three were reported, and none were taken seriously. It is suspected that in addition to his wife, several Catholic priests, a marriage counselor, a former colleague and a senior FBI field supervisor knew about or expressed concerns about Hanssen's activities [25]. Unfortunately, the two instances that were not reported were not observables (to the FBI) and therefore were not considered for use in the testing of the

RPM. However, for completeness, the events are included in the short history of Hanssen's FBI career that follows. Also note that unless specifically cited, all information regarding Hanssen came from Adrian Havill's book, *The Spy Who Stayed Out in the Cold: The Secret Life of FBI Double Agent Robert Hanssen* [26].

4.3.3 The Early Years (1976-1978).

Robert Phillip Hanssen was sworn into the FBI on January 12, 1976 on his second attempt to get in [27]. He was married to Bonnie Wauck (his wife of seven years) and already had two of his eventual six children, Jane and Susan, when he entered the FBI at age 31. After initial training in Indianapolis, he was assigned to the White Collar Crime Squad in Gary, Indiana. His first boy (3rd child), John was born in 1977 while he was assigned to Gary.

4.3.4 Hanssen Crosses the Line (1979-1981).

In August 1978, Hanssen was assigned to the FBI Field Office in New York [28], where his 4th child, Mark Edward, was born in 1980. During their three-year stay in New York, beginning in 1979, Hanssen offered several Russian agents secrets in exchange for money. In 1981, he was caught counting $20,000 in $100 bills by his wife. He boasted of his deals, but she made him promise to never do it again and go to a priest [27]. Hanssen did visit with Opus Dei priest, Robert P. Bucciarelli, who considered turning him in, but then thought it a breach of clerical ethics. Instead, he told Hanssen to give the cash to charity, which Hanssen did.

The Hanssens were members of Opus Dei, a conservative and controversial Catholic organization with US roots in Chicago dating back to 1949. With only 84,000

members worldwide and only 3,000 in the US, it is exclusive and some critics say cult like, claiming members practice self-mortification and self-flagellation to share the pain of Christ. By 1981, longtime Hanssen friend, Paul Moore, grew tired of lectures from Hanssen regarding visits to strip clubs for farewell parties with co-workers. Hanssen claimed it was an occasion of sin to do that.

4.3.5 Hanssen Assigned to Washington (1981-1985).

From January 1981 to September 1985, Hanssen was assigned to the FBI Headquarters in Washington, D.C., first to the Budget Unit and then to the Soviet Analytical Unit [28]. In 1983, the Hanssen's 5th child, Greg, was born. Hanssen was promoted when he moved into the Soviet Analytical Unit. During this period, Hanssen claimed that educating his kids in Opus Dei schools would hopefully lead to a new world order in the future that his children could possibly lead. Somehow, Hanssen sent six children to exclusive and very expensive schools on a limited income. In 1985, the Hanssen's last child, Lisa, was born.

4.3.6 Hanssen Betrays Again (1985-1987).

Hanssen was reassigned to New York to work in the FBI Field Office Intelligence Division in September 1985. Just prior to Hanssen's arrival in New York, his boss claimed the FBI needed to recognize that the pay was low, the cost of living was high, and that it was easier to lure an agent to the other side. Hanssen arrived and witnessed first hand how expensive it was compared to his pay of $34,000 per year. In October 1985, after a five-year hiatus from espionage, Hanssen sent a letter outlining his intent to sell secrets to his Soviet handlers at the home of a Soviet embassy official [29]. In another

letter, Hanssen detailed how to transfer information and payments via secret drop locations and signals [28].

Between 1985 and 1991, Hanssen gave up 6,000 pages and 26 disks of secret documents, including nuclear deployment plans and satellite positions, and the identities of at least nine Soviets who were spying for the US or being recruited to spy [30]. At least two of the Soviet spies that Hanssen identified were eventually executed and one imprisoned as a result of his information [31]. In return he received over $600,000 (plus $800,000 in a Moscow bank), some jewelry (reportedly diamonds [31]) and a Rolex watch [27].

In 1985, Hanssen ended public displays of affection with his family, appearing busy and distracted, due to an important job. During his second tour in New York, fellow employees dubbed him “Doctor Death” because of his shallow complexion and predilection for wearing the same black suit five days per week [25]. Others nicknamed him “Digger” and “The Mortician” because of his slight stoop and aloof demeanor [30]. During this period, Vlad Azbell, a part time New York counter-intelligence document translator witnessed Hanssen ignoring sensitive info about the Soviet Union, not processing it through proper channels and discarding info, but did not report it. Later, when he did report it, the report was ignored and Hanssen retaliated by having Azbell undergo polygraph testing because he was Russian.

4.3.7 Continued Espionage (1987-1991).

In 1987, Hanssen was once again assigned to FBI Headquarters in Washington, D.C., where he remained for the rest of his career, holding various positions, including

Supervisory Special Agent in the Intelligence Division's Soviet Analytical Unit (1987-1990), Inspector's Aid in Headquarters Inspections Staff (1990-1991), Program Manager in the Soviet Operations Section (1991-1992), Chief of National Security Threat List Unit (1992-1994), FBI's Washington Field Office (8 months in 1994), Office of the Assistant Director for the National Security Division (1994-1995), FBI's senior representative to the Office of Foreign Missions of the US Department of State (1995-2001) and finally, after suspicions were raised, Hanssen was assigned to the Information Resources Division (2001), where he was constantly monitored [28].

Shortly after arriving in Washington, Hanssen put an $80,000 cash down payment on his $205,000 house after only receiving $47,000 profit for his New York home. In 1987, once again, Hanssen enrolled his children in expensive elite Opus Dei schools, on barely $60,000 per year salary. In 1988, Hanssen paid cash for $80,000 in home improvements, to include a finished basement, recreation room, fireplace, television, computer, and deck, and his wife even wondered how they could afford it. By 1989, Hanssen was a self-taught computer hacker and programmer, and expressed excessive interest in hacking. He also tried to convince the FBI, members of his family, and his Soviet handlers to become "wired" and attempted to bring them into the electronic age.

In 1989, the FBI began investigating the claims that State Department official Felix Bloch was working with Soviet agents. When Hanssen found out about it, he told his handlers, and saved Bloch from capture. Hanssen later mulled around in his supervisors office agonizing over who could have possibly tipped off Bloch. Hanssen was promoted in 1990 in conjunction with his move to the FBI Headquarters Inspections

Staff. In 1990, records indicate that Hanssen gave his brother-in-law, George Beglis, several thousand dollars to buy a Mac 2 computer for his architectural firm.

In 1990, Hanssen "befriended Priscilla Sue Galey, a stripper who became addicted to cocaine, but believed he was absolved since no sex ever took place." [27] He believed he was saving her, by buying her a Mercedes (even though his wife was still driving an older minivan), fixing her teeth, buying her jewelry, and giving her a credit card. He eventually spent over $100,000 on her and even took her with him on a business trip to Japan [25]. Later, in 1992, when she got hooked on cocaine and started spending extra money on the credit card, Hanssen took it away and abandoned her, even when she was arrested and phoned him for help [27].

4.3.8 Communism Falls, but Hanssen's Behavior is Still Suspect (1991-1998).

In 1991, when communism was declared dead, Hanssen went underground [27]. In 1992, James Bamford, an investigative author, was sent to Moscow to interview Viktor Cherkashin, Hanssen's handler, about which Hanssen expressed excessive interest in seeing the extra film footage, worried that something might have been said that could have compromised him. Later, Bamford noticed Hanssen's excessive interest in the Felix Bloch case. Hanssen reveled in showing others how much smarter he was than his superiors and in 1992, to make a point that the FBI had serious security holes in its systems, Hanssen hacked into his boss' computer [25]. Between 1992 and 1996, the Hanssens receive several traffic violations as they attempted to maintain their busy lifestyle.

In 1993, Hanssen physically assaulted Kim Lichtenberg, an FBI administrative assistant, after she left early from a meeting in his office [27]. During the investigation, Lichtenberg swore in a statement to Richard Spicer and Garrett Davis (FBI investigators) that Hanssen grabbed and shook her a few days earlier in front of witness agent Frank Figluisi. She also claimed that Hanssen touched Betsy Carroll, an FBI employee, in ways that made her uncomfortable, and that Hanssen had a habit of walking up to desks and just staring at employees. When asked if he needed help, he would say no and walk away. Lichtenberg filed charges with the police, but the case was not prosecuted because the FBI said it was an internal affair, however, Hanssen was suspended for five days because of the incident [27]. Later that year, Lichtenberg claimed Hanssen was always hacking into someone's computer hard drive and pointing out how easy it was to get their classified info and that "there were a lot of reasons to look into Hanssen." [26]

In 1994, Bamford was exposed to Hansen's fixation with Opus Dei, Catholicism, and fighting the godless commies, which he found too much to handle. In 1995, David Major, Hanssen supervisor, noticed the same zeal, and said Hanssen put religion into most conversations, saying that without religion, man is lost. In 1997, Earl Edwin Pitts, another counter-intelligence double agent, was captured by the FBI. During his 70-hour debriefing, he was asked if he knew anyone at FBI headquarters working for the Russians. Pitts said he did not, but he knew of a few odd incidents with Hanssen and talked about him hacking into others' computers. The FBI said that they knew about it and ignored it.

4.3.9 Everything Happens in Threes (1999-2001).

In 1999, after an eight-year break from espionage, Hanssen resumed contact with his now Russian handlers and continued to sell secrets until his capture in February 2001 [28]. In 1999, despite all of Hanssen's religious fanaticism, he bragged to co-workers about having a middle-aged crush on "hottie" Catherine Zeta-Jones. It also appears that Hanssen became more sexually deviant towards the end of his career. "In the months prior to being caught, Hanssen spent hours in his basement cruising porn sites, even posting masturbatory fantasies online and using the real name of his wife and friends." [27] He even boasted of secretly setting up a camera in his bedroom so an old friend could watch the Hanssens having sex, claiming his wife "may be the only teacher at the elite girl's school…who is also a porn star!" [30]

In November 2000, Russian double agent Sergey Tretyakov turned over all of Hanssen's dead drop packages containing all the information he disclosed to his handlers. Tretyakov did not know who the American double agent was, but the FBI found Hanssen's fingerprints on the packaging and put him under constant surveillance. In February 2001, Hanssen was caught red-handed at a dead drop and taken into custody. He later agreed to a deal with prosecutors to avoid the death penalty by fully cooperating with authorities. He is currently serving a sentence of life in prison without the possibility of parole; he is 62.

4.3.10 Hanssen's Initial Response Vector.

Hanssen worked for the FBI, so the model works nicely as it is populated thus far, because the FBI is a US government agency that uses the Adjudicative Guidelines for its

employees as well. Based on Adrian Havill's account of Hanssen's life before the FBI [26], it is clear that Hanssen was extremely intelligent, earning a bachelor of science degree in chemistry from Knox College in 1966, gaining entrance into the highly competitive Northwestern University's dental school and transferring into Northwestern's prestigious Kellogg School of Management where he earned an MBA in accounting. Hanssen felt that he was smarter than most people around him, often bragging about it. In addition, prior to joining the FBI, Hanssen joined the Chicago Police Department. While attending the Police Academy, he was pulled out of class, enrolled in the police department's secret C-5 unit, and sent off to a covert espionage center to learn counter-intelligence. Hanssen excelled in the section, but was told by his supervisor that he was too smart for the street and should join the FBI. Given this background, Hanssen's Initial Response Vector represents him at the beginning of his FBI career (Figure 29). He exhibited a moderate level of stress and had just received a Top Secret security clearance in a high profile job at the FBI. His self-esteem was high and he was definitely confident in his abilities to do his job, as he was over qualified for the position.

Influence	Response Vector
Stress	1
Have Criminal record	0
Self Esteem	-1
Use of legal substances (Caffeine, Nicotine, Social drinking)	0
Use of Narcotics/Addictions (alcoholism, gambling)	0
S/TS clearance	2
High profile job	1
Satisfaction with company/organization	0
Expectations for advancements (promotion/pay raise)	0
job security/stability	0
workload, quantity/ability to meet deadlines	0
Amount of and ability to deal with complex technology	0
Experience required for job	-1
Community involvement	0
Relationship with family	0
social commitments (relationship w/friends or foreign influence)	0
Involved in illicit/illegal relationships	0
Religious practices	0
Satisfaction with salary	0
family financial stability/security (debt, savings, retirement, etc.)	0
Relationship with Co-workers	0
desire to cover for inadequacies	0
Greed	0
Feeling of invincibility - can't get caught	0
Name recognition (narcissism)	0
Experienced rejection	0
Opportunity (lack of Organized Defense)	0
Satisfaction with country/politics (patriotism)	0
State of the Economy	0
concern for world condition (foreign preference)	0

Figure 29. Hanssen's Initial Response Vector

4.3.11 Hanssen's Career Stimuli.

Lastly, Hanssen's Career Stimuli were generated. What follows here is a brief description of the observable situations that occur during Hanssen's career, the year in which they occur, and the specific events in the Event Matrix they correspond to. Note the specifics of these events were once again drawn from Adrian Havill's book [26]. In total, there are 46 events listed, starting with his entrance into the FBI in 1976 and ending

shortly before his capture in 2001 (Figures 30 and 31). These events are based on observed or reported incidents by the FBI or someone close to Hanssen that could have reported the incidents. Note, Hanssen's Initial Score is shown in 1975, just prior to his acceptance into the FBI.

Year	Description	Stimulus
1976	Sworn in to FBI	Change in work environment (positive)
1976	Assigned to Indianapolis	Change in work environment (positive)
1976	Assigned to Gary Indiana	Change in work environment (positive)
1977	3rd Child (John) Born	Change in Family (positive)
1978	ASSIGNED to NYC Aug 78 - Jan 81	Change in work environment (positive)
1978	"I wanted to be a spy ever since I was a child."	Alarming Statement
1978	Bonnie says she and Bob had a secret Swiss bank account.	Alarming Statement
1980	4th Child (Mark) born	Change in Family (positive)
1981	ASSIGNED to DC Jan 81 - Sep 85	Change in work environment (positive)
1982	Lectures long time friend against going to strip clubs for farewell parties with co-workers, saying that it was an occasion of sin to do that.	Scrupulosity (Religious Fanaticism)
1983	5th child (Greg) born	Change in Family (positive)
1983	Promotion to Soviet Analytical Unit	Change in work environment (positive)
1984	Educating his kids in Opus-Day schools, so they could lead a new world order in the future.	Scrupulosity (Religious Fanaticism)
1985	6th child (Lisa) born	Change in Family (positive)
1985	ASSIGNED to NYC Sep 85 - Aug 87	Change in work environment (positive)
1985	Bob's boss said that the FBI needed to be aware that the pay was low.	Salary anomaly
1985	Pay is not commiserate with the job.	Salary anomaly
1985	Public displays of affection, though always rare, had ended.	Personality Quirk
1986	Vlad Azbell, a part time NY counter intelligence document translator, claimed that Bob was ignoring sensitive info about the Soviet and not process it through proper channels.	Reported Insider Transgression
1986	Vlad did say something, and nothing was done about it. Bob sought revenge and had to undergo polygraph testing - Vlad was Russian.	Reported Insider Transgression

Figure 30. Hanssen's Career Stimuli (part 1)

Year	Description	Stimulus
1989	Bob's boss, David Major, recalled Bob would come into his office and agonize about who had alerted Felix Bloch (it was Bob himself).	Excessive Interest
1990	Bob got promoted and assigned to the FBI inspection staff.	Change in work environment (positive)
1990	Records show that Bob gave his brother in law, George Beglis, several thousand dollars to buy and Mac 2 computer for his Architectural firm.	Unexplained Affluence
1990	Bob meets Priscilla Sue Galey (PSG), stripper at Joanna's club, within days gave her several thousand dollars in $100's to get her teeth fixed.	Unexplained Affluence
1990	Gave PSG expensive jewelry, flowers.	Unexplained Affluence
1991	Gave PSG a 1985 Mercedes 190-E sedan purchased with cash and an American Express card.	Unexplained Affluence
1991	Bob spends over $80,000 on PSG.	Unexplained Affluence
1992	Bob gives up quest to save PSG when she over uses the Credit card and buys drugs.	Action out of Character
1992	James Bamford goes to Moscow to interview Bob's handler, Viktor Cherkashin, and notes Bob expresses a keen interest in seeing the extra film footage	Excessive Interest
1992	James Bamford notes Bob's fascination with Felix Bloch	Excessive Interest
1992	Traffic tickets for Bob, Bonnie, and the kids.	Illegal Activity (Minor)
1993	Abuse of Kim Lichtenberg	Illegal Activity (Major)
1993	More accusations of shaking and inappropriate touching at work, in front of witnesses.	Illegal Activity (Moderate)
1993	More accusations of stalking and harassment at work.	Illegal Activity (Moderate)
1993	Bob is suspended for 5 days without pay for KL incident	Reprimanded
1993	Lichtenberg claims Bob was always hacking into someone's computer hard drive and " there was a lot of reasons to look into Bob."	Reported Insider Transgression
1994	Bamford exposed to Hansen's fixation with Opus-Day, Catholicism, fighting of godless communists	Scrupulosity (Religious Fanaticism)
1995	David Major, Bob's boss notes Bob's religious zeal, and said Bob put religion into most conversations	Scrupulosity (Religious Fanaticism)
1997	Earl Edwin Pitts, fellow counter Intel double agent is captured and implicates Bob.	Reported Insider Transgression
1999	Bob fantasizes about Katherine Zeta Jones in public.	Action out of Character

Figure 31. Hanssen's Career Stimuli (part 2)

4.4 Testing the Model

The objective of the test is for the model to show a clear difference between results generated from Hanssen's career (a known insider threat) and the results generated from the Typical Employee's "normal" career (not known for causing insider damage). The test methodology is as follows: Introduce stimuli from the Typical Employee into the

model and then introduce stimuli from Hanssen's career into the model for comparison. It is important that the stimuli are observable (as established above) and that the results are plotted on the same graph using the same time scale. The following three sections show the RPM outputs, including the score, the linear regression of the score and the change in scores versus time, but not the employees' Current Response Vectors, as they are simply used as inputs to the RPM when the next event occurs.

4.4.1 Typical Employee's Outputs.

The Typical Employee started with an Initial Score of 6, which rose to a peak score of 1063 and finished at a final score of 946, following the 53 stimuli (Figure 28 above) entered, one at a time over the course of 13 years, into the RPM (Figure 32).

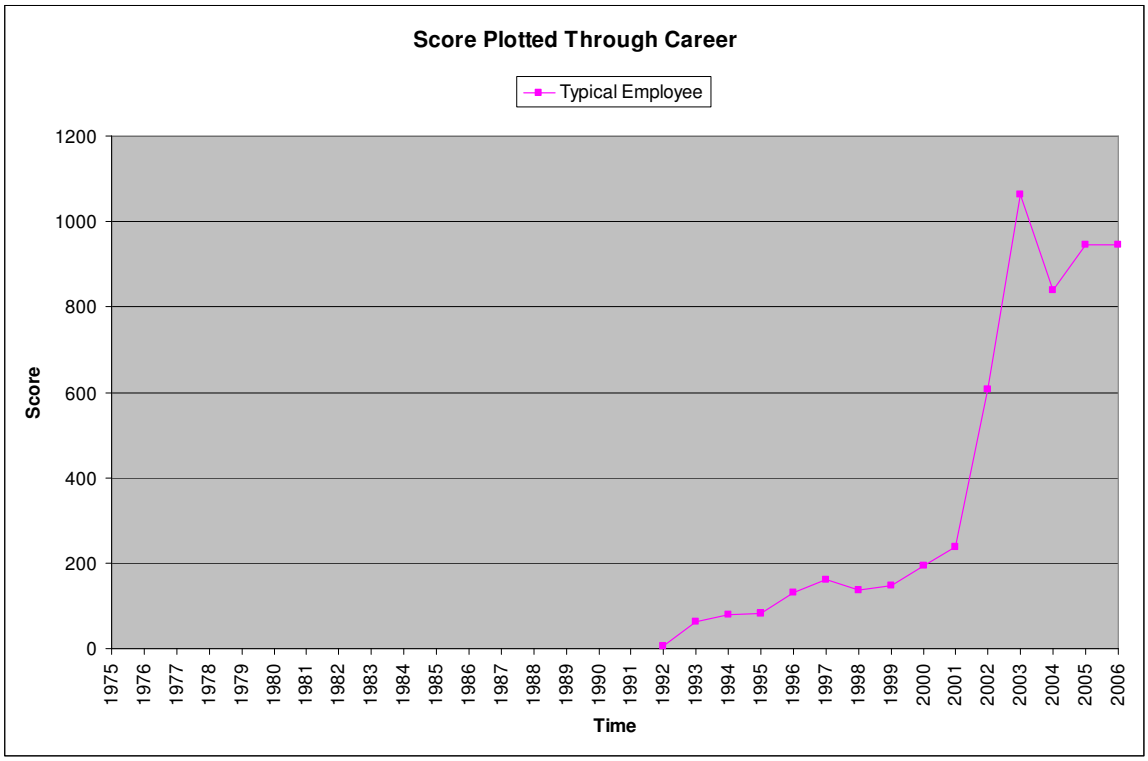

Figure 32. Typical Employee's Scores Plotted Through 13-year Career

Next, the linear regression of the employee's scores, show the kind of slope a Typical Employee generates, which represents the norm (Figure 33). The regression shows an overall slope of approximately 76.

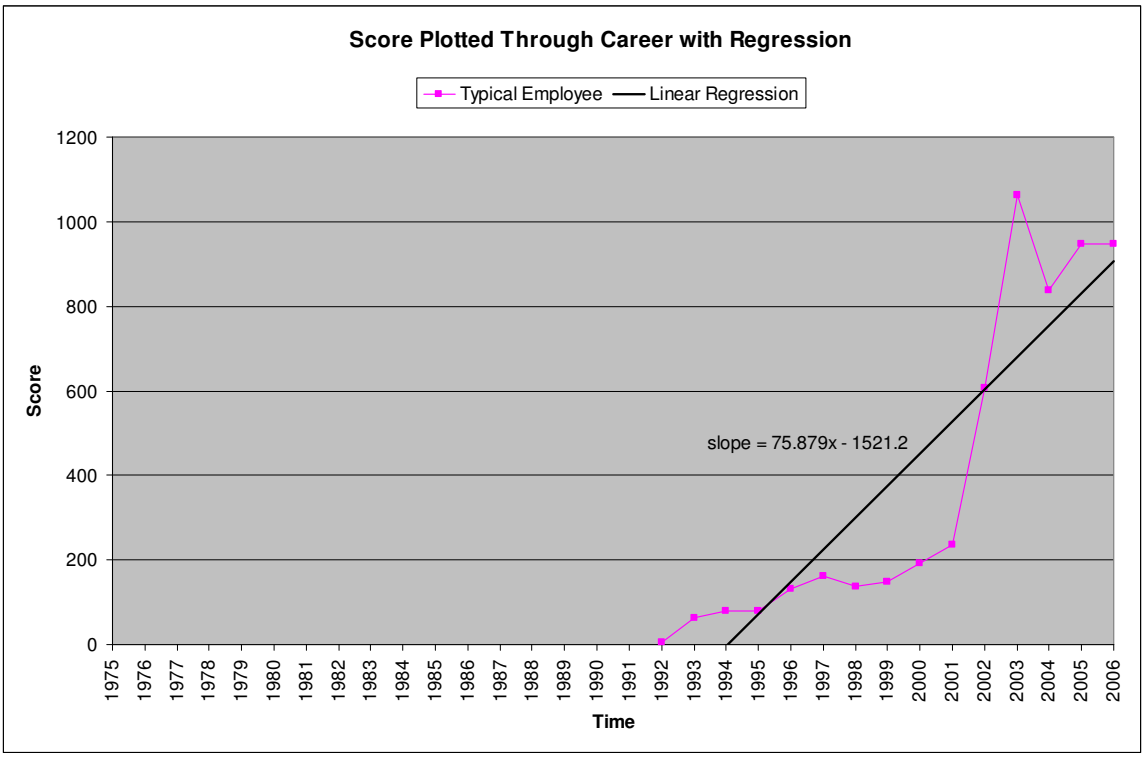

Figure 33. Linear Regression of Typical Employee's Scores

The third and final output is the Change in Scores Versus Time. This output is most useful because it shows the peaks and valleys of employee risk, significant, because a return to zero after a spike, or fluctuations near zero are indicative of normal behavior (Figure 34).

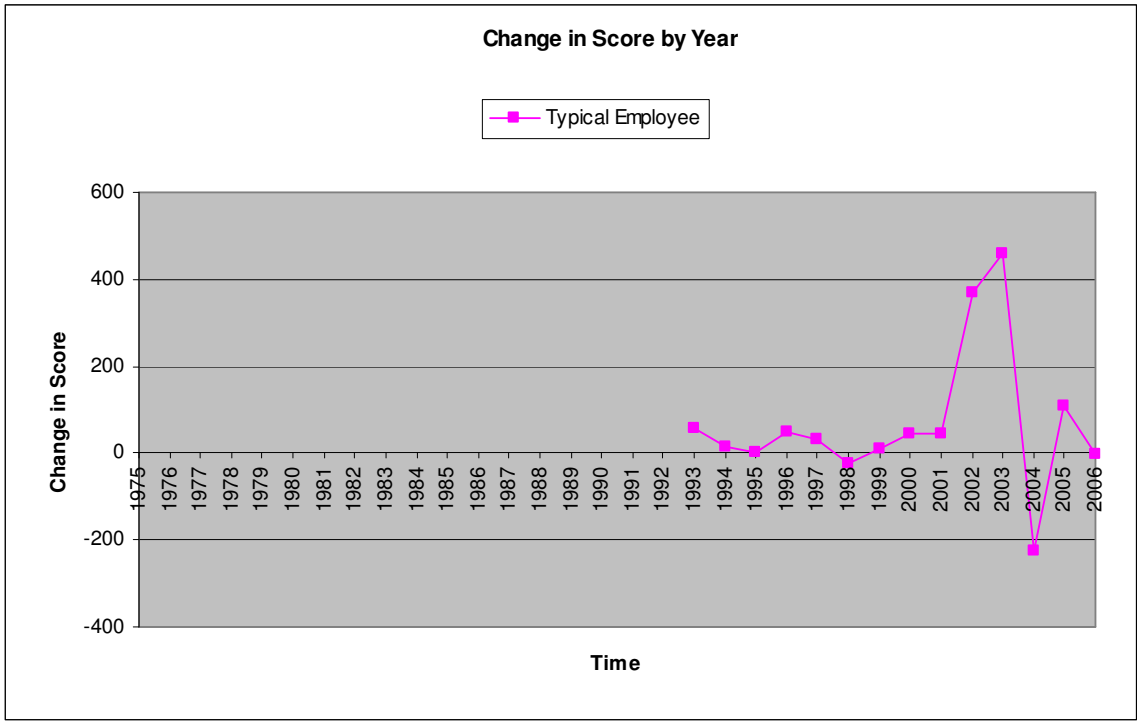

Figure 34. Change in Score Versus Time for Typical Employee (by Year)

The significance of this graph is three-fold. First, the change in scores versus time is obtainable over any size time window the organization desires. In this case, the time period chosen was one year because the data was entered by year, which serves as the smallest time unit available for this test. The figure displays the actual periods of time when the Typical Employee is at higher risk and when he or she is at lower risk. Second, because normal behavior tends to center around zero, as is the case for most of the Typical Employee's graph, it is easy to tell when employees severely deviate from the norm. Third, as everyone goes through rough times, depicted in the graph in 2002-2003, it is acceptable to see the change in scores increase during bad times, but eventually things

return to "normal", also depicted in the graph in 2004. These results alert security personnel to time periods when employees are at increased risk for causing insider damage.

Some organizations want the ability to perform trend analysis by increasing the period of time under scrutiny, creating a window, for example. For larger windows, the curve smoothes out as the size of the window increases (Figure 35).

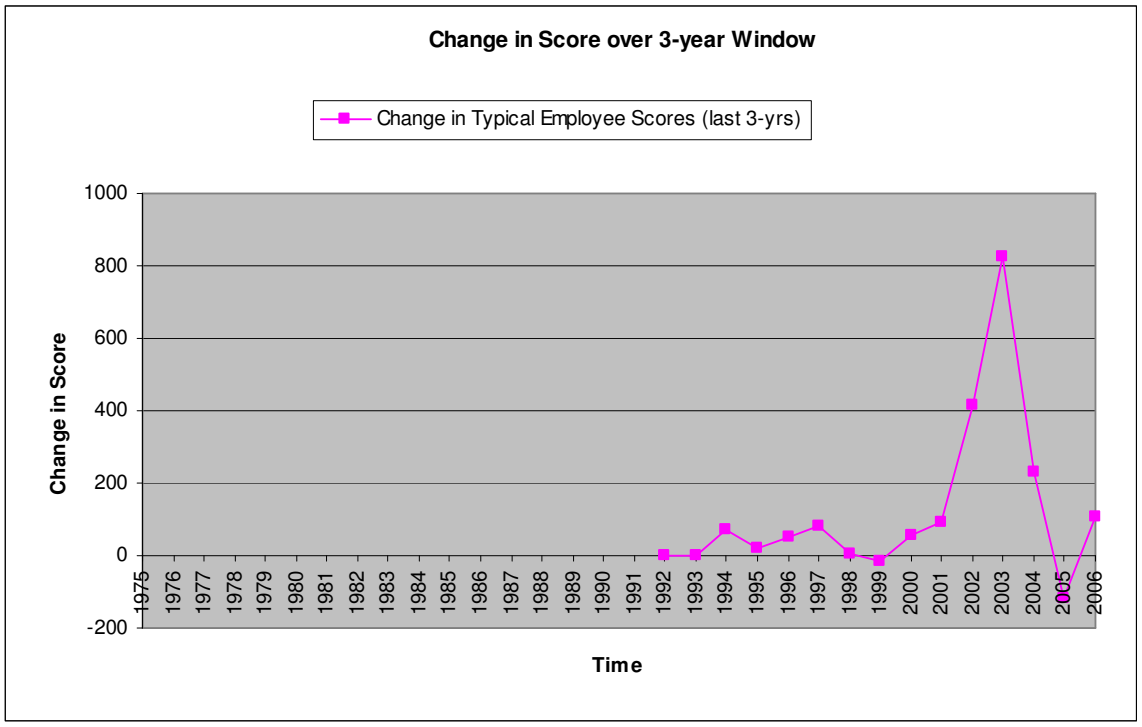

Figure 35. Change in Score Versus Time for Typical Employee (over 3 years)

In this case, the time window is 3 years long and examines periods of heightened risk more closely. For example, the jump in score between 2002 and 2003, shown in Figure 34 above, is not very significant, but when the events of 2003 are looked at in

conjunction with the events from 2002, as shown in Figure 35, a different story is told. Likewise, Figure 34 shows the employee as "recovered" from the events of the previous two years, but Figure 35 shows the trend in the 3-year window, where the employee still has a slightly elevated level of risk. Basically, memory has been added, which helps security personnel get around the tendency to look at current events in a vacuum, and compels them to consider events from recent years when evaluating the current situation.

4.4.2 Hanssen's Outputs.

Hanssen started with an Initial Score of 2, which rose to a peak of 7278 where it finished following the 46 stimuli (see Figures 30 and 31 above) entered, one at a time over the course of 25 years, into the RPM (Figure 36).

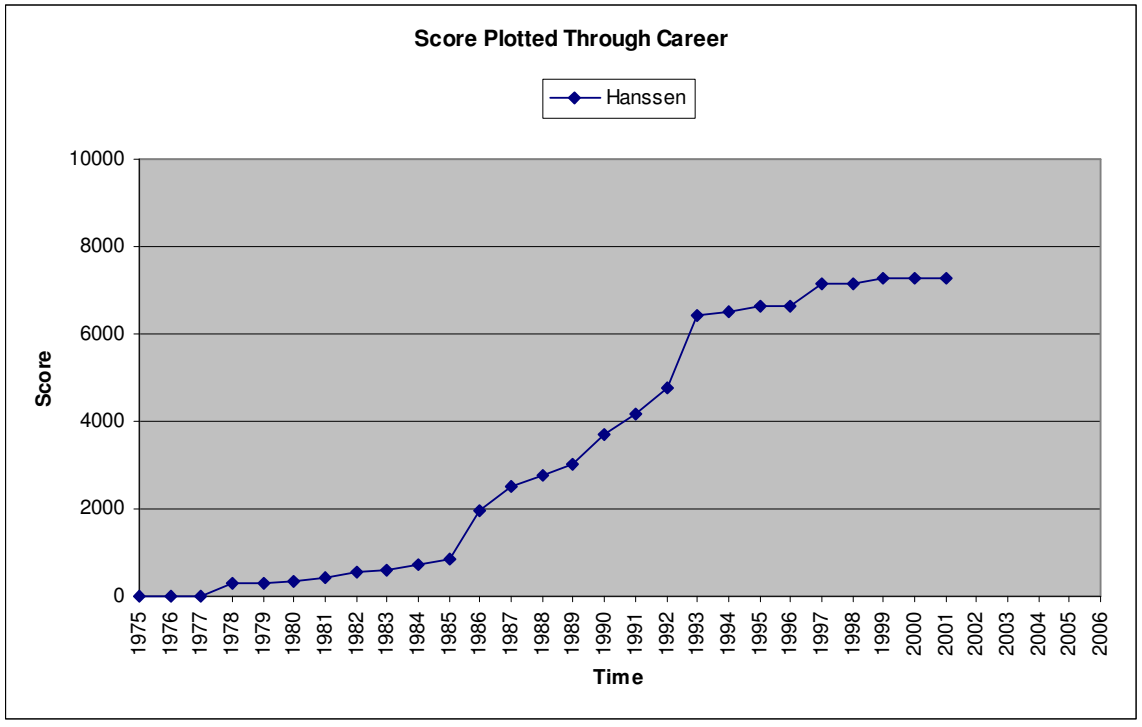

Figure 36. Hanssen's Scores Plotted Through 25-year Career

Shown next, is the linear regression of Hanssen's scores (Figure 37), which shows a much higher slope than seen in the Typical Employee's scores (Figure 33 above). The regression shows an overall slope of approximately 355.

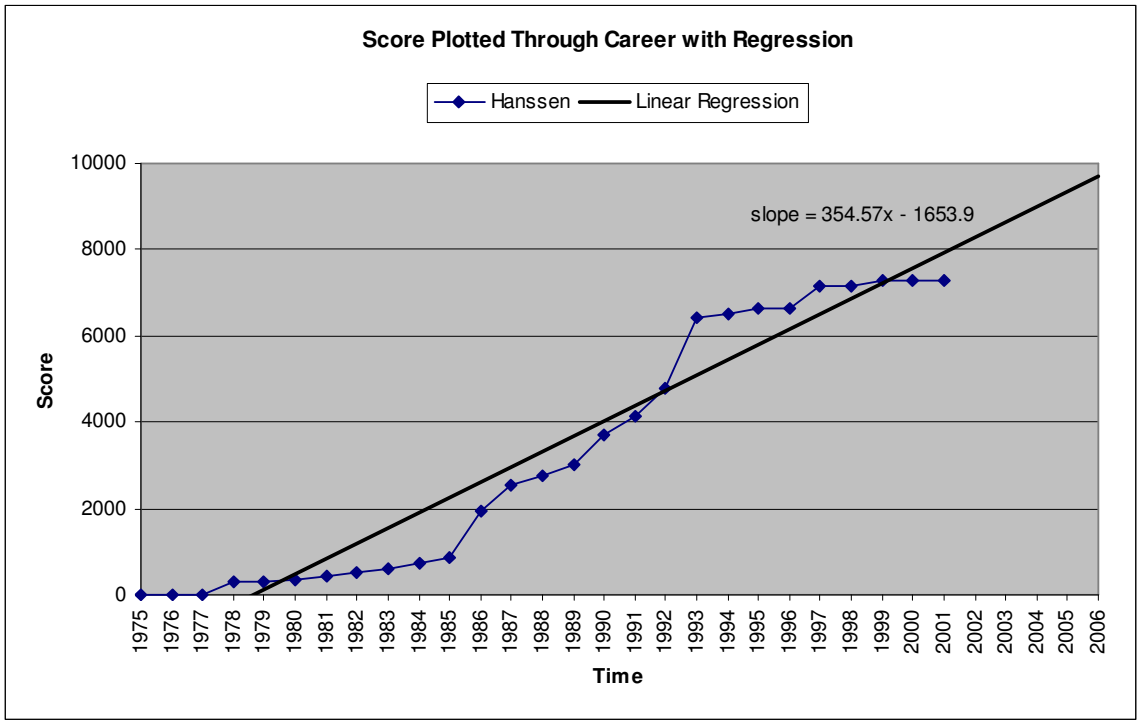

Figure 37. Linear Regression of Hanssen's Scores

The Change in Scores Versus Time output really identifies Hanssen as a high-risk employee (Figure 38). The time period here is one year, because it is the smallest time unit available for the test, but the graph shows huge spikes indicating extreme risk to the organization. Unlike the Typical Employee, Hanssen rarely returns to zero, in some cases spiking to even higher risk levels before completely returning to a lower risk status.

Hanssen's graph does not tend to center around zero, but rather floats around 100 when not injecting large spikes into the curve.

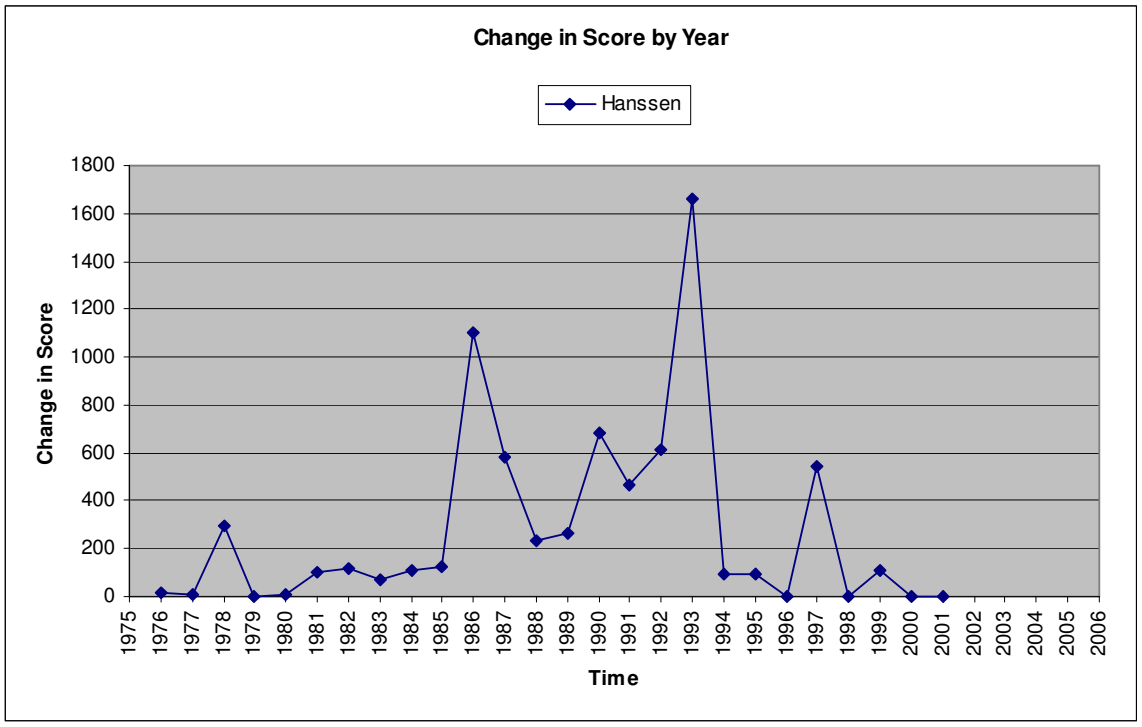

Figure 38. Change in Score Versus Time for Hanssen (by Year)

Performing a trend analysis on the change in Hanssen's scores over a 3-year window produces similar results with slightly smoothed edges (Figure 39). As with the 3-year window for the Typical Employee, the 3-year time period smoothes out Hanssen's risk levels, but amplifies the level of risk to the organization he poses, exhibited by the large change in scale on the y-axis of the graph. Clearly, with outputs such as this, security personnel are able to take the appropriate measures to mitigate possible insider damage caused by an employee with an elevated risk for causing insider damage.

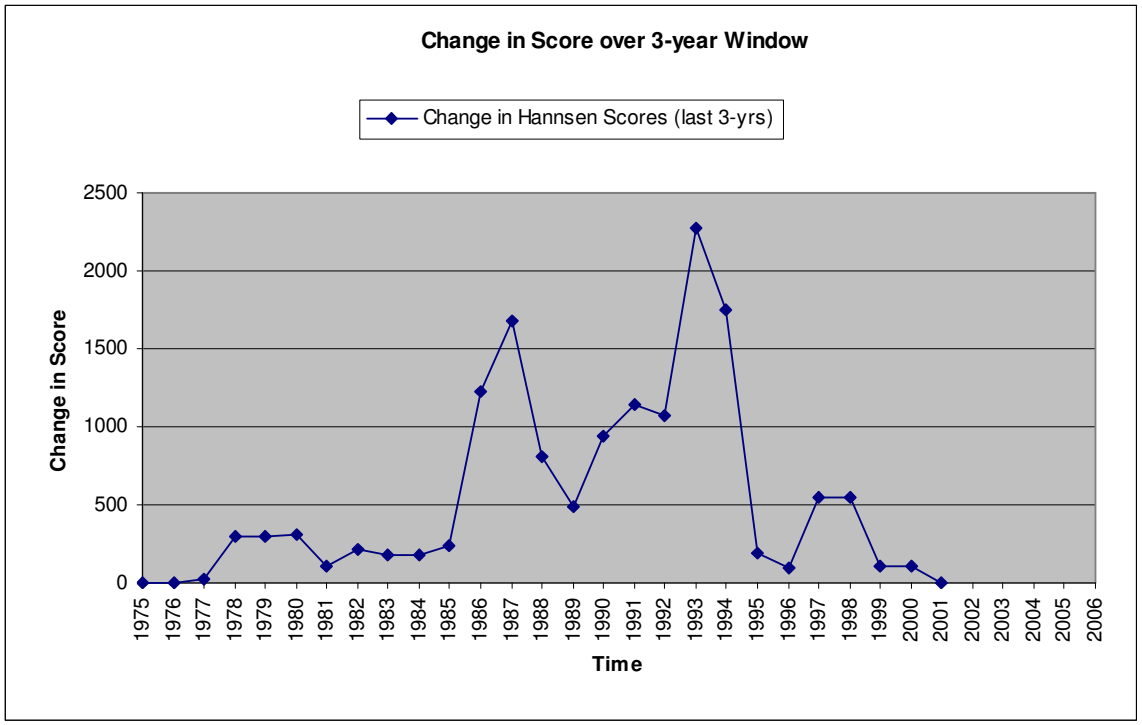

Figure 39. Change in Score Versus Time for Hanssen (over 3 years)

4.4.3 Result Comparisons.

Hanssen's score is roughly seven times the Typical Employee's score, a telling figure by itself, but there are some troublesome variables, such as the fact that Hanssen's scores cover a career nearly double the length of the Typical Employee's career. Expecting the score to double because the career length is double is reasonable, but multiplying it by a factor of seven is not. Never the less, examining the scores together graphically is beneficial, as long as comparisons are made on the same scale (Figure 40). This graph shows a clear difference in magnitude between the Hanssen scores and the Typical Employee scores, and organizations that wish to set thresholds are able to see how easy it is to detect scores that exceed them. So the first RPM output has shown a

significant increase in risk in one employee when compared to the other; enough of a difference between the malicious insider and the normal insider to warrant an extra look by security personnel.

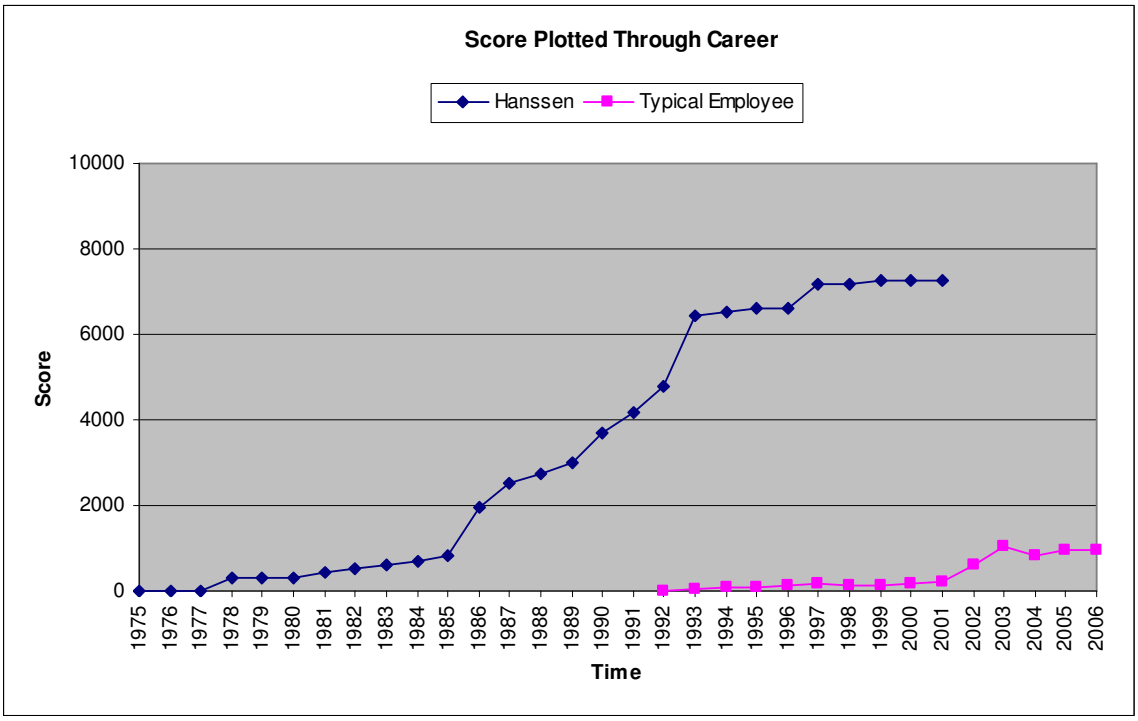

Figure 40. Both Employees' Scores Plotted on the Same Scale

The next metric available for comparison is the linear regression of the scores for both employees. Again, it is obvious that the Hanssen slope of 355 is larger than the Typical Employee's slope of 76, by a factor of 4. However, looking at the separate graphs is misleading, as the linear regression of the Typical Employee's scores looks much steeper than that of the Hanssen scores (see Figures 33 and 37 above). This is due to the

difference in the scales, and is alleviated by plotting both sets of scores on the same graph (as in Figure 40) and then finding the linear regression of each (Figure 41).

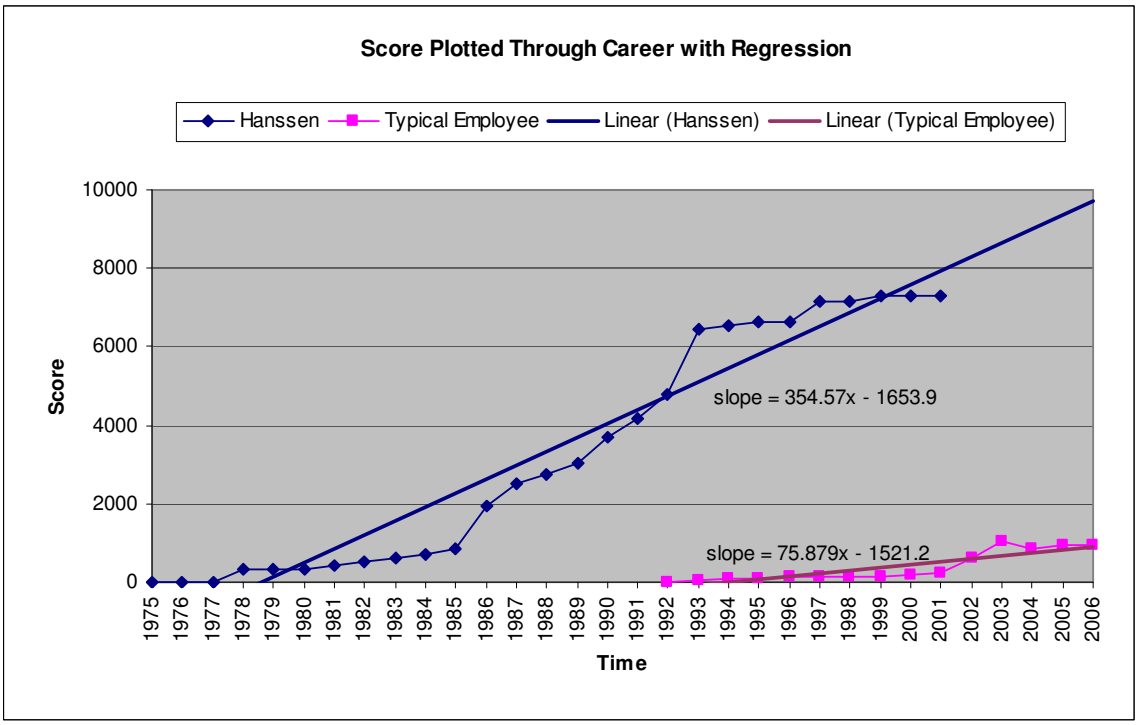

Figure 41. Linear Regression of Both Employees' Scores Plotted on the Same Scale

Now, not only does the output make the difference in slopes numerically apparent, but also makes it graphically obvious. No longer is the Typical Employee's slope steeper than Hanssen's slope, and there is actually a quite visible degree of difference between the lines. This result is useful for organizations interested in establishing the Typical Employee's slope as the norm before looking for angles of. The second output of the RPM has successfully displayed a useful metric for security personnel to use to identify employees with increased risk of causing insider damage.

As mentioned in Chapter III, another method of using the linear regression of scores is to compare the rise in slopes throughout the employee's career and compare to an established norm. For example, if an organization were to use the Typical Employee's linear regression of scores as the norm, and then track an employee's score regression annually, it might prove useful (Figure 42). Additionally, by plotting the scores annually (in different colors), it is easier to see the slopes by year as well.

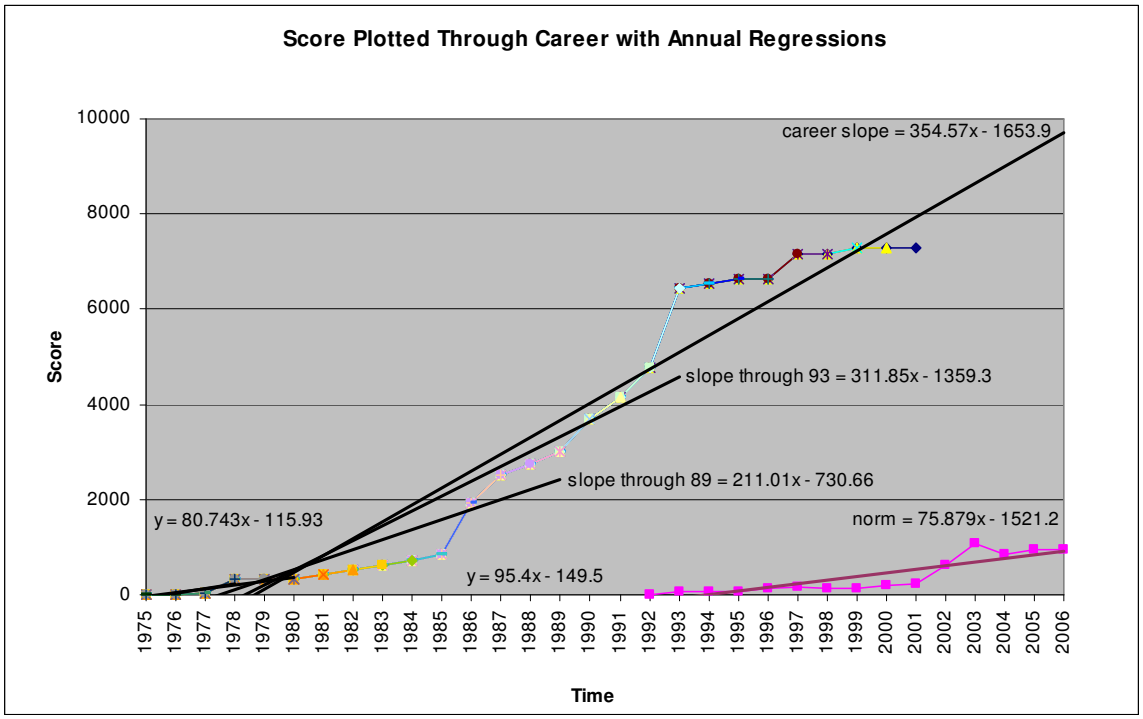

Figure 42. Linear Regression of Hanssen Scores at Various Points in His Career

Looking at this graph, the organization begins to see a trend, where by 1986, Hanssen's slope is nearly 50 points higher than the norm, and even earlier (not shown here), by 1980, very early in Hanssen's spying career, the slope has surpassed the norm by

ten points. This is significant because the primary goal of the RPM is to identify employees with heightened risk for causing insider damage, but it is also useful in predicting heightened risk early, potentially reducing the amount of damage an insider inflicts.

As with the previous outputs, more information is gained about employee risk levels and their potential for causing insider damage from a comparison of employees against the Typical Employee. In addition, as with previous outputs, the Change in Score Versus Time metric proves most useful when plotting both employees on the same scale (Figure 43).

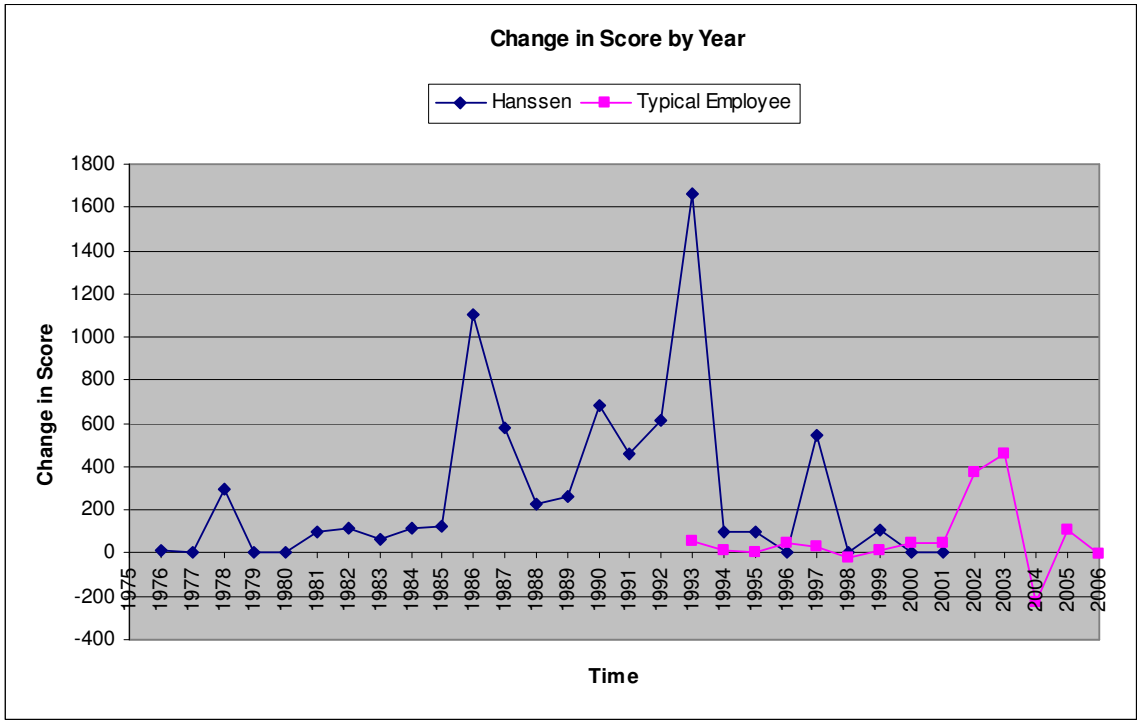

Figure 43. Change in Score Versus Time for Both Employees (by Year)

This graph shows that all but one of Hanssen's large spikes in risk are larger than the largest spike found on the Typical Employee's graph. Additionally, it is clear that most of Hanssen's graph sits well above the majority of the Typical Employee's graph. In other words, for a vast majority of the time, Hanssen's scores are increasing more than the Typical Employee's score increase. This certainly indicates the increased risk Hanssen poses over the norm, not to mention the indicator exposed by the large spikes on the Hanssen graph that dwarf the largest spike in the normal graph.

Unlike with the separate 3-year window graphs of the employees, security personnel are better able to leverage the quality of information gained by a 3-year window graph of both employees on the same scale (Figure 44).

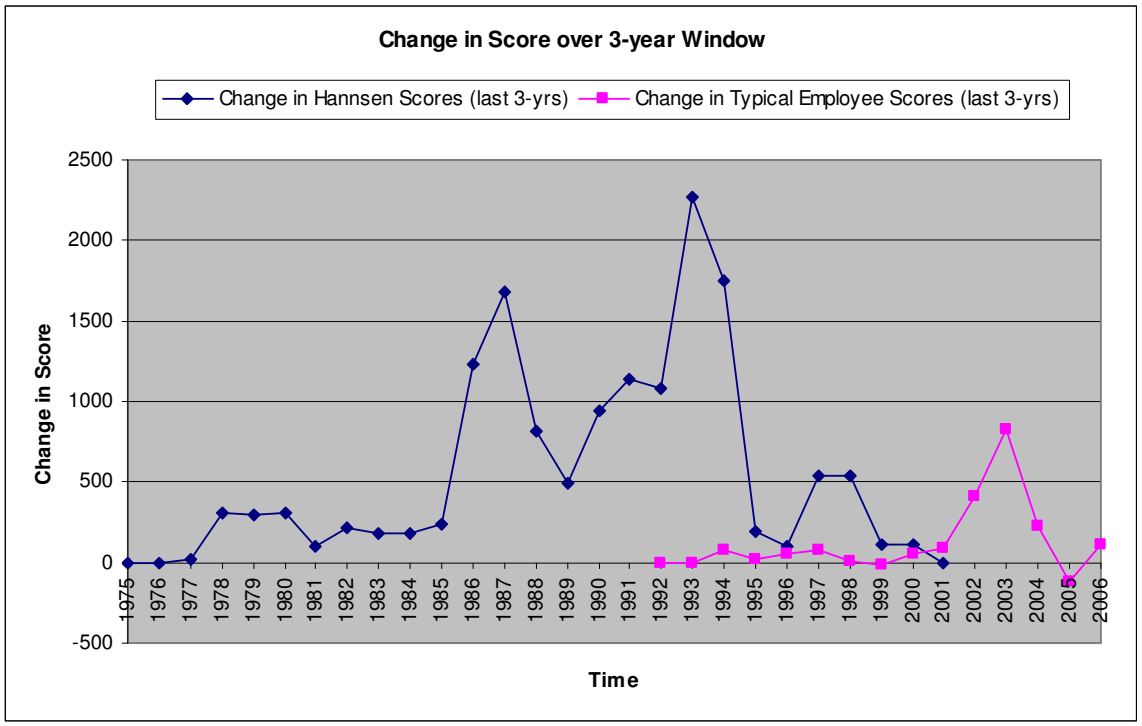

Figure 44. Change in Score Versus Time for Both Employees (over 3 years)

This graph magnifies the extent to which Hanssen's scores are not only higher than the Typical Employee's scores, but also are increasing at a faster rate. Now, if security personnel consider events from the previous three years, when analyzing Hanssen's risk, they observe his score increase by about 250 to 300 points in 3-year windows during inactive years and anywhere between 500 and 2000 points in 3-year windows during active years. When compared with the norm of roughly zero points in 3-year windows during inactive years and anywhere between 250 and 750 points in 3-year windows during active years, it is clear that the RPM is capable of differentiating between a normal insider and a malicious one.

4.4.4 Sensitivity Testing.

Completing model sensitivity testing is necessary before the model is certified as working. It is important to know how small changes in the static matrices affect the output scores, slopes, and changes in scores verses time.

C-code was written to randomly change one value in either matrix. After selecting an employee to use during the test, the program evaluates the employee with the model, changes one of the matrices, and then re-evaluates the employee with the model. Both sets of scores were compared to see how a small change in the matrix affected scores, and various affects were expected. For example, if the change to the matrix occurs in a place where the influence or event does not have effect over the employee, no change is expected. Second, if a change in one of the matrices occurs in a place where the influence or event is heavily in force in the employee's calculations, a larger change is expected. Third, if the matrix change only minimally affects the mathematics, then a small amount

of change is expected. As a result, various amounts of change are expected, which makes watching for change a bad metric to measure the sensitivity of the RPM. Conversely, the major purpose of the model is to differentiate between malicious and non-malicious insiders, so the obvious metric to look at here is the ability of the model to differentiate between the two, given a small amount of change in one of the matrices.

The C-program is used to change one of the matrices and re-evaluate one of the employees (either Hanssen or the Typical Employee) with the RPM. The other employee remains unaffected and is compared to the changed employee to see if the model still differentiates between the two after one of the matrices has been changed. Either matrix is available for testing, using any employee and any amount of change, even large amounts. If the influence matrix is selected, the program randomly selects 1 of 30 rows and 1 of 30 columns to pinpoint the exact cell to modify by the amount of change selected. If the event matrix is chosen, the program randomly selects 1 of 27 rows and 1 of 30 columns to pinpoint the exact cell to modify by the amount of change. Once the cell is modified, the matrix is used as an input to the model along with the other matrix and the chosen employee's vectors. The output is compared to the original output, using the Change in Scores Versus Time metric. 320 separate tests were simulated with the following distribution (Figure 45).

Static Employee	Matrix	Change Injected	# of Tests Perfromed
Typical Employee	Event	1	10
Typical Employee	Event	2	10
Typical Employee	Event	5	10
Typical Employee	Event	15	10
Typical Employee	Event	-1	10
Typical Employee	Event	-2	10
Typical Employee	Event	-5	10
Typical Employee	Event	-15	10
Typical Employee	Influence	1	10
Typical Employee	Influence	2	10
Typical Employee	Influence	5	10
Typical Employee	Influence	15	10
Typical Employee	Influence	-1	10
Typical Employee	Influence	-2	10
Typical Employee	Influence	-5	10
Typical Employee	Influence	-15	10
Hanssen	Event	1	10
Hanssen	Event	2	10
Hanssen	Event	5	10
Hanssen	Event	15	10
Hanssen	Event	-1	10
Hanssen	Event	-2	10
Hanssen	Event	-5	10
Hanssen	Event	-15	10
Hanssen	Influence	1	10
Hanssen	Influence	2	10
Hanssen	Influence	5	10
Hanssen	Influence	15	10
Hanssen	Influence	-1	10
Hanssen	Influence	-2	10
Hanssen	Influence	-5	10
Hanssen	Influence	-15	10
Total # of Tests Performed			**320**

Figure 45. Current Distribution of Sensitivity Tests Performed

Many of the tests resulted in scores changing, but none of the Changes in Score Versus Time graphs changed remarkably. Changes to the Influence Matrix were clearly more noticeable, because more influences are used in the calculations than events, due to most of the events being turned off. A random injection of change to an event that is not

used (or unused influence, for that matter, which is less likely) does not result in a change in the overall score during the test. Most importantly, in every case, there was still a clear differentiation between the Hanssen graph and the Typical Employee graph. None of the tests presented a situation where the differences between the graphs became ambiguous.

The result of the sensitivity testing is significant because it shows that the Risk Predictor Model is robust, with changes even as high as fifteen (several times larger than the largest matrix value) resulting in minimal change to the overall appearance of the Change in Scores Versus Time graphs.

4.5 Summary

This chapter detailed all the steps necessary to populate, test, and analyze the results of the Risk Predictor Model, to include an in-depth case study of notorious FBI double agent Robert Hanssen. Beginning with the Adjudicative Guidelines used by all US government agencies to grant employees security clearances, continuing with a description of how the model was populated for the test, an explanation of the Typical Employee, and a look at the Hanssen case study, the model was primed for testing. Following the test, an analysis of the model outputs was discussed, along with the significance of each output observed. Chapter V begins with a discussion on the relevance of this research, looks at the importance of the outputs observed, and looks ahead to the future.

V. Conclusions

This chapter wraps up the discussion of the Risk Predictor Model. Chapter IV showed the model's capabilities and the success to which it was capable of assisting the fight against insider threat. This chapter discusses the relevance of the model and its outputs, as well as possible future work and a brief conclusion to this research.

5.1 Relevance of the Model

The model addresses two of the three DoD 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 vulnerability and threat on the DoD risk model (see Figure 8 above). By focusing on the area of highest concern by determining which employees pose the greatest threat to the organization, the model reduces the overlap between vulnerability and threat in the risk model.

It also addresses four of the DoD's six key elements to minimizing the impact of insider threat; establish trustworthiness (of employees), strengthen security practices (by providing security personnel with a new tool and a bit more deterrence), detect problems (by establishing employees' risk potentials), and react/respond (by flagging high-risk employees). 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.

For the DoD, "the objective is to minimize the impact of the insider threat and to minimize the potential damage to DoD information or inflicted on DoD information and information systems by significantly reducing information system vulnerabilities to a wide range of misuse and abuse." [3] The objective is not to totally prevent the insider threat, because the problem is too big and requires much more research. Instead, the DoD has implemented activities designed to combat insider threat while technology is being developed. *Vigilance Now* [3] focuses on security awareness, prevention, and deterrence. With DoD emphasis on individual accountability using personnel policies 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" [3], insiders are typically caught only after causing significant damage. Even by improving deterrence visibly, the DoD recognizes the need for more effective "methods and tools that improve deterrence" [3]. The Risk Predictor Model augments all of these activities, first by strengthening personnel policies, then by

pre-loading data mining activities with data regarding individual employee risk levels and finally by serving as an effective method of deterrence.

The Risk Predictor Model also clearly fits the DoD's second activity, *Vigilance Looking Forward from a Strong Foundation* [3], which 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. Although The Risk Predictor Model is classified as IT and certainly not a solution to insider threat, it clearly heightens security awareness by identifying the personnel within an organization that have increased risk of causing insider damage. Likewise, in establishing personnel security practices, the DoD states "mitigating the insider threat begins with personnel selection and determination of suitability for service." [3] Basically, the DoD expects certain behaviors from insiders, right from the beginning. The Risk Predictor Model, populated using the 13 Adjudicative Guidelines for Determining Eligibility for Access to Classified Information, has the potential to continue to screen personnel throughout their careers on a continual basis just as if they were submitting their initial security clearances. Additionally, the DoD wishes to use IT to continue "coordinated, collaborative research and development efforts needed to improve authentication, prevention, detection and monitoring" while maintaining "empirical information on insider misuse, abuse and maliciousness to evaluate the character and significance of insider misuse, abuse and malicious activity." [3] The Risk Predictor Model exactly satisfies this mantra. Finally, the DoD wishes to focus on

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." [3] Implementation of the Risk Predictor Model dovetails nicely with this last DoD endeavor. 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 it fullest potential.

5.2 Reflections on the Data Obtained

The model successfully produced outputs that showed the difference between employee total scores, the divergence of slopes between a known insider (Hanssen) and a "typical" employee, and most convincingly, the difference between the change in scores versus time of malicious and non-malicious employees. Additionally, the model is robust, capable of handling large changes in the static matrices with expected change, but relatively minimal change to overall employee profiles. If implemented, the Risk Predictor 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. Finally, the indicators produced by the model show potential risk employees pose to becoming an insider, but

when coupled with other indicators generated by other models and research, security personnel are able to act earlier because the RPM provides them with an indicator of potential risk. In other words, one or two indicators from other sources are not enough for security personnel to take action under normal circumstances, but armed with predictions of which employees have high risk for causing damage, security personnel are prompted into action.

5.3 Future Work

The Risk Predictor Model uses human behavior concepts to mitigate insider threat by predicting which employees are higher risk for becoming malicious insiders. There is little research in this area and the model serves as a stepping-stone into further research involving human influences and modeling.

As identified in Chapters III and IV, population of the model is left to organization subject matter experts, hopefully with human behavior experience. However, further research done by those with human behavior experience to make the task of populating the model easier and more accurate is necessary. Finding a way to populate the influence and event matrices in such a way as to avoid possibly inaccurate results makes the model more useable. For example, an organization that decides employees who are late for work more than twice are an extremely high risk for insider damage, but conversely chooses to ignore employees who attempt to access unauthorized information invariably shows tardy employees as high risk. This is the "garbage in, garbage out" principle, but there is inherent danger in this area. The example used here is

extreme, but organizations struggle with how to populate their matrices. Further research done in the area of human behavior helps alleviate this problem.

On a more fundamental level, the RPM has only been tested on small examples and the one rigorous case study described in Chapter IV. Due to the success the model has shown in this research, it has potential use by many organizations, however, populating the model using a completely different case study is desirable to ensure similar results.

Finally, the purpose of this research was to show the need for and present a model useful to security personnel in mitigating insider threat. A good tool or computer software program designed to implement the Risk Predictor Model would significantly improve the possibility that the power of the model ends up in the hands of security professionals who need it.

5.4 Conclusion

Nothing replaces the relationship good supervisors have with their subordinates, however, even good supervisors tend to tackle crises in a vacuum. They help their employees through the current problem as best they can, often without considering crises from the past. A model that tracks these crises over time greatly benefits any organization, by bringing a big picture view of the potential danger an employee poses based on heightened risk.

The goals of this research were to establish the need for a human behavior model, propose a model, and test it, all with the expectations that it mitigate insider threat. This research has met each of these goals. The insider threat problem is a people problem, for

it is people who perpetuate the crimes. The better human behavior is understood, the better organizations are capable of mitigating the problem. The Risk Predictor Model proposed is built on a foundation of human behavior studies. Using influences that affect people, rather than tracking emails or logins, gets right to the core of the trouble; human nature. Finally, the model was rigorously tested using a known perpetrator of insider damage and was successful in clearly differentiating between a known malicious insider and a non-threat. As a result, the Risk Predictor Model presented in this research adds to the various tools security personnel use to mitigate insider threat.

Appendix A: Sample Populated Influence Matrix

Influence	stress	Criminal record	Self Esteem	Use of legal substances	Use of Narcotics/ Addictions	S/TS clearance	High profile job	Satisfaction with company/organization	Expectations for advancements (promotion/pay raise)	job security/stability	Workload, Quantity/ability to meet deadlines	Amount of and ability to deal with complex technology	Experience required for job	community involvement	Relationship with family	Social commitments	Illicit relationships	Religious practices	Satisfaction with salary	family financial stability/security	Relationship with Co-workers	desire to cover for inadequacies	Greed	Feeling of invincibility - can't get caught	Name recognition	Experienced rejection	Opportunity (lack of Organized Defense)	Satisfaction with country/politics	State of the Economy	concern for world condition
Stress	0	0	1	1	1	0	0	1	0	0	0	1	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	1
Have Criminal record	1	0	0	0	0	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	0	0	0
Self Esteem	1	0	0	1	1	0	0	0	1	0	1	1	0	1	1	1	1	0	0	0	1	1	0	0	0	1	0	0	0	0
Use of legal substances (Caffeine, Nicotine, Social drinking)	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0
Use of Narcotics/Addictions (alcoholism, gambling)	1	1	1	1	0	1	1	0	1	1	1	1	0	1	1	1	1	1	0	1	1	1	0	1	0	1	0	1	0	0
S/TS clearance	1	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	1	0	1	1	0	1	0	0	0
High profile job	1	0	0	0	0	0	0	0	0	1	1	0	0	1	0	0	1	0	0	0	0	1	0	1	1	0	1	0	0	0
Satisfaction with company/organization	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0
Expectations for advancements (promotion/pay raise)	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	1	1	1	0	1	1	0	0	1	0
job security/stability	1	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	1	1	1	0	-1	1	1	-1	0	0	0
workload, quantity/ability to meet deadlines	1	0	1	1	0	0	0	1	1	1	0	0	0	1	1	1	1	1	1	0	1	1	0	0	0	1	0	0	0	0
Amount of and ability to deal with complex technology	1	0	1	0	0	0	0	1	1	1	1	0	1	0	0	0	0	0	0	1	0	1	1	0	-1	-1	1	-1	0	0
Experience required for job	0	0	1	0	0	0	0	1	1	1	1	1	0	0	0	0	0	0	0	1	0	1	1	0	-1	-1	1	-1	0	0
Community involvement	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Relationship with family	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
social commitments (relationship w/friends or foreign influence)	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
Involved in illicit/illegal relationships	1	1	0	0	0	1	1	0	0	0	1	0	0	1	1	1	0	1	0	1	0	1	0	1	0	0	1	0	0	0
Religious practices	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	0	1	0	0	0	1	0
Satisfaction with salary	1	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	1	0	0	1	0	1	1	0	0	0	0	0	1	0
family financial stability/security (debt, savings, retirement, etc.)	1	0	1	1	0	1	0	0	0	0	0	0	0	1	1	1	1	0	1	0	0	1	1	0	0	1	0	1	1	1
Relationship with Co-workers	1	0	1	0	0	0	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
desire to cover for inadequacies	0	1	0	1	0	1	1	0	1	1	0	1	0	0	0	0	1	1	0	0	1	0	0	1	1	0	0	0	0	0
Greed	0	1	0	0	0	1	1	0	0	0	0	0	0	0	0	0	1	0	1	0	1	0	0	0	1	0	0	0	0	0
Feeling of invincibility - can't get caught	0	1	0	1	1	1	1	0	0	1	0	0	0	0	0	0	1	0	0	0	1	0	1	0	1	0	1	0	0	0
Name recognition (narcissism)	1	1	1	0	0	1	1	0	1	1	0	1	0	1	0	0	1	1	0	0	1	1	1	1	0	1	1	0	0	0
Experienced rejection	1	0	1	1	1	0	1	1	1	1	1	0	0	0	0	0	1	0	0	1	1	1	0	0	0	0	0	0	0	0
Opportunity (lack of Organized Defense)	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	1	1	0	0	0	0	0
Satisfaction with country/politics (patriotism)	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	1	1
State of the Economy	1	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	1	0	0
concern for world condition (foreign preference)	1	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	1	0	0

Appendix B: Sample Populated Event Matrix

Event	stress	Criminal record	Self esteem	Use of legal substances	Use of Narcotics/Addictions	S/TS clearance	High profile job	Satisfaction with organization	Expectations for advancements	job security/stability	workload	Complex technology	Experience required for job	community involvement	Relationship with family	Social commitments	Illicit relationships	Religious practices	Satisfaction with salary	family financial stability/security	Relationship with Co-workers	desire to cover for inadequacies	Greed	Feeling of invincibility - can't get caught	Name recognition	Experienced rejection	Opportunity (lack of Organized Defense)	satisfaction with country/politics (patriotism)	State of the Economy	concern of world condition
Alarming Statement	2	2	0	0	0	2	2	2	0	2	0	0	0	0	0	0	2	0	2	2	0	2	2	2	2	0	2	0	2	0
Reported insider transgression	4	4	4	0	0	4	4	4	4	4	-4	0	0	0	4	4	4	0	4	4	4	4	0	-4	4	4	-4	0	4	4
Action out of Character	0	0	2	2	2	0	0	0	0	0	-2	0	0	0	0	0	2	0	0	0	2	2	0	0	0	0	0	0	0	0
Salary anomaly	1	0	1	0	0	0	0	1	0	-1	1	0	0	0	0	0	0	0	1	1	0	0	1	0	0	0	0	0	1	0
Excessive Interest	2	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	2	0	0	2	0	2	0	0	0
Scrupulosity (Religious Fanaticism)	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	1	0	0	1	1	0	1	1	1	0	1	0	1
Personality Quirk	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	1	0	0	0	0
Unexplained affluence	0	3	0	0	0	3	3	3	3	0	0	0	0	-3	0	0	3	0	3	-3	0	3	3	3	0	0	3	0	3	0
Legal Activity (Minor)	0	0	1	1	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	1	0	1	0	0	0	1	0	0	0	0
Legal Activity (Moderate)	2	2	2	2	0	2	2	0	2	2	0	0	0	2	2	2	2	0	0	2	2	2	0	-2	0	2	0	2	0	0
Legal Activity (Major)	3	3	3	3	0	3	3	0	3	3	0	0	0	3	3	3	3	0	0	3	3	3	0	-3	0	3	0	3	0	3
Reprimanded	2	0	2	2	0	2	2	2	2	2	0	0	0	0	0	0	0	0	0	0	2	2	0	-2	2	2	0	0	0	0
Increased Absenteeism/Tardiness	1	0	0	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	1	1	0	0	0	1	0	0	0	0
Change in Mental Health (positive)	-2	0	-2	-2	-2	-2	-2	0	-2	-2	-2	0	0	-2	-2	-2	0	0	0	-2	-2	0	0	0	0	0	0	0	0	0
Change in Mental Health (negative)	2	0	2	2	2	2	2	0	2	2	2	0	0	2	2	2	0	0	0	2	2	2	0	0	0	2	0	0	0	2
Change in Physical Health (positive)	-2	0	-2	-2	-2	0	0	0	0	-2	-2	0	0	-2	0	0	0	0	0	-2	-2	0	0	0	0	0	0	0	0	0
Change in Physical Health (negative)	2	0	2	2	2	0	0	0	0	2	2	0	0	2	0	0	0	0	0	2	2	2	0	0	0	2	0	0	0	2
Change in work environment (positive)	1	0	-1	0	0	0	0	-1	0	-1	1	1	1	0	0	0	0	0	-1	-1	1	0	0	0	-1	0	0	0	0	0
Change in work environment (negative)	1	0	1	1	0	1	1	1	1	1	1	1	1	1	1	1	0	0	1	1	1	1	0	0	0	1	0	0	1	0
Recently fired	2	2	2	2	2	2	2	2	2	2	-2	0	0	2	0	0	2	0	2	2	2	2	0	0	0	2	2	0	2	0
Recently retired/quit	2	0	0	0	0	2	0	0	0	0	-2	0	0	-2	-2	-2	0	0	0	2	0	0	0	0	0	0	2	0	0	-2
Catastrophic event	3	0	3	3	3	0	0	0	0	0	0	0	0	0	0	0	0	-3	0	3	0	3	0	0	0	0	0	3	0	3
Change in family status (positive)	2	0	-2	0	0	0	0	0	0	0	0	0	0	0	-2	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0
Change in family status (negative)	2	0	2	2	2	0	0	0	0	0	0	0	0	2	2	2	0	-2	0	2	0	2	0	0	0	2	0	0	0	2
Financial impact	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0	0	2	0
Foreign interaction	2	0	0	0	0	2	0	0	0	0	0	0	0	2	2	2	2	0	0	0	0	0	0	0	0	0	0	2	0	2
Hostile environment	3	0	0	0	0	3	3	3	0	0	0	0	0	3	3	3	0	0	3	0	0	0	0	0	0	0	0	3	0	3

Bibliography

1. *Webster Comprehensive Dictionary International Edition*. Vol. 2. 1995, Chicago: Ferguson Publishing Co.

2. *Webster Comprehensive Dictionary International Edition*. Vol. 1. 1995, Chicago: Ferguson Publishing Co.

3. *Final Report of the Insider Threat Integrated Process Team*. 2000, Department of Defense.

4. *Insider Threat Study*. 2006, National Threat Assessment Center.

5. Mills, R.F., *CSCE 525 - Introduction to Information Warfare*. Fall Quarter 2004, Air Force Institute of Technology, Wright Patterson AFB, OH.

6. Shulyupin, C. *Human behavior*. 2004 [cited; Available from: http://en.wikipedia.org/wiki/Human_behavior.

7. *Influence*. 2006 [cited; Available from: http://en.wikipedia.org/wiki/Influence.

8. *Model*. 2006 [cited; Available from: http://en.wikipedia.org/wiki/Model.

9. *Model (abstract)*. 2004 [cited; Available from: http://en.wikipedia.org/wiki/Model_%28abstract%29.

10. *Profiler-2000: Attacking the Insider Threat*. 2000, AFRL/IF and Carnegie Mellon University

11. Marisa Reddy Randazzo, P.D., Dawn M. Cappelli, Michelle M. Keeney, Ph.D., Andrew P. Moore, Eileen F. Kowalski, *Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector*. 2004, U.S. Secret Service and CERT Coordination Center: Washing DC and Pittsburg, PA.

12. *AFOSI Counterintelligence Awareness Briefing*. 2006, Air Force Office of Special Investigations - Systems Protection Division/Technology Protection.

13. Janssen, W., *Technical Director for Information Risk Management*. 2005: National Security Agency

14. Sterman, J.D., *Business Dynamics: Systems Thinking and Modeling for a Complex World*. 2000, Boston: McGraw-Hill.

15. Gharajedaghi, J., *Systems Thinking: Managing Chaos and Complexity*. 1999, Boston: Butterworth Heinemann.

16. Holon. *Polytomous Rasch model*. 2004 [cited; Available from: http://en.wikipedia.org/wiki/Polytomous_Rasch_model.

17. Holon. *Rasch model*. 2005 [cited; Available from: http://en.wikipedia.org/wiki/Rasch_model.

18. Faber-Espensen, R. *Likert scale*. 2004 [cited; Available from: http://en.wikipedia.org/wiki/Likert_scale.

Bibliography

19. Amead. *Psychometrics*. 2001 [cited; Available from: http://en.wikipedia.org/wiki/Psychometrics.

20. Lowenstein, T. *Life Stress Test*. 1997 [cited; Available from: http://www.cliving.org/lifstrstst.htm.

21. King, J., *MATLAB for Engineers*. Engineer's Toolkit: A First Course in Engineering. 1998, Melno Park, California: Addison-Wesley.

22. *Linear Regression*. 2002 [cited; Available from: http://en.wikipedia.org/wiki/Linear_regression.

23. *Adjudicative Guidelines For Determining Eligibility For Access To Classified Information*. 1997.

24. McGrath, P.B., *Clinical Manager of Anxiety Services at Linden Oaks Hospital at Edward*. 2006: Naperville, Illinois.

25. Rodriguez, P.M., *Diary of a Spy*, in *Insight Magazine*. 2001.

26. Havill, A., *The Spy Who Stayed Out in the Cold: The Secret Life of FBI Double Agent Robert Hanssen*. 2001, New York: St. Martin's Press.

27. Havill, A. *The Last Day in the Sun*. 2001 [cited; Available from: http://www.crimelibrary.com/terrorists_spies/spies/hanssen/1.html.

28. *USA v. Robert Philip Hanssen: Affidavit in Support of Criminal Complaint, Arrest Warrant and Search Warrants*, in *Stefan A. Pluta*. 2001, US District Court for the Eastern District of Virginia.

29. Katherine L Herbig, Martin F Wiskoff, *Espionage Against the United States by American Citizens 1947-2001*. 2002, Defense Personnel Security Research Center (PERSEREC): Monterey, California.

30. Davey, M., *Secret Passage*, in *The Chicago Tribune*. 2002: Chicago.

31. *Espionage Cases 1975-2004: Summaries and Sources*. 2004, Defense Personnel Security Research Center (PERSEREC): Monterey, California.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ORGANIZATION.

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
13-06-2006	Master's Thesis	May 2005 - June 2006

4. TITLE AND SUBTITLE

Mitigating Insider Threat Using Human Behavior Influence Models

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Puleo, Anthony J., Captain, USAF

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Air Force Institute of Technology (AFIT/EN)(Bldg 640)
Graduate School of Engineering and Management
2950 Hobson Way, WPABF, OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT/GCE/ENG/06-04

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Insider threat is rapidly becoming the largest information security problem that organizations face. 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 risk-based 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 an in-depth case study on Robert Hanssen, the FBI's double agent who sold the Soviets secrets for more than twenty years.

15. SUBJECT TERMS

Insider Threat, Human Behavior, Influence, Model, Risk Prediction

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Dr. Robert F. Mills (ENG)
U	U	U	UU	119	19b. TELEPHONE NUMBER *(Include area code)* (937) 255-3636 x4527; robert.mills@afit.edu