Technical Report 09-02
August 2009

Insider Risk Evaluation and Audit

Eric D. Shaw
Consulting & Clinical Psychology, Ltd.

Lynn F. Fischer
Defense Personnel Security Research Center

Andrée E. Rose
Northrop Grumman Technical Services

Approved for Public Distribution: Distribution Unlimited
Defense Personnel Security Research Center

Technical Report 09-02 **August 2009**

Insider Risk Evaluation and Audit

Eric D. Shaw, Consulting & Clinical Psychology, Ltd.

Lynn F. Fischer, Defense Personnel Security Research Center

Andrée E. Rose, Northrop Grumman Technical Services

Released by – James A. Riedel

BACKGROUND

Previous insider threat research by Shaw and Fischer identified individual, situational and contextual factors associated with insider offenses. Building upon these authors' research, this study documents and discusses the rationale, previous research, and process for developing a tool to be used for detecting insider risk within an organization. The authors identify organizational audit questions, pointing to the best security practices derived from the findings and implications of empirical and case study work. While much insight has been gained regarding behavioral and technical characteristics of employees who attack critical government and industry information systems, this tool or guide is intended to address specific organizational vulnerabilities to a broad range of insider risks.

HIGHLIGHTS

This report on the development of a management tool for security managers and their counterparts in human resource departments will help to assess personnel security programs and organizational processes on various dimensions of insider risk. The goal is to minimize the risk of a broad range of adverse insider behaviors. Based on past studies of insider offenses, the authors identify several areas of effective management intervention to mitigate the probability of damage. For each area, a series of self-audit questions point to the presence or absence of policies, safeguards, or best practices that should be considered by security or other management personnel as proactive measures to minimize insider risk. The study recommends that this tool be used to assess an organization's current level of vulnerability to adverse insider behavior and as an aid to the formulation of an insider risk mitigation plan that is preventative and proactive.

Defense Personnel Security Research Center
99 Pacific Street, Suite 455-E
Monterey, CA 93940-2497

REPORT DOCUMENTATION PAGE

REPORT DOCUMENTATION PAGE	**Form Approved OMB No. 0704-0188**	
The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.		
1. REPORT DATE: 20090819	2. REPORT TYPE Technical Report 09-02	3. DATES COVERED (From – To) January 1996 - August 2009
4. Insider Risk Evaluation and Audit	5a. CONTRACT NUMBER:	
	5b. GRANT NUMBER:	
	5c. PROGRAM ELEMENT NUMBER:	
6. AUTHOR(S): Eric D. Shaw, Lynn F. Fischer, Andrée E. Rose	5d. PROJECT NUMBER:	
	5e. TASK NUMBER:	
	5f. WORK UNIT NUMBER:	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Defense Personnel Security Research Center 99 Pacific Street, Suite 455-E Monterey, CA 93940-2497	8. PERFORMING ORGANIZATION REPORT NUMBER PERSEREC: Technical Report 09-02	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITOR'S ACRONYM(S)	
	11. SPONSORING/MONITOR'S REPORT NUMBER(S):	
12. DISTRIBUTION/AVAILABILITY STATEMENT: (A) Distribution Unlimited		
13. SUPPLEMENTARY NOTES:		
14. ABSTRACT: The purpose of this study is to present the rationale, previous research, and process for developing a tool to be used for detecting insider risk within an organization. Based on past studies of insider behavior, the authors identify several areas of effective management intervention to mitigate the probability of damaging behaviors. For each area, a series of self-audit questions point to the presence or absence of policies, safeguards, or best practices that should be considered by security or other management personnel as proactive measures to minimize insider risk.		
15. SUBJECT TERMS:		

16. SECURITY CLASSIFICATION OF: UNCLASSIFIED			17. LIMITATION OF ABSTRACT:	18. NUMBER OF PAGES: 79	19a. NAME OF RESPONSIBLE PERSON: James A. Riedel, Director
a. REPORT: UNCLASSIFIED	b. ABSTRACT: UNCLASSIFIED	c. THIS PAGE: UNCLASSIFIED			19b. TELEPHONE NUMBER (Include area code): 831-657-3000

Standard Form 298 (Rev. 8/98)
Prescribed by ANSI td. Z39.18

PREFACE

This report represents the next logical step by the authors to present findings from empirical and case study research previously conducted on the insider threat, in the form of a practical guide to employers and security practitioners. Defense Personnel Security Research (PERSEREC) reports by Shaw and Fischer such as *Ten Tales of Betrayal,* in 2005, and *A Survey of Innovative Approaches to IT Insider Prevention, Detection, and Management,* in 2006, offered insight into what lies behind insider offenses, along with recommendations to security managers.

This contribution to the security community addresses the broader insider risk based on the premise that sound personnel security practices—preemployment screening, security awareness, monitoring, and active intervention in the case of employee disgruntlement—help mitigate a wide range of insider threats including espionage against the United States and IT sabotage by disgruntled, self-serving or other insiders. This report contains a systematic compilation of specific ideas and suggestions for management intervention as preventative measures.

The final phase of this effort will be to develop an audit tool, based on the tables in this report's appendix, and place it on the PERSEREC website.

James A. Riedel
Director

EXECUTIVE SUMMARY

The purpose of this study is to provide security managers and their counterparts in human resource departments with a management tool for evaluating the effectiveness of their personnel security programs and organizational policies and processes for minimizing the risk of adverse insider behavior.

Insider risk continues to be a significant threat to national and corporate security. While arrests for espionage have decreased in recent years, the theft of classified and sensitive information and technology by trusted insiders, often on behalf of foreign adversaries and competitors, continues to be a serious problem. In the private sector, the fact that increasing percentages of corporate value (now as much as 75%) are directly linked to such intangible assets as intellectual property indicates that these organizations are increasingly vulnerable to malevolent insider behavior**.**

The Defense Personnel Security Research Center (PERSEREC) continues to examine espionage, IT sabotage and other forms of adversarial insider behavior as one of its primary research concerns. PERSEREC devotes significant resources to understanding the scope, causes, and consequences of trust betrayal by insiders. Insider risk applies, in a broad sense, to any activity by military, government, or industry employees whose actions or inactions, by intent or negligence, result (or could result) in the loss of critical information or valued assets. These activities can pose a threat to national security, endanger the lives or well-being of other employees, or destroy a successful company. Such behaviors include espionage against the United States, theft of intangible assets or intellectual property, sabotage or attacks against networks and information systems, theft or embezzlement, illegal export of critical technologies, and domestic terrorism or collaboration with terrorist groups.

While these crimes and offenses may seem dissimilar, the offenders themselves are frequently driven by the same motivations—greed, disgruntlement, conflicting loyalties, ego-satisfaction—and they often exhibit similar early indicators or precursors of subsequent damaging behavior. It follows that security managers in industry and government who adopt or promote best practices and policies designed to detect these precursors and intervene effectively will be best positioned to minimize the probability of an array of potential threats.

Based on past studies of insider behavior, we have defined several areas of effective management intervention to mitigate the probability of damaging behaviors. These include policies and practices, recruitment, preemployment screening, training and education, continuing evaluation and policy implementation, and employee intervention. In addition, we discuss features of organizational context that would magnify insider risk (i.e., cultural, political, economic, sector-specific and organization-specific factors).

For each of these areas, we start with an introductory discussion and conclude with a series of self-audit questions designed to sensitize management personnel to the risks their organization may face. Multiple positive responses to any of these questions may mean that the organization is vulnerable to the specific organizational risk issues related to the area in which those questions fall. Strategic plans to mitigate adverse insider behavior should incorporate those additional policies and safeguards.

Previous studies have found that many of the information technology insiders who perpetrated malicious acts had been problem employees elsewhere. Others were inappropriately assigned to positions for which they were unqualified or were in other ways incompatible. Adequate recruitment and preemployment screening could have prevented the resulting losses. In other cases, the manner in which the organization intervened with the at-risk employee actually escalated rather than mitigated the risk. These and other findings indicate that a number of basic organizational processes associated with employee hiring, placement, employee monitoring and management have direct implications for organizational security. The self-audit questions, standing alone, provide (1) an evaluation tool for assessing the current level of vulnerability of any organization to damaging insider behavior and (2) a means for developing an insider risk mitigation plan.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF TABLES IN APPENDICES

INTRODUCTION

Insider risk refers to the risk that a trusted or authorized person will participate in a behavior that causes damage to his or her employer. Trusted and authorized individuals having authorized physical or logical access to a workplace are commonly labeled as insiders. Insider risk continues to be a significant threat to national and corporate security. According to the 2007 Computer Security Institute survey, there was a 17% increase that year in reports of insider abuse, with 59% of respondents reporting insider problems (Computer Security Institute, 2007). While arrests for espionage have decreased in recent years, the theft of classified and sensitive information and technology by foreign adversaries continues to be a serious problem. In the private sector, increasing percentages of corporate value (now as much as 75%) are directly linked to such intangible assets as intellectual property, indicating that these organizations are increasingly vulnerable to malevolent insider behavior**.**

The Defense Personnel Security Research Center (PERSEREC) has continued to study insider espionage and sabotage as one of its primary concerns, and it has devoted significant resources to understanding the scope, causes, and consequences of trust betrayal by supposedly trusted employees. Insider risk applies, in a broad sense, to any potentially adverse activity by military personnel or employees in government or industry whose actions or inactions, by intent or negligence, result in the loss of critical information or valued assets. These activities can pose a threat to national security, endanger the lives or well-being of other employees, or even destroy a successful company. Such behaviors include espionage against the United States, theft of intangible assets or intellectual property, sabotage or attacks against networks and information systems, theft or embezzlement, data modification for personal gain, illegal export of critical technologies, and domestic terrorism or collaboration with foreign terrorist groups.

While these crimes and offenses may seem dissimilar, the offenders themselves are frequently driven by the same motivations—greed, disgruntlement, conflicting loyalties, ego-satisfaction—and exhibit similar early indicators or precursors of subsequent damaging behavior (Band et al., 2006). It follows that the security managers in industry and government who adopt best practices and policies designed to detect these precursors and intervene effectively will be best positioned to minimize the probability of the aforementioned array of potential threats.

Earlier studies of espionage and computer abuse in the corporate and government sector have focused on fairly narrow behavioral, motivational, and technical case chronologies while not examining organizational or situational factors that can contribute to or mitigate insider risk. However, these studies have produced significant organizational information, and preliminary results have highlighted multiple aspects of organizational stress, processes, and practices with implications for insider risk.

For example, many of the information technology (IT) insiders who perpetrated malicious acts in these studies had been problem employees elsewhere. Others were inappropriately assigned to positions for which they were unqualified or were in other ways incompatible. In many other cases, the manner in which the organization intervened with the at-risk employee actually escalated rather than mitigated the risk. These and other findings indicate that a number of basic organizational processes associated with employee hiring, placement, employee monitoring and management have direct implications for organizational security (Shaw & Fischer, 2005).

The purpose of this report is to establish the empirical basis for developing an evaluation tool that will provide security managers, particularly those working in DoD components, the Defense industry and critical infrastructure, with a management aid for evaluating the effectiveness of their personnel security programs and organizational processes for minimizing the risk of insider violations.

It should be noted that the number of persons who actually commit insider misconduct is small compared to the number of total employees. There is a serious concern associated with preemployment screening in general and screening for insider risk in particular. The current project seeks to increase organizational sensitivity to individual and group indicators of risk across the entire organization throughout the employee life cycle (recruitment through termination) rather than recommend a particular profile, indicator or mechanism for identifying individuals at risk for insider actions. Nor are we attempting to prescribe formulas for action, such as denying an applicant a job based on a single or cluster of indicator items.

BACKGROUND

Initially, the authors developed an inventory of insider organizational risk factors based on lessons learned from empirical analysis of a relatively large number of insider cases, academic research, and organizational consultations. For example, through collaboration and joint research with the Carnegie Mellon Software Engineering Institute's (SEI) Insider Threat Team, the authors had access to analyses of over 250 cases, as well as to over 100 additional cases in a PERSEREC database. Conclusions and recommendations also draw from an examination of over 85 private insider consultation cases by Shaw. In addition, we have referenced many of the leading personnel security guidelines from industry (International Organization for Standardization 27002 (2007) to assure compatibility of our findings and industry standards.

The authors take a retrospective view of insider cases, examining the perpetrators' interactions with the organization as the risk of the insider attack increased over time, and then asking the following questions:

- Did the organization adequately account for cultural, social, political, legal, economic and other local pressures and stressors in its environment that increased the risk of insider activity across its many potential targets?
- Did the organization lack any important policies or practices (e.g., preemployment screening, employee monitoring) that could have alerted it to the risks presented by this employee in a more timely way, deterred this individual, managed the risk, or prevented his or her actions?
- Did any of the organization's policies and practices have unintentional consequences that made it harder to deter, manage, or prevent insider risks, or did they even increase the risk of insider actions?
- Did the manner in which the organization enforced, or failed to enforce, existing policies and practices contribute to the insider's risk?
- How could modification of the organization's policies and practices have improved the organization's ability to prevent, detect, deter, and manage insider risk?

Several assumptions underlie the approach used in this study. The first assumption was that insider acts do not occur suddenly or in isolation from previous observable behaviors, including interactions with organization personnel and resources. We assume, and prior research supports the finding (Band et al., 2006), that insiders travel down a critical pathway toward their attacks, influenced by specific preexisting risk factors and interactions with their environment. This assumption implies that managers may become aware of their effect on an insider's progression and, in some cases, act in a manner to reduce the odds of serious effects on the organization.

It also follows from this finding that the odds of individuals becoming insider risks increase as the individuals acquire more negative characteristics, such as difficulty getting along with others, and adverse experiences (i.e., supervisor conflict, termination). However, due to a lack of controlled research, we do not know if individuals with all the risk indicators documented by Band et al. (2006) are at significantly greater risk than individuals without any, or with fewer, indicators for insider actions. The authors of this report assume that the insider problem is significant enough to use the best data available to try to suggest ways to mitigate the risk. However, we can not assume that an individual with one or more insider risk factors is in danger of committing insider acts. Rather, we suggest that the accumulation of insider risk data be used to guide policy development and investigative resources. In the case of the insider risk evaluation and audit tool proposed in this report, we recommend that the organization be in a position to detect these risk factors and intervene effectively to investigate and manage insider risk.

For example, a percentage of our cases involved persons recruited from personal or family networks. In many of these cases the recruitment was associated with reduced screening of their background risks and with biased treatment of their online and interpersonal behavior when risk issues arose. However, we have no controlled, prospective research that indicates that such affiliated individuals are at any greater risk for insider events or are treated any differently when risks are discovered. Our focus in identifying this risk is not to discourage the use of these recruitment channels based on limited evidence. For example, we suspect that the use of employees personally known by, and affiliated with, current employees may serve as a deterrent to insider activity in many contexts. Rather, our aim is to sensitize the user to the risks that have been associated with the recruitment of such individuals so that if risk issues arise among such persons, they can be addressed with greater awareness and insight.

The second assumption underlying the approach used in this study is that all organizations perform basic tasks for the recruitment of new employees, for their training, socialization, assignment to duties, compensation, promotion or demotion, and mechanisms for their termination. It is in the course of these interactions with their employees that organizations can act to prevent, deter, detect, and manage insider risk.

Several additional assumptions also influenced the production of this tool. For the research reasons cited above, this tool is not designed to be an infallible predictor. The risk of false positives for any single, or even multiple risk factors, is much too great to use these measures in this fashion. For example, the fact that preemployment screening reveals that a candidate for employment has a history of some type of security violation may or may not be grounds for rejection, depending on the organization, the position at issue, and other information about the employee. However, it may become a vital piece of information if the employee’s subsequent behavior raises a concern regarding information security violations. In addition, we have focused our efforts on raising general issues concerning these risk factors and producing generic questions that need to be adapted to a user's specific organization and the context in which it operates.

Another potential set of biases comes from the data on which these conclusions are based. While our case data have been supplemented by consultation experiences that have not involved case prosecution or other legal actions, the vast majority of the cases we studied have been successfully prosecuted in court. While this adds some assurance of the breadth and factual basis of the data, prosecuted cases probably represent the tip of the iceberg of overall insider events. Our assumption is that these cases are more serious in terms of damage experienced by the organization, and may differ from nonprosecuted cases in other ways. Thus, our conclusions are not based on data involving inadvertent employee actions that have negative consequences. Many estimates indicate that these less serious episodes represent a significant portion of insider activity and risk. Nor have we included cases of purposely planted "moles" who have entered an organization with the premeditated purpose of committing espionage, sabotage, theft or other adverse insider activity. Obviously, recruitment, screening and other risk reduction measures, discussed below, will not be as effective in detecting moles or professional agents.

Lastly, a draft of this report was reviewed by two panels of industry security professionals from the American Society of Industrial Security (ASIS). These subject-matter experts represented government contractors, critical infrastructure industries, and cutting-edge, web-based, IT companies. The experts reviewed the audit tool for completeness and relevance across a range of organizational settings, including operations in emerging markets where Western cultural, political, legal and economic assumptions are less relevant than in the United States. We also asked for feedback regarding the practicality and potential acceptance of the practices found within the tool. In addition, we asked our panelists to compare their experiences with cases resolved without law enforcement involvement to the vast majority of cases in our database, which involved prosecution and conviction. The advice and reflections of these highly experienced private-sector security managers provided additional insight on several areas of management intervention and confirmed that our final product would be valued by the security profession in industry and government.

THE ORGANIZATION IN CONTEXT: GENERAL FACTORS MAGNIFYING INSIDER RISK

Contextual Risk Factors refer to cultural, social, political, economic, sector and specific local factors exerting stress on the organization that may translate into increased insider risk (See Table A-1 in Appendix A). Differences in ethical assumptions related to physical and intellectual property, group loyalty, or communications due to cultural differences may be at the root of conflict and misunderstanding between organizational branches located in different countries or between employees and staff when there are cultural, ethnic or national differences. Political, social or even military conflicts within an organization's community can also have a direct affect on employees when they associate the organization with one side of a confrontation. Even if the organization is not in any way involved in local political, military or social conflicts, staff members may be individually affected in a manner that can exacerbate insider risk. Economic pressures within the organization's community can have a direct effect on employees, including an increase in financial stress, leading to greater insider risk.

Other sector-specific stressors, such as a decrease in the price of the organization's product, shortages of raw materials, labor conflicts, technological change, intensified competition or other forces that affect the industry or sector, can translate into direct stress on vulnerable employees. Additionally, specific organizational events (i.e., layoffs, mergers, pay reductions, outsourcing, and technological changes) can cause increases in employee stress and disgruntlement.

Finally, many organizations are high profile targets for penetration by adversaries, criminal groups, and competitors as a result of their missions, products, or services. Detailed knowledge of one's adversaries and vulnerable targets is also critical to estimating insider risk. This has become even more urgent lately as data reveal a growing trend toward insider-outsider collaboration in many cases (Cappelli & Moore, 2008). In general, these contextual factors act as a risk-multiplier when the organization-specific audit questions are under consideration.

CULTURAL FACTORS

In some non-Western societies, loyalty to the employer—especially a foreign employer—may be secondary to loyalty to the family, nation, political party, religion or ethnic group. Conventional Western cultural expectations regarding loyalty, sacrifice, and dedication to the organization above other parties usually do not apply in this environment.

For example, a large organization began tracking the appearance of products in a major South Asian market having a striking resemblance to those manufactured in its Chinese plant. According to cross-cultural threat assessment expert, Dr. Harley Stock, an investigation revealed that after having met production quotas from headquarters in the U.S. plant, managers and employees used the remaining inventory to produce an identical product under a separate name. They saw no ethical or business conflict in this activity, popularly referred to as the “third shift” since this above-quota production typically occurs after normal business hours.

According to Stock, cross-cultural differences in assumptions regarding ownership of physical and intellectual property and company versus community loyalties were in play in this relationship. Stock noted that most Chinese express personal loyalty first to the state, followed by their family, and only then to their employers, especially if the employer is a foreign company. Lack of understanding of these differences in cross-cultural assumptions led to an insider company within this organization that had used its resources to go into direct competition with the parent company (H. Stock, personal communication, December 23, 2008).

Other differences in cultural assumptions and loyalties can, and have, influenced insider risk. As in the case above, cultural miscommunication can occur on a corporate level or on a personal level when employees, particularly supervisors and subordinates, experience miscommunication or conflicts based, in part, on differences in social expectations and norms. For example, Shaw, Post, and Ruby (1999) described the case of a U.S. company with a bank systems administrator who sabotaged accounting servers after a series of conflicts with his supervisor led to his reduction to a part-time consultant. This conflict was significantly aggravated by cultural, professional, and gender differences between this male, Indian national and his female, conservative, Irish-Catholic, nontechnical supervisor from whom he had great difficulty taking direction.

For organizations with affiliates, partners, or other relationships abroad or even with significant representation by different cultural groups within the United States, cultural factors can lead to very direct and subtle tensions that can increase the likelihood of insider risk. In addition, different parts of the same organization located in the same location may have very different internal cultures that affect insider risk. For example, a research wing of an organization may place higher value on the free exchange of sensitive information than a production or marketing division.

Herbig (2008) has summarized the recent literature on globalization and its implications for national allegiance and loyalty. Herbig’s report describes the many challenges to traditional national loyalty posed by the globalization of a high-tech workforce with attachments across traditional national boundaries. These challenges include:

- The sense of persons, living a transnational lifestyle, that they are “above” identifying themselves with one state.
- That interest and involvement, among immigrants to the United States, in events and politics in a native country tend to increase over time rather than diminish.

- Many transnational entrepreneurs or “sojourners” straddle multiple countries and make decisions based on self-interest rather than loyalty to a state.
- A growing trend by many nations to more easily grant dual citizenship so as to not endanger the benefits of a globalized economy.

These and other important trends associated with globalization identified by Herbig have direct implications for insider risk and present new risk indicators that require integration in insider risk analyses. In summary, cultural differences, especially those now accelerating along with globalization, can directly affect the type of insider risk an organization faces and how these risks are managed. While different policies and practices can be adapted to various cultural settings, these variations can also be confusing to personnel and undermine the effectiveness of policies applied in one location that were designed to prevent, deter, detect, or manage insider risk in another.

Table A-1, in Appendix A, presents a series of questions designed to sensitize employers to the risks their organization face from these contextual issues.

POLITICAL OR SOCIAL FACTORS

With or without the significant background risks of distinct cultural differences, political or social conflicts in the organization’s environment can also multiply the opportunities for insider risk. Political or social conflicts may be as stressful to employees as military conflict or terrorism. More subtle political conflicts such as an unpopular local zoning ordinance (affecting the organization) or pressures to comply with immigration laws may also result in organizational stress. For example, a U.S. government organization in Iraq may have to deal with attempts by extremist groups to penetrate the organization and compromise its employees.

Government and corporate groups may also have to be concerned about insiders participating in whistle-blowing or trust betrayal in the context of political conflicts. This can affect the organization by arousing strong feelings among personnel or provide rationale for actions by disgruntled employees. For example, a Muslim employee of an American firm in London was spotted at an antiwar protest. Later he was traced to an indicted Islamic cleric, assisting him with his web campaign to recruit followers for his mosque. This individual’s anger regarding the war in Iraq led him to conduct political activities that placed his organization in jeopardy. In another recent case, a mentally unstable individual working in a Defense industry attempted to contact Al Qaida to offer information regarding U.S. military assets in Iraq after becoming angry about U.S. policy toward the Islamic world.

ECONOMIC FACTORS

Generalized economic pressures such as recessions, inflation, deflation, trade disruptions and other global economic forces can have both general and specific effects on organizations that translate into direct economic pressures on employees.

As of this writing, numerous established financial institutions have disappeared, automotive manufacturers are at risk, and retail businesses are failing at record rates. These economic factors translate directly into insider risk as affected employees face possible loss of employment or other negative economic options and generally feel insecure and disgruntled regarding their fate.

SECTOR-SPECIFIC FORCES

Technological innovation, increased competition, shortages of raw materials or skilled workers and other pressures within a sector can also result in economic pressures on employees. These stressors may result from job loss or reductions in pay and arouse temptations to use proprietary information to improve employment prospects with a competitor. For example, layoffs within the financial sector resulting from mergers and acquisitions have greatly increased the risk of insider attacks by former and current disgruntled employees.

ORGANIZATION-SPECIFIC SOURCES OF RISK

Many organizations suffer inherently greater levels of insider risk due to the competitive nature of their business, their reputation, overseas locations, their technological dependence on highly skilled, difficult-to-monitor employees, the sophistication and determination of their adversaries, or aspects of their organizational location or functions. For example, military and intelligence organizations that must often hire extensively from local workforces abroad are routinely the target of penetration and recruitment efforts by adversaries. Computer chip manufacturers exist in a highly competitive environment and must hire highly skilled individuals worldwide that may have little loyalty to the organization. Other organizations, such as the National Aeronautics and Space Administration and Carnegie Mellon’s Computer Emergency Response Team, are chronic penetration targets because of their functions and reputation. These efforts may involve outside hackers or social engineering efforts aimed at employees. Credit card companies and their technological contractors have also been regular victims of attacks by compromised insiders due to their access to valuable personal financial information.

In summary, cultural, social, political, economic, sector and organizational-specific contextual factors can directly affect insider risk. While the balance of this report focuses on internal organizational policies and practices critical to the detection and management of insider risk, these contextual factors should be considered as risk-multipliers when organizational personnel attempt to estimate and mitigate the insider threat.

FUNCTIONAL AREAS FOR RISK MITIGATION

For the purposes of this report, organizational-management functions have been broken down into several functional internal organizational areas for risk mitigation relevant to the prevention, deterrence, detection, and risk management of adverse insider behavior:

- *Policies and Practices* refers to the rules and guidelines governing employee behavior that have proven critical to deterring, detecting, and correcting potentially harmful behaviors by employees and others. Policies and practices can mandate employee screening, generate both human and IT monitoring and detection systems to enforce regulations, and establish guidelines for investigation and consequences when these risk behaviors are detected. The absence of policies and practices has actually facilitated insider activity and prevented successful prosecutions of significant insider violations. Not only should these guidelines exist, they also must be documented and easily accessible to employees, contractors and subcontractors.
- *Recruitment* refers to the manner in which an organization solicits individuals to apply for employment. While some traditional recruitment methods have been extremely useful to organizations, they have also been implicated in some insider incidents as having contributed to an increase in the risk of misconduct. These recruitment practices have included the use of placement groups or “body shops,” bounties, recruitment bonuses or employee rewards for referring recruits, and the recruitment and preferential hiring of employee family members or friends. While many of these processes may prove highly valuable in employee recruitment, in some cases they have exacerbated other insider risks when they have resulted in reduced screening or contributed to internal social networks that compete for employee loyalty with the organization.
- *Preemployment Screening* refers to the manner in which organizations proactively examine potential employees, including contractors, subcontractors and temporary hires, for personal and professional history and characteristics related to their qualifications, fit, and risks as employees. Numerous subjects who committed insider misconduct would probably not have been hired by their organizations if prior activities and personal characteristics—which are the routine target of preemployment screening measures—had been detected.
- *Training and Education and Evaluation of Training Effectiveness* (TEE) refers to the way the organization provides formal training and education regarding its policies and practices, especially those directly related to insider risk. TEE also refers to the way in which the organization assesses the effectiveness of education and training efforts through direct evaluation of employee learning and skills, as well as the impact on the risk behaviors targeted in the education and training programs. The frequency with which these TEE programs are updated to take account of feedback on employee learning and risk behavior and to incorporate new information related to insider risks is also examined.

- *Continuing Evaluation and Policy Implementation* refers to the manner in which employees are monitored for continued reliability and personnel security policies are implemented in the work environment. This includes reporting concerns about policy fairness and violations, violation detection, investigation and evaluation, documenting investigative results; determining and administering consequences; and measuring the extent to which policies are put into practice.
- *Employee Intervention Assessment and Planning* follows from *Continuing Evaluation* and addresses the manner in which managers and their multidisciplinary teams consider possible negative effects of disciplinary or other remedial actions with employees prior to the intervention. Previous research suggests that the routine assessment of an employee's risk of engaging in an insider event prior to serious disciplinary action or other intervention is necessary when he or she has a history of technical violations or problems that were of a security concern. This is especially true prior to the employee's departure from the workplace by involuntary or, in some cases, voluntary termination.

Figure 1 provides an overview of these functional areas in which management can intervene for the mitigation of insider risk. It reflects the life-cycle of the employee from recruitment to termination. Following hiring, typical employees enter into an indoctrination or initial socialization phase during which they are exposed to the conditions of employment, organizational policies, and security awareness and education. For the remaining period of employment they are subject to continuous evaluation, on-the-job monitoring, and the reinforcement of security awareness and training that focuses on security and personnel policies. For most employees, this phase will continue until retirement or voluntary resignation. For others, issues may arise concerning their loyalty, reliability, honesty, or performance that will require timely and effective intervention by management (supervisors, human resource personnel, or security officials). It is this latter category of management activity that is most problematic since an inappropriate or poorly timed response by a manager can result in greater risk or actual damage than would have occurred were the situation better handled.

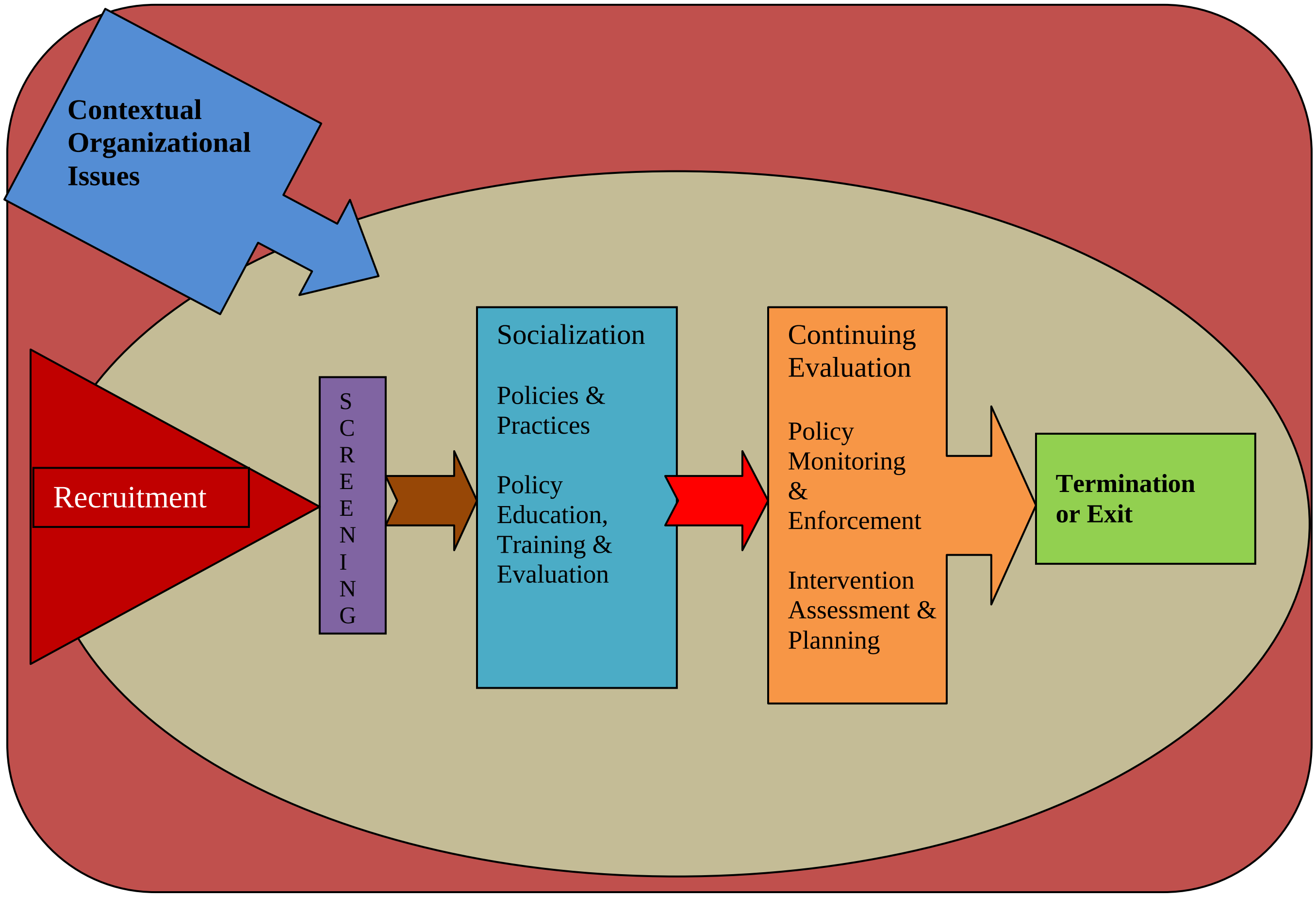
Contextual Organizational Issues
Recruitment
SCREENING
Socialization
Policies & Practices
Policy Education, Training & Evaluation
Continuing Evaluation
Policy Monitoring & Enforcement
Intervention Assessment & Planning
Termination or Exit

Figure 1 Overview of Assessment Tool Components

POLICIES AND PRACTICES

This section reviews a general list of organizational policies and practices that are relevant to prevention, detection, and management of insider risks. Furthermore, we present policies and strategies for investigation and intervention. In academic literature, case studies and anecdotal reports, the presence of these policies and practices directly relevant to the insider threat has proven critical to protecting organizational assets. They can deter potentially harmful behaviors by employees and others, prompt both human and IT monitoring and detection systems to reinforce the policies, and establish parameters for investigation and consequences when these risk behaviors are detected. Absence of relevant policies and practices has facilitated insider activity and prevented successful prosecutions of significant insider violators.

The following listing gives a general overview of the types of policies and practices that have been linked to reduced insider risk. Policy and practice guidelines must be documented and easily accessible to employees and others who work for, or with, the organization. The section on “Training, Education ” (page 27) describes the education and training programs that are essential to communicate these policies and practices to employees and others to ensure that they understand them and how they are implemented. This section summarizes some of the evidence supporting the importance of policies and practices.

Shaw and Fischer (2004) found that security and personnel policies were lacking in eight out of the 10 cases of the insider attacks they reviewed. Missing policies and practices that could have deterred or prevented the attack, led to earlier detection of risk, helped manage the at-risk employee, or reduced the odds of the attack, included:

- Employee candidate screening and hiring.
- Hiring of relatives or social contacts.
- Protecting intellectual property.
- Termination procedures.
- Computer system access controls.
- Controlling physical access to the workplace.
- Response to threats and violence in the workplace.
- Implementing computer system back-up controls.
- Use and sale of company property.
- Response to substance abuse.
- Mandatory and voluntary referral to employee assistance programs.
- Reporting of interpersonal and IT security risk behavior.
- Prohibitions against informal help desk support.
- Response to accidental or inadvertent errors with security implications including policies and consequences addressing repetitive violations.
- Establishing safeguards against inadvertent losses such as encryption of data at rest to reduce the damage from the theft or loss of laptops.
- Monitoring IT systems security and safeguards against user misuse or unauthorized access.
- Overdependence on a single individual, use of two-man or other rules to provide redundancy of critical knowledge, and monitoring of critical users or staff by others.

In addition, the authors found many difficulties with the enforcement of existing policies and practices in eight of the 10 insider events they examined. Examples include failure to enforce rules regarding reporting of sexual and online harassment, limits on remote access after termination, personal use of organizational property, employee assistance program or mental health evaluation referrals when employees display behaviors of concern, termination of customer access after failure to pay fees, consequences for interpersonal or online violations, and limits on weekend access to facilities by visitors.

As part of their efforts to model IT sabotage and espionage within an organization, Carnegie Mellon's Insider Threat Group at the Computer Emergency Response Team (CERT) examined IT espionage and sabotage subjects and followed their progress as they interacted with their organization and the level of threat increased (Band et al., 2006). By tracking the emergence of observable behaviors accompanying increasing levels of risk, the researchers were able to identify organizational behaviors (including failures to detect risk or failures to act) that could have influenced subject behavior toward greater or less risk. This finding had direct implications for organizational policies and practices to prevent, deter, detect, and manage insider risks.

An important part of the CERT modeling effort was identifying observable behaviors common to most of the cases that offered a direct challenge to the organization's ability to detect the risk and manage it in a manner that decreased the odds of the insider episode. The researchers identified six observations common to both the IT sabotage and espionage cases they studied that challenged the organization. Findings included:

- Most saboteurs and spies had common personal predispositions that contributed to their risk of committing malicious acts.
- Stressful events, including sanctions by the organization, contributed to the likelihood of insider attacks.
- Behaviors of concern—often violations of accepted behaviors or rules—were observable before and during the insider acts.
- Technical actions by many insiders could have alerted the organization to planned or ongoing acts.
- In many cases organizations failed to detect or ignored rule violations.
- Lack of physical and electronic access controls facilitated both insider sabotage and espionage (Band et al., 2006).

The breadth of these findings has implications for a wide range of organizational policies and practices.

Table 1 (page 16) presents observations made by CERT researchers and relates them to an area of policy and practice vital to an organization's ability to manage insider risk. These observations point to recommendations or best practices for mitigating insider risk. For example, personal predispositions that may increase a subject's risk of insider activity (e.g., the risk posed by previous rule-breaking behaviors) can be evaluated at the time of preemployment screening. In addition, these risk characteristics need to be reflected within policies and practices, especially those that deal with the rules governing interpersonal behaviors. In turn, employees must be educated to recognize these predispositions in the form of observable behaviors and be trained on how to report these risks and react when confronting them. Relevant human and IT detection and recording programs must be in place to record the occurrence of these behaviors, whether they involve human resource records or employee monitoring software, and scripts must be in place that guide how the organization responds when these personal predispositions manifest themselves in the form of observable risks.

Table 1
Relevance of CERT Organizational Challenges in Five Audit Areas

Observed CERT Organizational Challenges	***PreEmployment Screening***	***Policies & Practices***	***Training, Education, Evaluation***	***Monitoring & Enforcement***	***Enforcement & Termination Assessment and Planning***
Subject personal predispositions	Capability to screen out at-risk candidates	Policies covering possible negative behaviors by persons with insider risk factors	Training programs designed to help employees recognize, report and deal with these negative behaviors indicative of insider risk	HR and IT systems to record reported behaviors and procedures, and to enforce rules and contingencies when violations occur	Specialized teams to evaluate the subject and violation in order to plan the most useful response—especially security-related termination
Observed behaviors of concern	Knowledge of candidates' previous interpersonal behaviors of concern	Policies and practices that identify interpersonal and technical observable behaviors of concern	Employee education and training to recognize and report behaviors of concern, and when necessary, intervention	Initiating evaluations and interventions when risk is reported. Systems for recording and monitoring results.	Specialized expertise and research to evaluate the most appropriate interventions when risk is reported
Technical risk indicators	Knowledge of candidates' past technical behaviors of concern	Policies and practices covering technical security risk behaviors	Educate and train employees on technical policies and practices, implementation and reporting risk behavior	Systems for recording concerning technical behaviors and initiating interventions	Specialized expertise and research to evaluate the most appropriate interventions when risk is reported
Detection and reaction to violations	Knowledge of candidates' capabilities or experience in evading or reacting to detection systems and interventions	Policies and practices governing mandatory contingencies when violations are detected	Educate and train employees on procedures when violations are detected	Procedures to verify violations are detected, policies followed and results of intervention are evaluated for effectiveness	Specialized expertise and research to review and evaluate success of detection and intervention operations
Physical and electronic access controls	Knowledge of candidate expertise with or previous experience in evading access controls	Policies and practice guidelines covering physical and electronic access controls	Employee education and training programs on access controls, reporting problems, implementing contingencies	Procedures to ensure problems or violations with access controls are recorded and interventions implemented	Specialized expertise exists to assess problems or violations with access controls. Design intervention for specific employees and access issues

Personal predispositions will also figure strongly as the organization assesses the subjects and the risks they present, and determine the best enforcement actions (discussed later in the report) to pursue, whether it is referral to an employee assistance program or a careful termination plan. In the area of technical and physical access controls, it would be useful to gather information on any problems a candidate has had with access controls in past jobs or any specialized expertise he or she possesses with access controls. Such knowledge can be taken into account in hiring, job assignment and information access decisions. There must also be clear policies regarding physical and electronic access controls, and employees must be educated on their existence and trained on their implementation. Human and technical means for detecting, monitoring and reporting access controls problems must exist and these problems must be recorded in a manner that also triggers intervention when specific risks are identified. Within the framework of policies and practices, these interventions must be planned by qualified personnel familiar with the employee, policies, and the technical issues governing access controls.

Table A-2 (See Appendix A, page A-6) is a self-evaluation and audit checklist of specific policy and practice areas that should be covered within an organization's basic governance structures.

RECRUITMENT RISKS

Past studies and consultations involving persons committing insider IT abuse have shown that some traditional recruitment methods have negative security implications. These problematic recruitment methods include:

- The use of placement groups such as head hunters, recruiting firms, or subcontracting organizations that have as their main purpose placement of individuals within organizations for a fee, or charge, for this placement, attached to the employee's salary. These groups have little internal infrastructure other than for the purpose of supplying such candidates.
- The use of bounties by which employees are rewarded for recruiting candidates who are subsequently brought into the organization when they encourage the hiring of persons from within the employee's social network.
- The hiring of employee family members, spouses or other relations, as well as friends or social relations, whose presence may constitute a natural faction or coalition that can bias internal decisionmaking and compete for employee loyalty to the organization.

As noted above, these practices can benefit organizations and could actually discourage insider activity. However, in a number of cases, these recruitment practices have been associated with specific insider risks. The potential side effects of these practices are described to increase user awareness of the potential problems associated with these practices rather than to discourage their use.

Table A-3 (See Appendix A, page A-9) organizes recruitment concerns into a series of questions to be addressed during an insider risk audit.

Placement Groups

Placement groups such as head hunters and recruiting firms operate by charging a fee for supplying an organization with employee candidates who are subsequently hired. Their income is derived from the initial placement of the employee in that position and most employees of such organizations operate on a per-head commission. The priority of these groups is, therefore, on the placement of as many individuals as possible. They operate predominantly in the private sector. In the government sector, subcontracting organizations, especially the smaller ones owned and run by a few individuals, operate in a similar manner but derive their income from a monthly or yearly fee added on to the employee’s salary. While these may have a larger investment in the length of time the employee remains employed by the organization, the placement of as many persons as possible is also their major goal.

In past studies of IT insiders who committed sabotage or espionage, these placement organizations contributed to the risk posed by these subjects by failing to screen them for known risk factors. This was particularly damaging and avoidable when the hiring organization also relied on the placement group for this screening or failed to screen the employee on its own or closely monitor his or her initial behavior.

Examples of this type of problem include the episode associated with Case Study 7 from Shaw and Fischer (2005) in which a prime contracting organization hired an individual to work at the Internal Revenue Service (IRS) from a subcontractor. This subcontractor assured the prime contractor that it had conducted a background investigation. However, not until the IRS conducted its own security check was the individual shown to have previous criminal convictions and to be under investigation for sabotage at his previous employer. In the 2 months he was employed at the IRS, he was cited for multiple human resource and technical violations and for attempting to sabotage the servers on which he worked.

In another illustration of this problem, a systems administrator was arrested in New York for the sabotage of accounting servers on which he worked at a financial institution prior to being notified he was being laid off and reduced to a quarterly consulting position. Shortly after his arrest and arraignment, he got a job at another New York financial institution through a recruitment firm. The Federal Bureau of Investigation (FBI) agent who arrested the suspect was aware of this event and informed the suspect’s new employer of the risk associated with his arrest and subsequent conviction (Shaw & Stroz, 2004). Without this informal warning from the alert agent, the new financial institution would have acquired a very high-risk systems administrator.

Bounties

Bounties refer to fees paid to current employees when their successful efforts to bring new employees into the organization are rewarded with a cash payment. While in the majority of cases bounties are a successful recruiting tool, they have also been associated with efforts by disgruntled employees and by employees with other risk factors, to bring persons from their social network into the organization. There have been various risks associated with this behavior in cases of IT employees assessed for risk of espionage and sabotage. The main feature of this risk is the potential for these employees to form a coalition with the employee-sponsor against the organization's management.

Examples of such cases include the episode described in Case Study 1 in Shaw and Fischer (2005) in which an academic programmer was allowed to hire students to support his development efforts at an organization deploying new software for online trading on Wall Street. These hires were also of the same foreign national origin and religion as the academic programmer, which was different from that of the majority of employees at the firm. When the organization replaced the academic employee in favor of programmers with greater commercial production experience, it faced a mutiny from the academic programmer's earlier hires. The behavior of the academic coalition included withholding vital information about the system needed to take the software into the production environment and, eventually, a denial-of-service attack that kept the system from operating.

In another example from a case consultation, a Help Desk employee was encouraged to place his "friends" within the IT department of an American media company abroad. However, his friendship network was actively involved in supporting the activities of a local radical cleric under indictment for terrorism-related activities in the United States. By the time the company recognized this situation from a chance sighting of this employee on television leading an antiwar protest, the employee and his network of five colleagues had requested a prayer room at the company for their meetings. The employees were actively assisting the cleric with their IT capabilities, when one of their wives discovered their activities. The wife threatened to tell her brother, a British soldier, about the relationship with the cleric. The employees were later recorded discussing the need to assassinate the soldier.

Bounties may be particularly dangerous when the relationship with the current employee influences objectivity or the thoroughness of screening procedures on the part of the organization. Or the use of bounties may increase the risk of hiring a dangerous individual when the association with the current employee increases the likelihood that his candidate will be hired over another individual with similar qualifications who would have been more thoroughly vetted or monitored during his initial work experience.

Recent data on the risk of fraud by IT personnel from Carnegie Mellon's Software Engineering Institute's Insider Risk Team also support the idea that insider collusion may be associated with insider risk. According to Cappelli and Moore (2008), there was collusion with another insider in 32% of insider episodes of fraud involving theft of data for financial gain and 44% of fraud events involving data modification for financial gain. Thus, any recruitment process that encourages such collusion without mitigating risk measures may increase the risk of insider violations. Cappelli and Moore's results also emphasize that when a company hires an individual it is also facilitating access by that person's social and professional contacts, and they may include persons with malicious intent. For example, the authors also found collusion with an *outsider* in 68% of insider events involving theft of data for financial gain, and in 49% of cases involving data modification for money. These results also indicate the importance of thorough background investigations that delve into an applicant's social networks.

Hiring Employee Family Members

Recruitment from within family and social networks has many of the same potential problems as bounties. The hiring and placement of persons with previously established relationships and loyalties can facilitate the formation of competitive factions within an organization, as well as the potential to bias human resource and technical regulatory monitoring and interventions targeting risk factors by relatives or friends of employees.

For example, in Case Study 10 from Shaw and Fischer (2005), the subject was hired due to his father's management position at the victimized petroleum processing plant. This led to systematic biases in the manner in which this employee was placed in his position, reviewed, subjected to discipline and sanctions, and generally held accountable for his interpersonal and technical behavior within the organization. After his father was replaced as plant foreman and his previous expectations regarding his workplace protections and entitlements began to dissolve, this employee's behavior resulted in different factions challenging the organization, and in workplace violence, IT sabotage, and other policy and legal violations.

Current and former relatives of employees, as well as personal friends, are also likely to be affected by the organizational stressors of their close colleagues or relatives, and may react to these stressors in ways that are subtly or overtly damaging to the organization. For example, in the example cited above, the subject's father—now retired—sought to intervene through his former connections to protect his son and, by doing so, attempted to disrupt the sanctioned policies and practices of the organization.

Informal practices, such as employing family members as summer interns, may also lead to a higher likelihood that they will be hired full-time. Aldrich Ames, the notorious CIA spy, was originally hired as a summer employee at the agency due to his father's employment there. The Ames case is an excellent example of the manner in which family connections within an organization can protect individuals from unbiased assessment, evaluation, and consequences of their actions.

Avoiding False Positives and Applying these Observations

How can these observations be applied without encumbering successful and productive recruitment efforts associated with placement groups, bounties or hires through social and family networks? If current policy or practice does not limit the use of these programs, then an organization may well be advised to make sure it conducts its own separate screening of all applicants and be wary about referrals from individuals with a history of behaviors of security concern within or outside the organization. Such individuals with risk indicators—further down the critical pathway toward insider event risk—may be more likely to collaborate with their new hires against the interests of the organization. Or their poor morale or disgruntlement may more easily spread to their family or social contacts within the organization. Table A-3 in Appendix A (page A-9) offers a range of self-evaluation and audit questions related to recruitment methods.

PREEMPLOYMENT SCREENING

Preemployment screening refers to the manner in which organizations examine potential employees for personal history and characteristics related to their qualifications, fit, and risks as employees. Numerous individuals who committed insider acts would probably not have been hired by their organizations if these prior activities and personal characteristics, which are the routine target of preemployment screening measures, had been successfully detected.

For example, in a study of insider attacks performed by Carnegie Mellon's Insider Threat Team from the Software Engineering Institute (SEI), Randazzo, Keeney, Kowalski, Cappelli, and Moore (2004) found that 27% of subjects committing these acts within the Banking and Finance sector had prior arrest records. In another study by the SEI team, Keeney, Kowalski, Cappelli, Moore, Shimeall, and Rogers (2005) found that 30% of the insiders committing attacks within critical infrastructure organizations had been arrested previously, including arrests for violent offenses (18%), alcohol- or drug-related offenses (11%), and nonfinancial/fraud-related theft offenses (11%). In parallel research, Shaw and Fischer (2005) found that half of their insider subjects drawn from critical infrastructure industries had a prior history of arrest or hacking violations.

The SEI team identified a series of personal predispositions or characteristics of insiders convicted of violations including espionage and sabotage (Band et al., 2006). In addition to a history of previous rule violations, these predispositions included serious mental health disorders and interpersonal skills and decisionmaking biases. The SEI team conducted a literature review to determine if other personal characteristics that might be detected at preemployment screening contributed to the risk of insider activities. The results (Phelps, Cappelli, Moore, Shaw & Trzeciak, 2007) indicated that these personal predispositions corresponded closely to findings from the academic literature that related psychological characteristics to the risk of counterproductive work behaviors (CWB). CWBs have been defined by Sackett (2002) as “any intentional behavior on the part of an organizational member viewed by the organization as contrary to its legitimate interests.” Though broader than the definition of insider threats, this area of research includes a variety of both self-destructive and retaliatory behaviors, including espionage, sabotage, theft, fraud, and vandalism.

In general, the case study results indicate that certain historical actions (e.g., arrest or previous security or policy violations) and personal characteristics (e.g., serious mental health problems, drug abuse, personality issues) have been associated with insider activities. However, it should be noted that many more persons will have a history of these actions (or possess these personal characteristics) than will commit insider offenses. This sets up the potential for false positives and the danger of screening out persons who may possess one or more of these characteristics but would not commit insider acts.

In addition, other preemployment screening measures, such as the personal interview, honesty testing, and psychological testing, have been designed to detect personal characteristics, attitudes and beliefs that have been associated with CWBs. The use of these and other tests should be part of a professionally designed battery tailored to the specific needs, risks, and legal limitations of a particular work environment.

Verifying Information on the Employment Application

Traditional employment applications contain data on a candidate’s name, address, contact information, aliases, past addresses, Social Security number, citizenship, birth date, driver’s license, employment and education history, and certification and licenses, as well as other information that can be verified by a potential employer. Simple verification of these facts can expose potential employees who may not only be unable to perform their job but may be seeking entry into the organization for illicit purposes. In addition, a detailed holistic approach to employment application materials may reveal inconsistencies that denote red flags. For instance, are dates of employment on an applicant’s resume consistent with dates from past employers? Is the applicant attempting to hide a gap in employment that might raise security concerns? Most applications also contain a signature line stating that false entries are grounds for termination of the application process or subsequent employment. In several cases from Shaw and Fischer (2005), employees who appeared technically qualified either lied about their certifications, were connected to active hacker groups, or had significant gaps in their skills due to a lack of formal training or certification that were not exposed on their applications or explored by the company prior to their hiring.

Background Checks

In some past cases, investigation of the insider revealed a personal history of behaviors that could have been exposed through background checks that would have added valuable information about the risks associated with hiring the individual. In some cases, this history involved past criminal activity, civil violations, restraining orders, employment problems, or problematic financial activities.

In a portion of these cases, these actions were directly or indirectly related to the subsequent insider violation. For example, in one case noted above, a suspect under indictment who was subsequently convicted of destruction of a company's financial servers walked directly from the court room into a job interview arranged by an IT recruiting firm. The hiring firm did not check his background and only learned of his indictment when the FBI agent on the case found out the individual had applied for a similar position in another financial institution. Case Studies 2, 3, 7 and 9 from Shaw and Fischer (2005) also had previous, undetected violations related directly to their subsequent insider attacks.

To determine if an applicant has previously engaged in criminal activities or questionable behavior, civil and criminal record checks should be conducted. Civil records provide information on possible personal irresponsibility, such as lawsuits, judgments and liens. Such financial irresponsibility increases risk that candidates will engage in illegal activities for financial gain. Criminal record checks are usually obtained from police departments and courts. However, for local, state, and federal positions, as well as for occupational licensing, criminal records can be obtained from the FBI's Criminal Justice Information System, the FBI's Civil Fingerprint file, and the FBI's Violent Gangs and Terrorist Organization file. Private sector employers have the option to use free and fee-based online resources.

Checking an applicant's background has recently been extended to the world of online activity. Looking for candidates' names on search engines, examining their personal sites on such locations as Facebook, or even assessing their role play in alternative online social networks like Second Life, may now be as important to a successful background check as traditional sources. According to *The New York Times* (Calmes, 2008), the Obama transition team examined the online activities of applicants for significant jobs in the new administration, including their Facebook sites and any blogging activity. Although there is currently no legal limitation on using this information, some experts believe that court challenges from employees tripped up by these data are inevitable (VTZ Law Blog, 2008).

Personal Interview

In past cases reviewed by the authors, social skills problems have rendered many insiders high maintenance or difficult to deal with in the workforce. The escalation of personal conflicts into major insider incidents was also quite common. While these characteristics may not appear flagrantly in a job interview, signs of interpersonal difficulties may be present.

In addition, the personal interview may be used to test a candidate's reactions to personal and professional stress, understand his or her ethical sensitivity and past reactions to negative work developments, or develop more indepth personal references ("Name two people who would give you a negative reference and what would they say about you?"). The personal interview may also serve as a check on information submitted in the job application, such as the candidate's level of education, skills, training, experience, and personal background information. In cases where the applicant will have access to sensitive and critical data or systems, it may be worthwhile to have access to interviewers trained to detect psychological symptoms of deception, or attitudes, beliefs, or personal characteristics associated with dishonesty or CWBs.

Professional Reference Checks

While there are legal pressures on former employers against providing full and honest assessments of past employees, there are signals and codes among human resource personnel that provide insight to sophisticated employers. Rather than assuming that checking a candidate's personal references will be pro forma, these assessments can reveal bogus employment claims, undisclosed gaps in employment, and unreported employment problems or sanctions, as well as serious violations or crimes. While some candidates will count on reticence from former employers, those employees who have suffered insider events are often more willing to discuss these applicants, especially if the case has been prosecuted.

Drug and Alcohol Testing

Drug testing is an important preemployment screening method because candidates who use drugs may impair their ability to protect classified or proprietary information. Furthermore, excessive use of alcohol and prescription drugs, as well as substance abuse, have been observed as symptoms of underlying psychological problems that accompany and contribute to insider risk. For example, Case Studies 7 and 10 from Shaw and Fischer (2005) involved individuals who were, respectively, using and selling illegal drugs at work and using firearms when inebriated to make threats against a supervisor.

Intensive Psychological Assessment Measures

Intensive psychological assessment measures refer to honesty testing, psychological assessment and the polygraph. These measures provide a more active and intrusive exploration of candidate characteristics, beliefs, attitudes and actual behavior. These tests are more controversial because their reliability and validity have been questioned and have been the focus of legal and legislative actions. As noted above, these methods should only be used as part of an overall preemployment screening battery that has been professionally designed and validated for the specific work setting, position, employees involved, and legal requirements governing the organization. The use of these measures should also be correlated to the risk presented within the position of concern. In addition to deployment costs, the use of these instruments also has been shown to negatively affect employee attitudes toward their organization, and that should be taken into account.

Honesty Testing

Over the past several years, honesty and integrity testing in the workplace has become more prevalent. There are several reasons for this. First, organizations that had in the past used polygraph testing for their employees were forced to stop due to new legislation. Second, a high rate of employee turnover, especially in entry-level positions, was costly but by utilizing enhanced screening approaches employee turnover and costs were reduced. Third, these measures reduced employee theft. Finally, organizations tend to hire more conscientious employees when honesty and integrity tests are given to employment candidates because the tests screen people based on their attitudes and beliefs about dishonest behavior.

For example, one of the most widely accepted honesty tests—the Psychological Screening Inventory (PSI)—focuses on discriminating those who steal from those who do not based on their values, beliefs, attitudes and past behaviors. According to Joy (1999), persons more likely to steal see themselves as average people in a dishonest world, rationalize their behavior based on the belief that everyone does it, are more tolerant of dishonesty and theft, and spend more time thinking about stealing and being tempted to steal. In addition, these individuals tend to report more past actions associated with dishonest behavior.

Personality Testing

In examining personal characteristics correlated with the risk of CWBs, academic researchers use dimensions of personality defined by the Five Factor Model (FFM) rather than the medical concepts of psychiatric or personality disorders. The FFM includes the personality factors of openness to experience, extraversion, conscientiousness, agreeableness, and neuroticism or emotional stability. These concepts have been operationalized in several well accepted versions of personality tests, including the NEO Personality Inventory Revised (NEO PI-R). Significant literature supports the notion that the FFM and the maladaptive traits from Axis II of the Diagnostic and Statistical Manual of Mental Disorders, DSM-IV (American Psychiatric Association [APA], 1994) have substantial relationships (Rolland & De Fruyt, 2003; O'Connor & Dyce, 2001; Lynam & Widiger, 2001; Widiger & Costa, 1994; McCrae et al., 2001).

Phelps, Cappelli, Moore, Shaw and Trzeciak (2007) reported that the relationship between FFM dimensions and CWBs is widely supported. For example, Hough (1992), while not specifically differentiating among CWBs, included the criterion of "irresponsible behaviors." Irresponsible behaviors included absenteeism, counterproductive behaviors, disciplinary issues, and drug and alcohol use on the job. Significant correlations were found between irresponsible behaviors and measures of achievement, agreeableness, and openness from FFM psychological tests. Salgado (2002), specifically reviewing and differentiating the literature on FFM and CWBs, found 44 studies conducted between 1990 and 1999 that examined the relationship between FFM constructs and either deviant behaviors (17), absenteeism (13), work-related accidents (9), or turnover (5). In general, these results indicated that conscientiousness and agreeableness were significant, valid predictors of workplace compatibility. More recently, Mount, Ilies, and Johnson (2006), with a sample of 141 customer service personnel, found significant relationships between the FFM personality dimensions and interpersonal and organizational CWBs as mediated by job satisfaction. The results supported a significant relationship between the FFM construct of agreeableness and interpersonal CWBs, between conscientiousness and organizational CWBs, and direct relationships between job satisfaction and CWBs and a mediating effect between agreeableness and CWBs.

Another approach to screening employees for maladaptive traits involves psychological tests that attempt to assess personality disorders, from Axis II of the Diagnostic and Statistical Manual of Mental Disorders, DSM-IV (American Psychiatric Association [APA], 1994). Although academic researchers have not been successful in finding correlations between these characteristics and CWB's, these personality disorders—especially malignant narcissism and psychopathic or sociopathic disorders—have been associated with espionage in post-hoc, prison-based assessments of espionage subjects (Director of Central Intelligence, Community Research Center, n.d.). For example, the U.S. government uses several assessment tools to screen its job candidates and incumbents for personality disorders. They include the Minnesota Multiphasic Personality Inventory (MMPI-2), the Millon Clinical Multi-Axial Inventory (MCMI-III), the California Psychological Inventory (CPI), the Sentence Completion Questionnaire (Krofcheck & Gelles, 2005). Other agencies also use Hare's Psychopathy Checklist-Revised (PCL-R) to screen its potential employees for psychopathy. Studies are also underway to assess the effectiveness of the Shedler-Westen Assessment Procedure (SWAP) (Westen & Shedler, 1999a; 1999b) for detecting personality disorders. However, this instrument must be used by trained clinicians who have interviewed candidates for employment and may therefore be too expensive for broad use in employee screening.

Consistent with earlier comments regarding the necessity for a broad array of screening instruments designed for the specific setting, findings of the existence of extreme scores on conscientiousness or agreeableness or high scores on personality disorder traits might not disqualify an individual for employment. However, in combination with at-risk scores on honesty testing, questionable references or background data, and in the context of a highly sensitive position, the scores might contribute to an overall decision against hiring. In addition, if such an individual were hired on a probationary basis and subsequently displayed behaviors of concern, these scores would suggest that these behaviors do not represent isolated incidents but are related to significant personality issues.

Polygraph

As noted above, legislation has limited the use of the polygraph for preemployment screening in private business settings. Only companies with sensitive federal contracts, work within the security industry, or facilities affecting public health and safety may use polygraph exams. While the use of polygraphs with current employees is controversial outside these contexts, this test is often used in investigations of insider activity. Generally, the costs and these constraints make the use of the polygraph outside these settings impractical for all but the most sensitive government positions involving access to critical information and vital systems. See Table A-4 in Appendix A (page A-11) for a comprehensive list of preemployment screening measures from which to select in the tailoring of a screening policy.

Summary

Table A-4 in Appendix A contains a comprehensive list of preemployment screening measures for consideration in the design of a screening policy. However, the design of a preemployment screening program must take into account a number of complex occupational, psychometric and legal considerations, in addition to the insider risk issues affecting the specific organization involved.

TRAINING, EDUCATION AND PROGRAM EFFECTIVENESS

The section on Policies and Practices (page 12) described the need for policies and practices directly relevant to the mitigation of insider risk, as well as the importance of enforcement programs to ensure that these policies and practices are taken seriously and reinforced by organizational sanctions. This section on Training and Education and Evaluation of Training Effectiveness (TEE) examines the organization’s success at providing formal training and education regarding its policies and practices. It also assesses the extent to which the organization measures the effectiveness of education and training through direct evaluation of employee learning and skills, and the impact on the risk behaviors targeted in the education and training programs. The frequency with which these training and education programs are updated to take account of feedback on employee learning and risk behavior and to incorporate new information related to insider risks is also examined.

Initial Indoctrination

Often when employees join an organization they are simply referred to a policy and practice manual that provides guidance on rules governing the employee's interactions with fellow employees, the public, and employee resources, including IT. The previous section noted the potential increase in insider risk when policies and practices designed to prevent, deter, and aid in detection or manage insider risk are absent or unenforced. However, even if these policies and practices exist, they can be rendered ineffective if employees are not educated on their content and trained on their implementation. Active education and training regarding these policies and practices are vital to ensuring that employees:

- Are aware of these policies and practices and how they are implemented.
- Comprehend the reasons for these measures and their role in supporting the security and success of the organization.
- Understand the consequences should these guidelines be violated.
- Believe in management's determination to protect the organization through its enforcement of these guidelines.
- Support the implementation of these measures by participating in associated reporting and enforcement.

Support for the importance of training and education practices, especially security awareness programs, comes from studies on the relationship between these efforts and insider risk, computer abuse and general criminology research, and case studies and anecdotal reports. For example, Shaw and Fischer (2005) concluded that "a review of the recent history of insider cyber-crime and abuse shows that some of these damaging events could have been avoided by adequate security training, education, and awareness for employees having access to, or control over, critical information systems." In addition, it is a basic tenet of both general deterrence and rational choice theories of crime prevention that potential perpetrators must be aware of and believe in the speed and certainty of the consequences of their acts in order to be deterred or prevented from attempting these crimes (Phelps et al., 2007).

Security Awareness

Within general deterrence theory, Straub (1986; 1990) identified two principal factors likely to reduce the incidence of computer crime within an organization: (1) increases in the severity and certainty of deterrents and (2) the presence of software designed to prevent computer abuse. When they examined the separate and combined effectiveness of both preventative (such as password and access controls) and deterrent information security measures, Hoffer and Straub (1989) found that the combination of these measures significantly reduced computer abuse. Kankanhalli, Teo, Tan, and Wei (2003) also found that deterrent and preventative efforts, along with top management support, significantly improved on information security effectiveness. In the area of the application of rational choice theory to deter computer crime, Phelps et al. (2007) noted that when individuals consider committing an insider offense, their knowledge about the consequences of those actions plays into the decisionmaking process. These theoretical arguments for the importance of training and education programs are supported by findings from previous CERT studies indicating that 65% of insiders do not consider the possible negative consequences associated with carrying out their attacks (Randazzo et al., 2004).

Employees' failure to understand and acknowledge the constraints on their behavior and the consequences of their acts, as communicated by education and training programs, has been associated with a range of insider violations from misunderstanding about appropriate use to theft of intellectual property. According to another case consultation several years ago, a computer engineer in training at an army facility accessed private and commercial computers using a government system and downloaded files to official storage media (Shaw & Fischer, 2005). The audit trails suggested that the trainee was using the government server to store pirated game software and possibly pornography. When these unauthorized communications first came to light, the trainee's supervisor ordered him to offload unauthorized software from the server and hand over the disk to the network manager. Various agency files were lost or erased, possibly intentionally, in the process. The trainee who used the government computer for personal recreation and communications apparently believed mistakenly that free use of the system came with his position. This and other cases support the need for specific educational programs regarding rules and policies regarding IT use, in order to minimize unintentional and malicious insider activities. Often employees or temporary contract personnel are simply unaware of guidelines for the use of official systems and about technical countermeasures that either prevent abuse or identify the abuser.

Failure to ensure that employees are aware of their security obligations to protect proprietary information has contributed to serious losses in the past. In 1994, a Chinese national on the programming staff of Ellery Systems, a Boulder, CO, software firm working on advanced distributive computing software, transferred over the Internet the firm's entire proprietary source code to another Chinese national working in the Denver area. The software was then passed on to a Chinese company, Beijing Machinery. The code was highly sophisticated communications software for NASA that Ellery Systems was preparing to commercialize. The employee is alleged to have sold the code to Chinese interests for $550,000. Soon the firm lost its competitive advantage and was forced into bankruptcy. As described by its former CEO, 25 employees lost their jobs. Several million dollars of U.S. government investment were also lost. Due to the lack of adequate laws at the time covering the theft of intellectual property, the government was unable to prosecute the offenders. In addition, the government's case was weakened by the fact that the firm had not adequately advised its employees about the need to protect and control its proprietary information. [1]

Employee Responsibilities

In addition to informing employees in order to prevent or deter their violations, education and training programs can prevent insider misconduct by leading to early reporting of risk behaviors observed by other employees. For example, Keeney et al. (2005) found that in 61% of their insider cases, individuals from another area of the insider's life knew something of the insider's intentions, plans, or ongoing activities. In 31% of the incidents studied, there was some indication that the insider's plans were noticeable, such as stealing administrative-level passwords, copying information from a home computer onto the organization's system, and approaching a former coworker for help in changing financial data. In 35% of these incidents, the insider made plans, including discussions with competitors and coconspirators, or construction of a logic bomb on the organization's network. Stronger and more effective security awareness training may improve employee attention to, and reporting of, these pre-attack indicators.

Employees also need to know how to respond to suspicious behaviors directed toward them personally, including recruitment efforts or other forms of social engineering that constitute indicators of insecurity in the workplace (Wood & Marshall-Mies, 2003). Adversarial groups or foreign intelligence services are known to target vulnerable employees who for one reason or another are susceptible to cooption or compromise. This is one reason why initial employment screening should focus on personal vulnerabilities. Employees should also have some knowledge of how foreign and domestic adversarial groups operate: how they elicit privileged information from unsuspecting employees or engage in social engineering to obtain passwords and access codes for critical information systems.

Wood and Fischer (2002) have also argued that employees must be informed about appropriate action for dealing with the personal problems that have triggered security problems, such as, financial crises, alcohol abuse or mental and emotional problems, not only with regard to coworkers but to themselves. Most organizations provide confidential employee assistance programs that will, at no cost to the employee, offer initial counseling, short-term treatment, or referral services for employees undergoing a crisis.

Best practices in these critical policy and practice areas include the implementation of a carefully designed educational program for executives, supervisors, and members of the general workforce. In addition to inclusion of information security responsibilities on employment contracts, mentioned in Table A-5 (See Appendix A, page A-15), all employees need information about policies regarding workplace conduct, conditions of employment, and opportunities for employee assistance. It is

[1] This account of the case was obtained by Lynn F. Fischer during a personal interview in 1995 with the former proprietor of Ellery Systems.

also essential that no ambiguities exist in the minds of employees about acceptable and unacceptable usage of official or company-owned information systems or about an employee's responsibility for reporting illegal or inappropriate behaviors by coworkers.

Security managers who typically provide inhouse security training should ensure that all employees are informed about the requirement for maintaining the confidentiality of proprietary information and intellectual property. Failure to do this may result in loss of profit or a threat to national security. For organizations that have custody of U.S. government classified information, training and briefing requirements for cleared employees are established in the *National Industrial Security Program Manual* (NISPOM) and in several government regulations that address the safeguarding of government classified information and other critical assets. In addition, cleared employees are required to sign a nondisclosure agreement as part of their initial indoctrination and, in the Department of Defense, they must provide a verbal attestation that they have been briefed about and fully understand their responsibilities for safeguarding national security information.

Security and awareness training should also address special needs and requirements of employees, such as special threat advisories, advice and guidance prior to foreign travel or attendance at international conferences, and consultation prior to leaving an organization, known as a termination briefing. Each of these training actions by a security manager will review an employee's responsibilities for protecting critical information and assets and advise the individual about appropriate responses to situations in which he or she may be at risk.

It is also essential that employees are fully aware of security measures in place to protect the organization from adverse insider behavior, such as theft, computer system abuse or misuse, or illegal activities or transactions in the workplace. These measures may include monitoring of online behavior or telephone usage. Similarly, employees should be informed from the time of their initial employment about policies regarding discrimination, workplace violence, sexual harassment, and grievance procedures. Regrettably, in the past, organizational response to at-risk or threatening behaviors by uninformed disgruntled employees has led to damaging consequences (Shaw and Fischer, 2005). An effective and well planned educational program can be an effective deterrent to adverse insider behavior. There are a number of recommended best practices regarding the planning and implementation of such programs. One is that it should be a continuing effort using a variety of delivery methods tailored to the characteristics of the employee population (Roper, Grau & Fischer, 2006). Another is that it should be based on achieving specific performance objectives. The behavioral outcome of an educational program is that employees will avoid risky or illegal behaviors and do the right thing when confronted with potential security vulnerability.

Assessment of Training and Education

Lastly, it is beneficial for security educators to conduct a periodic review and assessment of the effectiveness of their educational and awareness strategies. There are a number of ways to assess the effectiveness of training and education: direct comments and feedback from employees, tracking the frequency of trends and security incidents, employee reporting, and voluntary participation in educational events (Roper, Grau & Fischer, Ch. 15, 2006). Also, training records of all activities should be maintained. Regardless of the level of success, due diligence requires that the security manager, on behalf of the organization, not allow errant employees the opportunity to claim that they were not advised about their custodial or security responsibilities.

Three relatively recent developments have raised the bar for training and education programs in both government and corporate settings. The implementation of Sarbanes-Oxley requirements in the financial sector and the Health Information Portability and Accountability Act (HIPAA) in government and private healthcare sectors created a need for training and education programs targeting every affected employee. These legislative initiatives led to the development of training and education programs requiring employees to learn and demonstrate competence in policies and practices governing information controls before they could function in their positions. The third development has been continuing innovation in employee monitoring (EM) technology, which is covered in more detail in the next section. Many of the EM systems deployed in corporations today include the potential to interact directly with users when they violate policies or wander into gray areas. The direct relevance of the violation to the employee’s work and the immediate provision of consequences, linked to tutorials or supervisory attention, offer a uniquely effective training opportunity, while cutting down on the need for less productive training classes. Individuals receive the educational resources they need based on their behavior. Another advantage of this approach is that these systems catch many of these violations before they are executed. By reducing the number of violations that security mangers and compliance officers are forced to record and evaluate, these systems allow personnel to pay greater attention to potentially higher-level risk behaviors. Records of these errors or violations across employees can also highlight areas for further efforts for security educators (Shaw & Wirth-Beaumont, 2006). Table A-5 (See Appendix A, page A-15) identifies topics that should be covered in a program of education and awareness for employees, in addition to the policy and practice areas described in the last section.

CONTINUING EVALUATION AND POLICY IMPLEMENTATION

The section on Training and Education and its Effectiveness on page 27 focuses on programs to prepare employees to deal with challenges associated with insider risks. This section addresses how these programs are implemented in the work environment with specific attention to how effectively they function.

Effective *continuing evaluation*, a central concept in personnel security, is based on the assumption that, however effective initial screening and security indoctrination may be, over time, trusted employees may become vulnerable to compromise or may not be able to deal with stress and frustrations in ways that ensure their trustworthiness. With few exceptions, for example, past espionage offenders were found to be fully worthy of government trust at the time of their first employment, but only later, sometimes for reasons they never fully comprehended, they succumbed to temptation or became embroiled in conspiracies hatched by other betrayers of trust.

For this reason, it is essential for organizations to adopt and implement reasonable risk-management policies and procedures for monitoring the workplace behaviors of trusted employees, whether it be reviews of audit trails, online usage and access, or compliance with security policies and guidelines. This is important since researchers have observed that in many cases a particularly egregious or damaging behavior is often preceded by adverse or at-risk acts of lesser seriousness that may reflect an employee's growing state of disgruntlement or desperation (Band et al., 2006). The recognition of precursor behaviors that might lead to something more damaging signals to management that it is time for intervention to address a problem, whether it takes the form of counseling, employee assistance program referral, intensified monitoring and supervision, or administrative action such as suspension or termination.

Depending on contextual risk factors discussed in pages 6 through 9, the level of external threat, and the sensitivity of information and assets possessed by an organization, its management must be concerned also with employee behavior and associations outside the workplace. Organizational policy may require the periodic repetition of initial screening actions conducted during hiring. These could include credit checks, criminal record checks, and Internet searches. The U.S. government, for example, currently requires full periodic reinvestigations every 5 years for all employees, military service members, and government contractor employees who hold a top secret security clearance. Continuing evaluation for any employee need not be intrusive or threatening; however, where indicators point to enhanced risk, it is incumbent upon management to respond in ways that will not intensify the risk.

Continuing evaluation goes hand in hand with, and is complemented by, programs that enhance security awareness and education (i.e., programs that clarify and define security responsibilities in the workplace, the importance of protecting organizational interests and assets, and which reinforce employee obligations to report security concerns to management and to security officials).

The most recent literature on insider activities, prior to and during seriously damaging behavior, indicates that improvements in employee monitoring linked to more systematic and thorough investigation and intervention could significantly reduce insider risk. For example, earlier sections have highlighted recent insider research findings indicating that:

- The risks presented by insiders contemplating or actually in the process of committing violations are often widely known among employees, family members and social contacts.
- Management is often not only unaware of these risks but also does not know that a subject is disgruntled.
- Management often fails to deal with signs of employee risk effectively causing the problem to escalate rather than resolve.
- Managers often fail to enforce existing policies covering risky behavior by employees (Shaw & Fischer, 2005).

The results of work by Randazzo et al. (2004) give strong support to the idea that improved reporting by peers, family, and social contacts could have prevented many insider attacks against corporate IT systems. Among their findings, which support the conclusion that prior adverse indicators should put these insiders on the risk radar screen before they escalate their adverse behaviors, are:

- Eighty percent of insider subjects raised official attention for concerning behaviors such as tardiness, truancy, arguments with coworkers, and poor job performance.
- In 97% of these cases, supervisors, coworkers, and subordinates were aware of these issues.
- In 37% of the total cases, the insiders' attack planning activity was noticeable by online (67%) or offline (11%) behavior, and, in some cases, both online and offline (22%) behavior.
- In 31% of the cases, others had specific information about the insiders' plans, intentions, and activities, including coworkers (64%), friends (21%), family members (14%) or someone else involved in the incident (14%).
- Fifty-eight percent of the insiders in this study communicated negative feelings, grievances, or an interest in causing harm to the organization—39% communicated negative feelings about the organization or an individual in that organization, or another individual, and 69% communicated these negative attitudes to someone outside the organization.
- In 20% of the cases, the insider made a direct threat to harm the organization, or an individual, to persons not directly involved in the issues.

Shaw and Fischer (2005) found that signs of disgruntlement in their subjects appeared from 1 to 48 months before the attack and that the time period prior to the attack—during which there were active problems requiring company intervention—ranged from 12 days to 19 months. These results indicate the existence of a window of opportunity during which employers' awareness of risk linked to effective interventions can reduce the threat of an attack. In addition, in about a third of these cases, the authors found that slowness in management awareness of employee disgruntlement could have expanded this window of opportunity by weeks and months.

As noted earlier, in eight out of 10 cases reviewed by Shaw and Fischer, management interventions were ineffective in preventing the insider attack and appeared to contribute to risk escalation. Lack of enforcement of a policy or practice covering an issue related to an insider's pre-attack behavior was also an organizational problem in eight of the 10 cases.

Table A-6 in Appendix A (page A-16) summarizes these concerns regarding an organization's ability to monitor, implement and enforce its policies related to insider risk into a series of questions for self-audit.

MANAGEMENT INTERVENTION: ASSESSMENT AND PLANNING

Research on insider threats supports assessing an employee's level of risk prior to initiating disciplinary action, including termination, or some other form of intervention. Studies of insider attacks consistently focus on the subject's perception of being wronged by the organization prior to insider misconduct. Within the academic literature, studies have linked perceived injustice to both sabotage (Crino, 1994; Crino & Leap, 1989; DiBattista, 1989, 1996; Neuman & Baron, 1997; Robinson & Bennett, 1997; Skarlicki & Folger, 1997; Sieh, 1987; Tucker, 1993) and theft (Greenberg, 1993).

A 2005 study, supporting the use of an evaluation of risk prior to a sanction-related intervention, found that 92% of insider cases were triggered by a specific event or a series of events (Keeney et al., 2005). These events included employment termination (47%), dispute with a current or former employer (20%), and employment related demotion or transfer (13%). Eighty-five percent of the insiders held a grievance prior to the incident, and in 92% of these cases, the insider's grievance was work-related. Fifty-seven percent of the insiders were perceived by others as disgruntled employees.

Similarly, Shaw and Fischer (2005) found that insider attacks were preceded by the subject's perception of experiencing stressors, including sanctions from the organization. In all but one of the cases examined, the attack was preceded by demotion, failure to receive a promotion, or termination. The authors also found that eight of their 10 subjects had experienced some type of management or human resources intervention for an interpersonal or IT problem prior to the attack, supporting the finding that subjects are engaged in a negative dynamic with their organizations prior to the incidents. The authors also reported that in eight cases, management interventions were ineffective and, in fact, contributed to the escalation of abuse. They concluded that these trends strongly argued for more careful assessment of risk and planning prior to interventions.

Findings of a high rate of conflict with management, including sanctions against the employee less serious than termination, support the need for a careful risk assessment prior to disciplinary action or decisions that violate important employee expectations, such as not receiving an expected promotion. However, evidence for the need for careful pretermination assessment of risk prior to the subject being terminated for cause is even more compelling. While only a small percentage of terminated employees return to attack their organizations, eight of 10 of the subjects in Shaw and Fischer's study attacked after termination. Termination was clearly an ineffective management intervention when it came to preventing insider attacks.

More recent data from CERT (Cappelli & Moore, 2008) support the need for careful risk assessments prior to management interventions but also highlight the need for careful risk assessment and planning around terminations, even when the subject resigns voluntarily. For example, CERT has extended its research to subjects who steal or modify data for financial gain or steal data for business advantage. Known issues for persons convicted of theft or data modification for financial gain included a perceived hostile work environment, problems with supervisors, and expected layoffs. Among employees who engaged in theft for business advantage, 71% stole intellectual property. Ninety-five percent of these subjects resigned before or after the theft, and 68% of subjects stole information within 3 weeks of their resignation. Work issues that contributed to the theft reportedly included disagreements over ownership of intellectual property, compensation, relocation, being passed over for promotion, layoffs, and problems with a supervisor. This last finding strongly indicates that a review of an employee's access and copying or transfer of information just prior to, or immediately after, giving notice could reveal and prevent damage from this form of insider action.

Numerous case examples illustrate the need for careful assessments prior to serious interventions, as well as for accompanying termination planning (Shaw, 2006). The case of "Bill" from Shaw and Fischer (2005) is a good example of the importance of a preintervention assessment. Prior to a careful assessment of risk involving a computer engineer responsible for the safety controls at a petroleum processing plant, the engineer had got into a physical confrontation at work, refused to give anyone a copy of the password to the safety control systems, and reportedly burned an effigy of his supervisor, which he then riddled with bullets from his Kalashnikov assault rifle modified to handle a 30-round magazine automatically. This subject's refusal to supply the password to the safety control systems, as well as his efforts at sabotage to make his supervisor look bad while he was on suspension, were examples of escalations despite management interventions. The company involved was fearful of terminating this employee because of the potential for violence and called in an outside psychological risk consultant to help its interdisciplinary team assess and manage this employee. After careful assessment, a plan was developed to attempt to address the employee's concerns and to help him manage his emotions and behavior. The plan involved medical assistance for the employee and his wife (who had terminal cancer and was actively suicidal), placing him on paid leave, efforts at rehabilitation by the employee assistance program, and ongoing therapy and evaluation. The plan eventually led to the employee's termination but is credited with avoiding the very serious risk of additional sabotage and violence that abrupt termination probably would have provoked.

A recent case in the legal system involves allegations against a computer engineer at an Intel facility in Hudson, NY, who gave notice of his intention to resign in May, 2008. (Bray, 2008). Biswahoman Pani allegedly told his supervisor that he would be resigning effective June 11th but would be on vacation from May 29th until that date. Unknown to the company, Pani began working with a rival company on June 2nd and used his access to Intel's computer system to download sensitive documents with valuable competitive intelligence. Only after an Intel employee learned of Pani's employment with the new company was the FBI called in and Pani's computer access checked. This case supports the argument made above by the CERT data for routine assessment of theft risk when a critical employee with access to valuable information gives notice, particularly if he, like Pani, has shown signs of disgruntlement. The case also emphasizes the need for careful monitoring of access and auditing of employee use of systems prior to and after notice is given.

Assessment Resources

In order to complete the recommended assessment of an at-risk employee, the organization must have the resources and procedures in place to refer employees, review records, conduct interviews to evaluate risk, and plan and institute recommendations. Critical capabilities to fulfill these tasks include:

- Policies and procedures for identifying employees for referral for risk assessment.
- A risk assessment methodology for insider and other related risks such as violence, on which an established team is trained.
- Back-up personnel in specialized fields such as psychology, law, and personnel investigations (depending on the organization's capabilities).
- Team membership on call representing Human Resources, Legal, Employee Assistance, Physical and IT Security, Operations, and persons with supervisory experience with the employee.

These personnel must be in a position to review the employee's history and background within and, as needed, outside the organization (history of risk factors such as previous arrests, alcohol-related problems, debt, recent stressors such as divorce, medical problems, etc.) in order to advise management on the employee's likely reaction to the proposed action, whether it is a demotion, transfer, termination or other actions. In particular, the team must be able to assess the risk of the intervention increasing the likelihood of a serious negative consequence such as sabotage, espionage, theft of information, or violence. If this is the case, the team needs to be able to recommend strategies to reduce this risk, deter it, or provide safeguards against these consequences. The team will need to be in a position to formulate creative interventions that address their concerns regarding the specific risks posed by an individual, so it is critical that a broad range of organizational professionals be involved and present. In addition, because not all risks can be avoided, the team will need to be in contact with law enforcement, judicial and other authorities if a risk of serious property damage or personnel injury is possible. Table A-7 in Appendix A (page A-17) presents a number of audit questions pointing to best practices for a risk mitigation plan.

CONCLUSION

The good news from several empirical studies of the development of insider cases over time across multiple types of organizations is that many of the employees who have the potential to commit damaging acts are already on the radar of their human resource and Security offices for displaying counterproductive interpersonal or technical behaviors (Randazzo et al., 2004; Keeney et al., 2005; Shaw & Fischer, 2005; Band et al., 2006). Therefore, more effective organizational efforts to detect and manage insider risk may produce more secure workplaces.

This technical report is based on empirical reviews of subjects' interactions with their organization with the goal of producing a practical framework or management tool to help concerned security, human resource and other supervisory personnel improve their organization's chances of intervening with at-risk employees more effectively. The evaluation and audit questions found in the appendix are based on data from hundreds of insiders. In the process of answering any of the self-evaluation and audit questions for an organization or applying any of the best practices to which they point, a security manager should also keep in mind the following questions: How likely is it that existing preemployment screening measures would keep a risky employee out of the workforce? How soon would management know if an employee was receiving preferential treatment from a supervisor, allowing him to violate an important human resource or security policy? Would current policies regarding intervention for an at-risk employee reduce or escalate the risk of an insider attack? If a key technical employee had started collecting proprietary information just before giving his termination notice, would this be detected?

PRACTICAL APPLICATION

We recommend that Security, Human Resources, Legal, Management and other personnel use this self-audit approach to assess the extent to which their organization is:

- Aware of contextual factors in the environment that can increase insider risk.
- Aware of the potential contributions of recruitment processes to insider risk.
- Collecting information during the screening process on candidate characteristics that may produce insights into, or reduce, insider risk.
- Using information from the screening process to reduce insider risk by rejecting a candidate, modifying his or her assignment, monitoring performance, or using this information to make subsequent decisions on how to manage an employee when behaviors of concern arise related to insider risk.
- Equipped with policies and practices that contribute to the prevention, detection, and successful management of insider risk.
- Successful in educating and training employees at all levels on the content and processes associated with these policies and practices.

- Successful at monitoring and enforcing compliance with these policies and practices.
- Able to assess the risk associated with important employment events such as demotion, termination or other negative outcomes for an employee, and able to act to reduce the risk of insider violations associated with these events.

In addition, we believe that a more complete overview of organizational insider risks resulting from this self-audit approach can be helpful in a number of other important personnel security decisions. For example, each user may wish to assign relative scores to the strength or weakness of his or her insider risk mitigation capabilities for each component of this assessment (such as High, Medium or Low Risk). An organization such as a Department of Defense element requiring a facility clearance may receive a low score on risks resulting from lack of employee screening. On the other hand, this element may receive relatively higher risk scores for its employee monitoring and security awareness efforts, depending on their implementation and effectiveness. With this assessment of an organization's relative strengths and weaknesses in mitigating insider risk in hand, it should be easier to make important personnel decisions on both a strategic level and individual level. For example, the Department of Defense element above is very dependent on employee screening derived from background investigations for federal security clearances. However, if this organization is operating in one of many regions of the world where it is difficult to perform even basic background checks on employees, its strongest protection against insider risk may be degraded. The results of the insider risk evaluation tool can then help security personnel understand that their monitoring and security awareness programs may need improvement to compensate for the degradation of their strongest insider personnel security protection asset in the new environment.

The same approach can also be applied to the design of insider risk mitigation plans for individual employees. For example, risk assessment results may be useful in a number of ways in the case of a current employee who has displayed a "concerning" behavior indicative of increased risk, such as an IT security violation or an altercation with his supervisor, and who now requires an insider risk evaluation. The results of the assessment, for example, may identify data the investigator may or may not have within the organization's databases. Examples of such information directly relevant to the investigation could include:

- Data on the recruitment channels through which this employee entered the organization, as it may affect his internal social network and the odds that he or she may be involved in policy violations with others, or that the person has received special treatment due to his relationship with a referring employee.
- Information from the background data gathered on the employee during his or her hiring and screening process.

- Data not available on this individual as a result of gaps in the background and screening process that may have to be obtained to make a decision regarding his or her insider risk potential.
- Information verifying that the employee was informed of the relevant policies and practices he or she violated and agreed to abide by these rules in the employment contract or security awareness training.
- The availability of personnel records for this employee, including reports of previous problems understanding and adhering to policies and practices, getting along with coworkers or previous supervisors, etc.
- The availability of logs and other monitoring channels that will help an investigator assess the scope of the employee's activities on the network or his or her communications with others within and outside the organization.

After the investigation and the design of a risk mitigation strategy using these data, the same information can be used to plan for any potential reactions the employee may have to implementation of the plan. If the employee is being terminated, is his access also being analyzed and blocked? If the employee is being disciplined but remaining in the organization, what types of counterproductive work behaviors can be anticipated as he reacts to the bad news? Do the insider risk assessment results indicate that the organization is protected from these acts or do new measures need to be instituted?

CONTINUING EFFORTS

This endeavor attempts to sensitize concerned personnel to their influence over the emergence and escalation of insider risk. The evaluation and audit questions identify potential gaps in organizational capabilities to influence the insider process, and suggest ways these gaps can be addressed to improve insider personnel security.

In future efforts we hope to improve the usefulness of this methodology in several ways, including:

- Inclusion of more specific and detailed questions that can make the risk assessment even more useful.
- Modification of questions for different types of organizations performing in different environments.
- Addition of more positive, mitigating efforts by an organization that can provide a more realistic and reliable evaluation of insider risk.
- Inclusion of a section characterizing the organization's insider risk history so that the baseline frequency of insider incidents can contribute to more realistic risk predictions.
- Restructuring of the evaluation questions so that weights can be assigned to the answers to deliver actual risk scores by evaluation section. These additions

would also allow users to measure changes in their insider risk mitigation capabilities.

REFERENCES

American Psychiatric Association. (1994). *Diagnostic and statistical manual of mental disorders*, 4th Ed. Washington, DC: Author.

Americans with Disabilities Act of 1990, 42 U.S.C. § 12101 et seq.

Band, S.R., Cappelli, D.M., Fischer, L.F., Moore, A.P., Shaw, E.D., & Trezciek, R.F. (2006). *Comparing insider IT sabotage and espionage: A model-based approach* (CMU/SEI-2006-TR-026). Pittsburg, PA: Carnegie Mellon, Software Engineering Institute.

Bray, H. (2008). Ex-Intel worker accused in theft. Boston Globe. Retrieved September 12 2008, from http://www.boston.com/business/articles/2008/09/12/ex_intel_worker_accused_in_theft/

Calmes, J. (2008). Retrieved on September 22, 2008, from http://www.nytimes.com/2008/11/13/us/politics/13apply.html?_r=1&bl&ex=1226725200&en=8493bad0556dcca4&ei=5087%0A&oref=slogin

Cappelli, D.M., & Moore, A.P. (2008). Risk mitigation strategies: Lessons learned from actual insider attacks. Paper presented at RSA Conference April 9, 2008, Session DEF-203, San Francisco, CA.

Cappelli, D.M., Moore, A.P., Phelps, D., Shaw, E.D., & Trzeciak, R.F. (2007). *Research methodology for the CERT insider threat project: Modeling human behavior in cyberspace* (FOUO). Pittsburg, PA: CERT Program, Survivable Enterprise Management, Carnegie Mellon University.

Computer Science Institute. (2007, September 14). CSI computer crime and security survey shows average cyber-losses jumping after five-year decline. Press release. San Francisco: Author.

Crino, M.D. (1994). Employee sabotage: A random or preventable phenomenon? *Journal of Managerial Issues, 6*, 311–330.

Crino, M.D., & Leap, T.L. (1989). What HR managers must know about employee sabotage. *Personnel, 14*, 31–38.

DiBattista, R.A. (1989, December). Designing a program to manage the risk of sabotage. *Supervision*, 6–8.

DiBattista, R.A. (1996). Forecasting sabotage events in the workplace. *Public Personnel Management, 25*, 41–52.

Director of Central Intelligence, Community Research Center. (n.d.). *Personality characteristics of convicted espionage offenders. A Slammer Psychology Team Technical Report* (FOUO).

REFERENCES

Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681 et seq.

Greenberg, J. (1993). Stealing in the name of justice: Informational and interpersonal moderators of theft reactions to underpayment inequity. *Organizational Behavior and Human Decision Processes, 54*, 81–103.

Herbig, K.L. (2008) *Allegiance in a time of globalization* (PERS-TR-08-10). Monterey, CA: Defense Personnel Security Research Center.

Hoffer, J.A., & Straub, D.W. (1989). The 9 to 5 underground: Are you policing computer crimes? *MIT Sloan Management Review, 30*, 35-43.

Hough, L. M. (1992). The "Big Five" personality variables—construct confusion: Description versus prediction. *Human Performance, 5,* 139–155.

International Organization for Standardization 27002 2005. (2007). *Information security standard.* Geneva, Switzerland: Author.

Joy, D.S. (1999). Basic psychometric properties of a pre-employment honesty test: Reliability, validity and fairness. In J. Jones (Ed.), *Pre-employment honesty testing: Current research and future directions.* Westport, CT: Greenwood Publishing.

Kankanhalli, A., Teo, H.-H., Tan, B. C. Y., & Wei, K.-K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management, 23,* 139-154.

Keeney, M.M., Kowalski, E.F., Cappelli, D.M., Moore, A.P., Shimeall, T.J., & Rogers, S.N. (2005). Insider threat study: Computer system sabotage in critical infrastructure sectors. *Joint SEI and U.S. Secret Service Report.* Retrieved from http://www.cert.org/archive/pdf/insidercross051105.pdf

Krofcheck, J.L., & Gelles, M.G. (2005). *Behavior consultation in personnel security: Training and reference manual for personnel security professionals* (Rev. ed.). New York: Yarrow Press.

Lynam, D.R., & Widiger, T.A. (2001). Using the five-factor model to represent the DSM-IV personality disorders: An expert consensus approach. *Journal of Abnormal Psychology, 110,* 401-412.

McCrae, R.R., Yang, J., Costa, P.T., Dai, X., Yao, S., Cai, T., et al. (2001). Personality profiles and the prediction of categorical personality disorders. *Journal of Personality, 69,* 155-174.

Mount, M., Ilies, R., & Johnson, E. (2006). Relationship of personality traits and counterproductive work behaviors: The mediating effects of job satisfaction. *Personnel Psychology, 59,* 591-622.

Neuman, J.H., & Baron, R.A. (1997). Aggression in the workplace. In R. Giacalone & J. Greenberg (Eds.), *Antisocial behavior in organizations* (pp. 37–67). London: Sage.

O'Connor, B.P., & Dyce, J.A. (2001). Rigid and extreme : A geometric representation of personality disorders in five-factor model space. *Journal of Personality and Social Psychology, 81*(6), 1119-1130.

Phelps, D., Cappelli, D.M., Moore, A.P., Shaw, E.D., & Trzeciak, R.F. (2007). Research methodology for the CERT insider threat project: Modeling human behavior in cyberspace (FOUO). Pittsburg, PA: CERT Program, Survivable Enterprise Management, Carnegie Mellon University.

Randazzo, M.R., Keeney, M.M., Kowalski, E.F., Cappelli, D.M., & Moore, A.P. (2004). Insider threat study: Illicit cyber activity in the banking and finance sector. *Joint SEI and U.S. Secret Service Report*. Retrieved from http://www.cert.org/archive/pdf/bankfin040820.pdf

Robinson, S.L., & Bennett, R.J. (1997). Workplace deviance: Its definition, its nature, and its causes. In R.J. Lewicki, B.H. Sheppard, & R.J. Bies (Eds.), *Research on negotiation in organizations* (pp. 3–28). Greenwich, CT: JAI Press.

Rolland, J.P., & De Fruyt, F.D. (2003). The validity of FFM personality dimensions and maladaptive traits to predict negative effects at work: A six-month prospective study in a military sample. *European Journal of Personality, 17*(S1), S101-S121.

Roper, C.A., Grau, J.A., & Fischer, L.F. (2006). *Security education, awareness and training: From theory to practice.* Burlington, MA: Elsevier.

Sackett, P.R. (2002). The structure of counterproductive work behaviors: Dimensionality and relationships with facets of job performance. *International Journal of Selection and Assessment, 10*(1), 5-11.

Salgado, J.F. (2002). The big five personality dimensions and counterproductive behaviors. *International Journal of Selection and Assessment, 10,* 117-125.

Shaw, E.D. (2006). The role of behavioral research and profiling in malicious cyber insider investigations: Digital investigation. *The International Journal of Digital Forensics and Incident Response*, *3*, 20-31. Exeter, UK: Elsevier.

Shaw, E.D., & Fischer, L.F. (2005). *Ten tales of betrayal: The threat to corporate infrastructures by information technology insiders: Analysis and observations.* Monterey, CA: Defense Personnel Security Research Center.

Shaw, E.D., Post, J.M., & Ruby, K. (1999). Profiling the dangerous IT professional. *Security Management. 3*(12).

REFERENCES

Shaw, E.D., & Stroz, E. (2004). WarmTouch software: Assessing friend, foe and relationship. In T. Parker (Ed.), *Cyber adversary characterization: Auditing the hacker mind.* Rockland, MA: Syngress.

Shaw, E.D., & Wirth-Beaumont, E. (2006). *A survey of innovative approaches to IT insider prevention, detection, and management.* Monterey, CA: Defense Personnel Security Research Center.

Sieh, E.W. (1987). Garment workers: Perceptions of inequity and employee theft. *British Journal of Criminology, 27,* 174–191.

Skarlicki, D.P., & Folger, R. (1997). Retaliation in the workplace: The roles of distributive, procedural, and interactional justice. *Journal of Applied Psychology, 82*, 434–443.

Software Engineering Institute, Carnegie Mellon. (2006). *Comparing insider IT sabotage and espionage: A model-based approach* (CMU/SEI-2006-TR-026). Pittsburg, PA: Author.

Straub, D.W. (1986). Controlling computer abuse: An empirical study of effective security countermeasures. Unpublished doctoral dissertation, Indiana University, Bloomington, IN.

Straub, D.W. (1990). Effective is security: An empirical study. *Information Systems Research, 1,* 255-276.

Tucker, J. (1993). Everyday forms of employee resistance. *Sociological Forum, 8*, 25–45.

VTZ Law Blog. (2008). Retrieved September 22, 2008, from http://www.vtzlawblog.com/2008/03/articles/employment-policies/approach-with-caution-conducting-background-checks-using-facebook-myspace-or-the-internet/

Westen, D., & Shedler, J. (1999a). Revising and assessing Axis II, Part I: Developing a clinically and empirically valid assessment method. *American Journal of Psychiatry*, 156, 258-272.

Westen, D., & Shedler, J. (1999b). Revising and assessing Axis II, Part II: Toward an empirically based and clinically useful classification of personality disorders. *American Journal of Psychiatry*, 156, 273-285.

Widiger, T.A., & Costa, P.T. (1994). Personality and personality disorders. *Journal of Abnormal Psychology, 103,* 78-91.

Wood, S., & Fischer, L.F. (2002). *Cleared DoD employees at risk – Report 1: Policy options for removing barriers to seeking help.* Monterey, CA: Defense Personnel Security Research Center.

Wood, S., & Marshall-Mies, J.C. (2003). *Improving supervisor and coworker reporting of information of security concern* (PERS-TR-02-3). Monterey, CA: Defense Personnel Security Research Center.

OTHER SOURCES CONSULTED

American Association of Motor Vehicle Administrators (AAMVA). (n.d.). *AAMVA fraudulent document recognition training: Model training program.* Arlington, VA: Author.

American Association of Motor Vehicle Administrators (AAMVA). (2004). *AAMVA DL/ID security framework.* Arlington, VA: Author.

American Society of Industrial Security SIS GDL PBS 09. (2006). Preemployment background screening guideline. Retrieved March 25, 2008, from http://www.asisonline.org/guidelines/guidelinespreemploy.pdf

Baker v. Director, 39 Ark. App. 5, 6, 832 S.W.2d 864, 865 (1992).

Buck, K.R., & Rose, A.E. (2004). *Crime and self-reporting: Phase I.* Monterey, CA: Defense Personnel Security Research Center.

Buck, K.R., & Rose, A.E. (2005). *Screening for potential terrorists in the enlisted military accession process.* Monterey, CA: Defense Personnel Security Research Center.

Buck, K.R., Rose, A.E., & Richmond, D.A. (in press). *FIPS 201 Part 1 Identity proofing implementation options.* Monterey, CA: Defense Personnel Security Research Center.

Center for the Protection of National Infrastructure (CPNI). (2007). Personnel security: Threats, challenges, and measures. Retrieved March 31, 2008, from http://www.cpni.gov.uk/Docs/Pers_Sec_TCM_v2.pdf

Chandler, C.J., & Jung, C.L. (2007). *Evaluation of ACES business rules for identifying counterintelligence issues* (FOUO). Monterey, CA: Defense Personnel Security Research Center.

Department of Defense. (2000). DoD insider threat mitigation: Final report of the Insider Threat Integrated Process Team. Falls Church, VA: Information Assurance Technology Analysis Center.

Department of State - 25. (n.d.). Overseas records. Retrieved April 14, 2008, from http://www.state.gov/documents/organization/102788.pdf

DiBattista, R.A. (1991). Creating new approaches to recognize and deter sabotage. *Public Personnel Management, 20*, 347–352.

Dubin, J. (2005). *The little black book of computer security.* Loveland, CO: Penton Technology Media.

Federal Trade Commission. (n.d.). Avoid fake-degree burns by researching academic credentials. Retrieved April 14, 2008, from http://www.ftc.gov/bcp/conline/pubs/buspubs/diplomamills.shtm

Heuer, R.J. (2000). *Adjudicative desk reference*. Monterey, CA: Defense Personnel Security Research Center.

Heuer, R.J., & Condo, J.L. (2006). *Summary and explanation of changes to the adjudication guidelines approved by the President December 29, 2005.* Monterey, CA: Defense Personnel Security Research Center.

Kramen, A.J., Massey, K.R., & Timm, H.W. (2000). *Guide for preventing and responding to school violence.* Monterey, CA: Defense Personnel Security Research Center.

Kramer, L.A., Heuer, R.J., Jung, C.L., Gonzales, J.L., & Richmond, D.A. (2007). *Security issues of CI concern in DoD background investigations* (FOUO). Monterey, CA: Defense Personnel Security Research Center.

Kramer, L.A., Heuer, R.J., & Crawford, K.S. (2005). *Technological, social, and economic trends that are increasing U.S. vulnerability to insider espionage.* Monterey, CA: Defense Personnel Security Research Center.

Quandt, S. (2006). *The insider threat benchmark report: Strategies for data protection.* Boston, MA: Aberdeen Group. Retrieved March 24, 2008, from http://www.techworld.com/cmsdata/whitepapers/3454/Apani_Aberdeen_Insider_Benchmark.pdf

Rose, A.E., & Buck, K.R. (2004). *Crime and self-reporting: Phase II* (FOUO). Monterey, CA: Defense Personnel Security Research Center.

Rose, A.E., & Buck, K.R. (2007). *Fraudulent document recognition training for the Department of Defense community*. Monterey, CA: Defense Personnel Security Research Center.

Shaw, E.D., & Fischer, L.F. (2005). *Ten tales of betrayal: Attacks on corporate infrastructure by information technology insiders*, *Vol. 2, Case Studies* (FOUO). Monterey, CA: Defense Personnel Security Research Center.

Timm, H.W., Buck, K.R., & Chandler, C.J. (2004). *Information discovered during Automated Continuing Evaluation System database checks of interest to counterintelligence units* (FOUO). Monterey, CA: Defense Personnel Security Research Center.

Timm, H.W., & Chandler, C.J. (1996). *Combating workplace violence: Guidelines for employers and law enforcement.* Monterey, CA: Defense Personnel Security Research Center.

Youpa, D.G., Carney, R.M., Wiskoff, M.F., & Tippit, J.D. (2000). *Review of private sector personnel screening practices.* Monterey, CA: Defense Personnel Security Research Center.

APPENDIX A:

RISK EVALUATION

OVERVIEW OF ASSESSMENT METHOD PROTOTYPE

Based on the rationale described in the text of the main report, the following assessment framework is designed to help users gauge their organization's relative vulnerability to insider threats. As noted in the report, the authors have distilled empirical analysis of a relatively large number of insider cases, academic research, and organizational consultations on insider challenges into a series of lessons learned. These data were subjected to a series of systems dynamics exercises with multidisciplinary experts in which personal characteristics and modus operandi of actual insiders were matched against organizational capabilities to prevent, deter, detect, and manage insider risk in post-hoc as well as prospective case reviews. This methodology is described in greater detail in Band et al. (2006).

One of the conclusions from this analysis and these exercises was that an organization's ability to mitigate insider threats is synergistic across many of its personnel and technical management capabilities. Organizations that employ effective recruitment, screening and socialization methods and perform continuing evaluations of employees, especially after behaviors indicative of insider risk are observed, are better positioned to mitigate insider risk. In addition, organizations that effectively communicate, monitor, and enforce their insider-related policies are more likely to prevent, detect, deter, and effectively manage insider risk. Not only did the absence of these capabilities diminish an organization's ability to reduce insider risk, but risk was exacerbated. In many of the cases studied, the organization's relatively uninformed interventions escalated insider risk.

Finally, an organization's environment and reputation can significantly influence insider risk. Yet in the literature on insider threats the organization's context has been relatively neglected. Thus the combination of cultural, political, military, economic, sector, competitive forces and stressors faced by an organization feature in our assessment of the magnitude of the insider risk an organization currently faces.

Based on these findings and assumptions, this prototype takes the user through the seven organizational components displayed Figure 1 from the text of the report. The user is asked to evaluate the insider risk his or her organization may face due to contextual factors. The more significant these contextual stressors, the greater the pressure on internal organizational mechanisms for risk reduction. As mentioned in the report, contextual factors in our assessment scheme act as force multipliers. The greater these contextual pressures, the more the insider risk.

The next step requires the user to identify the presence and effectiveness of insider risk mitigation measures. The greater the number of internal organizational mechanisms for risk prevention, deterrence, detection, and management, the less insider risk occurs in the organization. These mitigation mechanisms are explained in detail in the report.

CONTEXTUAL ORGANIZATIONAL ISSUES

Table A-1 poses a series of questions designed to sensitize users to the risks their organizations face from these contextual issues. Multiple positive responses to any of these questions mean that the user's organization is more vulnerable to the specific organizational risk issues contained in subsequent sections. This indicates that in any strategic plan to mitigate adverse insider behavior, additional policies or safeguards are warranted.

Table A-1
Contextual Organizational Risk Issues

Type of Risk	***Factors that May Magnify Insider Risk***
Cultural	Does your organization have branches, suppliers, subcontractors or other affiliates abroad where differences in cultural beliefs and values may affect loyalty to the organization versus other local groups? Does your organization have branches, suppliers, subcontractors or other affiliates abroad where differences in language, cultural beliefs and values can complicate communication and lead to conflicts?
Political	Does your organization have branches, employees, suppliers, subcontractors or other affiliates with access to your resources or information in areas where there is intensive social, political or military conflict that may result in increased insider risk?
General economic	Is your organization currently suffering from general economic forces that place unusual financial stress on employees? Is your organization currently affected by economic or financial stressors that influence its treatment of employees in a manner that could increase insider risk such as, reduced benefits, stock options, retirement contributions or other incentives for loyalty?
Sector-specific	Is your organization affected by specific sector stressors that place economic or competitive pressures on employees?
Organization-specific	Is there anything about your organization's function, affiliation, reputation, competitive environment, adversaries or other characteristics that would increase pressures on employees, resulting in greater insider risk?

POLICIES AND PRACTICES TO MITIGATE INSIDER RISK

Table A-2 is a checklist of specific policy and practice areas that should be covered within an organization's basic governance structures. Not all policy areas may apply to an organization. However, it is not enough to have excellent policies on the book; employee must be informed of their meaning and how they may affect their working relationships and behaviors. Policy and practice guidelines must be clearly documented and easily accessible to employees and be the subject of education and training programs.

Table A-2
Policy and Practice

Audit Questions
Does your organization have policies facilitating preemployment screening?
• Information gathered to evaluate suitability of job candidates
Does your organization have policies that protect the security of organizational information and IT resources?
• Job descriptions and employee contracts include descriptions of information security responsibilities including implementing and maintaining policies, and protecting organizational assets scaled for each employee position • Email, network, website and databases are protected by relevant policies and practices • Incident Management Recovery • Access controls and change management, configuration control, logging, auditing, monitoring • Routine probationary monitoring of new users • Specialized monitoring of system administrators and other "super users" • Policies and practices addressing the risks and consequences of inadvertent damage or losses, including records of these losses
Does your organization have policies that allow for an employment probationary period with increased monitoring for new hires?
• Policies and practices exist to allow new hires to be monitored closely for insider security risks during an initial period of performance ▪ Closely examine technical and interpersonal behaviors for a probationary period
Does your organization have policies protecting the physical security of facilities?
• Facility access and egress of persons, information and property
Does your organization have policies that limit employee use of property for non-work reasons and establish boundaries between personal and professional activities that utilize work time and resources?
• Rules governing employee and others access to, use, distribution of organization assets and personal activities on work time (surfing the web, personal appointments, etc.).
Does your organization have clearly defined policies regarding the ownership and sharing of organization intellectual property?
• Rules describing organization and employee rights to intellectual property • Procedures for answering questions regarding ownership and benefits from IP • Contingencies for rule violations
Does your organization have policies and practices for disaster recovery that may deter insider actions?
Does your organization have policies regarding outside business involvements and contacts and the reporting of these contacts?
• Rules governing permissible employee business or consulting relationships and information sharing • Procedures for reporting relationships, resolving ambiguities, and contingencies for rule violations • Agreements covering disclosure of information, competition after leaving the organization, operation of side businesses, etc.
Does your organization have policies that define the privacy of employee, customer, client and other sensitive personal information?
• Rules governing the protection and permissible release of employee, customer, client information, especially sensitive personal information • Organizational rules for the implementation of state and federal privacy mandates such as HIPAA, Sarbannes-Oxley (Sox), other regulations regarding possible violations of privacy protections
Does your organization have guidelines describing the organizations right to monitor and audit employee activity on proprietary systems as well as their interpersonal behavior?
• Rules and procedures are established, described and acknowledged by employees as a condition of employment or access to resources such that there are no legal impediments to

Audit Questions

monitoring or actions taken based on results

- Do these policies and practices allow for intensified monitoring of individuals when violations or other risky actions indicate the need for more effective monitoring?
- Does your organization have means to collect and record adversary efforts to recruit or compromise employees?
- Are there policies allowing for intensified monitoring of individuals with mental health, alcohol, substance abuse or other personal problems who are and are not in treatment for these concerns?

Does your organization have policies describing how employees report grievances and their own and others' risk behaviors?

- Procedures exist for employees to report grievances, problems and concerns about themselves and others and for investigating and reacting to these reports in a manner that promotes social justice within the organization
  - Protections against false reports, retaliation for reports, penalties for nonreporting of serious security issues

Does your organization have policies describing unacceptable workplace interpersonal behaviors?

- Guidelines exist covering illegal and disruptive interpersonal behaviors, reporting these behaviors and resulting contingencies for investigating and reacting to these reports.
  - Reports of: violence and threats
  - Sexual harassment
  - Online behavior
  - Equal Employment Opportunity rules
  - Attendance
  - Vacation and leave
  - Drug and alcohol use
  - Weapons
  - Dress and hygiene
  - Fraternization and relationships at work
  - Interpersonal respect
  - Conflict resolution, etc.

Does your organization have policies describing how to identify and respond to at-risk employees?

- Guidelines for recognizing and addressing signs or symptoms that an employee is:
  - Experiencing stress
  - Engaged in interpersonal conflict
  - Guilty of technical violations
  - Susceptible to social engineering
  - Other signs that he may be at risk for insider violations

Does your organization have policies and practices designed to improve loyalty and reduce the risk of insider activity as well as reporting of risky behavior?

- Stock options
- Rewards for periods without security violations
- Rewards for ideas to improve security

Does your organization have clear policies describing how employee benefits and compensation are obtained and changed?

- Policies for determining benefits and pay are clearly outlined
- Criteria and procedures for changes in pay and benefits are fair and clear

Does your organization have clear policies describing how employee evaluation and advancement are accomplished?

- The manner in which employee performance is evaluated and related to pay, promotion, privileges, benefits, and consequences, etc. are clearly described

Does your organization have clear procedures describing access to and benefits of employee assistance programs and other employee support services?

- Services, policies and procedures to assist employees and their families with personal, psychological, financial, legal and other stressors which have been related to insider risk are in place and accessible to employees, including provisions for privacy, voluntary and involuntary referral and referrals by others

Audit Questions
Does your organization have a good conduct policy?
• Policies exist that allow employees to be terminated for legal violations or behavior that damages the reputation of the organization
Do your organizational policies and practices extend to trusted partners?
• These important policies and practices related to insider risk are applied in appropriate or parallel form to all personnel working with the organization, including contractors, subcontractors, temporary employees, clients and customers who utilize shared resources, etc.
Does your organization have policies and practices mandating security awareness training?
• Is this training tailored for the specific risks and adversaries faced by your organization?

RECRUITMENT METHODS INFLUENCING INSIDER RISK

Table A-3 organizes recruitment concerns into a series of questions to be addressed during an insider risk audit. The greater the number of positive responses to these questions, the greater the potential risk of vulnerability to insider problems from recruitment practices and the greater the corresponding need for awareness of these risks and potential countermeasures. While individual responses to these questions are designed to highlight possible risk areas, the audit results are also designed to be cumulative, allowing users to evaluate their overall risk to insider threat activities.

Table A-3
Recruitment Methods

Audit Questions
Does your organization utilize the services of head hunters, recruitment firms or other placement groups?
• To what extent do you rely on these service providers to screen candidates for risk factors associated with insider violations?
• To what extent do you validate or supplement screening conducted by these providers?
• What is the attrition of employees recruited in this manner compared to those recruited by other means?
• Have employees recruited in this manner been implicated in policy or legal violations or other insider acts?
Does your organization encourage employees to facilitate recruitment and hiring through the payment of a bounty?
• Are there any restrictions on the eligibility of bounty candidates according to their social or family relationship with the employee?
• Are there any restrictions on the eligibility of candidates based on the history of behaviors of concern or risk presented by the person referring the candidate?
• Are there any restrictions on where the recruited employee may serve within the organization in relation to the recruiting employee's position?
• What is the attrition of bounty-recruited employees versus employees recruited by other means?
• Have employees recruited in this manner been associated with insider violations or risks?
Does your organization allow the hiring of candidates related to current or former employees?
• Are there any restrictions on the positions in which these employees may serve in relation to their employee relatives?
• Are there any restrictions on such hiring when the internal referral comes from someone with a history of behaviors of concern or other risk factors?
• What is the attrition of recruited family members compared to nonfamily employees?
• Have any employees, who are family members, been implicated in insider violations or risk-related behavior?
Does your organization allow the hiring of candidates with close personal relationships with current or former employees?
• Are there any restrictions on the positions in which these employees may serve in relation to their employee friends?
• Are there any restrictions on such hiring when the internal referral comes from someone with a history of behaviors of concern or other risk factors?
• What is the attrition of recruited social contacts compared to non-family employees?
• Have any friends been implicated in insider violations or risk-related behavior?

PREEMPLOYMENT SCREENING RISKS

Table A-4 summarizes available preemployment screening methods. The information collected during preemployment screening help hiring managers make informed decisions and mitigate the risk of hiring a “problem” employee. The table presents several screening methods; however, not all methods will be appropriate for all organizations and job positions. The methods chosen to screen prospective employees will likely depend on the sensitivity of the industry and the job position.

Table A-4
Preemployment Screening[2] Audit Questions

Screening Measures and Targeted Information	***Mitigated Risks***
Does your organization review employment applications for completeness?	
• Current name and address, phone and email • Alias • Address history (previous 7 to 10 years) • Social Security number • Citizenship • Date of birth • Driver's license number and state of issuance • Criminal history, to include type, level and date of offense • Employment history • Education • License or certification information • Applicant signature authorizing release of information • Applicant signature attesting to the truthfulness of responses	• Misconduct[3] • Inability to perform job duties
Does your organization conduct personal interviews?	
• Topics of discussion: ▪ Level of education ▪ Previous work experience ▪ Skills • Use the interview to evaluate: ▪ Interpersonal skills ▪ Reactions to personal and professional stress ▪ Negative work experiences or references ▪ Ethical decision-making patterns ▪ Information provided in the employment application	• Hiring employees using fraudulent identities • Inability to perform job duties
Does your organization verify authenticity of government issued documents	
• Applicant's government issued documents (i.e., social security card, passport, driver's license, etc.) are inspected for evidence of counterfeiting or tampering. ▪ Social Security numbers (SSN) can be verified at www.ssa.gov	• Hiring an employee with a fraudulent identity
Does your organization verify employment eligibility?	
• Identity vetting via the Department of Homeland Security's E-Verify program will confirm U.S. Alien Registration numbers, naturalization certificate numbers, or passport numbers	• Hiring an employee with a fraudulent identity • Hiring an employee with fraudulent immigration documents
Does your organization review credit reports?	

[2] The extent to which private sector employers may prescreen applicants is limited by federal legislation (Fair Credit Reporting Act, Americans with Disabilities Act, Title VII of the Civil Rights Act, etc.). Personal information gathered for employment purposes must be related to the position for which the applicant is a candidate.

[3] Within a court of law, misconduct typically requires "some act of wanton or willful disregard of the employer's interest, a deliberate violation of the employer's rules, or a disregard of the standard of behavior the employer has a right to expect of its employees." Baker v. Director, 39 Ark. App. 5, 6, 832 S.W.2d 864, 865 (1992).

Screening Measures and Targeted Information	***Mitigated Risks***
• Credit reports reveal: ▪ Aliases - identity vetting ▪ Unlisted residences ▪ Identify foreign bank accounts and foreign relationships ▪ Bankruptcy ▪ Tax records ▪ Foreclosures ▪ Judgment ▪ Liens ▪ Lawsuits ▪ Unexplained affluence (i.e., rapid pay-down of mortgage) ▪ Amount and types of credit consistent with age of subject	• Hiring an employee with a fraudulent identity • Personal misconduct • Financial misconduct
Does your organization contact personal references?	
• Personal reference checks can confirm or reveal ▪ Identity ▪ Current residence ▪ Current occupation and employer ▪ Personal misconduct	• Hiring an employee with a fraudulent identity
Does your organization conduct neighborhood interviews?	
• Neighborhood interviews can confirm or reveal: ▪ Identity ▪ Current residence ▪ Personal misconduct	• Hiring someone with a fraudulent identity • Personal misconduct
Does your organization contact professional references?	
• Professional references can confirm or reveal: ▪ Identity ▪ Employment history ▪ Misconduct ▪ Terminations	• Harassment
Does your organization verify education records?	
• Education records can confirm or reveal: ▪ Identity ▪ Level of education and training, including licensing and certification ▪ Authenticity of institution and degree	• Hiring someone with a fraudulent identity • Inability to perform job duties
Does your organization check civil records?	
• Civil records will reveal: ▪ Aliases - identity vetting ▪ Bankruptcy ▪ Tax records ▪ Foreclosures ▪ Judgment ▪ Liens ▪ Lawsuits ▪ Unexplained affluence	• Hiring someone with a fraudulent identity • Personal misconduct • Financial misconduct
Does your organization check criminal records?	
• Criminal records will reveal: ▪ Arrests, charges and convictions ▪ History of violent behavior ▪ Substance abuse	• Espionage • Sabotage • Personal and professional

Screening Measures and Targeted Information	***Mitigated Risks***
• Criminal records can be obtained from local police departments, local, state and federal courts and state central repositories of criminal history information (CHRI). ▪ Police departments may not release records, even when presented with a release signed by the employment candidate ▪ Only "open record states" will provide access to the state's repository of CHRI for noncriminal justice purposes.	• Misconduct • Workplace violence
• Free and fee-based online resources for conducting checks of law enforcement agencies and courts:· ▪ National Court Check: Public Access to Court Electronic Records, AKA PACER. Access to case and docket information from the Federal Appellate, District and Bankruptcy court, and the U.S. Party/Case Index ▪ Trial Courts (not all states provide this resource) ▪ Appellate Courts (not all states provide this resource) ▪ State Supreme Court Online Docket (not all states provide this resource) ▪ Department of Public Safety or State Police criminal records checks (not all states provide this resource) ▪ Online Driver Records (not all states provide this resource) ▪ Sex Offender Registry: www.nsopr.gov ▪ Inmate Information (not all states provide this resource) ▪ Federal Bureau of Prisons for prisoner information ▪ Interpol: www.interpol.int	
• Commercial vendors providing criminal background checks ▪ LexisNexis ▪ Choicepoint	
Does your organization conduct fingerprints checks?	
• FBI's Criminal Justice Information System (CJIS) ▪ Each fingerprint submission is checked against the Integrated Automated Fingerprint Identification System, and name checks of the National Crime Information Center ▪ Fingerprints can be submitted via Livescan, an electronic fingerprinting service or via rolled ink prints on finger and palm print cards	• Fraud • Espionage • Sabotage • Workplace misconduct • Workplace violence • Hiring someone with a criminal record
• FBI Civil fingerprint file ▪ Fingerprints are collected on federal employees and contractors, military service members, resident aliens and naturalized citizens	• Hiring someone with a fraudulent identity • Fraud • Workplace misconduct
• FBI Violent Gangs and Terrorist Organization File (VGTOF) ▪ Regularly updated by the Terrorist Screening Center ▪ GOTF conducted on all submissions to the FBI's CJIS	• Fraud • Espionage • Sabotage • Workplace misconduct • Workplace violence
Does your organization conduct Department of Motor Vehicle (DMV) and National Driver Register (NDR) record checks?	
• DMV and NDR record checks will reveal: ▪ Aliases - identity vetting ▪ Drug and alcohol-related convictions ▪ Current and previous addresses ▪ Physical description of driver	• Workplace misconduct • Workplace violence • Workplace misconduct
Does your organization conduct a homeland security search?	
• OFAC Specially Designated Nationals and Blocked Persons • DTC Debarred Parties	• Espionage • Sabotage

Screening Measures and Targeted Information	***Mitigated Risks***
• Bureau of Industry and Security (formerly BXA)	• Workplace misconduct
Does your organization conduct additional watch-list checks?	
• FBI Most Wanted • Interpol Most Wanted • United Nations Consolidated Terrorist List • European Union Terrorist List	• Espionage • Sabotage
Does your organization search overseas records?	
• Overseas records can confirm or reveal: ▪ Identity ▪ Interactions with foreign governments ▪ Interactions with U.S. embassies ▪ Foreign criminal history	• Espionage • Sabotage • Workplace misconduct
Does your organization test for illegal drug use?	
• Drug testing will reveal: ▪ Use of illicit drugs ▪ Illegal use of prescription drugs	• Workplace misconduct • Policy violations • Security violations • Disgruntled employee • Workplace violence • Workplace harassment • Inability to perform job duties
Does your organization conduct informal online searches?	
• Google • Facebook • MySpace • Peoplesearch.com	• Hiring someone with a fraudulent identity • Hiring someone with a fraudulent work or education history • Hiring someone with a criminal record
Does your organization evaluate risk-related personal associations?	
• Personal or professional connections to persons or groups with known risk factors • Social networking search engines • ERIK, NORA, ANNA	• Security violations • Workplace misconduct • Workplace violence
Does your organization conduct honesty testing?	
• Purposes of psychological testing: ▪ Honesty ▪ Integrity ▪ Reliability	• Workplace misconduct • Policy violations • Security violations
Does your organization conduct mental health and personality testing?	
• Purposes of psychological testing: ▪ Psychological disorders ▪ Personality disorders ▪ Likely organizational aptitude and behavior	• Disgruntled employee • Workplace violence • Workplace harassment • Inability to perform job duties • Impaired judgment, reliability & trustworthiness
Does your organization conduct polygraph exams?	
• In specialized, legal settings involving high risk. • A polygraph exam can: ▪ Deception detection regarding personal history or intentions ▪ Identify those who may be more likely to engage in counterproductive behavior	• Espionage • Sabotage • Workplace misconduct • Policy violations • Security violations • Inability to perform job duties

TRAINING, EDUCATION AND PROGRAM EFFECTIVENESS

This section assumes that policies and practices that are not recognized, understood and adhered to may be of marginal effectiveness and that training and education are essential to policy effectiveness. Table A-5 identifies topics that should be covered in a program of education and awareness for employees, in addition to the policy and practice areas described in a previous section of the report.

Table A-5
Training, Education and Program Effectiveness

Audit Questions
Do specific training and education programs addressing policy and practice areas relevant to insider risk exist, including:
• Job descriptions and employment contracts describe employee responsibilities for information security and protection of sensitive information and resources. Also included are consequences for failing to protect these assets • Rules for a probationary period with increased monitoring for new hires • Information and personnel security in the workplace • Physical security of facilities • Employee use of organizational property outside of work • Boundaries between personal and professional activities that utilize work time and resources • Ownership and sharing of organization intellectual property • Handling and management of sensitive, proprietary or classified information • Outside business involvements and contacts and the reporting of these contacts • Privacy of employee, customer, client and other sensitive personal information • The organizations right to monitor and audit employee activity on proprietary systems • Description on how employees report grievances and their own and others' risk behaviors • Defining unacceptable workplace interpersonal behaviors • Guidelines for reporting and addressing unacceptable workplace behaviors • Employee benefits and compensation • Employees' evaluation and advancement • Describing access to and benefits of employee assistance programs and other support services • Describing the good conduct policy • Applying policies and practices to trusted partners • Adversary awareness training describing possible observable insider risk behaviors, pre-attack planning, recruitment or other suspicious behaviors • Adversary awareness training describing the collection methods of adversary groups that may be targeting the organization and its employees, including through the use of insiders • Adversary awareness training appropriate to international organizational sites, employees and travel • Guidelines on recognizing, reporting, intervening with and following-up on employees identified as at risk for insider acts
Are these training and education efforts appropriately structured for the needs of different employee groups such as managers, systems administrators, human resource personnel, etc?
Are these training and education programs updated according to new information regarding these issues, changes relevant to organizational risks?
Do these training and education programs require attendees to demonstrate their competence in these areas as a condition of program completion?
Are employees asked to demonstrate their competence in these areas through other means such as exercises or red team programs?
Are training and education programs modified based on their impact on target issues?
Are training and education programs modified based on employee feedback regarding their effectiveness?

CONTINUING EVALUATION AND POLICY IMPLEMENTATION

Once effective insider risk management policies are established and communicated, they must be monitored and contingencies for compliance and noncompliance must be enforced in an effective manner. Without effective monitoring and enforcement, compliance will lapse and insider risk will escalate. Table A-6 presents concerns regarding an organization's ability to monitor, implement and enforce policies related to insider risk into a series of questions for the audit user.

Table A-6
Continuing Evaluation and Policy Implementation

Audit Questions
Does your organization track the frequency and effectiveness of employee reporting of at-risk behaviors through its designated programs and channels?
Do you actively investigate these reports in a manner that does not deter future reporting?
Does your organization utilize specialized, trained, multidisciplinary staff outside the at-risk employee's reporting structure to investigate risk reports?
Do these specialized staffers follow standardized investigative and reporting procedures when looking in to these reports of risk, including guidelines for evaluating risk in multiple categories including insider espionage and sabotage, violence and theft of intellectual property (IP)?
Are the results of these investigations stored and recorded regardless of outcome, and accessible, so that future reports regarding personnel may be evaluated in context?
Are there clear options for management intervention—sanctions, referrals, further monitoring, or other steps that should be taken as a result of investigative findings?
Are the processes, rationale and justification for management intervention documented to ensure that these steps and their possible outcomes are considered carefully?
Are actual management actions enforced without discrimination, recorded, and subsequently evaluated for effectiveness?
Are records of employee at-risk behaviors, investigations, and management actions maintained and analyzed as input to new policies, practices, or interventions?
Does your organization perform periodic or follow-up database checks or other investigative actions normally associated with pre-screening to ensure that continuing employees remain reliable and are not subject to compromising factors?
Does your organization maintain and advertise the availability of an Employee Assistance Program to which employees can turn for confidential short term treatment and referral?

MANAGEMENT INTERVENTION

Research on insider events consistently indicates that many organizational interventions after employees have displayed concerning behaviors, rather than mitigate the problem, have caused insider risk to escalate. As noted in the report, this was particularly the case when an employee was rapidly terminated without sufficient evaluation and assessment of risks of retaliation against the organization (Keeney et al. 2005). Organizations that assess insider risk and design risk mitigations plans prior to management intervention will minimize insider risk. Table A-7 describes seven recommendations that represent a coordinated strategy for effective employee evaluation and management intervention.

Table A-7
Management Intervention

Audit Questions
Do policies and procedures exist for identifying employees at-risk before interventions that may cause negative employee reactions and increase insider risk?
Do policies and procedures exist for referring at-risk employees facing negative personnel actions to appropriate teams for evaluation?
Does a specialized team, including HR, legal, employee assistance programs, physical and IT security, and behavioral science members, exist to evaluate the risk of insider espionage, sabotage, theft as well as traditional risks of violence, harassment, etc.?
Are procedures in place to guide team members on assessment procedures?
Is the team trained, exercised and prepared to execute such assessments?
Do Team members have established relationships and liaison with law enforcement, judicial, specialized medical, social service and other community personnel whose assistance and collaboration may be important for case management?
Do policies and practices exist to facilitate implementation of team recommendations designed to reduce identified risks?