Application of the Critical-Path Method to Evaluate Insider Risks

Eric Shaw and Laura Sellers

But when [past] cases are reviewed in depth, it becomes clear that a lack of appreciation exists for the factors that increase the risk that insiders will undertake hostile acts against their organizations.

Introduction

Governments and institutions of many kinds have faced the danger of hostile acts by insiders from time immemorial. In the case of the US government, such hostile acts have included betrayals by employees who supplied secrets to hostile powers, committed sabotage, and fatally attacked fellow employees. Relatively recent examples of such activity include the espionage activities of Aldrich Ames, Larry Chin, and Robert Hanssen; the Wikileaks revelations of Bradley Manning; the disclosures of Edward Snowden; and the violent assaults against fellow Americans by Nidal Hassan and Aaron Alexis.[a,1]

After each of these events investigators produced reports which, in 20/20 hindsight, assessed the damage and demonstrated that warnings of risks had been missed. These case-based, "One should have seen the writing on the wall" exercises often produce increased awareness and some revisions in policies and practices in screening, adjudication, and risk assessment. But when these cases are reviewed in depth, it becomes clear that a lack of appreciation exists for the factors that increase the risk that insiders will undertake hostile acts against their organizations.

Our purpose in this article is to draw on the most recent and comprehensive empirical studies of insider hostile acts—ranging from formal academic efforts to collections of in-depth case reports—to demonstrate that there exists a common set of factors and a similar pattern of individual and organizational behavior across the many occurrences during recent years. We will describe these factors and the indicators of heightened risk and place them in the context of a "critical-path" analysis, an approach that has been used in business and medical fields to identify the interrelationships of processes and their most critical and vulnerable points. We will apply this framework to historical cases and discuss the implications for counterintelligence and security personnel, as well as for intelligence officers engaged in recruitment activities focused on the insiders in targeted foreign institutions.[b]

a. We use the DoD definition of "insider" contained in DoD INSTRUCTION 5240.26, 15 October 2013, as "A person with authorized access, who uses that access, wittingly or unwittingly, to harm national security interests or national security through unauthorized disclosure, data modification, espionage, terrorism, or kinetic actions resulting in loss or degradation of resources or capabilities."

b. See Eric D. Shaw and Harely V. Stock for a version of this analysis in *Behavioral Risk*

This critical-path approach describes the personal predispositions that have contributed to individuals' committing acts against their organizations.

What the Case Data Shows

Our effort to better understand these recurring betrayals began with a review of individual cases. We examined case data to answer the following questions:

- What vulnerabilities—personal predispositions that posed risks—did insider offenders bring to their organizations?
- What stressors and/or triggers appeared to activate or exacerbate these underlying vulnerabilities?
- What were the signs of risk that supervisors, coworkers, and personal contacts should have been able to see?
- What were the organizational obstacles and management problems that interfered with successful interventions with these individuals?
- Why did interventions make matters worse rather than reduce risk?

The pattern of answers to the above questions provided the foundation for the critical path along which a simply troubled employee turned into a danger to the organization and the people who worked in it. This critical-path approach describes the personal predispositions that have contributed to individuals' committing acts against their organizations. It details the personal, professional, and financial stressors that "squeezed" underlying predispositions and resulted in disgruntlement and behaviors—e.g., violations of policies, rules, or even laws—that could have provided warning of increased insider risk.

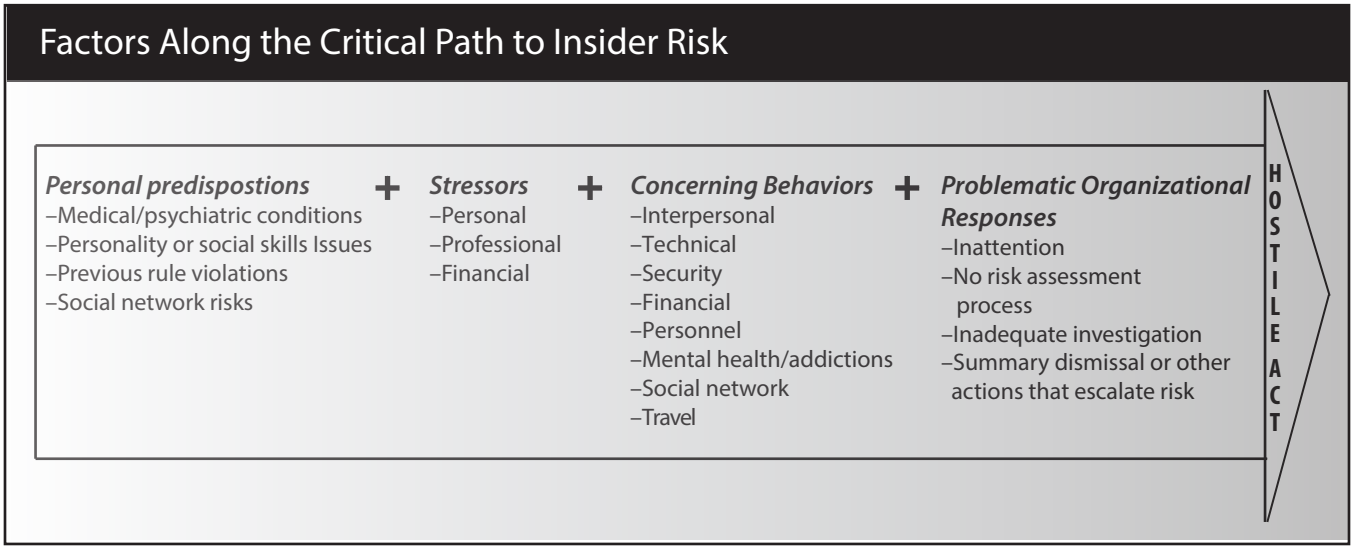
Visibly concerning behavior often puts individuals on management's radar. Unfortunately, management efforts to respond are often complicated by obstacles to acquiring complete or clear information. In addition, legal, bureaucratic, and psychological constraints exist. Often these obstacles result in abrupt or limited responses that elevate risk. Inadequate organizational responses, together with the accumulation of predispositions and stressors, create the environment in which at-risk employees can plan and execute attacks.

Steps Down the Critical Path to Insider Risk

The four elements of the model—personal predispositions, stressors, concerning behaviors, and problematic organizational responses—are shown in the graphic below. In addition to the specific elements, research in the field has shown that:

- the likelihood, or risk, that individuals will commit hostile acts against their organizations increases with the accumulation of factors acting on them over a period of time;

Indicators of Malicious Insider Theft of Intellectual Property: Miseading the Writing on the Wall (Symantec White Paper, 2011).



- the accumulation of these factors appears to follow in roughly the chronological sequence suggested in the graphic;[2]
- the number of employees who can be said to have exhibited or been affected by all of the factors represents a very small proportion of any organization's population;
- even if all of the factors can be said to describe an employee, mitigating factors or successful organizational interventions can take people off the path to a hostile act.

Personal Predispositions

Normal and well-adjusted people do not commit hostile insider acts. The personal characteristics that predispose individuals toward becoming insider risks include:

- the existence of a medical or psychiatric disorder affecting judgment;
- maladaptive personality characteristics, social skills, or decisionmaking that affect a person's ability to get along with others or to function within normal social and organizational constraints;
- a history of rule violations;
- social-network risks consisting of relationships with persons who have adversarial or potentially compromising interests; and
- unusual travel, possibly indicative of contact with organizational adversaries or divided loyalties.

Many inside offenders got into trouble with other groups and even the law before they joined the organizations in which they become dangers.

Medical or Psychiatric Disorders

Medical or psychiatric disorders refer to medical conditions or serious mental health problems, or both, that affect perception, judgment, self-control, and decisionmaking—e.g., alcoholism, anxiety, depression. Alcohol abuse has reportedly figured prominently in the lives of individuals convicted of espionage. A 2010 study of 24 convicted US spies found that 20 had difficulties with alcohol: 11 were characterized as heavy drinkers, nine reported an increase in drinking during spying, seven had DWI convictions, and, 16 reported a family history of alcoholism.[3] Aldrich Ames was perhaps one of the most widely known spies with a severe alcohol problem, including an extensive record of alcohol-related violations acquired before and after he joined the CIA.

Personality or Social-Skill Problems

Many inside offenders had problems following rules, or preferred social isolation to being part of a group. Their behaviors ranged from extreme shyness and avoidance of others to bullying, exploitation, and manipulation of peers. Personality disorders are systematic biases in the ways in which individuals select and process information that helps them see themselves and others in the world. Narcissistic, psychopathic, and avoidant personality characteristics have been cited as prominent in espionage cases, including the case of Jonathan Pollard who is known to have had marked personality issues. He was bullied throughout his childhood, had difficulties staying at schools or jobs, used drugs, and compulsively lied to impress others, even when his stories were unbelievable.[4]

History of Rule Violations

Many inside offenders got into trouble with other groups and even the law before they joined the organizations in which they became dangers. They frequently violated organizational policies, practices, or rules or committed minor or major civil or criminal violations. For example, John Walker Jr. was arrested for burglarizing a gas station in 1955. A local judge gave him the choice of jail or military enlistment. One early study of insiders who used computer technology to attack information systems within US critical infrastructure found that 30 percent of their subjects had significant prior violations, including arrests related to violence, alcohol or drug abuse, and fraud.[5]

Social-Network Risks

Many insiders had histories of contacts with persons who had criminal background or competitive interests. Social-network risks included contact—face-to-face, telephone, or digital—with members of an adversarial or competitive group prior to employment with the organizations they betrayed. Some of these contacts may have occurred in the context of family, social, romantic, or professional relationships with others. Because of the very consistent evidence that criminal activity runs in families, a family history of criminal activity or membership in an adversary group has been shown to be a social-network risk. Two generations of Robert Hanssen's family were involved

Two generations of Robert Hanssen's family were involved in police corruption, and Hanssen reported that this "really lowered the bar" for him to act as he did.

in police corruption, and Hanssen reported that this "really lowered the bar" for him to act as he did. Bradley Manning was affiliated with hacking groups prior to his military service.

Any pre-employment contact with members of groups that pose risks to an organization—even those accounted for by professional responsibilities—can be included in this category. Potentially risky groups will vary for each organization depending on its core functions, but they may include criminal groups—hackers, as in the Manning case—and adversary political or national groups soliciting classified or sensitive information—Wikileaks, terrorist organizations, or foreign military and intelligence organizations.

Travel History

Travel history has been shown to be significant. Thus a subject's record of immigration or travel to or from areas associated with adversarial groups or individuals is a potential indicator. This travel might be in connection with education, tourism, family visits, and official duties or involve emigration from such an area. For example, Ana Montes—the Defense Intelligence Agency analysts who spied for Cuba—traveled extensively, a fact that may have influenced her political allegiance and provided opportunities for recruitment by adversaries. She reportedly spent many summers with her family in Puerto Rico, where her father was an outspoken advocate of Puerto Rican independence. She spent her junior year of college in Madrid, where she may, in fact, have been recruited by Cuban intelligence. After graduation she worked in administrative positions in a law firm and social service agency in Puerto Rico.[6]

In sum, personal predispositions such as those described above serve as potential foundations for insider risk by biasing judgment, signaling a propensity for rule violation, and creating the potential for the creation of adversarial identification or affiliation. However, only a small minority of persons with these characteristics or experiences goes on to commit insider actions, and only after they have been exposed to additional stressors on the critical path.

Personal, Professional and Financial Stressors

Stressors in people's lives can be negative or positive events that result in changes in personal, social, or professional responsibilities that require people to spend effort and energy to adjust. While everyone experiences stress in life, research indicates that stressors especially place pressure on those who possess vulnerable predispositions and can lead such individuals down the next step on the critical path.[a,7]

Several authors have made the connection between professional stressors and espionage, and a 2010 study found that 78 percent of insiders experienced at least one negative work-related event—e.g., poor performance review, stressful work environment, or interpersonal problems—prior to communicating with a foreign government, and 92 percent of insiders experienced at least one negative work-related event prior to providing a foreign government with controlled or classified information.[8]

Family tragedy was the stressor in the case of Thomas Dolce, an Army civilian employee convicted of espionage. In an interview, he described the stressors:

> *I was a real mess for about three years… My mother died very suddenly. And I think that I did not fully appreciate at the time just what the impact of that was. Roughly a year after my mother died, my wife was diagnosed as having cancer. And we both suffered with that for about three years before she died. It was during those three years that the bulk of the* [espionage] *activity took place.*[9]

Financial stress has clearly been implicated in numerous cases. Harold Nicholson, Aldrich Ames, Leandro Aragoncillo, and Brian Regan are examples of spies motivated initially, in part, by financial stress.

Concerning Behaviors: The Obscured "Writing on the Wall"?

Studies of inside offenders have shown that most were known to have committed some form of concerning or problematic behavior before acting directly against their organization. These actions included violations of policy and standard procedure, professional conduct, accepted

a. This formulation is consistent with a psychological model of juvenile crime called General Strain Theory.

practice, rules, regulations, or law through action or inaction (failure to report) that had been observed by managers, supervisors, and coworkers. Specific examples of concerning behaviors in espionage cases have included reports of "kooky" behavior by Jonathan Pollard (threatening to sue his supervisor, dramatic lies of kidnapping and torture) and Ana Montes reportedly leaving an urgent professional meeting at the Pentagon during a crisis and her alienation of colleagues within her specialty area.

Broadly speaking, the manifestation of any form of personal predisposition (medical/psychiatric problems, personality issues impacting behavior, rule violations and unreported contacts with potential adversaries) that occurs during—as opposed to before—employment is also considered concerning behavior. Other concerning behaviors include troublesome communications between coworkers, in person, online, in social media, or in other ways. The above-cited 2010 study of insider actions involving organizational computer systems found violations of organizational personnel policy after the perpetrators had gone through stressful events—and before they had acted against their organizations. Eighty percent of offenders studied had come to the attention of their organizations because of some form of concerning behavior, including tardiness, truancy, arguments with coworkers, or security violations.[10] Other forms of concerning behavior have included technical security violations, unreported foreign travel, and financial misconduct.

Concerning behaviors may also signal the form an insider's attack might take when it occurs. For example, before he carried out his assault in the Washington Navy Yard, Aaron Alexis had several reported weapons violations. Bradley Manning posted a video of the inside of a secure classified information facility (SCIF) on YouTube, and Robert Hanssen hacked into his supervisor's computer to acquire sensitive information.

Other concerning behaviors include troublesome communications between coworkers, in person, online, in social media, or in other ways.

Problematic Organizational Responses

The last element in this critical-path model is problematic organizational behavior in response to at-risk employees, including inaction, inattentiveness, or lack of understanding of the factors described above. Admittedly, formidable—and often understandable—obstacles prevent managers from learning about the concerning behavior of their employees. These include guidelines governing privacy and information exchange, bureaucratic silos, and limited communication between responsible government offices and contracting organizations, local law enforcement, and other outside groups like health-care providers. In addition, in some settings coworkers are reluctant to report concerns to management for fear of putting a person's career at risk, anxiety about retribution, or the perception that a troubling employee might even be favored by management.

Certain actions management might take in response to learning of a potential insider threat could, in fact, elevate the risk of damaging actions or even trigger them. For example, overly aggressive investigative steps or interviews uninformed by an appreciation of a subject's psychology can backfire and increase the risk the employee will act. For example, several years after being terminated for misusing his position as chief information officer to monitor the communications of key executives, the officer launched hacking attacks against the company. After being caught he said the manner in which security personnel had abruptly, rudely, and angrily dealt with him--humiliating him in the process--motivated his hacking.

Finally, organizational leaders often do not sufficiently appreciate how an intervention, especially a termination, can actually escalate insider risk because they have not sufficiently considered the implications of dismissals. The above-cited study shows that more than 80 percent of incidents of sabotage of critical infrastructure information systems were perpetrated by dismissed employees.[11]

Commission of the Hostile Act

At the end of the critical path, the commission of a crime or hostile act seldom occurs without planning and a variety of preparations. Such activities might involve surveillance or research; solicitation of the cooperation of witting or unwitting others; the acquisition of resources or skills; rehearsal of activities to gauge a plan's safety and effectiveness; and attempts at authorized or unauthorized access

At the end of the critical path, the commission of a crime or hostile act seldom occurs without planning and a variety of preparations.

to obtain, replicate and transfer targeted information; deception or other forms of operational security, to name a few.

Given the number of activities involved, it is not surprising that some will be observed. Researchers examining insider attacks on information systems in the financial sector found that in 37 percent of cases examined, insider attack planning was noticeable through online (67 percent) or offline (11 percent) behavior, and in some cases both online and offline (22 percent) behavior. In 31 percent of the attacks, other people—coworkers (64 percent), friends (21 percent), family members (14 percent) or someone else involved in the incident (14 percent) had specific information about an insider's plans, intentions, and activities.[12]

Historical Examples through the Critical-Path Lens

The table on the facing page illustrates the critical-path analysis through the historical examples of Benedict Arnold's treachery in 1780 during the Revolutionary War[a]; Bradley Manning's (now Chelsea Manning's) path to the 2010 delivery to Wikileaks of an enormous store of classified information; and Aaron Alexis's attack in the Navy Yard in Washington, DC, in September 2013.

The three cases each show potentially troublesome personal predispositions and significant histories of personal and professional stress, including problems immediately preceding the commission of their insider acts. In each case, problematic organizational responses occurred, generally involving insufficient concern about the extent to which the subjects were disgruntled or inadequate inquiries into exhibited worrisome behavior. The resultant inaction in these cases became the problematic organizational response.

Also evident in these cases, though not shown in the table, was the fact that signs of preparation to commit hostile acts were present. Benedict Arnold carried on covert communications and held personal meetings with his British handlers. Bradley Manning shopped his materials to two news organizations and was in communication with members of the hacking community, which was aware of his disgruntlement and plans. Aaron Alexis attempted to purchase handguns, bought a shotgun and a hacksaw to shorten the barrel, spent hours at a range practicing prior to his attack, and somehow smuggled the weapon in to the Navy Yard.

How the Critical-Path Approach Can Help

While many of the concerning behaviors of these historical examples are a matter of public record, admittedly the discovery of these kinds of pieces of information in current circumstances is made difficult by the above-mentioned restrictions on the acquisition of information subject to privacy and other protections. Still, the critical-path approach supplies investigators with information targets and rationale for pursuing leads.

In addition to providing general investigative and risk assessment guidance, the critical-path approach can provide a useful empirical framework. Like the itemization of concerning behaviors displayed in historical examples, analysts and investigators can identify and might assign points (values) to risk issues in each category. For example, subjects might be given a total insider risk score, with the result compared to other known cases.[13] Such values might help investigators prioritize resources and narrow the range of possible investigations. Because the factors can change over time, it can also be used to monitor at-risk populations such as subject with particularly sensitive duties or previous risk issues. Another advantage of the method is that it could produce testable research hypotheses—e.g., Do events on the critical path occur in the hypothesized order?—that could contribute to more valid and reliable screening, adjudication, and risk assessment.

Finally, the approach could be applied to the asset recruitment and management process to supplement or complement existing frameworks.[b] For example, the cumulative risk score of a prospective agent could be used to evaluate the likelihood that a target is susceptible to recruitment or

a. Thanks to Robert Rice for his counterintelligence analysis of the Arnold case and Drs. Carol Ritter and Stephen Band for their substantive and editorial reviews.

b. See for example, Randy Burkett, "An Alternative Framework for Agent Recruitment: From MICE to RASCLS" in *Studies in Intelligence* 57, No. 1 (March 2013).

Critical Path to Insider Risk in Three Historical Cases

Personal Predispostions	Stressors	Concerning Behaviors
Benedict Arnold Daredevil; show-off; frequent fights; arrests for assault and disorderly conduct; smuggling; numerous personal and professional relationships with British officials.	History of significant family deaths; paternal alcoholism; crippling physical problems and war injuries, professional reversals, llawsuits; significant financial stress.	Relieved for insubordination; petulant letter to Congress expressing feeling victimization; insults members of court martial; convicted of misdemeanors; disgruntled letter to Washington; charged with abuse of power; reprimanded by Washington; declines command offered by Washington; approaches French for a loan.
Chelsea (Bradley) Manning Long-term history of psychological issues including gender identity disorder, oppositional defiant disorder; targeted for bullying; pulled knife on his step-mother; long-term connections to hacker community.	Significant family disruptions, including divorce, parental alcoholism, and depression, forced relocation; suffered bullying and school failures; job losses; problems in military service.	Recommended for discharge at basic training; reprimanded for posting YouTube video of inside of SCIF; referred for psychiatric treatment; violent reaction to performance counseling; demoted and slated for discharge.
Aaron Alexis Long-term adult history of psychological problems, anti-social behavior, arrests and difficulty getting along with others.	Child of divorce; plagued by mental health problems; complained of discrimination and racism; financial stress.	Counselled for performance issues; tells police he is being followed by people sending vibrations into his body; arrested for disorderly conduct; discharged from Navy for pattern of insubordination, disorderly conduct, unauthorized absence, intoxication; arrested for shooting out tires of vehicle in Seattle in 2004; multiple treatments for psychological issues.

The organizational response and hostile actions: *George Washington was apparently unaware of the depth of Arnold's disaffection and unconcerned about suspicious queries Arnold had made about American spies working against the British. In addition, Arnold kept concealed his communications and meetings with the British until he was ultimately revealed.*

The organizational response and hostile actions: *The Army ignored both Manning's supervisor's recommendation to discharge him and psychological advice not to deploy him; his weapon was taken but not his accesses after a demotion, a violent episode, and planned discharge. Deeper investigation might also have revealed statements of his intention to leak information to friends, media contacts, and on-going communications with known hackers and WikiLeaks.*

The organizational response and hostile actions: *Aaron Alexis's violence risk and psychiatric problems were documented in police records that neither a security clearance organization or his employer accessed—he had never been convicted of a crime. Had they possessed this information prior to employment counseling, the risk to Navy Yard would probably have been avoided.*

too great a risk for recruitment. Regularly updated scores might also help case officers evaluate the implications of changes over time in an potential recruitment's situation.

In Sum

The science of determining security risks remains in its infancy, its ability to actually predict who will engage in some kind of harmful insider action not well established. While review in hindsight of insider incidents frequently creates the impression that there was writing on the wall, it is rarely simply a matter of overlooked or ignored visible clues.

Our hope in placing factors related to insider risk into the critical-path framework has been to suggest a way in which counterintelligence and security personnel might better assess risks associated with employees who have come to their attention and to

help in prioritizing investigative resources.

We do not suggest that this framework is a substitute for more specific risk evaluation methods, such as scales used for assessing violence risk, IP theft risk, or other specific insider activities. We suggest that the critical-path approach be used to detect the presence of general risk and the more specific scales be used to assess specific risk scenarios.

In our view, the critical-path framework—which has demonstrated its utility in other fields for decades—represents the best available device for applying knowledge acquired from research on past hostile insider acts to today's work of detecting general risks.

❖ ❖ ❖

Endnotes

1. Department of Defense INSTRUCTION NUMBER 5240.26 May 4, 2012, Effective October 15, 2013 USD(I), SUBJECT: Countering Espionage, International Terrorism, and the Counterintelligence (CI) Insider Threat, available at http://www.dtic.mil/whs/directives/corres/pdf/524026p.pdf
2. Rhiannon Weaver, "A preliminary chronological analysis of events in the DIA/CERT insider threat database (Software Engineering Institute, Carnegie Mellon University (Unpublished manuscript, 2010—rweaver@cert.org).
3. Richard Heurer, *Adjudicative Desk Reference*, *Background Resources for Personnel Security Adjudicators, Investigators, and Managers*, Version 3.2, June 2010, Alcohol consumption, 3 at http://www.dhra.mil/perserec/adr/index.htmf.
4. Ronald J. Olive, *Capturing Jonathan Pollard: How One of the Most Notorious Spies in American History Was Brought to Justice*, (US Naval Institute Press, 2009).
5. Michelle Keeney et al., *Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors* (US Secret Service, 2005).
6. Scott W. Carmichael, *True Believer, Inside the Investigation and Capture of Anna Montes, Cuba's Master Spy* (US Naval Institute Press, 2007).
7. Robert Agnew and Helen Raskin White, "An Empirical Test of General Strain Theory," *Criminology*, 30 (November, 1992): 475–99.
8. Weaver, "A preliminary chronological analysis."
9. Lynn F. Fischer, "Espionage: Why Does It Happen?" (Defense Security Institute, http://www.hanford.gov/files.cfm/whyhappens.pdf 10-3-2000).
10. Ibid., 8.
11. Ibid.
12. Marisa R. Randazzo et al., "Illicit Threat Study: Illicit Cyber Activity in the Banking and Finance Sector," (National Threat Assessment Center, US Secret Service, 2005)
13. Mark F. Lenzenweger et. al., "Toward an Empirically-based Taxonomy for Espionage: A New Rating System and Multivariate Statistical Results." Paper presented at the 2nd Annual National Security Psychology Symposium, Chantilly, VA, June 2014. Version may be obtained from mlenzen@binghamton.edu

Other readings

S. R. Band et al. "Comparing IT Sabotage and Espionage: A Model Based Analysis—Technical Report ESC-TR-2006-091 (Software Engineering Institute, Carnegie Mellon University, 2006)

Dawn M. Cappelli , Andrew Preston Moore, Daniel Phelps, Eric Shaw, Randall F. Trzeciak Technical Report Modeling Human Behavior in Cyberspace. Pittsburgh, Pa. (FOUO). http://www.researchgate.net/publication/265695219_Research_methodology_for_the_CERT_insider_threat_project_Modeling_human_behavior_in_cyberspace_(FOUO)

Herbig, K.L. & Wiskoff, M. F., Espionage against the United States by American citizens 1947–2001 (Technical Report: 02-5) (Defense Personnel Security Research Center, 2002).

Herbig, K. L., *Changes in Espionage by Americans: 1947–2007* (Technical report 08-05) (Defense Personnel Security Research Center, 2008).

Moore, A., Cappelli, D., Caron, T., Shaw, E., Spooner, D. and Trzeciak, R. (2011)"A Preliminary Model of Insider Theft of Intellectual Property," Technical Note CMU/SEI-2011-TN-013, June. Available at www.sei.cmu.edu/library/abstracts/reports/11tn013.cfm

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

Wood, S. & Wiskoff, M. (1992). Americans who spied against their country since world war II (Technical Report: 92-005). Monterey, CA: Defense Personnel Security Research Center.