WHITE PAPER:
BEHAVIORAL RISK INDICATORS OF MALICIOUS INSIDER THEFT OF INTELLECTUAL PROPERTY

White Paper

Behavioral Risk Indicators of Malicious Insider Theft of Intellectual Property: Misreading the Writing on the Wall

Eric D. Shaw, Ph.D.

Harley V. Stock, Ph.D., ABPP, Diplomate, American Board of Forensic Psychology

IMG
INCIDENT MANAGEMENT GROUP

Confidence in a connected world. Symantec™

Behavioral Risk Indicators of Malicious Insider Theft of Intellectual Property: Misreading the Writing on the Wall

Eric D. Shaw, Ph.D. and Harley V. Stock, Ph.D., ABPP, Diplomate, American Board of Forensic Psychology

CONTENTS

Executive Summary

Today's corporate and government leaders are besieged by reports of economic espionage and theft of intellectual property (IP) by individual agents, organized hackers, corporate competitors and even nation states.[1] Reports of rampant intellectual property theft have contributed to an anxious, war-time mindset[2] as economic competition has replaced political and military confrontation between major world powers. According to earlier reviews, the theft of trade secrets has cost U.S. businesses more than $250 billion per year and these thefts are increasing exponentially and should double within the next decade.[3] According to other sources, 60 percent of companies polled reported they had experienced attempts to steal their proprietary information. The most frequent perpetrators were current or former employees or partners in trusted relationships such as customers, contractors, vendors, and joint venture partners.[4] FBI reports have confirmed insiders are a major target in opponent efforts to gain proprietary information and are also a leading source of these leaks. This has further increased leadership anxiety[5] and contributed to significant concerns regarding organizational loyalty and trust. With this type of stress already high, the actions of a low-level, disgruntled Army private who released sensitive and classified information via Wikileaks in 2010 pushed many organizational leaders to consider nightmare scenarios involving the loss of their own proprietary and sensitive information through the efforts of targeted or disloyal insiders.

This report addresses the high level of organizational anxiety regarding the potential theft of sensitive, proprietary, intellectual property or similar critical data by insiders. It describes what we know so far about the people and organizational conditions which contribute to this risk. As clinical and forensic psychologists aiding corporate security, law enforcement and national security organizations, we take primarily a behavioral approach to this sort of crime. This review emphasizes the contribution of individual and organizational, rather than technological, factors. We hope a clearer, empirically-based understanding of these elements will lead to careful and rational approaches to this problem and help to lower levels of organizational anxiety. While the problem is significant and growing, it is also manageable. This report provides a theoretical framework within which insider intellectual property (IP) theft may be viewed and reviews the available empirical research on this topic, with an emphasis on describing the people and organizational precipitants involved.

Through review of existing empirical data, the report provides insight into the conditions that contribute to malicious insider IP theft. Some of the more salient findings from the review include:

- **Insider IP thieves are more often in technical positions**—The majority of IP theft is committed by current male employees averaging about 37 years of age who serve in mainly technical positions including engineers or scientists, managers, salespersons and programmers. The majority of IP thieves had signed IP agreements, indicating that policy alone—without employee comprehension and effective enforcement—is ineffective.
- **Typically insider IP thieves already have a new job**—About 65 percent of employees that commit insider IP theft had already accepted positions with a competing company or started their own company at the time of the theft. About 25 percent were recruited by an outsider who had targeted the data and about 20 percent of thefts involved collaboration with another insider.
- **Insider IP thieves most often steal what they have authorized access to**—Subjects take the data they know, work with and often feel entitled to. In fact, 75 percent of insiders stole material they had authorized access to. This complicates an organization's ability to protect their IP through technical controls and supports the need for more direct discussions with employees about what data is and is not transferrable upon their departure and should be an overt part of any employee IP agreement.
- **Trade secrets are most common IP type stolen by insiders**—Trade secrets were stolen in 52 percent of cases. Business information such as billing information, price lists and other administrative data was stolen in 30 percent, source code (20 percent), proprietary software (14 percent), customer information (12 percent), and business plans (6 percent).
- **Insiders use technical means to steal IP, but most theft is discovered by non-technical employees**—The majority of subjects (54 percent) used a network—email, a remote network access channel or network file transfer to remove their stolen data. However, most insider IP theft was discovered by non-technical versus technical employees.

- **Professional setbacks can fast-track insiders considering stealing IP**—Acceleration on the pathway to insider theft occurs when the employee gets tired of "thinking about it" and decides to take action or is solicited by others to do so. This move often occurs on the heels of a perceived professional set-back or unmet expectations. This demarcation from intention to volition, or action, explains why some insider theft appears to be spontaneous, when it isn't.

The report concludes with recommendations for organizations seeking methods to deter, prevent, detect and manage this form of insider risk.

Methodology

This effort is a critical review of the available empirical literature on behavioral factors impacting insider theft of intellectual property. We have attempted to synthesize results from different research groups and methods (case reviews, surveys, incident reporting and real world investigatory experience) and reconcile them with current theories that address the critical who, what, where, why, when and how of this violation.

However, our understanding of this problem is limited by several relative weaknesses in the available literature. For example, like most forms of crime, the frequency of insider theft of intellectual property is likely under-reported. This affects our general understanding of the frequency of this problem and appears to skew the substantive available data on the topic. For example, the best available data sets on IP theft episodes come from studies of successfully prosecuted cases. While the use of prosecuted cases may increase the reliability of this data, it may also bias our overall sample of IP theft cases toward more severe episodes in which victims felt they needed law enforcement powers or legal redress to stop the violation or limit its damage. If only 28 percent of respondents report referring computer crimes to law enforcement[6] then we may be missing cases in which firms feared reputational or competitive damage, the offense was of insufficient magnitude, or the victims felt that a law enforcement referral was unlikely to yield significant benefits (versus the costs).

A number of groups conduct surveys of corporate security professionals (for example, Computer Security Institute, Ponemon Institute) and publish data on computer system intrusions (Verizon, Breach Security). Even though most of the survey data regarding the frequency and characteristics of IP theft is submitted anonymously, it appears likely that respondents are drawn from computer and security professionals with a willingness to participate in polling on the topic. This is probably not an accurate representation of organizations impacted by IP theft and also likely under-represents the frequency and impact of the crime. The Computer Security Institute's 2011 Survey offers a sophisticated methodological comparison of the relative strengths and weaknesses of these different survey and incident review methods. The approach used by each of these organizations varies and has direct implications for their findings. For example, Verizon's 2010 Data Breach Investigations Report[7] now includes 257 U.S. Secret Service investigative cases and appears to have increased their assessment of the frequency of insider versus outsider attacks as a result of this added data. However, because the vast majority of these attacks were never reported to law enforcement, this data helps balance the view derived from prosecuted cases. Finally, for illustrative purposes, the authors have drawn from their own case history experience aiding in corporate investigations of these acts and helping company personnel manage insider risk in cases both reported and not reported to law enforcement.

Insider Espionage and IP Theft in General: The Critical Pathway Approach

Researchers of insider crime have largely given up efforts to extract fixed profiles of perpetrators in favor of more complex portrayals of subjects interacting over time within their organizations. This more comprehensive method of characterizing the evolution of these acts in context has been labeled a "critical pathway" approach. This perspective attempts to explain how the personal predispositions of a subject can make him susceptible to the temptation of such acts can interact with contextual stressors, the influence of outsiders and the subject's on-going relationship with his organization, to move him or her down a pathway toward increased likelihood of participation in these offenses. This critical pathway framework describing the characteristics, events and organizational interactions of insiders who have committed espionage, sabotage, theft of sensitive information or intellectual property are observed retrospectively interacting within their personal and professional environments, has been utilized by several researchers.[8,9,10,11,12] For example, an early critical pathway model for insider violations including espionage, sabotage and theft of proprietary information[11] described the personal predispositions of a subject which might influence his vulnerability toward insider theft. Personal and professional stressors which accumulated over time were found to interact with these individual predispositions to increase this risk. Fortunately, in most cases the results of this interaction produced a concerning behavior—an overt violation of an organizational policy, practice or rule—which was visible to management. Unfortunately, management's reaction or lack of reaction thereof to this obviously concerning behavior often increased the odds the subject would escalate his risk and increased the likelihood of insider attacks.

Table 1 below describes our review of the general components of the Insider Risk Critical Pathway model.

Table 1. Overview of 5 Critical Pathway Components

1. Personal Predispositions in Individuals Vulnerable to Insider Risk Present Prior to Joining the Organization
A history of **serious mental health problems**
Social skills problems or biases in interpersonal decision-making including a sense of entitlement, lack of empathy for others, insensitivity to the consequences of actions, etc.
Previous violations of law, or organizational policies or practices
A **social or professional network risk** such as a friendship, family member, or social or work contact who is affiliated with an adversary or competitor or a source of risk for the employee (an addicted spouse).
2. Examples of Personal Stressors Noted in Subjects At-Risk for Insider Acts
Financial Problems • Relationship, marital or family difficulties • Significant medical problems • Legal problems • Relocation
3. Examples of Professional Stressors Noted in Subjects At-Risk for Insider Acts
Demotion or failure to achieve anticipated advance • Loss of seniority or status in merger or acquisition • Disagreements regarding intellectual property rights • Transfer • Disappointing review • Conflicts with coworkers
4. Examples of Concerning Behaviors or Violations of Policy, Practices or Law Observed in Subjects At-Risk for Insider Acts
Disruptive conflicts with coworkers or supervisors • Violations of information, physical, personnel security • Violations of financial rules • Violation of travel policies • Tardiness or missing work • Unreported personal or professional social network risks

Table 1. Overview of 5 Critical Pathway Components—continued

5. Examples of Maladaptive Organizational Responses to Subject Concerning Behaviors
Failure to detect the concerning behavior
Failure to investigate the concerning behavior
Failure to appreciate the implications of an investigated concerning behavior
Failure to act or deal with the concerning behavior
Reaction to the concerning behavior that escalates insider risk (for example, preemptive termination without adequate risk assessment, planning, precautions)

Researchers using this Critical Pathway approach[6,7,8,9] have described it as a narrowing "funnel" or "reverse pyramid" as in Figure 1 below, because there are many more people at the base than actually go on to commit insider theft. In each successive phase the sheer number of people decreases while their willingness to act increases. Unfortunately, while these critical pathway components are derived from case studies of insiders, there are not yet controlled studies to determine the relative balance of persons with, versus without, these characteristics, who go on to commit these attacks. In addition, mitigating factors may prevent an individual from going down this critical pathway from committing an insider violation. For example, treatment for a psychological personal predisposition, intervention to ameliorate a personal or professional stressor, effective intervention at the onset of a concerning behavior, a new security protocol, or a decision to leave the organization could take a potential insider off this path.

Figure 1. The Progression of Events Along the Critical Pathway

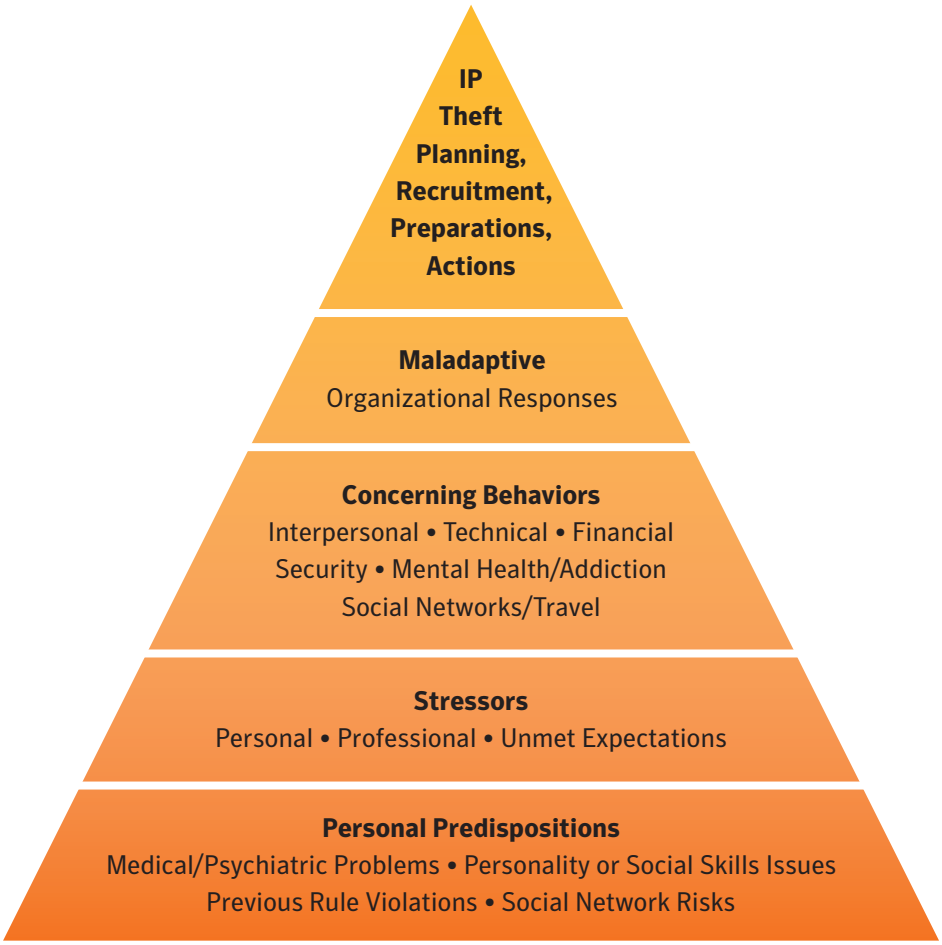

Table 2 below displays critical pathway components observed in two recent cases of IP theft from the authors' investigative caseloads. Subject 1 took proprietary data he had worked on, containing unique financial processes and client information, with him to a new job after he felt betrayed by coworkers and supervisors and was terminated. He also destroyed his former firm's copies of this information remotely after his departure. His employer sought and won a civil injunction against his possession and use of this material. Subject 2 took critical programming information with him to a new job and lied to his employer about the timing and location of his new employment after personal and professional conflicts in the workplace.

Table 2. Observed Critical Pathway Components in Two IP Theft Subjects

Critical Pathway	Subject 1	Subject 2
Indicators of Personal Predispositions	Prone to angry impulsive acts, blames others for his problems indicating biases in personal/social decision-making	Signs of depression, sense of entitlement, blames others for problems, difficulty accepting criticism
Personal Stressors	Personal debt due to spending beyond means	Marital separation and conflict, family conflicts
Professional Stressors	Poor review, placed on probation, terminated	Felt he received unfair performance review, difficulty arranging desired transfer, conflict with supervisor over review
Concerning Behaviors	Trading "irregularities" discovered in subject use of system	Tardiness, missing meetings, late on project deadlines, protests review and initiates investigation of supervisor, goes around supervisors to CEO
Maladaptive Management Responses	Termination without removal of subject's remote access or return of his secure token	Failure to appreciate level of subject disgruntlement, failure to prevent remote downloads

Both subjects presented risk elements associated with the Critical Pathway. Both display *psychological predispositions* of concern indicating problems with social skills as well as a sense that they were somehow above the rules and entitled to special treatment. Neither subject appeared to be able to accept responsibility for their mistakes, insisting on blaming others. Subject 2 also displayed signs of depression (probably as a result on on-going marital and work problems) in both his face-to-face and email communications. Both subjects also had *personal stressors*, including debt and family problems. At work, both subject were disappointed in their performance evaluations and had been sanctioned for problematic professional behaviors. *Concerning behaviors* included violations of company trading rules for Subject 1 and overt policy violations by Subject 2 (tardiness, missing meetings) as well as a host of unusual personnel decisions which were not overt violations of policy or practice but did signal significant disgruntlement. *Maladaptive organizational responses* included a rather abrupt termination of Subject 1 which was poorly coordinated with the IT and Security departments and left him with remote access. In the case of Subject 2, management failed to appreciate the depth of his disgruntlement despite steady escalation and complaints, did not catch his downloading of sensitive and valuable intellectual property while he was allegedly "on vacation" just prior to his departure, and were fooled by his deception regarding the timing of his resignation and the location of his new employment.

But, what about subjects who have critical pathway predispositions and experiences who have not committed insider violations? How to distinguish between those who think about IP theft and those who actually engage in these activities will be described below.

Statistical Profiles of IP Theft

Some of the best available information and analysis on insider violations in general, and IP theft in particular[12], come from the Carnegie Mellon University's (CMU) Computer Emergency Response Team's Insider Threat group. These researchers have collected over 550 insider cases and examined them from a technical and behavioral perspective, over time, as they developed within their organizations. The fact that they have relied on successfully prosecuted cases has increased the validity of their data and analysis. Other sources of information on the frequency and characteristics of insider IP theft come from anonymous surveys of employees and security personnel at affected organizations (such as surveys conducted by the Ponemon Institute[13] and the Computer Security Institute[6]). This section summarizes the best available empirical research data from these sources. While CMU based its study on examination of 50 adjudicated IP theft cases, the Ponemon and the Computer Security Institutes conducted surveys with corporate employees. While the subjects and methods of the two groups differ, the stark picture of IP theft is very similar. This section will summarize the basics of who, what, where, when, how and why of IP theft by insiders according to these and other sources.

The Profile of Who Takes IP

According to Moore et. al.,[12] the majority of IP theft is committed by current male employees averaging about 37 years of age who serve in mainly technical positions. The most prevalent positions were engineers or scientists, managers, salespersons and programmers, in descending order of frequency. About 65 percent of these employees had already accepted positions with a competing company or started their own company at the time of the theft. Fifty-six percent of these subjects stole data within a month of their departure. This and other supportive findings from the CMU data have led to the suggestion that downloading and copying by critical personnel with access to sensitive data should be monitored whenever a resignation is proffered or such a possibility arises.

Perhaps as frightening as the frequency of insider thefts is the fact that these employees don't always act alone. In about a quarter of these cases the insider was recruited by an outsider who had targeted the data and about 20 percent of thefts involved collaboration with another insider.[12] The most frightening scenario we find in our case data related to these figures is the insider who organizes a group of coworkers to leave together, taking critical IP with them, with the last person out destroying the organization's original records.

What They Steal

In the CMU study, the insiders stole trade secrets in 52 percent of cases. Business information such as billing information, price lists and other administrative data was stolen in 30 percent, source code (20 percent), proprietary software (14 percent), customer information (12 percent), and business plans (6 percent).[12] The finding that 75 percent of these insiders stole material they had authorized access to supports the conclusion that subjects take the data they know, work with and, often, feel entitled to. The fact that these individuals are stealing data to which they had authorized access also complicates an organization's ability to protect this property through technical sensors.

When They Steal

Unlike other forms of computer crime, most of these IP thefts occur during working hours, at the work site, consistent with the subject's routine authorized access to this information. Most frequently these were quick attacks—over two-thirds lasted less than a month, consistent with their need to take the information on their way out and use it at a new job or to start a business.[12]

How They Steal

Hanley et al.[14] identified six channels through which insiders stole this information—email, removable media, printed materials, remote network access, file transfer or downloads to laptops. The majority of subjects (54 percent) used a network—email, a remote network access channel or network file transfer to remove their stolen data. The balance of these subjects stole the data from a host computer by placing it on a laptop or some form of removable media, rather than transferring it over the network. Hanley et. al.[14] have provided detailed examples of the methods used and especially interesting analysis of exfiltration method by type of data stolen. Table 3 below summarizes these findings (see Hanley et. al. page 14) providing the most frequent methods used by IP type.

Table 3. Type of IP Stolen by Leading Exfiltration Methods

Type of IP Stolen	**Leading Methods Used** (in relative order of use)[14]
Customer Data	Email, remote network access, laptop download
Source Code	Removable media, remote network access, file data transfer, laptop download
Business Plans	Remote network access, email
Trade Secrets	Removable media, email, remote network access
Internal Business Information	Email, remote network access, removable media, laptop
Proprietary Software	Laptop download, email, remote network access

Why They Steal

While insiders stole IP primarily to gain advantage at a new job or to start a business, about a quarter of the sample gave the stolen data to a foreign company or national entity. This indicates such entities are developing programs that are similar to those for recruiting spies, including the deployment of specialized techniques for this purpose. Common events or problems which preceded the thefts and probably contributed to subject motivation, included:

- Disagreements over ownership of IP
- Fights over compensation
- Conflicts over relocation
- Disagreements over the subject's role after a merger or acquisition
- Being passed over for promotion
- General conflict with a supervisor[12,15]

Employees At-Risk for IP Theft

These precipitants of IP theft tend to support the role of personal psychological predispositions, stressful events and concerning behaviors as indicators of insider risk. However, Moore et al.[12] has synthesized background information on the individuals involved, their motivation, their role and behavior in the organization, the organization's reactions to their behavior and their relationship to the information taken, to construct convincing in-depth systems dynamics models of the motivation and pathways of two distinct groups of employees at-risk for IP theft—the Entitled Disgruntled Thief and the Machiavellian Leader.

The Entitled Disgruntled Thief

According to Moore et. al.[12] about 60 percent of these subjects stole information they had been partially involved in developing. These subjects had also previously signed an IP agreement regarding this work. Either such IP agreements did not include significant penalties (legal or financial) or the employee did not believe the company would enforce the agreement. About a third of these subjects were dissatisfied with their job due to a rejected request for a promotion, raise or relocation, or they were concerned about being laid-off. Often they decided to look for a new job and use the information to increase their attractiveness to their new employer. Or after finding the new job they decided to take the information with them, either just to have it or to actually use it to further their position. Sometimes these subjects would deceive their employers about whether they had a new job, as was the case in the example cited above. Other times they felt entitled to take the information due to their participation in its creation and did not attempt to deceive their employers about their new positions. In either case, about a month before leaving, these subjects would acquire the information using authorized access, and copy it through the means described above. Results of employee interviews by the Ponemon Institute[13] indicate that 67 percent of employees who took company confidential or proprietary data did so to help them get or perform at a new job, confirming this pattern. This high rate of transfer argues for more direct discussions with employees about what data is and is not, transferrable with their departure and should be an overt part of any employee IP agreement.

While the Ponemon results[13] indicate that the problem may be widespread (59 percent of employees who leave, or are asked to leave, are stealing proprietary data), their results support the profile of departing thieves as motivated by their sense of entitlement and negative attitude toward the organization. The top rationalizations for employee theft included the arguments that "everyone else is doing it", "the information may be useful to me in the future," "I was instrumental in creating this information," "the company can't trace the information back to me" and "the company does not deserve to keep this information"(Ponemon Institute, 2009, page 4). Sixty-one percent of respondents with negative attitudes toward their company took data. Even among employees with favorable attitudes toward their company, 26 percent still stole data. Therefore, a company should not be lulled into a sense of complacency about an allegedly "good" employee. Unfortunately, this finding implies that even companies with excellent morale and loyalty are not immune from this risk.

The Machiavellian Leader

According to Moore et. al.,[12] unlike their disgruntled cousins, these subjects appear motivated by ambition in addition to dissatisfaction with the job. This subject has specific plans to use the proprietary information to develop a new product or attract customers away from his current employers to a new business. He may already be working with a new organization or has sold this information to one. According to Moore et. al.[12] 86 percent of these subjects stole data from an area they were directly involved in and in 62 percent of these cases they had at least directly contributed to the development of the data or product they took. Unlike the Entitled Disgruntled Thief, who takes the IP quickly before leaving, the Machiavellian Leader does more planning. For example, they may create a new business ahead of time, recruit colleagues to help them steal the information and join them at the new venture or coordinate their plans with an outside company or group. While most also take the information within a month of leaving, they can also start to remove it earlier. These subjects appear to be more likely to be motivated by personality factors such as ambition and greed, than pure disgruntlement or mental health disturbances. They are more likely to present a cool, detached and calculating demeanor than their more emotional, volatile and impulsive disgruntled "cousins."

How They Were Detected

The manner in which these violations were detected has significant implications for future mitigation efforts. In contrast to CMU's other insider cases, most insider IP theft was discovered by non-technical versus technical employees.[12] For example, coworkers reported suspicious behaviors, the former employee was noticed marketing a product or service similar to his former project, or a customer notified the business that they had been approached by the former employee. Sometimes the company involved was unaware of the theft until law enforcement notified them after discovering it during a related investigation.

While the Entitled Disgruntled Thief (EDT) displays signs of his discontent before he leaves, there may not be such signals from the Machiavellian Leader (ML). This type of thief is also more likely to recruit fellow employees for his scheme, especially when he lacks the expertise or access to acquire the data he needs to establish his new venture. Therefore, fellow employees may be the best source of data on this type of risk. As noted above, suspicious downloads prior to departure were a key indicator with the EDT, who displayed unusual copying within 30 days of leaving. The ML may also escalate his downloading acutely prior to departure but can also plan his "spin-off" over a longer-term period. Another tactic reported by Moore et. al.[12] we have seen in our cases is the departing employee with unusual travel who explains his remote access exfiltration of IP as routine use while on vacation or on sick leave. Other employees have lied about the timing of their departure and their new work destination. For example, one employee indicated that he was doing freelance consulting when he had actually gone to a competitor.

A Closer Look at IP Thief Psychology

Stock[16] has described the way in which many disgruntled individuals come psychologically to the point of committing insider violations, including IP theft, and then rationalize and plan such acts. Stock's model of "Pathological Organizational Affective Attachment (POAA)" examines the complex interactional process of subject motivation, emotions, cognitive processes, interpersonal dynamics and social exchanges that push a subject down the critical pathway to IP theft. His approach overlaps directly with elements of the critical pathway model, lending additional support to the value of these frameworks. However, the POAA provides additional psychological insight into the thoughts and feelings that move a subject toward action. At the same time the POAA offers useful psychological "levers," which if addressed, can help detect, deter or prevent insider acts. Table 4 below provides an overview of the POAA framework with examples of variables from each of its four conceptual categories.

Table 4. The POAA Conceptual Framework with Category Examples (Stock, 2006)

Conceptual Framework	Category Examples
Employee/Subject Variables	
Personal characteristics of individuals that influence the risk of IP theft including their psychological state, attributions, rationalizations for the act, motives, access to IP, self-control, and vulnerability to recruitment by others	Psychiatric illness, addiction, perceived injustice, authorized access to IP, diminished self-control—an employee drinks 8 beers per day, is in psychiatric treatment on psychoactive medications, blames his supervisor for his problems and feels his contributions are chronically unrecognized and unrewarded
Extra-Work Variables	
Situations or events that are occurring in the subject's life outside of the workplace but may be contributing to, or mitigating against, IP theft	Personal or family health issues, financial pressure, marital, family or personal relationships, availability of professional or social supports—the employee's parent is dying, his mortgage is "under water" and although he is in therapy he experiences chronic conflict with his family
Workplace Variables	
Working conditions, professional relationships, organizational culture, environmental pressures on the organization	The employee works in a physically uncomfortable environment, his co-workers do not like him, his company is contemplating disciplinary action against him, and the corporate culture supports, by ignoring, incidents of teasing and bullying against him. The company is under financial stress due to a drop in demand and price for their product
Target Characteristics	
Characteristics of the IP, subject relationship and attributions regarding the IP, security or other protections against theft	The employee has routine authorized access to the IP, the security measures to protect the IP are lax, the company has not noticed any changes in the employee's behavior—he feels emboldened by dress rehearsals of copying and removing the data, believes that he is "owed" personal access to the material due to his contributions and that stealing the IP will significantly hurt the company

When this model is deployed to evaluate employee risk and identify characteristics that can be manipulated to reduce this risk, subjects are viewed through the overlapping variables within the four conceptual categories. This model suggests not all

issues need to be addressed equally. For example, if an employee has a sense of perceived injustice (employee/subject variable) addressing this issue may reduce the need to steal in order to "get even." In this case, if work related behavior can be identified and changed, it may be sufficient to significantly reduce the risk. As the domain overlap increases, more complicated risk reduction strategies will be in order.

Each combination of risk behaviors will be unique for the individual under scrutiny. For example, a person who is experiencing financial problems or relationship issues (extra-work related variables) may be motivated for financial gain. An employee who believes they are not being treated "fairly" (work related variables) may use a justification mechanism to excuse stealing. If a person has an antisocial personality (employee/subject variable), they will justify their actions based on "everyone is stealing" or "the company makes a lot of money." The selection of a specific IP target (Target variable) may be determined by access, knowledge, and ability to overcome, security protections.

Whatever the motive for the theft, the employee becomes a goal-oriented tactician, evaluating the necessary knowledge, skills and activities for extracting the protected information without being caught. This operational planning is often dynamic, based on the protective challenges employed by the company, as Moore et. al.[12] have shown in their modeling of IP theft dynamics between the subject, organizational personnel and technical security measures. The employee's behavior, even on a pathway of theft, can take many detours. The greater the motivation and capacity of the rogue employee, coupled with ineffective or inappropriate applied surveillance or protective measures, the higher the likelihood of success. The perceived demands of tasks necessary to steal information, coupled with the unique psychology of the employee, will dictate the pathway, including acceleration and deceleration behaviors toward the target.

IP Theft Risk Indicators

If the empirical results, case data and assessment frameworks described above are combined, we can formulate a risk assessment process based on available data, to be used to evaluate IP theft risk for an individual. In addition, this framework can be used to prescribe policies and practices to improve prevention, deterrence, detection and case management. Tables 5 and 6 below contain the major components of this risk assessment list.

Table 5 displays subject psychological characteristics which may constitute risk factors for insider actions in general, and IP theft, in particular. These mental health issues, interpersonal assumptions and negative cognitions or attributions impact IP theft risk by laying the groundwork for disgruntlement or by helping the employee rationalize his actions, as described above. A history of previous violations and social network risks further increase the likelihood of insider acts such as IP theft. These predisposing personal characteristics may become particularly mobilized when personal and professional stressors are experienced.

As Table 5 indicates, psychiatric conditions and social skills problems and decision-making biases can lead directly to professional and personal conflicts on the job which feed disgruntlement risk. Employees with a history of previous rule violations elsewhere are at even greater risk for future violations. Social network risks refer to other disgruntled or calculating employees within the organization or individuals or organizations outside the organization who might facilitate or solicit employee participation in IP theft. As noted above, when these predisposing personal characteristics interact with personal and professional stressors an at-risk employee may begin to ruminate about unmet expectations, perceived mistreatment, blame or other negative attributions or beliefs characteristic of disgruntlement. Real or perceived organizational injustices can become increasingly difficult to tolerate and perceived mistreatment by coworkers and managers may become particularly difficult to bear. Prior to acting the subject may display signs of disgruntlement such as anger or withdraw and he may even share fantasies or plans related to an insider violation.

High Risk Factors of IP Theft

Table 5. Subject Psychological Risk Factors in IP Theft

Subject Psychological Risk Factors	Examples of Observable Workplace Risk Indicator
Personal Predispositions or Subject Factors	
Psychiatric or Medical Condition Impacting Perceptions or Judgment	Problems with task performance and social interactions impacting ability to perform job, reactivity, judgment; knowledge of psychiatric treatment or referral
Personality, Social Skills or Decision-Making Characteristics Biasing Perceptions Of Self and Others that Increase Social Conflict or Isolation	Difficulties getting along with others, feelings of being above the rules, impulsiveness, difficulty accepting responsibility with tendency to blame others. These psychological characteristics increase the likelihood of disgruntlement, especially in the presence of personal and/or professional stressors
Previous Violations of Rules, Policies, Practices or Law	Employee has history of previous violations of law or organizational rules governing finances, security, travel, IP, conflicts or interest, etc.
Social Network Risks	Employee has on-going contacts in professional community that could position him to exploit IP for personal gain, help establish independent business or new employment
Personal Stressors (in IP Theft)	Financial stress, family conflicts, family illness, personal failures or setbacks outside work
Professional Stressors (in IP Theft)	Supervisor conflicts, threats of lay-offs, unmet expectations for promotion, pay, responsibilities, training, benefits
Disgruntlement Indicators	
Observable Concerning Behaviors	Disagreements over ownership of IP, fights over compensation, conflicts over relocation, disagreements over the subject's role after a merger or acquisition, being passed over for promotion
Negative Attributions Regarding Organization **• Procedural Injustice** **• Distributive Injustice** **• Interactional Injustice** **• Impotency**	Employee believes wrongful behavior and unfair advantages or connections are rewarded, lack of work is rewarded while hard work is not, there is unequal versus equal treatment of employees, there is equal or nondiscriminatory treatment when it should be individualized and different, good behavior or innocence is punished, punishment is displaced onto persons who either do not deserve it or do not deserve the severity of the punishment, the punishment is disproportionate to the act or intent, wrongful behavior goes unpunished and management makes arbitrary rules. The organization is powerless to protect its interests and assets and can therefore be taken advantage of

Subject Psychological Risk Factors	Examples of Observable Workplace Risk Indicator
Disgruntlement Indicators (continued)	
Negative Feelings About Treatment by Others	Employee comments suggest he: • Believes coworkers and supervisors are out to harm him or his interest • Experiences coworkers and supervisors as adversaries/competitors who must be overcome • Feels unreasonable anger and blame toward others
Signs of Significant Anger or Mood Variation	Feelings of being provoked or forced to act, fantasies or discussion of getting even, feelings of violation, helplessness, discussions or fantasies about setting-up own business, taking work elsewhere, going independent, irritability and moodiness, physiological indicators of stress (knot in stomach), agitation, temper displays, unusual withdrawal
Rationalizations/ Justifications for Theft or Rule Violations	Everyone else is doing it, I was instrumental in creating this information, it can't be traced back to me, it makes my life easier not to have to recreate this at my next job
Unusual Technical Behaviors	Unauthorized Escalation of Access, use of coworker to achieve unauthorized access escalation, use of portable media, unusual remote access, anomalous copying or downloading especially prior to departure for travel, vacation, resignation or termination, signs of IP theft planning
Potential Interpersonal Indicators or Insider Risk	Formation of unofficial work groups outside official structure—especially if these connections compete with formal hierarchy, recruitment of other employees for unsanctioned assignments, unusual travel or professional contacts, side employment or starting own business
Pattern of Policy or Practice Violations	Finances (unauthorized expenditures), travel (unreported or unauthorized travel or travel expenses), information security (unauthorized use of thumb drives), physical security (unauthorized visits or access), unauthorized contacts with competitors
Behaviors Related to Leaving Organization	Reports of intention to resign or terminate employment, announced resignation, secretiveness or deception regarding employment plans or post-employment activities

Intention to Volition

While many employees have these personal predispositions to disgruntlement and may actually think about revenge or even ruminate about IP theft, most employees don't act on these thoughts and feelings. What is it that differentiates those who "think" about or even talk about theft and those who "do" theft? It is a cognitive shift from intention to volition. "Intention" is the psychological process in which the employee ruminates, or continuously thinks about, stealing the data. They may spend a good part of the workday plotting about what they are going to do, how they are going to do it, and anticipating the consequences of these actions. They may talk to their colleagues about their feelings and thoughts, without any specificity. Yet, they still don't act. Acceleration on the pathway to insider theft occurs when the employee gets tired of "thinking about it" and decides to take action or is solicited by others to do so. This move often occurs on the heels of a perceived professional set-back or unmet expectations. This demarcation from intention to volition, or action, explains why some insider theft appears to be spontaneous,

Table 5. Subject Psychological Risk Factors in IP Theft—continued

when it isn't. Consumed by increasing psychological pressure, the employee becomes frustrated by their indecisiveness or lack of goal achievement and decides to finally move forward to leaving the organization and taking the IP with him. This cognitive shift from intention to volition is a turning point from considering what action to take, to taking the action that was considered. The employee will now evaluate how realistic it is to attack the target; what countermeasures to perceived security need to be employed; other employees whom he can involve; the methods, materials and personnel needed; what his next job should be; and how to escape undetected.

We do not yet have controlled research on observable differences between employees with intentions versus volition and action. However, employees who go on to commit IP theft appear to display a propensity for action through concerning behaviors in the work environment. As described above, concerning behaviors include violations of policy or practice, manifestations of disgruntlement or signs of theft preparation that are potentially visible to others in the work environment.

The final ingredient in this insider IP theft assessment should involve a determination of whether the organization has made matters worse through some action or failure to act. For example, organizations often fail to recognize or respond to a risk indicator or respond in a manner that actually escalates the risk. If a disgruntled individual is further sanctioned without attention to the potential of IP theft, the sanction can lead directly to escalation toward the crime. If the organization is unaware of the level of disgruntlement or theft risk then they may miss concerning behaviors signaling this risk or actual elements of the theft such as downloading. For this reason, we recommend an IP Theft Risk Assessment prior to personnel actions or sanctions against an employee, especially if these acts are not in line with the employee's expectations.

Using the IP Theft Risk Assessment

Because we do not know how many individuals with these risk factors actually go on to commit IP theft, it is difficult to recommend a specific risk investigation strategy based on the potential costs of investigating false positive cases (persons with these characteristics who are not at risk for IP theft). Thorough risk assessments of disgruntled employees can prove expensive and may contribute to an undesirable working environment. However, at a minimum, we strongly recommend that any concerning behavior—especially resignation—trigger a risk assessment using these items. Items from Table 5 should be used to evaluate the employee's mental state in terms of risk issues.

In the next section we describe other organizational steps that can help prevent, deter, detect and manage IP theft risk by making sure the organization does all it can to detect and manage known risk factors.

Personnel Policies, Programs and Capabilities to Defend Against IP Theft

The Defense Personnel Security Research Center (Perserec) published a list of personnel policies, programs and organizational risk management practices that serve as an organizational audit for insider risk preparedness.[17] This report lists specific organizational personnel practices including employee recruitment, security awareness training, risk evaluations prior to interventions, and termination planning that can help manage the risk of insider IP theft, as well as other insider acts. This section of the report provides examples of how specific IP theft risks can be addressed by these and other recommended practices. Readers are encouraged to follow the link provided to the full report.

Avoiding Employees Vulnerable to Disgruntlement and Other Personal Predispositions Through Employee Screening

As their names above imply, the Entitled Disgruntled Thief and the Machiavellian Leader both present distinctive psychological profiles. Vulnerable to disgruntlement, feeling above the rules, lacking in loyalty and willing to exploit their coworkers for personal gain, these at-risk employees may stand-out on basic employee screening measures including applications, psychological testing, interviews, references, and on social media. In addition, they may have a history of previous violations of policies or laws that can be discovered on background investigations. Because the Machiavellian Leader likes to conspire with coworkers, he may also exploit incentives for hiring (employee bounties) by bringing in personnel from within his social/professional network as trusted collaborators. While the use of employee referrals are generally highly regarded by personnel security specialists, they can backfire when social connections offset employee screening standards, interfere with the enforcement of policies or practices or compete with organizational loyalty. These social connections can also facilitate social engineering or facilitate internal conspiracies. Shaw and Fischer[18] described such a case where a former professor of computer science hired several of his graduate students to help him build an online equities trading system for a company. However, when it came time to upgrade the team's production experience, members of the professor's coterie conspired to claim IP rights, refused to pass on code and then sabotaged the system.

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 pre-employment screening measures—had been detected. As noted above, the entire array of Personal Predispositions or Subject Variables may be subject to pre-employment checks through such measures as:

- Verification of application information
- Background checks
- Review of Social Media
- Personal interviews
- Professional references
- Personal references
- Alcohol and drug screening
- Honesty testing
- Psychological or personality testing
- Polygraph examination, under limited circumstances

Stock has surveyed the pre-employment screening processes of ten Fortune 500 companies and found significant gaps in the data gathered along with significant under-utilization of the available data for employment risk decisions. To address these shortfalls, Stock[19] has developed a computerized bio-data application process (Smart Application) that gathers large amounts of data from an applicant and utilizes sophisticated algorithms to organize the responses to assist the hiring manager in the decisional process. In particular, the bio-data application guides the next step, the job interview. Other recent improvements in employee screening include advanced algorithms for internet and social media searches and specialized training for interviewers.

The Relative Ineffectiveness of IP Agreements: The Need to Re-examine IP Theft Policies, Practices and Enforcement
The finding cited above that the vast majority of IP thieves had signed IP agreements supports the conclusion that the simple existence of a policy alone—without employee comprehension and effective enforcement—is ineffective. 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. According to Perserec,[18] 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

This requires a more aggressive approach to employee indoctrination, training, enforcement and security awareness programs. In addition, the failure of an organization to show effective employee indoctrination and training on IP theft policies and practices can weaken any legal remedy to address these violations. We recommend regular training on IP policies along with the re-signing of IP agreements, especially at the time of resignation or termination. As noted above, the overt description of information that may, and may not, transfer with a departing employee could be described in checklist form and signed by the employee. This should improve the effectiveness of IP agreements.

Lack of Employee Reporting of IP Theft Critical Pathway Risk Factors—the Importance of Security Awareness Training
One of the major goals of Security Awareness Training targeting IP theft is to make employees aware of the signs of IP theft risk in coworkers as well as external agents seeking access to organizational assets through insider recruitment. Although employees appear relatively willing to report overt violations of IP security, they are notoriously unwilling to report on many of the personal predispositions and attitudes that are risk factors for IP theft. According to another Perserec study of employee reporting of risk factors,[20] involving interviews and focus groups with employees and security personnel,[20] *"all of the participants, without exception, said that they would seldom report certain gray-area behaviors that they describe as too personal ("the more private things," as one put it). Such behaviors may include emotional or mental, financial, alcohol and drugs, and marital problems, and unusual personal conduct.* This research suggested that participants are reluctant to report these behaviors because they cannot see a link between that type of behavior and security; in other words, they are unlikely to be convinced of the security relevance of personal problems. This finding indicates that security awareness programs need to work harder to get coworkers and managers to understand the links between psychological issues and stressors and IP theft risk.[20]

The potential gains from improved coworker reporting of insider risk and plans is hard to underestimate, especially as the more case data we collect, the more frequent internal and external collaboration among IP theft conspirators appears. In 31 percent of the incidents examined in another CMU report[21] 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 percent of these incidents, the insider made plans, including discussions with competitors and co-conspirators. Fifty-eight percent of the insiders from another CMU study[22] communicated negative feelings, grievances, or an interest in causing harm to the organization and 39 percent communicated negative feelings about the organization or an individual in that organization. In 20 percent of the cases, the insider made a direct threat to harm the organization or an individual, to persons at work not directly involved in the issues.

Another gap in current security awareness training includes employee education on recognizing insider risk and disgruntlement in online communications. Shaw and Stroz[23] have described the appearance of online communications from disgruntled employees who have committed a range of insider acts and developed patented, specialized psychological content analysis software that identifies change in linguistic style and tracks these communications that may signal an acceleration on the pathway to IP theft. This can be done anonymously, without any violation of personal privacy, until security thresholds of concern are reached. Security awareness training could benefit from educational programs designed to help coworkers

recognize these online signs of disgruntlement as well as anonymous online methods for forwarding this content or reporting these concerns. For example, a multi-method approach to avoiding IP theft could incorporate a data loss prevention system that monitors end-user activities. Such a system could check for anomalous downloading by a disgruntled employee.

Maladaptive Organizational Responses: Missing the Problem, Under and Over-Responding—the Need for Careful Assessment and Planning Before Interventions

The entire premise of the IP theft risk assessment framework above derived from the Critical Pathway and POAA models is that employee risk of IP theft develops over time as the employee interacts with others, within and outside his organization. While initial screening and security indoctrination may be effective, 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 others. The same scenario applies to many individuals recently convicted of IP theft.

It was troubling that management often remained unaware of disgruntled employees at-risk for IP theft and that even when they investigated concerning work behaviors they failed to act in a manner that effectively reduced IP theft risk. In addition to improved education regarding these risks, this trend call for more careful assessment of insider risk prior to interventions with disgruntled employees and especially with disgruntled employees leaving the organization for any reason.

Post-hoc studies of insider communications[22,24] consistently indicate that they feel angry and victimized at work prior to their violations. Within the academic literature, studies have linked perceived injustice to both theft and sabotage.[25,26,27,28,29,30,31,32,33,34] Other reviews of insider violations indicate that they strike after an acute grievance with management over some type of sanction. For example, a CMU study[21] found that 92 percent of insider cases were triggered by a specific event or a series of events including employment termination, a dispute with a current or former employer and an employment related demotion or transfer.

We suggest that in addition to investigating concerning behaviors, managers and security personnel take further steps to consider likely employee reactions to perceived adverse management actions. By taking a proactive stance, vulnerable individuals can be identified early on the pathway to theft. Actions and issues that have been associated with increased risk of IP theft have been described in Table 5 above. In our experience, these assessments are best made by multidisciplinary teams consisting of HR professionals, HR Legal specialists, organizational health personnel, and forensic psychologists. Such a prepositioned and trained team can quickly gather information, analyze the risk and plan mitigation strategies.

Finding the the Entitled Disgruntled Thief and the Machiavellian Leader: Exit and Termination Planning

The need for an IP theft risk assessment is never as acute as when an employee appears to be headed out the door. The combination of potential disgruntlement, authorized access, a sense of entitlement to IP they have contributed to, as well as entrepreneurial fever combined with a tempting outside agent appear, to be potent ingredients for IP theft risk. It is under these conditions that IP thieves appear to initiate their illegal copying and transfer of proprietary assets. We recommend organizations deploy specialized termination and exit programs using the methods described above to address this risk.

Conclusion

We have examined the best available empirical data on IP theft and the theoretical frameworks describing the interaction between employee, organization and environmental variables in IP theft that appear most consistent with these empirical findings. This review produced pragmatic recommendations for managers and security personnel concerned with IP theft risk, including:

- An IP Theft Risk Assessment protocol for evaluating employee risk
- Organizational policies and practices that can contribute directly to the prevention, deterrence, detection and management of IP theft risk
- Innovations in the field of Insider risk management which can further aid in the reduction of this significant personal, business and national security problem

Risk Assessment Checklist

BUILD A TEAM: *To fully address insider theft, you need to have a dedicated team who create policies, drive training, and monitor and evaluate.*

- Create a cross-functional team to address insider theft comprised of representatives from teams such as HR, information security, physical security, occupational health, employee assistance (EAP), legal and a psychologist

ORGANIZATIONAL ISSUES: *Understand if your organization is at greater risk due to inherent organizational factors.*

- Does your company have remote offices, suppliers, or subcontractors where differences in cultures, politics or language could lead to potential conflicts?

PRE-EMPLOYMENT SCREENING: *The information collected during pre-employment screening help hiring managers make informed decisions and mitigate the risk of hiring a "problem" employee.*

Does your organization:

- Review employment applications for completeness?
- Conduct personal interviews?
- Verify authenticity of government issued documents?
- Verify employment eligibility?
- Review credit reports?
- Contact professional references?
- Check criminal records with background checks?
- Test for illegal drug use?
- Conduct informal online searches of social networking sites or general websites?

POLICIES AND PRACTICES: *This is a checklist of specific policy and practice areas that should be covered within an organization's basic governance structures.*

Does your organization have

- Information security policies that protect sensitive data and resources? Policies should address key issues such as:
    - Job descriptions and employee contracts that include descriptions of information security responsibilities
    - Targeted monitoring of high-risk email, web, storage, and endpoint systems,
    - Access controls and change management, configuration control, logging, auditing, monitoring
    - Specialized monitoring of system administrators and other "super users"
- Clearly defined policies regarding the ownership and sharing of intellectual property?
- Guidelines that describe the organization's right to monitor and audit employee activity on proprietary systems?
- Policies describing how employees report grievances and their own and others' risk behaviors?
- Clear policies describing how employee evaluation and advancement are accomplished?

- Clear procedures describing access to and benefits of employee assistance programs and other employee support services?
    - Includes 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
- Well defined termination processes in place to ensure that all access to corporate resources are cut off immediately upon termination of an employee?

TRAINING AND EDUCATION: *Policies alone are ineffective in preventing intellectual property theft. Training and education are vital to employees gaining awareness of policies, understanding their role in security and the consequences of violating guidelines.*

- 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
    - Rules for a probationary period with increased monitoring for new hires
    - Information and personnel security in the workplace
    - Ownership and sharing of organization intellectual property
    - Handling and management of sensitive, proprietary or classified information
    - Description on how employees report grievances, and their own and others' risk behaviors
    - Defining unacceptable workplace interpersonal behaviors
    - Describing access to and benefits of employee assistance programs and other support services
- Structure your training and education efforts appropriately for the needs of different employee groups such as managers, systems administrators, human resource personnel, etc?
    - Managers should be trained on the Critical Pathway. Let them know what signs to look for and how to take action.

CONTINUING EVALUATION: *Without ongoing monitoring and enforcement, compliance will lapse and insider risk will escalate.*

Does your organization:

- Track the frequency and effectiveness of employee reporting of at-risk behaviors through its designated programs and channels?
- Actively investigate these reports in a manner that does not deter future reporting?
- Utilize specialized, trained, multidisciplinary staff to investigate risk reports?
- Have clear options for management intervention—sanctions, referrals, further monitoring, or other steps that should be taken as a result of investigative findings?
- Maintain records of employee at-risk behaviors, investigations, and management actions maintained and analyzed as input to new policies, practices, or interventions?
- 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?
- Maintain and advertise the availability of an Employee Assistance Program (EAP) to which employees can turn for confidential short term treatment and referral?

1 Dilanian, K. (2011) "China Cyber Attacks Threaten U.S. Security, Official Says," Los Angeles Times, October 4, http://www.latimes.com/news/politics/la-pn-china cyberattacks-20111004,0,3051541.story

2 Nakshima, E. and Wan, W. (2011) "On red alert over cyber-spying," Washington Post, September 27, A1.

3 Almeling, D., Snyder, D., Sapoznikow, M., McCollum, W. and Weader, J.(2011) "Statistical Analysis of Trade Secret Litigation in State Courts," Gonzaga Law Review. No. 57.

4 American Society for Industrial Security International (2007) "Trends in Proprietary Information Loss," Survey Report, August http://www.asisonline.org/newsroom/surveys/spi2.pdf

5 Federal Bureau of Investigation (2011) http://www.fbi.gov/about-us/investigate/counterintelligence/economic-espionage

6 Computer Security Institute (2011) 15th Annual Computer Security Institute 2010/2011 Survey, CSI www.GoCSI.com

7 Verizon (2011)2010 Data Breach Investigations Report, Verizon http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf

8 Shaw, E.D. and Fischer, L. (2005) Ten Tales of Betrayal: An Analysis of Attacks on Corporate Infrastructure by Information Technology Insiders, Volume One," Monterrey, CA.: Defense Personnel Security Research and Education Center.

9 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, Vol. 3, pps. 20-31, Elsevier Publications, Exeter, UK

10 Band, S., Cappelli, D., Fischer, L. Moore, A, Shaw, E. and Trezciek, R. (2006) Comparing Insider IT Sabotage and Espionage: A Model-Based Approach, Technical Report CMU/SEI-2006-TR-026, Software Engineering Institute, Carnegie Mellon

11 Shaw, E. (2005) "Ten Tales of Betrayal: Challenges in the Prevention, Detection and Management of Insider Threats," Presentation at the Computer Security Institute, Washington, DC, November 14.

12 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

13 Ponemon Institute (2009) "Data Loss During Downsizing," Ponemon Institute, February.

14 Hanley, M., Dean, T., Schroeder, W., Huoy, M., Trecziak, R. and Montelibano, J. (2011) "An Analysis of Technical Observations in Insider Theft of Intellectual Property Cases,"Technical Note CMU/SEI-2011-TN-006,Feb.

15 Shaw, E. (2008) "The Insider Threat: Espionage, Sabotage, Fraud—Recent Findings, Implications, Innovations," Presentation at Super Strategies 2008 The Audit Best Practices Conference, Las Vegas, April 14.

16 Stock, H. (2008) "Early Warning Signs: The Psychological Aspects of the Insider Threat," RSA Conference (Executive Security Action Forum), April, San Francisco, CA.

17 Shaw, E., Fischer, L. and Rose, A. (2009) The Insider Risk Evaluation and Audit Tool. August 2009, Defense Personnel Security Research Center, Monterrey, CA. http://www.dhra.mil/perserec/reports/tr09-02.pdf

18 Shaw, E.D. and Fischer, L. (2005) Ten Tales of Betrayal: An Analysis of Attacks on Corporate Infrastructure by Information Technology Insiders, Volume Two: Case Studies," Monterrey, CA.: Defense Personnel Security Research and Education Center.

19 Stock, H. (2011) The Smart Application©, Incident Management Group, Plantation, FL.

20 Wood, S., and 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.

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

22 Randazzo, M., Keeney, M., Kowalski, E. Cappelli, D., and Moore, A. (2005)" Illicit Threat Study: Illicit Cyber Activity in the Banking and Finance Sector," Software Engineering Institute, Technical Report CMU/SEI-2004-TR-021.

23 Shaw, E.D., and Stroz, E. (2004). WarmTouch software: Assessing Friend, Foe and Relationship." In Parker, T. (Ed.), Cyber Adversary Characterization: Auditing the Hacker Mind. June. Syngress Publications, Rockland, Mass.

24 Shaw, E.D. (2004). "The insider threat: Can it be managed?" In Parker, T. (Ed.), Cyber Adversary Characterization: Auditing the Hacker Mind, June. Syngress Publications, Rockland, Mass.

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

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

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

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

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

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

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

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

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

34 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.

About Symantec

Symantec is a global leader in providing security, storage, and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. Headquartered in Mountain View, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our website.

go.symantec.com/dlp

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com

Symantec helps organizations secure and manage their information-driven world with security management, endpoint security, messaging security, and application security solutions.

12/11 21220067