Reprinted from Security Awareness Bulletin, No. 2-98

The Insider Threat to Information Systems[1]

The Psychology of the Dangerous Insider

Eric Shaw, Ph.D., Keven G. Ruby, M.A. and Jerrold M. Post, M.D.

In the information age, as we have become increasingly dependent upon complex information systems, there has been a focus on the vulnerability of these systems to computer crime and security attacks, exemplified by the work of the President's Commission on Critical Infrastructure Protection. Because of the high-tech nature of these systems and the technological expertise required to develop and maintain them, it is not surprising that overwhelming attention has been devoted by computer security experts to technological vulnerabilities and solutions.

Yet, as captured in the title of a 1993 conference sponsored by the Defense Personnel Security Research Center,[2] Computer Crime: A Peopleware Problem, it is people who designed the systems, people who attack the systems, and understanding the psychology of information systems criminals is crucial to protecting those systems.

- A Management Information Systems (MIS) professional at a military facility learns she is going to be downsized. She decides to encrypt large parts of the organization's database and hold it hostage. She contacts the systems administrator responsible for the database and offers to decode the data for $10,000 in "severance pay" and a promise of no prosecution. He agrees to her terms before consulting with proper authorities. Prosecutors reviewing the case determine that the administrator's deal precludes them from pursuing charges.

- A postcard written by an enlisted man is discovered during the arrest of several members of a well-known hacker organization by the FBI. Writing from his military base where he serves as a computer specialist, he has inquired about establishing a relationship with the group. Investigation reveals the enlisted man to be a convicted hacker and former group member who had been offered a choice between prison and enlistment. While performing computer duties for the military, he is caught breaking into local phone systems.

- An engineer at an energy processing plant becomes angry with his new supervisor, a non-technical administrator. The engineer's wife is terminally ill, and he is on probation after a series of angry and disruptive episodes at work. After he is sent home, the engineering staff discovers that he has made a series of idiosyncratic modifications to plant controls and safety systems. In response to being confronted about these changes, the engineer decides to withhold the password, threatening the productivity and safety of the plant.

- At the regional headquarters of an international energy company, an MIS contractor effectively "captures" and closes off the UNIX-based telephonic switching system for the entire complex. Investigators discover that the contractor had been notified a week earlier that he was being terminated in part for chronic tardiness. Further investigation finds the employee to have two prior felony convictions and to be a member of a notorious hacker group under investigation by the FBI. The employee reports he is often up all night helping colleagues with their hacking techniques. Additional investigation reveals that he is the second convicted hacker hired at this site. An earlier case involved a former member of the Legion of Doom who had been serving as a

[1] The article is based on "Insider Threats to Critical Information Systems, Technical Report #2; Characteristics of the Vulnerable Critical Information Technology Insider (CITI)." Political Psychology Associates, Ltd., June 1998. Address comments and questions to Jerrold M. Post, tel. (301) 229-5536 or email jmpost@pol-psych.com.

[2] Defense Personnel Security Research Center (PERSEREC) in Monterey, California, is now the Security Research Center of the Defense Security Service.

member of a corporate information security team. He had been convicted of computer intrusion at a local phone company. Neither individual had disclosed their criminal history or had been subject to background checks sufficient to discover their past activities.

As these case summaries from the files of military and corporate security investigators demonstrate, growing reliance on information technology increases dependence on, and vulnerability to, those tasked with the design, maintenance and operation of these systems. These information technology specialists—operators, programmers, networking engineers, and systems administrators—hold positions of unprecedented importance and trust. Malevolent actions on the part of such an insider can have grave consequences. This is especially true for information technology specialists operating within the critical infrastructure as identified in the 1997 President's Commission on Critical Infrastructure Protection's final report.[3]

These cases also demonstrate several points about the insider threat to the critical infrastructure. First, it is clear that insider problems already exist within the critical infrastructure, including the military, telecommunications, and energy sectors. Second, it appears that both inside and outside of our critical infrastructure, there is a tendency for managers to settle these problems quickly and quietly, avoiding adverse personal and organizational impacts and publicity. We do not really know how widespread the problems are. What is reported appears to be only the tip of the iceberg. Furthermore, we are at risk from repeat offenders, as perpetrators migrate from job to job, protected by the lack of background checks, constraints upon employers in providing references, and the lack of significant consequences for these offenses.

Finally, just as in organizations outside the critical infrastructure, the range of potential perpetrators and their motivations is broad. In many cases, acts of computer sabotage and extortion—like violence in the workplace—have been committed by disgruntled employees who are angry about lay-offs, transfers, and other perceived grievances. Other cases involve employees who take advantage of their position of trust for financial gain,[4] hackers who are employed within the critical infrastructure caught engaging in unauthorized explorations, and "well-motivated" employees who claim they are acting in the best interest of their organizations. Other perpetrators include "moles," individuals who enter an organization with the explicit intent to commit espionage, fraud or embezzlement. Overall, case investigators report that the number of computer-related offenses committed by insiders is rising rapidly each year.

The extent of the insider threat has also been addressed in corporate and government survey results. According to WarRoom Research's 1996 Information Systems Security Survey, 62.9 percent of the companies surveyed reported insider misuse of their organization's computer systems. The Computer Security Institute's 1998 Computer Crime Survey (conducted jointly with the FBI) reported the average cost of an outsider (hacker) penetration at $56,000, while the average insider attack cost a company $2.7 million. A comprehensive study conducted by the United Nations Commission on Crime and Criminal Justice which surveyed 3,000 Virtual Address Extension (VAX) sites in Canada, Europe and the United States, found that "By far, the greatest security threat came from employees or other people with access to the computers." While some researchers warn that survey data on computer crimes can be inaccurate due to unreported or undetected acts, such data is useful in characterizing a minimum level of threat and in drawing attention to the problem as a whole.

Paradoxically, in spite of the prevalence of the insider problem and the particular vulnerability of public and private infrastructures to the information technology specialist, there has been little systematic study of vulnerable insiders, while major investments are being devoted to devising technologies to detect and prevent external penetrations. Technological protection from external threats is indeed important, but human problems cannot be solved with technological solutions. Without a detailed examination of the insider problem and the development of new methods of insider risk management, such an unbal-

[3] According to the PCCIP report, infrastructure is defined as "a network of independent, mostly privately-owned, man-made systems and processes that function collaboratively and synergistically to produce and distribute a continuous flow of essential goods and services." Critical components of the infrastructure, those affecting national security and the general welfare, include: transportation, oil and gas production and storage, water supply, emergency services, government services, banking and finance, electrical power, and information and communication infrastructures.

[4] Our clinical experience indicates that seemingly simple cases of greed are rarely so simple when it comes to perpetrator motivation. Often there are other strong feelings and stressors behind the greed which complicate the motivational profile.

anced approach to information systems security leaves critical information systems vulnerable to fraud, espionage or sabotage by those who know the system best: the insiders.

Research in Progress

In response to the increasing recognition of the dangers posed by the insider threat to information systems, Political Psychology Associates, Ltd., under the auspices of the Office of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence), have undertaken a study to improve understanding of the personality, motives and circumstances which contribute to information technology insider actions. By constructing psychological profiles of perpetrators and mapping their interactions with the organizational environment as they move over time toward the commission of violations, the goal of the study is to contribute to improvements in security, law enforcement and counterintelligence policies and practices. Specific applications for improving screening, selection, monitoring and management of information technology specialists are a primary goal of this research. The findings will also have implications for case investigation, information assurance audits, red team exercises, and information warfare.

The Critical Information Technology Insider

From the broad array of employees who have access to computers, we are focusing on the information technology specialists who design, maintain or manage critical information systems. Employees in this professional category are of particular concern because they possess the necessary skills and access to engage in serious abuse or harm. Typical jobs include systems administrators, systems programmers and operators and networking professionals. We are using the term Critical Information Technology Insiders (CITIs) to designate this professional category.[5]

[5] By definition, the term Critical Information Technology Insider (CITI) excludes the mass of end users who use computers as part of their jobs but for whom computers serve as a tool and not as a job in itself. While end users are associated with their own set of risks, we are specifically concerned with information technology specialists, whose job functions elevate them well above the average end-user in terms of skill, access and potential damage.

Employment Contexts

The employment context is critical for understanding the relationship between the information technology specialist and the organization. The "insider-outsider" dichotomy is oversimplified, for in fact there is a spectrum of relationships between information technology specialists and organizations, which differentially affect loyalty and motivation.

Within the spectrum of "insiders," information technology specialists may serve as regular (full-time or part-time) staff employees, contractors, consultants or temporary workers (temps). In modern business practice, partners and customers with system access are also a source of exposure. In addition, former employees often retain sufficient access to the organization to remain an "insider" threat. Moles, information technology specialists who enter an organization with the intent to harm, are excluded from the current effort because they are potentially very different subjects from a psychological standpoint and present different screening and management problems. In this study we are primarily concerned with information technology specialists who develop their intent to harm the organization after being hired.

Employees (Full-Time and Part-Time)

Staff employees pose perhaps the greatest risk in terms of access and potential damage to critical information systems. As vetted members of the organization, employees are in a position of trust and are expected to have a vested interest in the productivity and success of the group. Considered "members of the family," they are often above suspicion—the last to be considered when systems malfunction or fail.

Among the several types of insider categories, organizations generally have the strongest influence and control over their own employees. To the extent that an employer is permitted by law to probe the background of a potential hire for security purposes, such investigations are much more likely to occur with prospective employees than with contractors, consultants, or temporary workers, whose roles in the organization are by design transient and who may or may not be vetted.

Employee CITIs who have caused damage have used their knowledge and access to information resources for a range of motives, including greed, revenge for perceived grievances, ego gratification, resolution of personal or professional problems, to protect or advance their careers, to challenge their skill, express anger, impress others, or some combi-

nation of these concerns. Three case examples serve to illustrate the employee threat:

Example 1: A senior MIS specialist at an international energy firm regularly created outages at Company sites around the world so that he could spend time abroad while gaining attention for his technical expertise.

Example 2: Michael Lauffenberger, a 31-year old programmer for the General Dynamics Atlas Missile Program, reportedly felt unappreciated for his programming work on a parts-tracking system. He planted a "logic bomb" in the system designed to erase critical data after he resigned. He then anticipated returning to rescue the company as a highly paid and valued consultant.

Example 3: Regional PC manager for the King Soopers supermarket chain Jay Beaman and two clerks were charged in an intricate computer fraud that cost the supermarket over two million dollars over two years. The motives are described by investigators as beginning with financial necessity but quickly escalating into greed and ego. Among the strategies used was manipulating the computer accounting system to funnel certain purchases into a dummy account. At the end of the day, the perpetrators would take the amount funneled into the dummy account right out of the cash registers and then delete the account, also erasing any trace of their fraud.

In examples 1 and 2, the employees used their knowledge and access to a critical system to create crises, which would magnify their importance and worth within the organization. Jay Beaman was able to use his position to both commit and cover up his fraud, emphasizing the vulnerability of organizations to trusted employees.

Contractors, Partners, Consultants and Temps

Contractors, partners, consultants and temps are included as a category separate from employees because they are often not, in practice, subjected to the same screening and background checks. Moreover, a lesser degree of loyalty to the firm or agency would be anticipated. Many organizations within the critical infrastructure but outside the intelligence community have little control over the pre-employment procedures and hiring practices utilized by a contractor or consulting group. This is true even though contractors and consultants (and sometimes temps) often have highly privileged access to the organization's information assets due to the increase in outsourcing of programming and other information technology functions.

While the contracting organization is well within its rights to require contractors to screen the employees that will be working within the organization or provide a separate screening process for contracted employees, such steps are rarely taken, putting the organization at risk. The same goes for consultants and temps, though the transient nature of the consulting or temporary working relationship presents practical barriers to more rigid screening processes. The hiring of former hackers by some computer security consulting firms further increases the risk of security compromises. Employers have also consistently underestimated the ability of contractors and consultants to take advantage of even limited access to important systems.

Example 4: A major international energy company recently discovered a logic bomb in software created by a contracted employee. It was installed as "job insurance" by the contracted employee with five prior convictions related to hacking. The contractor's firm failed to screen this employee who installed the code in anticipation of using it as leverage against his employer in case his criminal record was discovered.

Example 5: Zhangyi Liu, a Chinese computer programmer working as a subcontractor for Litton/PRC Inc., illegally accessed sensitive Air Force information on combat readiness. He also copied passwords, which allow users to create, change or delete any file on the network, and posted them on the Internet.

Example 4 illustrates the problems posed by poor screening measures and the vulnerability of organizations outsourcing their information technology functions. Example 5 demonstrates the espionage threat posed by contractors, though the motivations of this particular perpetrator are not yet clear. It also emphasizes the complex issues of loyalty in an international environment.

Former Employees

Former employees include individuals who no longer work at an organization but retain access to information resources directly—through "backdoors"—or indirectly through former associates. Anticipating conflict with an employer, or even termination, these perpetrators may prepare backdoor

access to the computer system, alternative passwords, or simply stockpile proprietary data for later use. The number of cases in which separated employees have returned to extract vengeance on their former employers indicates a need for improved management of the termination process. This is particularly the case in episodes involving large numbers of layoffs. Such reductions can result in a pool of disgruntled employees and former employees with access and motivation for vengeance.

> **Example 6:** Donald Burleson, a computer programmer for USPA & IRA Co., a Fort Worth securities trading firm, designed a virus after being reprimanded for storing personal letters on his company computer. The virus was designed to erase portions of the Company's mainframe and then repeat the process if a predetermined value was not reset in a specific location. After being fired, Burleson used a duplicate set of keys to return to the facility at 3 a.m. and employ an unauthorized backdoor password to reenter the system and execute the virus

The Indispensable Role of the Insider

It is important to note that the efforts of "outside" groups (including foreign interests) could be aided significantly by the assistance of parties within the organization with access to, and knowledge of, critical information systems. For certain secure, self-contained systems, the insider's access will prove indispensable. Whether the insider is recruited directly, indirectly (e.g. "false flag" recruitment), coerced through blackmail, or through "social engineering" is manipulated while unaware that he is providing assistance to an adversary, his collaboration is a tremendous force multiplier. The potential damage an insider can now commit has also been increased within the last decade by two related trends in information systems—consolidation and, for all intents and purposes, the elimination of the need-to-know principle. These changes, designed to improve information sharing, have removed obstacles to hostile collection. The hostile, sophisticated information technology professional now has many more opportunities to enter and damage larger systems. These vulnerabilities led one government information technology specialist, who focuses on system security, to refer to many allegedly secure government databases as "single point of failure systems."

> **Example 7:** On the programming staff of Ellery Systems, a Boulder Colorado software firm working on advanced distributive computing software, was a Chinese national who transferred, via the Internet, the firms entire proprietary source code to another Chinese national working in the Denver area. The software was then transferred to a Chinese company, Beijing Machinery. Ellery Systems was subsequently driven to bankruptcy by foreign competition directly attributed to the loss of the source code.

As illustrated by this case, the foreign connections of information technology specialists can increase their vulnerability to recruitment, manipulation, or independent hostile action.

Personal and Cultural Vulnerabilities

Case studies and survey research indicate that there is a subset of information technology specialists who are especially vulnerable to emotional distress, disappointment, disgruntlement and consequent failures of judgment which can lead to an increased risk of damaging acts or vulnerability to recruitment or manipulation. Moreover, there are characteristics of the so-called "information culture" which contribute to this vulnerability. This report is not an attempt to cast suspicions on an entire professional category whose role in the modern computer-based economy has become so critical. However, we must better understand the motivations, psychological makeup, and danger signals associated with those insiders who do pose a threat to our information systems before we can really address this problem.

Reports of past research and our own findings based on interviews conducted so far, lead to the conclusion that there are several characteristics which, when found together, increase this vulnerability toward illegal or destructive behavior. These include: computer dependency, a history of personal and social frustrations (especially anger toward authority), ethical "flexibility," a mixed sense of loyalty, entitlement, and lack of empathy.

Introversion

According to a 1991 study by Professor Kym Pocius, the psychological testing of over fifteen hundred computer programmers, systems analysts, programmer trainees, and computer science students in seven separate studies consistently found these groups to be "overwhelmingly represented by intro-

verts." Introverts differ from extroverts in being oriented toward the inner world of concepts and ideas rather than the outer world of people. They enjoy being alone, prefer their own thoughts to conversation with others and may be socially unskilled. They also tend to be over-conscientious, secretive, pessimistic and critical. Authorities on the subject tell us that introverts are harder to distract than are extroverts, yet they are more reactive to external stimuli. According to H. J. Eysenck, a prominent personality psychologist, introverts tend to "shy away from the world while extroverts embrace it enthusiastically."

We wish to emphasize that, unlike the traits we are about to delineate, introversion is characteristic of computer technology specialists as a group, as well as scientists and other technology specialists. Indeed, some 40% of the overall population demonstrate this trait. One could not eliminate introverts from the ranks of computer technology specialists without eliminating the specialty. However, the preference for individual intellectual pursuits as opposed to interpersonal activity means that the signs of employee disaffection which would be apparent for extraverted employees may not be so readily visible. They may only occur, in fact, on-line, so the introvert poses challenges to management.

The following vulnerabilities have been identified in individuals who commit dangerous acts. They are associated with the vulnerable subgroup within computer technology specialists.

Social and Personal Frustrations

Surveys of computer professionals and computer science students indicate the presence of a subgroup whose entry into the field is motivated, in part, by frustrations related to getting along with others. According to a 1993 study by Professor R. Coldwell, this subgroup reports a history of conflicts and disappointments with family, peers and coworkers. They report preferring the predictability and structure of work with computers to the lack of predictability and frustrations of relationships with others. These experiences appear to have left them with a propensity for anger, especially toward authority figures. They also tend to be less socially skilled and more isolated than are their peers. Noting the high incidence of anger and alienation in these computer science students, Coldwell labeled it "revenge syndrome."

These traits create an increased vulnerability to feelings of alienation, disgruntlement, and disappointment on the job. Not only are such employees more likely to have innate antagonism for their supervisors, but they are less likely to trust and to deal directly with authorities when problems arise. In turn, these characteristics may also make some of these employees more vulnerable to recruitment and manipulation.

Computer Dependency

Two identified subgroups of computer users include individuals who exhibit an addictive-like attachment to their computer systems and those who manifest a similar attachment to the on-line experience offered by networks such as the Internet. Behavioral scientists studying these subgroups have found that they spend significantly more time on-line than is necessary for their work, frequently report losing any sense of the passage of time while on-line, and find that their on-line activities interfere significantly with their personal lives.

The "computer-addicted" individuals studied by researcher Margaret Shotten (1991) reported their primary interest as exploring networks, and viewed breaking security codes and hacking as honorable means of gaining emotional stimulation by challenging and beating security professionals. They did not consider pirating software unethical.

Computer dependents share a history of social failures and ostracization; and they admitted that the computer replaces direct interpersonal relationships. Their family histories include a high percentage of aloof, cool, and disinterested parents and authoritarian fathers. On formal psychological testing, this group contains a high percentage of well-informed, scientific, problem-solvers who enjoy intellectual pursuits. They are significantly more likely to be independent, self-motivated, aggressive loners, who make poor team players and feel entitled to be a law onto themselves. They reportedly tend to exhibit an unusual need to show initiative to compensate for underlying feelings of inadequacy.

Other researchers found that many members of the Internet-addicted subgroup are deeply involved in computer-mediated relationships, including role-playing games. For many introverted, less socially skilled individuals, their computer-mediated social contacts are the least anxiety arousing of their interpersonal experience. In some cases, the sense of self, experienced on-line, becomes greatly preferred to the experience of self in the real world. Correspondingly, the on-line relationships of these individuals can displace affections and loyalties from real world ties. Noting the power of these relationships, many men-

tal health professionals have characterized them as therapeutic building blocks for some which can help make the transition to subsequent real world contacts. However, for other more vulnerable individuals, these on-line relationships may also constitute an avenue for influence, recruitment or manipulation with security implications.

Ethical "Flexibility"

Concerns have been raised about looser ethical boundaries within the so-called "information culture." Surveys in recent years of current computer professionals indicate the presence of a subgroup whose members do not object to acts of cracking, espionage and sabotage against information resources. This subgroup appears to maintain the position that if an electronic asset, such as a limited access file, is not sufficiently secure, then it is fair game for attack. A disturbing aspect of these finding is the association between decreased ethical constraints and youth, suggesting that this perspective may be shared increasingly among new and future employees.

A number of social phenomena have been cited by several researchers as contributing to this dangerous trend. Lack of specific computer-related ethical training and regulations within organizations have been implicated as contributing to lax employee ethical attitudes. Lack of similar ethical training in schools and at home by parents also contributes to this cross-generational trend. The boundary ambiguities of cyberspace, especially the lack of face-to-face connection, may also insulate perpetrators from the impact of their acts. The idea that exploring and even copying others' files inflicts no real damage has also been used to rationalize what would otherwise be considered privacy violations and theft in the outside world.

Finally, the computer industry has been implicated in the erosion of its own ethical standards. Some critics have suggested that the introduction of what they view as unrealistic and impractical restrictions on the use of purchased software produced contempt and disregard for these standards. Other critics suggest that the hiring and promotion of former hackers has sanctioned hacking and has even produced an incentive for this behavior.

Reduced Loyalty

Organizational loyalty among programmers and other professionals has been challenged increasingly by the high demand for their services and high rates of turnover in the profession. The resulting pressures to hire and retain computer professionals have also placed tremendous pressure on the security process.

Commenting on interviews with insider perpetrators of computer crime by the President's Council on Integrity and Efficiency, computer security expert Sanford Sherizan addressed the issue of distinct differences in programmer loyalty. Sherizan noted that there appear to be programmers who identify with the organization that pays them while others identify with the profession of programming itself. For these latter employees, their weak bond to the organization can lead to tensions in the workplace. Ambiguities about the "ownership" of intellectual properties in the form of source codes and other programs have also lead to a large number of conflicts between employers and computer professionals.

Entitlement

Our clinical investigations of vulnerable CITIs have consistently revealed two additional traits as risk factors, which have been alluded to but have not been emphasized. In assessments of CITI perpetrators from the energy and national security infrastructures, we have found that a sense of entitlement and anger at authority are consistent aspects of perpetrator motivation and personality.

A sense of entitlement, associated with the narcissistic personality, refers to the belief that one is special and owed corresponding recognition, privilege or exceptions from normal expectations. This sense of "specialness" is often associated with a self perception of gifts or talents which are unrecognized by others. The perception that this specialness is not being recognized by authority figures often combines with a pre-existing anger at authority to produce feelings in these individuals that they have been treated unjustly and are entitled to compensation or revenge. Often, this sense of entitlement is supported by special arrangements or exceptions to rules granted to highly valued but "temperamental" MIS employees. Thus employers actually reinforce this belief, up the ante, and contribute to what often becomes an inevitable crisis. The current shortage of information technology personnel may also influence feelings of entitlement among older information technology employees, who may resent special treatment and bonuses paid to new hires.

According to a 1991 report by psychologists Robert Raskin and Jill Novacek, individuals with these narcissistic tendencies who are under higher levels of daily stress are prone to "power and revenge fantasies in which they see themselves in a powerful

position able to impose punishment on those who have wronged them."

Our clinical sample helps validate a concern expressed by Coldwell about a group of programmers and computer science students who he characterizes as suffering from "revenge syndrome." Interviewees in this group appeared to present very similar perspectives and motives. As one interviewee in the previous study commented, when asked how he might utilize the power he was acquiring with his knowledge of programming, "I'll be getting my own back on the society that screwed me up."

Lack of Empathy

Disregard for the impact of their actions on others, or inability to appreciate these effects, has been a perpetrator characteristic noted consistently by investigators. It is also consistent with our clinical experience. Perhaps compounded by the impersonal layers of cyberspace, many computer perpetrators report never having considered the impact of their acts on other human beings. Many more appear incapable of placing themselves in their victim's shoes and imagining how the experience felt. This lack of empathy is a hallmark of individuals with narcissistic and anti-social personalities, and is consistent with the traits of reduced loyalty and ethical flexibility.

Summary of Vulnerable CITI Personal and Cultural Characteristics

In summary, the research literature which we have surveyed identifies a coherent cluster of risk factors characteristic of a vulnerable subgroup of Critical Information Technology Insiders (CITIs). The negative personal and social experiences of a subgroup of information technology specialists tends to make them more vulnerable to experiencing the personal and professional frustrations which have been found to drive insider espionage and sabotage. Their social isolation and relative lack of social skills probably reduces the likelihood of their dealing with these feelings directly and constructively. Their reported vulnerability to ethical "flexibility," reduced loyalty to their employers, feelings of entitlement, anger at authority and lack of empathy probably reduces inhibitions against potentially damaging acts. At the same time, their loneliness, social naiveté and need to impress others may make them vulnerable to exploitation and manipulation.

The presence of any or all of these personal and cultural vulnerabilities does not, however, a perpetrator make. Indeed, it is more often the dynamic interaction between the vulnerable CITI's personal psychology (including the vulnerabilities enumerated above) and the organizational and personal environment that leads the vulnerable CITI down a slippery slope, at the end of which an act of information system aggression occurs. These critical pathways—plural, for there are no set routes for the path to deviant, antisocial behavior—that a CITI perpetrator might travel are being defined and explored further in the course of our research program.

What we do know already is that there is a complex interplay of personal and cultural or environmental factors which, over time, funnel an individual toward insider actions and that an understanding of this critical pathway has implications for personnel screening, monitoring, case management, and training. We also know that predisposing traits and situational factors are only part of the problem. What might be called acute situational stressors such as marital or family problems, episodes of substance abuse, disappointments at work, threatened layoffs, or other stressful life events can trigger an emotional reaction leading to impaired judgment and reckless or vindictive behavior.

The Impact of Intervention

Nevertheless, there are also mitigating forces that appear to reduce the likelihood of committing such acts or defuse a specific threatening situation. Highest on the list of mitigating factors is effective intervention by supervisors, co-workers, family members and close friends. Intervention might lead to counseling, involvement with support groups, or medical assistance. It is essential, however, that those who might intervene recognize and respond to significant warning signs and symptoms.

The Critical Pathway in Insider Espionage

A lucid description of the critical pathway to insider actions comes from Project Slammer, a major study of Americans convicted of espionage. Project Slammer mental health professionals conducted extensive interviews and formal psychological assessments with convicted perpetrators, most of whom were insiders. They also interviewed their coworkers, supervisors and families to identify not only the characteristics of perpetrators, but also the chain of events which led to their acts of treason. The results identified an interaction of factors, none of which alone was sufficient to result in an act of espionage.

However, taken together and over time, these traits and experiences, common to many of the perpetrators, appear to have formed what we view as a common pathway to these acts. This pathway includes the following combination of events or "steps" which in some cases led to severe damage to national security:

- Predisposing Personal Traits
- An Acute Situational Stressor
- Emotional Fallout
- Biased Decision-making or Judgment Failures
- Failure of Peers and Supervisors to Intervene Effectively

As noted above, outside intervention is a critical mitigating factor on the path to insider acts. Unfortunately, in the insider espionage cases examined, it was often absent. Peers often assumed supervisors or others were aware of, and attending to, the problem. Supervisors often ignored the employee's problems, not wanting to deal with difficult individuals or not wishing to risk losing a valued member of the team. Often they attempted to manage the problem without considering the security risks involved. Sometimes the problem was pushed aside by transferring or firing the employee. It is interesting to note that a significant number of espionage offenders commit their acts after leaving their organizations. Abrupt termination does not appear to be a productive way to eliminate the security threat posed by such at-risk employees. Other supervisors incorrectly assumed that psychological referrals or on-going mental health counseling automatically took care of the problem and eliminated the risk of insider acts without requiring other intervention.

In the cases of destructive and criminal acts by vulnerable CITIs that we have analyzed to date, we are seeing a similar pattern in the sequencing of events. In a number of cases evaluated so far, we are confronted with examples of management failure to notice the problem, to accept the fact that a problem exists, or a willingness to tolerate dangerous behavior due to a desire to retain the services of a valued, technically competent employee. These findings have several implications for personnel management:

Pre-employment Screening

The critical path model views the probability of insider acts as the product of the interaction between predisposing traits, situational stressors and the organizational environment. Initial screening of employees should therefore emphasize the collection of information regarding traits, past and current behaviors (especially a criminal records check), and circumstances indicative of risk that is specifically tailored to the profile of the vulnerable CITI. Behaviors particular to the world of the computer professional should be central to this inquiry. Furthermore, successful screening will require that human resources and information systems recruiters be sensitized to the factors contributing to CITI risk to guide them in the hiring process.

Improved Management of CITIs

Overall, the three most general management errors we have noted regarding CITI offenders have been (1) the failure to understand the personality and motivation of the at-risk employee; (2) the failure to have clear, standardized rules governing the use of company information systems with explicit consequences of misuse; and (3) the failure to enforce rule violations. These problems often result in inadequate or even aggravating rules of conduct when constructive relief would be possible. Without organizational rules of conduct, employees have no guide to right and wrong and supervisors have no recourse to consequences when clear violations are discovered.

The company may also be held liable for illegal acts committed by employees in the absence of a well-defined and supported code of ethics. Solutions include specialized training for IT (information technology) managers to facilitate recognition of vulnerable CITIs and the selection of proper intervention techniques. The implementation of a comprehensive compliance program is also essential and should include a well-defined code of ethical behavior and support for employees facing ethical dilemmas or with questions regarding company policy.

Innovative Approaches to Managing At-Risk CITIs

For reasons discussed above, computer professionals present significant management challenges. In particular, monitoring their psychological state for risk using conventional observations is extremely difficult. As noted earlier, a subset of these individuals are likely to be more vulnerable to work-related stressors, while at the same time be much less likely to display overt signs of distress, complicating detection and delaying appropriate intervention by IT managers.

Compounding this problem is the shift of work-based communications toward computer-mediated communications in the workforce, a trend vastly

accelerated among IT professionals in general, especially among those CITIs who find e-mail or chat rooms their preferred channel for maintaining professional and personal relationships. The characteristics of the vulnerable CITI will inevitably require adapting traditional monitoring and intervention techniques to at-work electronic communications as the most effective means of understanding the psychological state and risk among these employees.

Innovative approaches for managing computer professionals include the creation of on-line environments designed to relieve work related stress by providing professional and constructive advice on dealing with problems in the office, e.g., on-line Employee Assistance Programs or job-stress hotlines. Electronic bulletin boards for logging anonymous complaints that can be monitored by management for purposes of addressing general grievances have also proven effective in some situations

One approach to effectively manage at-risk employees whose behavior has raised concern is to monitor their at-work electronic communications. This can be effectively used to detect changes in psychological state which warn of increased risk of destructive acts. While this approach raises privacy concerns, legal precedent has generally upheld the right of the employer to monitor their employees' use of company owned systems.

Comprehensive Information Security Audits

Finally, the critical path approach can also add a human element to the information security audit and its traditional emphasis on technological vulnerabilities and fixes. By reviewing the manner in which an organization selects, promotes, monitors, detects, manages and intervenes with problem CITIs, an investigator can gauge the organization's general sensitivity to insider risk and provide constructive solutions to managing the insider problem.

Only by adapting a comprehensive approach applying technological and human factors to information security can an organization adequately protect itself from both the outside threat of hackers and the more serious threat posed by the disaffected insider.

Editor's note: This is the first in a series of reports of research related to the issue of ensuring the reliability and trustworthiness of employees holding a position of trust in government and critical defense industries. We are grateful to Political Psychology Associates, Ltd. (PPA) for allowing us to publish this valuable interim report on the status of their research on the insider threat to critical information systems. Readers interested in further information on the Dangerous Information Technology Insider Project or for a full copy of the report when it is released, may contact Dr. Post at jmpost@pol-psych.com. In the next phase of this research program, PPA will be interviewing "insider" perpetrators of computer crime and is currently seeking interview subjects. PPA would welcome learning of perpetrators who might be available for interview on a confidential basis.