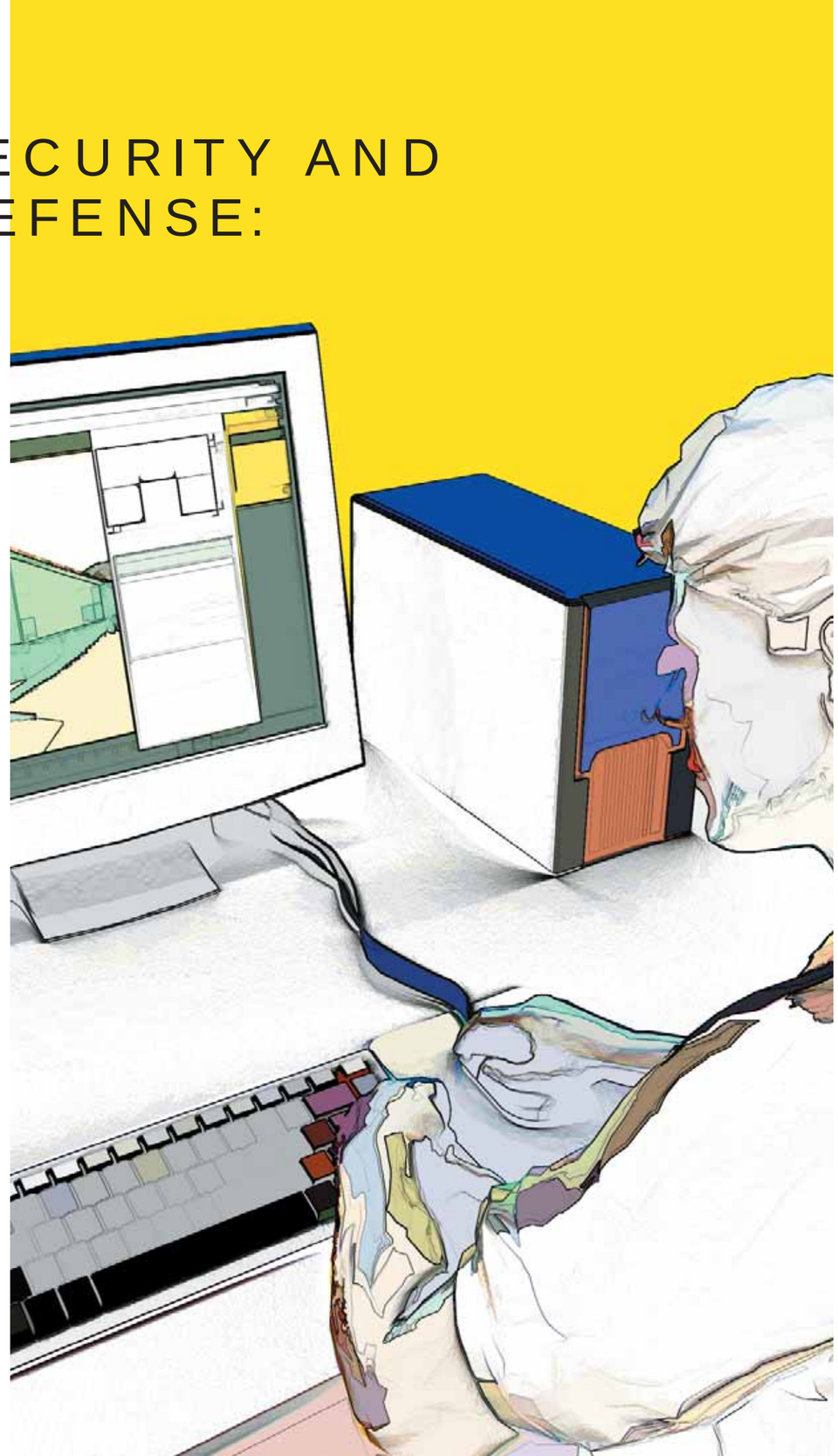
# HOMELAND SECURITY AND HOMELAND DEFENSE: The Insider Threat

By Martin Hershkowitz



All speeches, memoranda, magazine and journal articles, congressional discussions and the "talking heads" of television address their material on homeland security (HS) and homeland defense (HD) to an "outsider" attack (i.e., individuals or groups not belonging to the organization or locale under attack). Any attack against this country's infrastructure and population, against its very political, economic, social lifestyle by foreign or homegrown terrorist organizations is a dynamic target for the country's HS/HD protective efforts. However, there is a paucity of oral or written comment about the "insider" threat.

The insider is an employee who can thwart the HS/HD mission by a deliberate or inadvertent (that is, unplanned) act of sabotage against or theft of or damage to hardware, software, classified material and/or secured operational plans and programs. In light of the fact that there exist many sleeper saboteur and/or terrorist groups and willing support groups, it is no stretch of the imagination to recognize that moles may, and most likely do, hold critical insider positions within government, industry and HS volunteer groups. Add to this, that some criminal groups will see a source of high-tech equipment and secured information that can provide a significant profit, and the potential insider group will grow through additional moles and/or the threat of physical harm or social intimidation and extortion.

Unfortunately, not all insiders can be classified as saboteurs, terrorists or criminal moles.





Employees can be considered a potential insider threat if they are addicted to or a regular user of illegal drugs; an alcoholic or regular user of alcohol to extreme; psychiatrically or psychologically impaired; deeply indebted, particularly to unofficial or criminal money lenders; spousal and/or child abusers; or any other condition arising over time that might cause them to fail or be ineligible for a security clearance or position of trust.

## An Awareness of the Insider Threat

The insider can be responsible through malicious behavior or poor judgment for a variety of undesirable situations. One of the more readily recognizable areas is the attack of and damage to the organization's information resources, which can be directly related to the "bottom line." However, the form of malicious behavior or poor judgment that is most often overlooked by the organization's leadership is that which can lead to unacceptable damage to its facilities, employees and/or surrounding environment.

## Information Resources

Verdasys, a company specializing in information security solutions and protecting intellectual property, established a corporate policy for protecting its "precious assets" through enforcing usage policies with regulatory requirements and reducing offshore usage outsourcing risks, individual accountability and forensic investigation.

The Advanced Countermeasures for Insider Threat Workshop, February 3-4, 2003, cosponsored by NIST and ARDA, determined that "defending against insiders who would abuse their computer privileges is one of the most critical problems facing the information security community."

The RAND Corporation sponsored and participated in a series of workshops dealing with the insider threat, developing models for anticipating the threat and effectiveness against the malicious insider. Their report, "DOD Insider Threat Mitigation Plan: Final Report of the Insider Threat Integrated Process Team" (2000), contained over 50 recommendations, both short term and long term, regarding mitigating the insider threat.

The lDG News Service reported on April 30, 2004, that the Mohegan Tribe's Mohegan Sun Casino contracted with Intrusic of Waltham, Massachusetts, for technology "... to spot the surreptitious behavior that may indicate the workings of a rogue employee, malicious external hacker or compromised computer." John Pescatore, Vice President of Gartner, commented in the news release that a number of companies have appeared with products making similar promises, further saying that "... despite a plethora of choices, enterprise demand for insider threat detection products is still low."

Sharon Gaudin said in Network World, March 4, 2002, that the U.S. Secret Service authorized a study of insider-based computer security breaches to ultimately help IS executives protect their systems. Deputy Special Agent James Savage is quoted as saying, "Information data is the new currency of choice in the criminal community," further emphasizing that the organization's information resources have been identified as an area of significance to the insider threat.

The Defense Intelligence Agency's Counterintelligence and Security Activity produced a guide based on a 2002 study by the Defense Personnel Security Research Center "...to help its members understand their responsibilities for reporting suitability issues and potential espionage indicators that may surface in a colleague's behavior." The guide lists examples of suitability issues and potential espionage indicators.

Britain's MI5, in a security advice release entitled "Managing Staff Securely - The 'Insider' Threat," stated that "some external threats, whether criminal, terrorist or espionage, or from competitors seeking a business advantage, depend entirely upon the co-operation of an 'insider' in your organization or business, whether from your permanent, temporary or contract staff." The advice release contains a set of recommendations for determining suitability of new employees and some rules for controlling their access to sensitive information and a similar, but different, set of recommendations for hiring and controlling the access of contractor organizations and their employees.

## Other Than Information Resources

Although there is great concern over the potential damage an insider can cause to the organization's information resources, that damage is to the "bottom line" rather than to the total organization's facilities, employees, local community or surrounding region. Those industries and government facilities dealing with materials that can cause such unacceptable catastrophic impact, such as nuclear weapons, nuclear energy, hazardous chemicals, biological sources and/or explosives, as well as airborne, seaborne, rail

and road transportation, face an even greater need to deal with their insider threat. Unfortunately, very few have implemented a full anti-insider threat program.

One of the earliest reported concerns over the insider threat was by Daniel Hirsch of the Nuclear Control Institute in the early 1980s when he raised the issues of the truck bomb and the insider threat. He said at the time, "In the field of nuclear safeguards and security there is a tendency to protect against threats that are relatively easy to address and to ignore those that are somewhat more difficult." Hirsch added, "Even were nuclear facilities adequately protected against external attack ... the greatest security risk - the threat of action by insiders - would remain."

The North Carolina Department of Transportation in February 1999 recognized the catastrophic potential of the insider threat and established its "Controlled Substances Abuse and Alcohol Misuse Standard Policy and Procedure." Their policy is zero tolerance due to the magnitude of potential results of controlled substances abuse and alcohol misuse, which can range from personal injury or equipment damage to death of co-workers or the traveling public.

The U.S. Department of Energy (DOE) is responsible for all research, development, construction and stockpiling of the nation's nuclear weapons, where deliberate or inadvertent (that is, unplanned) sabotage by an insider can be catastrophic. DOE, recognizing this problem, established a Personnel Assurance Security Program (PSAP) [formerly, the Human Reliability Program (HRP)] to deal with the insider threat and established the Center for Human Reliability Studies to conduct annual training and continuing research on improved detection techniques and legal concerns. Initially, some 20,000 employees were trained and examined under the provision of the PSAP [see the Code of Federal Regulations (CFR) 10, Part 710, Subpart A, FR 10068, Vol. 56, No. 46 for details]. The military has a similar program entitled the Personnel Reliability Program (PRP). The somewhat milder requirements of the PRP at that time were due to the somewhat lesser catastrophic damage than could occur. In a 2004-revised regulation, the DOE published 10CFR, Part 712 reestablishing the HRP from the PSAP and making alcohol testing mandatory.

## Components of an Anti-Insider Threat Program

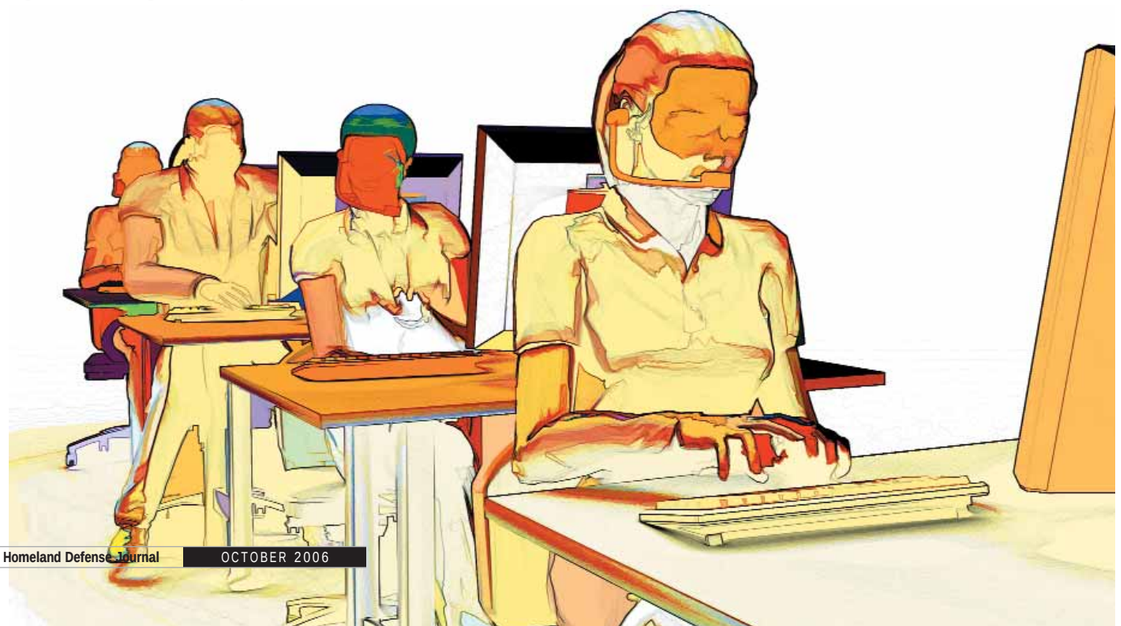
The program outlined below is one in the extreme for a threat whose successful outcome can be catastrophic in the extreme. An organization wishing to establish such a program should first determine the extent of damage to the HLS/HLD mission their insider threat can accomplish. With this "extent of damage" determination in hand the organization can then pick and choose among the components outlined below and the extent to which they may wish to incorporate each selected component.

## Medical Examination

Only those individuals involved in stressful, strenuous and/or laborious activities need to undergo a full physical examination under this program. Members of the military, including the Reserve Forces and the National Guard involved in HS/HD missions, Federal, State and Municipal police, firefighters, and First Responders are all candidates for an annual full medical examination. Other groupings can be added as the organization determines the need. Blood tests taken as part of the examination can provide further insight in other components. The Occupational Medicine Physician's responsibilities include a determination of the individual's ability to fully perform his or her position's tasks based on the physical examination, personal interview and results of the psychiatric and/or psychological examination(s).

## Psychiatric Examination

A psychiatric examination, including an interview by a Board Certified Psychologist a desirable for all employees involved in HS/HD missions in order to establish a psychological baseline for most of the employees and to eliminate the few who would be in danger of causing inadvertent (that is, unplanned) sabotage, even though they might not be a saboteur, terrorist or a terrorist's or criminal's unwilling accomplice. This examination can be repeated only when an employee begins to display characteristics that cause concern among fellow employees and management, or for a member of the military or First Responders exposed to a high degree of stress.







## Psychological Examination

A psychological examination by a Certified Clinical Psychologist should be performed every two or three years in order to build on the psychological baseline and to detect early signs of terrorist discipline breakdown or anxiety development among employees under continuing stress from the HS/HD missions. Desirable tools for this component are a Clinical Psychologist interview and both standardized and special purpose tests seeking signs of terrorist, criminal or untrustworthiness characteristics. The combination of this (these) examination(s) and the individual's psychological baseline form valuable input to the Occupational Medical Director's final medical determination.

## Testing for Illegal Use of Drugs

This component does not differentiate between the drug addict and the regular user of drugs. In either case, the employee is exhibiting the characteristics of untrustworthiness and can be considered to be dangerous to the success of the mission, either intentionally or inadvertently. Testing should be random in nature, with a requirement that every employee be tested at least once each year. The test should include protocols for all illegal drugs and for legal drugs obtained illegally.

## Testing for Alcohol Abuse

This component does not differentiate between the alcoholic and the use of alcohol to an extreme. In either case, the employee is exhibiting the characteristics of untrustworthiness or poor judgment and can be considered to be dangerous to the success of the mission, either intentionally or inadvertently. Testing for alcoholism can be accomplished by such standard measures as a physical examination by a physician or psychiatrist. Testing for the use of alcohol to an extreme is much more complicated, as it is typically detected by friends, family members and, occasionally, fellow employees. In this case, the detector will feel like a "snitch" for reporting the employee. This is not an easy problem to deal with; however, not dealing with it can surely jeopardize the mission. Mandatory random unannounced breath alcohol testing is desirable.

## Personnel Security Review

Only personnel security adjudicators or evaluators can review the full scope of problems that an employee can encounter. In particular, they should perform a National Security Review seeking information on any criminal activity on a national level. Next, they should review all police records in the counties of residence and employment as well as all surrounding counties to determine if the employee has a history of criminal activity or spousal and/or child abuse. Next would be a financial check to determine financial responsibility or the possibility of loans from an unofficial or illegal money source. The result of these searches and the results from the five components above yield a full picture to the personnel security adjudicator or evaluator of the trustworthiness or untrustworthiness of the employee being reviewed. The adjudicator or evaluator can then join with the Occupational Medical Director and management to determine the desirability of hiring or continued employment of the individual under consideration.

## Training

Training may be one of the most complex, but necessary components of an anti-insider threat program. In addition to exposing the employees to the extent of the program they will be required to undergo in order to be a member of the HS/HD team, all employees and management should be trained to recognize those characteristics that imply that an individual may be a saboteur, terrorist, criminal or simply dangerous person for their mission(s) and how to handle the next steps. Similar training for armed security guards adds the complexity that the individual is now armed and must be treated with the utmost of care. Occupational physicians, psychiatrists, clinical psychologists and personnel security adjudicators or evaluators should be trained and annually reminded to recognize the characteristics of interest and, to some extent, to understand each other's analytical concerns. Finally, attorneys should undergo annual training on national, state and local laws governing allowable incursion into an employees perceived rights. Many of these issues have already been decided in favor of the employer; however, the employees' attorneys continue to raise variations on each situation.

## Employee Rehabilitation Program

The employer should consider establishing an Employee Rehabilitation Program to assist employees who are found to be undesirable for a position on a HS/HD team. Such a program may assist in reclaiming a desirable employee for other meaningful activities. A Psychiatric Social Worker, aware of the malicious behavior or poor judgment exhibited by the employee and trained to seek a rationale for such behavior, may very well assist in uncovering a saboteur, terrorist or criminal, or an employee who is being extorted by them.

## A Concluding Thought

By now it should be obvious that the insider threat is as dangerous as the outsider threat and may be more so. Consider, for instance, the totally "clean" individual with well-hidden ties to the espionage, terrorist or criminal communities, whose sole charter as a "sleeper" is to infiltrate and eventually control the organization as the Chief Executive Officer, Chief Operation Officer, Chief Financial Officer or General Counsel (in the language of the mobster community of the 1940s, '50s, '60s and '70s, the "Button" man). The inappropriate actions of such a person in an organization's leadership can be catastrophic. The organization that recognizes the need and establishes a strong and efficient anti-insider threat program initially may see a slightly lower profit margin; however, they should see an increased requirement by others for these program components, which in the long term will greatly enhance their profits. More importantly, such organizations will improve the protection provided for their employees, facilities, local community and region by an enhanced HS/HD team.

Martin Hershkowitz is Executive Consultant for Hershkowitz Associates and Executive Advisor to the Managing Partner and Senior Homeland Security Advisor for the Greenville Group, LLC. He has served for 17 years as a Senior Security Officer for Nonproliferation and National Security concerned with the safeguards and security of nuclear weapons and the mitigation of the "insider threat." He is also a retired Maryland Defense Force (MDDF) Colonel. He is currently Editor of the State Defense Force (SDF) Publication Center, producing both the SDF Journal and the SDF Monograph Series, and is a member of the Executive Council of the Military Emergency Management Specialist (MEMS) Academy, sponsored by the State Guard Association of the United States.