LA-UR- 93-1181

Title: Addressing the Insider Threat

Author(s): Judith G. Hochberg
Kathleen A. Jackson
Jimmy F. McClary
Dennis D. Simmonds

Submitted to: The DOE Computer Security Group Conference

MASTER

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

Los Alamos
NATIONAL LABORATORY

Addressing the Insider Threat*

Judith G. Hochberg, Kathleen A. Jackson, J. F. McClary, Dennis D. Simmonds
Computing and Communications Division
Los Alamos National Laboratory
Los Alamos, New Mexico 87545

Abstract

Computers have come to play a major role in the processing of information vital to our national security. As we grow more dependent on computers, we also become more vulnerable to their misuse. Misuse may be accidental, or may occur deliberately for purposes of personal gain, espionage, terrorism, or revenge. While it is difficult to obtain exact statistics on computer misuse, clearly it is growing. It is also clear that insiders -- authorized system users -- are responsible for most of this increase. Unfortunately, their insider status gives them a greater potential for harm.

This paper takes an asset-based approach to the insider threat. We begin by characterizing the insider and the threat posed by variously motivated insiders. Next, we characterize the asset of concern: computerized information of strategic or economic value. We discuss four general ways in which computerized information is vulnerable to adversary action by the insider: disclosure, violation of integrity, denial of service, and unauthorized use of resources. We then look at three general remedies for these vulnerabilities. The first is formality of operations, such as training, personnel screening, and configuration management. The second is the institution of automated safeguards, such as single use passwords, encryption, and biometric devices. The third is the development of automated systems that collect and analyze system and user data to look for signs of misuse.

1. Introduction

The last few years have seen increased programmatic interest in protecting computerized information from the insider: the privileged user with ready access to a computer facility. This change is evident in the DOE's call for "a shift in emphasis ... to a more balanced program that will strengthen protection against insider threats" (DOE 1992). The Office of Safeguards and Security's current effort to protect materials control and accounting information from insiders also reflects this change (Espinoza 1991, Harris 1991). The increasing emphasis on the insider is largely a natural complement to the attention already paid to the outsider, i.e., the individual who must clandestinely enter a facility, if at all. Physical security defends against the outsider with barriers such as fencing and alarm systems. Computer security parallels these efforts with defenses such as passwords, intrusion detection systems (Denning 1987), and encryption. As the outsider threat remains very real, these areas require continued vigilance and further study.

With efforts to thwart the outsider well underway it is logical to broaden our focus to include the insider threat as well. Besides the question of balance, the threat posed by the insider exceeds the outsider threat, since insiders perpetrate approximately 80% of computer misuses (Maglitta 1992). The insider's knowledge of the computing system and its defenses, combined with his[1] user privileges, makes him inherently more dangerous than all but the most skilled outsider.

*Los Alamos National Laboratory is operated by the University of California for the United States Department of Energy under contract W-7405-ENG-36. This work was performed under auspices of the United States Department of Energy.

[1]Though the majority of abusive insiders are male (at least those who have been detected), espionage, sabotage, theft, and terrorism are professions open to both sexes, and we do not wish

Protecting against insiders as well as outsiders has become increasingly important as computers have come to play a larger role in our society. We have seen escalating computing involvement in the processing of a wide range of information vital to our national security:

- **Nuclear technology** - Computers design nuclear reactors and weapons, maintain inventories of nuclear materials, and manage the safety systems at nuclear power plants.

- **Government agencies** - Computers maintain Social Security, health, welfare, and tax records, and issue checks for those agencies.

- **Military services** - Computers provide for battle management, manage inventories, maintain service records, draw up payrolls, and issue paychecks.

- **Intelligence agencies** - Computers maintain and correlate human and electronic intelligence information, and analysts use them to process that information in the resolution of problems of interest.

- **Defense contractors** - Computers develop new technology and systems and to design new products. They record corporate sales, manage inventories, maintain employee records, draw up payrolls, and issue paychecks.

- **Financial institutions** - Computers conduct essentially all financial transactions in Western nations. Computers handle credit transactions (including credit card management), bank accounts, fund movements, and investments. Computers trade securities and stocks, often performing these functions automatically.

- **Law enforcement** - Computers maintain a record of past offenders and their *modi operandi*, outstanding warrants, and crime statistics.

At the same time, we have become aware of dangers to these systems besides the traditional one; that of Communist military espionage focused on stealing or buying classified information. They include strategically or economically motivated threats by foreign entities (including the former Soviet Union), criminals, and unstable or disgruntled employees. Adversaries can compromise computing systems by corrupting data or disrupting systems rather than (or in addition to) obtaining sensitive information.

It is impossible to gauge precisely how much computer misuse exists. Few victims are willing to reveal their losses (Parker 1983; 24), and fewer still are willing to discuss vulnerabilities. We can obtain valid representative data only from the numbers of cases tried and prosecuted under computer crime laws, and these represent only a few of the actual instances. Although it appears that the number of abusive insiders is low, the potential for harm by those who do exist increases as computers process more data of various kinds. We can expect steady increases in acts of crime, espionage, vandalism, and political terrorism by computer in the years ahead.

In this paper we take an asset based approach to insider threat guidance. We begin by characterizing the insider, the threat posed by variously motivated insiders, and the asset to be protected (computerized information). We identify four general ways in which computerized information is vulnerable to adversary action by the insider: disclosure, violation of integrity, denial of service, and allowing unauthorized access. We also identify three general remedies for these vulnerabilities. The first is *formality of operations*, such as training, personnel screening, and configuration management. The second is the institution of *automated safeguards*, such as single use passwords, encryption, and biometric devices. The third is the development of *automated analysis systems* that collect and analyze data to look

to appear biased. For convenience, however, the masculine pronoun has been used throughout, save when the specific person referred to is a woman.

for signs of misuse. We conclude with specific recommendations for directions to pursue in combating the insider threat.

2. The Insider

The greatest threat to a computer system is the adversely motivated insider with the access, technical knowledge, and skill required to create or exploit a vulnerability in the system. We define the insider as an individual with authorized physical or electronic access to a computer system. The insider can use this access to engage in such activities as system management, software design and trouble-shooting, or hardware repair. Note that this definition includes individuals who are not physically at a computing facility.

A broader definition of the insider would encompass individuals who perform activities that affect the computer system hardware or software during some stage in its life cycle, but who do not currently have access to the computer. These activities typically consist of designing, testing, modifying, and documenting system hardware or software, and often occur off-site. We will use the narrower definition in hopes of presenting a more coherent and substantive approach to the topic. Still, the reader should be aware that the broader category of insiders is also a source of vulnerabilities. For example, an off-site software or hardware designer could introduce a trap door or Trojan Horse that would allow him later access to the system, or introduce a virus that damages the system at a critical moment. As we produce more of our hardware and software system components overseas, there may be greater reason for concern. Techniques for protecting against the broader insider threat therefore deserve further study.

Three insider characteristics make him especially dangerous. First, the insider has ready access to information about the computer system and its defenses. As a user or manager of the system, he naturally acquires expertise as part of his daily work. He is likely to have superior knowledge of in house hardware and software systems (he may even have designed them!), enabling him to exploit subtle system weaknesses. He can learn about the system from coworkers and manuals, resources that an outsider cannot as easily access. He can then use this information to devise more sophisticated means of subverting the system's defenses. Second, the insider, by definition, has privileged access to the computer system itself, and therefore the opportunity to make use of his knowledge. Third, if the insider is in a managerial position, he may order subordinates to engage in activities that subvert security. He may work actively to create an environment where security is not taken seriously and is not enforced. He may falsely certify the performance of security measures.

A user with generous system privileges, such as a system manager, is best positioned for exploiting a computer system. However, even the least privileged insider has an advantage over the outsider in that he does not have to break into the system. An insider's value to an outside party and his propensity to criminal activity is not necessarily commensurate with his rank or position. Support personnel such as secretaries, computer operators, and technicians, have access to computer systems and programs. They can often provide useful information and can easily damage the system. In all positions, real or perceived slights as reflected in pay or status can create disgruntlement that can inspire misuse, or can make an employee vulnerable to exploitation by an outside party.

An insider can be motivated to commit an illegal act by money, ideology, compromise, or ego (the common acronym is MICE), singly or in combination.

- **Money.** Material gain has emerged as the top motive for espionage in America, it has always been the major motivator for computer crime. The insider may seek material gain by selling information stored on a computer system. He may modify data stored on the system to enable access to some saleable product or material, or may exploit the system for direct material advantage, e.g., by issuing checks to himself.

- **Ideology.** Ideologically motivated insiders may steal information or in some manner sabotage a computer system because of sympathy for an outside entity: an ideology, individual, organization, or a country. Ideology is rarely a motive for computer espionage in the United States, but it is frequently the motivation behind terrorist acts (Carroll 1977: 16-17; Parker 1983: 125-129).

- **Compromise.** The insider may be blackmailed. A hostile entity can threaten to expose damaging secrets about the insider if he does not act for them. The compromising activity is frequently the insider's initial act of espionage or crime. Once the insider has been induced onto the 'slippery slope,' an experienced handler will make it extremely difficult for him back out.

- **Ego.** The insider may want to avenge what he sees as ill treatment by his employer or government. He may be unbalanced, or may wish to bring some excitement into his life. An insider's ego might lead him to attack a system for reasons of spite or revenge. He may want to show that he is smart enough to beat the system.

In espionage activity against the United States and Great Britain we see a substantial shift from ideology toward greed and revenge as incentives for insider abuse. Ideology inspired the Cambridge recruits in the 1930s (Boyle 1979), and the Rosenburgs in the 1950s (Pincher 1987).[2] Although there is evidence of Americans leaking classified information for ideological reasons (Richelson 1988: 240), such cases are the exception. Jonathan Jay Pollard, an analyst for the Anti-Terrorist Alert Center of the Naval Investigative Service, claimed he spied for Israel for ideological reasons. Nonetheless, the Israelis quickly put him on the payroll to guarantee his continued cooperation (Black 1991: 420-422), and he accepted large amounts of money and expensive gifts. John Walker, a Navy warrant officer and communications specialist who spied for the Soviets for at least seventeen years, was entirely economically motivated (Earley 1988: 64-66). A desire to take revenge on the CIA for having fired him motivated Edward Lee Howard (Wise 1988).

3. The Threat

The United States government has for decades viewed Communist military espionage as the primary threat to computerized information. This emphasis has focused most efforts on preventing information leakage, almost excluding consideration of other threats. Obviously a substantial adjustment in this position is in order. The threat of foreign spying, especially from the Eastern Bloc, has diminished, though not disappeared. This means that future attacks on computer systems are likely to be smaller, less organized events carried out with fewer resources. Especially when considering the insider, we must also keep in mind a host of other threats.

- The threat of non-espionage related criminal activity is substantial. This threat derives from an individual or group, acting without outside direction, bent on a course of material gain (which may have also an element of revenge).

- The threat of destructive activities by 'true believers,' though proportionately small, still merits careful attention given the potential for damage. True believers act out of a sense of dedication to a cause or ideal. They are willing to engage in criminal activities that can, in the extreme, cause great harm to others. They usually engage in destructive acts such as sabotage and bombing.

[2] Some ideology may be present in espionage cases but cases involving computers are rare. We have used the Walker computer espionage case to illustrate motivation.

- The threat deriving from the unbalanced insider is considerable. This insider acts for no particular cause, entity, or material gain. An unbalanced insider may sabotage a computer system for thrills, revenge, or for irrational reasons.

- The threat deriving from negligence is arguably the greatest threat. This threat results from carelessness or mistakes by operators, programmers, and system administrators.

The following sections describe the various threat components in more detail.

3.1 Foreign Spying

The primary threat from foreign spying during the Cold War was that of the Eastern Bloc, aimed at obtaining military and technical information for the arms' race against the West. The disintegration of the Soviet Union and the Eastern Bloc, the decline in the Soviet economy, and the subsequent reorganizations in the parts of the KGB that the remaining republics have inherited, have all greatly diminished this threat. Security experts now describe the KGB as demoralized, badly funded, and much smaller than in the recent past; in sum, as "an insignificant threat" (Vrooman 1992). There is no indication that there will be any reversal in this trend.

We contend, however, that computerized information remains vulnerable to foreign spying for several reasons. First, the threat of military espionage still exist, though considerably reduced. Countries in the former Soviet Union will still covet American military technology. There is also a history of spying by other countries such as China, Libya, Iran, and Iraq (Allen 1988; 337-345). Up-and-coming nuclear powers, such as India, Brazil, and North Korea, and would-be nuclear powers such as Iraq, have strong motivations to attempt to acquire nuclear and military technologies. Israel and other friendly countries will still see the acquisition of classified intelligence as vital to their interests.

Second, we anticipate that the increasing importance of computer-based systems in active warfare will lead to attacks aimed at corrupting or destroying those systems. We may see new threat groups such as electronic terrorists or representatives of smaller countries who decide to exploit the simpler requirements of this attack.

Third, we expect espionage for economic motives also to increase. The United States is perhaps unique in its reluctance to spy for its industries (Burke 1992). Even before the recent changes in the Eastern Bloc, current American allies (e.g., France) engaged in economic espionage. As nations measure their power increasingly in economic terms, and as the threat from a common enemy recedes, some of our current political and military allies may become more inclined to engage in this type of activity to keep their industry competitive. In addition, the new found independence of Eastern Europe also brings with it a likely increase in economic espionage from those countries. As they struggle for economic survival, "their major [espionage] priority now is targeting us for economic and technological data vital to their survival" (LANL 1991). The United States intelligence community is therefore increasing its attention to this threat (Turner 1991, Betts 1992).

A final factor to consider is the psychology of the insider. With Communism and its attendant ideological stigma effectively removed from the scene, insiders might be more apt to cooperate with foreign powers. Indeed, they might take pleasure in aiding countries formerly under Soviet rule.

3.2 Computer Criminals

Experience suggests that the white collar worker in a position of trust is the most common computer criminal (Parker 1983; 277). This type of criminal is usually intent upon self gain of some sort, usually financial. These insiders generally act independently of any criminal

organization. The crimes with the highest monetary losses are those perpetrated by high-level managers in collusion with technical employees. The following list contains a representative sample of computer crimes against the government and private industry.

- Samuel L. Morison, an analyst at the Navel Intelligence Support Center, sold classified photographs to the British publication *Jane's Defence Weekly* (Allen 1988:185-187).

- Six current and former Social Security Administration (SSA) employees sold personal data from SSA computers to private investigators (Smith 1992).

- An IRS clerk used the IRS computer to transfer unclaimed tax credits from various taxpayers to a relative's account (Carroll 1977: 23).

- The chairman of the board and other senior executives of the Equity Funding Corporation of America created bogus life insurance policies that they sold for cash to reinsuring companies. The main purpose was to raise the company's profitability and to keep its stock, of which the executives were major holders, selling at high prices. The amount defrauded was close to $200 million (Whiteside 1978: 11-18).

- Michael Hansen, a computer crime and security consultant and an expert on electronic funds transfer fraud, used the Federal Reserve wire funds transfer system to move $10.2 million to Geneva, where he bought 9,000 carats of diamonds (Parker 1983:3-9).

- A timekeeping clerk discovered that she could modify a payroll computer system to allocate herself unearned overtime. When her employers discovered this, they decided not to undertake the expense of recoding the system or performing manual checks. Instead, they gave the clerk a new job with a higher salary for promising not to tell anybody what she did and how (Parker 1983: 71-73).

We emphasize that the frequency and severity of self-motivated crimes is not likely to be affected by the unraveling of the Eastern bloc. They may even become more frequent, as disclosure (as in Morison's case) might seem less traitorous in today's less threatening international climate.

3.3 True Believers

'True believers' are different from criminals who are intent on self gain. They usually dedicate themselves to organizations that aim to change society, and their motivation is more a "passion for self renunciation" than "self advancement" (Hoffer 1951: 21). They usually act by targeting computers for sabotage and destruction. True believer organizations include terrorist groups such as the Red Brigades in Italy and the Comite Liquidant ou Detournant des Ordinateurs in France. During the Vietnam War, radical students bombed several computer centers at American universities that were engaging in DOD research (Whiteside 1978: 5-8). Similar activity may have originated with extreme environmental or anti-nuclear organizations. There have been many attacks on computer facilities in Europe by such organizations, and the authorities suspect that collusion with computer center employees is frequently a factor (Parker 1983: 125). The activities of true believers become a significant concern when one considers that they may not balk at destroying whole economies in an attempt to achieve political goals. An electronic economy such as ours is vulnerable to attacks on key computers, data communications facilities, and computerized records.

3.4 Unbalanced Individuals

Acts that are psychotic or at least irrational characterize the unbalanced individual. When one considers that most computer systems are in the hands of a very few individuals, the mental stability of employees becomes a significant concern. For example, a night shift

computer operator at the National Farmers Union Service Corporation in Denver repeatedly used his car keys to short-circuit his computer's disk drive. After at least fifty-six such shutdowns over a two-year period, during which time his employer spent $500,000 trying to find the recurring trouble, closed circuit television surveillance finally caught him. He explained that his "overpowering urge to shut down the computers" resulted from his loneliness and wish to "go home early" (Parker 1983: 53-54).

3.5 Negligence

Carelessness or mistakes made by honest and mentally sound employees can inadvertently undermine the security of a computer system and destroy or compromise computerized information. Such errors "remain ... the leading risk to computer security today" (Adam 1992). This threat can result in the disclosure of classified information, corruption of data, interruption of service, loss of programs or data, or destruction of equipment and facilities.

Negligence springs from many sources. Many system personnel are inadequately trained. New in-house software is often not adequately documented and tested. Use of such software by individuals other than the author can result in inadvertent security problems. System administrators frequently give users more privileges than they need, or even set no limiting default privilege on new accounts. System administrators usually have too many other things to do than constantly check for potential security flaws. Carelessness may result in mistakes while performing routine work. For example, a programmer may delete important data files or software, an operator may accidentally shut down a system, or users may fail to follow security procedures while handling classified media.

4. The Asset: Computerized information

Computerized information, whether strategic or economic, is the asset of concern to us. In the domain of strategic information, American assets are threefold. Many foreign countries, both friendly or antagonistic, covet information regarding *military technology*. They may choose espionage as the most cost-effective way to acquire it. Computing systems most likely to be targeted are those at research and production weapons laboratories. They contain valuable information regarding nuclear and non-nuclear materials and weapons. American *intelligence* is also of great value to other countries and is therefore likely to be targeted. Even allies such as Israel regard U.S.-gathered intelligence data as so vital to their national interest that it justifies espionage. Finally, American *military systems* for active warfare, including battle management systems and control systems for computerized weapons such as the Patriot, are vulnerable as well. Compromise of these assets could severely influence battle outcomes in a computer-assisted or managed war such as Desert Storm.

Computerized information of economic value is also vulnerable. Especially valued and therefore especially vulnerable is research on energy technologies. As with information on military technology, it is often cheaper for a foreign country to acquire the fruits of American research by espionage than to develop new products itself. A foreign country also may see spying against American corporations as vital to keeping its industry competitive. Economic espionage also could give other countries an advantage in international economic negotiations; for example, a foreign negotiator might wish to discover precisely what internal subsidies and other devices America employs. Finally, information on financial holdings and transactions can be of direct economic value to an insider.

The insider can compromise computerized information in four general ways:

- **Disclosure.** The insider can show or give information to unauthorized individuals or organizations.

- **Integrity Violation.** The insider can delete or modify data. Modified data might be completely unusable, or can be timed to self-destruct at an inopportune moment. More subtle modification can produce a chain of errors in any work based on it, and a loss of confidence in all data on a system. Violation of integrity can be an end in itself; alternatively, it can be the means by which a computer criminal pursues material gain. For example, an insider can manipulate a nuclear materials control data base so that inventories do not detect missing stock. The missing materials may then be removed and sold, with no one the wiser.

- **Denial of Service.** The insider can make information unavailable to system users. At the least, denial of service is annoying and expensive. At worst, the result can be disastrous. For example, a missile guidance system, a major financial system, or telecommunications network may fail at a strategic moment. Denial of service is easier to accomplish than stealing information because one can simply overload a system, destroy crucial data, or sabotage the system. For this reason we may see antagonists such as electronic terrorists, small countries, or independent insiders choosing this form of attack. One source estimates that 77 percent of preventable losses involve denial or interruption of essential services (Carroll 1977: 10).

- **Unauthorized Access.** The insider can allow an outsider access to the system by compromising the system's defense mechanisms or by revealing how they can be breached from the outside.

5. The Solution

In this section we describe three complementary approaches to defending against the insider threat. They emphasize preventive measures rather than reactive ones. The first is the definition and enforcement of specific formal security policies for management and for all employees. The second is the institution of automatic safeguards to better enforce these policies. The third is the automated detection of security violations and anomalous behavior through the analysis of audit data. Our goal here is to give a survey of these approaches rather than an exhaustive analysis of all possible remedies for all possible vulnerabilities.

5.1 Formality of Operations

We define *formality of operations* as a corporate culture, or way of doing business, that emphasizes safeguards and accountability. The term can perhaps best be understood in contrast to the informal culture typified by a small start-up company or academic computing facility. In such an environment system managers frequently are not concerned with security. They do not attempt to define or enforce a security policy. All users have access to all aspects of the computing process; there are no passwords or permissions. Doors and desks are unlocked. Machines are always on and ready to be used by anyone who walks in. Any user can modify any software, tinker with any hardware, or delete or transmit any data file. Vital printouts can be copied, tossed in the trash, or removed from the facility. Such an environment, while undoubtedly liberating and stimulating, is vulnerable to the antagonistic insider.

In contrast to the computing environment sketched above, an environment governed by formality of operations builds barriers at appropriate points against the would be antagonist. Management is committed to security, and requires employees to follow a set of well defined security rules. Employees are screened before hiring and at regular intervals during their employment. Physical security keeps unauthorized personnel out of sensitive areas, and protects important printed and electronic media from tampering or removal. Passwords, file permissions, and encryption provide similar security on line. Software development and maintenance is undertaken in a careful and controlled manner using established principles of software engineering and configuration control. Hardware is kept in a safe place and in

spected regularly for signs of tampering. Violations of security policy are promptly identified and penalized.

The following paragraphs discuss various aspects of formality of operations. These aspects, we believe, must be part of any security-conscious organization. The reader should recognize that most of the policies discussed below are not novel. The important issue is the development of means by which they can be more rigorously implemented and enforced.

Management. Management must develop, test, document, and fully support a detailed and explicit security policy. This policy should set forth general goals, specific procedures to be followed, a regular system of inspections, and steps to be taken when a security violation occurs. It is management's responsibility to create an environment in which employees actively support security efforts. It is also important for management to create an administrative structure in which employees report suspicious behavior to an impartial authority outside their direct line management chain. This minimizes negative repercussions in case the reported employee is in the reporter's work group or line management, or in case the reported behavior turns out to be benign. Finally, management must respond promptly and positively to reports of security short-falls and inappropriate employee behavior, rather than ignoring or, even worse, punishing whistle-blowers.

The 'black vault' at TRW, Christopher Boyce's workplace, is a paradigm of poor management practices. Boyce removed or photographed classified information from the vault and passed it to a collaborator who then sold it to the Soviets. Included in a litany of unprofessional behavior alleged by Boyce were parties that involved "drug use, drinking, and horseplay." A TRW executive denied drug use but acknowledged a "limited use of alcohol on the premises." Boyce's immediate supervisor "pasted a chimpanzee's face on his security badge and had a few laughs with his subordinates when he had no trouble getting in and out of the ... special project building" (Allen 1988: 325-6).

Training. Employees must learn the elements of good security and the specifics of their facility's security policy. Such training will reduce, though not eliminate, employee mistakes that expose the computing system to abuse. While it may seem impractical to teach all users about even the fundamentals of computer security, the time spent on such an endeavor will not compare with the time wasted tracking down mistakes that occur repeatedly, or the loss that can occur with a major security breach. Training is particularly useful in stamping out behaviors that are both simple and dangerous, such as writing down passwords, leaving a logged-on terminal unattended, or 'sneaker-netting' a diskette (i.e., walking it) between machines rather than following formal file transfer procedures. Each employee must fully understand his responsibilities, both in performing specific security tasks (e.g., daily safe sign-outs), and in being alert to, and reporting, suspicious behavior by other employees. They also must be trained to recognize suspicious overtures from outsiders bent on recruitment.

Proper training might have helped stop U.S. Navy radioman Jerry Whitworth, who passed cryptologic materials to John Walker for sale to the Soviets. Whitworth spied for money and spent it conspicuously. His yearly salary was $23,000, but in a two-year period he spent $130,000. During one ten-day leave he spent $17,000. He gave large parties at expensive hotels, had $500 box seats at the opera, and lived in an expensive condominium. He rented a chauffeured Rolls Royce frequently, and even had it meet his ship when he returned from sea duty (Allen 1988: 98-101). Whitworth's fellow workers were suspicious of his affluence, which was inconsistent with his rank and salary, but did not raise the issue with his superiors. Proper training would have made it more likely, though not have guaranteed, that some fellow worker would have reported Whitworth's behavior.

Screening. All employees should be carefully screened before hiring, and after hiring at regular intervals. Pre-hiring screening can include tests for substance abuse and checking of resumes for inflated or incorrect claims. Post-hiring rescreenings can include tests for substance abuse and a search for evidence of suspicious levels of affluence. Screening and re-

screening also can include polygraphs. While a polygraph test should not be considered self-sufficient evidence, it may alert security personnel to a problem that can be verified by other means. In addition, the knowledge that polygraph tests are administered may itself serve as a deterrent.

Effective screening could have prevented many known insider security disasters. Pollard's résumé inflated his work experience and education, and he showed signs of suspicious levels of affluence when he began spying (Allen 1988: 283, 287-289). Walker's only background check was in 1965, years before he started work as a spy (Early 1988: 51). Christopher Boyce got his job at TRW thanks to the 'old-boy network' connection between his father, a former FBI agent, and another former FBI agent who managed security at TRW. Background investigators contacted and interviewed only friends of Boyce's parents, not Boyce's own circle of friends, who Boyce himself described as "...disillusioned longhairs, counter-culture falconers, druggie surfers, wounded paranoid vets, pot-smoking, anti-establishment types, bearded malcontents generally, many of who were in trouble" (Allen 1988: 324-325).

Physical security. Fences, locked doors, and access control devices (e.g., badge or palm readers) can limit the insider to those areas to which he must have access. Keys and off-hour access to the facility should be limited to those who require it. Safes and desks should be locked, logged-on terminals should not be left unattended, and passwords should not be entered when another person is watching. Two-man access rules can provide extra protection for critical areas or materials.

Proper attention to physical security could have detected the activities of Christopher Boyce and Ruby Schuler. Boyce removed CIA keylists to the KW-7 satellite network from sealed plastic envelopes, photographed them, then resealed the envelopes with an iron or a carelessly applied touch of glue. Security officers never detected the tampering (Allen 1988: 326). Schuler was an executive secretary to the president of Systems Control Inc., a small defense contractor to the U. S. Army. She used her knowledge of the combination to the president's safe to remove and copy secret documents about American missile defenses. In the president's absence she would occasionally even request, then copy, specific additional documents from the ballistic missile center in Huntsville. Schuler also used her secret clearance to escort uncleared collaborators into her supposedly secure office to collect documents (Allen 1988: 143-145).

On-line security. Just as physical security restricts site access, so on-line security restricts access to networks, individual machines, and individual files or directories. Passwords and other means of authentication restrict access to everything from entire networks to individual machines. The insider threat requires an even finer level of protection. File directory and even individual file protection that restricts access to a small set of users can protect data and software from unauthorized modification, deletion, or disclosure. Encryption can provide an additional level of security. If an insider does manage to access and copy an encrypted file, he can make no use of it unless he also possesses the cryptographic key.

Better on-line security could have prevented (or helped prevent) Jonathan Pollard from stealing intelligence information. Pollard had top secret security clearance and access to Sensitive Compartmentalized Information (SCI) about sophisticated technical systems of intelligence gathering on a 'need to know' basis. It was understood that those with SCI access codes would not look at information that was unrelated to their duties (Black 1991: 117). Because need-to-know adherence was left up to the individual employee, Pollard could browse, i.e., wander almost at will through files that he had no legitimate business to see. In keeping with security theory he was compartmentalized; in practice he had access to virtually whatever he said he needed (Allen 1988: 282-5).

Software integrity. Vital software must be protected from insiders who develop, maintain, and use it. Errors, temporary fixes, weak logic mechanisms, and deliberate trap doors, Trojan Horses, and viruses make a system vulnerable to compromise. Besides protecting

key software with the on-line security measures mentioned above, formal configuration control procedures can be used to ensure software integrity during the entire life span of a code. These include documentation and review of new software, testing, user training, and periodic validation of correct functioning.

Many problems could have been avoided with the implementation of software integrity measures. In one case, "several automotive engineers in Detroit discovered a trap door in a commercial time-sharing service in Florida that allowed them to search for privileged passwords on a trial-and-error basis." After discovering the password of the time-sharing company's president, they used it "to obtain copies of trade-secret computer programs that they proceeded to use free of charge" (Parker 1983: 83).

Hardware security and integrity. To prevent a hands-on attack on the system, key hardware can be kept in an area with restricted access. Badge readers can limit access while providing a record of access. Regular and random inventories and inspections can be used to verify that machines have not been tampered with.

Enforcement. A final key aspect of formality of operations is the enforcement of security policy. In the long term, the easiest means of enforcing security procedures is by automating them, as discussed below. Until such safeguards are in place, line management and security personnel must monitor employee behavior to verify that security policy is followed. This involves general alertness to inappropriate behavior and periodic, random inspections. Once identified, violations must be penalized, with penalties ranging from censure and retraining to firing or criminal prosecution. Publicizing violations and their punishment may make for bad publicity, but can deter other insiders from taking similar actions in the future.

Pollard's case well illustrates the danger of lackadaisical enforcement. Soon after Pollard began work for the Navy's Field Operational Intelligence Office, he contacted a military attaché at the South African embassy. When U.S. officials learned of this contact, Pollard's top-secret and special clearances were withdrawn. Pollard appealed, and the clearances were eventually restored over the Director of Naval Intelligence's objections (Allen 1988: 283-284). A short time later Pollard began spying for Israel.

5.2 Automatic Safeguards

The Achilles heel of formality of operations is human nature. Security measures are frequently unwelcome diversions from the main stream of users' work. As a result, users often neglect to apply even the most rudimentary security procedures. They often fail to change vendor supplied default system passwords, and pick easy-to-guess passwords for their accounts. They leave key on line files unprotected, with open read and write permissions. They ignore 'mandatory' training sessions, failing to keep up to date with system developments. If such errors of omission could be eliminated, much of the danger posed by the insider would be eliminated as well.

The next generation of computer security will address this problem by taking formality of operations one step further, enforcing it just as automatic seatbelts enforce the often ignored seatbelt laws. They will do this by providing *automatic safeguards*: mechanisms that make deliberate violations of security policy more difficult, while protecting the system from accidental violations by users. Automatic safeguards are particularly important in software usage, chiefly because all insiders have access to software (as opposed to access to the computing site and hardware). Moreover, the bulk of work done on the computer, whether remote or on site, concerns developing and using software. Finally, because many users believe that formality of operations makes this work more difficult, it often takes a lower priority to getting the job done quickly. For example, it is easier to give another user access to all one's files than to evaluate and grant permission for each file individually. It is easier for code developers to work independently than to work as a group, checking each others' code.

Sneaker net is faster than controlled file transfer. Users often focus on these short-term gains rather than long-term productivity and security.

Below we provide several examples of automatic safeguards. Many of these capabilities are already available, while others are under development.

- Prompting a system manager to replace vendor-provided default system passwords.
- Encrypting all files above a certain security level.
- Requiring two-person rules for access to key software, whether stored in physical media (e.g., tapes in safes) or on-line.
- Requiring users to use random, computer-generated passwords, or passwords with a life span as short as a single logon.
- Verifying software integrity to ensure against illegal modifications. Some encryption algorithms can be used for this purpose (Russell 1991:171).
- 'Policing' machines on a network at regular intervals to check for security vulnerabilities, such as crackable passwords or key files unprotected by compartmentalization and passwords (Farmer 1990, LLNL 1989).
- Keeping widely used software in a central, read-only library from which users check it out as needed, with copies timed to self-destruct after a certain interval.
- Terminating system privileges if a user fails to keep up with training requirements.

5.3 Automated Data Collection and Analysis

Automated monitoring of system and user behavior, coupled with computerized analysis of the resulting data, can help protect computer systems from the insider. Data collection and analysis require installation of appropriate hardware or software to audit relevant behavior, and of software to analyze the resulting information. Two analytic methodologies dominate the arena of audit record analysis: *expert systems* and *anomaly detection* (Lunt 1988, Vaccaro 1989, Winkler 1990). Because each approach has its advantages, an ideal system should combine both.

Expert systems are based on expert rules that encode security policies and suspicious user behaviors. They are appropriate for types of invalid behavior that are well understood and have observable and quantifiable signs. For example, attempts to browse through files outside one's need to know are evidenced by an unusual number of file accesses and file access errors, both of which can be observed from file system audit logs. An expert system would therefore watch for file accesses or file access errors that exceed a threshold determined through interviews with security personnel or data analysis. Los Alamos's production system, the Network Anomaly Detection and Intrusion Reporter (NADIR) exemplifies this approach (Jackson 1991, Hochberg 1993).

Anomaly detection identifies user behavior that falls into categories not yet proscribed by formality of operations. This approach uses statistical techniques to 'learn' patterns of normal behavior; deviations from the norm are then reported as suspicious. For example, if John Doe's behavior one day is markedly different from his normal behavior, this may suggest that another user is masquerading as John Doe. In another example, if the number of files deleted per minute on a given system suddenly spikes upward, this may suggest that a destructive virus has been turned loose on the system.

A key issue to be resolved is how a monitoring system should (or can) respond to suspicious behavior. Most current systems produce reports periodically or on demand. Ideally, such reports display (in graphs and numbers) the patterns of system usage during a specified interval. They also should provide listings of suspicious users, specific rules violated, and anomalies detected. The next generation of monitoring systems will include near real-time notification of serious violations or anomalies so that perpetrators can be caught in the act. In addition, these future systems may trigger real-time countermeasures. Such responses could be punitive, such as tracking down and disabling or removing the perpetrator's computer account.[3] Another possibility is the addition of a 'tracer' to files that could be used to track down a perpetrator. Countermeasures also could be defensive. Lawrence Berkeley Laboratory's Clifford Stoll stopped an intruder from removing data files by shorting a line connection with his key chain, thus inducing intermittent electronic interference (Stoll 1989: 154, 225). This discouraged the intruder without alerting him to the fact he had been detected. Similarly, some kind of interference could be used to frustrate an offsite, or slow down an onsite insider. This would give security personnel time to respond. More drastically, the monitoring system could shut down a computer entirely or deny access through a particular port. Developing such responses is a key area for future research.

The general formality of operations issue of software integrity is especially important for software used for automatic data collection and analysis. If the designer or maintainer of such software 'turns' against a facility, he is in a remarkable position of power to cover up any adversarial actions that he takes. He may delete data that reveal his actions, or block reporting of any suspicious activity for himself. To protect against such actions, security software should be kept under rigorous configuration control so that it cannot be clandestinely altered. Whenever possible, data and results from different levels of the analysis should be compared to make sure that nothing has been tampered with. For example, on our NADIR system, which combines data from several service nodes on our network, we could check that users with heavy file system activity also show commensurate logon activity. Such comparisons would force a would-be antagonist to alter two sources of data rather than one.

Systems such as NADIR assist and complement formality of operations. Together they provide defense in depth, through multiple levels of protection. A good illustration of this principle concerns the security policy that requires each user to have a valid computer account, and to use only that account. Formality of operations enhances this security policy with training, while automatic safeguards enforce the use of computer-generated, limited term random passwords. Expert systems can terminate all user privilege after several incorrect passwords have been entered, thus halting an insider's efforts to guess his way into another user's account. Anomaly detection can detect an insider who has managed to enter another user's account, by observing deviations from the other user's normal behavior. If any one of these safeguards fails, the others still have a chance of preventing misuse from occurring.

5.4 Broader Considerations

While protecting computerized information is a key consideration for all organizations that rely on such information, it is not their only goal. Restricting cost is necessary for all organizations. Closely connected to cost is efficiency. Security measures must not become so burdensome that personnel can no longer be productive. Finally, employees' privacy must be respected, for ethical, practical, and legal reasons. We will discuss these three considerations in turn.

Cost. Achieving security is an expensive undertaking. Personnel must be hired or assigned to develop a security policy, screen and train employees, and perform inspections. Physical

[3] If access control is seen as building a wall around sensitive systems or files, these aggressive countermeasures can be compared to pouring hot oil on an attacker.

and hardware security involve costs in materials (e.g., safes and access control devices) and in personnel to maintain the systems, once installed. On-line security and software integrity measures, automatic safeguards, and systems for automatic data collection and analysis, all require a substantial initial investment in design and testing. They also require a commitment of personnel for maintaining the systems, once installed.

However, security failures can be vastly more expensive. The cost of repairing a damaged financial or telecommunications network, rebuilding months of work on system software, or having one's military equipment fail in battle, dramatically outweigh the cost of good security. In addition, a very strong argument can be made that long term, formality of operations instituted for security reasons saves money in other ways. For example, the failure to follow formal software engineering procedures can lead to costly projects' being abandoned, or revised at great expense. This is evidenced in a General Accounting Office survey of nine federal software projects (costing a total of $6.8 million), which found that only two percent of the software contracted for was usable as delivered. Of the remaining software, most were not delivered (47%), and a full 19% were abandoned or reworked (ACM 1985).

Efficiency is cost in terms of productivity. As with cost, security demands a high price but more than returns the investment. Training, rescreening, and cooperating with security inspectors subtracts hours from employees' workdays. Procedures designed to limit access to vulnerable areas and files make it harder for legitimate employees to use those areas and files. On-line systems that enforce access control, test for software and data integrity, and analyze user behavior may slow down machine and human efficiency.

This downside can be minimized, however, if efficiency is kept in mind while designing and implementing security procedures. Moreover, the same considerations that argue for an overall savings in cost can be applied to productivity. Security failures lead to a large expense in man-hours and dollars. Formality of operations can lead to better efficiency, such as when programmers do not have to trouble-shoot and repair informally developed software.

Privacy is an issue still poorly resolved in computer security, especially the automatic auditing of user activity. While many organizations take the position that they have the right to police all activity on their systems, counter arguments to this position can be made. From a legal perspective, federal wiretap statutes have already been applied to at least some auditing systems, typically those that monitor user activities at the keystroke level. However, it appears that even such detailed monitoring is legal if users are warned (e.g., by a banner displayed on the screen upon logon) that it is being done. From an ethical perspective, one can argue that auditing user activity is intrusive and dehumanizing. From a pragmatic perspective, one can argue that it will lead to employee hostility and decreased loyalty, thus possibly increasing the odds of insider attacks. These issues are currently being actively debated in the computer security community (Leighninger 1990, Schaefer 1991). For three years they have been the topic of a well attended annual conference on Computers, Freedom, and Privacy.

6. Conclusions and Recommendations

We conclude that the protection of computing systems from attacks by insiders will depend more on the intelligent application and enhancement of existing capabilities than on technological breakthroughs. This conclusion leads to the following recommendations:

1. It is essential that we protect sensitive computing systems by *formality of operations*. Systems can be designed that assist in this endeavor by providing *automatic safeguards*. The primary challenges are to impose formal operations so that they do not appear to be more bureaucratic than beneficial. We must avoid making them so complex that they guarantee non compliance, and must ensure that they do not attempt to deny necessary functions. How to design such a system is a question that needs to be studied.

2. We should support formality of operations with an automated, continuous security testing program. This program should test each component of a computing network. It would help to ensure that proper system management practices are in place. In addition, it would detect known vulnerabilities and prevent their inadvertent reintroduction.

3. We should support formality of operations with extensive *automatic data collection and analysis* of audit log information. Systems to analyze the information should use both *expert rules* (to detect explicit attempts to violate security rules and practices) and *anomaly detection* techniques (to detect unusual behavior of a system or users of a system). A prime need here is the development of methods for systematic testing of these systems using data from known misuse attempts.

4. To protect against an attack by surreptitious code imbedded in an otherwise legitimate code, more work must be done on developing effective software integrity techniques. For simple codes and data files, software integrity can be verified by comparing current versions of source code and data files with secure and trusted versions. For more complex codes, we suggest identifying violations of software integrity by watching for deviations from the code's normal pattern of execution behavior. This technique also may allow computer virus detection without knowing specific charact strings or code contained by the virus.

5. We can greatly enhance protection against insider attacks by storing and transmitting information in encrypted form. Computing systems should provide the necessary encryption tools for users to do this in a simple non-intrusive way. We therefore recommend that effort be devoted to developing efficient, easily used key management and encryption tools.

In closing, we note that these recommended measures will benefit computer security beyond the scope of our limited insider problem. The threat deriving from the broader category of insiders (encompassing individuals who work on hardware or software at some limited stage in their life cycles) is a serious one. Software integrity measures will help guard against much of this danger. Other security measures aimed at insiders, such as automatic analysis systems, add protection against outsiders.

Acknowledgments

We thank Alex Marusak of the Computing and Communications Division, and Jo Ann Howell, William Hunteman, and Richard Strittmatter of the Nuclear Technology and Engineering Division, for their expertise and contributions.

References

ACM 1985 — *ACM Sigsoft Software Engineering Notes*, (Volume 10, Number 5, October 1985).

Adam 1992 — Adam, J. A. *Data Security* (IEEE Spectrum, Volume 29, p. 19)

Allen 1988 — Allen, T. B. & Polmar, N. *Merchants of Treason* (New York, Delacorte Press, 1988)

Betts 1992 — Betts, M. *CIA Steps up Foreign Technology Watch* (Computerworld, April 20, 1992)

Burke 1992 — Burke, G. P. *Espionage and More Benign Forms of Economic Intelligence: A Tour d' Horizon* (International Security Forum, Spring 1992)

Black 1991 — Black, I. & Morris, B. *Israel's Secret Wars* (New York, Grove Weidenfeld, 1991).

Boyle 1979 — Boyle, A. *The Fourth Man* (New York, Dial Press, 1979)

Carroll 1977 — Carroll, J. M. *Computer Security* (Los Angles, Security World Publishing, 1977)

Denning 1987 — Denning. D. *An Intrusion Detection Model* (IEEE Transactions on Software Engineering, Vol. 13, No. 2, February 1987).

DOE 1992 — The Department of Energy's (DOE) fiscal year 1993 Budget Overview.

Earley 1988 — Earley, P. *A Family of Spies* (New York, Bantam Books, 198?)

Espinoza 1991 — Espinoza, J. & R. Rivas. *Alarm Communications and the Insider Threat.* (Sandia National Laboratories, SAND91-0941).

Farmer 1990 — Farmer, D. & Spafford, E. *The COPS Security Checker System* (Proceedings of the Summer Usenix Conference, June 1990).

Harris 1991 — Harris, L., Ballman, J., Howell, J., Prommel, J., Vaccaro, H., and Whiteson, R., *Report on Design and Testing of Computer Security Technologies Integrated into a Generic MC&A System* (Los Alamos National Laboratory, 1991).

Hochberg 1993 — Hochberg, J. G., Jackson, K. A., Stallings, C. A., McClary, J. F., DuBois, D. H., & Ford J. R. *NADIR: An Automated System for Detecting Network Intrusion and Misuse* (Los Alamos Technical Report, LA-UR 93-137).

Hoffer 1951 — Hoffer, E. *The True Believer* (New York, Harper and Row, 1951)

Jackson 1991 — Jackson, K. A., DuBois, D. H., Stallings C. A. *An Expert System Application for Network Intrusion Detection* (Proceedings of the 14th National Computer Security Conference, October 1991).

LANL 1991 — *European Political Changes, The Same Threat - Different Targets,* (Security System Bulletin, 4th Quarter 1991, Los Alamos National Laboratory Extracted from the Office of Counterintelligence Quarterly Newsletter, Vol. 1, No. 4, September 1991).

Leighninger 1990 — Leighninger E. V. *Discerning an Ethos for the Infosec Community: What Ought We Do?* (Proceedings of the 13th National Computer Security Conference, October 1990).

LLNL 1989 — *SPI - Security Profile Inspector, Installation and User's Manual* (Lawrence Livermore National Laboratory, 1989)

Lunt 1988 — Lunt, T. F. *Automated Audit Trail Analysis and Intrusion Detection: A Survey* (Proceedings of the 11th National Computer Security Conference, October 1988)

Maglitta 1992 — Maglitta, J. & Mello, J. P. *The Enemy Within* (Computerworld, December 7, 1992)

Parker 1983 — Parker, D. B. *Fighting Computer Crime* (New York, Charles Scribner's Sons, 1983)

Pincher 1987 — Pincher, C. *Traitors* (Harmondsworth, U. K., Penguin Books, 1987)

Richelson 1988 — Richelson, J. T. *Foreign Intelligence Organizations* (Cambridge, Mass., Ballinger Publishing Company, 1988)

Russell 1991 — Russell, D. & Gangemi, G. *Computer Security Basics* (Sebastopol, CA, O'Reilly & Associates, Inc., 1991)

Schnefer 1991 — Schnefer, L. J. *Employee Privacy and Intrusion Detection Systems: Monitoring on the Job* (Proceedings of the 14th National Computer Security Conference, October 1991).

Smith 1992 — Smith, J. M. *SSA Employees Accused of Selling Personal Data* (Government Computer News, Jan. 6, 1992, p. 58).

Spafford 1991 — Spafford, E. H. *Preventing Weak Password Choices* (proceedings of the 14th National Computer Security Conference, October 1991).

Spafford 1992 — Spafford, E. H. *Common System Vulnerabilities* (Software Engineering Research Center, Department of Computer Sciences, Purdue University, March 1992).

Stoll 1989 — Stoll, C. *The Cuckoo's Egg*, (New York, Doubleday, 1989)

Turner 1991 — Turner, S. *Intelligence for a New World Order* (Foreign Affairs, Fall 1991, pp. 150-166)

Vaccaro 1989 — Vaccaro, H. S. *Detection of Anomalous Computer Session Activity*. (Proceedings of the 1989 Symposium in Security and Privacy, May 1989).

Vrooman 1992 — Robert S. Vrooman, Internal Security Officer, Los Alamos National Laboratory, March 1992. Personal communication with the authors.

Winkler 1990 — Winkler, J. R. *A UNIX Prototype for Intrusion and Anomaly Detection in Secure Networks* (proceedings of the 13th National Computer Security Conference, October 1990)

Whiteside 1978 — Whiteside, T. *Computer Capers* (New York, Thomas Y. Crowell Company, 1978)

Wise 1988 — Wise, D. *The Spy Who Got Away* (New York, Random House, 1988)

DISCLAIMER