Theft While Traveling

Your information and valuables are far more vulnerable to theft while traveling abroad than in the United States. Principal targets for theft include:

- Government and business documents of interest to the local intelligence service.
- Personal documents (passport and other ID and travel documents) of interest to criminal organizations, including those that arrange illegal immigration to the U.S.
- Laptop computers are of interest to everyone -- for the information on them, for resale, or for personal use. See Security of Laptops.
- Expensive jewelry, cameras, and any other items that are easy to sell.

You have special vulnerabilities in your hotel room, elsewhere in your hotel, while in the airport or on the train, with sensitive equipment in transit, and in any office to which local foreign nationals have unrestricted access.

Hotel Rooms and Vaults

"Bag operations" is the term commonly used to describe surreptitious entry into hotel rooms to steal, photograph, or photocopy documents; steal or copy magnetic media; or download from laptop computers. Bag operations are common. In fact, they are routine procedure in quite a few countries.

Bag operations are typically conducted by the host government's security or intelligence service, frequently with cooperation of the hotel staff. Hotel security staffs commonly maintain close contact with the local police and government security service. It is common for retired government security and intelligence officers to obtain employment in the security offices of major hotels and corporations. Bag operations may also be conducted by the corporation you are dealing with or by a competitor company. They may be done during the day while you are out of the room or at night while you are asleep. Yes, they do take the risk of coming into your room while you are sleeping!

Government and business travelers often report that their belongings have been searched while they were absent from their hotel room. In some cases, they have returned to their room soon after departing, to retrieve a forgotten item, and find persons in their room claiming they are there to repair a broken TV, etc. Seldom is anything missing; the purpose is only to copy documents or download information from a traveler's laptop computer. Sometimes there is little effort to conceal the search. Other times it is more subtle. If done correctly, the traveler will not be aware of the search.

Leaving sensitive government or company information in your hotel room, even in a locked briefcase or the safe provided in your room, is an invitation for material to be copied or photographed while you are out. Hotel vaults are not much better. In most cases, foreign intelligence officers can gain access to hotel lockboxes or vaults without you becoming aware of the compromise.

Never leave a laptop computer with sensitive information on it in the room unattended. Keep it in your personal possession at all times or don't take it on the trip. If you must take a laptop, use encryption to protect sensitive files and perform regular backups to ensure no loss of vital information in case of theft.

Suitcase and attaché case locks may delay the trained professional for a few minutes but will not protect your sensitive information. Nevertheless, it is wise to keep your luggage locked whenever you are out of the room. Although locks will not inhibit the professional thief or intelligence agent, they will keep the curious maid honest. Curious hotel employees are even more likely to remain honest if combination locks are set so that the combination for each piece of luggage is different. For attaché cases with two combination locks, use different combinations for each lock.

The only solution to the security problem is to take as little sensitive information as possible when traveling overseas, and to carry what you must take on your person, possibly on computer media. Computer diskettes and CD-ROMs must also be carried with you at all times.

If you must carry sensitive information, the following suggestions may be helpful.

- While asleep or in the shower, engage both the dead bolt and the privacy latch or chain on the hotel room door. A hotel's emergency keys can override the dead bolt locks, so the latch or chain is your principal source of security. (Note: Many hotel rooms have a door to a connecting room. This is a potential vulnerability, as these doors do not normally have a privacy latch or chain.)

- Utilize a portable or improvised burglar alarm while asleep. Two ash trays and a water glass are quite effective as an alarm when placed on the floor in front of the door into your room. Place a water glass in one ashtray and balance the second ashtray on top of the glass. If a straight chair is available, place it next to the door and put the ash tray/water glass alarm on the edge of the chair where it will fall with enough racket to wake you.

- When leaving the room, make a mental or written note of how your suitcase or other personal property that would not normally be touched by the cleaning personnel was left. Any movement might suggest that others were in the room to examine your belongings. The same procedure is even more effective to check for surreptitious entry while you were asleep.

- Jewelry or other valuables should normally be left at home, but you may need to protect a substantial amount of money. Guidelines for protecting money from thieves are different from those for protecting sensitive information from the local intelligence or security service. Money should not be kept on your person. It should be kept in a safe in a local office or in the hotel’s safe deposit box or safe. This is safer than a room safe and may also make the hotel liable for any loss. Liability laws in many countries provide that the hotel is not liable for the loss of

guest property unless it is in the "care, custody and control of the hotel." Additional protection may be gained by double enveloping all valuables, initialing across the seams, and then taping all edges and seams (over the initials).

- If you determine that an item is missing, conduct a thorough search prior to reporting the incident to hotel security. Do not expect to receive a copy of the security report, as it is an internal document. The incident should be reported to the local police, the security officer at the nearest U.S. Embassy or Consulate, and your insurance carrier. Hotel security can provide a letter verifying that you reported property missing.

Elsewhere in the Hotel

There are a number of areas of your hotel where you are particularly vulnerable to theft.

- Rest Rooms: Female travelers should be careful about placing purses on hangers on the inside of the lavatory doors or on the floor in stalls -- two frequent locations for grab and run thefts. On occasion, unauthorized persons use rest rooms for other types of theft or to deal drugs or engage in prostitution.

- Public Telephones: Areas around public telephones are often used by criminals to stage pickpocket activity or theft. Keep briefcases and purses in view or "in touch" while using phones. Safeguard your telephone credit card numbers. Criminals sometimes hang around public telephones to gather credit card numbers and then sell the numbers for unauthorized use.

- Hotel Bars and Restaurants: Purse snatchers and briefcase thieves are known to work hotel bars and restaurants waiting for unknowing guests to drape these items on chairs or under tables, only to discover them missing as they are departing. Keep items in view or "in touch". Be alert to scams involving an unknown person spilling a drink or food on your clothing. An accomplice may be preparing to steal your wallet, briefcase or purse.

- Pool or Beach Areas: These are fertile areas for thieves to take advantage of guests enjoying recreation. Leave valuables in the hotel. Safeguard your room key and camera. Sign for food and beverages on your room bill rather than carry cash.

- Prostitutes take advantage of travelers around the world through various ploys, including use of "knock out" drugs and theft from the victim's room. Avoid engaging persons you do not know and refrain from inviting them to your guest room.

Airports and Trains

Airports, railroad terminals and trains are easy targets for pickpockets, thieves, and terrorist bombers. Unattended baggage is an obvious risk. Checked baggage is also at risk and should never contain valuables such as a camera or sensitive papers. It is not unusual for government and business travelers to report broken suitcase locks and rearranged contents.

Theft from sleeping compartments on trains is surprisingly common. Train thieves spray chemicals inside sleeping compartments to render the occupant(s) unconscious in order to enter and steal valuables. Using this technique, valuables can be stolen from under a sleeping person's pillow. A locked door may be helpful but is no guarantee.

Laptop computers are a prime target for theft everywhere, but they are especially vulnerable in airports. They are stolen for the value of the information on them as well as for the value of the computer.

According to Safeware, an insurer of personal computers, 10% of all laptop thefts occur in airports. Airports offer an inviting atmosphere for thieves due to large crowds, hectic schedules, and weary travelers. Laptop thefts commonly occur in places where people set them down -- at security checkpoints, pay phones, lounges and restaurants, check-in lines, and restrooms. Two incidents at separate European airports demonstrate the modus operandi of thieves operating in pairs to target laptop computers:

- Airport security at Brussels International Airport reported that two thieves exploited a contrived delay around the security X-ray machines. The first thief preceded the traveler through the security checkpoint and then loitered around the area where security examines carry-on luggage. When the traveler placed his laptop computer onto the conveyer belt of the X-ray machine, the second thief stepped in front of the traveler and set off the metal detector. With the traveler now delayed, the first thief removed the traveler's laptop from the conveyer belt just after it passed through the X-ray machine and quickly disappeared.

- While walking around the Frankfurt International Airport in Germany, a traveler carrying a laptop computer in his roll bag did not notice a thief position himself to walk in front of him. The thief stopped abruptly as the traveler bypassed a crowd of people, causing the traveler also to stop. A second thief, who was following close behind, quickly removed the traveler's laptop computer from his roll bag and disappeared into the crowd.

All travelers, both domestic and international, should be alert to any sudden diversions when traveling, especially when transiting transportation terminals. If victimized, travelers should report the thefts immediately to the authorities and be able to provide the makes, model information, and serial numbers of their laptop computers, or any other items of value.

Sensitive Equipment in Transit

Sensitive equipment may be stolen so that it can be copied through reverse engineering. For some purposes, it may be sufficient to only gain access to the equipment for a brief period.

For example, a cleared company participated in an air show that took place overseas. The company shipped over an operational $250,000 multi-mode radar system that can be used on fighter aircraft. At the conclusion of the air show, the radar system was packaged for return shipping by company personnel, and the radar assembly was actually bolted to the shipping container. The shipping container was routed through a third country with the customs seals intact.

Upon being opened by company personnel, it was discovered that the radar was no longer bolted to the shipping container. As a result, the radar system was damaged beyond repair. It was determined that the radar was properly bolted down at the time it was prepared for shipment. It also was determined that the country that sponsored the air show was keenly interested in the radar's technology. It is not known whether the intruder's failure to re-bolt the radar was an oversight or was done deliberately to destroy evidence of whatever was done to examine the radar.

Lesson learned: The company did not really need to take the entire radar assembly to the air show. A mock-up without the internal mechanisms could have been set up along with photographs of the internal components.

Overseas Offices

Offices of U.S. Government agencies and U.S. businesses in foreign countries are vulnerable both to burglary and to theft of information by local national employees.

> For example, the Western European office of a large American corporation was burglarized in an obvious case of industrial espionage. Located on the sixth floor of a 12-story office building, it was entered from the outside window ledge by breaking the window. The thieves ignored the company's expensive computers and other valuable items and went directly to their target -- the company's marketing and business data, client and business contact lists, and banking information.

Foreign offices of U.S. Government and business organizations are staffed, in part, by local citizens. In many countries, some of these employees cooperate voluntarily with the local security or intelligence service or are pressured or coerced into doing so.

In one allied Western European country, collecting proprietary information from the offices of American and other foreign corporations with offices in that country is known as "economic patriotism." Collected information is provided routinely to local competitors

of the U.S. companies. In many countries, local national employees are also debriefed for assessment data about the American personnel.

Foreign intelligence interest is not necessarily determined by an employee's rank in the company. Researchers, key business managers, and corporate executives can all be targets, but so can support employees such as secretaries, computer operators, technicians, and maintenance people. The latter frequently have good, if not the best, access to competitive information. Additionally, their lower pay and rank may provide fertile ground for manipulation by an intelligence agency.

Protection of sensitive information is very difficult under these circumstances. Discussion of all the physical and technical security requirements for protection of proprietary technologies and sensitive commercial information is beyond the scope of this security guide.