



Guidelines for Protecting U.S. Business Information Overseas

Other

Western Hemisphere; East Asia & Pacific; Europe; Near East; South Central Asia; Africa

6/1/2005

Chapter I.
Introduction 1

Chapter II.
Guidelines 3
What Information Should We Protect 3
The Information Audit 3
Levels of Information Protection 3
General 3
Heightened Awareness 4

Chapter III.
American Attitudes 5
Exploitation of Our Traits 5
Sociability 5
Status 5
Ambition 5
Ethnic Feelings 6

Chapter IV.
Office 7
Need for Awareness Program 7
Ideal General Security Level 7
Relocation 7
High Security Areas 7
General Office 8

Chapter V.
Home 11



Chapter VI.
Personnel 13

Chapter VII.
Communications 15
Introduction 15
Electronic Transmissions Routine Procedure 16
Electronic Media Path 16
Electronic Transmission Threats and Vulnerabilities 16
Threats 17
Vulnerabilities 17
Suggested Counter-Measures 18
Effects of Telecommunications on Computer Security 19
Video Conferencing 20
Courier 20

Chapter VIII.
Computers 21
Computer Technology 21
The International Business Traveler 21
Computer Theft 21
Unauthorized Access 22
Foreign Customs 22
Working From Hotels 23
Special Risks When Using Cellular PCs 23
Virus Contamination and Detection 23
The Office Manager Stationed Overseas 24
Physical Access to Computing Facility 24
Telecommunications Lines 24
Magnetic Media Control 25
Use of Encryption 25
Distributed Printer Control 25
Cross Border Flow of Information 25
Computer Security Guidance 26

Chapter IX.
Travelers 27
Increased Risk 27



Our Vulnerability 27
Scientific Conferences 27
Eavesdropping 27
Hotel Rooms and Vaults 28
Destruction of Information Waste 28
Communications 28
Be Alert 28

Annex I.
Home Security Checklist

Annex II.
Office Security

Annex III.
Computer Security Checklist

Overseas Security Advisory Council
U.S. Department of State

FOREWORD

Read through this booklet with the objective of learning specific ways to protect your business information, and most important, to raise the level of awareness of yourself and co-workers to the threat.

The guidelines which follow are suggested to assist American organizations and their personnel abroad in planning to meet their individual needs and circumstances.

Individuals should ensure, however, that any approach chosen is best suited to their corporate and individual situation.

Chapter I. Introduction

Each day America becomes driven more and more by information. Proprietary information is our chief competitive asset, vital to both our industry and our society. Our livelihood and, indeed, our national strength depend on our ability to protect industrial and economic data.



The struggle between capitalism and communism was decided essentially over two issues - the desire of humanity for freedom and the relative effectiveness of each system's economic competitiveness. While of utmost importance during the period of the Cold War, the need to protect economic information looms even larger in the coming years.

Recent revelations in the media indicate strenuous efforts on the part of some foreign intelligence agencies to benefit their national industries. These efforts have included eavesdropping, hotel room burglaries, and introduction of "moles" as well as other sophisticated intelligence techniques. Our foreign competitors' interest in our information has never been more intense.

Our strengths lie in the intelligence and creativity of our society. Having been made aware of the threat to our information, our scientists and business people can apply their talents to the protection of valuable United States commercial information assets and thus contribute to our nation's economic security.

This booklet outlines some steps that may be taken to protect information and to raise the general level of awareness to the threat by Americans living, working or travelling abroad.

Chapter II. Guidelines

What Information Should We Protect?

Information that is not generally known outside a given American business or industry could give us a competitive advantage.

Such information need not be revolutionary, but can, and most probably will be, a simple improvement in the way a certain American industry produces a product or does business. It may pertain to a technical modification, a new technique, personnel policy, or a management concept. The key question - does it enhance our competitiveness?

The Information Audit

In practical terms an information audit requires each business unit, staff, or research manager to review his/her operation with the objective of answering one question - what qualities of my unit or business cause it to be unique and thus give it a competitive advantage?



Once this audit has been conducted, a security professional can estimate the cost of a reasonable level of protection, thus allowing the manager to make a business decision as to how much he/she is willing to spend to protect the competitive information.

Frequently, such protection is cost free because procedural changes can often address the vulnerable areas. In any event, the audit allows the manager to make an affirmative, active business decision on protecting competitive information, rather than passively letting the issue lie unaddressed and hoping for the best.

Levels of Information Protection

General

The normal and prudent security steps taken by a business to protect its people, facilities and information, provide a base line of protection. Security of personnel, facilities and information, in fact, go hand-in-hand. Prudence dictates, for instance, that unescorted visitors, unauthorized personnel and the general public be restricted from research, production and business areas where competitive information is processed. Existing security controls can be improved or modified toward this end and thus retard or prevent the compromise or theft of competitive information.

Heightened Awareness

This extra effort provides a heightened level of protection, forcing a thief to first penetrate general security precautions and then face the special protective measures established for competitive or proprietary information.

A major contributor to this level of protection is an increased awareness on the part of the people working with the information as to the value of what they are doing.

Ideally, through education and awareness training, employees will appreciate and support the protection of information. Once this is instilled, effectiveness of the effort increases since the people involved with the

information will realize that the competitive edge of their company, and thus possibly their jobs, depends upon them doing their part.

Security professionals are not the ultimate solution to the protection of information, as even a security expert cannot be proficient in every aspect of a company's business. Rather, the



people who work with the information must be the final authority. They know what to protect and will most likely recognize many of the more subtle attempts to illicitly learn the information.

The time and money invested to protect information is most efficiently spent when it is used to raise the awareness level of each employee.

Chapter III. American Attitudes

Exploitation of Our Traits

Many Americans possess personality traits which increase their vulnerability to the classic routines of espionage. Just as they were used during the Cold War, many of these techniques are now being applied by some foreign intelligence agencies to obtain proprietary or sensitive American business information.

Sociability

Americans characteristically want to be liked, and in order to gain approval we tend to be social and gregarious even with casual contacts. Similarly, we generally place a high value on candor and on trust, and tend to be more open towards those who display these traits.

Status

The phenomenal accomplishments of American enterprise in business, war, and world leadership has instilled in many of us a feeling of superiority toward other cultures and has caused us to place

great emphasis on money, materialism and status as measures of success. These values and attitudes render many of us susceptible to an approach which exploits our perceived obsession with wealth and "things".

Ambition

Americans tend to be ambitious, oriented toward job advancement and professional recognition.



These three personality traits - sociability, status and ambition - are logical targets for those attempting to apply a direct approach to either deceive Americans into carelessly providing competitive information or to seduce the unprincipled to cooperate in turning over such information to business rivals.

Additionally, these traits may reinforce the feelings of loneliness and isolation experienced by some Americans living abroad, especially when those persons are concurrently under pressure to succeed in a foreign environment. Those who are without the support of familiar neighbors, friends and relatives can be vulnerable to people who offer friendship, understanding and flattery, but who may also have an ulterior motive - gathering competitive business information.

Ethnic Feelings

American society is a paradox because our ancestry stems from every race and culture.

On the one hand we represent a unique culture to which we feel a strong sense of pride and loyalty. On the other, many of us also feel a strong sense of identity with our ancestral roots.

Foreign intelligence services may attempt to take advantage of the sense of ethnic identity felt by many Americans to elicit competitive information based upon appeals by persons of similar ethnic or cultural background.

Indeed, an approach based on ethnic or cultural similarity may not be what it seems. An intelligence service may attempt a "false flag" recruitment, in which an American with a strong sense of ethnic identity is approached on the basis of aiding his/her ancestral country, when in reality the real recipient of the information is a different country entirely.

Chapter IV. Office

Need for Awareness Program

The American business or research office overseas is a principal target of those seeking to compromise American competitive business information.

Frequently, office security standards are lower overseas than in the United States, for several reasons. In many locations, for instance, crime is of little concern and liability is not a major problem.



A strong awareness program may well be necessary before attempting to initiate security standards required by information protection. In fact, attempting to establish the security standards without an awareness program will probably doom the effort to failure, as employees are generally reluctant to support any effort without fully understanding why it is necessary and how it will benefit them and their company.

Ideal General Security Level

The following represents the ideal for establishing a general security level. What is possible may entail establishing security at a substantially lower level.

Security personnel should control the access to all office perimeter openings and be in control of all keys and access cards to these openings. All employees and non-employees should be issued and wear proper identification in clear view on their outer garment whenever they are in office areas which contain competitive information.

Relocation

Security of competitive information should be integral to any other business decisions made which involve the relocation of business or research offices overseas. The types of data at risk should be catalogued and the possibility of loss factored into management's decision making process. If the decision to relocate is made, security concerns should influence the building site, location and type of construction.

High Security Areas

Certain offices or portions thereof may require designation as high security areas if they contain highly sensitive competitive information to which access is limited. In these instances, entry should be restricted to only those persons who possess special identification and who are specifically permitted entry via a higher level access control device than those devices utilized at the perimeter of the building.

A procedure, such as a receipt and copy accountability system, should be established for the authorized removal of all competitive information blueprints, drawings and other documents contained in the general building area or high security areas.

All visitors and suppliers should be escorted throughout the premises by the person they are visiting. Security restrictions for admittance to high security areas, as outlined above, must be



established and observed.

Visitor tours of buildings containing competitive information should be discouraged. All visitors must be controlled, documented, and required to wear a photo identification. Visitor tours of high security areas should be prohibited.

Remember the earlier discussion on foreign intelligence operations. Do not acquiesce to a visitor's entry into a sensitive or high security area simply because he/she appears to be a "buddy" or because you are concerned that he/she will be offended if denied entry. Any visitor who employs those tactics should be brought to the attention of the security officer.

High security areas include, but are not limited to, design studios, strategic planning areas, engineering and research facilities, mail rooms, telephone switching rooms, computer facilities and other similar areas.

General Office

Photo copiers, facsimile machines and other reproduction equipment should be restricted to high security areas, if practical. If this cannot be done, the equipment should be provided with access control devices to prevent unauthorized usage.

Lockable file cabinets, desks and vaults should be provided in office buildings to secure competitive information when not in use or when being stored. There must be adequate control over keys, combination locks and/or access cards to maintain the effectiveness of these devices. The manager in charge of a particular area of the office building is responsible for ensuring that procedures are in effect to control the issuance of keys and/or access cards to ensure their retrieval when employees change assignments, retire or leave the company. In addition, a regular program of changing locks and combinations on file cabinets, desks, offices, and vaults used to store competitive information, should be implemented. These should be changed as follows: at predetermined intervals (but not less than once a year), after keys or combinations have been lost or otherwise subjected to possible compromise, and on the departure of employees from the organization who knew or had access to the combinations and/or keys.

In addition to documentation being secured and accounted for, such items as photographs, slides, negatives or other facsimiles of confidential company products and processes must be adequately secured. A log to assure accountability for these materials should also be maintained and reconciled on a regular basis.



A "clean desk" policy should be encouraged throughout the office building during all non-working hours. In high security areas, a "clean desk" policy is mandatory.

Cleaning maintenance of the general building areas, especially high security areas, should be done only when responsible company supervisors are present to monitor such activity.

All competitive information - documents, records, photographs, slides, negatives or other facsimiles - must be positively destroyed when they are no longer needed. Each work area should have adequate shredding capabilities or controlled disposal functions available for the proper destruction of such competitive information no matter what form it is in. Each functional area is responsible for verifying that such competitive information is disposed of properly.

After the disposal process is completed, the assigned observers must insure that the residue does not contain any document or record fragments of sufficient form to represent a risk of disclosure.

All unstaffed openings - windows as well as doors - to the perimeter of the office building as well as to high security areas should be provided with intrusion alarm monitoring so as to insure the detection of unauthorized personnel. Alarm systems should be supplemented by lighting, as discussed below. The alarm signal must be collected at a location where a speedy and appropriate response can be provided.

The entire perimeter of any office building which serves as a perimeter barrier should be adequately illuminated during hours of darkness. Other perimeters, such as walls, fences and natural barriers, must also be illuminated to both detect and deter persons attempting to gain unauthorized access to the building. Adequate interior "night" lights should be left on whenever the building is not occupied.

Chapter V. Home

Many of the same principles which apply to maintaining a safe and secure office apply equally to a residence. These elements will vary depending on the environment and the associated risk factors. As a minimum, however, the level of protection afforded competitive information taken home must be equal to or greater than the standard of protection it is afforded in the office.

Access to residential buildings where competitive information is located must be limited to only authorized persons. This will require appropriate locking devices and an alarm system



which will detect an attempted intrusion and alert authorities and other responsible parties.

Specific area(s) within the residence should be designated for working on competitive information. Access should be limited to authorized family and service personnel. Such information, when left unattended, should be secured in an appropriate container. Control of the keys for these containers should be limited.

Cleaning activities should be done only when competitive information items are cleared from the area, secured, or when the area is monitored by the owner, custodian, or user of the information.

A favorite technique of information thieves is the examination of trash containers. Consequently, the disposal of competitive information should be accomplished at home only if appropriate shredders are provided. If not, such materials should be transported to the workplace where they may be properly destroyed.

Chapter VI. Personnel

The majority of competitive information theft cases which occur in the United States involve a company's own employee(s). We know of no reason why this should be any different overseas.

Behind many of these cases are the same motivations and human frailties which we experience in other types of thefts: illegal or excessive use of drugs or alcohol, money problems, personal stress and just plain greed.

In some cases, two other factors have been detected - 1) fear of firing or layoff, and 2) falsification by the information thief of resume information.

When local laws allow, it is prudent to conduct background investigations on prospective employees. Such investigations should include as a minimum, the applicant's history of criminal convictions, credit records, and verification of resume, including educational history. Successful clearance in these areas, while not airtight, decreases the likelihood that the prospective employee will become an information thief.

A difficult problem is presented when a foreign intelligence agency is involved in attempting to coerce or persuade its nationals to provide competitive information. A local or foreign employee who is otherwise a good corporate citizen, may feel the pressure of patriotism or



intimidation by an all powerful government agency to provide competitive information belonging to his/her American employer.

An employee's rank in the company is not necessarily commensurate with the interest of a foreign intelligence agency. 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.

Although it is not the purpose of this publication to discuss management practices, it is important to note that in relations with lower ranking employees, loyalty goes in both directions.

Treating people fairly and providing a decent wage engenders loyalty and thus enhances security.

While there are no easy answers to the problem of a foreign intelligence agency targeting an American company, common sense applications may help. Clearly relating a company's competitive information to the amount of employees' paychecks and bonus, and even to the future existence of their jobs, may help.

Application of "need to know" procedures will also help. Carefully compartmentalizing competitive information on that basis provides two advantages. First, it slows or stops an information thief. Secondly, it may well provide an indicator of attempted thievery by highlighting those employees who attempt to obtain competitive information beyond their authorized "need to know".

Chapter VII. Communications

Introduction

Because they are so easily accessed and intercepted, corporate telecommunications present a highly vulnerable and lucrative target for anyone interested in obtaining trade secrets and competitive information. Increased usage by businesses of these links for bulk computer data transmission and electronic mail makes telecommunications intercept efforts cost-effective for intelligence collectors worldwide. As an example, approximately half of all overseas telecommunications are facsimile transmissions which, because they are emanations, may be intercepted by foreign intelligence services since many of the foreign telephone companies



are foreign owned. In addition, many American companies have begun using what is called electronic data interchange, a system of transferring corporate bidding, invoice and pricing data electronically overseas. This type of information is invaluable to many foreign intelligence services which support their national businesses.

Many corporations are falsely reassured in assuming that because

access to their computers is controlled, specific files can be read only by authorized users. It has been demonstrated, however, that an innovative "hacker" connected to computers containing competitive information, can evade the controls and access that information. For example, in a widely publicized case, referred to as the "Hanover Hacker Case", a foreign intelligence service employed computer hackers to access U.S. restricted data bases, obtaining both software and defense-related information. The service was able to do this because, although the computers themselves were secure, the telecommunications network that linked them was vulnerable by virtue of poorly implemented security mechanisms.

A typical economic espionage operation scenario might be as follows:

- A foreign intelligence service rents an office near the targeted U.S. firm or in another location strategically selected to provide easy access to telecommunications facilities or transmissions used by the U.S. firm.
- Sophisticated electronic listening posts are set up in the office and manned around the clock.
- The listening posts eavesdrop on telephone, fax, telex and computer communications.
- All intercepted communications are fed into computers, which sift through the material for valuable data.
- Reports and briefs are prepared and passed to the foreign rival of the U.S. firm.

Economic espionage, serious today, will certainly continue to increase as international relations become more and more a matter of economic, rather than military competition.

This threat is exacerbated by the increased use of extremely vulnerable electronic communications. We simply must assume that all overseas telecommunications are intercepted, recorded, organized into reports and reviewed for economic intelligence by everyone interested in the information. To stay with our foreign competitors, we must



"button-up" all competitive and proprietary communications.

Electronic Transmissions Routine Procedure

Most foreign common carriers are government-controlled or -owned. Trade secrets/data, marketing strategies, and personnel information which are discussed or sent over host country telephone lines are easily obtained by foreign interests.

Electronic Media Path

Electronic data is recovered easiest when a signal is not multiplexed or mixed with other data signals, i. e. data transmitted from a telephone instrument to a telephone switch. Only a minimal investment is required to retrieve data not masked with other voice or data. For this reason, it is better to use standard dial-up versus dedicated lines. Data/voice that is routed on major transmission paths (such as microwave, satellite transmission) have less likelihood of being monitored by hackers or low cost monitoring operations, because the cost of sifting through such a volume of information to access one target is often cost prohibitive. However, a well-financed intelligence gathering operation may find satellite or microwave transmissions the best intercept opportunity, since they can be monitored at great distances with little or no threat of detection.

Electronic Transmission Threats and Vulnerabilities

A threat is a fact, idea, situation, person, or thing which is perceived to menace, exploit or attack any vulnerability in security safeguards. Anyone involved in international communications should be aware of the following threats and vulnerabilities.

Threats

- Many foreign phone systems are either owned or controlled by the host government. This allows the government to easily monitor transmissions of selected U.S. organizations.
- Intelligence agencies of third party nations, terrorists, and criminals also monitor electronic transmissions. While monitoring is more difficult for them than for the host country, the equipment required for such surveillance can be easily obtained by almost anyone.
- Business and technical data obtained from U.S. corporations may be, and often is, provided to foreign competitors and potential customers.



- Personal information obtained may be used to kidnap executives for financial gain or political purposes.
- Electronic equipment, such as facsimile machines, telephones, and desktop computers, may be altered to make electronic monitoring easier. These alterations may be made either to the transmitting/receiving device itself or to the lines leading to and from the devices.

Vulnerabilities

- Telecommunications monitoring may be done at a phone company's switching facilities; phone lines may be tapped or bugged; or microwave transmissions may be intercepted anywhere between the two microwave transmitters. In any event, telecommunications monitoring may be virtually undetectable.
- Telephones do not necessarily cease transmitting once they are hung-up. Conversations taking place near a phone may be transmitted to the foreign state's phone system switching facility and can be monitored anywhere between the phone and that facility.
- Employees of U.S. organizations are often not aware of the threat to their transmissions.
- Most international U.S. corporate telecommunications are not encrypted. Some countries do not allow encryption of telecommunications traffic within their borders, but it should be considered where feasible for any transmission of competitive information.
- Many telecommunications transmissions will contain "key words", used to identify information of interest to a third party. A key word can be the name of a technology, product, project, or anything else which may identify the subject of the transmission.
- Encryption should be the first line of defense since it is easier for foreign intelligence services to monitor lines than to place "bugs", however encryption will provide little if any security if a careful examination for audio "bugs" elsewhere in the room is not conducted.

Suggested Counter-Measures

Below is a list of suggested actions which may be taken in order to improve the security of your telecommunications transmissions. The suggestions may be augmented by other measures which may be applicable to your organization.



- Neutralize the vulnerability of telephones. A small, company controlled switch installed within the facility can help ensure that conversations are not transmitted through handsets which are "hung-up", and can also serve to decrease the threat of covert line access.
- Avoid "key words" or phrases which may be used by intelligence agencies and others to search recorded conversations for subjects of interest. Examples would be project names, product names, the names of persons of interest (e.g. heads of state, CEO's, etc.) and classification labels such as "sensitive" and "company confidential".
- Positively identify all parties participating in phone conversations or receiving the facsimile transmissions.
- Whenever possible, utilize your corporate transmission facilities instead of those of the host government.
- Corporate offices should be located in facilities totally controlled by the corporation.
- Always keep at least one phone and facsimile machine secured in a container equipped with a combination lock, and restrict access to the combination. This will help maintain the integrity of that equipment.
- Check connecting lines to telecommunication devices (telephones, computers, fax machines, etc.) monthly to ensure that the line has not been replaced or modified by unauthorized personnel.
- Placing stickers on phones warning of hostile monitoring will be helpful to maintain awareness.

Effects of Telecommunications on Computer Security

Telecommunications technology provides for electronic "highways" which now enable a person to directly access a computer system on another continent. Many U.S. corporations are dependent for their very survival on data being stored and processed on these computers. It is therefore mandatory that access control security software and procedures are implemented for any computer interfacing with a network or telephone system.

Hacking into computers is now a standard tool for those involved in espionage and computer crime. Once an intruder has gained entry, he/she may be able to view, change, or destroy



valuable company data and information. Electronic terrorism, placing a corporation's information assets at risk, is also possible.

Consider the following tips to reduce the possibility of unauthorized access through networks:

- Apply access control software and procedures to the corporation's networks; keep the intruder off the "highway". Also ensure that the corporation's computer systems are protected.
- Mandate that all users change passwords at least once every 60 days, allow no more than three consecutive invalid passwords before suspending a user ID, and insure that all passwords are at least six characters in length. Also, encourage employees to use passwords which do not relate to their lives (names of family, pets, sports teams, etc.). Hackers often gain entry by simply guessing passwords. These precautions will make their job harder.
- Control the phone numbers to the corporation's networks and computer systems as competitive information. Minimize their distribution and notify corporate employees that the numbers should be guarded.
- Test corporate networks for the existence of unauthorized modems which could provide access to eavesdroppers.
- Encrypt computer to computer sensitive transmissions, to include electronic mail.
- Require all personnel to agree in writing before they are granted access to corporate networks and computer systems, that they will keep competitive information confidential and will abide by the corporation's information protection standards.

Video Conferencing

The threat to video conferencing is essentially the same as that to other types of telecommunications, in that adversaries can purchase or replicate specific equipment used by an American company and then either tap into the line or use other means to monitor both audio and video.

Although encryption is available for some video conferencing installations, many countries do not allow any type of encryption and others allow only that type which they can break.

In summary, video conferencing can be monitored. Though such monitoring requires a greater



effort, the capability is well within the means of a foreign intelligence agency.

Courier

Because of the extreme vulnerabilities to telecommunications and the restrictions placed upon the use of data encryption in many foreign countries, it may be best to handcarry information to, from and within overseas areas. The same precautions should be taken for hand-carried packages as for hand carried personal computers, as described on the next two pages under the subheading Computer Theft. That is, the package should never be out of the courier's direct control. It should stay with the courier at all times and never be checked in one of the temporary storage lockers often found at airports and in train stations, even for a short time.

Chapter VIII. Computers

Computer Technology

Computers can pose enormous security problems. While they contain great volumes of information, they also concentrate it, and if not protected, they can make the task of the information thief much easier.

The emergence of low-cost technologies, such as small computer systems, presents major opportunities for management to enhance productivity and reduce operating costs. The radical increase in offices driven by the personal computer has taken computer security out of the hands of a small circle of experts who once focused on securing self-contained computer rooms.

Computers were once stationary objects, secured by placing them behind locked doors. Today, many computers (e.g. notebook and laptop PCs) are designed and manufactured to enable them to be carried from one place to another as an aid to daily business activities.

It is now recognized that the information stored in and processed by a computer is often more valuable than the equipment itself. Assuring the confidentiality, integrity and availability of that information has become a common concern for an ever-widening group of managers, information systems professionals and end-users.

The International Business Traveler



Business travelers who carry and use personal or laptop computers are at risk - particularly if they are unaware of common sense security measures which should be adopted to protect computers and their contents from theft and unauthorized data access.

Computer Theft

It is obvious to a knowledgeable observer by the distinctive shape of the carrying case and the special care taken by the owner, when a person is carrying a computer. Because of this, the PC is a clear target for its intrinsic value. A ready market for stolen equipment and the computer's compact size make the theft a very lucrative, low risk venture for the criminal.

A personal computer should never be checked with other luggage, but should always be part of your carry-on baggage that will stay with you at all times.

Likewise it should never be checked in a temporary airport or train station storage locker, even for a short time.

Greater risk is associated with the information stored on the hard disk of the personal computer. There has always been a degree of risk associated with carrying competitive information in a briefcase, although the bulk and weight of documents limit the number. However, it is possible to store thousands of notes, memos, and full documents on a personal computer hard disk drive. Therefore, the loss or theft of a PC poses a significantly greater risk of valuable information loss than ever experienced in the past.

Unauthorized Access

Unauthorized access occurs when someone accidentally or deliberately reads, modifies, or deletes computer files without your specific permission. Because personal computers do not typically impose data access controls, it is your responsibility to protect your data. While using your computer, protect the information from casual, "over-the-shoulder" viewing by others. Log-on and data encryption software can provide additional protection.

Obviously, as the size and clarity of portable computer screens continue to increase, so too does the vulnerability to unauthorized observation by people in airport waiting rooms, cafeterias or snack bars, as well as in your plane seat. Positioning oneself so that it is impossible for others to observe the screen can be achieved in a restaurant or snack bar, but is very difficult if not impossible in one's plane seat. One possible strategy is to work on more mundane, non-confidential, non-sensitive work on the plane, and make the presumption that



the screen will indeed be observed. Sometimes the aircraft crew will prohibit use of a portable on the aircraft.

Foreign Customs

The traveler must bear in mind that a portable computer is a valuable asset. The national requirements for bringing in such a device vary from country to country, e.g., some countries absolutely forbid bringing in a personal computer except one manufactured in that particular country. Therefore, before even starting on the trip, it is important to check with your legal and security offices concerning customs requirements and necessary documentation. Otherwise, long delays, risk of confiscation, and possible frustrating experiences in attempting to communicate in another language may await the traveler at the airport.

Working From Hotels

Persons traveling in the U.S. expect high quality telephone service. It would not be appropriate to assume that the same will be the case when traveling overseas. In many countries, the telephone service is owned and operated by the national post, telephone and telegraph company. The quality of service, as well as the technical standards and conventions used, will vary dramatically from country to country. For example, in many countries, it is impossible to simply pull the removable jack from the telephone handset in the room, and plug it into the modem in the PC. Types of jacks and connections differ from country to country, and sometimes within the same country.

Your company may be targeted by a foreign intelligence service which is able to monitor your communications. In most foreign countries only a few central "switching points" serve to control all international telephone calls whether voice, fax or data stream. Intelligence agencies can tap into these sources without indicating to you that such activity is underway. (See Telecommunications Lines)

Special Risks When Using Cellular PCs

The cellular portable computer is relatively new technology, having unique security considerations which one might easily overlook. The system is essentially a personal computer with an integrated modem, which is a device used to change signals understood by telephone technology into signals understood by computers, and vice versa. There is also a built-in cellular telephone which allows a person with a single action to place a call to a computer system, connect the personal computer to it, and interact with a host computer. Sometimes overlooked with this technology is the fact that cellular telephone communications



use radio signals and are, therefore, vulnerable to unauthorized interception, recording, and subsequent analysis. The necessary monitoring equipment is readily available to foreign intelligence services and to the more sophisticated business espionage agent. Therefore, one should consider carefully whether such interception is acceptable.

Virus Contamination and Detection

Special care must always be taken when receiving a PC program from someone else because the program being given to you may have been contaminated by a computer virus without the knowledge of the person giving it to you. Unfortunately, many viruses are intended to destroy files on a person's hard and/or floppy disks, which could have a catastrophic effect on the user of the PC. Since much has already been said about computer viruses, it is not necessary to review theory again here. Suffice it to say that whenever someone copies a program from a bulletin board, or receives a floppy disk from someone else, that program or floppy disk should be scanned to identify any known viruses present within the programs in question. Many such virus scanning programs are available at reasonable cost, and their use is highly recommended.

The Office Manager Stationed Overseas

There are many security considerations which anyone providing computing services to multiple users must provide, regardless of where the computing facility is located. They include physical access control, magnetic media control, the effective operation of access control sub systems, restricted utility program control, testing for system vulnerabilities, classification of competitive information in the system, printer controls, special controls of the enterprise's most important information, access from terminals not under the enterprise's control, use of supplemental, contractor or vendor personnel within the facility, and finally disaster backup and recovery. When the facility is located overseas, the following additional security issues must be considered:

Physical Access To Computing Facility

Because one cannot assume that employment practices are the same from country to country, it is not always possible to dictate what employees can do or where they can go. For example, in certain countries it is not permitted to log the fact that a specific person accessed a specific data set at a certain time on a certain date, because such a log could be misused to inappropriately monitor his/her work habits, speed, productivity, etc. Likewise, in some countries, there are resident fire marshals in the facility who do not work for the enterprise, but



are authorized access to each and every part of the physical facility. Factors such as these must be understood and carefully planned for.

Telecommunications Lines

U. S. telecommunications carriers are private corporations, subject to stringent government controls in the public interest. Often, in other countries, the public carrier is a governmental agency responsible for post, telephone and telegraph. In some, the distinctions between the interests of private industry and the national economy as a whole are blurred. In those, the telephone agency could monitor the telephone lines and provide the information gathered to its own private industry to the detriment of an American company. Because this possibility could be compounded by the activities of a foreign intelligence service, it would be prudent to carefully evaluate practices for the transmission of important competitive information.

Magnetic Media Control

For some of the same reasons pertaining to telecommunications, the manager must be sensitive to mailing or physically carrying magnetic media from one country to another. While the metal detection devices used at most airports no longer damage the information on magnetic media, other dangers, such as an interaction with the local customs authorities, could be far more damaging to a business. In either mailing or carrying, accountability is lost once the material is turned over to local customs personnel to be "cleared". Often, the time involved as well as the other details of what "cleared" means are not always spelled out to private industry.

Use of Encryption

One method of protecting the secrecy of competitive business information is through the use of encryption technology. Simply stated, encryption is the process whereby information which is normally readable is rendered incomprehensible by either physical devices or programs so that it can be transmitted over public telephone lines with no fear of it being compromised. Once received, the encrypted information is decrypted back to understandable language. The Data Encryption Standard (DES), one of the best algorithms used to encrypt and decrypt data, may not be exported from the United States without special licensing. Likewise, some countries do not permit the importation of a DES program without special licensing agreements. Even if DES can not be used, one would be well advised to consider using some method of data encryption to try to preserve the secrecy of competitive data.



Distributed Printer Control

Generally, physical access to printers used within a computing center is well controlled. However, small, powerful, distributed printing facilities, which can be readily hooked-up with printed output routed directly to such devices by any employee, are coming increasingly into use. It is strongly recommended that attention be given to ensuring that printed output may be picked up only by the information owner or his/her representatives. This can be accomplished by placing the printers in a room having a key, cipher lock, or other controlled access system.

Cross Border Flow Of Information

A security/privacy issue not normally encountered in the United States is that of competitive information, such as human resources files on employees, or the data base of customer accounts, being accorded the status of an individual. Because it falls under national privacy legislation, a business may not always be at liberty to send a data base containing aggregations of records outside the country. Although one might wonder what a customer account data base has to do with privacy rights, the fact remains that different countries may have very stringent national laws specifying what is permissible and what is not. The manager must understand and respect such laws on export of data from a country, or risk unwittingly running afoul of the law.

Chapter IX. Travelers

Increased Risk

American business persons face significantly higher risk of information loss while traveling than when engaged in normal activities at or near the corporate headquarters. The risk to information associated with travel stems from the traveler's lack of familiarity with the country being visited and disorientation caused by an unfamiliar environment. The recommended security procedures listed in this section outline basic security practices necessary for the protection of information while traveling overseas.

Our Vulnerability

Scientific Conferences

Historically, scientific conferences and trade association meetings have been targeted by some foreign intelligence agents seeking defense related information. Today these meetings are still targeted, but the goal is to learn economic information - information that will improve



the position of our foreign competitors. Individuals engaged in collecting information are not necessarily intelligence officers of the foreign government. Many times they are business persons, managers, corporate officers, sales people, scientists, engineers, and other technical personnel. There is a growing trend for foreign corporations to employ former intelligence officers for industrial work. We can protect ourselves by practicing discretion and remembering that not only time, but information, is money.

Eavesdropping

Discussions on airplanes are overheard by those around you. Eavesdropping can result in gathering meaningful information in a radius of 6-8 seats.

Recent revelations in the media specifically mention valuable information gathered by eavesdropping on conversations held on aircraft and in bars and restaurants.

Information of competitive value should not be discussed in public places.

Hotel Rooms and Vaults

Hotel rooms are not secure. Leaving important company information in your room, even in a locked briefcase, 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 without you becoming aware of the compromise. Reduce your hard copy material as much as possible and carry what you must take on your person, possibly on computer media; but recognize that in the age of laptops even these cannot be left where others can gain access to them.

Destruction of Information Waste

Keep unwanted material until you can dispose of it securely. Ideally, paper should be burned or shredded. If shredded, the type of shredder should cut horizontally and vertically. Floppy disks should be cut in small pieces and discarded.

Communications

Avoid sending facsimiles or conducting sensitive conversations on local or international telephone lines. Fax, telex, and data systems are all vulnerable to interception, particularly in overseas hotels. On important issues, go to the extra trouble of identifying company travelers



for the purpose of carrying information rather than entrusting it to less secure electronic means.

Be Alert

Be aware of new acquaintances who probe for information or attempt to place you in a compromising situation. In an unusual situation, have an American colleague present.

The watchword in travel while in foreign countries is discretion.

Appendix I

Home Security Checklist

Home Security Checklist

Access to residential buildings.

- Limited to authorized persons.
- Appropriate locking devices.
- Alarm system required. Monitor so as to insure timely and appropriate response.

Specific work areas for competitive business information.

- Specific work area identified.
- Limit access to authorized persons.

Storage facilities.

- Appropriate controlled facilities provided.
- Limit distribution of keys and combinations to authorized personnel.

Cleaning activities.

- Performed in competitive information work/storage area only when information is secure and/or owner or custodian is in attendance.



Disposal of competitive information.

- Provide approved shredder or
- Collect and return to workplace for proper destruction.
- Competitive business information should not be recycled.

Appendix II Office Security

Office Security

Access control.

- Perimeter.
- All openings controlled by security personnel or system.
- All employees wear photo identification in clear view.
- Non-employees wear name and affiliation identification (one day badges).

High security areas.

- High security areas designated for highly sensitive information.
- Access limited to those persons provided special identification and access based upon a "need to know" basis.

Property removal.

- Authorization required for removal of competitive business information.

Visitor control.

- All visitors and suppliers should be escorted.
- All visitors should wear special identification which is controlled and documented.
- Special clearance to be required for admittance of non-employees.
- Visitor tours should be discouraged but if conducted, carefully controlled.
- Visitor tours of high security areas are prohibited.

Copiers, communications and reproduction equipment.

- Photo copiers, facsimile machines and other reproduction equipment should be restricted to "high security" areas if practical.



- If above is not possible, equipment should be provided with access control devices or placed in a controlled environment based on sensitivity of information handled.

Storage facilities.

- Secure facilities are to be provided for storage of competitive information such as desks, offices, safes, vaults, filing cabinets, etc.

Lock and key control.

- Adequate control over keys, combination locks and/or access cards.
- Management person responsible for issuance of keys and/or access cards and their retrieval.
- Locks and combinations changed on regular interval.
- Other competitive information in addition to documents, i.e., photographs, slides, negatives, etc., must also be adequately secured and accounted for and reconciled on a regular basis.

Clean desk policy.

- Encouraged through all offices during non-business hours.
- Clean desk policy required in "high security areas".

Cleaning/Maintenance

- Should be done during times when responsible company supervisors are present to monitor such activity.

Disposal of all competitive information.

- Must be destroyed when no longer needed.
- Each work area must have adequate shredding capabilities or controlled disposal functions.
- Each functional area is responsible for verifying that competitive information is properly disposed of.

Alarm devices.

- All unstaffed office building perimeter openings and high security areas are to be provided with a monitored alarm system.



- Alarms are to be monitored so as to provide appropriate response.

Lighting

- Adequate lighting is to be provided for all perimeter lines and barriers during hours of darkness.

Appendix III Computer Security Checklist

Computer Security Checklist

International Travel

- Does the local power supply match your system's requirements? Are electrical power transformers, filters, surge protectors or uninterruptible power supply (UPS) units available to protect your equipment?
- Does the government impose restrictions on the import of computer hardware and software into the country?

Environment

- Will the computer be used in a low humidity area where damage from static electricity may be sustained? Are carpets treated? Are humidifiers available?
- Will the computer be used in a hot, dusty climate? Are office temperature controls sufficient? Are dust covers available?

Physical Security

- Is the work area kept clear of soft drinks, coffee and other liquids which, when accidentally spilled, may damage equipment?
- Are diskettes physically labelled and handled as directed by the manufacturer? Are sensitive diskettes sufficiently write-protected to avoid accidental or malicious damage or destruction?
- Are backup copies stored off-site?
- Is the computer sufficiently protected from acts of sabotage, tampering and theft?
- Are modems (particularly those with an automatic answer feature) disconnected or powered off when not in use?
- Are film printer ribbons, sensitive printouts and diskettes burned, shredded or degaussed as appropriate to prevent inadvertent information disclosure?



System Security

- Are spare, user-serviceable parts available in the event of failure?
- Are backup copies of software and data produced periodically?
- Has a backup system (contingency) been identified to continue critical operations in the event of a failure/disaster? Has it been tested?
- Are system hardware and/or software controls present to authenticate individual system users? Are passwords changed frequently and are they easily guessed?
- Is a security erase or file scrub program present on the system that will over-write sensitive data on the hard disk when a file is deleted? Is it used?
- Are sufficient controls in place to prevent violation of manufacturer's copyright and license agreements?

Virus Protection

- Are software and data diskettes received from reliable, trustworthy sources?
- Is software received from outside sources scanned for computer viruses with current virus detection software?