Corporate espionage is an increasingly serious threat for a business traveler. The perpetrator may be a competitor, opportunist, or foreign intelligence officer. In many countries, domestic corporations collect competitive intelligence with the help and support of their government. To mitigate this risk, your organization's critical information and technologies should not reside on any hard copy or electronic device you take unless it is absolutely necessary, and if so, then you must safeguard the physical access to the information by using encryption and keeping the material on your person at all times. Hotel safes are not adequate protection.

Critical business information may include:

- Customer data
- Employee data
- Vendor information
- Pricing strategies
- Proprietary formulas and processes
- Technical components and plans
- Corporate strategies
- Corporate financial data
- Phone directories
- Computer access protocols
- Computer network design
- Acquisition strategies
- Marketing strategies
- Investment data
- Negotiation strategies
- Passwords (computer, phone, accounts)

Before You Go

Familiarize yourself with local laws and customs in the areas you plan to travel. You are expected to obey their laws, which may include dress standards, photography restrictions, telecommunication restrictions, curfews, etc.

Plan your wardrobe so that it does not offend the locals, nor draw unwanted attention to yourself. Americans are perceived as wealthy and are targeted for pick pocketing and other crimes. Do not wear expensive-looking jewelry and avoid wearing American team sports shirts or baseball caps that might indicate you are an American.

Make copies of your passport, airplane ticket, driver's license, and credit cards that you take with you. Keep one copy at home; carry a second copy with you but separate from the originals. This will help speed the replacement process if they are lost or stolen.

Do not take unnecessary identification or credit cards in case they are stolen. Take only what is necessary. Obtain traveler's checks if needed.

Establish points of contact for your family to contact and for your foreign hosts to contact in the event of an emergency. Register your trip with the State Department. Obtain the phone number and address for the US Embassy or Consulate in the country(s) you plan to visit.

Take any necessary medications with you in their original containers and keep them in your carry-on luggage (not checked baggage) during the flight. Verify you have adequate medical insurance.

Obtain specific pre-travel country risk assessments for the country(s) you plan to visit from your security officer, the State Department, and/or the FBI. There may be specific issues you should be aware of and prepare for that will ensure your safety and peace of mind.

Visit www.osac.gov for security news and reports for the country(s) you plan to visit.

Sanitize your laptop, telephone, & PDA, prior to travel and ensure no sensitive contact, research, or personal data is on them. Back-up all information you take and leave that at home. If feasible, use a "clean" laptop, phone and a new email account while traveling. Or **If you can do without the device, Do Not Take It!**

Cell phones can be hacked to steal contact lists, usernames, passwords, and browser history.

Use up-to-date protections for antivirus, spyware, security patches, and firewalls.

Clean out your voice mail. When you access your messages, the pass code may become compromised and others may then retrieve your messages.

During Your Stay

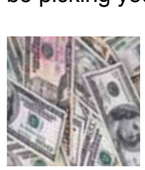
Protect your passport! Theft of American tourist passports is on the rise. It is recommended that you carry your passport in a front pants pocket or in a pouch hidden in your clothes, and that it remain with you at all times. Some hotels require you to leave it at the desk during your stay and they may use it to register you with the local police--a routine policy. Ask for a receipt and be sure to retrieve your passport before continuing your trip. If your passport is lost or stolen, report the situation immediately to the nearest US Embassy or Consulate.

Be courteous and cooperative when processing through customs. Do not leave your bags unattended. Stay alert.

Use authorized taxis. You could be overcharged, robbed or kidnapped when using "gypsy" taxis.

Do not invite strangers into your room.

Avoid traveling alone, especially after dark. Be conscious of your surroundings and avoid areas you believe may put your personal safety at risk. Be wary of street vendors and innocent-looking youngsters. While one person has your attention, another might be picking your pocket.



Do not carry large amounts of cash. Always deal with reputable currency exchange officials or you run the risk of receiving counterfeit currency. Keep a record of your financial transactions.

Beware that theft from sleeping compartments on trains is common.

Do not leave drinks unattended – someone could slip a drug into it that causes amnesia and sleep.

Avoid long waits in lobbies and terminals, if possible. These areas may harbor pickpockets, thieves, and violent offenders. Laptop theft is especially common in airports.

At the airport, a thief preceded a traveler through a security checkpoint. After the traveler placed his laptop computer on the x-ray machine conveyer belt, a second thief set off the metal detector causing a delay. The first thief then stole the traveler's laptop after it passed through the x-ray machine.

If you are arrested for any reason, ask to notify the nearest US Embassy or Consulate.

Beware of new acquaintances who probe for information about you or who attempt to get you involved in what could become a compromising situation.

Avoid civil disturbances and obey local laws. If you come upon a demonstration or rally, be careful; in the confusion you could be arrested or detained even though you are a bystander. Be mindful that in many countries, it is prohibited to speak derogatorily of the government and its leaders. It may be illegal to take photographs of train stations, government buildings, religious symbols, and military installations.

Avoid any actions that are illegal, improper or indiscreet. Avoid offers of sexual companionship; it may lead to a room raid, photography, and blackmail. Do not attempt to keep up with your hosts in social drinking. Do not engage in black market activities. Do not sell your possessions. Do not bring in or purchase illegal drugs or pornography. Do not seek out political or religious dissidents. Do not accept packages or letters for delivery to another location.

An American was given a letter by a man he had never met. He tried to return the letter but the man ran away. That evening national security officers visited the American and admonished him for taking the letter.

Keep a low profile and shun publicity. Do not discuss personal or business information with local news media and be careful what type of information you share with foreigners. They may have been directed to obtain information in order to exploit you or your company. Politely redirect the topic. The FBI can provide tips on how to recognize deceitful elicitations.

Evade criminals and terrorists by being aware of your surroundings and alert to the possibility of surveillance. Take mental notes of anyone following you and promptly report it to the appropriate security officials and/or the US Embassy or Consulate. In general, criminals will strike when their target seems most lax about his/her security. If anyone grabs you, make a scene—yell, kick and try to get away! If you are kidnapped, remain alert and establish a program of mental and physical activity for yourself; try to remain calm and non-threatening.

Do not gossip about character flaws, financial problems, emotional relationships, or other difficulties of your fellow Americans or yourself. This information is eagerly sought by those who want to exploit you or your fellow travelers.

State Department's travel website: www.state.gov/travel

Center for Disease Control for Travelers' Health: www.cdc.gov