

Risks You May Not Know About

Vigilance is key when identifying a corporation’s security risks and protecting its employees at home and on the road

A conversation with Juval Aviv

INsight spoke with Juval Aviv, President & CEO of Interfor, Inc., an international corporate intelligence and investigations firm, as well as the author of Staying Safe: The Complete Guide to Protecting Yourself, Your Family, & Your Business. A former Israeli counterterrorism intelligence officer before founding Interfor, Mr. Aviv has more than 30 years of experience working with corporations and other entities, both domestically and internationally, on security measures for the protection of assets and personnel.

INsight: You have said, “In an open society, the greatest risk is not knowing that you are at risk.” For corporations, what are the greatest risks they may not know about and for which they are ill-prepared?

Juval Aviv: Open societies are necessarily more forgiving and lax when it comes to security and safety vulnerabilities. Unfortunately, corporations that are based in such societies exhibit many of the same qualities. Security is usually designed to be non-intrusive and hidden from employees. Unfortunately, this concept is counterproductive and dangerous in today’s global economy. Due to this stance, many corporations are not positioned to confront existing and potential risks.

For example, most people are familiar with the concept of IT vulnerabilities. However, most people do not realize that the greatest IT vulnerability is not a system or technology; it is the mechanism in which employees interact with those systems. A corporation can have the best IT security in the world; however, if an employee loses his laptop at an airport or accesses his corporation’s network from an unprotected wifi interface at home, the vulnerabilities are not contained or mitigated. This risk becomes even more significant when you consider the increasing number of home-offices that corporations are shifting towards. A “clean-desk” policy or password protection system may be enforceable at a corporate office, but what happens when an employee works from home? Many people don’t even lock their doors during the day let alone worry about securing proprietary information.

Travel also exposes companies and their employees to increased risk, particularly in terms of securing proprietary information. Any time documents or information are taken away from a company’s secured facilities, there will be increased risk, both to the safety of their employees and the information that they are taking with them. Often this is overlooked and travel coordination is left completely up to the individual employee.

Overall, I consider the greatest vulnerabilities facing industries today to stem from what we call “human risk variables.” Specifically, I am referring to all the risks posed to a corporation by current or former employees, whether malicious or not. It is difficult to find a balance between providing adequate security for your company and clamping down so hard that your security measures hamper productivity or make your employees feel like they work in a prison. By giving employees the freedom that they need to feel comfortable and do their jobs efficiently, companies are unfortunately putting themselves in a position where a vital part of their security plan is in the hands of potentially thousands of employees.

In your experience, which of these risks is the most misunderstood or overlooked?

Again the human factor comes into play. People tend to forget that there may be fraudsters, identity thieves or maybe even terrorists who are actively trying to penetrate the security of their company. They become complacent and casual and the idea of personal risk seems remote. That is



when mistakes are made. The most costly and complex security measures in the world can be foiled by a lax employee.

Are some industries more vulnerable to these risks than others?

While no industry is invulnerable, some clearly face greater risks than others. For example, industries that have attracted the attention of activists, like high profile companies that have a reputation for polluting the environment or biotech companies, would be more vulnerable to risk. The pharmaceutical industry, obviously, would be at a very high risk from both counterfeiters and terrorists. Defense contractors, financial companies, food suppliers, all are at a greater risk. Any industry that makes a product for mass consumption, or which if disrupted would have a great economic impact on the country or the world, is more vulnerable. Vulnerability, though, really depends on the effectiveness of the individual company's security measures and the control they have over proprietary information and ingress to their facilities.

What steps can corporations take to effectively address these potential threats?

Addressing the problem of human risk variables is really just a matter of consistent and frequent training and testing. Employees need to be reminded to dispose of their trash properly, shut off power to their computers at night, lock up sensitive documents, and report lost I.D. and entry cards immediately. Employees too, out of an

Ultimately, by taking responsibility for travel safety, a company is not only protecting a valuable employee but their proprietary information as well.

ingrained habit of being polite, will often open doors to strangers who don't have entry cards or fail to question unauthorized people in sensitive areas. They need to know that simple things like this can expose their company and their fellow employees to great risk. They need to be reminded of security practices and measures on a regular basis to keep them top of mind.

In terms of threats coming from outside the company, obviously IT security is paramount. However, without a well-trained staff and good physical security measures, IT security is worthless.

For smaller companies that may not have a top notch security director on staff, it might be a good idea to hire a consultant who can help assess and coordinate their security plans. If you have a security staff on site, it

is vital that all aspects of security, including IT and physical security, be coordinated among the various departments.

What are the travel safety risks that often are overlooked by a corporation and its executives, consultants and other frequent flyers? Would you share some examples of problems that business travelers encounter? What are some solutions?

The best thing anyone can do when traveling, especially overseas, is to research and plan ahead. Check out government websites for travel warnings. Go online and read local news in the area in which you will be traveling to check for political unrest or violence. Get recommendations for good hotels in safe neighborhoods, preferably an American or European chain hotel as they will have modern hygiene standards and will have the best security.

Often, business travelers will choose hotels in business districts so that they will be near their clients or the locations of their meetings. Business districts in many cities, however, tend to be rather deserted at night and may not be the safest place to be after hours. It is preferable to stay in neighborhoods with restaurants and nightlife, where

Travelers should be inconspicuous with laptops, expensive cell phones and PDAs. Not only do these items attract petty thieves, but they contain valuable information that could cost their company large sums of money or expose them to risk.

there will be more street traffic and probably more of a police presence.

Alternately, crowded streets and squares are more likely places to harbor pickpockets. In volatile countries, crowds are likely targets for kidnappers or terrorists. These areas should be avoided.

If you are going to a third-world country, cabs may not always be safe and are often unregulated and unmarked. Get a recommendation for a reliable car service. It requires a bit of extra coordination but could save you a lot of trouble in the end.

What steps can a corporation take to help ensure safe travel for its employees?

If a company wants to ensure travel safety for its employees, it is best that they take responsibility for the travel planning and hire a travel expert or a reliable firm with global experience and connections. Leaving preparations up to a harried executive or an inexperienced assistant is more likely to end up in last minute arrangements and poor preparation.

Employees need to be reminded of security practices and measures on a regular basis to keep them top of mind.

If your employees are traveling outside the country, it would be a good idea to provide them with a mobile phone that works internationally and encourage them to check in on a regular basis. Your company should

also keep scanned copies of visas, passports and tickets that can be emailed to an embassy or consulate in the event of an emergency or if the originals are lost.

There are also companies that specialize in executive travel safety. They will know the safest hotels, areas to avoid and in less stable countries, they can provide executive protection services such as bodyguards or what we call “secure drivers.”

Medical evacuation companies like MedJet Assist provide medically-equipped planes staffed with trained medical personnel that will fly a client from wherever they are to a hospital of their choice in the event of a medical emergency. These services can be established for a relatively inexpensive annual subscription. Such services do differ from coverage that is provided by major credit cards in a number of important ways.

Ultimately, by taking responsibility for travel safety, a company is not only protecting a valuable employee but their proprietary information as well.

What are the employee’s responsibilities in traveling safely?

Employees must take the brunt of responsibility for their own safety. Any amount of advance planning and preparation can fall apart if a situation changes, so ultimately it will be up to the individual. Employees should be familiar with their travel plans and schedule before they leave. They should know how to contact the nearest embassy or consulate if there is trouble.

They should leave contact information at home and at work and while it seems obvious, if they are new to international travel, they should know how to dial their home or office for assistance from a foreign phone. They should also keep extra copies of all of their travel documents and identification in a secure place, like a hotel safe.

They should dress appropriately for the region that they are visiting. For example, business attire may not be the best idea when traveling in an impoverished area as it conveys the idea that they have money. This is a particularly sensitive issue with Western women traveling in third-world countries where social and religious mores, especially in relation to women, are very different. Clothing that would seem conservative in the United States may be scandalous or offensive in another country and could attract negative attention.

It is also a good idea to keep a certain amount of cash concealed somewhere on their person in case they are pickpocketed or mugged.

Travelers should be inconspicuous with laptops, expensive cell phones and PDAs. Not only do these items attract petty thieves, but they contain valuable information that could cost their company large sums of money or expose them to risk.

The most important thing for anyone to remember when traveling in an unfamiliar place is to keep your eyes open and obey your instincts. If a hotel does not feel safe, then move. If a driver makes you uncomfortable, take another car, etc. It may feel

silly in the moment, but often our instincts are a real signal that we are in danger and it is best to just go with it.

What risks do you see on the horizon that will affect corporations in the next few years? How can corporations best prepare today for future threats?

As companies continue to move away from the traditional 9 to 5 scenario where their employees work in a central location and leave that work behind when they go home, we will continue to see more opportunities for corporate fraudsters and thieves to attack. It is becoming more and more difficult to keep a lid on proprietary information as the workplace is decentralized and increasingly varied tasks are subcontracted out to foreign companies. The best thing any company can do to protect themselves against future threats is to go on the offense and plan, prepare, drill and plan some more.



...when traveling in an unfamiliar place, keep your eyes open and obey your instincts.

For more information on Juval Aviv's recommendations on corporate security and travel safety, his book, "Staying Safe", is available on Amazon.com. For physical security consultations or executive travel coordination please contact Don Aviv at Interfor, Inc. • 212-605-0375 or don.aviv@interforinc.com.

Safety Steps

Many executives and sales people frequently find themselves traveling alone, often to unfamiliar foreign destinations. Negotiating strange cities and countries on one's own can be hazardous, especially for women, who are far more likely to be robbed or attacked than men. Below are a few safety tips that might be particularly useful for women traveling alone:

- Avoid hairstyles like ponytails or braids that can be easily grabbed or pulled from behind.
- Avoid large or flashy jewelry. You are obviously more likely to be a target and you could be injured if a thief yanks a bracelet from your wrist or a necklace from your throat.
- Dress conservatively when traveling abroad, especially in economically depressed non-Western countries.
- Consider wearing a cheap wedding ring, even if you are not married. Especially in developing countries, a married woman is viewed as the property of another man and therefore off limits. This can help you avoid unwanted male attention.
- Consult maps before you walk or take public transportation and walk briskly and confidently, as if you know where you're going. Women looking lost or reading maps or searching distractedly through their purses are more likely to become victims.
- The most likely places for women to be attacked are parking lots, garages and public restrooms. Use valet parking if it is available and street parking if it is not. Use public restrooms only in busy restaurants or hotels.
- Most rapists or kidnappers are looking for someone who will not put up a fight. Scream, fight and try to run away and your attacker will most likely move on to an easier target.
- If someone is trying to snatch your purse, do not resist — let your bag go and then shout for help rather than risk assault.

THE FOLLOWING TIPS ARE GOOD IDEAS FOR ALL TRAVELERS:

- Take particular care when choosing your hotel. Aim for a hotel on a well-trafficked street with neighborhood restaurants and late-night stores. Business districts can often be deserted at night.
- Also choose a hotel with a reception or concierge desk with a clear view of both the entrance and the elevators. This is more likely to deter those who wish to rob or do harm as it will be difficult to enter unnoticed.
- Always ask that someone from the hotel escort you to your room and wait while you open the door and check to see that the room is empty.
- Do not choose street level rooms or rooms with balconies and French or sliding doors.
- Particularly if you are traveling in a foreign country, it is a good idea to conceal some money somewhere in your clothing, i.e., a hidden pocket or money belt. That way, if you do get mugged, you're not left helpless.
- Always carry a cell phone that works internationally. Program the numbers for your hotel, local hospitals, local police and the American embassy into your phone. Make sure that someone back home has these numbers as well.

Reprinted with permission from *Intelligencer*, Vol. 7, No. 2, Winter 2008, published by Interfor, Inc., 575 Madison Avenue, Suite 1006, New York, NY 10022. For further information, visit www.interforinc.com