SMI

Top Five Ways Business Executives are Spied Upon Overseas and How They Can Protect Themselves

Today's business environment is fast paced, ever changing and highly competitive. Global interconnectivity, coupled with competitive geopolitical realities, has created a new corporate dynamic that allows for few allies. Being one-step ahead of the competition is no longer a matter of securing a holiday bonus; it is vital to a company's survival. For these reasons, economic and industrial espionage operations – often collectively referred to as corporate espionage – are at an all time high.

According to recent statistics published by the FBI, at least 23 foreign governments actively target U.S. corporations for their proprietary trade information. But the threat is not just from state intelligence units. Increasingly the greatest percentage of corporate espionage is being conducted by private companies, those who would sooner skip investing millions in R&D and jump directly to a final product. Theft of intellectual property from both sources costs U.S. businesses over $300 billion per year. An overwhelming amount of this intelligence is stolen from executives when they travel abroad for business, most often without the individuals even realizing that they have been targeted or that their materials have been compromised. Government intelligence services, business competitors, and private collectors compete and conspire in this exchange and theft of proprietary information at levels the business world has ever known. It is imperative that any company and executive understand the risks implicit in business travel today. Only then can you begin to ensure the safety of vital trade secrets.

The five most common ways in which business travelers are spied upon overseas are:

1. E-mail hacking – This is particularly prevalent in Wi-Fi areas, such as airport business lounges or Internet cafes. If you can access the web in a public forum, someone else can access your computer. Uploading keylogging software or hacking into your emails is simply a matter of interest after that. If you think this sounds far-fetched, just tune into the scandal at the FDA. Whistleblowing employees at that agency had screenshot and keylogging spyware uploaded on their computers without their knowledge. Every email they sent, and every website they visited, was monitored by investigators. In Russia, in 2011 alone, over half a million phones and emails were officially tapped by the government. The technology is there. Do your competitors have the will to use it? Probably.

2. Cell phone interceptions – A common practice in hostile government run counties is to require registration of a SIM card with your passport. Yet even in countries where you have given no such information, monitoring your location, listening to your calls, reading your texts, and browsing your emails is not science fiction anymore. For as little as $300 dollars your competition could purchase cellphone malware which, among other intrusions, could be used to turn on your microphone and listen in to any conversation you may be having on or off the phone. Say, the boardroom?

SECURITY MANAGEMENT INTERNATIONAL, LLC
Intelligent Security Solutions

www.smiconsultancy.com/counter-espionage

3. Hotel intrusions – This includes breaking into a traveler's hotel room for any number of reasons. Once in a room, collectors can download anything from the unencrypted electronic devices we leave lying around the room (think of how often you simply stick your laptop in your suitcase). They can also install listening or imaging devices before or during your stay. A hotel room, hotel safe and hotel lock do not belong to us. The case of ESPN sportscaster Erin Andrews being spied upon and taped using a reverse peephole lens, or the more dramatic instance of the alleged Mossad attack on a Hamas leader in a ritzy Dubai hotel show just how wrong our perceptions of hotel safety can be.

4. Elicitation – When a trained intelligence officer coaxes valuable information out a traveler during casual conversation, it may seem as if you only had an innocuous conversation with a passing stranger. Elicitation may not include the gadgets we have come to expect of spies, but the threat is no less dangerous. Individuals trained to leverage your personality, be it ego, money or ideology, can quickly turn a mid-level employee into a fountain of proprietary information. We only need look so far as Greg Chung's case to see a Boeing engineer turned spy for China. He was not an executive or a high-powered attorney. But he nevertheless managed to leak hundreds of thousands of documents that put China's space program on the map.

5. Physical and Electronic Surveillance – When you combine phone hacking and hotel intrusion, the result is often choreographed surveillance. Surveillance is not just a man in the hotel lobby snapping a picture when you leave though. It is when a traveler's movements are tracked, his conversations monitored and recorded, his routine memorized and his vices documented. In 2009, a British diplomat was filmed in a Ural brothel, allegedly by the FSB. They intended to blackmail him, using the evidence of impropriety as leverage. Even if surveillance does not produce anything worthy of blackmail, knowing your habits, conversations and meetings gives the competition a head start. With miniature cameras so easy to come by, and cabbies eager to make an extra few bucks, is it too James Bond to imagine you may be a target of covert monitoring.

Fortunately, the world is not some giant Quentin Tarantino movie. The threat is real, but it is not all-consuming. There is a way to keep you and your organization's secrets safe.

As a result of long and successful careers in the field of intelligence, augmented by first hand experience traveling to over 120 countries, SMI associates have developed the "Counter-Espionage for Business Traveler's Course" – a first of its kind training program that educates corporate executives to aid them in identifying and protecting themselves from overseas espionage threats. This valuable one and a half day course could save your organization millions.

The only question remains, how long are you going to wait before your company's secrets are no longer secret?

SECURITY MANAGEMENT INTERNATIONAL, LLC
Intelligent Security Solutions

www.smiconsultancy.com/counter-espionage