Foreign Economic Collection and Industrial Espionage Cases Targeting Americans are more Prevalent than Ever

By
Luke Bencie

As today's business environment has become globally interconnected, foreign intelligence activities have extended beyond traditional targets in the U.S. intelligence community and other national security structures. Hostile intelligence services, as well as "private collectors", now target a wide variety of corporate executives, which has compounded the risk of foreign economic collection and industrial espionage like never before.

In previous decades the threat of physical or electronic surveillance from international intelligence services applied primarily to U.S. diplomats or those individuals responsible for transporting R&D materials. In today's world, however, anyone can be a target of foreign collection activities. Of particular interest to foreign "collectors" are American business travelers.

According to the Office of the National Counterintelligence Executive (NCIX), over $300 billion worth of intellectual property is stolen from U.S. companies each year. In many of these cases, the information was extracted while an executive was traveling abroad for business. Furthermore, in most instances, the executive never realized that his or her sensitive materials had been compromised. As such, a recent annual report to Congress on foreign counterintelligence concerns stated, "the United States private sector is seen as an irresistible 'soft target' for foreign intelligence collectors."

The most common methods to obtain sensitive information from travelers are through electronic surveillance and exploitation of laptops/PDAs/cell phones, the use of elicitation techniques by trained intelligence officers against unwitting business people, and surreptitious hotel room intrusions. Bribery, blackmail, sexual entrapment and extortion are also common methods, however those operations expose the espionage intent, thus removing the clandestine aspect of the theft.

According to recent FBI statistics, 23 foreign governments actively target the intellectual property of US corporations, while over 140 countries spend resources to acquire American technology. The top U.S. technologies targeted for theft include aeronautics, information systems, lasers and optics, sensors, marine systems, and electronics. Additionally, ONCIX warns that the rapid expansion of social networking software and virtual world technology offer new venues for making contacts and transferring information.

Economic vs. Industrial Espionage

Before proceeding further, it is important to note the differences between economic and industrial espionage, as both terms are often times mistakenly used interchangeably. The key difference between the two forms of collection methods is that economic espionage involves the assistance of a government intelligence service, while industrial espionage is purely a covert or clandestine collection performed by an industry competitor (that is not to imply, however, that former intelligence officers do not carry out these industrial espionage operations).

It should come as no surprise that countries such as China, Russia, France, Iran, Cuba, Israel, Japan, and India are commonly alleged to have involvement with the theft of valuable U.S. business secrets. Most of the time these countries deny any involvement with economic espionage activities, however on some occasions they are caught "red-handed" or simply boast about their successes. One of the most notable cases (or myths – depending upon who you ask), involved the admission from retired director of the French intelligence service (Direction Generale de la Secuirite Exterierure – DGSE) Pierre Marion. Marion, on more than one occasion confessed publicly to installing audio devices in the business class cabin of Air France flights to listen in on the conversations of American businesspersons.

To justify the action, Marion was quoted as saying:

"This espionage activity is an essential way for France to keep abreast of international commerce and technology. Of course, it was directed against the United States as well as others. You must remember that while we are allies in defense matters, we are also economic competitors in the world."

Despite the French admission, the most immediate threat to American business travelers still remains from China. Businessmen and women traveling to Beijing, Shanghai, Hong Kong and even Taipei need to be especially vigilant, as the likelihood for eavesdropping, intrusion operations, and electronic interception is extremely high. Unlike many other countries, the Chinese recognize the need for all of its citizens to contribute to the foreign collection efforts – almost as a point of patriot duty.

China's pursuit toward modern economic prosperity became evident when during the 1980s President Deng Xiaoping unveiled China's 863 Program. The 863 Program was Xiaoping's personally approved National High-Tech R&D initiative. Per a 2009 interview with China's former Minister of Science, the objective of the 863 Program was as follows:

"…to boost the innovation capability in the high-tech sectors, particularly in strategic high-tech fields, in order to gain a foothold in the world arena; to strive to achieve breakthroughs in key technological fields that concern the national economic lifeline and national security; and to achieve leap-frog development in

key high-tech fields in which Chinas enjoys relative advantages or should take strategic positions…"

In other words, it is the decree of the Chinese government that the theft of foreign economic secrets is an acceptable, and necessary, responsibility of all Chinese citizens. This concept is particularly reinforced to those Chinese who may actively travel abroad and have access to foreign companies and organizations, universities, national laboratories, or tradeshows.

Industrial espionage is equally as prevalent, and problematic, as economic espionage. Although foreign government involvement is not present, the amount of financial damage that can be inflicted upon a company through the loss of a formula, blueprint, methodology, or proposal can cost upwards of hundreds of millions – if note billions - of dollars.

According to ASIS International, Fortune 1000 companies fall prey to industrial espionage attacks on average of 2.5 times per year. The cost alone to secure and investigate these attempted intrusions can range anywhere from the tens of thousands to millions of dollars. Therefore, it is safe to say the problem of both economic and industrial espionage is not going to disappear any time soon.

Conclusion

It should come as no surprise to anyone that a number of nations friendly to the United States continue to engage in economic espionage. Likewise, the on-going threat of industrial espionage from foreign private sector competitors is equally pervasive. With the billions of dollars that are stolen from American businesses each year, the only immediate solution to the problem is to implement effective countermeasures that reinforce strong operational security practices.

Unfortunately, many companies recognize the need for these practices only after their secrets have been stolen and millions of dollars in research and development funds have been lost. Corporations should protect themselves now before their company secrets are no longer secret!

About the Author

Luke Bencie is the President of Security Management International, LLC. He has traveled to over 120 countries for the U.S. Government, as well as the private sector, and frequently lectures on counterintelligence, foreign economic collection, and industrial espionage. His latest book, *Among Enemies: Counter-Espionage for the Business Traveler,* is now available everywhere.