THE FLYNT GROUP INC.

ACTIONABLE KNOWLEDGE ®

Protecting the Crown Jewels:

Information Security for the Business Traveler

FlyntGroup.com

THE FLYNT GROUP INC.
ACTIONABLE KNOWLEDGE®

PO BOX 20111
KANSAS CITY, MO USA 64195
877.FLYNTGP (359.6847)
INFO@FLYNTGROUP.COM
WWW.FLYNTGROUP.COM

Flynt Group White Paper
Protecting the Crown Jewels: Information Security for the Business Traveler

"There are no areas in which one does not employ spies." Sun Tzu

Increasingly, foreign governments and competitors target business travelers to gain important proprietary and confidential information. Information frequently targeted for theft includes business strategies, client lists, product specifications, financial data, and other intellectual property (IP). In cases when a country subsidizes its domestic industries, or if specific technologies are a national intelligence collection focus, intelligence agencies selectively target business travelers.

To remain connected to our organizations, all of us rely on electronic devices, including laptops, smart phones, tokens, and other tools. These communications devices are easily compromised and present an information security vulnerability that may be exploited for economic espionage. Without a comprehensive information security program and adequate training, the use of electronic devices while abroad enhances the likelihood of theft or compromise of critical proprietary information and intellectual property. In some regions, attempted theft of IP is a given.

We hope that this Flynt Group White Paper informs your discussions and planning of a prudent, pragmatic information security program for your organization. Flynt Group has extensive experience in delivering tailored, comprehensive programs, technologies, and training to mitigate the full spectrum of travel-related threats, globally. We can discreetly assist you with managing the risks of present and emerging threats to your intellectual property during business travel, in turn protecting your personnel, assets, information, and operations overseas.

Flynt Group's mission is to equip our clients with *Actionable Knowledge*® to wisely manage their risk positions and achieve their goals across a broad spectrum of hazards and threats. Should we be able to provide any further information, please contact us at 816.243.0044, or via email at Info@FlyntGroup.com.

Sincerely,

Bill Flynt

Bill Flynt, Ph.D., LTC (R)
President
The Flynt Group, Inc.
"Actionable Knowledge"®

The Risk

A component of a company's value is its proprietary information and intellectual property. Whether it is a novel technology or a unique method for delivering a service, intellectual property is a "crown jewel" — something that gives the firm a competitive advantage and that is central to its performance. Theft of the "crown jewels" threatens a company's bottom line, and potentially even its survival.

Globally, many governments and competitors actively seek to identify and illicitly obtain intellectual property (IP) and proprietary information. Illegal competitive intelligence by private firms and hostile intelligence services is a known risk during business travel. This is especially true in emerging economies and in countries where the government subsidizes a particular industry, or, where the government has placed a priority on obtaining certain technologies. Such practices occur in all countries, and are a given in China, India, Russia, Israel, and several others. In March 2012, General Keith B. Alexander, Commander, United States Cyber Command, noted in his testimony before the Senate Armed Services Committee, that "[s]tate-sponsored industrial espionage and theft of intellectual capital now occurs with stunning rapacity and brazenness, and some of that activity links back to foreign intelligence services."[1] General Alexander further commented that private companies were being "looted" by foreign intelligence services.[2] Recent Federal Bureau of Investigation testimony during hearings before the House Committee on Homeland Security, Subcommittee on Counterterrorism and Intelligence, placed the loss to U.S. companies to economic espionage during Fiscal Year 2012 at $13 billion, and growing.[3]

Business travel to countries known for aggressive economic espionage poses increased risk to not only the business traveler, but also to the company and its clients. A well-designed, equipped, and trained information security program greatly enhances protection of a company's "crown jewels" and protects its employees, intellectual property, clients, assets, and operations.

Theft of Mobile Devices and Sensitive Business Information

Mobile devices such as laptops, smart phones, and tablet computers are attractive targets for unethical competitive intelligence, as well as petty criminals. Because of the devices' inherent value and portability, criminals actively target them in airports, hotel rooms and restaurants, as well as on public transportation and the street. Business travelers who fail to exercise precautions risk the devices and the sensitive data they contain—or access remotely—to theft or loss.

Criminal theft is the most common threat to these devices; however, there are other risks as well. Foreign governments and competitors are known to selectively target company representatives to collect sensitive information detailing mergers, acquisitions, programs, research, investment, and other areas.

---

[1] Gertz, B. (2012, March 28). Inside the Ring: Nuclear Risk. *The Washington Times*. Retrieved from http://www.washingtontimes.com/news/2012/mar/28/inside-the-ring-nuclear-risk/?page=2.
[2] *Ibid*.
[3] Dilanian, K. (2012, June 29). Foreign spying against U.S. companies on the rise, FBI says. *Los Angeles Times*. Retrieved from http://articles.latimes.com/2012/jun/29/business/la-fi-economic-espionage-20120629.

With respect to at least one specific threat actor, the depth and breadth of intellectual property theft is staggering. In addition to companies within the defense industrial base, the specified threat actor has aggressively targeted, with military precision: the information technology; manufacturing; petrochemical; and biotechnology sectors, including companies such as Boston Scientific, Abbott Laboratories and Wyeth.[4] Regarding Chinese economic espionage, the security technology company McAfee stated "over the past five to six years [the theft of intellectual property] has been nothing short of a historically unprecedented transfer of wealth—closely guarded national secrets . . . source code, bug databases, email archives, negotiation plans and exploration details . . ., document stores . . . and much more has 'fallen off the truck' of numerous, mostly Western companies and disappeared into the ever-growing archives of dogged adversaries."[5] Regarding the private sector, McAfee issued this particularly dire warning—that the entire top 2000 Fortune firms should be divided into two groups consisting of "those that *know they've been compromised* and those that *don't yet know*."[6]

Small businesses, however, are not immune to economic espionage. Recent analysis by the security technology company Symantec has revealed that 36 percent of all targeted attacks during the first six months of 2012 were directed at businesses with fewer than 250 employees.[7] Symantec cyber security experts warn that "it may be that your company is not the primary target, but an attacker may use your organization as a stepping-stone to attack another company . . . Access to intellectual property and strategic intelligence can give [the foreign intelligence service or competitor] huge advantages in a competitive market."[8] As such, travel overseas by small businesses proffer the same economic espionage threat as those faced by larger enterprises, often without the same internal information security risk mitigation resources. Business travelers are "attack vectors" that threats can use to steal intellectual property.

Theft of information may not involve physical theft of a device. A sophisticated adversary may compromise a device by installing a software application, replacing a component and its firmware, or the addition of a hardware sensor enabling ongoing economic espionage against the victim. This approach offers distinct advantages for the foreign government or competitor. First, it reduces suspicion and the risk of discovery by the business traveler. A sophisticated adversary may not require physical possession of the device to compromise it, and if physical access is required, a foreign intelligence agency or sophisticated competitor requires only a moment with the device to alter it. Second, it provides the threat opportunity for deeper exploitation and collection. In the case of a weak corporate travel security program, there is the high likelihood that the device will be connected to the company's network after completion of travel; this is especially true if the device is a dedicated employee laptop. Once connected, the malware can infiltrate and map the company's network, equipping the adversary with wide latitude to steal large amounts of sensitive,

[4] Hytha, M. (2011, December 11). China-Based Hacking of 760 Companies Shows Cyber Cold War. *Bloomberg Businessweek*. Retrieved from http://news.businessweek.com/article.asp?documentKey=1377-aNCSG7At.q8w-653I7S7OCHT5CHS02QEIPS8J4A.
[5] Alperovitch, Dmitri, Vice President, Threat Research, McAfee. (2011). *Revealed: Operation Shady RAT* [White Paper]. Retrieved from http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf.
[6] *Ibid* (emphasis original).
[7] Help Net Security. (2012, Jully 11). *Targeted attacks focus on small businesses*. Retrieved from http://www.net-security.org/secworld.php?id=13225&utm.
[8] *Ibid*.

proprietary information. Another technique is to install malware on a traveling employee's device by transferring files using USB drives during project team collaboration, giving a USB drive as a gift, phishing emails, and numerous other attacks.

Information Security Best Practices

A comprehensive, tailored corporate travel security program is a best practice in mitigating the theft of intellectual property. At the user level, many protective measures should be applied to assist in maintaining information security while traveling, including: locking the device when not in use; requiring a strong password for each application; limiting mobile device access to sensitive information (e.g., limiting access to the company email and networks); limiting data on the device to only that essential to support productivity during travel; use of disposable phones; ensuring antivirus and malware detection applications are updated prior to travel; immediate wiping of computers on return from abroad; and, other associated actions to prevent compromise. Dedicated, non-production devices should be used for all foreign travel, especially to those countries known for economic espionage. These devices should never be connected to any company production network, and should only have the applications essential to support productivity during travel. If not feasible to dedicate devices solely for travel, then following travel all devices must be inspected for both physical and cyber tampering or modification, and sanitized by cyber security personnel. Additionally, all storage media (e.g., USB drives, SD cards) should similarly be dedicated to travel support and wiped clean on return from travel.

The use of strong encryption and two-factor authentication are essential practices for protection of sensitive or proprietary information. Whole disk encryption, without a boot circumvention option, is a best practice and data should be encrypted at rest, in use, and in transit.

Device accountability and protection is critical. Business travelers must ensure they keep computers, smart phones and other electronic data and communications devices as carry-on baggage when traveling and on their person in-country. Travelers should never check these devices with other luggage and should protect any portable storage media. Smart phones should have their batteries and SIM cards removed, and only enabled during specified communication windows. Use of secured communications equipment (e.g., encrypted satellite communications) to discuss sensitive business matters such as mergers is a best practice and readily available as a commercial solution, however travelers should confirm before travel with their Chief Security Officer that such equipment is permissible to travel to, possess, and use in that region and/or country.

Travelers should be aware that foreign customs officers' requests to examine a laptop computer or other electronic communications device outside the control or sight of the traveler are often an attempt to compromise the device. If unavoidable, the device should be assumed to be compromised. Devices should be kept close to the traveler at all times and never loaned for another's use, set anywhere a street criminal could easily grab it, or left where hotel staff could access it. In all cases, if a device leaves the traveler's direct control for any period, especially in countries known for aggressive economic espionage, the traveler and the company should assume the device and its information are compromised.

Hotel staff provides foreign intelligence services and competitors the opportunity to collect sensitive information. Countries known for aggressive economic espionage have hotel staff members acting as their agents. Business travelers should accept as a given that their hotel rooms will be entered, searched, and seeded with both hidden microphones and video cameras. Similarly, hotel networks and Internet services should be considered as monitored; travelers should use alternative, less-easily compromised arrangements for Internet access (e.g., a portable satellite terminal). Travelers should never use a computer or facsimile machine at a foreign hotel or business center for transmitting sensitive information. Sensitive papers and notebooks should be protected using similar practices as for electronic devices.

Wireless devices are especially vulnerable to collection activities, and can be used to track the traveler's movement within the country. Device microphones, cameras, and GPS services can be remotely activated without the traveler's knowledge or indication on the device.

Use of electronic devices during travel—both overseas and domestic—presents risks. In most countries, the traveler should not have any expectation of privacy in Internet cafes, hotels, client offices or other uncontrolled spaces; travelers must be aware that foreign telecommunications systems and hospitality service industries (e.g., hotels, limousine services) frequently cooperate with their country's intelligence or security service. Monitoring of business travelers by foreign intelligence services is routine and transmitting sensitive information from overseas locations poses significant risks to the traveler and the enterprise.

Conclusion

Overseas business travel is essential in the global marketplace. However, companies and their traveling personnel should be aware and alert to the risks of economic espionage by foreign countries and competitors. To mitigate these risks, a comprehensive travel security program is critical to the protection of sensitive or intellectual property—a corporation's crown jewels.

Flynt Group consultants listen carefully to ensure alignment with your specific objectives and then deliver tailored, full-spectrum travel security packages, technologies, services, and training programs. From *Street to Boardroom, Globally*®, the intensity of our focus on our clients' interests and the uncompromising quality of our consulting drives our operations. We understand that we must earn and protect our clients' trust. We do it every day.

Integrity is our code. Our discretion is absolute.