

North Carolina Law Life

NC: Cutting Edge R&D and Cutting Edge Corporate Espionage

By: Donna Ray Berkelhammer. Monday, May 14th, 2012

The **Federal Bureau of Investigation** estimates that corporate espionage has cost American companies \$13 billion from trade secrets stolen by company insiders and given to hostile foreign governments.

To combat this growing threat, largely sponsored by China, the FBI is starting an economic



espionage awareness campaign in key hot spots to educate American workers about corporate espionage and suspicious behavior. Initial campaigns will start in areas with high concentrations of government contractors, including Chicago, San Francisco, Los Angeles and **North Carolina**.

According to the latest economic espionage report to Congress from the Office of the National Counterintelligence Executive, foreign collectors are most interested in the following areas:

- Information and communications technology, which form the backbone of nearly every other technology;
- Business information that pertains to supplies of scarce natural resources or that provides global actors an edge in negotiations with U.S. businesses or the U.S. government;
- Military technologies, particularly marine systems, unmanned aerial vehicles, and other aerospace/aeronautic technologies; and
- Civilian and dual-use technologies in fast-growing sectors like clean energy, health care/pharmaceuticals, and agricultural technology.

Much of this information is easily available and can be taken on flash drives, cell phones or other small devices by greedy, disgruntled, unhappy or financially needy employees, as well as people who are vulnerable to blackmail or have allegiances to other countries.

http://www.nclawlife.com/

<u>Richmond</u> • <u>Christiansburg</u> • <u>Fredericksburg</u> • <u>Research Triangle</u> • <u>Mclean</u>

Copyright Sands Anderson PC

Certain corporate policies and procedures governing access to sensitive documents can help, but the FBI is highlighting suspicious activities and providing a hotline for reporting:

You can help as well. In our experience, those who purloin trade secrets and other sensitive information from their own companies and sell them overseas exhibit certain behaviors that coworkers could have picked up on ahead of time, possibly preventing the information breaches in the first place. Many co-workers came forward only after the criminal was arrested. Had they reported those suspicions earlier, the company's secrets may have been kept safe.

Here are some warning signs that MAY indicate that employees are spying and/or stealing secrets from their company:

- They work odd hours without authorization.
- Without need or authorization, they take proprietary or other information home in hard copy form and/or on thumb drives, computer disks, or e-mail.
- They unnecessarily copy material, especially if it's proprietary or classified.
- They disregard company policies about installing personal software or hardware, accessing restricted websites, conducting unauthorized searches, or downloading confidential material.
- They take short trips to foreign countries for unexplained reasons.
- They engage in suspicious personal contacts with competitors, business partners, or other unauthorized individuals.
- They buy things they can't afford.
- They are overwhelmed by life crises or career disappointments.
- They are concerned about being investigated, leaving traps to detect searches of their home or office or looking for listening devices or cameras.

If you suspect someone in your office may be committing economic espionage, report it to your corporate security officer and to your **local** FBI office (704.672.6100) or submit a tip online at https://tips.fbi.gov/.

If you want help setting up corporate policies to help protect trade secrets, contact one of our **business attorneys**.

http://www.nclawlife.com/

Richmond • Christiansburg • Fredericksburg • Research Triangle • Mclean

Copyright Sands Anderson PC