the Atlantic

Ben W. Heineman Jr. - Ben Heineman Jr. has held top positions in government, law and business. He is the author of *High Performance with High Integrity* (Harvard Business Press, 2008).

The Very Real Danger Beyond Cyberhackers: Inside Leaks

By Ben W. Heineman Jr.

January 10, 2011

Inside employees stealing valuable secret information are still a great threat to governments and corporations.

This age-old problem was brought home by the above-the-fold news that three senior managers at Renault in France had been suspended without pay for allegedly disclosing secrets about electric car technology to improper parties. ("Spying Probe Centers on Electric Cars," *Wall Street Journal*, January 7, 2011.)

Even in this computer age, real people inside real institutions do not need sophisticated computer techniques to steal real, important secrets.

Even in this computer age, real people inside real institutions do not need sophisticated computer techniques to steal real, important secrets.

This may also be the case in the recent WikiLeaks furor where an army private, in essence, allegedly stole information (the cables) to which he had legitimate access in order to transmit it improperly to others outside government.

These cases raise different issues than those posed by "cybersecurity," a concept which has, of course, been accorded great attention in our wired era. In lay terms, the concept primarily means developing defenses against attacks by outsiders against an organization's computer systems for such malignant purposes as theft or destruction. Virtually every major government, every major corporation and every major university have programs exploring the meaning and methods of this "new, new thing." And well they should. The capacity of a cyber attack to cripple essential services -- electricity,

transportation, financial transactions, military operations -- or purloin highly valuable technology is clearly a threat of the first order.

Yet, as a society, we must still pay serious attention to theft the traditional way: from the inside by current or exiting employees whose motives may include money or revenge.

A few recent cases:

- A former Boeing engineer was sentenced last February to 16 years in prison for stealing trade secrets relating to rockets for use by the Chinese.
- A former DuPont engineering employee was sentenced in March 2010 to 18 months in prison for stealing information to a Korean company.
- Three former Starwood Hotel executives stole confidential documents on a "life-style" hotel concept which they took to Hilton. This led to a court settlement last December that includes a substantial (undisclosed) payment by Hilton and an order enjoining Hilton for entering this line of business for two years. A New York grand jury is still evaluating whether a crime was committed.
- A Dow Chemical scientist was charged last year with economic espionage for China under a statute passed in 1996 to address the growing problem of commercial theft in a highly competitive global economy.

This threat of inside theft is especially salient at a time of accelerating technological competition among commercial entities in both developed and developing markets. Although the information may be private, the implications for national security and foreign policy may still be significant as economic growth and technological advancement are core national interests of most countries.

And major corporations do expend significant resources on cybersecurity (although there is still much to be done) and on the historic task of making sure that proprietary information is not disclosed to outsiders in more conventional settings. But unless they have sensitive technology that is part of a formal classified military program, companies rarely can afford detailed security checks on potential employees at the hiring stage. Nor at the time of promotion into sensitive positions, do they usually explore the risk of theft. And, when employees exit, it can be very difficult to ensure that they have not secreted away important information properly lodged on their computers in the past for future improper use.

The Renault and WikiLeaks cases remind us that, even in this computer age, real people inside real institutions have quotidian access to real information and do not need sophisticated computer techniques to steal real, important secrets. The Economic Espionage Act of 1996 gives federal prosecutors the means to attack these insider

thefts, and the head of the Criminal Division has said this should be a DoJ priority. So, too, corporate programs relating to their own employees need to be reevaluated in light of new global competitive realities.

In short, the effort on cybersecurity against outside attackers needs to be matched by efforts in preventing theft by insiders the old-fashioned way.

###