WikiLeaks Breach: Lessons Learned Regarding Trade Secret Theft

Insights
11.29.10

If the recent WikiLeaks release of more than a quarter-million sensitive files is not a wake-up call to companies about the need to proactively protect confidential information, nothing is. The lesson is clear. When it comes to protecting trade secrets, preventative measures are as important, if not more important, than remedial measures.

If you have not followed the details of the Wikileaks breach, the basic facts are these. Bradley Manning, a young Army Pfc., is accused of stealing hundreds of thousands of classified diplomatic files and memos and feeding them to WikiLeaks, a website known for publishing anonymous submissions of sensitive data while attempting to preserve the anonymity of its contributors.

According to Manning, his theft of documents was simple: "I would come in with music on a CD-RW labelled with something like Lady Gaga... erase the music... then write a compressed split file." Hiding his conduct was not difficult either. "No one suspected a thing. [I] listened and lip-synched to Lady Gaga's Telephone while 'exfiltrating' possibly the largest data spillage in America history."

With U.S. diplomats scrambling to mend fences worldwide as a result of the countless disclosures, the Pentagon announced that it has enacted new security measures to prevent others from inflicting similar damage with little more than a portable computer memory stick. According to the Pentagon, it has ordered the deactivation of the "write" capability on all computers on the defense department's classified network and limited the number of computers that can be used to transfer data from the secret domain into the open. The new protocol requires that two people be involved in any such transfer to ensure it is properly authorized.

The Pentagon has also required the development of "procedures to monitor and detect suspicious, unusual or anomalous user behavior." This includes an accelerated installation of monitoring software on all secure computers, many of which do not currently have such software. While these measures are a good start, it is surprising that the United States government was not a little further along the curve when it came to preventing the misappropriation of classified information. Companies should take heed. A trade secret lost is forever lost.

Pfc. Manning summed up the flaws that enabled him to carry out his theft: "Weak servers, weak logging, weak physical security, weak counterintelligence, inattentive signal analysis.... A perfect storm." The bottom line – don't leave yourself vulnerable to the whim of a disgruntled employee.

Michael R. Greco is a partner in the Employee Defection & Trade Secrets Practice Group at Fisher Phillips. To receive notice of future blog posts either follow Michael R. Greco on Twitter or subscribe to this blog's RSS feed.

Related People

Michael R. Greco
Regional Managing Partner
303.218.3655
Email