THE WALL STREET JOURNAL.
WSJ.com

September 24, 2014, 11:47 AM ET

What Business Can Learn From Intelligence

ByThomas H. Davenport

I just read the interesting story about Edward Snowden in Wired, and I can't quite figure out what I think of the man. He seems neither the patriot that James Bamford (not surprising, given his background) portrays him to be, nor the traitor that some argue. The story certainly nourishes the increasing concern that the U.S. spies on its own citizens and national allies. And there is little doubt after reading it that a disgruntled employee (or contractor) can walk out an intelligence agency's door with a "pocket full of thumb drives."

However, there is little doubt that the intelligence sector in the U.S. (including the Central Intelligence Agency, the National Security Agency, parts of the Federal Bureau of Investigation, Homeland Security, and many other agencies) and elsewhere is quite accomplished at several aspects of data management and analytics. It's also clear that businesses can learn from these organizations in several respects. Below are a few lessons from which business leaders could draw.

Focus on intelligence about the external environment. Just the notion of gathering and analyzing "intelligence" is something businesses could emulate. Some businesses have competitive or customer intelligence operations, but most firms lack a systematic approach to learning about important aspects of the external environment. In most organizations there is no role that is responsible for making managers aware of intelligence that may affect the business. No one would argue that intelligence isn't important for a country, but for some reason its importance has not been realized in the business sector.

Use "sigint" as well as "humint." The intelligence sector has historically made use of "sigint," or signals intelligence deriving from electronic communications interception, and "humint," or human intelligence from human analysts in the field or at headquarters. Recently, sigint has been somewhat more of a focus. However, organizations like the CIA and the FBI still maintain human-staffed listening posts in the field, and all intelligence agencies rely in part on human analysts to make sense of intelligence. Companies should also make use of both electronic and human intelligence sources; the intelligence-gathering and analyzing function will not be fully automated anytime soon. If you want to know about your customers, for example, you should examine their online behaviors, but also talk to them, and to your salespeople about them.

Invest in technical infrastructure. Signals processing in the intelligence sector has been facilitated by extensive investment in technical infrastructure. Recently, for example, the NSA constructed a massive data center in Utah on behalf of the entire intelligence community. Prior to this, it began construction on a $1B supercomputer data center at its Ft. Meade, Maryland headquarters. The NSA is reputed to harness more computer MIPS (millions of instructions per

second) in its machines than any other organization on earth. Intelligence agencies have long worked on building broad capabilities and infrastructure for intelligence gathering and analysis, and firms should do likewise.

Try to eliminate silos. One of the problems that plagued the U.S. intelligence sector in the past was fragmented silos that prevented information sharing. It is well-known, for example, that some agencies were aware of some activities by the 9/11 terrorists, but the intelligence wasn't shared widely. Since that time, the U.S .has established the Office of the Director of National Intelligence (ODNI), a role and organization that is attempting to break down barriers to sharing intelligence. The ODNI has made some progress in this regard, creating tools like Intellipedia (a Wikipedia-like system) to share intelligence across agencies. As of January 2014, the "Top Secret" layer of Intellipedia had 113,000 content pages with 255,000 users. Businesses also have data and analytical silos, and should work toward bridging them with new organizational structures and other means.

Identify the key entities on which you want to collect intelligence. The U.S. intelligence sector has developed a series of lists of entities on which it collects intelligence. They include terrorists (in the Terrorist Identities Datamart Environment, or TIDE, the consolidated Terrorist Watchlist, and the Secure Flight air passenger system), suspicious activities, terrorist organizations, and countries. It's important to decide in advance what entities are worthy of your intelligence-gathering. In business, this might include competitors, key customers, partners, and even potential hires.

Work closely with your ecosystem partners, but monitor security. The intelligence sector is quick to embrace new partners for software, services, and other external capabilities. In Israel, for example, some of the leading commercial tools for voice analysis were developed in conjunction with the Israeli intelligence sector. In the U.S., companies like Palantir, Recorded Future, Endeca, Attensity, and many others were engaged by intelligence agencies. The CIA even has a venture capital arm, In-Q-Tel, to invest in firms that provide useful tools and services for the intelligence sector. Of course, Edward Snowden worked for intelligence contractor Booz Allen Hamilton when he took intelligence documents from the government, so security is obviously paramount in working with external vendors. There are just as many high-value ecosystem partners for businesses, and the same rules of cooperation and security apply.

The comparison between corporate business intelligence and national intelligence is apt not only because they share part of their names. Business intelligence in companies has typically been quite narrow and limited with respect to data types and topics. Adopting some of the approaches used by the intelligence sector could make companies much more aware of important activities in their external environments.

Thomas H. Davenport is a Distinguished Professor at Babson College, a Research Fellow at the Center for Digital Business, Director of Research at the International Institute for Analytics, and a Senior Advisor to Deloitte Analytics.