



Illustration by Stephanie Dalton Cowan

ANALYTICS FOR EVERYONE

November 2014 Print Issue

By Mark Tarallo

It's ubiquitous. From targeted ads on Facebook to customer loyalty cards to Gmail cookies, companies are hungry for information about you. Business intelligence—the gathering and analyzing of information for purposes of commerce—is rapidly advancing, on several fronts, not least in security. The amount of information available to organizations and employees is ever increasing. Big Data keeps getting bigger, analytical methods grow more and more sophisticated, and the number of tools available to extract meaning from that information multiply.

The most prevalent trend in business intelligence, some experts say, is the democratization of data crunching. The use of sophisticated analytical tools is no longer the exclusive province of one or two specialized analysts in the organization. Instead, these tools are being made available to employees on the front lines, whether they be members of a sales team or security officers working at a remote location. Mobile applications and cloud computing are making access to these tools easier.

Here, Security Management takes a look at few examples of cutting-edge business intelligence practices and how they apply to security, such as a solution derived from creative analysis of social media data and the mobile use of integrated analytics for crisis management situations. We then look at the big picture and survey some broader trends in business intelligence and their relationship to security, and take a peek at a few challenges the future may hold.

Social Media

Social media monitoring is becoming a popular practice in the business community. Whether it be for a reputation management program or for obtaining feedback on a particular service or product, more organizations are monitoring channels like Twitter and Facebook.

For example, international security expert Hart Brown has developed a business intelligence tool that goes beyond monitoring. Brown, who sits on the ASIS International Crisis Management and Business Continuity Council, is an intelligence veteran who has worked at both the U.S. Department of Defense and the U.S. State Department. A few years ago, Brown was international security manager for a company that was highly active in various regions of Mexico. Given its engagement, the firm needed timely news coverage of all the regional markets in Mexico that it was involved in.

But this proved hard to come by. In regions outside of major cities, there was often sparse coverage; CNN-type breaking news reports did not exist. And sometimes, when sufficient media were present, news agencies were pressured by criminal cartels not to report certain

developments. "In that country, news is very complicated, and in many cases censored," Brown says. "We just could not get reliable information about what was going on." Twitter, however, had the reach that traditional media did not.

As Brown describes it, he was in need of a system that would accomplish two main objectives. First, he needed an early warning or alert system that the stability of a particular town or region was being threatened. Be it a fire, earthquake, gunfight, kidnapping, or some other event, he wanted to know as soon as the incident started happening.

Second, he wanted to be able to gauge the event's severity—specifically, how disruptive it would be, and whether its impact was increasing or diminishing over time. This included an ability to assess how much stability had returned the day after an event, which would help the company decide if it had to alter its operations on the ground. A straightforward social media monitoring system would not be sufficient to achieve these two objectives, according to Hart: "It certainly wasn't enough for me. We had to put some analytics to it," he says.

So Brown built a solution through the use of Netvibes, a program popular in the advertising and marketing fields for social media and news tracking. First, he had to ensure that he knew the language spoken by the local community. Whatever the event, he learned the various phrasings used to describe it, including colloquialisms that locals might use on Twitter. He did this by combing through volumes of reports of traditional media and identifying keywords to use in the algorithm.

He then established baselines for the keywords, which represented how many times they would occur in normal everyday Twitter discourse. Brown could then measure the rate of change when an event occurred and usage of the keyword shot up. For example, on a normal day without incident, the Spanish word for gunfight may occur 10 times—in innocent contexts, such as in a movie description. When a real gunfight occurs, the usage number may spike to 100, or a rate of change of 10 times the baseline.

Brown arranged for the system to send out an e-mail alert when the spike reached a certain level—signifying a noteworthy event was under way. Typically, such an alert would go out less than hour after the actual start of the event—a testament to the real-time power of Twitter.

Once the tool saw frequent use, it became evident that the steepness in the keyword usage spike correlated to the severity of the incident in

question. For example, in April, the city of Tampico “turned into a war zone” due to violence from drug cartels and gangs. “We were able to see the war was starting within an hour,” Brown says. The spike was roughly 40 times above the normality baseline, and from that steep spike Brown could tell that the local reaction was serious enough to drive many residents and businesses into lockdown mode. “As far as the initial shock—there’s absolutely a correlation,” Brown says.

The correlation is so solid that it helps Brown make real-life operations decisions. For example, after one violent event, Brown was unsure whether the company’s equipment trucks could drive through the area. Brown gauged the level of chatter, and made the assessment: “There’s a lot of checkpoints and it’s going to be slow, but there’s not violence.” The trucks were sent forward; the assessment held true.

Crisis Intelligence

Brown’s intelligence tool, in essence, uses social media data to analyze the extent of an event’s destabilizing force. Some businesses, however, use intelligence tools that deploy analytics on the fly, and in equally challenging situations.

Imagine, for example, that you are a chief of security for a large company that has a strong presence in Colombia. There is an earthquake in Bogota, where your company has several offices and many employees. The city is engulfed in chaos, and your employees have no idea who might be affected, or if anyone is in distress and needs assistance.

Such a situation demands a rapid analysis of all available information, so that some sort of response can be taken. However, “you can’t act if you don’t have good information, and you don’t know where your people are,” says Dan Richards, CEO of Global Rescue, an emergency evacuation and field rescue firm.

During these challenging situations, some firms use a type of business intelligence tool that consolidates different platforms within crisis management and response environments into a mobile application, Richards says. These types of systems combine and correlate different data sets, such as the firm’s enterprise footprint and the parameters of the event, to give each user a quick and clear picture of where employees and assets are and what areas of the city have been affected.

These tools also integrate with a communication component that allows for messages to be sent to selected employees or to everyone. The system tracks who received and replied to messages and who did not, analyzes this information, and then continually updates each employee’s status.

“When you look at any major crisis when there’s a lot of people involved, a lot of time is wasted in trying to confirm that people who may be in distress are actually hurt,” Richards says. The system also keeps track of all operational responses that the company has taken in real time and automatically informs employees who need to know such updates.

In addition, these systems can be set up to periodically ping a staffer’s smartphone, so that the return ping “leaves a breadcrumb trail” as to the employee’s location, Richards says. In this way, if an event like an earthquake or flood disables a staffer’s device, the last location before the device stopped working can be ascertained.

In Richard’s view, the use of such business intelligence systems for crisis management is growing, in part because “there’s relatively lean staffing in security.” A company of 10,000 employees, for example, may have only six crisis management executives. “That’s not an advantageous ratio,” Richards says. “You need to have a set of tools that will be extraordinarily effective.”

Data Analysis

A tool such as the one Richards describes, which tracks the whereabouts and status of employees in the field, may also be used in noncrisis situations by a company with a highly mobile work force. “With more people working at home, and off site, keeping track of this decentralized work force has become an increasing challenge,” Richards says.

But whether it is used in chaotic or calm times, it can be used by any employee who needs to know the status of workers in the field. And that’s reflective of a current trend discussed in a report, *The Top Ten Business Intelligence Trends for 2014*, recently issued by Tableau Software.

The report finds that the practice of data science is moving from the high-level specialist to the employee in the business community. Data analysis is becoming part of the skill set of ordinary business users, not just a few experts. “We’re starting to see a mass adoption of data tools,” says Ellie Fields, a vice president at Tableau, which specializes in business intelligence.

Part of this trend is what Fields calls “embedded analytics.” More firms are making analytical tools available to employees on the front lines, such as members of a traveling sales force or security guards patrolling a site. By way of explanation, Fields offers a hypothetical scenario: “Wouldn’t it be great if security guards knew that between 1 and 3 is the time when most threats happen, and that they usually happen on this side of the perimeter?”

And that security officer who uses a mobile application for a crime data analysis may also be representative of another business intelligence trend—the increased use of predictive analytics. “We’re collecting data on things we didn’t used to have,” Fields says, and that means there is more raw material to analyze and construct sophisticated performance prediction models. “Now people are saying, ‘Let’s see if we can predict when we will have machine failure, based on past results,’” she says.

The increased use of business analytical tools has intersected with the rise of cloud computing, and this combination has spawned another recent trend: cloud analytics. So far, this has not occurred on a wide scale, as some organizations still have security concerns about moving sensitive data to the cloud. “I don’t think the three-letter agencies are adopting the cloud anytime soon,” Fields says.

But other organizations have become comfortable with cloud security and have embraced the concept. Cloud storage can make data access from mobile devices easier; the same advantages apply to analytical programs in the cloud, which can be accessed from mobile devices, like an iPad, and make for more agile, self-serve intelligence, Fields explains.

Big Data

Overload is not the only challenge when it comes to the advance of business intelligence and the growing reliance on Big Data. The increased use of intelligence tools will likely also increase privacy concerns. Take, for example, the crisis intelligence tool that pings smartphones to track the recipient’s whereabouts. Such knowledge could be abused. “Some humans don’t want to be found,” Richards says. “As a society, we will have to grapple with those issues.”

Data collection itself, even for business purposes, can also be viewed as intrusive. To take just one example, Amazon is now offering brick-and-mortar stores a payment-processing device, called Local Register, which will allow the online giant to track a consumer’s offline purchases. Such technologies will spur more discussion about letting people opt out of some data collection processes.

Moreover, while business intelligence tools are indeed becoming much more common, the skills needed to use those tools to best advantage are less widespread, Brown says.

This is particularly true for analytic tools that require queries to obtain information. “Everyone wants a piece of the Big Data scene, but what you find is that it becomes very, very complicated and the queries that you are using become very sensitive,” Brown says. “We have a lot of people using analytics that may not really understand what it is they are querying. Every minor change in the query can have a significant impact on findings,” Brown said.

Overall, the proper use of intelligence tools is an “art meets science” proposition, and collectively the business community “still has a ways to go” before analytical data skills become commonplace among company staff, Brown says. “I don’t think we’ve reached the point now where we can fully migrate from analysts.”