THE WALL STREET JOURNAL.
WSJ.com

January 7, 2015, 11:03 AM ET

An Optimistic Lens on Cybersecurity

By Thomas H. Davenport

Welcome to my first guest column of 2015, in which I will try to inspire some optimism. Fortunately, there are many signs that the world is getting better from an informational standpoint. Not only is there Big Data, but also much more interest in and availability of external data, more focus on information that provides context, and more desire for predictive analysis. Being broader in our information focus, trying to turn data into insight, and anticipating events rather than simply responding to them—all these orientations are making both companies and the world at large better places to work and live.

The most recent example of these trends I have noticed is in cybersecurity. We all know by now that 2014 was the first time that cybersecurity became an issue of extreme importance to many organizations. It was the year that Target Corp.'s CEO resigned in part because of its customer data breach in the previous year. We also became aware of new breaches at UPS, The Home Depot, Morgan Stanley, JPMorgan Chase & Co., AOL, Gmail, eBay Inc., and of course Sony Pictures Entertainment. It was, I believe, the first time the data breach topic has come into serious focus by a U.S. president—in his end-of-year remarks on Sony Pictures, in the breach of White House data, and perhaps also in the rumored breach of President Obama's own credit card data from JPMorgan Chase. So cybersecurity has everybody's attention.

Thus far, however, it's primarily been a lot of retrospective attention. There's a breach or a hack and everyone scrambles to find the problem. Of course, that's usually too late to do much about it. So the trend in cybersecurity is to try to predict, anticipate, understand context. As one manager I interviewed put it, "People are tired of showing up after the damage is done."

How do you anticipate cybersecurity threats when they can come from virtually anywhere? I suppose you could get really good at typing "POS malware directed at US retailers" (or whatever your location and industry are) into Google, but that could become a little tedious. There are more systematic ways to assess threat intelligence, such as those provided by the company Recorded Future.

I knew about this company from its founding in 2008 in my Cambridge, Mass. hometown. It was created by Christopher Ahlberg, a smart and enterprising Swede who had previously founded Spotfire, a visual analytics software company eventually acquired by Tibco. Recorded Future (RF) analyzes Internet data to see what the world is saying about certain topics. Given Mr. Ahlberg's visually-oriented academic and business background, it's not surprising that the outputs of RF are displayed in visually attractive dashboards.

A couple of years ago I wrote a case study about RF, but at the time it was a little unclear what its niche was. Some big companies were using it for marketing and physical security purposes, a few hedge funds were scouting investment opportunities and risks, and the bulk of the company's customers were government intelligence agencies. Of course all of those industries can benefit from learning more about current and future issues on the Internet, but other in than the intelligence agencies, there wasn't a pressing need.

The fastest-growing application for RF now, however, is cybersecurity. The need is obvious, and many companies are interested in becoming much more proactive and anticipatory about threat intelligence. One financial services firm's cybersecurity director told me:

We are increasingly looking outside our enterprise and attempting to be more predictive about threats. With tools like Recorded Future we can assess huge swaths of behavior at a high level across the network and surface things that are very pertinent to your interests or business activities across the globe. Cybersecurity is about predicting and understanding human behavior, and much of that is previewed on IRC channels, social media postings, and so on.

This company is also increasingly using RF to create partnerships with its physical security organization. The cyber director commented that increasingly he is asked to check the RF dashboard for threats and protests in countries where employees are traveling. Physical travel and cybersecurity are increasingly intertwined anyway, as is the case with "Dark Hotel" malware at business hotels in the Asia-Pacific region (which I learned about through an RF blog post).

Another cybersecurity professional, Dave Ockwell-Jenner at the aviation technology and services firm SITA, says that RF has alerted them to at least two important events in the few months they have been using it. One involved a data breach at an air travel industry organization in which SITA participates, and SITA was able to wall off that entry into their domain. Another involved a breach of credentials at an airline customer and partner of SITA, and SITA was able to notify the airline before they knew of it otherwise—certainly a value-added service to a customer.

Mr. Ockwell-Jenner notes that RF's detailed work on names and taxonomies is a key part of its value. "You wouldn't believe how many organizations are named SITA," he said. It saves a lot of time for the company SITA not to have to sift through threats aimed at the South India Term Abroad organization, for example.

The bad news of 2014 seemed to be that the bad guys of cybersecurity were winning. The good news of 2015 is that there are tools like Recorded Future's that can help the good guys identify the bad guys and their tricks before they succeed.

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.