Data Will Be Essential to Agencies' Missions in 2020

Government and industry leaders predict 'the rise of the CDO' and more.

James Mersol

Mon, 01/06/2020 - 09:36

Photo Credit: Olivier Le Moal/istock

In 2020, data will become even more crucial to IT and digital services, serving as the foundation of automation and future innovation.

Government leaders at the AI and RPA CXO Tech Forum highlighted how data will drive innovation and empower other technologies, including blockchain and virtual reality. With innovation comes security, as data becomes a threat vector in addition to the foundation of modernization.

GSA CDO Kris Rowley explained how he views his role in the agency, which is working on a number of initiatives to harness the power of its data.

“I have to flow throughout the organization,” Rowley said. “I have to coalesce leadership around common problems, common priorities, common theories.”

In industry, some predictions for data in 2020 stem from emerging trends in 2019. Data will be the "fuel for IT modernization," said Splunk Vice President for Public Sector Frank Dimina. These predictions tie in with emerging trends in 2019, with the opportunities and ways to mitigate risk growing stronger in the new year.

2020 is expected to bring the rise of the chief data officer in government. The CDO role will become crucial for federal IT, not only because every agency is federally mandated to have one, but also because agencies will recognize the role in connecting complex datasets to the agency’s mission and in breaking down silos to do so.

Cybersecurity will also continue to be a priority in 2020, especially as data becomes all the more critical. Dimina’s second prediction for 2020 trends is that “AI and machine learning become a target,” and attackers may attempt to corrupt or poison the data underlying these technologies. With this new threat vector, the triad of attacks on data will be complete: leaks affect the confidentiality of data, ransomware affects the availability of data, and poisoning affects the integrity of data.

While the implications of this prediction are dire, those working with data understand the importance of a proactive defense against these attacks and are planning defenses now.

“The issue for a baseline for security is, ‘Is the enemy already in the baseline?’ and you baseline the enemy into your system,” Air Force CTO Frank Konieczny said at an AI conference in December. “It’s a question that you have to ask.”

Konieczny did not share what solutions the Air Force is implementing — the details of defensive measures are rarely made public — but did say that questions like this are also informing where the Air Force implements AI and machine learning to minimize risk and maximize its potential as a force multiplier.

“Blockchain is going to leave bitcoin behind,” Dimina said in another prediction. Blockchain already has several applications beyond cryptocurrency, but in 2020 those applications will become well known and widespread enough to quell misunderstandings and myths about the technology.

In December, HHS Senior Advisor to the CIO Oki Mek, one of the biggest proponents of blockchain in government, suggested the technology is a way to protect patient data and enable automation to categorize large datasets.

“We need machine learning not only to make sense of the data, but to categorize datasets as well. That’s why I say blockchain is key,” Mek said. “I think blockchain is the missing link to the internet.”

In a CyberCast interview, Mek further discussed blockchain and its applications both in data protection and in reducing the amount of time and paperwork in the acquisition process. He anticipates that automating the authority to operate (ATO) process will drastically shorten the time it takes to evaluate risk while simultaneously improving the level of transparency in the process.

As the Department of Veterans Affairs is strategizing, augmented reality and virtual reality will move beyond their current use in the gaming industry to find broader application across IT. CISA CTO Brian Gattoni predicted that AR will be an important component of both physical security and cybersecurity in April.

“Where [physical and cybersecurity] converge, it’s important to understand how a cyber event can cause a kinetic effect,” he said. “How do we … advise [a] national-level event or that national critical function of our view of risk because I have a human on the ground and the entire power of big data in [their] hands to do real-time risk analysis?”

Gattoni suggested AR could be used to image a security office or server room ahead of a major even, like the Super Bowl, and then compare against that location on the day of the event to see what has changed, both physically in the room and on the systems in that room.

At the same event, Jeremy Wiltz, assistant director of the FBI’s enterprise services division said that AR and VR simulations also have applications for training. While cybersecurity professionals already have playbooks for what to do in the instance of a breach or other incident, simulated exercises could instill literal muscle memory in a way that a paper exercise cannot.

Splunk's Dimina illustrated a third example where electric car technicians can use AR to guide charging station installations as a real-time instruction manual. The use case, demonstrated at Splunk’s .conf19 in October, will be a springboard toward on-the-job training, bringing data literacy to those who are not trained data scientists.

2020 will see greater “consumerization” of data, Dimina said.

View printer friendly version
data
blockchain
data protection
artificial intelligence
augmented reality
virtual reality
Standard