October 26, 2015

How to move beyond 'moats and castles' in cyber defense

When you get a splinter, your body immediately distributes antibodies to prevent infection. If only our computer networks functioned in a similar way.

The federal approach to cybersecurity currently relies a lot on Band-Aids, said Lisa Schlosser, deputy administrator of e-government and information technology at the Office of Management and Budget, during a panel discussion at the ACT-IAC Executive Leadership Conference.

It's necessary, she added, based upon the status of agencies' cyber posture. But encryption and continuous monitoring, for example, both seek to minimize the damage. And they can do so in a meaningful way, with the former bringing with it the potential to reduce cyber incidents by as much as 50 percent.

NASA CIO Renee Wynn on the need to move beyond cyber Band-Aids. Lars Schwetje/Staff

But ultimately, the goal is to reach broader systemwide security that is engrained in a network's DNA.

"Moats and castles have stopped being a method of defense," added NASA CIO Renee Wynn, where agencies try to isolate their systems and networks in an effort to keep the malicious actors out. The need to share information makes that approach impossible.

"So then, how are we going to change this?" Like the human body's response to the splinter, which Wynn shared with the ELC audience, computer networks need to automatically isolate the intrusion, "then give information back to figure out how to proceed."