NEW THREATS MEANS NEW SOLUTIONS

Whether it's the ability to pay parking tickets, speeding tickets, file permits, apply or disburse benefits, the internet has transformed the way government delivers services. Although these changes provide much needed relief to citizens, there is also a dark side to digital solutions: the risk of cybersecurity has increased. The digital economy has brought many benefits to citizens, but it also requires government to be more proactive than ever to combat threats.

"We see the threat landscape changing so quickly that it is changing the way we are reacting, and that is actually shaping the landscape of government," said Jen Nowell, Senior Director, Strategic Programs, Symantec Public Sector, in an interview with GovLoop. "One driver is trying to provide many more services to the citizen online. And when doing that, we must be making sure we are focused on identify theft and other security-related issues, as they are now shaping government."

And as government adopts more web services, the way the public sector approaches cybersecurity requirements must evolve. Agencies must take a new approach and think about the variety of ways people access information. That often means they must go beyond checking off boxes for compliance.

"The way things used to be, officials took a checklist approach to security. They would ask, what is the bare minimum I can do to show that I am compliant with government security standards? That's now morphing to something more than just check the box to let's make sure a control is in place, and that it's improving my security posture," said Ken Durbin, Continuous Monitoring and Cybersecurity Practice Manager, Symantec Public Sector.

With programs like Continuous Diagnostic Management (CDM), agencies now use stronger frameworks and controls to protect information and move past the checklist approach. If a breach were to occur, there is much more liability as OMB and related agencies are providing organizations ways to execute cyber initiatives.

The evolution of cyber strategies is important to consider, but as both Nowell and Durbin noted, security does not mean simply deploying a new IT solution.

"We are always talking to our customers trying to find out what their needs are, but it really doesn't end there. They may buy our products, but if they do not deploy them correctly or they are not turning on all the features that are available to them, are they really getting the true protection of the product? I think staying engaged with our customers post sale making sure they are using the products correctly goes a long way in making sure they are improving their security," said Durbin.

Having specific touch points with clients is essential for Symantec, and as their cyber solutions mature, client needs often change.

"Organizations' challenges are always changing, because what the latest vulnerability or threat is right now is always changing. It's different for different customers, and as customers mature in their security program, then they start to experience different things, different threats," said Nowell.

Yet one of the common challenges continues to be network awareness. "The common denominator is that people don't always know what they have. So what I hear most from people is, 'If I could just understand where my network begins and ends, I could then really be able to secure it and lock it down,'" said Nowell.

Durbin added some additional commentary on the challenge of network awareness. "When talking to CIOs and CISOs it is quite surprising when they freely admit they may not have an accurate view of what is deployed on their network, both hardware and software. When you dig a little deeper and ask why, it comes down to priorities, money and the labor force to get it done."

But even when agencies have deployed tools to gain improved network awareness, they are still challenged. "An interesting twist on the problem of network visibility is highlighted by a conversation we had with one agency. They said, 'Look, I got four different tools telling me what's out on my network and they all disagree. I need someone that can help me take those different inventory reports and tell me what I actually have.' So sometimes the issue could be a problem of having too many tools letting you know what is going on," said Durbin.

Having the proper IT solutions and network insights is imperative to securing your agency as well as protecting against emerging threats. By taking some small steps to understand who is on your network, and what IT tools you need to stay secure, your agency can improve its overall security posture, and protect our critical information.