Most Cybersecurity Targets 'Just Basic Foundational Things' Under Attack

And the methods used typically aren't that sophisticated.

Amanda Ziadeh
Wed, 08/15/2018 - 16:49

Alissa Johnson, chief information security officer at Xerox (middle), speaks at the GovernmentCIO Media Tech Forum December 2017. Photo: Jeremy Long/GovernmentCIO Media

The cybersecurity challenges organizations face don't differ that much in government and industry, and what's in hackers' crosshairs is pretty much the same, according to Alissa Johnson, chief information security officer at Xerox.

Johnson should know: Prior to her current role, she served as deputy chief information officer for the White House's Executive Office of the President under the Obama administration, and did a stint as a cryptologic engineer at the National
GovernmentCIO Media sat down with Johnson at Black Hat to discuss the differences in private and public sector cyberthreats, the threat she finds most concerning and the importance of bidirectional information sharing.

GovernmentCIO Media: So, your keynote wasn’t open to press. Can you share what you talked about?

Johnson: I go with the Dr. J moniker, which is really a 76ers basketball player (Julius Winfield Erving II) from back in the ‘70s-‘80s timeframe. I talked about what Dr. J did on the basketball court; he defended the entire court. And that’s what we have to do: We can’t just defend our territory, our little small network. We’ve got to look bigger than that. It’s about building our partnerships and increasing our visibility. It’s all across sectors, and it’s all across from private to public partnerships as well.

GCIO: How does information sharing differ when comparing your current role with your time at the White House?

Johnson: When I was at the White House, I had so many I call “friends,” and now I have to phone a friend, it’s a very different scenario. If someone even thought something was happening, I had so many different vendors that were just so willing to help without strings attached, just because they had that level of patriotism and that level of passion for making sure that we were safe and our data was safe and secure. Now, I’m here on the private sector side, and I’m calling with, “Hey, I need some help,” and I get an account executive who knows an account executive. So, I have to really lean on relationships.

We have [Information Sharing and Analysis Centers] here on the private sector side, it’s still very siloed, so that amount of information sharing needs to still happen. We do that in other forums, but at a certain point, there are so many different forums, how many do you want to participate in?

GCIO: I attended the Homeland Security Cybersecurity Summit in New York City, where they announced the new Risk Management Center. Is that something you’re looking into?

Johnson: Yes, so I’ve had a lot of conversations with DHS about ensuring that they are not just owners and receivers of data, but also participants in the entire
community, in sharing of that information as well. I understand they have a certain focus from a homeland security perspective, but for the greater good, let us all participate in that and find a way for us all to share without all the sensitivities.

**GCIO:** So, what are the most concerning cybersecurity threats you are seeing right now?

**Johnson:** I would have to say the spear-phishing attacks, because they are so sophisticated. There’s a cybersecurity technology side that’s difficult, but it’s easy. We’re smart enough to learn and defeat and know the technology part. It is our emotional senses, our culture, that we have to change and that’s what makes the phishing so concerning to me, because as we train customers, as we train staff, we’re now having to retrain them and tweak them so that they know that even though this email looked like it came from our CEO, it really didn’t.

**GCIO:** How do you tackle that challenge?

**Johnson:** We’re really having to educate, because [adversaries] are going after those who aren’t really as tech savvy in that area, and that’s what our weakest link is. When I think of the sophistication of nation-state threats, it leads me back to phishing attacks. That’s their way in. So now, it’s not just about training people; it’s about changing culture. And not just culture of employees and staff and all of those that work at the company, but your customers. If you’re a government person, that’s about the American people.

So, we have to tackle it through education, but we also have to tackle it through our own systems and tools. I’m a big component of a [zero trust model](#).

**GCIO:** What’s a big cybersecurity culture difference you noticed in government and industry?

**Johnson:** One of the questions I get a lot is, “which one has the most challenges?” They all have different challenges — one side didn’t have more challenges than the other. I will say, areas of government are used to being locked down. I worked years at NSA, and it was the norm for me to leave my phone in the car, and go in and work and not have access to internet. And then, I get to private sector and I can do all of these things, but there’s a certain amount of scrutiny that we have on the private sector side because of boards, and because of that level of globalism, too. That necessarily doesn't transfer over to the government side. So, it’s really, really
different on both sides.

**GCIO:** What about in terms of the actual vulnerabilities you’ve seen on both sides? Because government is more accustomed to being locked down in that aspect, does it mean it sees fewer vulnerabilities?

**Johnson:** No, they don’t. But what I’ve seen is that the methods and tools that hackers are using to try to break in and get us at the State of the Union are the same tools and methods that they’re trying to use at Xerox. They tweak it, ever so slightly, to match. We talk about it as the “dark web” — it’s not a big operation. I actually think of it as the “The Wizard of Oz:” you pull back the curtain and you see it’s one guy trying to scare everyone else.

It’s definitely scary, and I’m not trying to say that the hacker community is not something to be feared; it definitely is, because of the amount of sharing that they do and the tools they have at their disposal. You can find something for $2.99, you can find something for $12.99 and a 12-year-old can buy it and be very, very destructive. But it’s not $500 to buy that same tool to attack Xerox; it’s still $12.99 or $2.99. And then, they’re smart enough to just tweak it ever so slightly so that it matches whatever you want.

The supply chain vulnerabilities that happened at Target . . . the breach that happened at Sony . . . even the breach that happened at Equifax, it’s just basic foundational things that are being attacked. There’s no secret sauce. They’re attacking ports that are open that shouldn’t be open, patching that hasn’t been done — basic stuff. So, I look at it from that perspective. It’s not that different, folks. Which is why I say, the sharing across all, it’s not that hard, people.

*Responses have been edited for clarity.*