EXECUTIVE VIEWPOINT
A Conversation with
RON ROSS

RON ROSS
Fellow, National Institute of Standards and Technology

The NIST computer scientist discusses upcoming guidelines for strengthening the resiliency and privacy protections of agencies' IT systems

What new NIST guidelines can help agencies develop a more adaptive approach to cyberthreats?

We've been working on a new publication, and we've moved up the release date by about a month because of the urgency of it. It's NIST Special Publication 800-160, Volume 2, and it's titled "Systems Security Engineering: Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems." We plan to release the initial public draft on March 21.

The publication looks at the fact that we're deploying computers into lots of critical places and talks about how we can deal with advanced persistent threat — those high-level adversaries with lots of resources, lots of capabilities, lots of skills who are constantly attacking our critical systems.

How do we have systems that are cyber resilient, which means they can operate after they've been attacked and have the resilience to continue to support critical missions and business operations? That's probably one of the most important questions that we're going to deal with in the next couple of years.

> How do we have systems that can continue to support critical missions and business operations **after they've been attacked**?

Obviously, we want the industry to be able to implement some of those best practices to build more trustworthy, secure components and systems. But for agencies, 90 percent of our stuff is already installed. What do you do with all that?

This document is going to give people strategies for that as well because agencies aren't going to get rid of everything as they modernize.

When we try to protect systems today, there are three major objectives we try to do. We harden the target. That would be doing some basic things like two-factor authentication, encryption, access control mechanisms. Most of these things are reflected in the NIST security controls.

We know that even if an agency is doing everything right, sometimes adversaries still get in. So the second thing we focus on is trying to limit the damage they can do once they're in. One way to do that is by not allowing them to move laterally or making it very difficult for them to move. The other way is to limit their time on target through virtual machine technology, where you're refreshing the software on a regular basis.

The third thing is you try to make the system what we call survivable or resilient, which means it can operate even while under attack. It may be a little bit degraded at some point, but it's not catastrophic.

What we're trying to do with this publication is deal with cyber resiliency. How do we arrange things, and what kind of things can we do? What strategies can we put into place to make that system difficult to get into and then difficult to bring the whole house down? That's the bottom line.

Why is an adaptive approach to cybersecurity important?

I'm not sure everybody is prepared for the world that we're starting to emerge into in the 21st century. Most of us look at computers, smartphones, tablets or laptops as a black box. You are interacting

Over the next year, you'll see a **full integration of privacy into all our FISMA pubs**. It's going to stand side-by-side with security as an equal partner, every bit as important as security.

with the screen, and you are running the apps and all that. I call that the above-the-waterline view. It's like you are in the ocean, and half of you is above the waterline looking around having a good old time. Meanwhile, below the waterline, there are sharks.

The average person is not really concerned about what's going on below the waterline because that's not where their world view is. They're dealing with the application level. Meanwhile, incredibly complex software, hardware, firmware and systems are below the waterline. That complexity is where the adversary is attacking every day. That's the part we have to start to fix.

Sometimes there are things you know you have to do but you never do them. Even with all this danger out there, the culture still drives us to more technology, more apps, more smartphones and more tablets. I think we are literally addicted to that whole world because of social media and all the technology. It's doing things we never imagined it could do.

We're going to have to create more resiliency. And "adaptive cybersecurity strategies" may be an appropriate term to capture that whole new world we're moving into.

How does adaptive cybersecurity fit into IT modernization plans?

We can just go ahead and modernize like we always do, or we can start to take advantage of some new things. One is moving additional federal applications and systems to the cloud. Everything's not going to go to the cloud, but FedRAMP gives you some confidence that you can move certain of your applications and maybe even reconfigure or redesign some of the systems to take better advantage of cloud technology.

The second one is to develop more shared services. In other words, how many HR or payroll systems does the federal government need? If you could combine them and have one service that all the agencies can use, then think how much cost you can eliminate. And you can then turn that cost savings into greater protection for that shared service.

Whatever's left might be termed high-value assets. After the Office of Personnel Management breach, the Department of Homeland Security started looking at everything we consider a high-value asset. It's looking at what those systems do, why they're critical, what they're connected to — either a direct connection or through secondary or tertiary connections. That's how adversaries tend to get in, through those transitive connections. By looking at those things, we can say, "OK, if we move a lot of stuff to the cloud and we move stuff to shared services, then we can really focus like a laser beam on those high-value assets."

And we can apply some of the security engineering guidance that NIST is producing with greater strength, including some of the security controls that are more difficult but necessary, to help protect those high-value assets. We can focus on that instead of trying to do everything and not doing a good job at it.

We also want to make sure that we protect all the data that the citizens expect us to protect, so we're integrating privacy into our guidance.

We're modernizing five publications that have been around since the original Federal Information Security Management Act — including 800-53, the security and privacy controls catalog, and 800-37, the Risk Management Framework.

That framework traditionally focused only on security risk management. The new 800-37 Revision 2 is going to focus on managing risks for security *and* privacy.

Over the next year, you'll see a full integration of privacy into all our FISMA pubs. It's going to stand side-by-side with security as an equal partner, every bit as important as security.

I've never been busier in my 20 years at NIST. I should have retired a year ago, but I can't seem to pull the trigger because there's still too much to do. And I just want to see this problem solved once and for all. ■