ISSUES TO WATCH

Growing Threats and Changing Relationships

Mark Weatherford has led information security organizations at multiple levels of government, as well as the private sector. He was the first deputy undersecretary for cybersecurity at the Department of Homeland Security under President Barack Obama. He served as chief information security officer (CISO) for the states of California and Colorado. And he was vice president and chief security officer at the North American Electric Reliability Corp., a regulatory authority that oversees reliability of the power grid.

We talked to Weatherford about emerging security threats and the changing cybersecurity relationship between states and localities and the federal government.

What is your perception of the cyber threat environment right now, and what does it mean for states and localities?

I try to avoid using fear, uncertainty and doubt in this business. But I also think it's important to be honest. We are living in a precarious threat environment. When a single person with a laptop and internet access who lives halfway around the world can create chaos for state and local governments that are responsible for large numbers of constituents, this is a threat we need to pay attention to.

Most of the cybersecurity people I know in state and local government are devoted and professional, but far too often, they are working with limited resources. They're not in a fair fight. You have little cities that are going head-to-head with nation states.

We're beginning to see direct federal funding for state and local government cybersecurity, along with new incident reporting requirements. What's your take on this changing intergovernmental relationship?

I think it's getting better, but the federal government still too often acts like the older and smarter sibling. In reality, the feds don't understand the challenges of working with residents and running a small security operation on incredibly limited resources. So some of their pronouncements come off as high and mighty. I will say, however, that CISA has come a long way. They are actively working with state and local agencies on a daily basis with funding and a variety of other resources.

One thing I worry about with the new State and Local Cybersecurity Grant Program, however, is that organizations will buy shiny new tools without considering the resource tail that comes with them. You need to train your people and update and maintain these technologies. I've been advising small jurisdictions to consider managed security services instead of buying one-off solutions that will require more work than they can do.

What cybersecurity issues should state and local officials be paying more attention to?

One is managing supply chain risk. We used to think of supply chain from a logistical perspective — how do I get a product from point A to point B. Cybersecurity has changed that concept. Now we need to understand the components that go into our technology, how it's being updated, who has access to it and how it's being managed across its entire life cycle. That's why efforts like the Software Bill of Materials initiative, which was included in President Biden's 2021 executive order on cybersecurity, are getting a lot of attention.

Another important issue is the convergence of physical security, IT security and operating technology (OT) security. Traditionally, these have been viewed as separate disciplines. It's more important than ever to see the relationships between these security disciplines because bad guys don't care which they compromise. And if these disciplines are siloed, it's much easier for an attacker to pivot to other parts of the organization once they're inside.

What advice do you have for CISOs and their bosses?

CISOs need to get out more often. Technical people tend to live in a technical world, but security doesn't exist in a vacuum. CISOs need to build relationships — sometimes really close relationships — with others in their organizations. For executives, I would say, know who your CISO is and talk to them regularly. I've seen some pretty embarrassing conversations where government executives were asked, who's responsible for security in your organization? And you get this blank look; they don't even know who the person is.

SHUTTERSTOCK.COM