Q&A

Executive Viewpoint

A conversation with Michael Duffy

Associate Director, Cybersecurity Division, Cybersecurity and Infrastructure Security Agency

This interview continues at Carah.io/2022-FCW-Sept-Gov

How is the cybersecurity landscape changing for government agencies?

Our rapid and significant migration to cloud and hybrid environments since the start of expanded remote work has required a different approach to protecting critical data and users. The basics are still absolutely necessary regardless of where data resides. Knowing what you have and where it is and keeping up with cyber hygiene hasn't changed much in principle. It's more about how we apply those principles to these new environments.

At the same time, threats are increasing and growing more sophisticated, cross-cutting and persistent. As a result, cybersecurity teams are finding themselves needing to work more closely with organizational elements and specialty areas, such as procurement, policy and legal experts for complex topics like supply chain risk. The leadership team needed to adequately address enterprise cyber risk is widening by necessity. This expansion is a good thing, but it requires agencies to adapt governance models to this new landscape.

In addition, agency cyber teams have been in an "always-on" state for several years. There have been many significant governmentwide and national-level events that cyber practitioners have had to work through for weeks or months at a time. It takes substantial time and resources to respond and recover. This is time-intensive and detracts from longer-term planning, and it also requires highly skilled practitioners, who are in short supply across agencies. This, unfortunately, has become the status quo and how cyber response works. This needs to change.

To address this landscape, CISA is working to build a more cohesive, focused community of practice and to defend our federal enterprise by managing it more like a unified IT enterprise. As agencies tackle the same priorities and challenges, CISA has enhanced our efforts to share guidance, proven practices and direction. We've increased the number of cybersecurity solutions we offer directly to agencies and the number of mandated actions that individual agencies must take with this "enterprise" concept in mind.

Furthermore, the federal government is mindful of the broader IT community upon which we depend and is integrating security expectations into our contracts with vendors and forging new partnerships through entities like the Joint Cyber Defense Collaborative established by CISA. We're also thinking strategically about how to gain more operational visibility into agency data regardless of where it resides. As the landscape changes, there is too much for an individual organization to take on alone; acting as an enterprise is critically important.

Why is zero trust a key element of the Executive Order on Improving the Nation's Cybersecurity?

Our federal government maintains a large remote-work footprint and a high demand for cloud services. Adversaries have found opportunities in that environment, and to some degree, our existing architectures not only did not adequately prevent adversaries' activities but facilitated their movement across networks.

In addition, because the SolarWinds intrusion campaign and the Log4Shell vulnerability captured so much attention, there's always some danger in thinking that these are the most likely or dangerous types of attacks moving forward and that building a defense for these specific situations is sufficient for the road ahead. Too often our strategic response tends to be tactical and shaped by one scenario. We are looking to do more than plug holes. We want to prepare for these attacks and more, ensure resiliency more broadly, and establish a better foundation.

The government's focus on zero trust principles comes from our collective understanding that addressing the underlying architectural challenges raised by those events and others must be at the core of our approach to effective cybersecurity. We need to change the way we build defensible architectures for sustainability and resiliency, and we need to promote the right level of security investment for decades to come based on the attacks we've experienced and will likely experience in the future.

How is CISA helping agencies implement zero trust?

CISA's focus has been on the people, process and technology aspects of adopting and operationalizing zero trust. We have made a concerted effort to add to the body of knowledge for applying zero trust across agency networks. That's where our Zero Trust Maturity Model and the Cloud Security Technical Reference Architecture come in. We also conducted a series of well-attended workshops over the last year that brought together security experts and agency leaders to walk through the implementation of the Zero Trust Maturity Model's five pillars.

It can feel like a pretty steep climb to implement zero trust, and as the operational lead for government cybersecurity, CISA recognized the need to provide clarity, focus and support to federal agencies throughout the process. Defining the initial steps in the maturity model was critically important for us. CISA's CyberStat interagency workshop series provides consistent messaging to agencies and allows us to lead zero trust implementation discussions and generate content that meets agencies where they are on their zero trust journeys. Regardless of whether they're at step one or step nine, agency leaders can reference this content to see what the next level of maturity should be and how they can work toward it.

What other guidance and support does CISA offer to agencies?

For years, CISA has provided a full catalog of technical support and solutions. We offer services and capabilities that either fully or partially satisfy zero trust principles, and we are expanding those programs. For example, the Continuous Diagnostics and Mitigation program creates the foundation for asset management and cyber hygiene, and these are foundational to enabling zero trust in time. CDM has been integrating expanded endpoint detection and response solution deployments to give even greater operational visibility to agencies and CISA.

In addition, CISA's Protective Domain Name System service gives agencies state-of-the-art protections and encryption for DNS traffic. We are currently onboarding federal agencies, and it will be available to all agencies in 2023. We're pleased to roll out this complementary security service in parallel with the zero trust strategy.

Finally, we are building a dedicated unit at CISA focused on tailored federal agency cybersecurity assistance. This new CISA group, the Federal Enterprise Improvement Team, will provide direct support and lead targeted improvements based on agency, CISA and federal enterprise needs.

How can agencies overcome the cultural obstacles to improving cybersecurity?

It is critically important that the entire organization is in sync about the way forward. For example, an agency mission owner is focused on delivering services to the American people and other government agencies. There can obviously be some friction on the cybersecurity side of mission operations when a patch needs to be applied or a legacy system needs to be replaced. Overcoming such obstacles requires cross-functional planning with budgets in mind, building trust when cybersecurity work temporarily affects other mission work, and educating employees and leaders about cybersecurity. CISA frequently gets requests for cyberthreat briefings to mission owners to help agency cyber teams bring them to the table to tackle these challenging IT issues. I do think we've seen an encouraging trend where more agencies and organizations consider cybersecurity as a core mission-enabling function critical to achieving all broader aims.

But we're also seeing a second cultural challenge as cyber roles have been increasing across agencies. There are more cyber practitioners in government than ever before, and that's a good place for agencies to be. But it also means cybersecurity management within an agency must be well-coordinated, if not fully centralized, with clear accountability. In some organizations, the chief information security officer might not be leading the agency's zero trust implementation or patch management because it is run by some other IT organization within the department. Clearly defined governance structures are important in these cases.

Due to the challenging cyber landscape, agency cybersecurity actions must occur in cyber-relevant time. There can't be a delay because of any complexities in the organization. A unified, enterprisewide, singularly focused effort allows us to communicate better at the agency level as well as at the CISA cross-government level. It also allows us to gain operational visibility so that individual agencies and CISA can take better, faster, more impactful actions based on the risks we see across the enterprise. ■