



Elevate Cyber to Support the Mission

Between executive orders and National Institute of Standards and Technology (NIST) directives, cybersecurity can too easily become a compliance exercise for government agencies. While it's important to check all those boxes, the cyber defense bar should be set higher.

When it comes to cybersecurity, zero-trust strategy and even strategies around securing artificial intelligence (AI), "the metric ultimately is the mission," said Dan Bradley from the Cybersecurity and Infrastructure Security Agency (CISA). "We're not doing it simply for cyber reasons. We're trying to protect and enable a mission."

In a recent GovLoop roundtable, he and other leaders from government and industry explored how best to secure that mission.

Roundtable Participants:

Paul Blahusch, Chief Information Security Officer, U.S. Department of Labor

Dan Bradley, Federal Enterprise Improvement Team, CISA

Adam Edelman, Federal Technologist, Snowflake

Sallie Edwards, Researcher, NIST National Cybersecurity Center of Excellence/MITRE

Keegan Mills, HQE Engineering and Cyber Technology Lead, Marine Corps Systems Command

Current Cyber Challenges

A number of structural challenges can get in the way of agencies' efforts to deliver effective cyber protections.

- **Distributed data:** When it comes to data, "we used to be able to keep it inside our castle somewhere. But now, data is everywhere," said DoL's Paul Blahusch. In this environment, "we need to make sure that we're protecting that data wherever it is."

NIST is well aware of the challenge. "When we're talking about data no longer being in-house ... we need to all be working together to leverage the best guidance, the best information," said Sallie Edwards, a researcher at NIST.

- **Complex data:** The varied nature of modern digital information makes it harder to secure. Given all its varied forms, including structured and unstructured, "data is really a huge challenge," Bradley said.

It can be hard to apply security measures consistently across disparate data types, and yet "the confidentiality, integrity, availability of our data is really foundational to what we are trying to accomplish," he said.

- **The need for data-sharing:** The rise of AI in particular calls for ready availability of data. "The ability to share information is what will drive these models to produce better AI results," said Adam Edelman of Snowflake.

The need to collaborate over common data raises security concerns. But strong protections can help to drive effective data-sharing. "If we can appropriately tag the data and understand it, then we can share it more. That's what our chief data officer and chief evaluation officer are really interested in," Blahusch said. "As we improve security of the data, it will blossom out and allow more data-sharing."

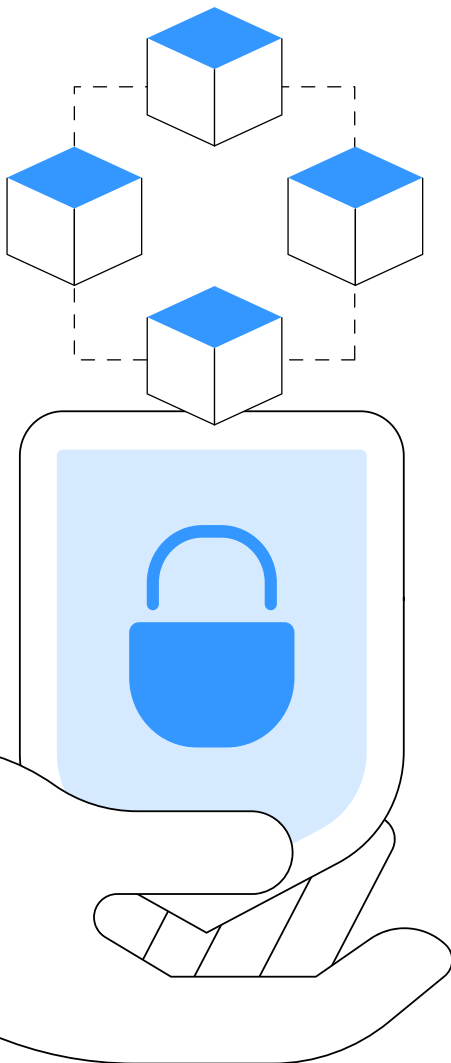


7 Strategies for Elevating Cybersecurity

Federal agencies can take several key steps to secure their increasingly complex IT ecosystems.

In the big picture, this means steering toward “a data-centric architecture, data-centric security,” said Keegan Mills, engineering and cyber technology lead for Marine Corps Systems Command. This requires “really changing the definitions to focus on those things that we actually care about: the data, the identities and the services that are providing that interaction,” he said.

How best to get there?



1. Focus on Progress, Not Perfection

No cyber strategy will be entirely fool-proof. Agencies shouldn't let that stand in their way. “Get started. Make some progress. Because every vulnerability, weakness or hole we can plug is a win for us. If we get a little bit better, that's a win,” Blahusch said. “We're never going to be able to get 100 percent. Don't worry about that. Just get better.”

That being said, “not all vulnerabilities are created equal,” Mills said. Faced with limited resources, it's important to prioritize, to start by remediating the risks that have “the biggest impact to mission.”

2. Build on the NIST Framework

The release of the NIST Cybersecurity Framework (CSF) 2.0 creates an opportunity for agencies to improve their strategies. Too often, agencies and system integrators lack a shared vocabulary around cybersecurity. The CSF offers “a single framework” to unify their efforts, ensuring everyone is “able to speak the same language,” Edelman said.

The CSF can help agencies rank their cyber efforts in order of importance. In the face of resource constraints, “CSF allows us to identify what's most critical in light of our risks and objectives,” Bradley said.

3. Identify Your Assets

To implement effective security, you have to know what you're securing. “People still get breached because they don't know what their assets are, they don't monitor them, so they're not patched, they're not configured right,” Blahusch said.

External-facing systems and mission-critical systems in particular must be accounted for in a robust cyber strategy. In order to effectively secure these systems and their data, “we have to know that they're out there,” Bradley said. With this in mind, IT asset management “is foundational. If you don't get that right, then you're just throwing cyber mechanisms out there, and hoping they stick,” he said.

4. Pay Attention to People, Culture

Strong cybersecurity requires not just technological safeguards, but also attention to people, processes and organizational culture. Today's environment requires a holistic approach, with all organizational elements working in unison. Representatives from all stakeholder groups "should be part of the data team, the data strategy," Edelman said.

Cyber concerns should be emphasized at all levels and reinforced with practical measures. "Security awareness training is no longer good enough," Edwards said. Training should come with phishing tests and other practical exercises to ensure everyone's on the same page.

5. Unify the efforts

In raising the cyber bar, agencies need to create strong connections between their technology operations, the security operations center (SOC) and governance efforts. Too often, these views are fragmented.

"You go to the IT operations crowd, and they'll say: This is what the enterprise looks like. You go to the SOC and you get a different view," Bradley said. "You go to the governance folks ... and you'll get a third, completely different view."

When all these perspectives are aligned, agencies are better able to apply the right tools for maximum effect, "instead of governance being done for compliance purposes," he said.

6. Have a recovery mechanism

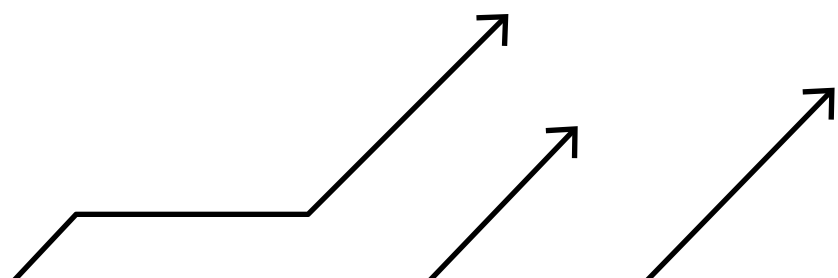
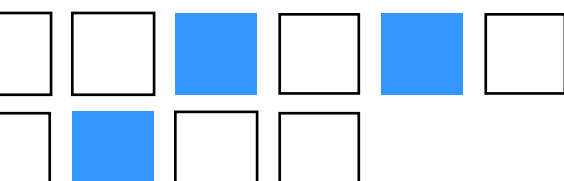
The point of security is to keep things running smoothly, "to provide that assurance and availability" in support of mission outcomes, Mills said. To that end, agencies need to have the means in place not only to prevent incidents, but to recover from an attack.

While breaches will surely occur, government can't afford to let those incidents become catastrophic. "In my world, I can't have the bitcoin scenario where, if the data's corrupted or if the blockchain is corrupted, it's gone forever," he said. "There has to be a recovery mechanism."

7. Mitigate risk in data-sharing

Agencies need to ability to share data securely in support of emerging AI use cases and a range of other needs. This poses inherent problems. "We ingest data from other sources, and that data itself may be a threat," Bradley said.

To share data effectively, agencies must "look at how our applications and services can process unsafe data, in a way that doesn't impose risk," he said. Robust cyber effectiveness "isn't just about protecting our own data. It's about processing data we receive from others, and not being caught co-opted by it."



Moving Forward

How best to make headway against the ever-changing cyber peril? These key strategies can help agencies move forward.



Leverage guidance: Agencies should take advantage of the abundant federal guidance on addressing the cyber threat. Given the complexities, “we have to leverage everything that NIST is putting out, everything CISA’s doing,” Bradley said. “We really can’t afford not to collaborate.”

Government has a variety of trusted resources available, “and the [CSF] is certainly one of those. It’s high-level and applicable to all types of organizations,” Edwards said. She also encouraged agencies to leverage the practical security implementation guidance that’s freely available at the National Cybersecurity Center of Excellence.



Shift to data-centric security: Data drives mission, and it ought to be at the core of any security strategy. “Shifting the focus to securing and making available data is the journey that we’re all on,” Mills said.

To secure data effectively, agencies need to identify microservices that connect all that data. “Right now we’re doing that at the application layer, and I think we’re going to move down the stack,” he said. “We need to be asking industry for tools that go deeper.”

AI will help drive that shift, he said, as it enables agencies to look beyond individual users or incidents to glean the kind of holistic insights that can drive a truly data-centric approach to security.



Focus on mission: Cybersecurity professionals can raise the bar by aligning their efforts in support of broader organizational outcomes.

“If you’re trying to just drive cyber for cyber’s sake, you’re not going to be as successful,” Blahusch said. “If you’re in cyber leadership in your organization, focus on mission. Think about the mission first.”

Strong cyber empowers the data-sharing that is increasingly critical to mission outcomes. “The more we share, the better,” Edelman said. “It certainly drives AI. But it drives all the other outcomes as well.”

With a focus on mission goals, cybersecurity leaders can go beyond mere compliance. They can lock down data in ways that keep it safe while still making it readily available across organizational silos, to fulfill the myriad crucial functions of government.



Click [here](#) to learn more.