FEDERAL NEWS NETWORK

EXECUTIVE BRIEFING SERIES

Investing in collaboration, data, people help DoD and DHS bolster cyber

BROUGHT TO YOU BY verizon

Investing in collaboration, data, people help DoD and DHS bolster cyber

BY DAISY THORNTON

You've no doubt heard the cliché, "Cybersecurity is a team sport." Originally coined to earn buy-in outside IT departments, that quip emphasizes the hard truth that cyber touches every user in every organization, making cybersecurity therefore everyone's job to some extent.

But among the defenders on the frontlines of the cyber battlefields, that cliché has taken on a new meaning: Your cyber team doesn't have to be limited to your own organization or, for that matter, even your own mission focus or business sector.

> We're working with our partners and the federal government, marrying that together and figuring out what are the right policies, procedures and things that need to be put into place so that we can work in lockstep to be able to then protect all of our assets and data.
>
> — Lamont Copeland, Managing Director of Federal Solutions Architecture, Verizon

Cyber leaders and chiefs within the departments of Defense and Homeland Security increasingly partner with one another and with the private sector to shore up cyber defenses and share threat information. It's become essential in creating a comprehensive approach to protecting the data and networks of federal agencies, the nation's critical infrastructure and systems within U.S. industry, pointed out leaders during a panel discussion on tackling cyber effectively now. In this briefing, we share the takeaways and insights from that discussion.

"We have partners that are on board with the Cyber Safety Review Board and what we're working on — looking at all the processes and procedures, looking at what the threat vectors are," said Lamont Copeland, managing director of federal solutions architecture at Verizon. "What are the things that industry can bring in to help agencies and industry understand what the threat vectors are? What are some of the protective measures? What are some of the things you should look out for when you're trying to protect all the different aspects of your environment?"

Creating mechanisms for collaborating on U.S. cyber defenses

The Cyber Safety Review Board, established by President Joe Biden's executive order on improving the nation's cybersecurity, evaluates major cyber incidents and makes recommendations on strategies for reenforcing cyber for both the public and private sectors. Members of the board include the Cybersecurity and Infrastructure Security Agency, DHS, the Federal Chief Information Officers Council, the Justice Department, the National Security Agency and industry technology leaders like Verizon.

CISA CIO Robert Costello credits the board with "doing good work" through its collaborative approach and focusing on the interdependencies now common among IT and critical infrastructure.

Another similar initiative Costello praised is the Joint Cyber Defense Collaborative, a threat information-sharing platform spearheaded by CISA. JCDC promotes sharing cyber intelligence to help agencies and industry stay agile and ahead of adversaries, develops proactive cyber defense plans, and shares cyber alerts and advisories with the nation's cyber community. Those efforts, he said, are beginning to expand into federal security operations centers now too.

> We're seeing automated and weaponized vulnerabilities coming at us faster and faster as we try and manage through all this change. Our number one goal is to ensure resiliency of the missions.
>
> — Rear Adm. Bill Chase, Deputy Commander, Joint Force Headquarters–DoD Information Network

"One of the things I always went back to in my prior role supporting law enforcement was our enemies don't play by the same ethical rules we do. The cartels don't sit around and say, 'Well, let's develop some policies and procedures before we utilize new technology.' So while I need all of those things, first and foremost, I am bringing an operator-centric mindset to my office," Costello said. "We need to live and breathe the mission so that we become a trusted partner and that [agencies and companies] want to come to us rather than either building their own solutions or going rogue or some of the other things that can happen."

At the same time, agencies are also leaning on industry to shore up weaknesses and provide necessary

technologies and expertise to federal cyber teams.

"In some areas, we need some more work in critical infrastructure, operational technologies in particular. That's not typically a strong suit for our military folks," said Rear Adm. Bill Chase**,** deputy commander for the Joint Force Headquarters–DoD Information Network (JFHQ-DODIN). "That usually requires a longer time in industry and the specialized approach that we tend to see on the industrial side. So that's an area we're going to have to lean on those partnerships … to understand and really to feed the mission and understand where we have building blocks in place but where we may not understand the risk."

Verizon's annual interactive Data Breach Investigation Report is also a source of useful information on cyber threats and attack trends, Copeland said. He said it helps provide information about what Verizon sees from both an infrastructure and a security aspect.

"You have a lot of things happening with hacking, malware, ransomware, which allow the threat actors to come do different things with stealing credentials, stealing information, putting in different things, which will then put our nation in a precarious position to be able to protect each one of our citizens, each one of our soldiers and all of our agencies," Copeland said.

"We're taking that information, and we're working with our partners and the federal government, marrying that together and figuring out what are the right policies, procedures and things that need to be put into place so that we can work in lockstep to be able to then protect all of our assets and data."

Managing cyber risk in an interconnected world

These kinds of partnerships also help agencies figure out how to best manage their risk. For example, the Army Cyber Command approaches it using a triaging method, said Ronald Pontius, the recently retired deputy to the ACC's commanding general.

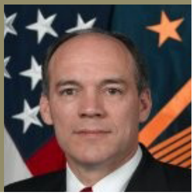
"As we look at the threat and we look at the vulnerability, that power of partnerships is absolutely key — given the scale and complexity we're talking about — to understanding the threat vector to start with," Pontius said. "We get a significant amount out there from Cyber Command, the National Security Agency, the broader Intelligence Community and increasingly the commercial space. If we can get that down to the lowest unclassified level, on one hand we may need nation level attribution or specifics that we might get from the IC. But in the field, what our cyber operators and defense folks actually need is, 'Just tell me what the next step is and how do I break that chain that will stop bad things from happening to my unit.' So commercial threat intelligence offers us a way to get that down without the more highly classified pieces."

Partnerships not only help the Army fully understand the mission space, they also help reveal the concerns of other organizations. That lets the Army decrease risk by reducing response times to actual incidents, Pontius said.

And that's a priority in other areas across DoD too.

JFHQ-DODIN is focused on managing cyber complexity at scale across the entire department by weighing compliance relative to risk, Chase said. No network is perfect, he said, but understanding risk helps to build resiliency, which makes missions more likely to succeed, he added.

> The Army is working on ensuring that all its data is visible, accessible, understandable, trusted and linked, interoperable and secure. We call that faultless.
>
> — Ronald Pontius, Former Deputy to the Commanding General, Army Cyber Command



One way the JFHQ-DODIN team accomplishes that is through daily evaluation of internet-facing components of the network. They examine the vulnerabilities, evaluate the threats and the likelihood of an incident, and use that to understand potential impact on the mission.

"The question I get asked most often is, 'What is the cyber risk to my mission?' And that's usually from a combatant command or other element," Chase said. "We have 45 different DODIN areas of operation and essentially those that provision networks. And that's the thing, the folks that you would expect — all of the services, the combatant commands — actually provision small portions of the networks themselves, usually in and around their headquarters. And then there's all the Defense agencies for absolutely critical things like moving logistics, making sure health care is still there, that the financial operations still go. Harnessing all of those and understanding the risk and stitching together that story is our priority for this year."

To do that, JFHQ-DODIN aims to standardize risk approaches into what Chase called "security areas." Those are generally internet-facing things that adversaries can gain access to, he said. The expectation is that standardizing risk approaches in those areas will increase the speed of decision-making.

JFHQ-DODIN is using endpoint data to understand where to apply operational and policy standards to establish a meaningful, continuous defense in depth. That becomes especially important when it comes to weapons systems, Chase said.

"This is an exciting time to be in cyber. There's a whole lot of change going on," he added. "We're seeing automated and weaponized vulnerabilities coming at us faster and faster as we try and manage through all this change. Our number one goal is to ensure resiliency of the missions."

> My office really needs to be on the bleeding edge or people just won't want to work here. One of the most important things to me is I have to make remote work really effective.
>
> — Robert Costello, CIO, CISA

Chase identified three key elements necessary to achieving that goal:

- First: Ensure everything JFHQ-DODIN does enhances mission readiness in some way. Outside of DoD, that translates to adding business value, he said.
- Second: Empower the technical and tactical levels within DoD, which will increase speed and reduce the amount of remediation that has to happen.
- Third: Enable situational awareness to start making more data-driven decisions.

"Is it really tracking toward reducing the complexity? How do we take steps in the meantime to translate, standardize and normalize those things, to get after the machine learning and bring to bear for some of these automated problems that are already being thrown against us?" he asked.

Keeping sight of the importance of data

JFHQ-DODIN isn't the only organization looking to better leverage data for its cyber defenses. Pontius said one of the Army's top priorities is to become more data-centric to improve decision-making.

"Data is a strategic asset," he said. "The Army is working on ensuring that all its data is visible, accessible, understandable, trusted and linked, interoperable and secure. We call that faultless."

One critical factor in that effort is the Army's migration to a cloud environment. Pontius said legacy systems often stovepipe data, reducing its visibility and accessibility. Then, underlying everything is identity, credential and access management, which supports auditability and is key to implementing zero trust.

On the cloud front, the Army has accomplished its migration to Office 365, which it calls Army 365. As of 2022, the entire service had transitioned to the environment, the second largest Office 365 deployment in the world. Pontius said it's currently on the unclassified network but will be moving to the secret environment in the next 12 to 24 months.

That kind of cloud-native adoption will help unify the Army's environment, leverage data as a strategic asset and achieve interoperability for better decision-making, Pontius said.

That's especially important for the Army given its scope and scale, with 1.4 million users worldwide. That's a massive attack surface to defend, he pointed out.

Putting increased focus on cyber workforce

But data is just one part of the equation: Agencies and their partners need to focus on workforce as well.

"The people and the data are the critical infrastructure, the things that we need to protect," Copeland said. As long as we're

making sure the data is protected and the endpoints out there delivering the data are protected too, we'll know we're providing the right services to our partners."

That's currently a major focus for CISA, which has a small workforce of around 3,000 people that Costello describes as "small but mighty."

"We're recruiting some of the best cyber minds in the country, and I need to make sure they have a good work experience," he said.

Costello said he's currently trying to build up his development, security and operations (DevSecOps) staff, as well as improve human resources and basic staff-level functions to help enable that workforce.

"It's a technical workforce," he said, and added, "My office really needs to be on the bleeding edge or people just won't want to work here. One of the most important things to me is I have to make remote work really effective. I have to make the devices you get something that cyber operators want to work with because there's nothing worse than trying to do your job and you have horrible IT."

That's a sentiment shared by some of his industry partners. Copeland said a top priority for Verizon is making sure operators in the field have the right devices to do their jobs on a daily basis. That requires a balance between security and speed, he said. It also requires paying more attention to the cybersecurity needs of edge devices.

Meanwhile, the Army has honed a recruiting strategy that boils down to four key actions: acquire, develop, employ and retain. That strategy encompasses the entire workforce — military and civilian — and emphasizes cultivating the workforce the Army currently has while simultaneously enhancing its recruiting environment to get new skill sets directly from hires coming out of colleges and universities.

Costello calls that "addressing the full lifecycle" of federal employment, from recruitment through career development.

"How do you grow in your federal career?" he asked. "How do we take advantage of the DHS cybersecurity service? How do we maybe even look at making it easier to come and leave from federal service — but while you're here, have a super, super successful career?"

These goals depend on diversity too, Costello said while acknowledging that IT is a male-dominated field — something that needs to be addressed in the recruiting strategy and in the culture of federal organizations.

The future of cyber defense

All of this focus on the workforce is geared toward one main outcome: creating a cyber workforce with the skills and the means to collaborate across organizational boundaries and develop a cybersecurity defense strategy that will benefit the entire nation.

“The partnership and discussions on how we all drive outcomes together and the continued evolution of moving toward that, that’s going to help us ensure that we’re securing these networks, securing the data, securing all the systems and mission sets that we need to be able to support — for all of our end users,” Copeland said. “I’ve seen a lot of that. There’s a lot of interaction and work between industry and the federal government to make sure that we are going at this together because there is that human element we’re talking about. We know what we need to do to be able to support each other, to support the networks that need to be delivered.”

Discover additional ways that Verizon partners with the Department of Defense at verizon.com/defense.

The sources in this article shared their comments during a Federal Executive Forum, presented by Trezza Media Group.