FEDERAL NEWS NETWORK

EXPERT EDITION

OPERATIONAL RESILIENCY

INSIDE THIS ISSUE:

Tackling long-standing inefficiencies

Modernization long-standing efficiencies

Mission centered enterprise organization

New improvements from NAVSEA

BROUGHT TO YOU BY:

VERITAS carahsoft

TABLE OF CONTENTS

Without a doubt, the coronavirus pandemic has been the government's biggest continuity of operations exercise in decades, if not ever.

It wasn't just a matter of ensuring people could easily access email or collaboration tools, but it was a matter of making sure agencies continue to meet mission goals in a timely and effective manner.

This e-book demonstrates how agency operations remained resilient in the face of one of the government's biggest challenges in a long time.

Mike Sydla, the division director for Information Management Resources Logistics, Maintenance and Industrial Operations at Naval Sea Systems Command headquarters, explained how employees during the pandemic worked to get aircraft carriers or submarines back in service.

Congressman Derek Kilmer (D-Wash.), chairman of the Select Committee on the Modernization of Congress, discussed how the emergency forced Congress to rethink some well-established practices.

The Government Accountability Office's a Disaster Resilience Framework gave agencies three broad principles for how keep their mission critical operations running.

Vijay D'Souza, GAO's director of Information Technology and Cybersecurity, said the pandemic helped prove out these concepts.

The one thing that these interviews highlighted is there is no substitute for preparation and planning. Organizations with a flexible and elastic technology infrastructure and which understands the value of their data are better prepared to have resilient operations in the face of a disaster.

Jason Miller
Executive Editor
Federal News Network

Disaster planning framework asks agencies to make some tough decisions

BY AMELIA BRUST

How can agencies be expected to budget and plan for worst-case scenarios which are statistically unlikely to occur? It's a difficult challenge but, as the coronavirus has demonstrated, a necessary one, hence why the Government Accountability Office published a Disaster Resilience Framework.

"They basically need to start out by identifying the risks to their systems," he said on Federal Monthly Insights Operational Resiliency. "I mentioned a natural disaster or it can be something like a pandemic – what you have to do is think about how each of those risks would affect each of the particular systems you have. Then what you need to do is you need to develop a mitigation strategy and figure out, you know, what would you do?"

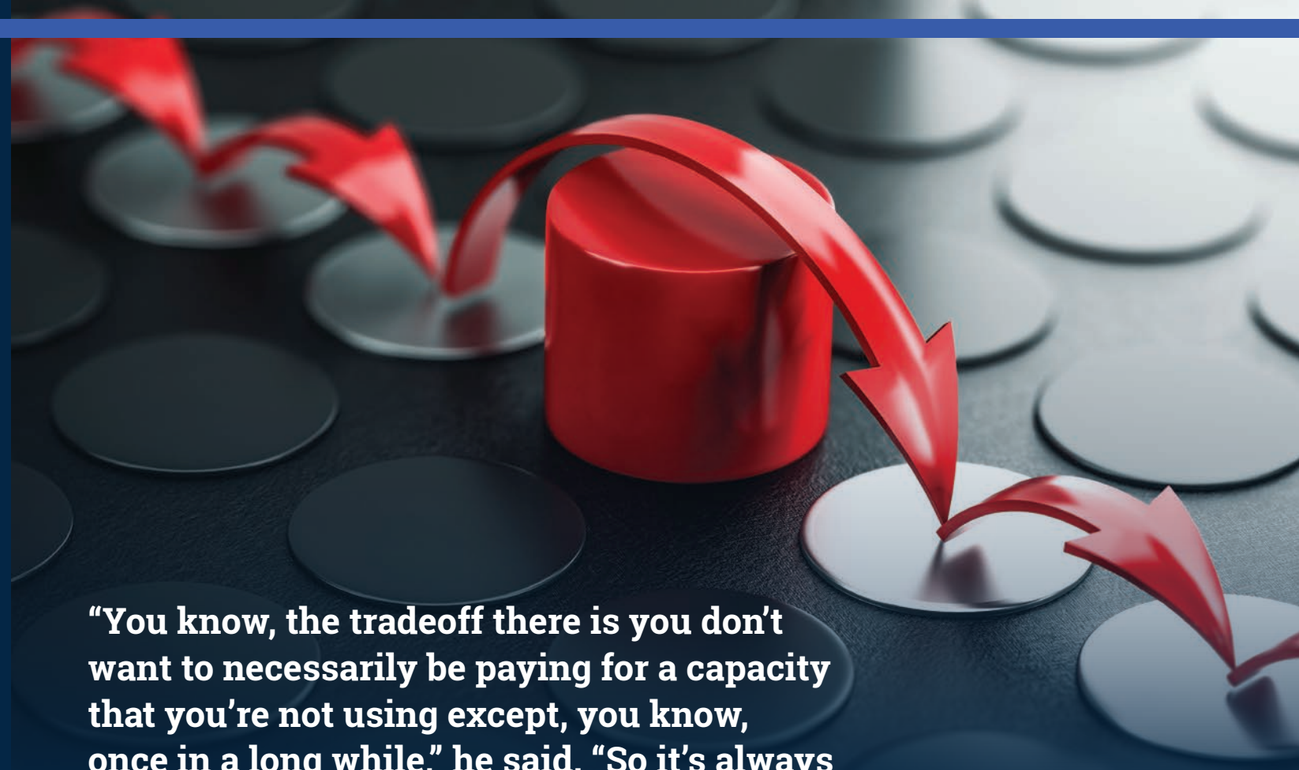
- VIJAY D'SOUZA, GAO'S DIRECTOR OF INFORMATION TECHNOLOGY AND CYBERSECURITY

Vijay D'Souza, GAO's director of Information Technology and Cybersecurity, said agencies have to consider their various business processes and what could impact them, then what can be done to offset those impacts and keep operations moving smoothly. A continuity of operations plan (COOP) should have HR, records management and payroll, but IT underlies all of those.

"They basically need to start out by identifying the risks to their systems," he said on Federal Monthly Insights — Operational Resiliency "I mentioned a natural disaster or it can be something like a pandemic — what you have to do is think about how each of those risks would affect each of the particular systems you have. Then what you need to do is you need to develop a mitigation strategy and figure out, you know, what would you do?"

Some options might be an alternate computing facility or cloud computing. But because cloud vendors have a variety of backup operations across multiple facilities, agencies must consider related staffing, D'Souza said.

"So, for example, if your staff were ill or unable to get to work, how would you run things? One of the things a lot of agencies are running into now is a lot of agencies are telework-friendly. There are certain IT functions that can only be done in the building, for example, maintenance, replacing equipment that fails, repairing things, applying certain patches. So that's a bit of a challenge," he said on Federal Drive with Tom Temin.



"You know, the tradeoff there is you don't want to necessarily be paying for a capacity that you're not using except, you know, once in a long while," he said. "So it's always a tradeoff as far as how much you want to pay for to keep that capacity in reserve."

- VIJAY D'SOUZA, GAO'S DIRECTOR OF INFORMATION TECHNOLOGY AND CYBERSECURITY

That's why, D'Souza said, having a disaster recovery or continuity of operations plan for each IT system is one of the federal IT security requirements.

That said, it's nearly impossible to plan for the scope and nature of pandemic until it happens. And although periodic testing is a requirement, D'Souza said that's difficult to accomplish at 100% capacity. But he said several agencies performed stress tests before moving to full telework.

"You know, the tradeoff there is you don't want to necessarily be paying for a capacity that you're not using except, you know, once in a long while," he said. "So it's always a tradeoff as far as how much you want to pay for to keep that capacity in reserve."

The other problem is that certain pieces of equipment for disaster situations are needed by everyone – web cams being an example this time around. D'Souza said he was lucky to have bought one coincidentally just before the pandemic, but for the rest of his agency they were few and far between. And having contracts with vendors to be on call in times of disaster is ideal, but when that situation occurs your agency will be one of dozens of customers asking for the same assistance simultaneously.

"So part of what you'll have to do as an agency is identify, kind of, what are your primary essential functions and then what are some things that could wait or be done later or done by alternative means?" he said.

Will the coronavirus be the push Congress needs to modernize long-standing inefficiencies?

BY AMELIA BRUST

It's doubtful that finding ways to conduct business during a global pandemic was high on the list of reasons for forming the Select Committee on the Modernization of Congress in 2019. But now, the timing could scarcely be more appropriate.

Proxy voting with or without quorum, video hearings, limiting member travel and maintaining social distancing at the Capitol have required lawmakers to reconsider the long-term viability of some well-established practices. For committee Chairman Rep. Derek Kilmer (D-Wash.), it meant picking up new skills quickly.

"I think there's a few different things at play. One, each member in their district is really active right now and has been through the course of this pandemic, in part, because there's a lot of holes in the dam," he said on Federal Monthly Insights — Operational Resiliency. "And I think most members of Congress and their staffs are trying to use every finger and every toe to plug those holes. Some of that is just doing really active case work with local businesses, or there's members of Congress, myself included, who become procurement professionals, when it comes to personal protective equipment, and testing capacity."

"Some have moved to more of a total virtual element, or a hybrid of that where staff can come in one or two staff per day and sort of rotate through that, to maybe oftentimes not any staff throughout the week or work remotely."

— REP. TOM GRAVES (R-GA.), VICE CHAIRMAN OF THE MODERNIZATION SELECT COMMITTEE

He also said passing legislation for necessary resources such as the Paycheck Protection Program is pressing.

But so is oversight, especially as trillions of federal dollars go out the door to businesses and individuals in the form of stimulus checks and unemployment. Kilmer and Rep. Tom Graves (R-Ga.), vice chairman of the modernization select committee, are also on the Appropriations Committee which is making use of virtual meetings.

But working from local district offices has not been easy either. Graves said it had been "a remarkable 90 days of adjustment and adaptation."

"We've seen in the district offices that every office has managed it a little bit different," he said on Federal Drive with Tom Temin. "Some have moved to more of a total virtual element, or a hybrid of that where staff can come in one or two staff per day and sort of rotate through that, to maybe oftentimes not any staff throughout the week or work remotely."

Getting around limited Wi-Fi and a dependency on Ethernet was a major challenge for district offices, he said members found, leading some staff to use their phones as hot spots.

For members who need to hold virtual town halls, Kilmer said, the question arose of Congress bulk purchasing video conference subscriptions to keep constituent communications open.

"You've seen the Executive Branch, implement some innovations during the pandemic where Congress could also take action. So for example, the requirement for wet signatures, obviously, when members of Congress are dispersed all over the country, that's pretty tough," Kilmer said. "And so looking at accelerating the use of digital signatures is something that Congress so far has not really taken advantage of, and I think is something that will require a look and may likely see a recommendation from our committee."

Meanwhile, the select committee has suggested easier tracking of legislation and members' voting records to improve transparency.

Until a vaccine for the coronavirus is found, Kilmer said it's unlikely all 435 members of Congress and their staff will return to the Capitol together. But with the select committee set to end this year, Kilmer said getting its recommendations to the larger body "can't wait."

"You've seen the Executive Branch, implement some innovations during the pandemic where Congress could also take action. So for example, the requirement for wet signatures, obviously, when members of Congress are dispersed all over the country, that's pretty tough."

— REP. DEREK KILMER (D-WASH.), CHAIRMAN OF THE MODERNIZATION SELECT COMMITTEE

HOW TO ACHIEVE OPERATIONAL RESILIENCY

THIS CONTENT AS BEEN PROVIDED BY VERITAS AND CARAHSOFT

Federal agencies and the people who staff them have had a crash course in how to keep operating effectively when a totally unexpected situation arises suddenly. What some of observers had referred to as a "black swan" event.

The pandemic has shown the importance of continuity of operations plans (COOP), and that they be tested and revised periodically. It has shown the importance of a robust and adaptable information technology infrastructure, and of how cybersecurity defenses must also be flexible and adaptable.

If you add up these factors, they amount to a more holistic concept that encompasses COOP, virtual private network capacity, and cybersecurity. You might call it operational resiliency.

"Operational resiliency really refers to the concept of any enterprise organization being ready to execute on its mission," says Alex Restrepo, senior principal for solutions marketing at Veritas.

He spoke as part of a discussion along with Scott Sloan, Veritas senior director of sales engineering for U.S. public sector, in a discussion with Federal News Network.

Restrepo said a given agency faces three potential impediments to its ability to reach its mission outcomes.

- Complexity of the IT environment itself. When organizations add new applications and data sources, they often layer new technology on existing, thereby multiplying the potential conflicts that can interrupt IT services. Another growing complexity factor is adoption of multiple commercial cloud services, along with continued operation and enhancements of agency data centers.

- Constantly morphing cybersecurity attacks. For instance, the sudden move to mass teleworking has caused a new wave of expertly-crafted phishing and ransomware attacks.

- Sudden unknown occurrences. "The unknown things like the current pandemic is an example of the unknown impacting business," Restrepo said.

"If I don't have good visibility into my entire infrastructure, it's very difficult for me to pivot and be agile in the face of changes like we're seeing right now."

– ALEX RESTREPO, SENIOR PRINCIPAL FOR SOLUTIONS MARKETING AT VERITAS

Sloan pointed out that while so far agencies have escaped crippling ransomware attacks, state and local agencies have not been so lucky. He cited the attack on Baltimore a year ago. The ransomware demand for the city's access to its data was $76,000.

"But they decided not to pay. This decision cost the city at least $18 million," Sloan said, adding it was a combination of the costs to restore its systems and of lost fees revenue while city business stopped.

Keeping resilient

Resiliency is more than the ability to steer around cyber attacks and respond to events like the pandemic or the more-frequent lapses in funding from Congressional logjams, according to Sloan and Restrepo.

A change in charter or regulation can also force a scramble. Nearly every year, for example, Congress tweaks and sometimes radically overhauls the tax code. That forces the need for rapid and reliable changes in IRS systems. The Small Business Administration faced two big changes at once. Not only did its people have to suddenly telework, but it also got a trillion-dollar assignment under the Payroll Protection Plan.

How to deal?

Fundamentally it requires visibility into your own infrastructure and into the nature and location of data.

"If I don't have good visibility into my entire infrastructure, it's very difficult for me to pivot and be agile in the face of changes like we're seeing right now," Restrepo said.

Secondly, and related to visibility is the ability to change the infrastructure, move data and applications around in failover situations, in some automated or orchestrated way. Planning for resiliency here will quickly reveal the complexity of an environment.

"Agencies thought they could do massive replacements of technology like moving everything to the cloud. But what we've been seeing is way more adding of technology than replacing it."

– SCOTT SLOAN, VERITAS SENIOR DIRECTOR OF SALES ENGINEERING FOR U.S. PUBLIC SECTOR

"You want to make sure you have good orchestration tools that are able to take into account the environment. And then move it non-disruptively when necessary," Restrepo said.

Technologies such as virtualization and containerization can aid the movement of workloads and dealing with sudden changes in demand.

Resiliency planning can also aid in another government-wide imperative, namely modernization. Removing complexity should be a component of modernization, Sloan said.

"Agencies thought they could do massive replacements of technology like moving everything to the cloud. But what we've been seeing is way more adding of technology than replacing it," he said. "The result can be a tangle of overlapping and redundant systems that cost money, slow innovation and hinder the agencies from identifying new mission opportunities."

NAVSEA keeps work on ships, fleet moving amid social distancing

BY AMELIA BRUST

The Navy operates with a fair amount of open space, namely the world's oceans. But even the service wasn't immune from challenges around workforce social distancing due to the coronavirus pandemic. The problem was particularly timely for the Navy's IT workforce.

Mike Sydla, the division director for Information Management Resources Logistics, Maintenance and Industrial Operations at Naval Sea Systems Command headquarters, said keeping everything moving has meant embracing a new mindset but also keeping some workers in shipyards to continue fleet work.

"Right now at the Naval shipyards, we have about 45,000 employees daily working on carriers and submarines, getting them up and ready to go for the nation," Sydla said on Federal Monthly Insights — Operational Resiliency.

"A lot of things that we've said we'd never do, we realized we could do, and we're now embracing that new change and technology — particularly the remote operations."

— MIKE SYDLA, DIVISION DIRECTOR FOR INFORMATION MANAGEMENT RESOURCES LOGISTICS, MAINTENANCE AND INDUSTRIAL OPERATIONS AT NAVAL SEA SYSTEMS COMMAND HEADQUARTERS

He called it a "finely orchestrated dance." When a carrier comes into dry dock and Sydla's team begins working on it — that means about 10,000 employees are coming in and out at any given time. He must make sure they're at the right place with the right tools and doing certified work so that the ship can get out and rejoin the fleet as soon as possible.

"So it is technically impossible not to do this with the IT tools — the scheduling tools, the planning tools, material tools — that we bring to the table. And so our goal as part of this organization is not only just to keep what we're doing but to increase the productivity" he said on Federal Drive with Tom Temin. "If we can increase it by 20%-to-30%, that's a big savings but also more importantly, it gets those aircraft carriers or submarines back to the Navy, to be deployed."

NAVSEA is one of five systems commands in the Navy and is responsible for planning of buying ships, purchasing ships, maintaining and eventually disposing of them. Sydla said about $30 billion is flowing through the process at any given time, while the $9.7 billion industrial operations in particular focuses on sustaining assets such as submarines, carriers and surface fleet.

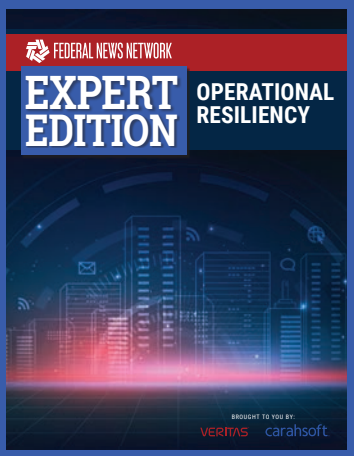
But little of this is easily conducive to telework. NAVSEA let employees in overhead positions telework for the first time due to COVID-19, and staff made greater use of online collaboration tools. Waterfront workforces have remained on site every day, but Sydla said they've done well to isolate themselves and practice social distancing while getting ships out.

"A lot of things that we've said we'd never do, we realized we could do, and we're now embracing that new change and technology — particularly the remote operations," he said. "It was something that I didn't think the mindset would ever change because a lot of folks are like, 'I can't guarantee people are working unless I see them.'"

Now more ideas for distance support are emerging. The IT team used managed services to get people from the operations center working remotely, aside from a few people to come into the office and reboot servers or perform other tasks. Sydla said they looked at the procurement tools they had purchased and finally said, "okay, it's time to move forward."

"And so our goal as part of this organization is not only just to keep what we're doing but to increase the productivity" he said on Federal Drive with Tom Temin. "If we can increase it by 20%-to-30%, that's a big savings but also more importantly, it gets those aircraft carriers or submarines back to the Navy, to be deployed."

— MIKE SYDLA, DIVISION DIRECTOR FOR INFORMATION MANAGEMENT RESOURCES LOGISTICS, MAINTENANCE AND INDUSTRIAL OPERATIONS AT NAVAL SEA SYSTEMS COMMAND HEADQUARTERS


FEDERAL NEWS NETWORK
EXPERT EDITION
OPERATIONAL RESILIENCY
BROUGHT TO YOU BY:
VERITAS
carahsoft