

carahsoft®



ΕΙΣΑΓΩΓΗ
ΣΤΗΝ ΕΛΛΗΝΙΚΗ
ΕΠΙΧΕΙΡΗΣΙΑΚΗ
ΕΚΔΟΣΗ ΤΗΣ
ΕΠΙΧΕΙΡΗΣΙΑΚΗΣ
ΕΚΔΟΣΗΣ ΤΗΣ
ΕΠΙΧΕΙΡΗΣΙΑΚΗΣ
ΕΚΔΟΣΗΣ ΤΗΣ

Thank you for your interest
in exploring this content.

Carahsoft is the **Trusted Government IT Solutions Provider**® supporting a broad portfolio of industry-leading technologies through NASA SEWP V, GSA MAS and a wide range of other contract vehicles.

As the **Master Government Aggregator**®, Carahsoft connects government agencies, industry partners, and technology providers to deliver innovative, mission-focused solutions.

In partnership with Cisco, we provide technology solutions that drive modernization, strengthen operations, and ensure compliance with evolving government standards.



To learn more about how Carahsoft can support your technology needs, please visit carahsoft.com



Explore More Resources:
carah.io/ciscoresources



Join Events & Webinars:
carah.io/ciscoevents



Discover Technology Solutions:
carah.io/cisco



Learn About Procurement:
carah.io/ciscocontracts



Connect With Our Team:
Cisco@carahsoft.com
(571) 590-7300

Cybersecurity Beyond IT

Why Operational Readiness Matters for Government Leaders

Cybersecurity is no longer just an IT responsibility—it is now central to operational resilience, continuity of government services, and public trust. In a recent interview with State Gov Today, Cisco Cybersecurity Executive Advisor Helen Patton discussed why cyber resilience has become a leadership issue for government organizations.

Cyber incidents now have the potential to disrupt emergency response systems, transportation networks, utilities, and other critical functions that communities rely on every day.

During large-scale events or cyber incidents, operational readiness depends on coordination across agencies and critical infrastructure providers. The ability to share information and coordinate responses quickly can make the difference between maintaining services and widespread disruption.

Cybersecurity Now Directly Impacts Government Operations

For government agencies, cyber incidents can directly affect public safety and critical operations. Ransomware attacks have shown how quickly public services can be affected when systems go down.

As Patton emphasized during the discussion, cybersecurity decisions now directly influence operational continuity and public confidence,

making cyber resilience a leadership responsibility, not simply a technology concern.

That shift is also changing the role of cybersecurity leaders. Chief Information Security Officers (CISOs) and security teams are increasingly expected to translate technical cyber risks into business and mission impacts that executive teams can act on—from service disruption and recovery timelines to continuity of operations.

“Cybersecurity incidents are no longer just technology events—they are operational events that directly affect public trust and service delivery.”

Operational Readiness Depends on Coordination

During a cyber incident, success often depends on relationships built long before the crisis. Organizations must be able to communicate quickly and coordinate response efforts while keeping essential services running. In government, that can mean ensuring 911 systems remain available, public systems stay online, and agencies continue operating during disruption.

Coordination often extends across federal, state, local, and private sector organizations, including municipalities, schools, and critical infrastructure providers. However, many organizations still struggle to define clear coordination roles during

cyber disruptions, slowing response when speed and collaboration matter most.

Shared intelligence and faster reporting improve threat visibility and help states support local entities more effectively. Because government organizations operate differently from the private sector, operational resilience depends heavily on the ability to work together under pressure. Trust plays a critical role in enabling that coordination.

AI Can Strengthen Cyber Defense, but Human Judgment Still Matters

AI-enabled security tools are helping organizations improve visibility, accelerate threat detection, and ease pressure on overstretched teams. For government agencies facing workforce shortages and increasing operational demands, AI and digital workers can help security teams operate more efficiently.

At the same time, AI is reshaping the cybersecurity landscape and introducing new risks that require careful oversight. Public sector leaders are paying closer attention to the accuracy of AI-generated information and whether these tools can be trusted in real-world situations. As a result, agencies are placing greater emphasis on responsible AI deployment and built-in governance and security.

Patton stressed that human judgment remains essential, especially when decisions affect critical public systems, constituent services, or safety outcomes.

"AI can improve speed and visibility, but leadership still depends on people making informed decisions in moments that matter."

AI can help identify patterns and accelerate response efforts, but it cannot replace the judgment and operational context needed during high-stakes situations.

Building Resilience for the Future of Government

State and local government leaders are under increasing pressure to maintain secure, uninterrupted services while modernizing operations and adopting AI technologies.

Agencies are now expected to maintain operational continuity while preserving public trust during disruption. As threats evolve, balancing innovation with human oversight will remain essential to cybersecurity leadership.

Cisco helps public sector organizations strengthen operational resilience through secure infrastructure, improved visibility, and AI-enabled security designed to support uninterrupted government operations and public trust.

Watch the [full conversation](#) with Helen Patton to learn how government leaders can strengthen operational readiness, improve cyber resilience, and support uninterrupted constituent services.

Contact us to learn more: Cisco@carahsoft.com.