Symantec by Broadcom | Carbon Black. by Broadcom | carahsoft

FEDInsider

SPECIAL FEATURE

Doing More With Less in Federal Cybersecurity

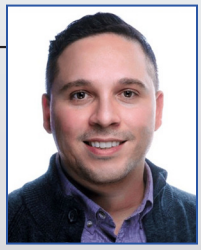
A **March 2026 Forrester Consulting study** highlights how budget cuts, staffing shortages and evolving threats are forcing agencies to rethink how they defend and respond.

Featured Experts:

- **Keith Busby**
  Acting CISO & ISPG Director,
  Centers for Medicare & Medicaid Services

- **Richard Verwers**
  Federal Sales Director, Broadcom Business,
  Carahsoft

- **Carlos Rivera**
  Senior Analyst,
  Forrester



Federal agencies are under pressure to sustain cybersecurity operations with tightening budgets and workforce reductions, even as threats grow more sophisticated. Insights from a recent Forrester Consulting study, commissioned by Carahsoft and sponsored by Broadcom, found that 52% of respondents cite budget constraints as having a moderate or significantly negative impact on their department's ability to maintain core security operations. They also attribute staffing shortages to their current level of operational strain (56%), forcing agencies to rethink priorities across network security, data protection and incident response.

During a recent **FedInsider webinar**, government and industry experts were joined by a guest Forrester senior analyst to discuss key study findings and how agencies are addressing today's cybersecurity challenges.

The State of Cybersecurity in the Government

Forrester Consulting's recent study, *"Smarter Security for Leaner Budgets and Teams: The Tech Transforming US Government Operations*". It surveyed over 200 cybersecurity decision-makers in various agencies following the Department of Government Efficiency's reductions in budget and resources.

The study revealed three major breaking points for agencies: security operation coverage gaps, workload growth and the impact on incident readiness. "Security teams will be operating with a tighter budget, experience lower hiring and they will see an increase in demand," said Carlos Rivera, Senior Analyst at Forrester.

This will create gaps in cyber expectations in terms of coverage, the speed to remediate incidents, compliance and more. These factors will be weighed against the agencies' capacities to meet expectations based on the resources available.

Richard Verwers, Federal Sales Director for Broadcom Business at Carahsoft, is seeing this first-hand. "We are hearing consistently from agencies that they need to do more with less, and do it smarter," Verwers said. "Since last year, budget and headcount reductions mean agencies operate in a reality where resources are constrained."

Verwers said federal customers are also actively trying to reduce tool redundancy that contributes to operational strain, and they often don't have a unified picture of their environment – making it harder to prioritize risk.

Forrester's study also found staffing shortages to be one of the top factors contributing to operational strain. Verwers said this is driving a push to automate repetitive tasks like alert triage and policy enforcement something that can make up for lower staffing levels if deployed correctly.

"Agencies are being much more intentional about focusing on high-impact areas like network security, data protection and incident response. Agencies are not just trying to do everything better, but also doing things more effectively," said Verwers.

At the Centers for Medicare and Medicaid Services (CMS), this means cyber resilience has become more of a mission – shifting the conversation from just preventing each incident and remediating every vulnerability, to ensuring that critical services continue even when something goes wrong.

"We acknowledge we have limited resources like everyone else," said Keith Busby, Acting CISO and ISPG Director for CMS, "forcing us to be more disciplined from a priority standpoint, ensuring that we are focusing on high-value assets, the most critical systems and all of the sensitive data that we have."

That means reducing tool sprawl, addressing major vulnerabilities and exploits first, prioritizing zero trust principles, securing users and modernizing systems with a "secure-by-design" approach.

Operating Safely with Constrained Resources

The overwhelming sentiment in Forrester's survey is that operational strain is being driven by staffing shortages, budget limitations and the lack of cross-functional alignment within organizations, Rivera explained.

Throughout the study, four top challenges were cited: severe workforce reduction, lower morale driving institutional stability, disruption of core services and operational paralysis. These challenges compound operational gaps and existing security problems. “All of that leads to fewer improvements which increases the chance of incidents, but it’s also increasing the amount of work for agencies,” Rivera said.

And it’s not a lack of technology causing problems, but rather, having the right technology operating in a way that reduces workload instead of adding to it, Verwers said. “Most agencies we work with have a strong security stack. But as the study points out, complexity, tool sprawl, lack of integration and limited automation are major sources of operational strain.”

Instead of adding more tools, agencies must make existing tools more effective so that analysts spend less time managing their tools and more time responding to threats. At CMS, addressing those constraints starts with prioritizing high-value assets, critical assets and those with the agency’s largest pools of sensitive data. For example, any assets that would cause big impacts to citizens if they were knocked offline for 30 days now get fully prioritized.

“To protect those key areas, we are looking at what kind of shared enterprise security services we can offer and leverage. Not every system needs a specific, unique security tool. We can lean into toolsets that we can offer across the entire agency to protect them equally,” said Busby.

Doing More with Less: How to Move Forward & Secure Systems

Based on Forrester’s findings, the study provided solutions that position these constraints as an opportunity for agencies to reassess cybersecurity strategies and prioritize high-impact initiatives – like streamlining investments, turning to automation and strengthening cross-functional collaboration.

Rivera said agencies should also be on the lookout for signals that can indicate internal organizational problems, like increases in turnover or backups in logging activities. “There is an opportunity for all organizations to do a natural self-assessment – to take a step back and not let the tools drive your strategy,” he said.\The strategy of CMS includes focusing on bringing in the right resources to support the technology and the processes needed. “If we bring something in for security and we don’t ensure it’s the right fit or think through how we will deal with the information coming out of it – then we have to ask if it’s meeting the capability we brought it in for,” Busby said. “Throwing money at a problem rarely fixes the problem; it just creates a more expensive problem.”

Busby’s advice is to be intentional. Fail fast and learn as you go. “Also, getting the right people to help you will make it all right,” he added.

And when it comes to simplifying and getting the right technologies in the right place, panelists agreed that the key was to start small and strategic. Organizations should first assess, take inventory and document everything. “In order to defend yourselves accordingly, you need to assess your current stance, inventory all of the assets and technologies you have in place today, and document it effectively,” Rivera said.

Communication is also key – making sure IT, security, operations and program leaders all understand the same risks and priorities. Forrester’s survey revealed that 81% of respondents believe that cross-functional collaboration could be helpful in addressing current cybersecurity challenges, and 82% of respondents emphasized the importance of leadership transparency.

“Many security challenges are not purely technical but organizational,” Verwers said. “Because if everyone is not aligned on priorities, you end up with fragmented efforts.” Communication and having a shared view of risk and data can also help agencies respond to an incident quickly and effectively. Establishing cross-functional governance models can also ensure everyone is working towards the same outcomes.

This is true organizationally and across government. Shared strategies, information and processes can help streamline federal cybersecurity practices, especially under resource constraints. “Even the best technology will not deliver value if the teams are not aligned in how they use it,” Verwers said.

Overall, the discussion showed that doing more with less in federal cybersecurity is not simply a matter of cutting costs or asking smaller teams to work harder. It requires agencies to be far more deliberate about what they protect first, how they reduce complexity and where automation and shared services can create real operational value. In a threat environment that is only becoming more demanding, the agencies best positioned to succeed will be those that align people, processes and technology around the risks that matter most and build resilience through focus rather than sheer volume.

FEDInsider

Hosky Communications Inc.
3811 Massachusetts Avenue, NW
Washington, DC 20016
Contact: **John Hosky**

(202) 237-0300
Info@FedInsider.com
FedInsider.com
Facebook.com/FedInsiderNews
Linkedin.com/company/FedInsider
@FedInsider

Symantec. by Broadcom | Carbon Black. by Broadcom | carahsoft.

Carahsoft
11493 Sunset Hills Road, Suite 100
Reston, VA 20190
Contact: **Avery Reynolds**

(571) 662-3260
BroadcomBD@Carahsoft.com
Carahsoft.com/Broadcom
Youtube.com/user/BroadcomCorporation
Linkedin.com/company/Symantec
Linkedin.com/company/Carbon-B1ack
@Broadcom