SANS | Research Program

SURVEY

SANS 2026 Cybersecurity Readiness in Government Survey Insights:

Is the Public Sector Ready for the Next Cyber Threat?

Written by **Ryan Nicholson**
June 2026

Foreword

Government cybersecurity has never operated in a vacuum, and the pressures facing public-sector defenders today make that reality impossible to ignore. Budget cycles move slower than threat actors. Hiring processes struggle to compete with private-sector salaries. Legacy infrastructure predates the cloud architectures now central to mission operations. None of these are new problems, but they are compounding ones, and the gap between what agencies need and what they can consistently deliver is growing harder to close.

The SANS 2026 Cybersecurity Readiness in Government Survey was designed to take an honest measure of where government cybersecurity programs actually stand. Not where policy says they should be, but where practitioners on the ground report they are. The 20 years of direct experience in Department of Defense environments that I bring to this analysis (including roles in network security, cloud defense, and compliance auditing), shape what this report asks and how it interprets answers.

What emerges from the data is a picture of meaningful progress alongside persistent structural friction. Most agencies now have formal cybersecurity strategies and established governance frameworks. That represents real work, and it shouldn't be minimized. But governance alone doesn't stop threats. The harder challenge, which this survey documents in detail, is converting strategic frameworks into operational capabilities that actually function at scale, under resource pressure, with the workforce available.

The findings here are a resource for practitioners and leaders who need to understand where the gaps are, where peer organizations are investing, and where the path from mid-stage maturity to optimized operations runs through workforce development, automation, and integration rather than yet another strategic initiative.

The work of securing public-sector systems is consequential. The people doing it deserve a clear picture of the landscape. That's what this report aims to provide.

—Ryan Nicholson
SANS Senior Instructor

CURRENTLY TEACHING
SEC502: Cloud Security Tactical Defense

CO-AUTHOR OF
SEC541: Cloud Security Threat Detection

The Operational Gap

Most government agencies now have a cybersecurity strategy. The harder problem is executing it. Formal frameworks and governance structures are widespread, but consistent operational performance (the ability to detect, respond, and adapt at scale) remains the exception rather than the rule.

Key Findings

Cybersecurity Strategy Adoption Is Uneven

Although 55% of organizations report having a fully implemented cybersecurity strategy, nearly a third are still developing or updating theirs, and many lack consistent annual review practices.

Maturity Levels Skew Toward Mid-Stage, Not Optimized

Although 65% classify themselves as "Established" or "Advanced," only 22% consider their programs truly "Optimized," with roughly 30% still in early or development stages.

Funding Is a Major Constraint

Just one-third of organizations report that their programs are fully funded, while more than half report partial or insufficient funding, and 63% cite budget limitations as a primary barrier.

Workforce and Skills Gaps Persist

Staff training and awareness (41%) and threat detection and response (40%) are the most resource-constrained areas, and more than half of organizations struggle to recruit and retain qualified cybersecurity talent.

Operational Pressure Points Are Widespread

Threat detection and response, compliance auditing, and third-party risk management consistently rank as high-pressure functions, compounded by competing organizational priorities that hinder execution.

Governance and Prioritization Challenges Undermine Progress

Many organizations find it difficult to turn strategy into action, as conflicting priorities, unclear ownership, and inconsistent governance models hinder the progress of cybersecurity initiatives.

Executive Summary

Over the past decade, government agencies have made notable progress in formalizing cybersecurity governance. Strategic planning, policy frameworks, and oversight structures that were once inconsistent across agencies are now more commonly established. The SANS 2026 Cybersecurity Readiness in Government Survey provides a baseline assessment of how these programs are organized, funded, and managed across federal, state, and local levels. The survey collected responses from 417 cybersecurity professionals representing a wide range of roles, including security leadership, engineering, operations, architecture, and risk management (see demographics at the end of report).

The results reveal a cybersecurity landscape that has significantly matured at the structural level. Most organizations report having a formal cybersecurity strategy and established governance processes, indicating that cybersecurity is now widely recognized as a mission-critical function rather than just a technical responsibility. However, the data also highlights an ongoing gap between strategic intent and operational capability. Although many respondents classify their programs as established or advanced, relatively few report reaching optimized cybersecurity maturity. This suggests that government organizations have largely succeeded in creating the governance frameworks needed to manage cybersecurity risk, but often struggle to convert those frameworks into consistently effective operational performance.

Funding constraints and workforce shortages are the biggest barriers to closing this gap. Only a small percentage of organizations say their cybersecurity programs are fully funded, and more than half of respondents find it difficult to recruit and retain qualified cybersecurity professionals. These challenges directly affect areas such as threat detection, incident response, workforce training, and security awareness.

Overall, the findings show that **the main challenge facing many government cybersecurity programs is no longer creating a strategy, but sustaining the resources and operational capacity needed to execute that strategy effectively**. Focusing on workforce development, funding alignment, and operational integration will be crucial for agencies striving to move from basic cybersecurity efforts to fully optimized security operations.

Strategic Maturity Has Increased

Government cybersecurity programs have made significant progress over the past decade. What was once a chaotic and mostly reactive security approach across many agencies has gradually transformed into organized governance and strategic oversight. Survey results indicate that most organizations now have formal cybersecurity strategies and well-defined governance frameworks (see Figure 1). This demonstrates a broader shift in how cybersecurity is perceived within government sectors. It is no longer just a technical issue; it's a vital part of mission risk management.

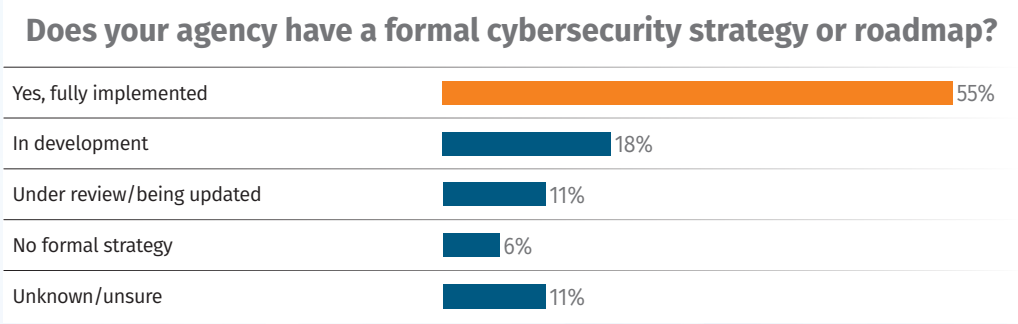

Figure 1. Cybersecurity Strategy

This level of strategic maturity shows notable progress. In earlier phases of building a cybersecurity program, organizations often focus on creating basic policies, defining roles and responsibilities, and establishing governance structures to guide security decisions. The widespread presence of formal strategies among respondents indicates that many government organizations have successfully advanced past those initial stages. Cybersecurity is now widely acknowledged as a leadership issue that requires ongoing planning, oversight, and coordination across technical and operational areas.

However, the data also shows that strategic maturity differs among government organizations. Many agencies say they have fully implemented strategies, but a significant number report that their strategies are still in development or being revised. This uneven progress reflects the complexity of modern government technology environments. Rapid changes toward cloud infrastructure, distributed workforces, identity-focused security models, and more advanced threat actors require organizations to continuously reevaluate how cybersecurity strategies are organized and carried out.

From an operational perspective, this pattern is typical. In many government settings, cybersecurity strategies must evolve along with broader modernization efforts, such as infrastructure upgrades, application migration to cloud services, and updates to identity and access management systems. As these efforts advance, cybersecurity strategies often need to be adjusted to deal with new risks and operational realities.

The broader implication is that government organizations have largely succeeded in establishing the governance foundations needed to manage cybersecurity risk. The remaining challenge is turning these strategic frameworks into consistent operational capabilities. Strategy alone does not improve security outcomes. Its value depends on organizations' ability to operationalize policies, processes, and technologies across complex environments. The next phase of program development should prioritize ensuring that current strategies are backed by operational capabilities that enable them to work effectively in practice, rather than focusing mainly on creating new strategic frameworks.

AUTHOR INSIGHT

Governance Is No Longer the Primary Barrier

Government agencies have made significant advancements in establishing cybersecurity governance. Strategic plans, policy frameworks, and oversight processes that were once inconsistent across agencies are now widely implemented. This shift reflects a broader understanding that cybersecurity risks directly affect mission continuity and public trust.

However, in practice, governance alone does not improve security outcomes. Many organizations now have clear strategies but struggle to turn them into operational capabilities that reliably detect and respond to threats. This underscores a common issue in cybersecurity development: Once governance structures are established, the main challenge is building the operational capacity needed to effectively carry out those strategies in complex environments.

Operational Capability Remains Uneven

Although strategic maturity has grown across government cybersecurity programs, the survey results indicate that operational capability has not kept pace. Most respondents rate their cybersecurity programs at an "Established" or "Advanced" maturity level (see Figure 2). These ratings generally reflect organizations that have implemented basic security controls, standardized policy enforcement, and established operational processes for managing cybersecurity risks.

However, few organizations report reaching an "Optimized" level of cybersecurity maturity. This gap highlights an important reality in government cybersecurity: Many organizations develop structured security programs but struggle to move beyond that to highly integrated and adaptive operational models.

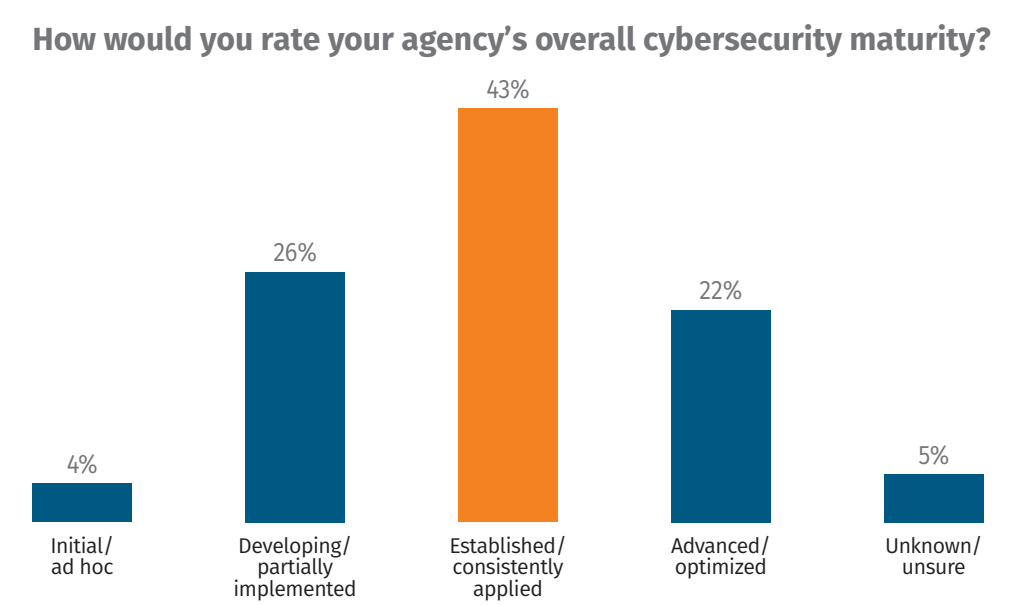

Figure 2. Maturity

Expert Corner

From the perspective of a cybercrime investigator who has worked intrusions, ransomware, and other forms of cybercrime, while supporting government organizations globally in building investigative and cybersecurity capabilities, these findings reflect what I consistently see across the public sector. Although progress has been made in governance and strategy, many organizations still struggle to implement effective security controls and align defenses with real-world threats.

A key gap is understanding cybersecurity as an adversarial problem. Many teams lack visibility into how attackers gain access, move laterally, and operate within compromised environments—as well as their motivations. As a result, they often misunderstand their true attack surface. Without that perspective, security efforts remain reactive and misaligned.

The most effective public sector teams invest in developing their workforce to think like attackers, then implement attacker-informed detection, response, and evidence-driven operations. Building that understanding at scale is critical to moving beyond mid-level maturity.

Conan Beach
SANS Certified Instructor Candidate

COURSE CO-AUTHOR

FOR589: Cybercrime Investigations

VIEW PROFILE

Transitioning from established cybersecurity programs to optimized security operations requires more than just policies and governance. Optimized environments usually feature seamlessly integrated security tools, automated detection and response processes, and advanced analytics that enable organizations to quickly and accurately identify and address threats. Achieving this level of maturity also relies on well-developed security operations centers, ongoing threat intelligence integration, and the ability to continually refine defensive strategies based on evolving threat activity.

In practice, developing and maintaining these capabilities is difficult in many government environments. Outdated infrastructure, disconnected technology systems, and slow procurement processes can delay the implementation of new security technologies or prevent the full integration of existing tools. As a result, organizations may have multiple security measures that function independently rather than as a cohesive defense system.

Operational complexity also can lead to a maturity plateau. Government networks often support numerous mission systems, legacy applications, and distributed infrastructure environments that weren't originally designed with modern security integration in mind. Ensuring security visibility across these systems requires extensive coordination among engineering teams, security operations staff, and system owners.

These factors help explain why many cybersecurity programs stay at mid-level maturity. Organizations have successfully implemented governance frameworks and basic controls but have not yet achieved the operational integration needed for fully optimized security operations.

This plateau emphasizes the importance of focusing on operational integration rather than simply adding more standalone security tools. Many organizations already possess the technology necessary to detect and respond to threats effectively. The real challenge lies in integrating those tools into cohesive workflows that enable analysts to work efficiently and consistently across the enterprise.

Resource Constraints Limit Optimization

Across nearly every area of the survey, resource constraints remain the biggest obstacle to improving cybersecurity maturity (see Figure 3). Only one in three organizations considers its cybersecurity program fully funded. Funding shortages and workforce gaps consistently emerge as the main challenges facing government cybersecurity efforts, widening the gap between strategic goals and operational realities.

Budget constraints remain a significant challenge for many organizations. Although cybersecurity is widely seen as a mission-critical function, survey results show that only a small percentage of organizations consider their programs fully funded. Most respondents report operating with partial funding or limited budgets, often forcing security leaders to make tough decisions about technology investments, staffing, and modernization efforts.

This funding gap can have ripple effects on cybersecurity efforts. Limited budgets might delay replacing outdated infrastructure, slow down the adoption of automation technologies, or restrict organizations' ability to expand security operations. Over time, these limitations can force security teams to rely on manual processes or fragmented tool sets for tasks that could benefit from automation and integration.

AUTHOR INSIGHT

Why Many Programs Hit a Plateau at "Established"

Many cybersecurity programs reach a point where policies, governance, and baseline controls are well established, but making further progress becomes difficult. Moving from a solid program to a more advanced security stance requires deeper operational integration. Security tools need to operate as part of coordinated workflows, analysts must have the training and authority to act quickly, and detection and response processes must run continuously throughout the organization.

In government environments, this shift can be particularly difficult because of legacy infrastructure, fragmented technology systems, and procurement processes that hinder modernization efforts. As a result, many organizations depend on effective security technologies that are not fully integrated into a cohesive defense framework.

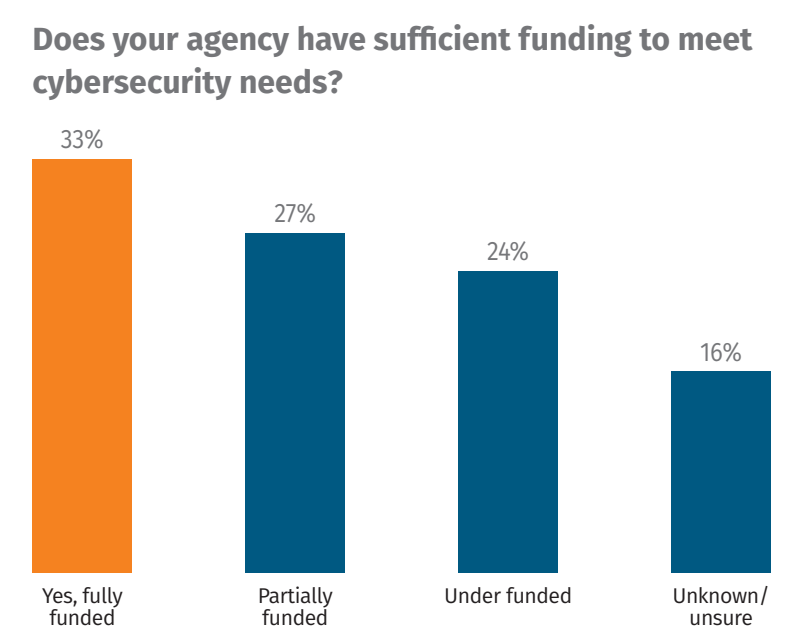

Figure 3. Funding

Partial Funding Is the Norm, Not the Exception

Only one in three organizations reports sufficient funding to meet cybersecurity needs. That means the majority of government security programs are making prioritization trade-offs every budget cycle—deciding which gaps to close and which risks to carry forward.

Workforce challenges present a major hurdle. More than half of respondents report difficulties in recruiting and retaining qualified cybersecurity professionals, emphasizing the broader talent shortage affecting the industry (see Figure 4). Government organizations face additional structural hurdles, including lengthy hiring processes, competition with private sector pay, and security clearance requirements that sometimes restrict the pool of eligible candidates.

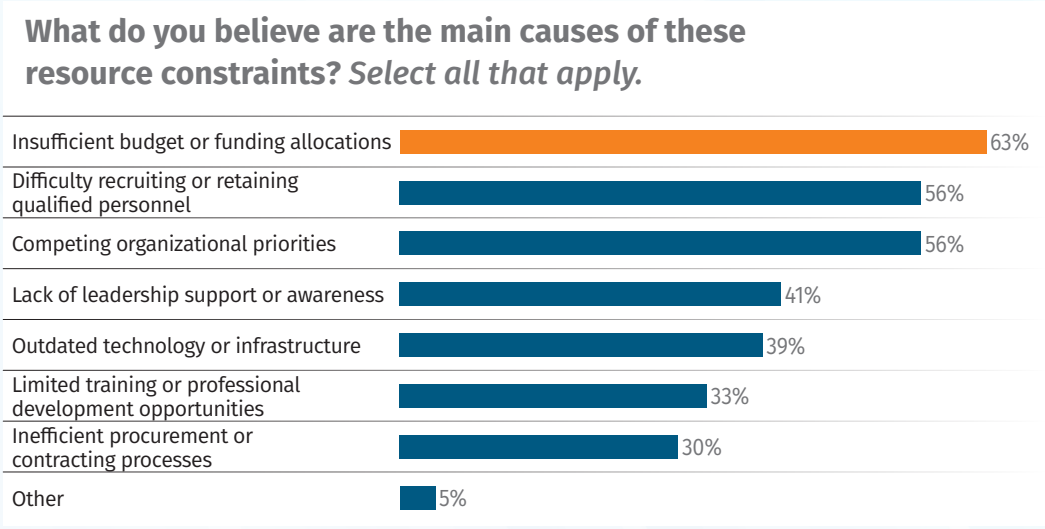

Figure 4. Causes of Resource Constraints

These workforce limitations directly impact operations. Security functions like threat detection, incident response, and security monitoring rely on skilled analysts to interpret alerts, investigate suspicious activities, and coordinate responses across teams. When staffing is constrained, organizations may struggle to maintain consistent monitoring or respond quickly to emerging threats.

The survey results highlight this trend by pointing out training and awareness programs, along with threat detection and response capabilities, as areas where organizations face the biggest resource challenges (see Figure 5). Both functions depend heavily on skilled personnel and ongoing investment in workforce development. Without enough staffing and training resources, even well-designed security systems can fall short of their full defensive potential.

AUTHOR INSIGHT

Workforce Capacity Defines Operational Capability

Technology alone cannot sustain effective cybersecurity operations. Detection, response, and threat analysis depend heavily on skilled personnel who can interpret data, investigate anomalies, and coordinate defensive actions across multiple teams. When organizations face ongoing workforce shortages, these operational functions become more difficult to maintain.

Government cybersecurity teams often face structural hiring challenges, such as lengthy recruitment processes, competition with private sector pay, and clearance requirements in certain environments. Over time, these constraints can cause small teams to manage large, complex infrastructures. In these cases, security programs may stay compliant and uphold governance standards while still struggling to achieve the operational flexibility needed for quick, adaptable threat responses.

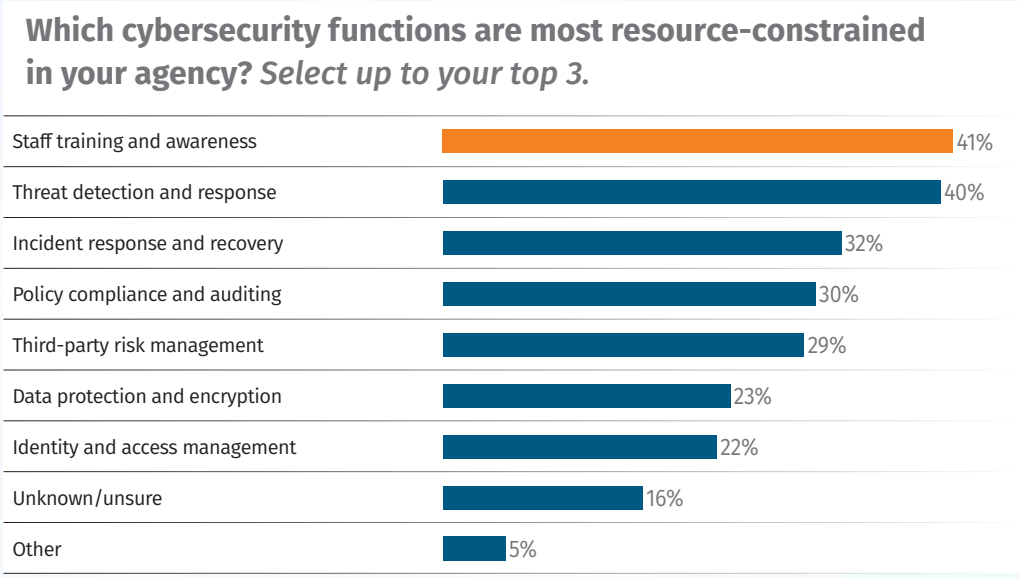

Figure 5. Resource-Constrained Functions

Taken together, these funding and workforce challenges explain why many cybersecurity programs stay at a mid-level maturity. Strategic frameworks might exist, but there are often not enough resources to fully implement them.

The implication is clear: The next stage of maturity will depend less on creating new cybersecurity strategies and more on securing the resources needed to effectively implement existing ones. Investments in workforce development, automation, and operational integration will be crucial in helping organizations move beyond current security programs toward fully optimized cybersecurity operations.

The Two Hardest Areas to Staff Are Also the Most Critical

Training and awareness and threat detection and response rank as the most resource-constrained functions in the survey. These aren't peripheral programs—they are the core of any functional security operation. Understaffing them doesn't just slow progress, it creates sustained exposure.

AUTHOR INSIGHT

Automation Is the Path to Operational Scale

As government environments grow more complex, security teams must monitor vast numbers of systems, applications, and user activities. Without automation, this workload can quickly overwhelm even the most skilled analysts. Automated detection, alert prioritization, and response orchestration let organizations strengthen their defenses while reducing the operational burden on security teams.

Automation doesn't replace skilled analysts. Instead, it allows them to focus on higher-value investigative and strategic tasks rather than repetitive monitoring. For organizations aiming to progress beyond mid-stage maturity, integrating automation into security operations workflows is typically the most practical way to achieve consistent and scalable cybersecurity defense.

Expert Corner

People, processes, and technology all play an integral role in formulating and successfully delivering on a forward-leaning strategic vision for any cybersecurity leader. Often underrepresented is leaning on the process lever as a means to offset budgetary challenges, workforce skills gaps, and other issues captured in the survey. Adversaries benefit from organizations that stovepipe and organizational leaders who are entrenched in the idea that their mission, datasets, and operations are so unique that sharing lessons learned, best practices, and threat insights cannot help provide collective defense across government organizations. Information sharing, collaboration, and partnership opportunities are easy wins that should be embraced.

John Doyle
SANS Certified Instructor;
Director of CTI Services
at Palo Alto Networks

VIEW PROFILE

COURSES TAUGHT

FOR578:
Cyber Threat Intelligence

Overall Assessment

The findings from the SANS 2026 Cybersecurity Readiness in Government Survey clearly show how cybersecurity programs across government agencies are evolving. Over the past decade, these agencies have made significant progress in building the fundamental structures needed to manage cybersecurity risks. Formal strategies, governance frameworks, and oversight processes are now common, reflecting a widespread understanding that cybersecurity is a mission-critical responsibility, not just a technical task.

The survey results also show that many organizations are still in a transitional phase of cybersecurity maturity. Although governance structures and basic controls are common, few programs have reached the level of operational integration and automation needed for fully optimized cybersecurity operations. Many organizations seem to operate at a mid-level maturity stage where policies and processes are in place, but operational capabilities are stretched across increasingly complex technology environments.

Funding limitations and workforce shortages significantly hinder bridging the gap between strategic intentions and operational capabilities. Security leaders are often tasked with modernizing infrastructure, enhancing threat detection, and supporting growing digital services despite tight budgets and limited staff. These challenges make it hard for organizations to fully implement cybersecurity plans or expand security operations to keep up with the complexity of modern government systems.

The survey results indicate that the next stage of cybersecurity maturity in government will rely less on creating new strategic frameworks and more on reinforcing the operational foundations needed to implement those frameworks effectively. Investments in workforce development, automation, and technology integration will be crucial for enabling security teams to function at scale.

If these structural challenges are addressed, many government cybersecurity programs are well positioned to transition from existing security measures to more adaptive and resilient defensive operations capable of responding to the changing threat landscape.

Strategy Without Capacity Is Just Documentation

The survey points to a consistent pattern: Organizations that have done the governance work are still falling short operationally because the resources to act on that governance aren't there. The bottleneck is no longer vision—it's execution capacity.

Demographics

To understand the state of the industry, this analysis draws upon data collected from the SANS 2026 Cybersecurity Readiness in Government Survey. All respondents work for a US government agency with 65% from Federal, 19% from State, 13% from Local, and 3% from other agencies. The top roles represented by respondents are Security Analysts or Engineers (29%) with the remaining from a variety of roles including IT Administrators, Information System Security Managers, and Cybersecurity Program Managers. The majority came from companies with 10,000 or more employees (31%), with a close follow from companies with 2,000 to 9,999 employees (19%). Lastly, numerous functions or services were represented: Defense/Homeland Security, Critical Infrastructure, Public Safety/Law Enforcement, Education, Utilities/Energy, Finance, Transportation, and Health and Human Services.

Sponsors

SANS would like to thank this survey's sponsors:

BROADCOM®

eset®

Google

tines

WIZ

SANS | Research Program

About the SANS Research Program

The SANS Research Program is a key initiative by the SANS Institute and a premier global provider of cybersecurity research and information. SANS Research Program is designed to provide cybersecurity practitioners and leaders with data-driven insights, thought leadership, and solutions that help them better understand and respond to evolving security challenges. All content is authored by SANS instructor experts from around the world who apply their years of experience from hands-on practitioner work in the field, advisory roles, and the classroom to provide education, guidance, and actionable insights that help make the cyber world a safer place.

To learn about sponsorship opportunities for research, content, and in-person or virtual events, email us at **Sponsorships@sans.org** or go to **www.sans.org/sponsorship**.

SANS | Research Program

Product Briefings for Cybersecurity Readiness in Government Survey

The 2026 Cybersecurity Readiness in Government Survey represents the latest edition of SANS Institute's poll of security professionals. The sponsors of this year's survey all offer advanced capabilities that we believe will be of interest to SANS' clients, and, for this reason, we're presenting the following product briefings on a relevant offering.

BROADCOM

SANS | Research Program

PRODUCT BRIEFING

From Strategy to Execution: How Broadcom Helps Government Agencies Close the Operational Gap

Insights from the 2026 SANS Cybersecurity Readiness in Government Survey

June 2026

The 2026 SANS Cybersecurity Readiness in Government Survey finds that most agencies have done the governance work. Formal strategies exist, frameworks are in place, and cybersecurity is widely recognized as a mission-critical function. What the data also shows is that governance alone has not translated into operational performance. The majority of government programs are stuck at mid-stage maturity, held back by funding gaps, workforce shortages, and tool environments that were never fully integrated. Broadcom's Symantec and Carbon Black portfolio was built for exactly this environment, bringing AI-powered prevention, endpoint detection and response, and application control together for the teams the survey describes.

The Operational Gap Is Real

The survey's central finding is one that government security leaders will recognize: Agencies have built the governance structures, but they cannot consistently execute against them. Only one in three agencies reports being fully funded. More than half report difficulty recruiting and retaining qualified cybersecurity professionals, while 39% point to outdated technology as a direct cause of their resource constraints. The qualitative responses describe agencies managing fragmented environments where security tools function independently rather than as a coordinated defense.

Key Findings

Most agencies are stuck at "Established" and cannot find the path to optimized.

65% of respondents classify their programs as "Established" or "Advanced," yet only 22% report reaching "Optimized" maturity. The survey is clear about what separates the two: integrated tooling, automated detection, and adaptive response capabilities. Symantec Endpoint Security Complete's AI-driven Incident Prediction feature, which has been trained on more than 500,000 attack chains, disrupts threats before damage occurs and delivers up to an 80% reduction in malware and ransomware risk, giving agencies a concrete path from "Established" to "Optimized."

Threat detection and response is underfunded in 40% of agencies, and the manual workload is compounding that gap.

40% of respondents identify threat detection and response as one of their top three most resource-constrained functions. When skilled staff is limited, slow investigation cycles make the problem worse. Carbon Black EDR provides continuous endpoint visibility and attack chain visualizations that let analysts understand how an incident unfolded and close the gaps that enabled it. Live response capabilities allow containment from anywhere, resulting in a 75% reduction in mean time to resolution (MTTR) that directly reduces the per-incident burden on understaffed teams.

Outdated infrastructure is preventing the operational integration agencies need most.

39% of respondents cite outdated technology as a primary cause of resource constraints, and the survey's qualitative responses describe agencies running disconnected tool sets that do not give analysts a unified view of their environment. Carbon Black Application Control enforces application trust across legacy-inclusive environments without requiring a continuously maintained hash library. The tool uses cloud-driven reputation, trusted publisher policies, and custom rules to keep what belongs running and stop what does not, reducing time spent reimaging machines and cleaning up malware by 75% each.

Broadcom's Symantec and Carbon Black portfolio does not assume an optimized security operation. The products are built to function in the constrained, complex, and legacy-inclusive environments in which government agencies actually operate, reducing the manual burden on small teams, extending the effectiveness of the analysts who are there, and providing the integrated visibility that fragmented tool sets have historically denied.

Platform Capabilities

Government security teams are also managing a volume problem that compounds every other constraint. When alert queues grow faster than teams can work through them, real threats get delayed or missed entirely, and analysts spend their shifts on noise rather than investigation. Broadcom's portfolio addresses this directly.

- **Symantec Endpoint Security Complete—**Symantec's Incident Prediction uses AI trained on more than 500,000 attack chains to identify and disrupt LOTL attacks and sophisticated threats before damage occurs. Machine learning and behavioral analysis differentiate between legitimate activity and real threats, delivering up to a 30% reduction in false positives so analysts are spending their time on confirmed incidents rather than noise.
- **Carbon Black EDR—**Continuous endpoint visibility, intuitive attack chain visualizations, and live response capabilities allow analysts to contain and remediate threats from anywhere. Carbon Black EDR reduces MTTR by 75%, directly cutting the per-incident workload that constrained government teams cannot currently absorb.
- **Carbon Black Application Control—**Symantec's trust-based application control works across complex, legacy-inclusive environments without requiring a maintained hash library. Cloud-driven reputation, trusted publisher policies, and custom rules keep authorized software running and unauthorized software stopped, reducing reimaging time and malware cleanup time by 75% each, saving 3,375 hours over a three-year span.

65% of respondents classify themselves as "Established" or "Advanced," but only 22% have reached "Optimized." Moving from mid-stage to optimized requires integrated tools and automated detection, not additional governance frameworks. Broadcom's portfolio provides the operational infrastructure agencies need to make that transition within the funding and workforce constraints the survey documents.

Request a Demo

https://engage.broadcom.com/ESG-contact-us