SHI | PUBLIC SECTOR

Research Study

New SHI study reveals the top 3 barriers in public sector cybersecurity

State and local government leaders offer candid insights into their latest IT challenges and investments.

Today's cybersecurity environment

The cybersecurity landscape is anything but simple. The increasing complexity of managing devices, workloads, and identities is compounded by the risk and volume of sophisticated security threats. Complicated, evolving attacks target vulnerabilities and require more advanced and agile cybersecurity solutions.

A 2023 SHI survey asked state and local government leaders across the U.S. to weigh in on pressing cybersecurity challenges – and the results are in.

From automation, funding, and visibility to legacy transformation and the security maturity journey, state and local governments face a growing demand to address cybersecurity concerns. The following study's insights will unveil the latest challenges, trends, and investments – and how your organization can solve what's next to bolster your security practice.

Discover what impacts state and local government cybersecurity, including:

- The greatest barriers to addressing their cybersecurity challenges.
- Their plans to fund cybersecurity staff and initiatives this upcoming fiscal year – and what changes are coming.
- Their need to secure funding and navigate grants.
- The increased investments in cybersecurity programs and projects in the next 12-18 months.
- The most-used cybersecurity frameworks and strategies.

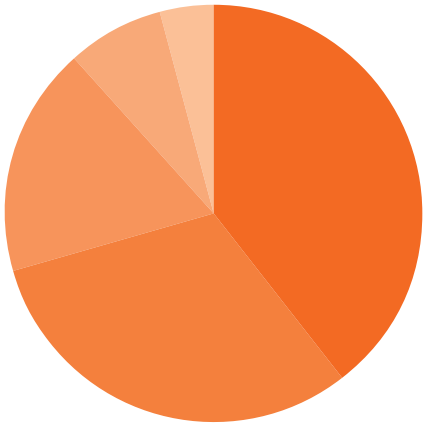
CONTENTS

Survey methodology

Conducted by the Center for Digital Government (CDG) in July 2023, the SHI national survey received 147 responses from state and local government leaders.

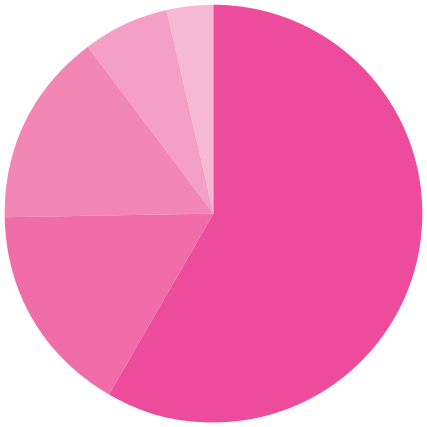
Most respondents represent decision-making, executive/senior management, or elected/appointed official roles.

Branch of government:



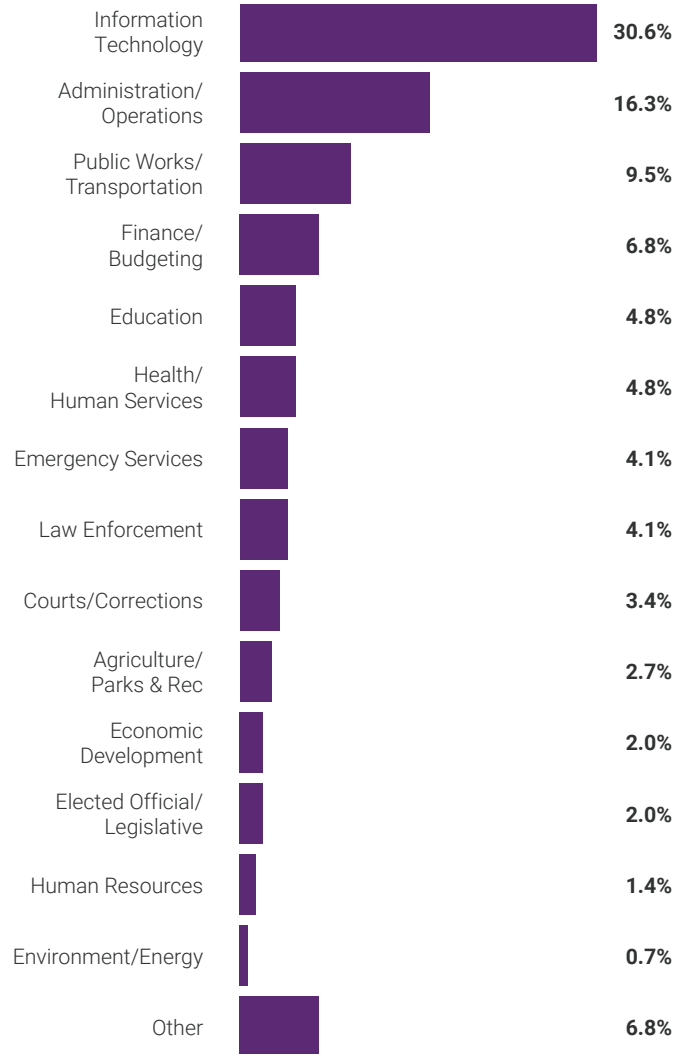
- **39.5%** City/town/village
- **31.3%** State
- **17.7%** County
- **7.5%** Special district
- **4.1%** Other

Job role:



- **58.5%** Executive/senior management
- **16.3%** Elected/appointed official
- **15.0%** Supervision/middle management
- **6.8%** Subject matter expert/non-manager
- **3.4%** Other

Agency or department function:



Critical barriers and challenges

When asked to identify the greatest barrier to addressing cybersecurity challenges, government leaders and IT executives revealed the top three obstacles.

36.1% of respondents said the growing complexity and sophistication of attacks were their greatest cyber barrier.

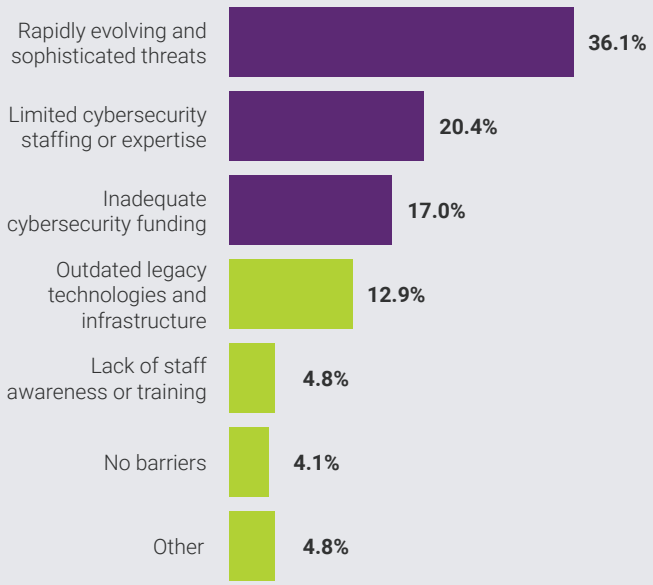
20.4% identified limited cybersecurity staffing or expertise as their biggest barrier to achieving their cybersecurity levels of service.

17% reported inadequate funding as a critical roadblock in their security journey.

The complex web of newly emergent vulnerabilities, an ever-expanding attack surface, and the technical, financial, and personnel restrictions placed on IT teams result in a cybersecurity environment that is difficult to secure and manage.

SHI Public Sector Senior Solutions Director Nick Casanova expands on the staffing challenge. “Not only can state and local governments not hire enough cybersecurity professionals, but they also have a very difficult time hiring contractors to fill the void,” said Nick. “This is because managed service contracts for staff augmentation are usually done at the state level with general pay-per-hour rates that are not in line or competitive with standard cybersecurity professional salaries.”

What is your organization’s biggest barrier to addressing cybersecurity challenges?



Critical barriers and challenges

When it comes to their current cybersecurity technology, the top challenge is managing growing devices, workloads, and identities – with nearly two-thirds (63.9%) of survey respondents selecting this answer. The results also showed that 37.4% of the government leaders struggled with complex solution deployment, tuning, and maintenance, while 32% lacked enough automation or had too many manual processes.

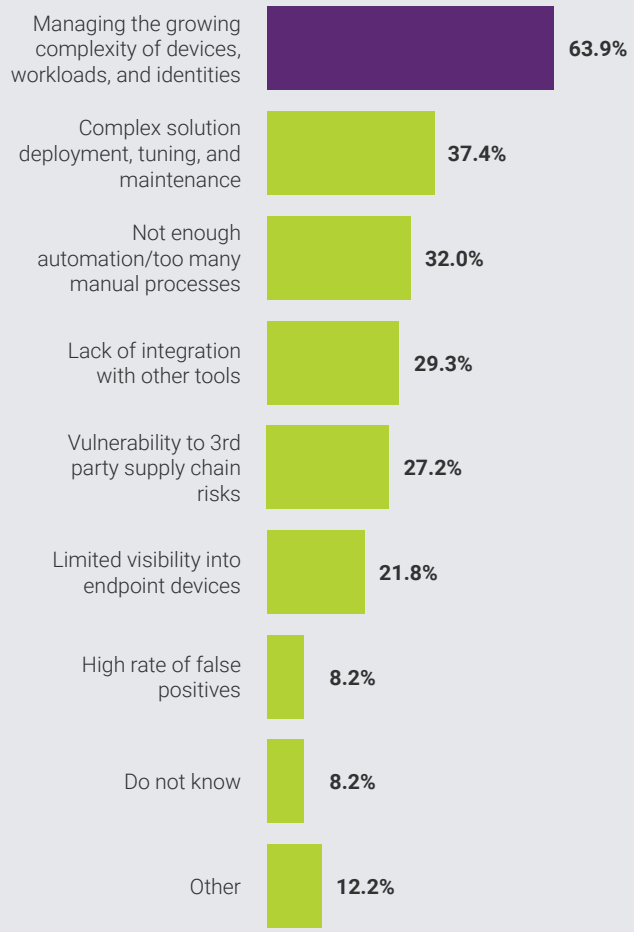
Additionally, about one-third of respondents chose lack of integration with other tools and vulnerability to third-party supply chain risks as leading challenges.

No longer seen as an isolated IT issue, government leaders recognize how interconnected cybersecurity functions are – touching tools, people, and processes across the organization. There is a pressing need to streamline and secure the many facets involved, including threat protection, improved automation, and training.

"Organizations are looking for help to make sense of that complexity and starting to really get the fact that everything is connected to everything else – and it's not going to go away," said VP of CDG and Governing Institute Todd Sander.

SHI Public Sector Field Solutions Engineer Steve Troxel adds, "We are now at a point where business leaders can't say they did not know about the cybersecurity risks of their actions."

What are your organization's top challenges with your cybersecurity technology? Please select up to 3.



The overall challenge can be summarized as complexity.

Evolving threats, limited staffing/expertise, proliferation of devices, and too many manual processes result in an environment that is difficult to secure.

The role of funding

Given the importance for cybersecurity technology, it's not surprising that funding plays a vital role in securing solutions and services in the public sector.

Respondents are most likely to use regular budget funding (78%) to fund cybersecurity staff and initiatives for the upcoming fiscal year. The data showed state respondents are much more likely to say they are relying on federal grants (33%) compared to counties (19%) and cities (9%).

Additionally, funding for the upcoming fiscal year was most often reported as either a slight increase (38.8%) or the same as the last fiscal year (28.6%). With less than 7% of respondents showing a decrease in cyber funding, the data emphasizes a growing business need for cybersecurity funding. SHI can help balance the mounting demand to address cybersecurity concerns and simultaneously maximize your budget to take these initiatives further.

Regarding budgets, many organizations are starting to ask the question: How much is enough? "They need to be really thoughtful about how much more they spend, especially now that they're rolling into the general fund approach to support cybersecurity," said Sander.

The modernization of technology is also likely to impact the conversation of how much to invest and where.

"Since we are at a more mature starting point for modern IT platforms and their capabilities, they frequently account for cybersecurity needs better," said Troxel. "This can make it easier for governments to meet cybersecurity controls today and is a great driver for application modernization. An example of this is native integration of platforms with multi-factor authentication products."

The disparity in security maturity will also impact where these funds go.

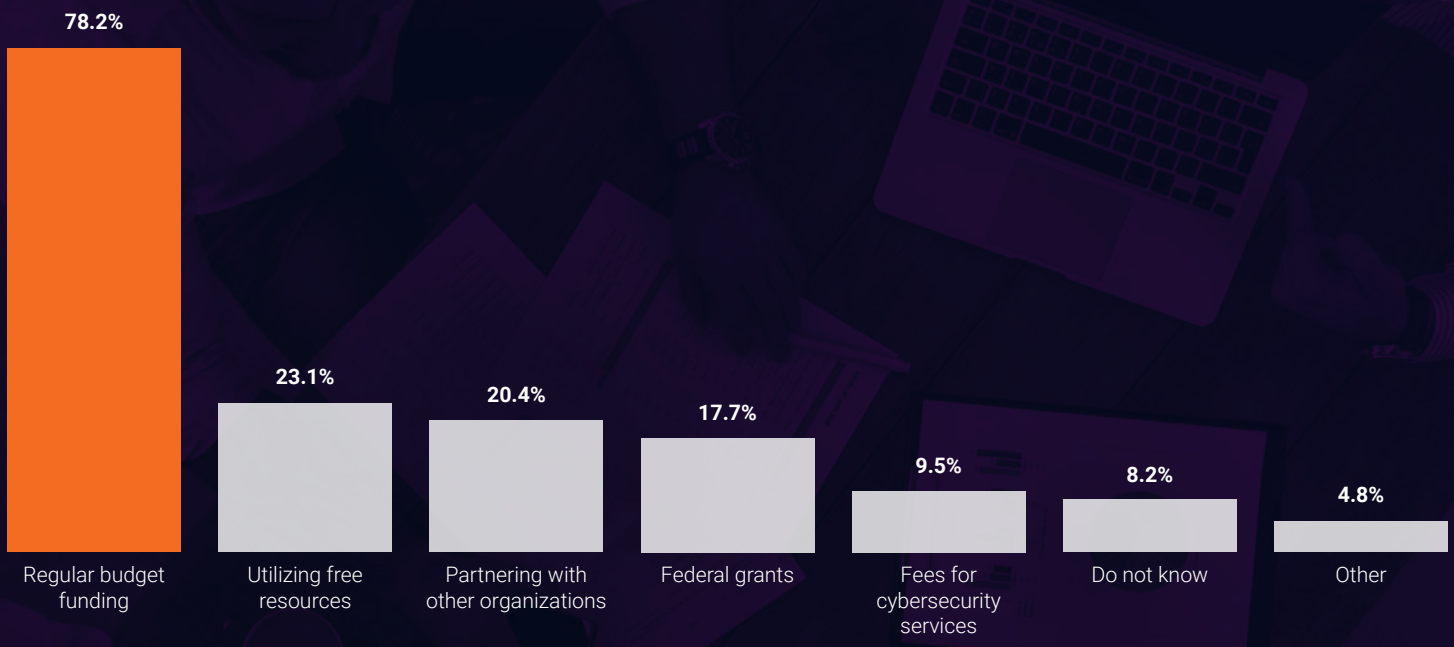
"While some organizations are still trying to catch up with establishing a basic package that addresses their needs, others that invested the most up to this point are considering: At what point do they get to the place where adding another dollar to cybersecurity spending doesn't equal another dollar's worth of improvement, protection, or benefit?" said Sander.

Cybersecurity funding needs continue to increase.

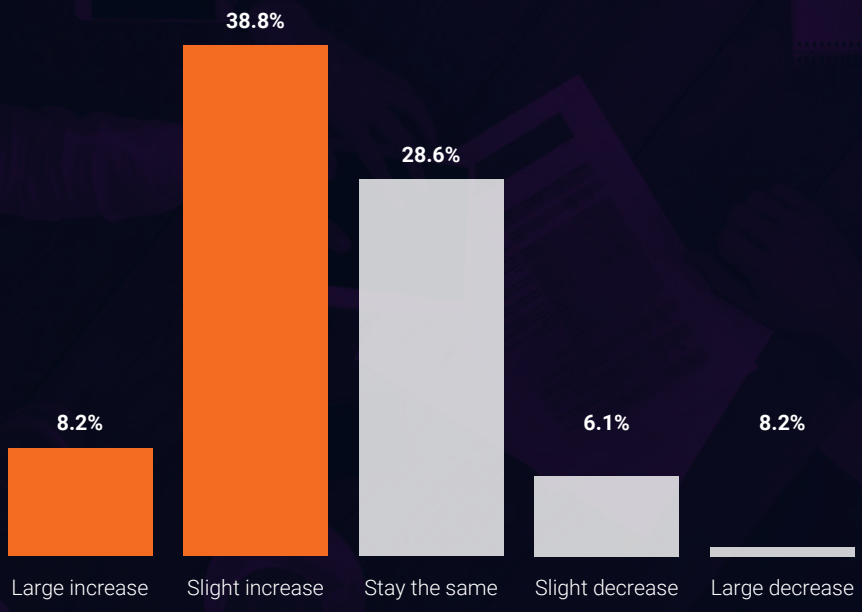
However, once most organizations establish baseline capability, the question of how much is enough will become more common.

The role of funding

How is your organization funding cybersecurity staff and initiatives for this upcoming fiscal year? Please select all that apply.



How will your organization's cybersecurity funding change for this upcoming fiscal year?



<7%

Less than 7% of respondents show a decrease in cyber funding

Learn how to maximize your budget and address cybersecurity concerns

Navigating grant funding

When asked where respondents need assistance in securing funding for cybersecurity, the following survey responses suggest nearly half of respondents are looking for support with grants. The data shows the majority needs help either identifying, securing, or managing grants.

Many state and local government leaders want to understand which grants they qualify for and gain awareness of available grants (45.6% and 44.9% respectively). Another leading answer showed that 36.1% of respondents needed assistance with applying for grants.

"Whether the grant programs are formula-based or proposal-based, state and local agencies must put NIST standards and federal requirements in place to qualify," said SHI Director of Growth Marketing Programs – Public Sector Robert Fass. "This is an area SHI's grants team has encountered, helping our customers align their plans and make sure they're complying with federal grants."

"We're seeing grants that have very specific stipulations around cybersecurity," agreed Troxel. "In some cases, to secure funding, you have to demonstrate that you have good cyber hygiene in the execution of that grant."

Navigating grant funding

The results also indicate the continual need to secure cybersecurity initiatives and the monetary requirements to reach a minimum level of protection.

"Governments have not gotten to the point with their general fund revenues or general fund appropriations to implement their full cybersecurity programs," said SHI Sr. Director of Government and Education Affairs Jeff Strane. "So, they're looking out for grant support as they need it, realizing they need to do something to fill the funding gap."

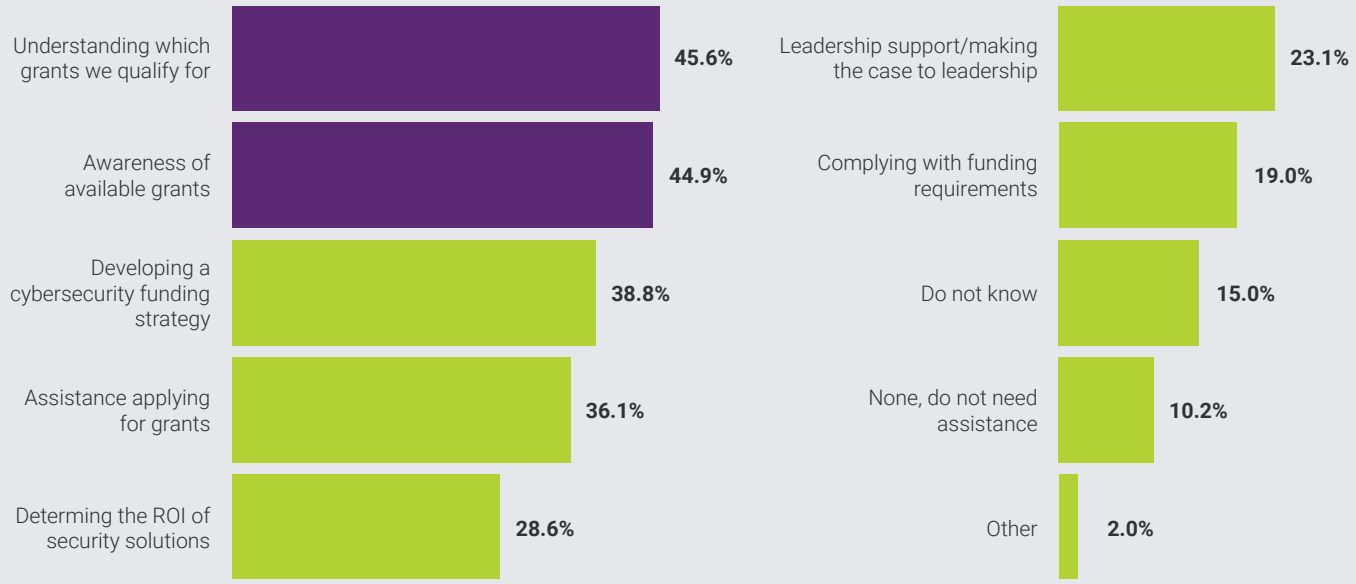
The focus on funding correlates with the earlier findings, where respondents said inadequate funding was a key barrier in addressing cybersecurity challenges. Grant funding can help state and local agencies close the gap and further their critical cybersecurity goals.

However, procurement plays an integral part in not only securing funding but also moving forward with cybersecurity investments at a pace and method that mitigates risk.

"We're seeing procurement offices return to RFPs [and pre-COVID processes]. But at the same time, our customers' biggest concern is the more rapidly evolving threat landscape," noted Troxel. "The collective approach of procurement professionals being more focused and careful on acquiring things – at a time when cyber incidents and the use of technology across lines of business is accelerating – is making it harder for government IT leaders to achieve their goals."

"Now that we're going back to business as usual in a post-COVID world, how do we take the streamlined processes and approvals forward and still maintain some of the more rigorous, structural aspects?" expanded Sander.

Where does your organization need the most assistance in securing funding for cybersecurity? Please select up to 5.



Investments for today and beyond

Government agencies must remain agile against threats, strategic in budget, and prepared with a future-ready strategy.

When asked which cybersecurity programs and projects are likely to have an increased investment in the next 12-18 months, the respondents selected several focus areas, including:

- **Application security**
- **Cloud security**
- **Cyber incident response plan**
- **Endpoint detection and response (EDR)**
- **Email security**
- **Identity and access management (IAM)**

Most respondents reported investments in all major cybersecurity areas besides secure access service edge (SASE).

In most of the cybersecurity areas, the highest responses indicate the agencies already invested in these areas and are often expecting to spend even more. Per focus area, the largest amount of respondents (40.1%) made an investment in email security, while the top answers for future investments reflected plans to focus on IAM (36.7%), cloud security (34.7%), and cyber incident response plan (34.7%).

Most areas the agencies plan to work on in the next year are not specifically technology-focused but instead internally focused.

"There's an emphasis on response plans and email, which is an individual employee focus," said Sander. "There's certainly a technology component, but it's more of an integrated programmatic approach. And it's people intensive. Identity and access management falls into that too."

SHI experts also predict that there will be different results in artificial intelligence and machine learning by next year.

"While AI may currently be within the realm of the IT experts like CISOs and CIOs, the rest of the management structure will grow in involvement and focus in the coming months and through 2024," said Troxel.

Investments for today and beyond

What are the cybersecurity programs / projects that are likely to have an increased investment in the next 12-18 months/?

	No focus	No current investment: will make commitments in next 12-18 mo.	Investments made: no plans for more investments in 12-18 mo.	Investments made: expect more investments in 12-18 mo.	Do not know
Application security (including API security)	16.3%	15.6%	19.0%	25.2%	23.8%
Cloud security	9.5%	17.0%	22.4%	34.7%	16.3%
Cyber insurance	19.7%	4.1%	27.9%	23.1%	25.2%
Cyber incident response plan	8.2%	15.6%	25.2%	34.7%	16.3%
Data encryption enforcement	14.3%	16.3%	23.1%	25.9%	20.4%
Endpoint detection and response	8.8%	10.9%	29.9%	30.6%	19.7%
Email security	6.1%	8.2%	40.1%	33.3%	12.2%
Governance, risk, and compliance	6.8%	17.7%	28.6%	31.3%	15.6%
Identity and access management	8.2%	12.2%	27.2%	36.7%	15.6%
Zero-Trust Model	18.4%	15.0%	8.2%	21.8%	36.7%
SASE (secure access service edge)	23.1%	13.6%	9.5%	12.2%	41.5%
Artificial intelligence/ machine learning	31.3%	21.1%	4.1%	16.3%	27.2%

Security program strategy

From continual threats to compliance challenges, organizations face a high-risk cybersecurity landscape – and its complex nature demands a well-established security program.

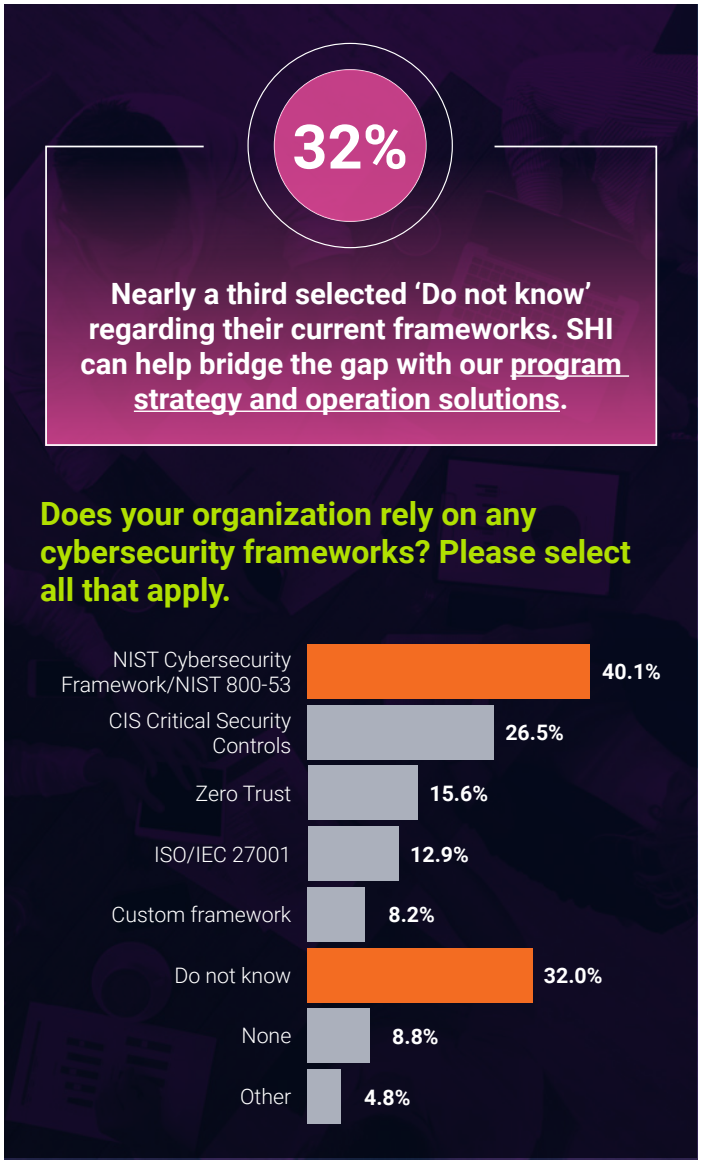
We polled state and local government agencies on their security program and strategy. When asked to select all cybersecurity frameworks they rely on, NIST Cybersecurity Framework/NIST 800-53 came out on top at 40.1%. This result indicates that a large group of respondents have a methodology in place to help them understand, manage, and reduce their cybersecurity risk.

The data shows state respondents are over twice as likely as city respondents and about 1.5 times as likely as county respondents to say they're relying on the NIST framework.

Respondents also reported relying on the CIS Critical Security Controls framework (26.5%), while only about 16% say they are using a Zero Trust framework.

However, nearly a third (32%) selected 'Do not know' regarding their current frameworks. SHI can help bridge the gap with our program strategy and operation solutions.

We work with you by evaluating the current state of your security program against industry practices and cybersecurity frameworks with strategy and assessment workshops. We'll develop a comprehensive security program strategy to help you manage risk, maintain compliance, and improve cyber maturity.



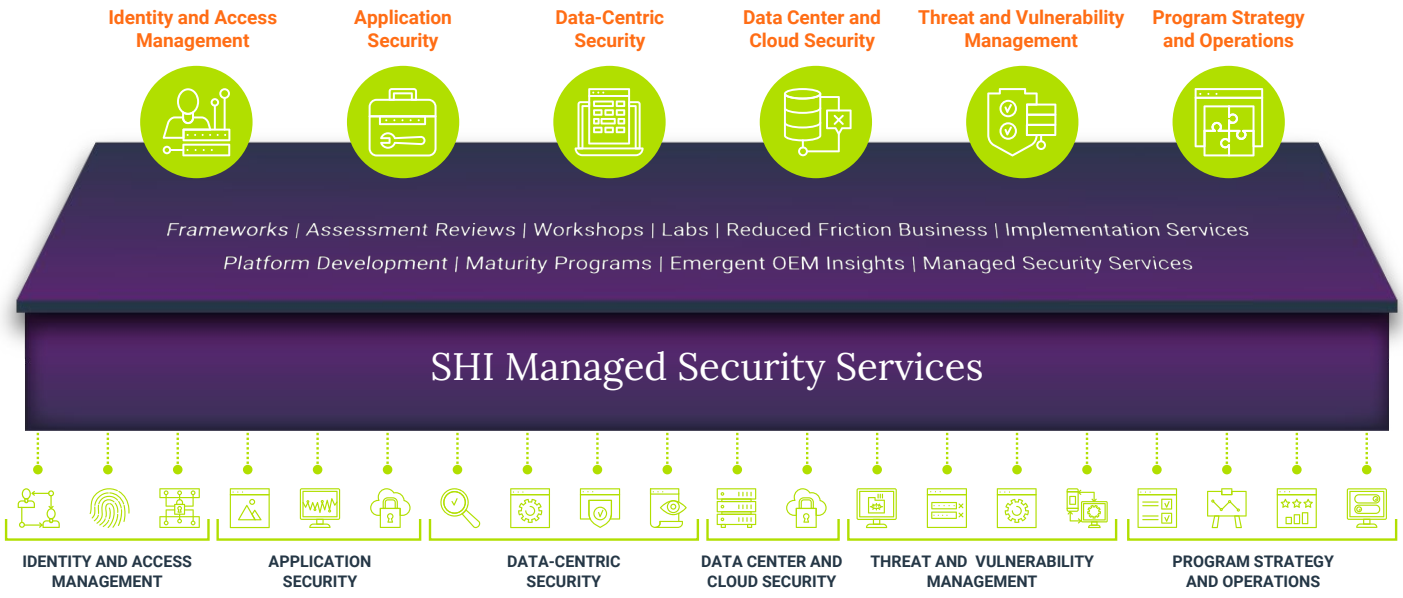
Solve what's next with SHI

The candid insights of state and local government leaders told us cybersecurity is growing: in its complexity to manage, in evolving threats, in proliferation of devices, in security funding needs, and in program strategy requirements.

Yet, the intricate web can be simplified – think of SHI as your personal technology partner. SHI's cybersecurity solutions can address your organization's challenges with insight, expertise, and resources. From protecting your attack surface and improving security maturity to easing procurement and funding, our experts understand today's cybersecurity environment and how to support and achieve your strategic objectives.

Our seamless selection, delivery, and financing options simplify hard decisions for leaders and IT teams – helping you select, procure, deploy, and manage with ease. The result: end-to-end visibility, protection, and response across the organization.

SHI Cybersecurity: Protect



Discover solutions for your rapidly changing cybersecurity environment.

SHI aligns security experts with your strategic objectives to solve cybersecurity challenges.

Get started with a deeper look into your security landscape. SHI's Security Posture Review evaluates your network security protocols and provides valuable insight into your security posture's implementation, maturity, and risk.

Request your Security Posture Review

Speak with a specialist