


OPPORTUNITIES FOR IMPROVING CYBERSECURITY VISIBILITY AT STATE & LOCAL GOVERNMENT AGENCIES

State and local government IT leaders manage a diverse range of computing assets — from cloud platforms to operational technologies that manage public utilities, traffic and safety systems. However, a significant portion of IT officials say they are under-equipped, under-staffed and under-resourced in addressing cybersecurity concerns.

A new survey suggests that a majority of S&L government officials have moderate visibility into the security posture of their systems, but clearly, there's a significant need for better real-time awareness and response tools — and for skilled talent to manage them.

PRESENTED BY **cyberscoop** | **statescoop**

SPONSORED BY  **tenable**



In a new survey of state and local government information technology and security decision makers, CyberScoop & StateScoop identify:

- The extent to which state and local (S&L) government organizations are using — and have security visibility into — an expanded range of computing assets.
- How that visibility varies between assets, including: cloud applications/platforms, mobile endpoints, web applications, containerized services, internet-enabled devices (IoT) and operational technologies (such as industrial controls systems).
- The visibility and control S&L organizations have over systems and devices operated by third-party contractors.
- The key challenges, gaps and opportunities S&L government leaders face in identifying and responding to cybersecurity threats.

TOP LINE FINDINGS

The state of cybersecurity visibility in state and local government:

- **Among S&L government respondents:**
 - 47% use cloud platforms
 - 37% use operational technology (OT)
 - 23% manage IoT devices/systems.
- **When it comes to security effectiveness:**
 - 54% say they are highly or completely effective securing cloud applications and platforms.
 - 51% say they are highly or completely effective securing operational technologies that manage water, energy, traffic and safety systems.
- **Key barriers to improving information security:**
 - 40% lack tools to identify, report and respond to vulnerabilities
 - 39% lack control over systems or assets outside their security infrastructure
 - 46% expressed a need for more adequately-trained personnel
- S&L officials worry most about potential risks of unsecured assets, and assets accessing networks from third-party systems.
- Tools such as real-time dashboards would substantial help communicate security risks.

WHO WE SURVEYED

CyberScoop and StateScoop conducted an online survey of pre-qualified state and local (S&L) government IT, cybersecurity and mission, business or program executives. A total of 125 S&L government executives completed the survey.

All respondents are involved either in identifying IT and network security requirements, evaluating or deciding on solutions and contractors, allocating budgets, or implementing or maintaining cybersecurity solutions. The study was completed in January 2018.

Government Respondents by Job Role:

22%

Executive level decision-maker/
elected official

25%

Mission, business or
program management

19%

IT / Network
management

10%

Information security
and risk management

21%

Other (*Analyst, help
desk, administrator,
integrator*)

4%

DevOps / Application
development

TECHNOLOGY IN USE

State and local (S&L) governments are significant users of cloud computing, operational technology, IoT systems and other systems.

Types of technologies used by S&L government agencies:



64%

Web Applications



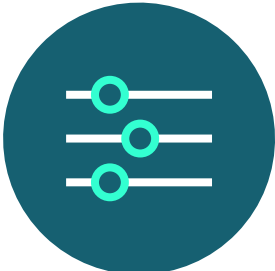
59%

Mobile Endpoints¹



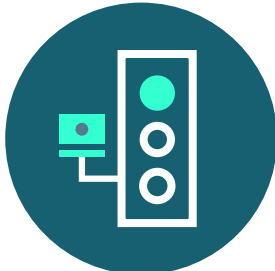
47%

Cloud Apps & Platforms²



37%

Operational Technologies³



23%

IoT Devices⁴



14%

Containerized Apps or Services

¹ Laptops, tablets, phones
² Public, private, hybrid services

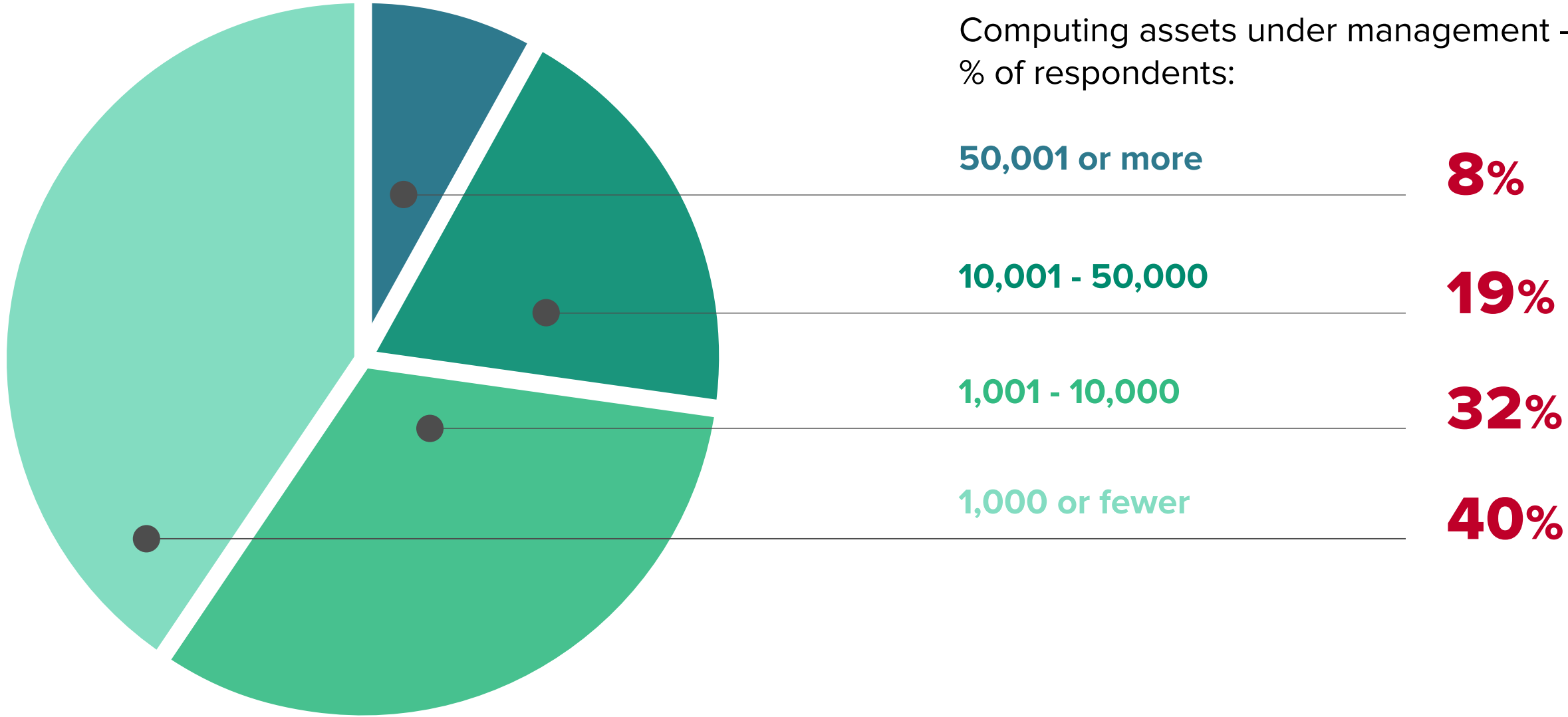
³ OT control systems for public utilities, safety, traffic
⁴ Environmental/energy sensors, traffic lights/cameras

TECHNOLOGY IN USE

The range of assets operating in S&L government environments varies widely.

Nearly 1 in 10 respondents manage and must secure more than 50,000 computing assets for their organization. More than 1 in 4 must manage and secure in excess of 10,000 computing assets.

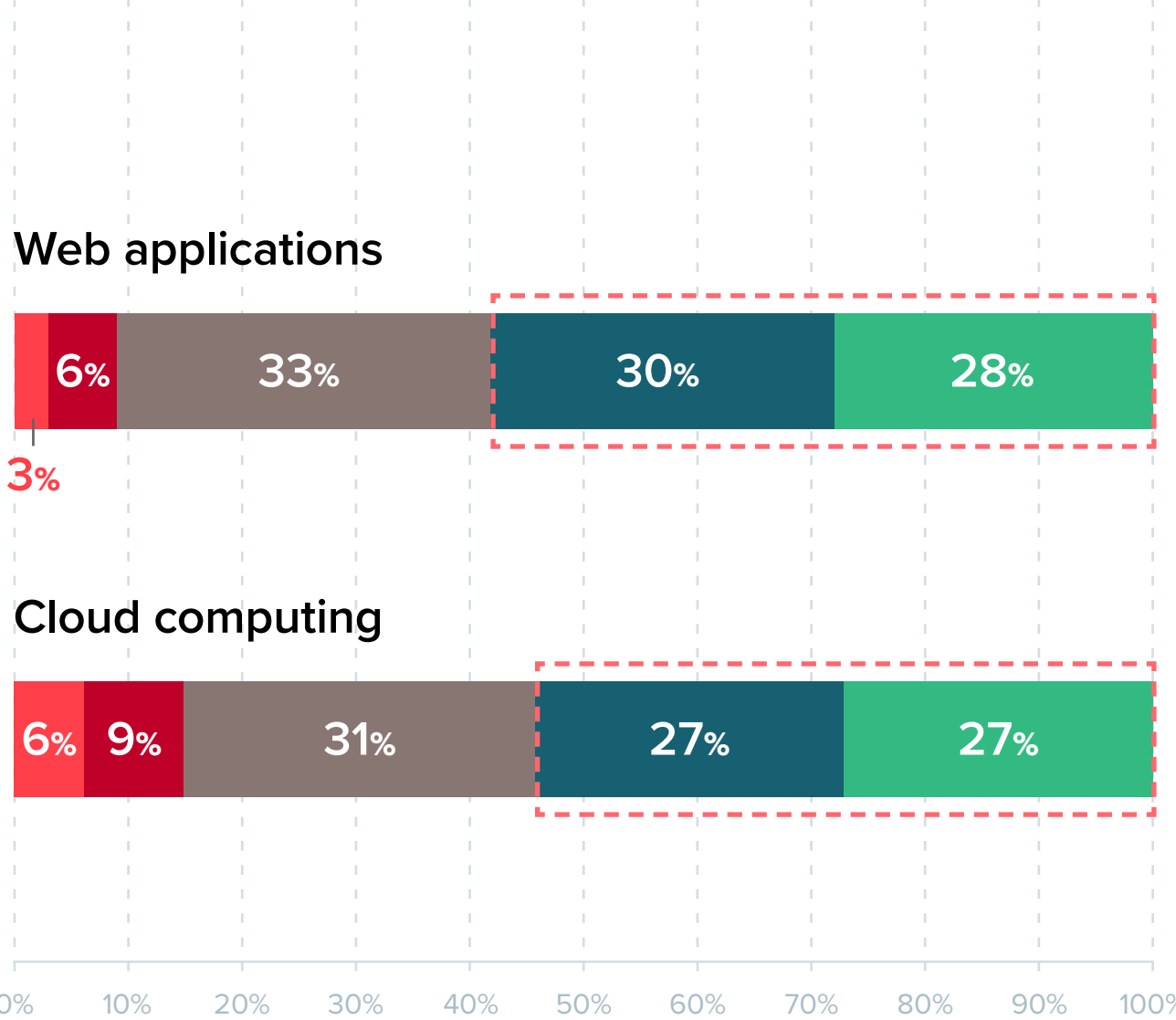
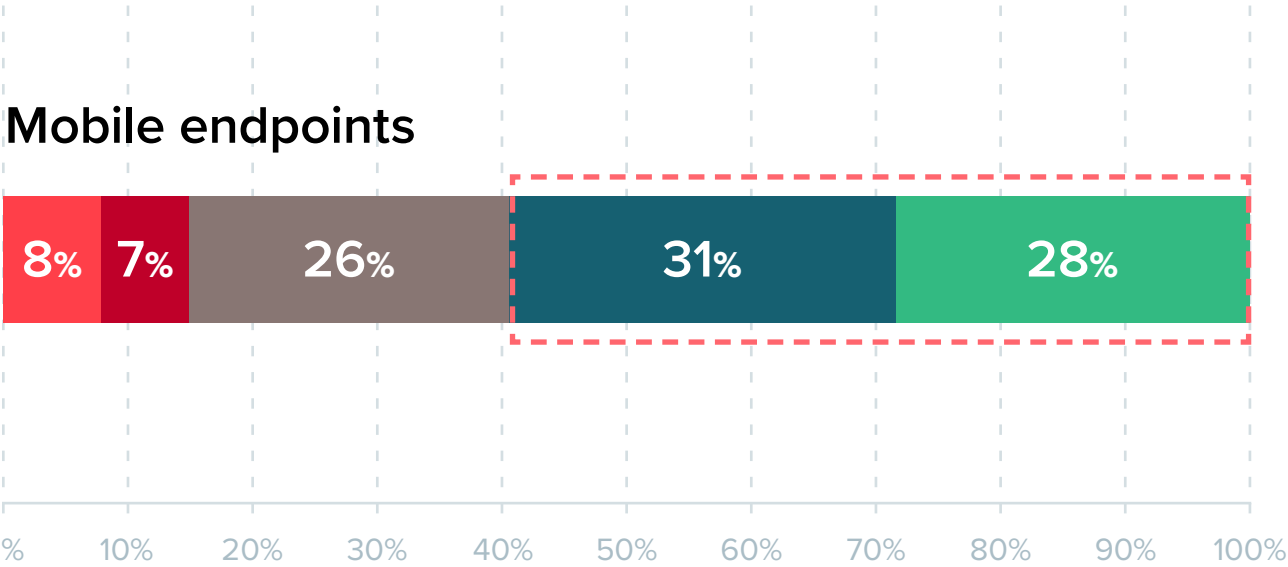
Computing assets under management – % of respondents:



Q: How many computing assets do you estimate operate in your environment? (Including on-premises or remote and cloud technologies, e.g. desktops, laptops, servers, storage devices, network devices, mobile phones and tablets, VMs, hypervisors, containers, IoT or Industrial Internet of Things [IoT] devices.)

SECURITY EFFECTIVENESS

S&L government IT leaders say they're most effective at securing mobile endpoints, web applications and cloud applications and platforms...



1 - Not at all effective 2 3 4 5 - Completely effective

SECURITY EFFECTIVENESS

S&L government officials also say they do moderately well at securing Operational Technologies...and systems operated by third party contractors... but are less effective at securing IoT devices and containerized applications used for DevOps.

Systems and devices operated by third party contractors, which connect to our networks



0% 10% 20% 30% 40% 50% 60% 70% 80% 90% 100%

1 - Not at all effective 2 3 4 5 - Completely effective

Operational Technologies, such as water, energy, waste, traffic and public safety management systems



IoT devices, such as road sensors, traffic lights, cameras, energy and environmental sensors



Containerized applications used for DevOps processes, such as Docker



0% 10% 20% 30% 40% 50% 60% 70% 80% 90% 100%

TOP SECURITY CONCERNS

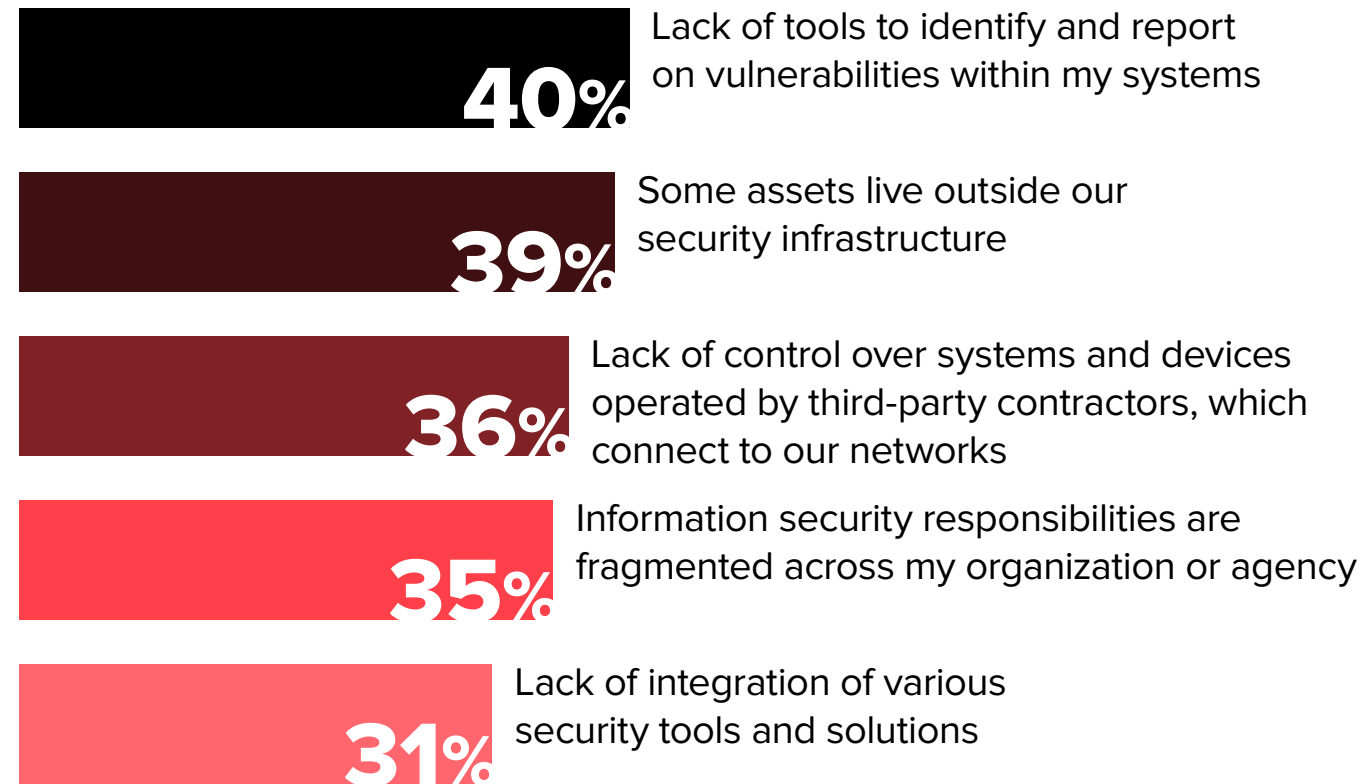
What keeps S&L government officials up at night?



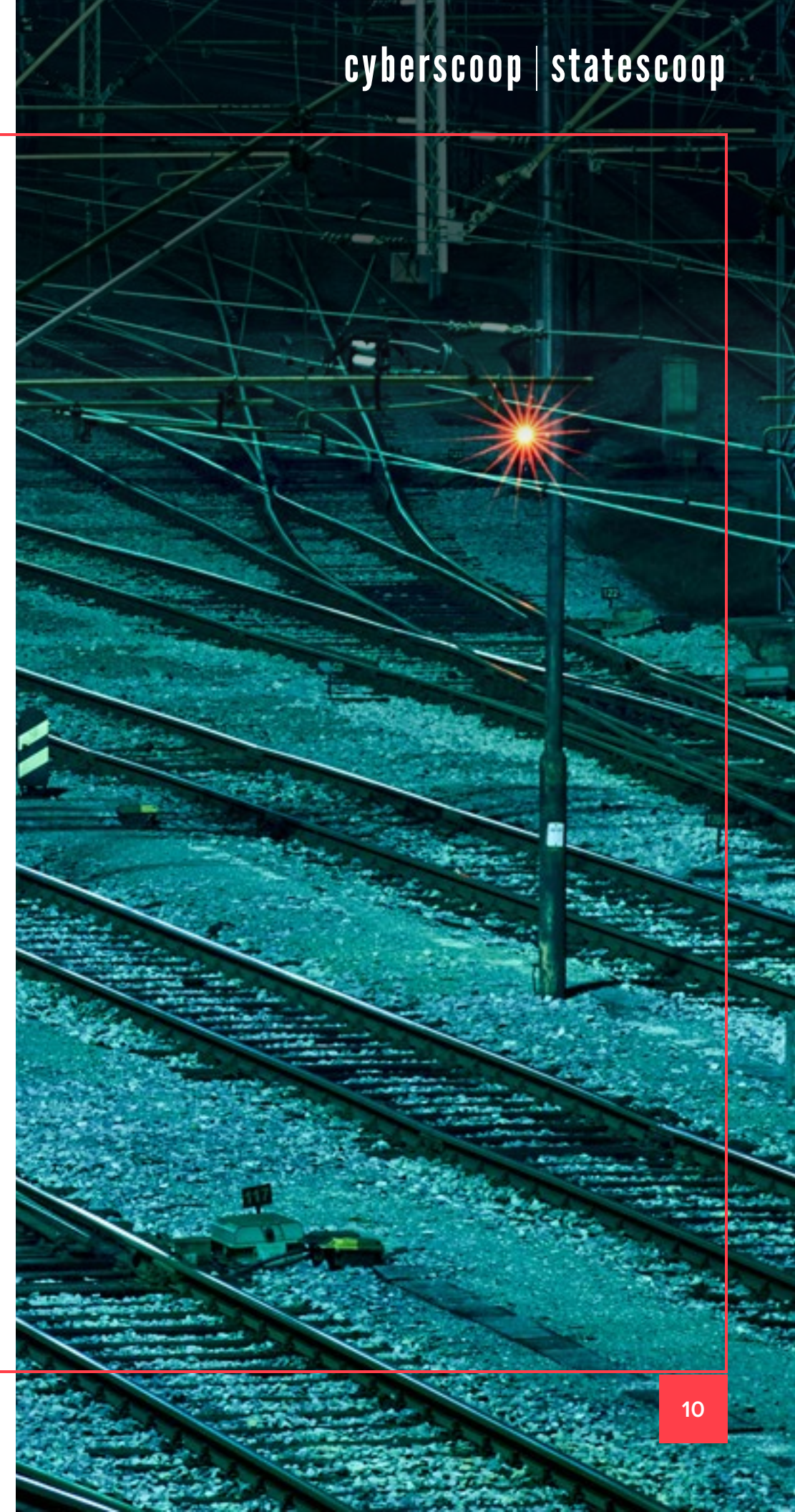
Q: Which top information security concerns keep you up at night? (Select up to five.)

TOP OBSTACLES PREVENTING FULL SECURITY VISIBILITY

What prevents full visibility across S&L computing environments:



Q: Which top issues prevent you from having complete visibility across your computing environment?
(Select up to three.)



TOP ENABLERS FOR IMPROVING SECURITY VISIBILITY

What S&L officials could use most to improve their security posture:



Q: Which of the following would enable you to make the greatest improvements to your information security posture? (Select up to five.)

TOP ENABLERS FOR IMPROVING SECURITY VISIBILITY

What would help DevOps teams most to ensure app security during development:



50%

Security education/
training for DevOps teams

44%

Integrated and automated
security tools and controls
within the CI/CD tool
chain and SDLC*

42%

Collaboration between
DevOps and security
teams

26%

Remediation guidance
for developers to fix
security issues during
development

25%

Enforcing DevOps
compliance with
security mandates
and standards

*CI/CD - Continuous integration/continuous delivery
SDLC - Systems development life cycle

SECURING THIRD-PARTY SYSTEMS

S&L executives take multiple steps to ensure security of third-party systems and devices:

50%

Access controls/
policies enforced
at network
connection point

35%

Endpoint device
security policies

48%

Require contractors
to comply with
national security
mandates, e.g.
NIST Cybersecurity
Framework, HIPAA,
PCI, CJIS)

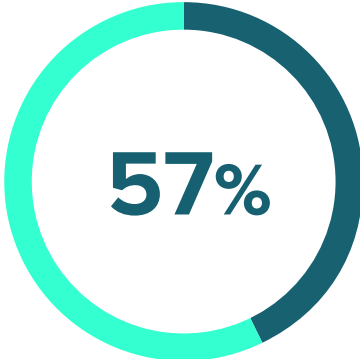
33%

Audits

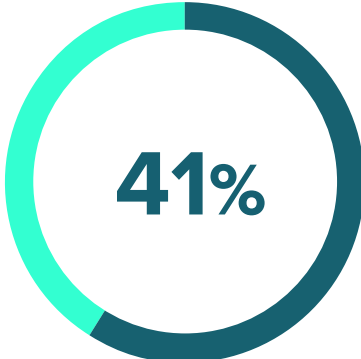
Q: How is your organization ensuring the security of systems and devices operated by third party contractors, which connect to your networks?
(Select all that apply.)

COMMUNICATING SECURITY RISKS TO LEADERS

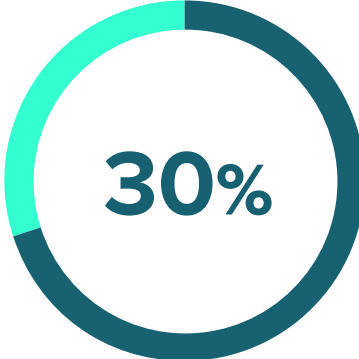
Communicating security risks and posture to S&L government leaders remains challenging for 2 in 3 respondents. Among the top reasons:



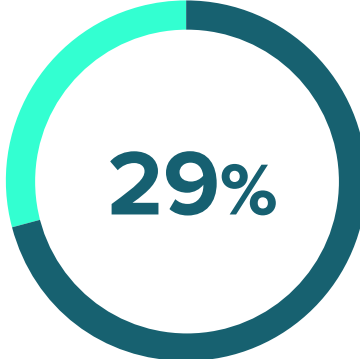
Officials don't understand the technologies and risks



Metrics are difficult for government leaders/decision-makers to understand



They only see me when we have a breach



We don't have the right metrics

COMMUNICATING SECURITY RISKS TO LEADERS

What works best? Real time dashboards are preferred most, but some leaders still prefer other methods:



45%

Real-time dashboard



41%

Narrative briefs



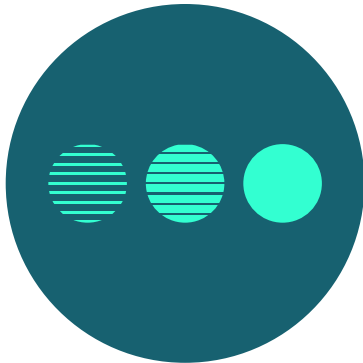
35%

Risk scores



32%

Spoken in-person update



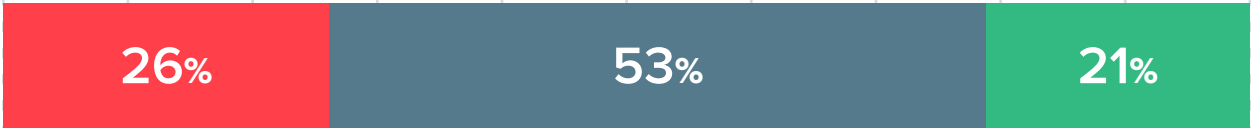
32%

Color-coded indicators, such as red, yellow, green

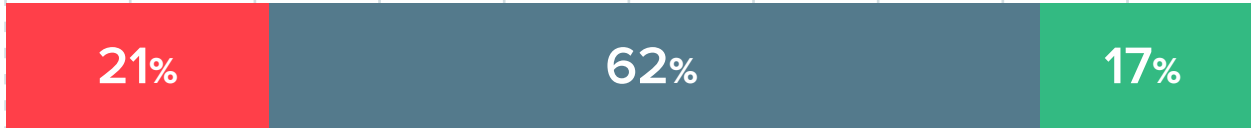
RESOURCE REQUIREMENTS

Only 1 in 5 S&L executives say their organizations are fully resourced with skilled/trained staff... and with the tools needed to detect/remediate security issues.

Skilled and trained staff to meet our security needs



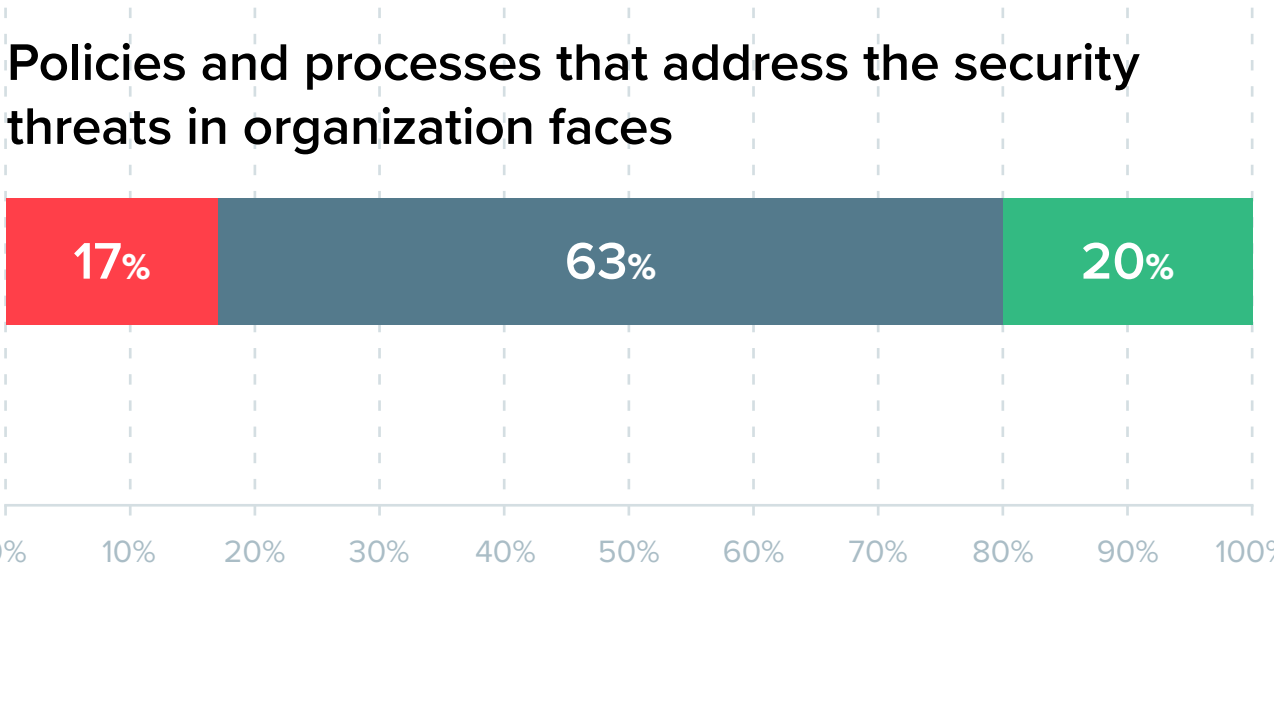
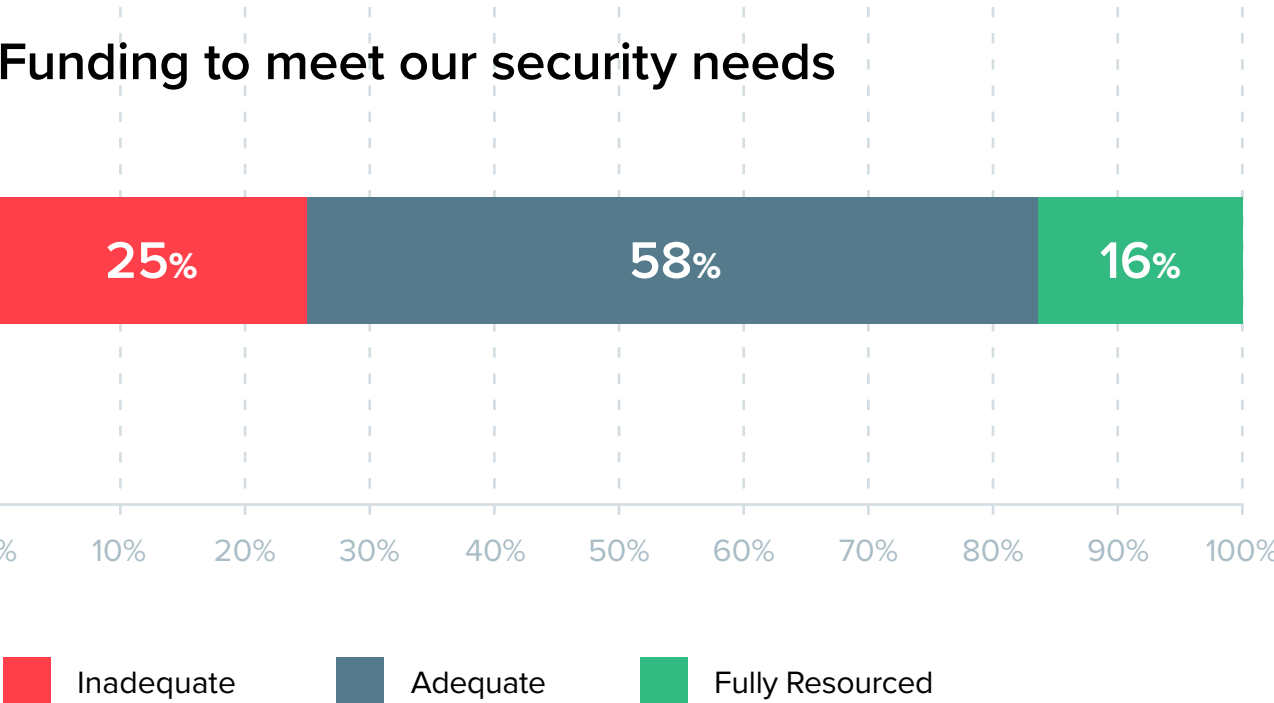
Tools to monitor, detect and remediate security incidents



Inadequate Adequate Fully Resourced

RESOURCE REQUIREMENTS

The vast majority of S&L executives contend they have adequate policies and processes in place to address security threats... but fully 1 in 4 S&L executives say their organizations are not adequately funded to meet their security needs.



CONCLUSIONS

- State and local government IT leaders face a particularly challenging security landscape because of the diverse range of computing systems they operate or oversee — from cloud platforms to operational technologies.
- Adding to that challenge is the lack of control those officials have over systems and devices operating beyond their security infrastructure, including third-party contractors.
- While a majority of those IT leaders have at least moderate visibility into the security status of their systems, 4 in 10 still lack the tools to identify and report on vulnerabilities within their systems and nearly half face a shortage of skilled cybersecurity talent.
- The findings clearly suggest a widespread, if not urgent, need for tools that can provide real-time situational awareness across a variety of networks, that can prioritize and automate remedial responses, and that more readily communicate security risks to senior government and elected officials.

cyberscoop

CyberScoop is the leading media brand in the cybersecurity market. With more than 350,000 unique monthly visitors and 240,000 daily newsletter subscribers, CyberScoop reports on news and events impacting technology and security. CyberScoop reaches top cybersecurity leaders both online and in-person through our website, newsletter, events, radio and TV to engage a highly targeted audience of cybersecurity decision makers and influencers.

statescoop

StateScoop is the leading media brand in the state and local government market. With more than 100,000 unique monthly visitors and 125,000 daily newsletter subscribers, StateScoop reports on news and events impacting technology decisions in state and local government. With our website, daily newsletter and events, we bring together IT leaders and innovators from across government, academia and industry to exchange best practices and identify ways to improve state and city government.

Learn more about Tenable

CONTACT:

Wyatt Kash
Senior Vice President Content Strategy
Scoop News Group
Washington, D.C.
202.887.8001
wyatt.kash@scoopnewsgroup.com

PRESENTED BY **cyberscoop | statescoop**

SPONSORED BY  **tenable**