



STATE & LOCAL GOVERNMENT

The Cybersecurity Posture Playbook

Six Steps to Better Vulnerability Management



Establish the risk picture



Prioritize exposure



Close the remediation gap



Make accountability a control



Manage legacy as a decision



Measure by resilience

For state and local governments, cybersecurity risk can become an operational problem long before a security incident occurs.

26%

Only 26% of critical vulnerabilities in the CISA Known Exploited Vulnerabilities Catalog were fully remediated in 2025. **See step three.**

Vulnerability assessments may reveal exposed systems, aging infrastructure, or gaps in remediation processes. Yet identifying a weakness does not automatically mean the organization has the resources, ownership, or processes to address it.

The challenge is not simply identifying risks. It is understanding which vulnerabilities pose the greatest threat to essential public services and ensuring those risks are addressed before they lead to operational disruption.

A weakness in a public-facing application could affect residents' access to services, while an overlooked system dependency could complicate recovery across multiple departments.

Effective vulnerability management requires turning technical findings into informed decisions, clear priorities, and measurable action.



Six Steps to Stronger Cybersecurity Posture

For state and local government executives, the following six recommendations provide a practical framework for strengthening cybersecurity posture, reducing operational exposure, and building long-term resilience.

These steps help leadership move beyond vulnerability reporting toward informed decisions and measurable risk reduction.

01 STEP ONE Establish the Risk Picture



A vulnerability scan tells you where weaknesses exist, but cybersecurity posture tells you what those weaknesses mean. That distinction should shape how leaders evaluate risk.

Consider two vulnerabilities with the same technical severity. One affects an isolated internal application. The other sits within an internet-facing system supporting an essential public service.

VULNERABILITY A

Isolated internal application



VULNERABILITY B

Internet-facing system supporting an essential public service



The severity score may be identical.

The consequence is not.

Effective vulnerability management therefore begins with context. Leadership needs a current understanding of:

✓ Critical systems and the services they support

✓ Hardware, software, cloud, and connected assets

✓ Known vulnerabilities and active exploitation

✓ Security controls and monitoring coverage

✓ Internet-facing assets and applications

✓ Unsupported and legacy technology

✓ Third-party dependencies

✓ Ownership of critical assets and remediation

CISA recommends maintaining a regularly updated inventory of organizational assets because asset visibility supports vulnerability detection and remediation.

For executives, the objective is not perfect technical inventory. It is **decision-quality visibility**. Leadership should be able to see where technology exposure intersects with operational consequence.



02

STEP TWO

Prioritize Exposure, Not Vulnerability Counts



Large vulnerability reports can create the appearance of precision without providing much direction.

A government organization may have thousands of open findings. That number alone says very little about its actual level of risk.

The more consequential questions are:

Prioritization should account for:

Evidence of active exploitation

Internet exposure

Criticality of the affected service

Access to sensitive or citizen data

Availability of compensating controls

Dependencies on other systems

Potential operational impact

Which vulnerabilities are most likely to be exploited, and what happens if they are?

A mature program does not ask teams to address everything at once. **It creates a defensible order of operations.**

03

STEP THREE

Close the Distance Between Identification and Remediation



A persistent challenge for public-sector organizations is that knowing about risk does not mean the organization is reducing it. **That gap deserves executive attention.**

26%

of critical vulnerabilities in the CISA Known Exploited Vulnerabilities Catalog were fully remediated in 2025

43 days

median time to full resolution

That makes remediation performance as important as detection capability.

Source: Verizon 2026 public-sector analysis

Executives should look beyond how many vulnerabilities security teams discover and instead ask whether exposure is actually declining.

INSTEAD OF ONLY MEASURING...		MEASURE...
Vulnerabilities discovered	→	Critical vulnerabilities remediated
Number of scans completed	→	Percentage of the environment covered
Total open findings	→	High-risk exposure over time
Patches deployed	→	Time to remediate critical vulnerabilities
Security incidents	→	Recurring vulnerabilities and root causes

The objective is not to drive every number to zero. It is to demonstrate that the organization's most consequential risks are being reduced at an acceptable pace.



04

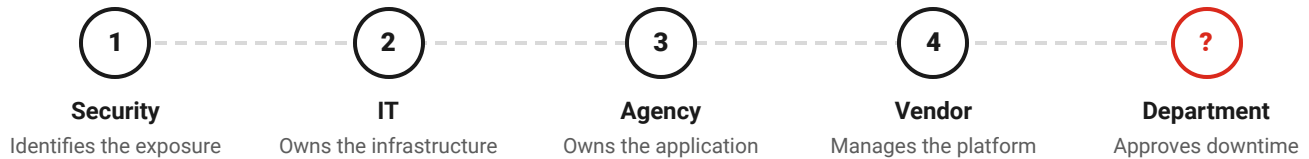
STEP FOUR

Make Accountability Part of the Control Environment



Technology can identify a vulnerability. **It cannot resolve unclear ownership.**

Remediation often crosses organizational boundaries. Security may identify the exposure. IT may own the infrastructure. An agency may own the application. A vendor may manage the platform. Another department may need to approve downtime.



Without clear accountability, a critical vulnerability can remain open while everyone assumes someone else is addressing it. **Leadership should establish:**

Who owns the affected asset	Who owns remediation	Who can accept or defer risk	When unresolved risk must be escalated	What requires executive visibility
-----------------------------	----------------------	------------------------------	--	------------------------------------

This is where governance becomes a security control in its own right.

A vulnerability without an accountable owner is an unmanaged risk.

05

STEP FIVE

Manage Legacy Technology as a Risk Decision



State and local governments cannot modernize every system simultaneously. Legacy platforms may support essential services long after vendors stop providing security updates. Replacing them can require significant funding, procurement, integration, and operational planning.

That reality does not eliminate the risk. It changes how the risk must be managed. For critical legacy technology, leadership should make an explicit decision:

A Modernize it. Plan migration toward supported platforms.	B Isolate it. Separate it and monitor for unusual activity.	C Apply compensating controls. Reduce exposure where patching isn't possible.	D Or formally accept the risk. Make it a documented leadership decision.
--	---	---	--

CISA recommends isolating legacy systems, monitoring them for unusual activity, and developing migration plans toward supported platforms. **What should not become an operating model is allowing known exposure to persist indefinitely because remediation is difficult.**



06

STEP SIX

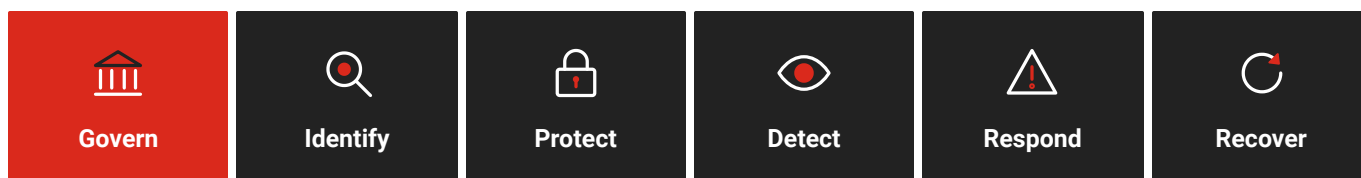
Measure Posture by Resilience, Not Prevention Alone



Even strong vulnerability management cannot guarantee that every weakness will be identified and remediated before an attacker finds it. That is why cybersecurity posture ultimately extends beyond prevention.

NIST Cybersecurity Framework 2.0 organizes cybersecurity risk management around six functions. Together, they establish a broader standard for executive oversight.

Can essential services continue—or be restored quickly—when technology is disrupted?



The organization must reduce preventable exposure while maintaining the ability to contain incidents and restore critical services when prevention fails. That is ultimately the standard against which cybersecurity posture should be judged.

The Executive Test

A mature vulnerability management program should give leadership clear answers to a relatively small set of consequential questions:

- 01 What are our most significant cyber exposures today?
- 02 Who is accountable for remediation?
- 03 Which critical government services depend on those systems?
- 04 How quickly are our highest-risk exposures being reduced?
- 05 Are any known vulnerabilities being actively exploited?
- 06 Where are legacy systems creating risk we cannot readily eliminate?
- 07 Can essential services continue or recover if those controls fail?

The value of cybersecurity posture is not a longer vulnerability report. It is the ability to make better risk decisions.

Across state and local government, the executive imperative is to keep technical visibility and operational action connected—with enough context to prioritize risk, enough accountability to drive remediation, and enough resilience to protect the public services that depend on both.



Frequently Asked Questions

01**How can state and local governments strengthen their cybersecurity posture?**

State and local governments can strengthen cybersecurity posture by improving asset visibility, prioritizing critical vulnerabilities, establishing remediation accountability, managing legacy technology, and building resilience to protect essential public services.

02**Why should government agencies prioritize cybersecurity exposure over vulnerability counts?**

Vulnerability counts alone do not reflect operational risk. Government agencies should prioritize weaknesses based on active exploitation, internet exposure, service criticality, system dependencies, and potential disruption to essential services.

03**How can government leaders improve vulnerability remediation?**

Government leaders can improve remediation by assigning clear ownership, establishing escalation procedures, tracking resolution times, and measuring whether high-risk exposures are declining rather than simply counting identified vulnerabilities.

04**How should state and local governments manage cybersecurity risks associated with legacy systems?**

Government agencies should evaluate legacy systems based on operational importance and exposure, then determine whether to modernize, isolate, implement compensating controls, or formally accept the associated cybersecurity risks.

**SHIELD**

Put the Playbook to Work

Talk with US Claro about **SHIELD · Security**: managed detection and response that protects people, sites and data.

Claro