Gartner

Safeguard Public Trust

5 steps to cybersecurity readiness for public sector leaders

Cybersecurity investments remain a top priority for public sector technology leaders

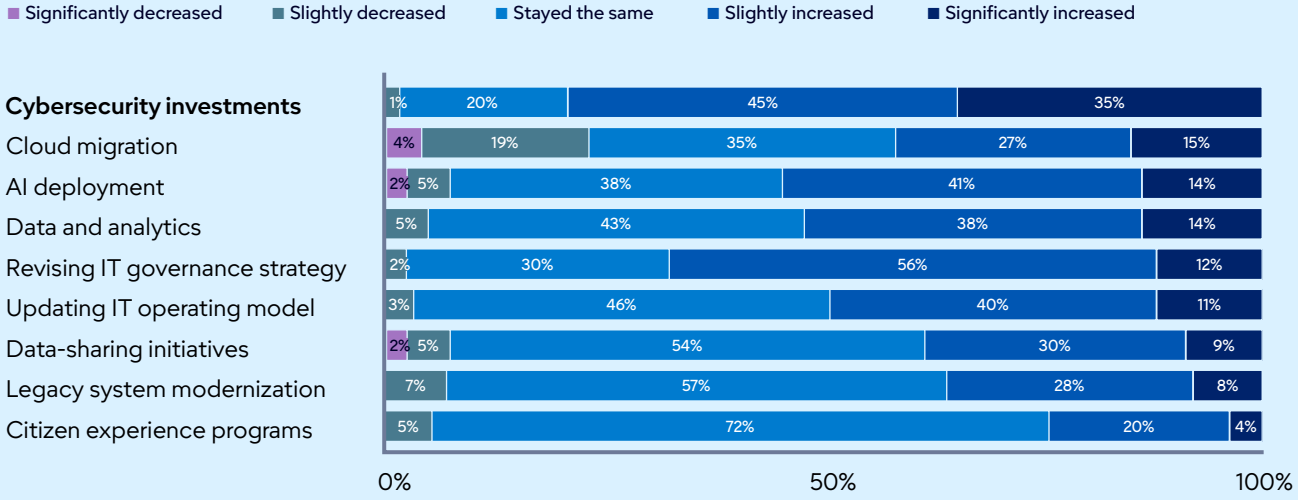
The 2025 Gartner Government Technology Leader Pulse Survey reveals that in response to geopolitical uncertainty and global disruptions:

80% **of global government technology leaders have made cybersecurity a higher priority.**

No matter the mission — delivering high-impact citizen services, securing infrastructure, collaborating with private sector security leaders on issues of national importance or protecting the integrity of military operations — boosting cybersecurity investment is just the start. To achieve lasting results, government leaders must align their organization's cybersecurity strategies, investments and tactics at every level.

Changes in priorities as a result of uncertainty

Percentage of respondents



n = 128 global government technology leaders

Q: How has your prioritization of each of the following technology and data initiatives changed because of the recent shifts in geopolitical stability?

Source: 2025 Gartner Global Government Technology Leader Pulse Survey

Note: Question only asked to respondents who selected "yes" that recent shifts in geopolitical stability were driving changes in prioritization and/or strategy for their organization. Percentages do not add up to 100% due to rounding.

Some of the top questions your peers are asking about cybersecurity readiness:

1 **How** can we effectively assess and improve our current cybersecurity posture?

2 **What** strategies should we adopt to proactively defend against emerging threats and vulnerabilities?

3 **How** can we build a security-conscious culture that meets legal requirements and prioritizes mission outcomes over process?

What are the key stages?

This roadmap provides a consistent approach to cybersecurity strategy planning, highlighting proven techniques public sector technology leaders can use to formalize security program planning and advance organizational mission objectives.

Strategize and plan

Key outcome: Define the security plan and key outcomes.

Establish the foundation by aligning the cybersecurity program with the mission priorities of your organization and the needs of citizens, political leaders and other government stakeholders.

Actions to take:

- ☐ **Understand** key mission priorities and define the program's success in terms of efficiency and effectiveness.
- ☐ **Identify** technology and other threat drivers that might interfere/delay implementation and execution.
- ☐ **Document** the program's value, goals and key stakeholders with roles and responsibilities.

Sample of Gartner client resources include:

Insights

- Top Trends in Cybersecurity for 2026
- Government CIO Pulse: Global Priorities in Response to Geopolitical Shifts

Analyst inquiry

- Identify goals and program value. Define key stakeholders with roles and responsibilities.

Assess program

Key outcome: Assess current state and develop a roadmap.

Evaluate the existing security environment, benchmark against other public sector organizations, and create a roadmap to close gaps and advance delivery of improved mission outcomes.

Actions to take:

- ☐ **Assess** current processes, tools and technologies, and then conduct vulnerability assessments.
- ☐ **Baseline** current maturity, define the target state and perform a gap analysis.
- ☐ **Prioritize** projects and allocate resources based on the likelihood of threats/risks and balance against mission objectives.

Sample of Gartner client resources include:

Tool
- IT Score for Security and Risk Management
- Cybersecurity Controls Assessment

Insights
- Cybersecurity Strategy Planning Best Practices

Complimentary resource
Get started with our Accelerators for Government CIOs.

Develop strategy

Key outcome: Develop the cybersecurity strategy.

Develop a comprehensive strategy document that enables initial implementation and positions cybersecurity as vital to advancing mission objectives.

Actions to take:

- ☐ **Establish** security team roles and responsibilities.
- ☐ **Identify** stakeholders to be accountable, consulted and informed.
- ☐ **Develop** critical competencies in cybersecurity; train for desired and missing skills.

Sample of Gartner client resources include:

Insights

- Cybersecurity and Risk Governance Practices
- Build a Diverse Team to Address the Cybersecurity Skills Shortage

Tool

- Create a Cybersecurity Strategy on a Page

Complimentary resource

Get started with the IT Executive Toolkit for Strategic Planning.

Communicate

Key outcome: Communicate and enable stakeholder buy-in.

Work with your organization's leadership and communications team to implement a communications plan that conveys the value of the program to both internal and external stakeholders.

Actions to take:

- ☐ **Track** metrics; seek feedback to assess and improve program effectiveness.
- ☐ **Implement** outcome-driven metrics and protection-level agreements to develop a cybersecurity value story.
- ☐ **Tailor** training and awareness campaigns to instill a culture of secure employee behavior.

Sample of Gartner client resources include:

Tool	Insights
• Present to the Board of Directors on Cybersecurity and Risk	• How to Describe Cybersecurity's Value to Executive Leaders
• Cybersecurity Business Value Benchmark	• Four Steps to Develop Outcome-Driven Metrics for Cybersecurity

Assess, optimize, improve

Key outcome: Assess, optimize and improve your security program.

Continuously monitor, measure and improve the cybersecurity program by tracking outcomes, enhancing skills and adapting to evolving threats.

Actions to take:

- ☐ **Develop** critical incident response capabilities and improve detection accuracy.
- ☐ **Revisit** maturity assessments and make course corrections for ongoing optimization.

Sample of Gartner client resources include:

Insights

- How to Respond to the 2025–2026 Threat Landscape
- 5 Initiatives to Move Toward Security Operations Excellence

Tool

- Cybersecurity Controls Assessment

Who needs to be involved?

The most successful public sector organizations establish cross-functional teams for their cybersecurity initiatives. We have outlined the recommended functions to involve and their roles to ensure the best success in hitting the milestones.

Mission-critical team members

CIO/Head of technology

Helps the CISO secure buy-in from the board, CEO and CxO peers for the cybersecurity program, aligns technology and cybersecurity strategies, and clearly communicates objectives organizationwide.

Chief information security officer (CISO) and team

Lead development of agile cybersecurity strategy and lead program implementation with key stakeholders.

Legislative stakeholders

Legislate and enact cybersecurity requirements (laws and directives) that set mandatory obligations for organizations affecting governance, technical controls and reporting timelines.

Chief data and analytics officer (CDAO) and team

Assist with data governance and classification and explore leveraging AI in security.

Software engineering leader and team

Responsible for secure delivery of software, working closely with the CIO, CISO and their teams.

Infrastructure and IT operations leader and team

Provide critical support and information via the change, asset, configuration and problem management processes.

Client Story

Environmental Protection Agency (EPA) Ireland Enhances Cybersecurity and Strategic Planning

Mission-critical priority

The CIO sought Gartner expertise to enhance cybersecurity. They needed to streamline ICT strategy and align operations with strategic goals. They also aimed to address sustainability and disaster recovery challenges.

How Gartner helped

Gartner analysis helped EPA Ireland elevate the ISO role and establish a dedicated cybersecurity team, enhancing their security framework with a specific budget. Gartner strategic models enabled EPA Ireland to create a concise, two-page ICT strategy, aligning technological vision with board expectations.

Outcome

By collaborating with Gartner, EPA Ireland **improved its security and reduced threats by 40%,** gained clear strategic direction and executive approval, and proactively addressed challenges such as sustainability and disaster recovery.

Watch the full story ↗

Actionable decision intelligence

Explore these additional complimentary resources and tools for public sector leaders:

eBook

Strategic Roadmap for Cybersecurity Leadership

Learn actionable steps and resources to establish and refine your cybersecurity strategy.

Download Now

Insights

A Government CIO's Efficiency Toolkit

Learn how government CIOs can drive efficiency, modernize IT and deliver measurable outcomes.

Learn More

Insights

Cybersecurity and AI: Enabling Security While Managing Risk

AI's hype and promise in cybersecurity is balanced by trepidation and risk. Here's where to focus.

Learn More

Tool

Accelerators for Government CIOs

Explore our step-by-step tools and diagnostics tailored specifically for government CIOs.

Learn More

Already a client? Get access to even more resources in your client portal. Log In ↗

Connect with us

Get actionable, objective decision intelligence to deliver on your mission-critical priorities. Our expert guidance and tools enable faster, smarter decisions and stronger performance.

U.S.: 1 855 322 5484
International: +44 (0) 3300296 946

Become a Client

Learn more about Gartner for Government IT Leaders
gartner.com/en/industries/government-public-sector

Stay connected to the latest insights

Gartner®