

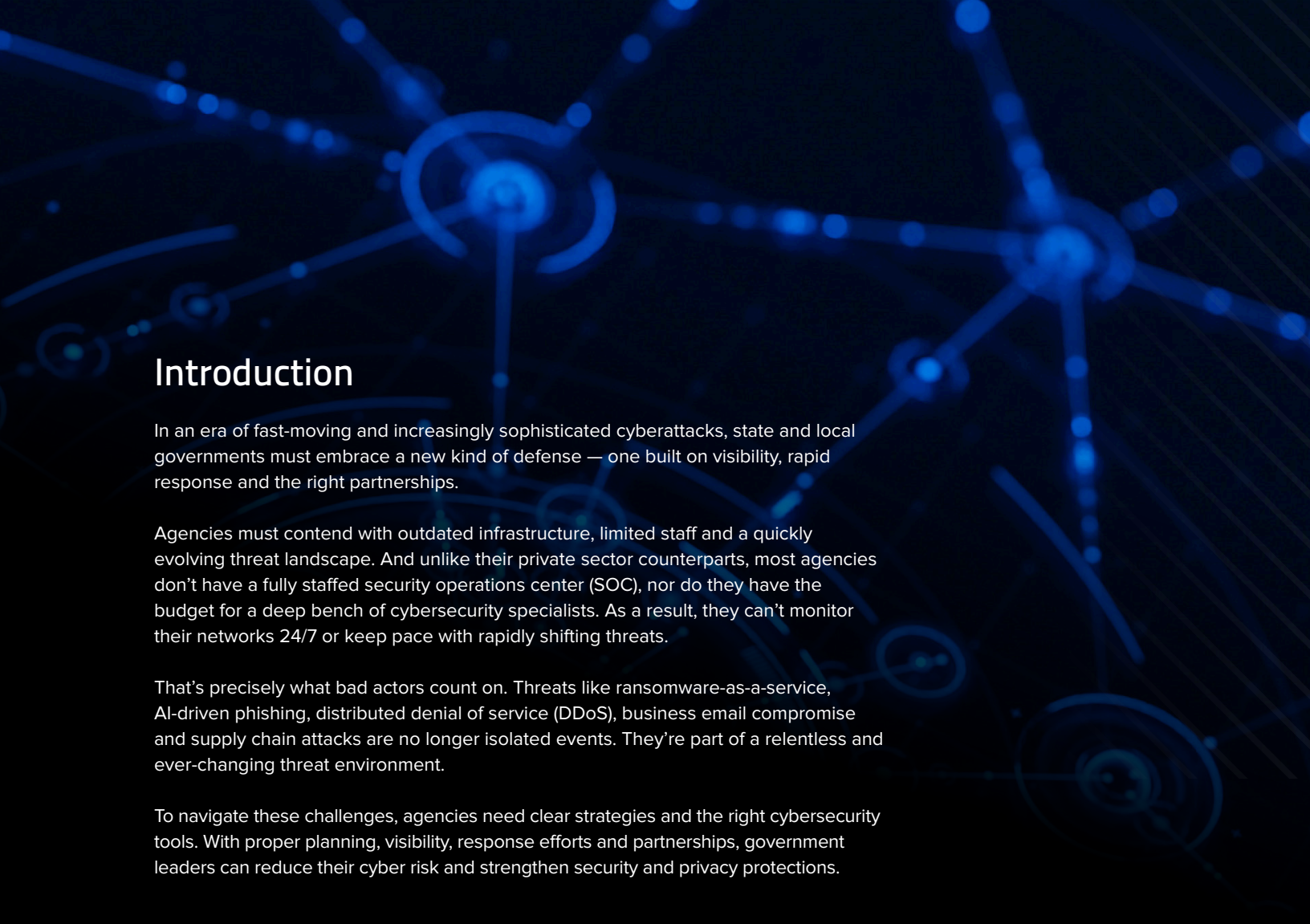


A GOVERNMENT TECHNOLOGY THOUGHT LEADERSHIP PAPER

Cyber Resilience for State & Local Government:

A Roadmap to Smarter, Faster, Stronger Defense

SPONSORED BY **SOPHOS**



Introduction

In an era of fast-moving and increasingly sophisticated cyberattacks, state and local governments must embrace a new kind of defense — one built on visibility, rapid response and the right partnerships.

Agencies must contend with outdated infrastructure, limited staff and a quickly evolving threat landscape. And unlike their private sector counterparts, most agencies don't have a fully staffed security operations center (SOC), nor do they have the budget for a deep bench of cybersecurity specialists. As a result, they can't monitor their networks 24/7 or keep pace with rapidly shifting threats.

That's precisely what bad actors count on. Threats like ransomware-as-a-service, AI-driven phishing, distributed denial of service (DDoS), business email compromise and supply chain attacks are no longer isolated events. They're part of a relentless and ever-changing threat environment.

To navigate these challenges, agencies need clear strategies and the right cybersecurity tools. With proper planning, visibility, response efforts and partnerships, government leaders can reduce their cyber risk and strengthen security and privacy protections.

What makes today's threats so dangerous

Many of today's cyber threats are orchestrated by well-funded global organizations and are more complex and coordinated than ever. They often rely on advanced social engineering, which exploits human behavior to gain access to systems. For example, attackers use legitimate-looking phishing emails or spoofed phone calls — and, increasingly, video calls — that appear to come from a trusted IT provider. In some cases, attackers even create a problem first, such as bombarding an employee with spam, and then follow up to “help resolve the problem.”

Supply chain compromise is also on the rise. Attackers won't target an employee or business directly but instead infiltrate trusted software vendors or third-party contractors, and then leverage those credentials to gain access to your network.

With automation and AI this is all happening faster than ever — meaning agencies have less time to respond to more convincing impersonation tactics and highly personalized attacks.

“AI is not changing the game that's being played,” says Alexandra Rose, director of government partnerships and Counter Threat Unit (CTU) research at Sophos. “It's changing the speed of the game.”

With proper
planning, visibility,
response efforts
and partnerships,
governments
can reduce
their cyber risk.

Top 3 Cyber Priorities for Governments

Government teams often juggle dozens of IT responsibilities, making it difficult to know where to focus cybersecurity efforts.

“When everything feels like a priority,” says Sophos Public Sector VP Rob Lalumondier, “focus on what’s going to reduce the most risk the fastest, while also making smart use of your limited budget.”

Cybersecurity experts generally agree on three priorities that can deliver the most significant impact without requiring agencies to build a security operations center from scratch. Start with these:

1

Protect endpoints & identities.

The vast majority of attacks begin with either a compromised device or a stolen credential. “Service data shows that about 90% of attacks we investigate involve either remote access tools or credential abuse,” Lalumondier says.

That’s why multifactor authentication (MFA), modern endpoint protection and strong access controls are critical. Use MFA across the board, stay on top of access and privilege management, and deploy advanced endpoint security to reduce your risk of compromise.

2

Set up around-the-clock monitoring & response.

Cybercriminals don’t take nights and weekends off. Yet many public sector teams lack the staff or resources for continuous monitoring, which makes them vulnerable during off-hours.

Managed detection and response (MDR) services extend security coverage around the clock without requiring an agency to build and staff its own SOC. MDR teams detect threats in real time, act to contain them and guide the impacted agency through cleanup and recovery. Threats can be detected and stopped before they spread, often within minutes.

3

See across your environment.

Today’s government IT environments span cloud platforms, on-premises infrastructure, third-party software and storage solutions, remote user devices and connected sensors — not to mention a patchwork of legacy systems. That complexity makes it hard to maintain situational awareness. Attackers can sneak in unnoticed, and security teams may not see signs of compromise until it’s too late. “Blind spots are inevitable if you don’t have a unified visibility plan,” Lalumondier says.

Visibility means more than just collecting logs. Tools that consolidate logs and telemetry data help security teams cut through the noise and identify real threats. Understanding the relationships between users, assets, events and behaviors lets your team identify and mitigate risks before they snowball into major incidents.

Your Cybersecurity Roadmap

🔗 **Develop a smarter cybersecurity strategy.** Threat intelligence can be a powerful tool, but only if it informs real decisions. Lists of IP addresses or file hashes, for example, can help block known threats, but they often become outdated quickly. The true value comes when intelligence links those types of indicators to real-world behavior, enabling security teams to prioritize the most potentially dangerous threats.

“Intelligence-driven security just means making smarter security decisions based on what’s actually happening in the threat landscape,” Rose says. “You don’t need to patch everything immediately. Patch what’s being actively exploited.”

Start by tightening up detection rules, adjusting defenses based on what’s happening, and focusing limited resources where they’ll have the most impact.

+ **The goal isn’t to get buried in data. It’s to use the best information to make faster, smarter decisions.**

🔗 **Move from alerts to action.** Detection technology is just one part of the equation. The real challenge is how you respond. “It’s not just about alerts,” Lalumondier says. “It’s about action.”

Too often, when agencies receive security alerts, they lack the capacity to investigate and respond quickly. “Sophos data shows that the average dwell time before detection in some networks is measured in days or weeks versus minutes or hours,” says Lalumondier. “Many attacks go unnoticed until the damage is already done.”

+ **Half of all public sector organizations take a week or more to recover from a ransomware attack, according to Lalumondier.**

That’s why more governments are turning to MDR services. These teams of security analysts keep watch 24/7, investigate anything suspicious and move quickly to contain threats before they spread. The mix of automation and human expertise lets them respond in real time and lock down compromised systems.

Sophos MDR, for example, integrates with existing tools like Microsoft, Palo Alto and CrowdStrike, and acts as an extension of an agency’s internal security team. “For IT teams that are stretched thin, MDR is a force multiplier,” Lalumondier says. “It brings expertise and speed to where it matters most.”

🔗 **Focus on culture change.** Cybersecurity is an organizational and culture issue as much as a technological one. Building a cyber-aware culture through executive leadership and regular employee training is critical.

Robust training programs reduce the risk of phishing attacks, improve cyber hygiene and foster a culture of shared responsibility. Tabletop exercises let departments fine-tune their incident response plans. And they provide good opportunities to include external vendors and service providers in the planning process, rather than only involving them after a cyberattack occurs.

Culture change also means getting buy-in from elected leaders, agency executives and budget directors. Communicate cybersecurity priorities to them in plain language focused on the business and operational impact of a potential attack. Present scenarios that illustrate the cost of a breach, including service disruption, data loss, recovery costs, reputational damage and loss of public trust.

⬢ Don't wait for a breach. Waiting to build cyber resilience until after a breach is a costly gamble. A much better approach is to take consistent, incremental steps to strengthen your defenses. Start with visibility and response. Document known vulnerabilities. Clarify individual roles and responsibilities in your incident response plans. Build relationships with external partners who can support you in a crisis before one happens.

+ Ask your vendors how they secure themselves, how they detect and respond to threats, and what happens when they are compromised.

You do not need to overhaul everything at once. “Incremental improvements really do make a difference,” Lalumondier says, “and they compound over time.”

Rose agrees. “Cybersecurity isn’t all or nothing,” she says. “Every new thing you do, or tweak you make, helps secure you against the threat actors.”

Build a defensible, sustainable cyber strategy

Prioritizing endpoint protection, 24/7 response and unified visibility helps agencies defend against today’s most dangerous threats without overburdening their internal teams.

Every agency — especially small IT teams with constrained resources — can dramatically improve cyber readiness by working with an MDR provider. The right company is far more than just a solutions vendor. They act as a trusted, strategic partner who can help you focus on visibility and response, and develop a plan for investing in your people and tools.

When public trust and critical services are at stake, resilience isn’t optional. It’s essential.

“You can’t defend what you can’t see,” Lalumondier says. “But if you know what’s happening and have the right support in place, you can stop a lot of these threats before they ever take hold.”





This piece was written and produced by the Government Technology Content Studio, with information and input from Sophos.



Produced by Government Technology

Government Technology is about solving problems in state and local government through the smart use of technology. Government Technology is a division of e.Republic, the nation's only media and research company focused exclusively on state and local government and education.

www.govtech.com

SOPHOS

Sponsored by Sophos

Sophos delivers superior cybersecurity outcomes by providing cybersecurity as a service to protect companies of all sizes from the most advanced cyberthreats. Our cybersecurity products and services include managed detection and response (MDR), firewall, email, endpoint (XDR), and cloud native security protection. Sophos products and services defend against ransomware, phishing, malware, and more. They connect through the cloud-based Sophos Central management console and are powered by Sophos X-Ops, our cross-domain threat intelligence unit. We provide fully managed security solutions so you can manage your cybersecurity directly with our security operations platform. Or, you can supplement your in-house team with Sophos' products and services.

www.sophos.com