



A GOVERNMENT TECHNOLOGY THOUGHT LEADERSHIP PAPER

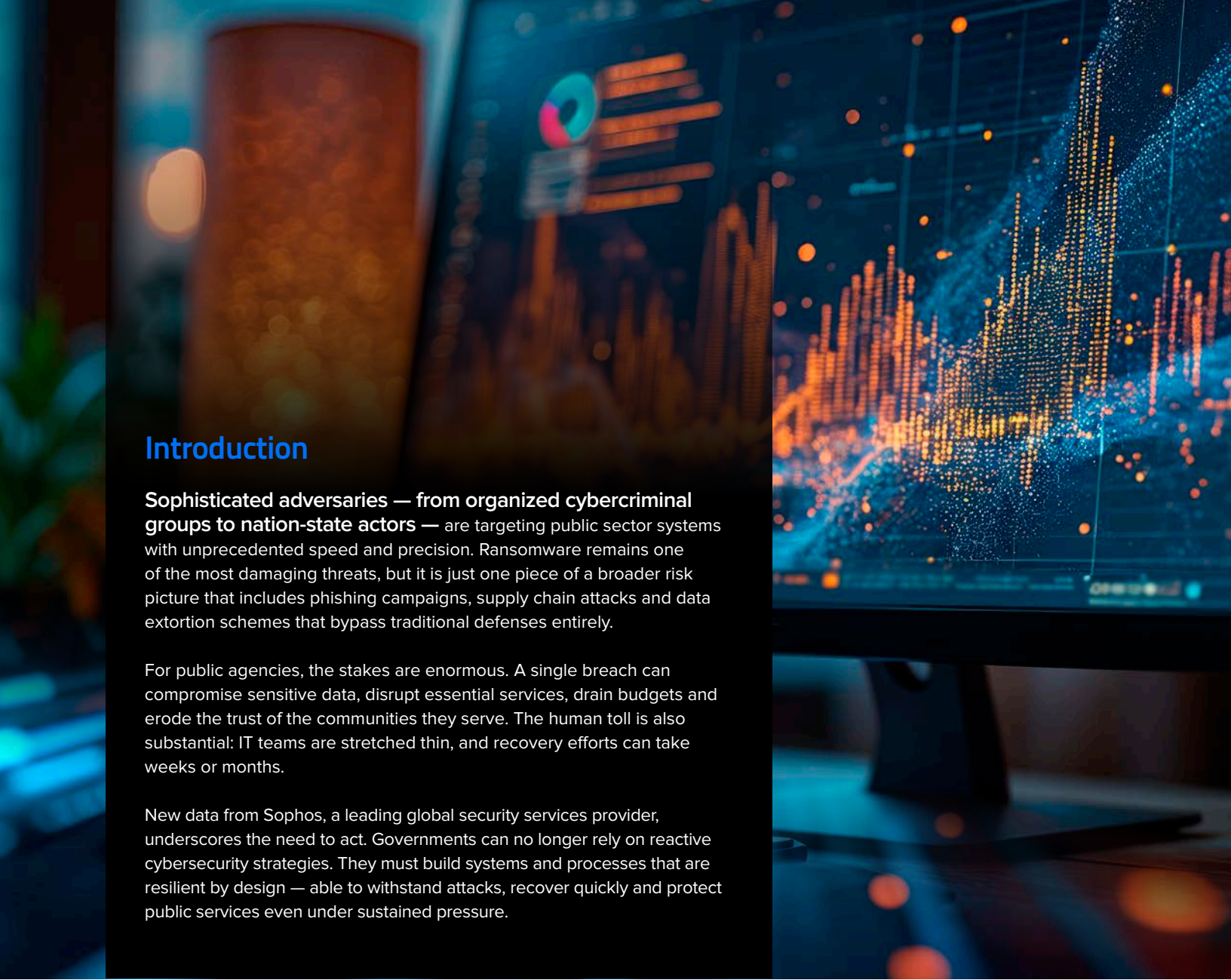
A futuristic digital tunnel visualization. The tunnel is formed by glowing blue and orange lines that recede into the distance. At the end of the tunnel, a city skyline is visible against a bright light. The overall color scheme is dominated by blue and orange.

# Secure by Design:

## A Plan for Ransomware Defense

SPONSORED BY

**SOPHOS**



## Introduction

**Sophisticated adversaries — from organized cybercriminal groups to nation-state actors —** are targeting public sector systems with unprecedented speed and precision. Ransomware remains one of the most damaging threats, but it is just one piece of a broader risk picture that includes phishing campaigns, supply chain attacks and data extortion schemes that bypass traditional defenses entirely.

For public agencies, the stakes are enormous. A single breach can compromise sensitive data, disrupt essential services, drain budgets and erode the trust of the communities they serve. The human toll is also substantial: IT teams are stretched thin, and recovery efforts can take weeks or months.

New data from Sophos, a leading global security services provider, underscores the need to act. Governments can no longer rely on reactive cybersecurity strategies. They must build systems and processes that are resilient by design — able to withstand attacks, recover quickly and protect public services even under sustained pressure.

## The shifting threat landscape

**The financial toll of cyberattacks is significant.** Sophos' State of Ransomware 2025 survey<sup>1</sup> found that about half of public and private sector organizations hit by ransomware paid the ransom, with an average payment of \$1 million. On average, organizations paid an additional \$1.5 million in recovery costs, including downtime, staff hours and network expenses.

**Equally concerning is the human impact.** Most IT professionals reported increased anxiety, stress or guilt. And 31% of teams said mental stress related to the attack led to staff absences.

**Attackers' tactics are becoming more fine-tuned.** For instance, the percentage of attacks in which organizations weren't even locked out of their data — but were still held for ransom — doubled from

A cyberattack costs an organization an **average of \$1.5 million**, not including actual ransom payments.

SOURCE: SOPHOS STATE OF RANSOMWARE 2025 SURVEY



3% to 6% last year. “Now, 6% may not seem like a lot, but it is a new trend where we are seeing threat actors don’t need to actually encrypt your data,” says Austin Cloward, senior sales engineer at Sophos.

“They will first infiltrate your data so that they can hold you for ransom as an extortion attack. One reason we believe they attempt to do that is they’re less likely to get caught.”

Once in, attackers can often remain undetected while they survey the entire environment. In one incident, the attacker not only locked up data — they read through the organization’s cyber insurance policy to determine just how much they could get. “The threat actor said, ‘I see that your policy limit is \$750,000. Your ransom is \$750,000. We will not budge,’” Cloward says.

And artificial intelligence, of course, is further helping bad actors improve their attacks, with increasingly convincing phishing and voice scams. Sophos found nearly a quarter of ransomware attacks on organizations with 1,001 to 3,000 employees began with a phishing email.

**31% of organizations** hit by an attack said the mental stress of the incident led to staff absences.

SOURCE: SOPHOS STATE OF RANSOMWARE 2025 SURVEY

## Where the Security Gaps Are

When Sophos asked public agencies why they think their organization fell victim to a ransomware attack, their answers identified concerning security gaps:



**49%** of **higher education institutions** attributed the **breach to an unknown weakness** in their defenses.



**45%** of **federal agencies** admitted they were **aware of weaknesses in their defenses** but hadn’t addressed them.



**42%** of **K-12 schools** said they **didn’t have sufficient cybersecurity experts** or monitoring systems.



**40%** of **local and state government** agencies blamed a **lack of necessary cybersecurity products** and services.

## The 3 Ps of Secure by Design

Secure by Design is a mindset of building security into systems from day one. Instead of bolting on protections after launch, Secure by Design calls for security requirements to shape the very architecture of hardware, software and services.

In practice, this approach assumes systems will be attacked and ensures they are built to withstand, contain and recover from those attacks. It prioritizes principles like least privilege, reducing attack surfaces, defense in depth, and embedding detection and response into the system itself. Secure by Design treats protection as a fundamental design goal alongside performance, usability and cost.

Organizations can take strides toward this mindset by focusing on three Ps: prevent, protect and prepare.

### 1. Prevent

Agencies need to conduct risk management, including vulnerability scanning, to understand where security gaps are and how they can proactively address them.

“If you’re not sure where to start in your security maturity journey, step number one should be continuous vulnerability scanning,” Cloward says. “That will help you patch issues before they get exploited.”

### 2. Protect

Around-the-clock threat detection and response is essential. The majority of attacks happen on weekends and between the hours of 2 a.m. and 4 a.m. when IT staff are more likely to be slow to respond.

If your agency doesn’t have in-house staff who can monitor your environment at all times, a managed detection and response services provider can help monitor endpoints, firewalls, servers and email security.


“Partnering with the right provider gives you that 24/7 monitoring and visibility across your entire environment,” Cloward says, “allowing you to identify and stop threats before a threat actor finds that gap in your security coverage.”

Other requisite protection technologies include AI-powered email security solutions and multifactor authentication. “If you don’t have two-factor authentication or multifactor authentication on your VPN,” Cloward says, “turn that on immediately.”

### 3. Prepare

Develop and maintain an incident response plan and review it at least twice a year, including anytime there’s a change in senior leadership or your cyber insurance policy. Make sure IT teams have current contact information.

A managed detection and response services provider can **monitor endpoints, firewalls, servers and email security.**



Schedule regular tabletop exercises that test your perimeter and your internal network to identify any vulnerabilities.

“Testing helps you identify the type of attack vectors that often get overlooked,” Cloward says. “It could be as simple as permissions. Maybe your standard users have more permissions than they need. A penetration test is a good way to identify that, whereas a vulnerability scan wouldn’t pick that up.”

Regular testing also helps identify potential misconfigurations within your network.

“Misconfigurations led to 67% of eventual ransomware incidents,” Cloward says. “The misconfiguration may not have been the root cause, but it’s what allowed the threat actor to continue the attack once they were inside.”

Agencies should also regularly practice restoring data to prepare them to respond rapidly in case of a real breach.

While considering these recommendations, public agencies should also follow Secure by Design principles like those emphasized by White House [Executive Order 14144](#).<sup>2</sup>

The White House’s directive pushes for Zero Trust, patching and continuous vulnerability management. It also directs organizations to make their cybersecurity policies machine readable.

“They want you to leverage the technology that is speeding up detection and response capabilities and that will help you stop threats,” Cloward says. “One easy way to do that is make sure documentation is machine readable.”

## Secure at Every Stage


For governments, the biggest security imperative is to shift from a reactive posture to a proactive one. By prioritizing prevention, protection and planning, IT leaders can reduce both the likelihood and impact of ransomware attacks. In doing so, they safeguard not only their systems but also the trust and safety of the communities they serve.

“As with anything in cybersecurity, it’s almost like a game of cat and mouse,” says Cloward. “We’re doing everything we can to stay a step ahead. Often, all it takes is one vulnerability to allow them to get in front of us again.”

The right strategy — one in which cybersecurity is baked in to all procurement and decision-making from the start — is the best way to move your organization toward a proactive security approach.

“Follow Secure by Design principles,” Cloward says. “When security is your priority, everything else will fall into place.”

Regular testing **helps identify potential misconfigurations** within your network.

- 
1. <https://www.sophos.com/en-us/content/state-of-ransomware>
  2. <https://www.federalregister.gov/documents/2025/01/17/2025-01470/strengthening-and-promoting-innovation-in-the-nations-cybersecurity?>

*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](http://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](http://www.sophos.com)