Springbrook

## 2026 Springbrook

# Cybersecurity Survey

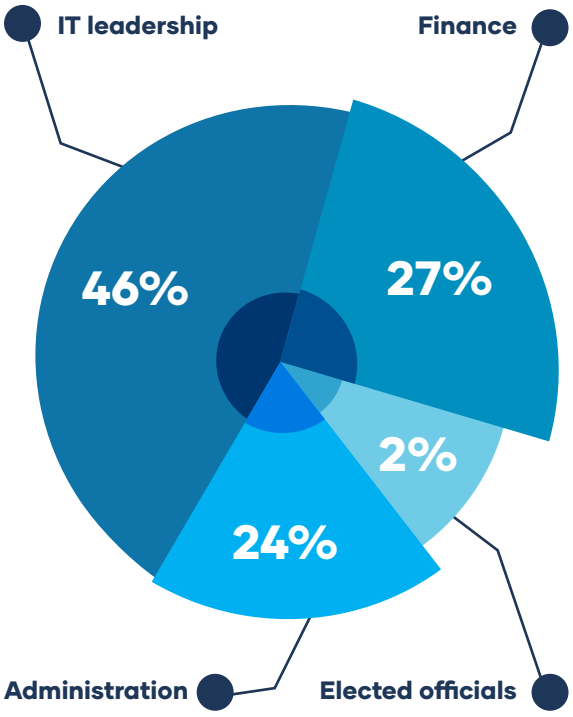
### A Two-Year Analysis of Cyber Readiness in Local Government

www.springbrooksoftware.com

Introduction

# Who We Surveyed and Why It Matters

**In 2024 and 2025, Springbrook surveyed nearly 350 local government professionals across the United States to understand how agencies perceive cyber risk, allocate cybersecurity funding, modernize their technology stack, and prepare for emerging threats.**




Respondents represented a wide range of roles — IT leadership (46%), finance (27%), administration (24%), and elected officials (2%) — and came from organizations serving populations from 100 to over 100,000 residents with staff sizes ranging from small teams of fewer than 10 employees to agencies exceeding 100 personnel.

**100–100,000+**
**Residents**

**10–100+**
**Employees**

This diverse participation reflects the operational realities of local government: resource constraints, aging infrastructure, decentralized systems, and rising cyber exposure. These agencies deliver the essential services that keep communities running, making their cybersecurity posture a critical component of public safety and trust.

- **Resource constraints**
- **Decentralized systems**
- **Aging infrastructure**
- **Rising cyber exposure**

The broader industry context makes this research especially important. While cybersecurity spending continues to rise, budget growth is slowing, even as AI investment accelerates faster than any previous technology cycle. Yet adversaries — from ransomware groups to nation-state actors — continue to scale attacks, leveraging automation, deepfakes, phishing-as-a-service, and credential-based intrusions at unprecedented speed.

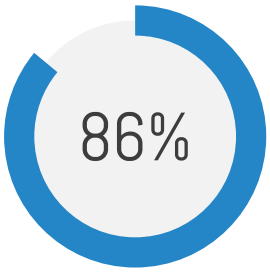
Our data shows this tension clearly. Local governments are modernizing — but unevenly. Cyber budgets are rising — but not fast enough. Cloud adoption is accelerating — but fragmentation remains high. And while cyber awareness is strong, key foundational practices are inconsistent.

**This report outlines where local governments are making progress, where gaps remain, and what the next 12 months of cybersecurity preparedness will require.**

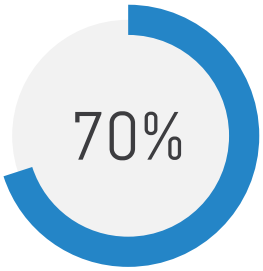
Section 1

# Awareness vs. Reality

## Awareness of Ransomware Attacks




**2024 |** 86% were aware of ransomware attacks occurring within their state.



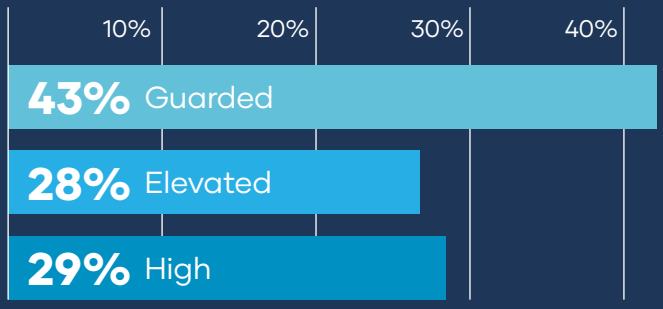

**2025 |** Only 70% reported awareness of ransomware attacks in their state.

Awareness remains high, but the decline may reflect either shifting communication patterns at the state level or simply the normalization of ransomware attacks. Given the continuous rise in attacks on public services, reduced awareness does not indicate improved safety — only more noise in the ecosystem.

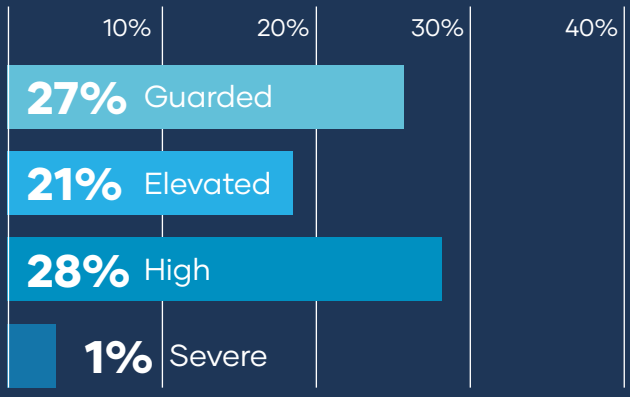
## Perceived Threat Levels

Roughly half of respondents across both years place their state at Elevated or High risk. This aligns with current attack patterns targeting local government networks, utilities, police departments, and public works systems.

### 2024



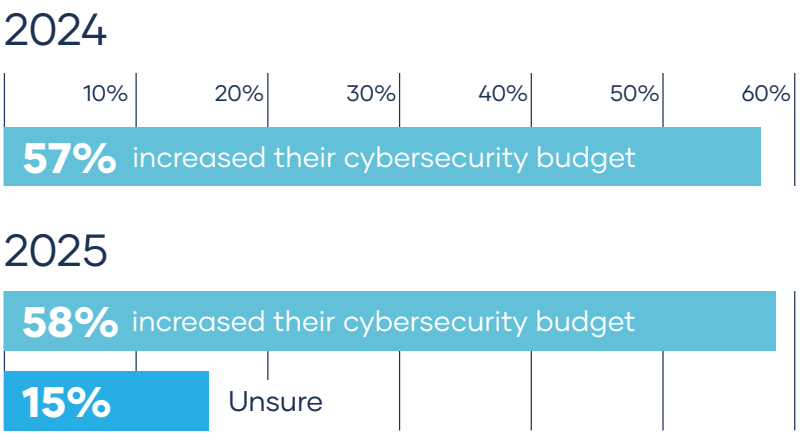

### 2025




**Key Trend:** The data shows consistent recognition of risk — but not necessarily urgency in addressing it.

Section 2

# Cybersecurity Budget Trends

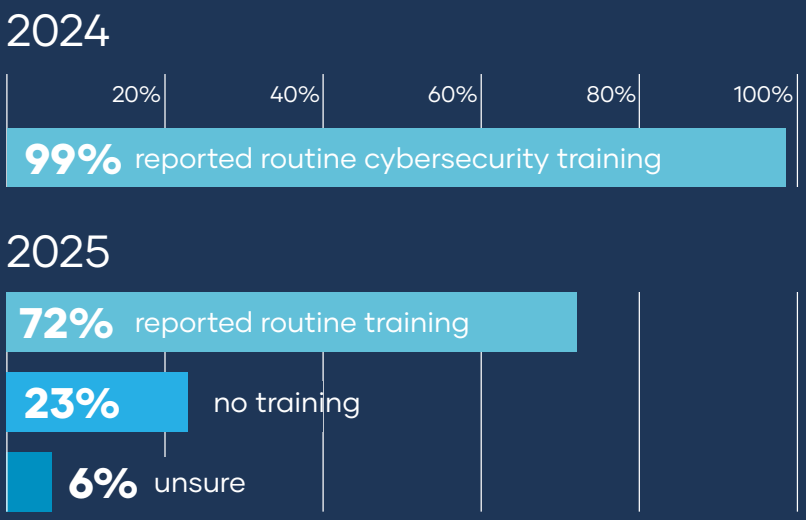


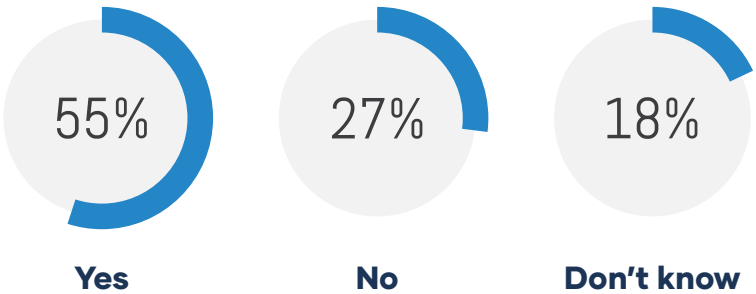

## Budget Direction

Budgets are rising — but slowly. The national trend shows cybersecurity spending increasing at a reduced growth rate, which aligns with our findings. Agencies are investing but still struggling to keep pace with rising threats and the increased cost of cloud, identity management, and AI-enhanced security tools.

## Cyber Training

The apparent drop reflects a shift from simple "yes/no" compliance training to more structured, ongoing programs. Agencies may be interpreting the question differently as the definition of "training" evolves — or some may still not be practicing consistent hygiene.




## Zero Trust Policies in 2025

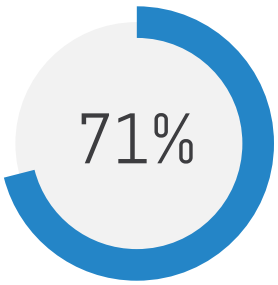
Zero Trust is gaining traction, but nearly half of agencies either lack a policy or do not know if they have one. This indicates a significant opportunity — and risk.

Section 3

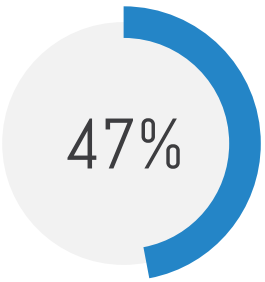
# Grants & External Funding

## Applications for the State & Local Cybersecurity Grant

2024 represented the early, high-volume rush of SLGCP applications. By 2025, application rates stabilized, and agencies reported improved clarity on outcomes.



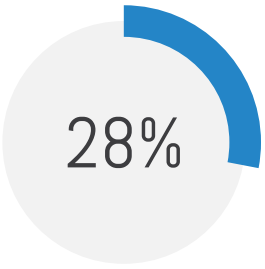

**2024**
71% applied



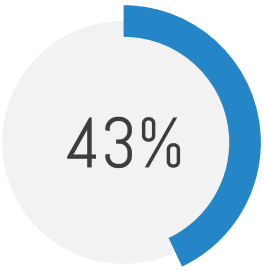

**2025**
47% applied

## Received Funding

Funding results improved in 2025, with a larger share of agencies reporting successful outcomes from their cybersecurity grant applications.



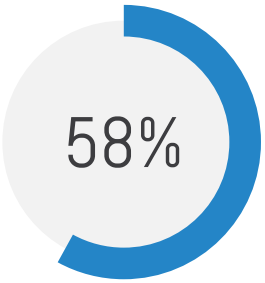

**2024**
28% received funding



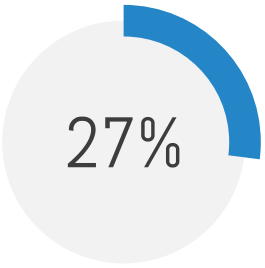

**2025**
43% received funding

## Uncertainty

Although uncertainty remains, fewer agencies were unsure of their funding status in 2025 compared to the previous year.




**2024**
58% didn't know if they received funds




**2025**
27% didn't know

**Key Insight:** Grant participation is normalizing — but awareness and communication gaps remain. Many agencies still lack the staffing or expertise to pursue cyclical grant opportunities or track multi-year allocations.

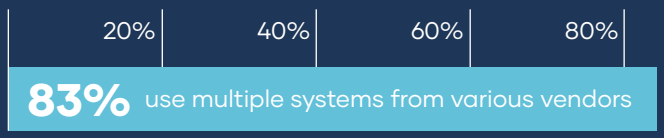
Springbrook

Section 4

# ERP Modernization & the Technology Stack

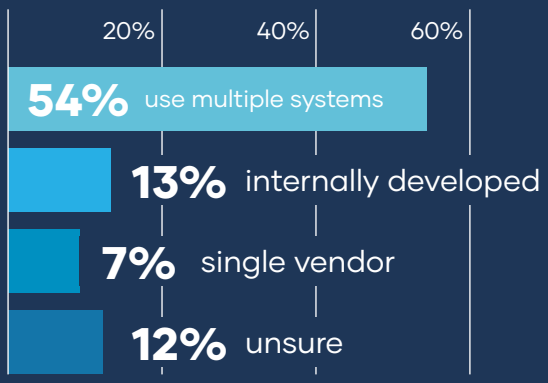
## ERP Fragmentation

### 2024



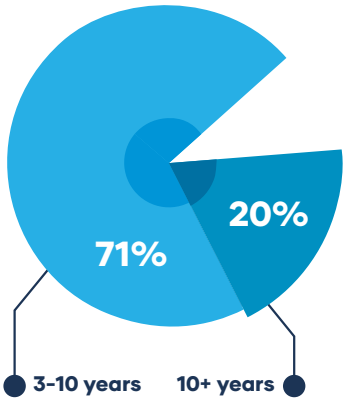

Fragmentation remains the dominant ERP pattern in local government. While the improvement from 83% to 54% suggests a shift toward consolidation, the high number of "don't know" responses and internal builds indicates ongoing complexity.

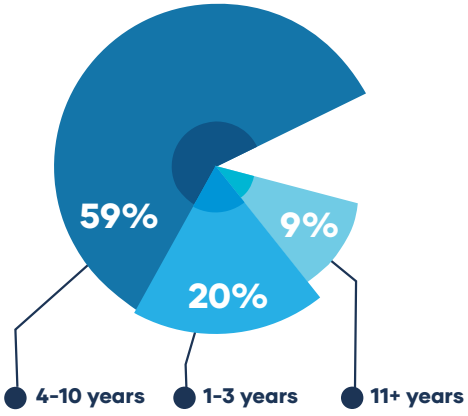
### 2025




## Risk Impact | Fragmentation increases:

- **Attack surface**
- **Patch management challenges**
- **Identity management complexity**
- **Incident response times**
- **Vendor accountability gaps**

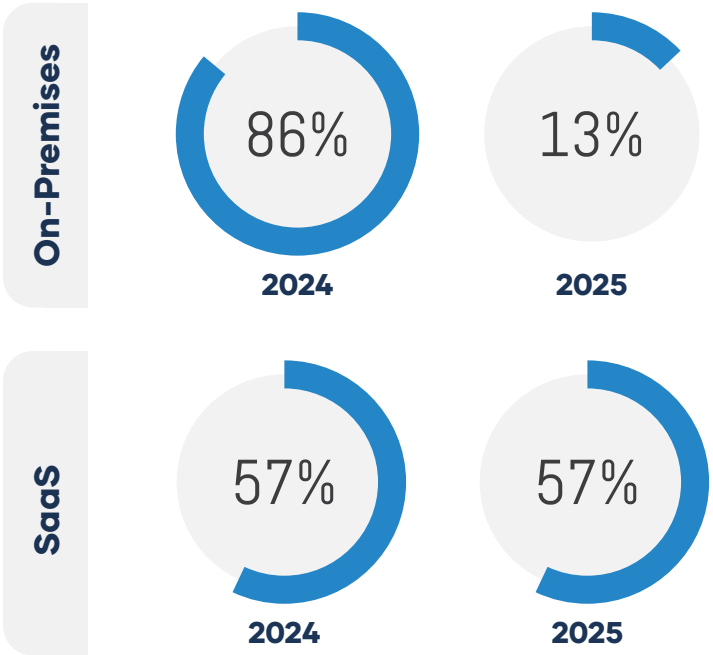



## Software Age

Local governments are upgrading — but steadily, not rapidly. The increase in systems aged 1–3 years indicates modernization activity, but legacy systems remain entrenched.

# Hosting: On-Premises vs. Cloud




The dramatic drop in on-prem responses in 2025 may reflect improved clarity in how agencies describe hosting models — or a meaningful acceleration in cloud adoption. Either way, the direction is clear: Local government is aggressively moving off on-prem infrastructure, even if not all systems meet full SaaS criteria.

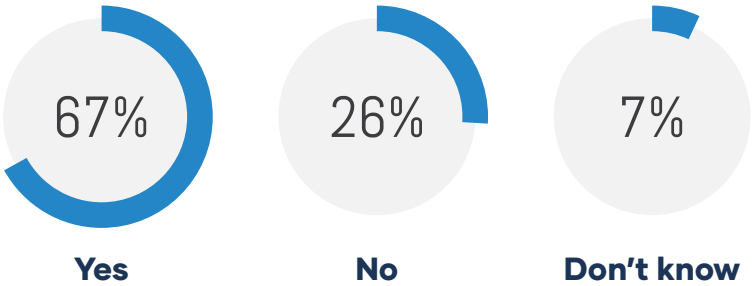
## .gov Domains in 2025

A .gov domain is one of the simplest, highest-impact security upgrades. The fact that 40% of agencies either lack one or are unsure indicates a basic gap in civic cybersecurity posture.

- **60%** Yes
- **34%** No
- **6%** Don't know

Section 5

# Trust in Existing Finance Platforms - 2025




While two-thirds trust their current system, one-third either distrust it or aren't sure — a significant number for mission-critical software. Combined with fragmented ERP environments and legacy systems, trust alone is not an indicator of security readiness.

Springbrook

Section 6

# What the Two-Year Trend Tells Us

**Across the two-year period, four core findings emerge:**

**1 Cyber risk awareness is high — but uneven.**

Respondents consistently rate their state at Elevated or High risk, yet awareness of real-world events declined and training responses became more varied.

**2 Budget increases are steady but modest.**

Local governments are spending more — but not enough to match the speed and sophistication of modern threats.

**3 Technology modernization is accelerating — but incomplete.**

More new systems, fewer on-prem solutions, but persistent fragmentation means cyber exposure remains high.

**4 Foundational best practices are not universal.**

Zero Trust, .gov domains, and grant utilization all show large gaps.

These insights point to a sector that is moving in the right direction but not fast enough.

Section 7

# What Agencies Can Do Now

**Based on the data and current cybersecurity trends, local governments should prioritize:**

**1 Consolidating fragmented systems.**

Unified platforms reduce risk and improve visibility across financial and operational systems.

**2 Accelerating cloud adoption**

True SaaS systems reduce patching workloads, improve resilience, and enable AI-enhanced security options.

**3 Implementing Zero Trust policies**

Identity protection and access control remain the highest-value security investments.

**4 Strengthening training and governance**

Training must evolve beyond "annual checkboxes" to continuous engagement.

**5 Pursuing cyclical federal and state grants**

Cybersecurity grants remain underutilized — especially by smaller agencies.

Section 8

# Conclusion

Local governments face unprecedented cybersecurity pressure as ransomware threats accelerate, AI-enabled attacks evolve, and legacy systems struggle to keep up. The 2024 and 2025 Springbrook survey results show a sector working hard to modernize — but still exposed by inconsistent practices, fragmented ERPs, and slow-moving infrastructure upgrades.

Modern, secure, cloud-native solutions like the **Springbrook Cirrus Finance Platform** offer the stability, security, and operational efficiency agencies need to protect themselves and deliver uninterrupted services to the communities they serve.

Springbrook remains committed to supporting local government with secure, purpose-built software — helping build the digital foundation of the modern, resilient, cyber-ready Smart Community.

## Your Next Steps Toward Cyber Resilience

### The Springbrook Cybersecurity Resource Center

Access more insights, best practices and actionable strategies to stay ahead of evolving threats.

### Explore the Cirrus Finance Platform: Your Digital Bridge to the Smart Community

Ready to modernize and protect your financial systems? Learn how Cirrus delivers secure, cloud-based financial management built for today's cybersecurity demands.

## Let's talk!

**866-777-0069 | springbrooksoftware.com**

**Join the 3,000+ agencies that are supported by Springbrook solutions. Enterprise-Class Finance Platform for Government.**