Springbrook

Springbrook 2023

# National Cybersecurity Survey

www.springbrooksoftware.com

Springbrook 2023

# National Cybersecurity Survey

## Agency perceptions and the reality of ransomware attacks and cybersecurity.

Between December 2022 and February 2023, the Springbrook Research Institute surveyed local government agency finance officers across the country on their understanding of cybersecurity and the threat landscape. Here are their responses coupled with data from industry sources and our assessments.

### Awareness Versus Reality

**38%**

of those surveyed were unaware of any agencies in their states suffering ransomware attacks.

**33%**

indicated the threat level in their states were "guarded", while 50% claimed it was "elevated." Only 17% stated it was "high."


2023 has been a record year for cyber attacks – with 106 publicly disclosed incidents (Jan-March), many of which were government organizations. [1]

58% of state and local government organizations were hit by ransomware in 2021, up from 34% in 2020 – an increase of 70% over the course of a year [1]. The number of attacks targeting the government sector increased 95% in the second half of 2022 [2].

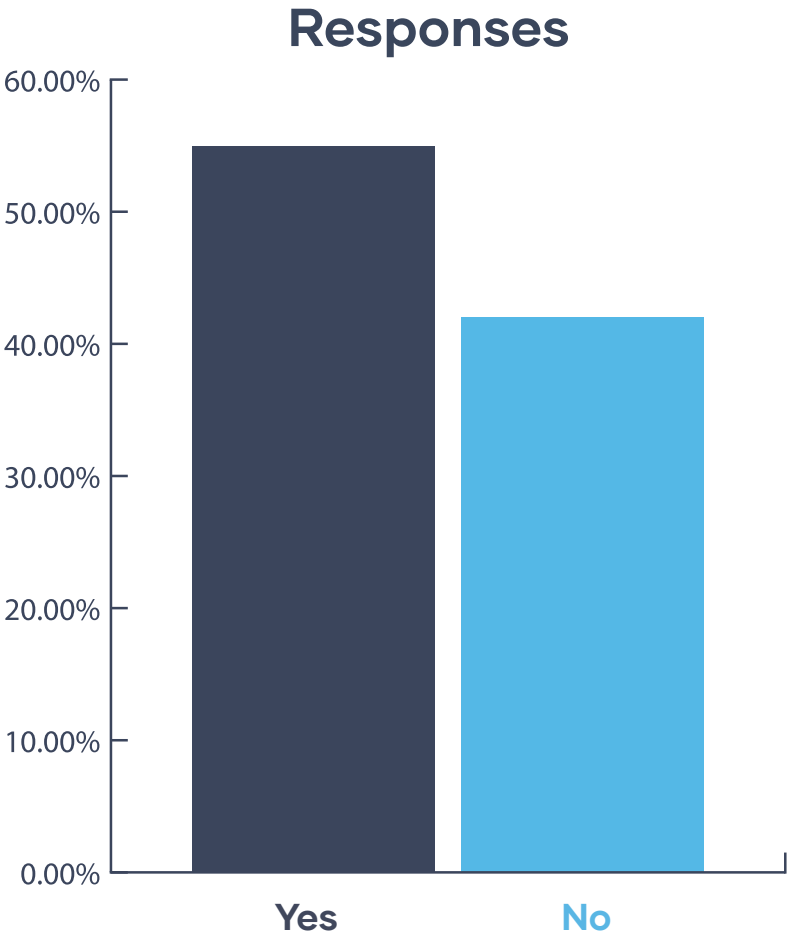
> "The guidance from security organizations Concerning ransomware attacks is"when," not "if." "

The State of Ransomware in State and Local Government 2022: Sophos (1)

Unprecedented Increase in Cyberattacks Targeting Government Entities: CloudSEK XVigil (2)

# Cybersecurity Budgets

## Are You Increasing Your Cybersecurity Budget In 2023?




57% of those surveyed indicated that they were increasing their cybersecurity budgets, while 43% stated that they were not.

**The good news is that 98% of respondents stated that they routinely practice cybersecurity training.**

63% answered that they were familiar with the National Association of State Information Officers, (NASCIO), the organization responsible for pushing cybersecurity initiatives, including the recent $1B State and Local Cybersecurity Grant Program that many agencies applied for earlier in 2023 [1].

The White House has made cybersecurity.  priority one.  The recently announced National Cybersecurity Strategy lays out additional plans for defending critical infrastructure, expanding cybersecurity requirements and defending and modernizing Federal networks. [2].

> **"The Cybersecurity Grant Has Two Functions: To Increase Awareness On Cybersecurity Issues And To Put Money In The Hands Of Agencies To Conduct Audits And Fortify Their Security. Every Agency That Is Not On The Cloud Should Be Actively Budgeting To Fortify Their Security Posture And Increase Their Cyber Hygiene."**

CISA.gov (1)

Fact Sheet: Biden-Harris Administration Announces National Cybersecurity Strategy (2)

# Cybersecurity Grant

**53% of respondents applied for the 2022/2023 State and Local Cybersecurity Grant Program [1]. Springbrook information on the grant can be found here. While 31% received funding, 56% admitted that they "did not know."**


This program, scheduled to disburse

**$400M**

in 2023, requires a state match and a local government competitive grant application to receive funds. Theprogram makes several demands of states, including creating a cybersecurity planning committee and and a statewide guide on how to spend funds.

> "[The Multi-State Information Sharing and Analysis Center (MS-ISAC)] did mention that stakeholders have reported difficulties in applying for the grants, including not having sufficient staff to be able to even write the grant proposals in the first place"

said **Marisol Cruz Cain,** director of the information and cybersecurity team for the Government Accountability Office (GAO). [2] Springbrook's guidance is to gather as much information as possible to successfully apply for these crucial grants. Leverage resources available from organizations like NASCIO and consider hiring a professional grant writer to assist in the process. The Grant is competitive and the dollars are limited.

CISA: State and Local Cybersecurity Grant Program (1)
GovTech: What's Next for State, Local Cybersecurity Grants? (2)

# The State of ERP's

## Age of Software

### 1-3 Years Old 19%

Our most interesting results came from a peek behind the curtain of the types of ERP's that our sampled agencies are relying on. We found that 9% used internally developed (home brewed) solutions, 63% used a combination of vendors and 53% used a solution from one vendor.

### 3-10 Years Old 47%

The final piece of the equation is reflected in the location of the software, with 67% answering that their software resided on premises, and 33% answering "not on premises" to the question, indicting that they were using some form of cloud-based solution.

### 10+ Years Old 34%

**Old software fails on multiple levels, including not meeting citizen expectations, providing an inefficient working environment for staff, and leaving a local agency open for cyber attacks. $1.93 is the average cost of a data breach in the public sector [1], making old software a very costly bet.**

**"With the availability of grant money and numerous vendor and online resources, the ability to move to secure, cloud-based solutions has never been more attainable."**

IBM: Cost of a Data Breach 2022 (1)

For more information: The Springbrook Cybersecurity Resource Center.

Cybersecurity Resource Center

For more information: Springbrook's Cirrus: Modern, secure cloud ERP solution:

Springbrook's Cirrus