The State of Ransomware in State and Local Government 2022

Javier Huito Pacheco
EAE
Javier.Huito@sophos.com

SOPHOS

About the Survey

5,600
respondents

199
State/Local Government respondents

31
countries

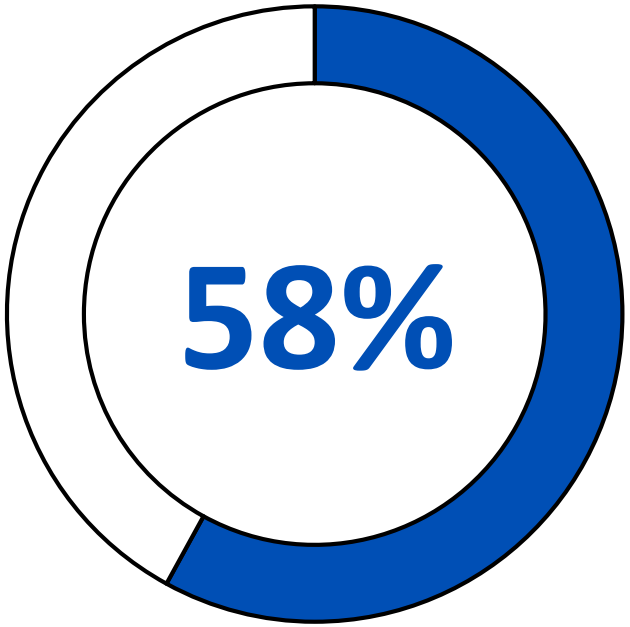
100-5,000
employees

Jan/Feb 2022
research conducted

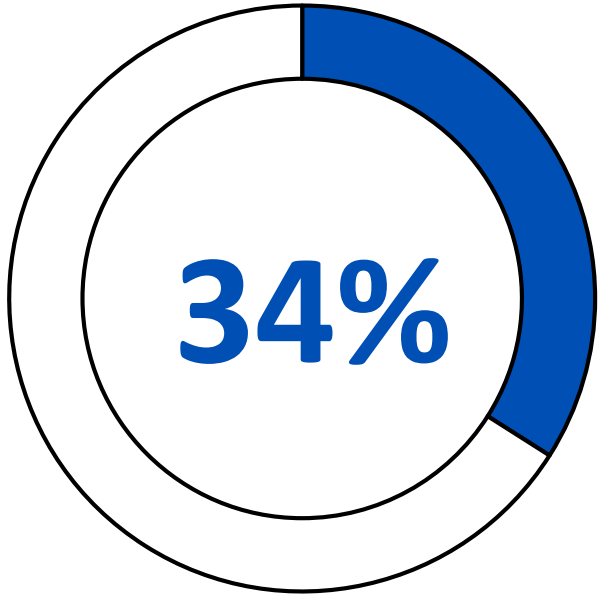
VansonBourne
research provider

The Reality of Ransomware

Ransomware Attacks in State and Local Government Increased Last Year



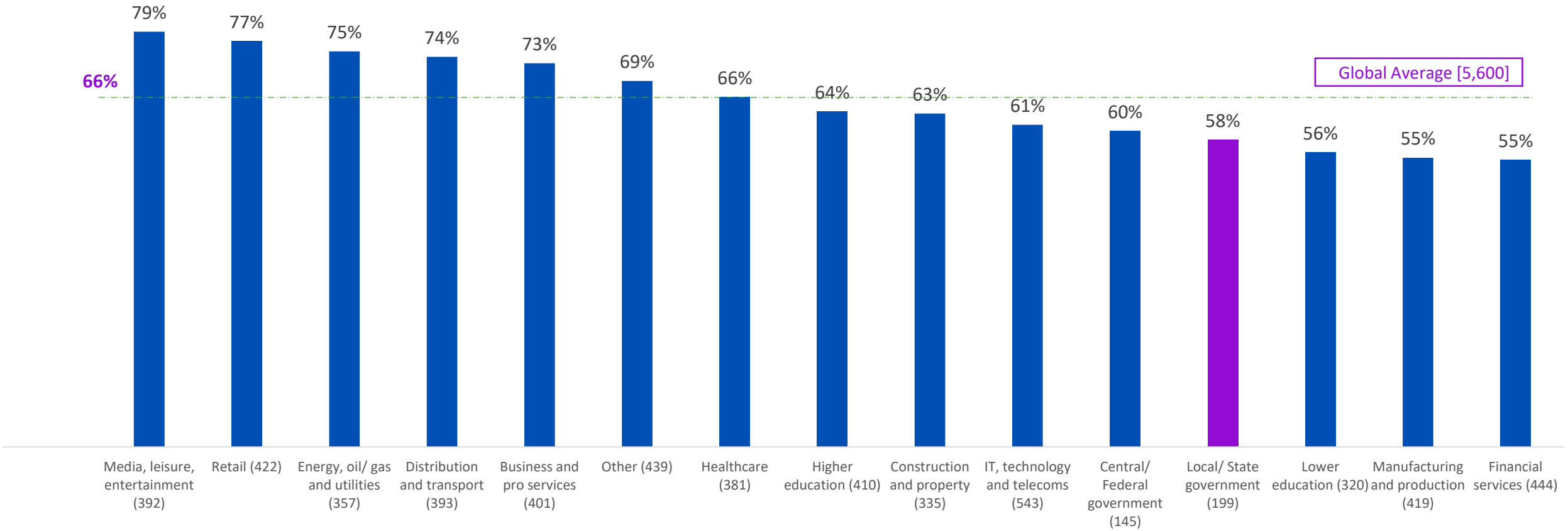
2021



2020

In the last year, has your organization been hit by ransomware? (2021: 199 local government respondents; 2020: 131 local government respondents): Yes

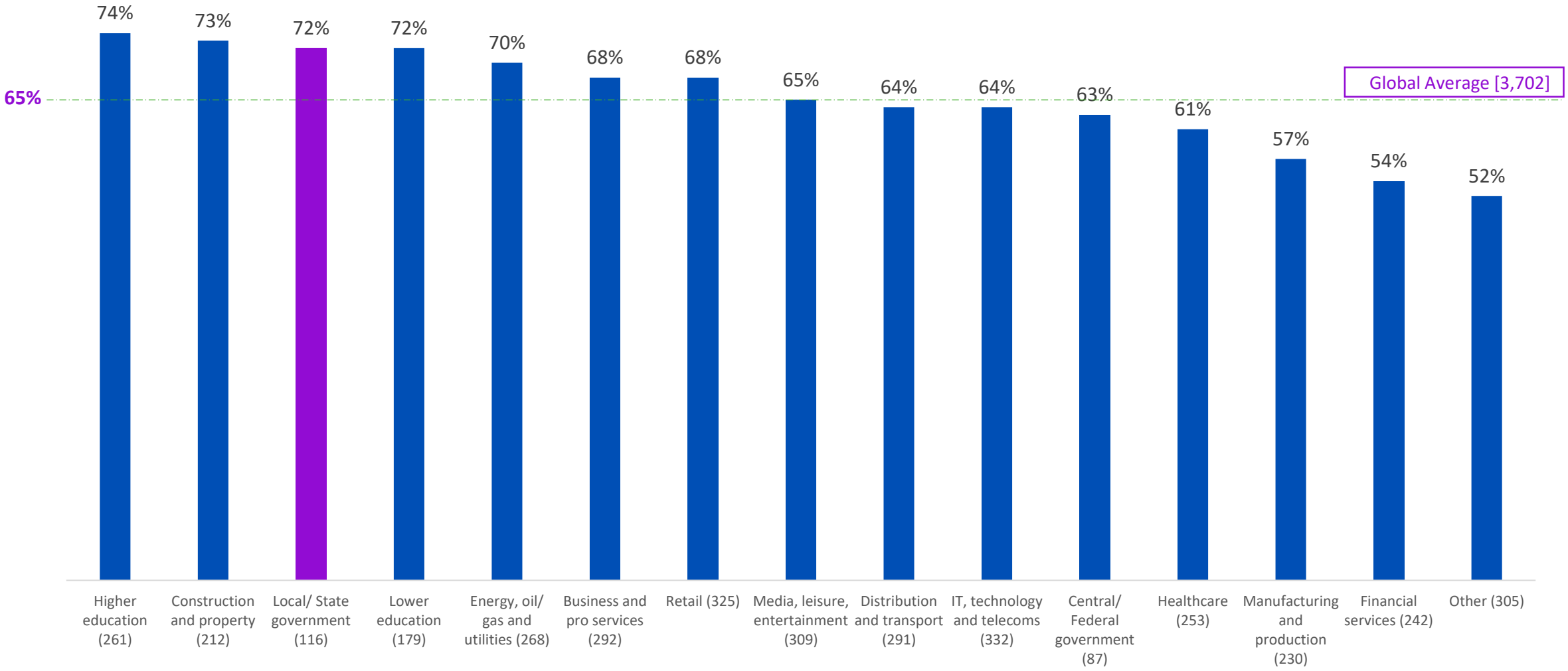
State and Local Government Has Below-Average Attack Rate



In the last year, has your organization been hit by ransomware? (n=5,600): Yes

SOPHOS

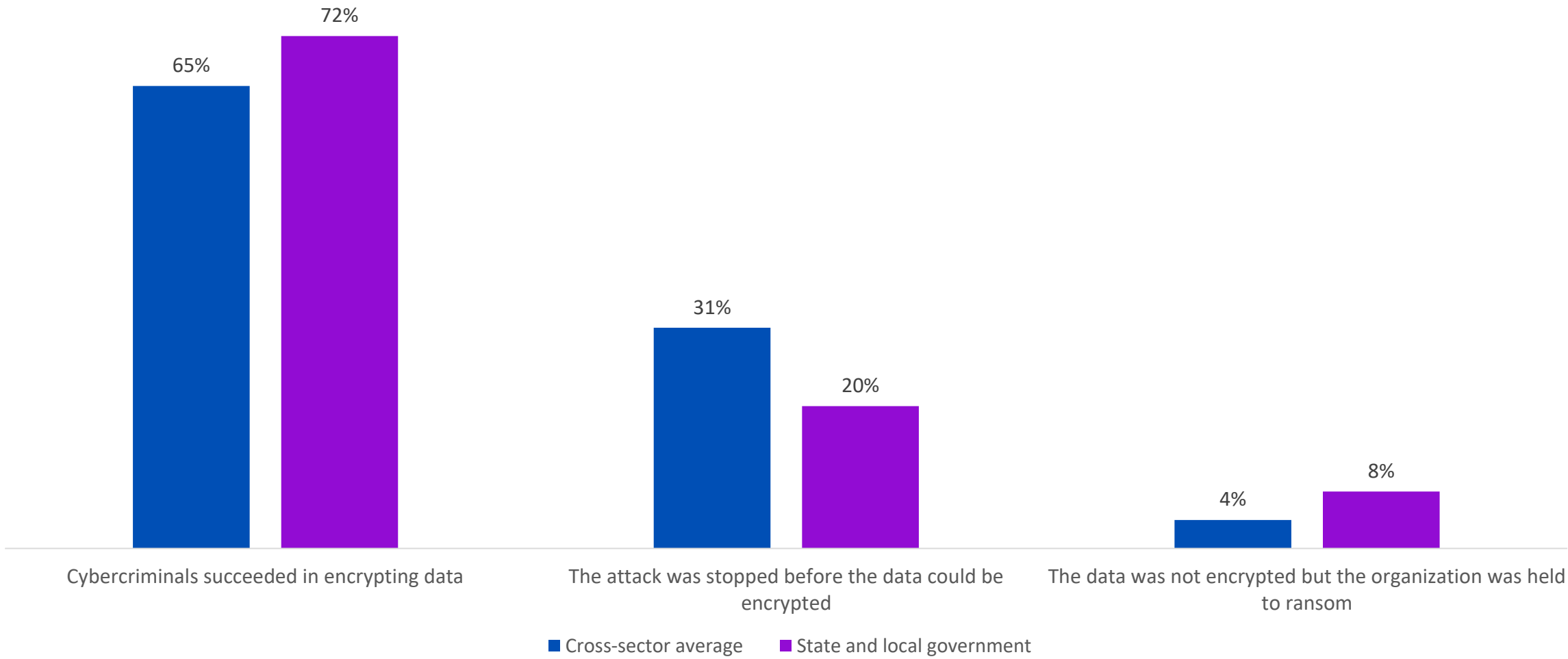
State and Local Government Has a High Encryption Rate



Did the cybercriminals succeed in encrypting your organization's data in the most significant ransomware attack? (n=3,702 organizations hit by ransomware in the last year): Yes

SOPHOS

Ability to Stop Ransomware Attacks by State and Local Government

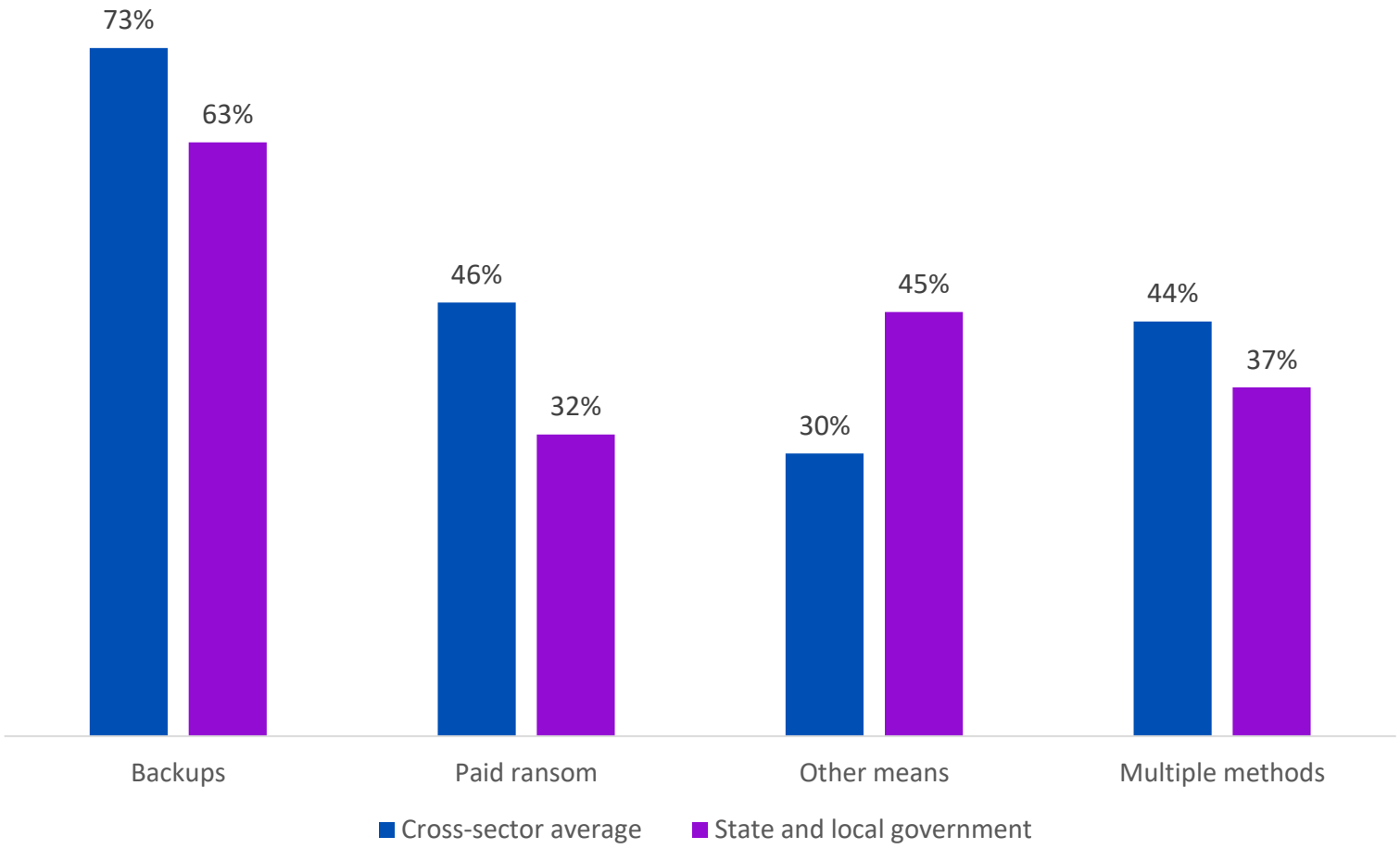


Did the cybercriminals succeed in encrypting your organization's data in the most significant ransomware attack? (3702 cross-sector; 116 state and local government organizations hit by ransomware in the last year)

SOPHOS

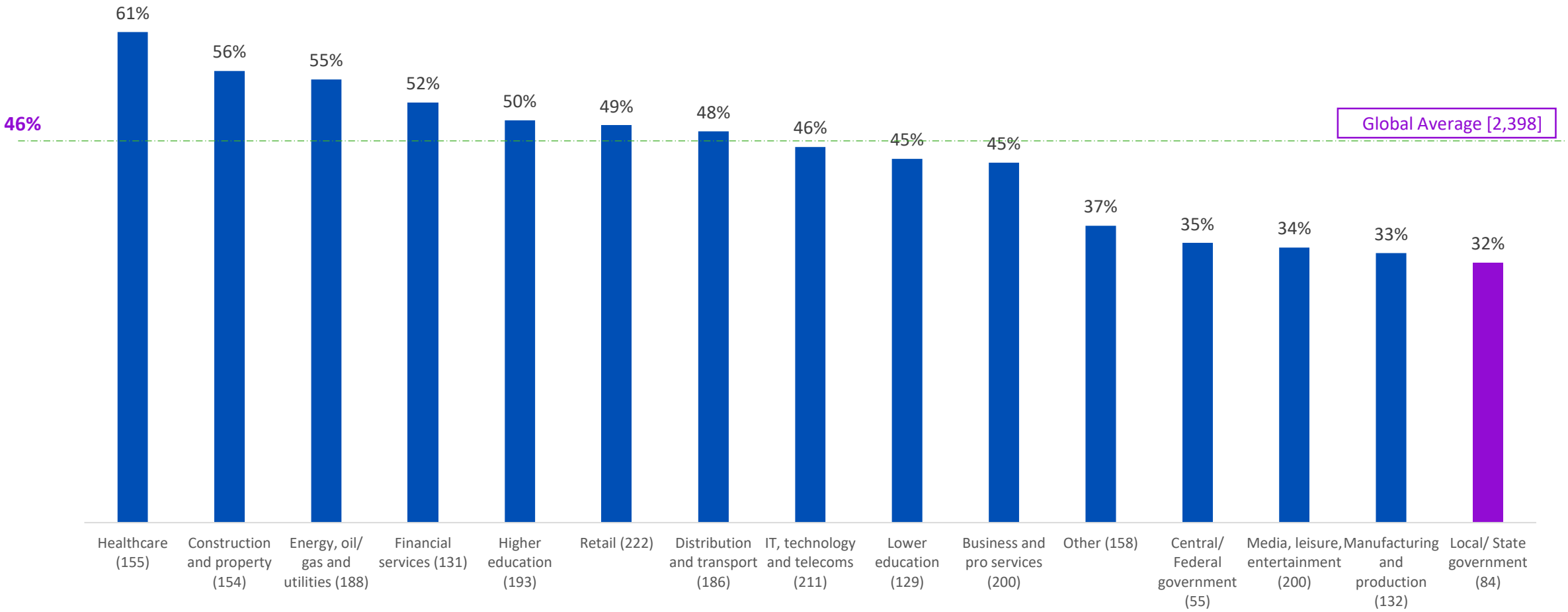
Most State and Local Government Victims Get Some Encrypted Data Back

99%
got some encrypted data back



Did your organization get any data back in the most significant ransomware attack? (2398 cross-sector; 84 state and local government organizations that had data encrypted): Yes, we paid the ransom and got data back, Yes, we used backups to restore the data, Yes, we used other means to get our data back.

State and Local Government Has Lowest Ransom Payment Rate



Did your organization get any data back in the most significant ransomware attack? (n=2,398 organizations that had data encrypted): Yes, we paid the ransom and got data back

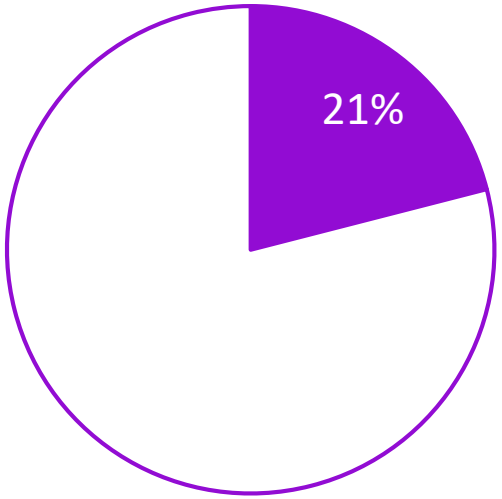
SOPHOS

Ransom Payments Have Increased Across Sectors

965 respondents shared the ransom payment

3X

Percentage paying ransoms of US$1M or more



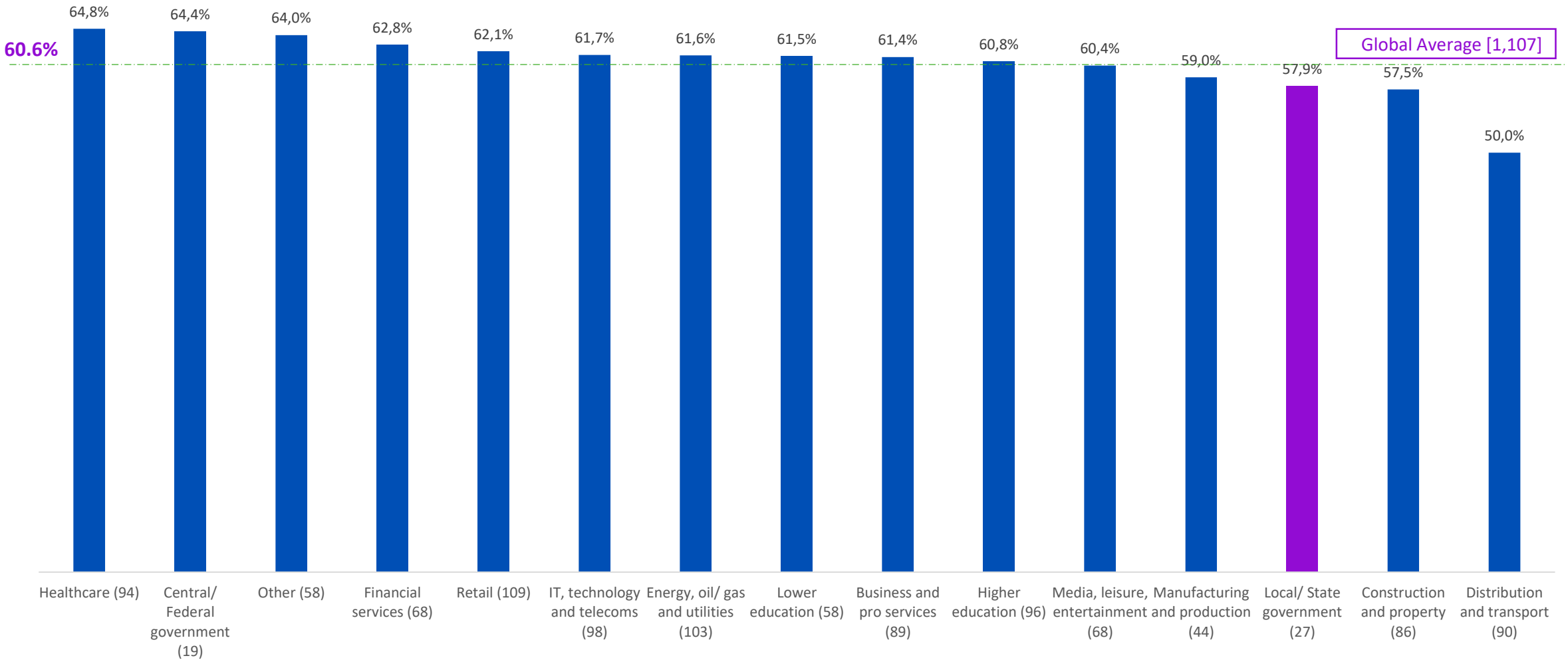
Percentage paying ransoms of less than US$10,000

$812,360

Average ransom payment

How much was the ransom payment your organization paid in the most significant ransomware attack? US$. Excluding "Don't know" responses and outliers. (n=965 organizations that paid the ransom).

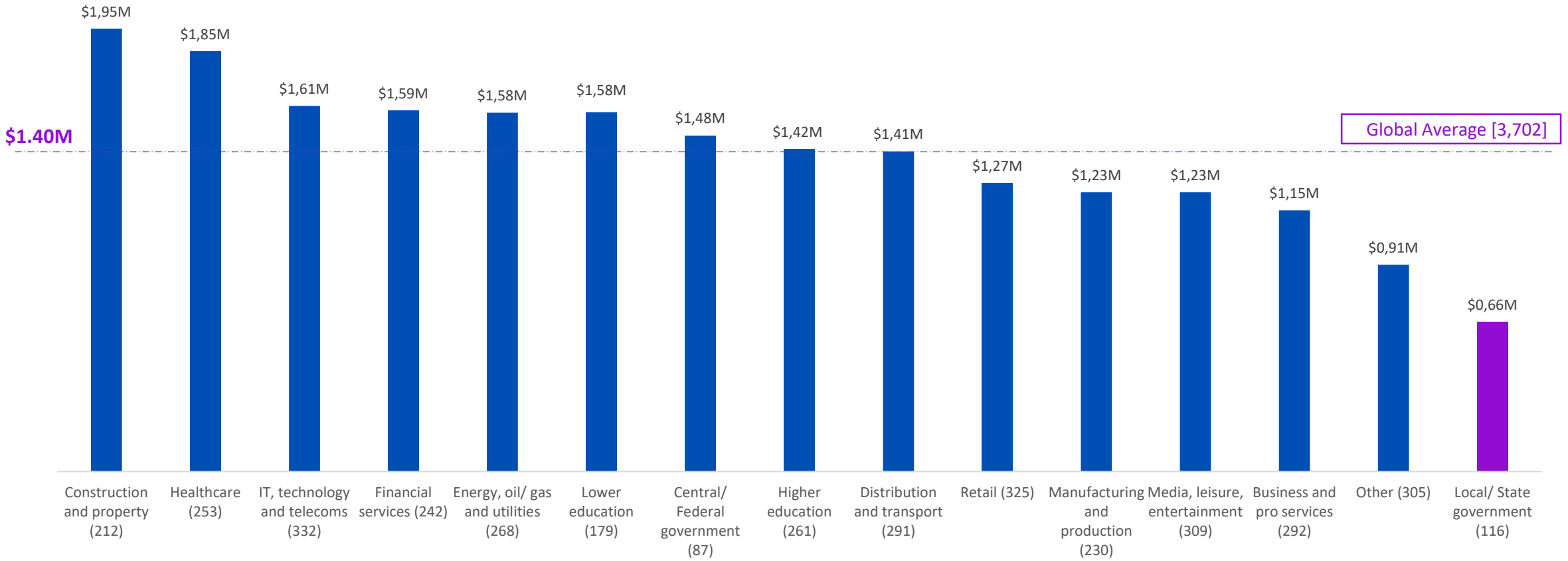
Percentage of Encrypted Data Recovered After Paying the Ransom



How much of your organization's data did you get back in the most significant ransomware attack? (1,107 organizations that paid the ransom and got data back)

The Impact of Ransomware

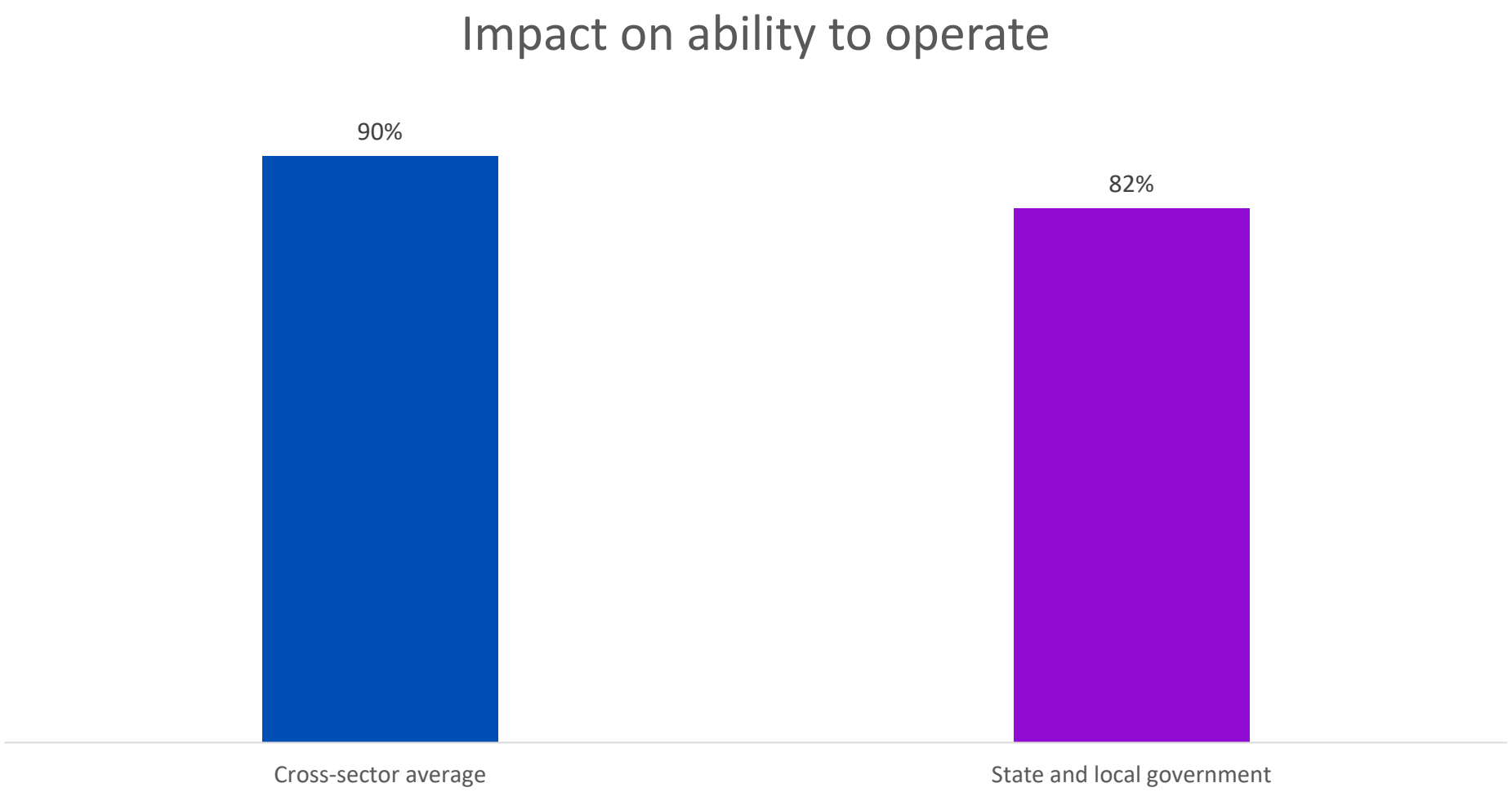
Cost to Rectify Attacks in State/Local Government Organizations



What was the approximate cost to your organization to rectify the impacts of the most recent ransomware attack (considering downtime, people time, device cost, network cost, lost opportunity, ransom paid etc.)? (3,702 organizations that were hit by ransomware)

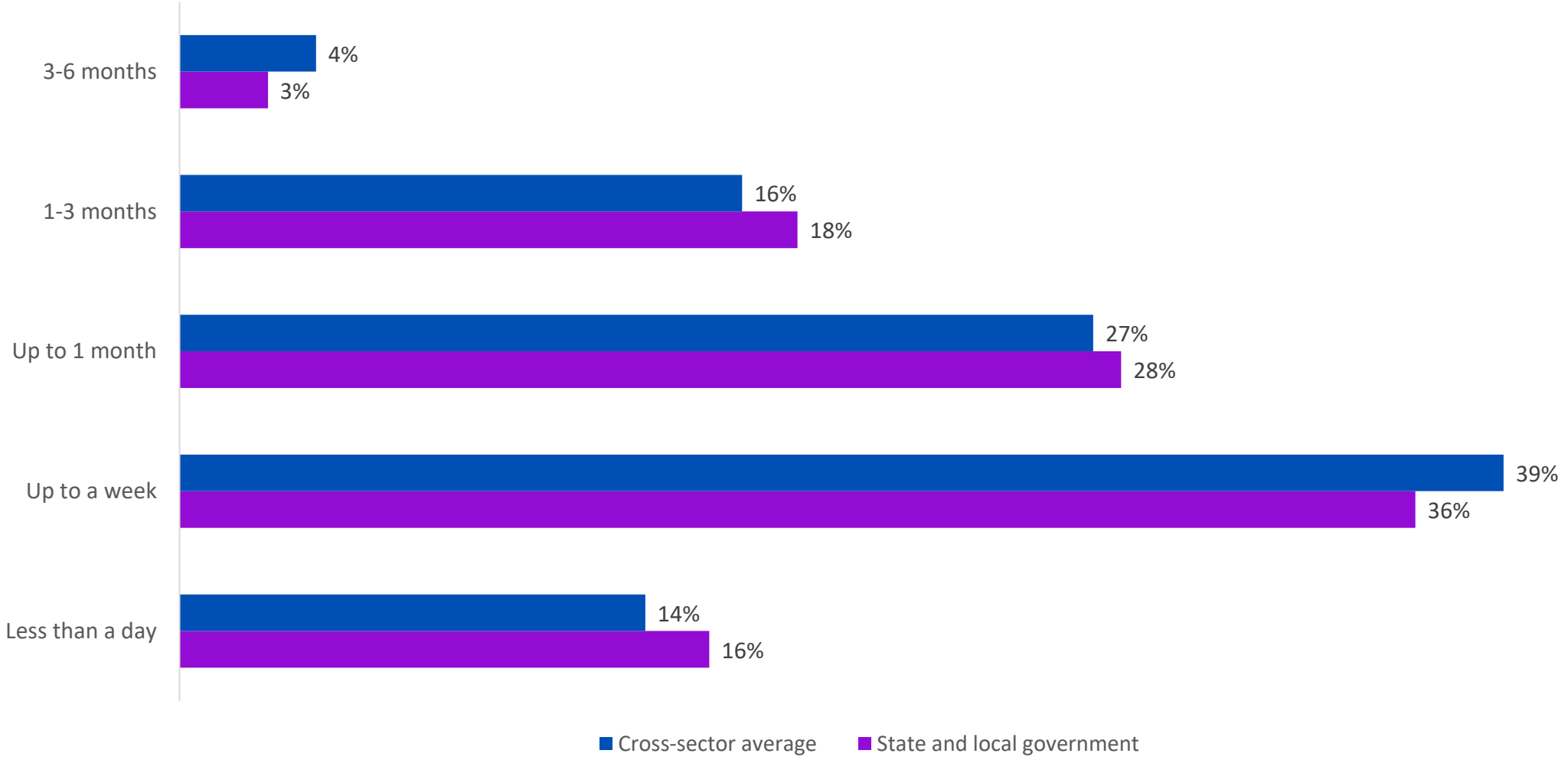
SOPHOS

Operational Impact of Ransomware on Victims



Did the most significant ransomware attack impact your organization's ability to operate? (n=3702; 116 local government organizations that were hit by ransomware in the previous year)
Excluding some answer options.

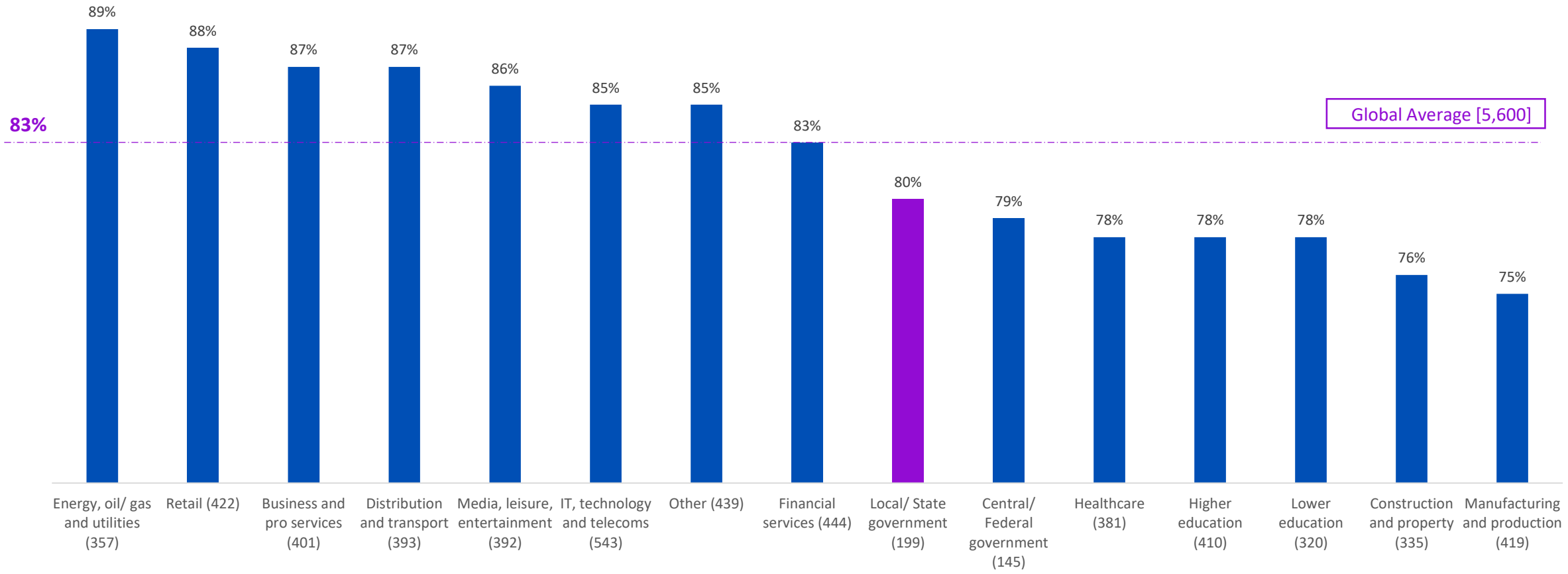
Ransomware Recovery Time in State/Local Government Organizations



How long did it take your organization to fully recover from the most significant ransomware attack? (3702/116 state and local government organizations that were hit by ransomware in the previous year)

The Role of Cyber Insurance

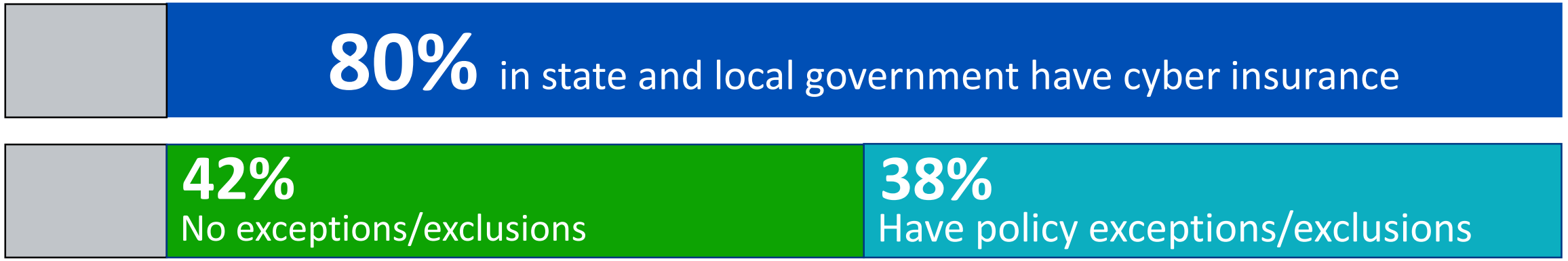
State and Local Government Has Low Cyber Insurance Coverage for Ransomware



Does your organization have cyber insurance that covers it if it is hit by ransomware? (base numbers in chart). Yes; Yes, but there are exceptions/exclusions in our policy

SOPHOS

Ransomware Insurance Coverage In State and Local Government



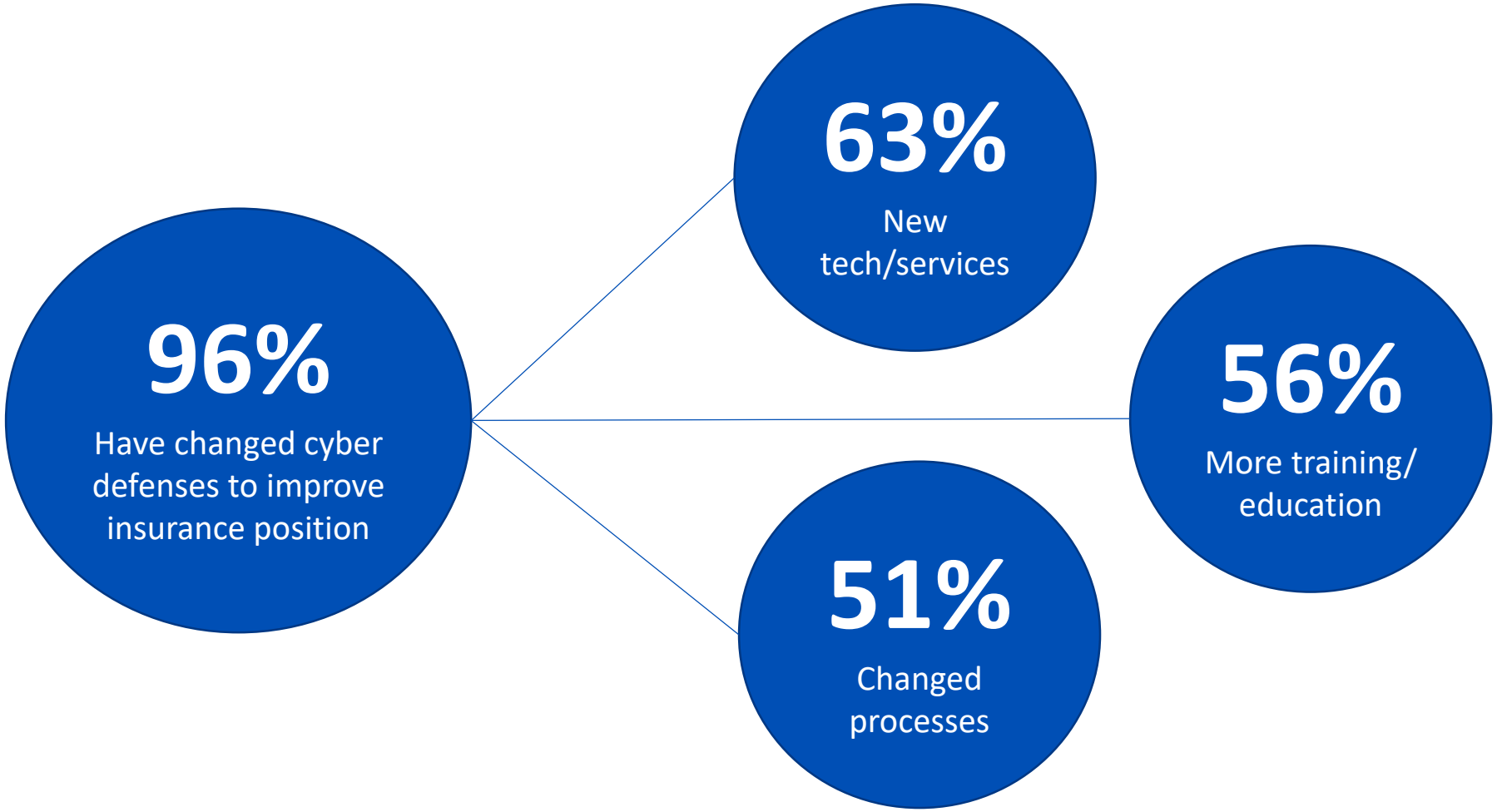
Does your organization have cyber insurance that covers it if it is hit by ransomware? (199 state and local government organizations that said "Yes" and "Yes, but there are exceptions/exclusions in our policy")

Cyber Insurance Getting Harder to Secure in State/Local Government

43%	Fewer providers now offer cyber insurance
55%	Higher level of cybersecurity needed
41%	Policies are more complex
33%	The process takes longer
28%	It’s more expensive

How has your organization’s experience of getting cyber insurance changed over the last 12 months? (176 state and local government respondents whose organization has cyber insurance)

Cyber Insurance Is Driving Improvements to Cyber Defenses



Over the last year has your organization made any changes to its cyber defenses to improve its insurance position? (176 state and local government respondents whose organization has cyber insurance. Excludes some answer options)

Conclusion

The State of Ransomware 2022 in State and Local Government

Ransomware attacks have increasing

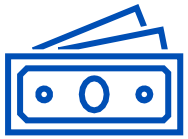
Data restoration via backups is considerably below average

Least likely to pay the ransom to restore data

Lowest average ransom recovery bill

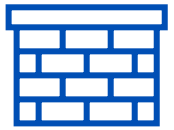
Ransomware has a major impact on ability to operate

Having cyber insurance is the norm



Below-average insurance payout rate, payout rate for clean-up costs considerably lower than the average

Securing coverage has got much harder



Organizations are improving their cyber defenses to get coverage

Five Top Tips to Minimize Your Exposure to Ransomware

1	Ensure high quality defenses at all points in your environment
2	Proactively hunt for threats – work with a services partner if needed
3	Harden your environment – XDR is a very useful tool
4	Have a cyber incident response plan
5	Make backups and practice restoring from them

How Sophos Can Help

How Sophos Can Help

1 Ensure high quality defenses at all points in your environment

Automatically block ransomware threats *before* they can be deployed

Lock down Remote Desktop Protocol to prevent adversaries using it to gain access

Identify and mitigate vulnerabilities in cloud environments to prevent exploitation

Provide cybersecurity awareness training and phishing testing for your users

How Sophos Can Help

2 Proactively hunt for threats

Managed by Sophos

Sophos Managed Detection and Response service

24/7 threat hunting, detection and response delivered by an expert team as a fully-managed service.

Managed by Customer

Sophos Extended Detection and Response

Enabling advanced threat detection, investigation and response across endpoint, servers, firewall, cloud workloads, email, mobile, and more.

How Sophos Can Help

3 Harden your environment

Sophos Extended Detection and Response

- Identify outdated and unsupported software and systems
- Check installed applications against online vulnerability information
- Identify security posture weaknesses in registry settings
- Easily access information on all applications inc. patch info and logs
- Identify devices without cybersecurity software installed

How Sophos Can Help

We've updated the visual for the report – use new vesion

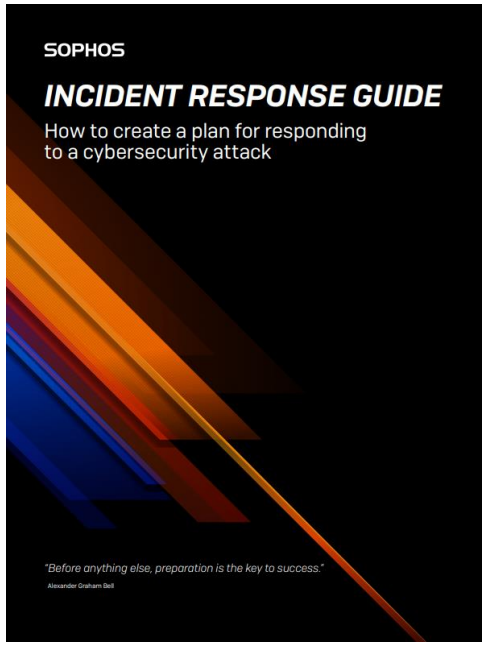
4 Have a cyber incident response plan

Sophos Managed Threat Response service

Includes 24/7/365 emergency incident response for active threats

Sophos Rapid Response service

24/7/365 emergency incident response available to all organizations – no need to be an existing Sophos customer



www.sophos.com/en-us/whitepaper/incident-response-guide

Multi-layered Defense Against Ransomware

SOPHOS
Cybersecurity delivered.

Top Ransomware Controls and How Sophos Can Help

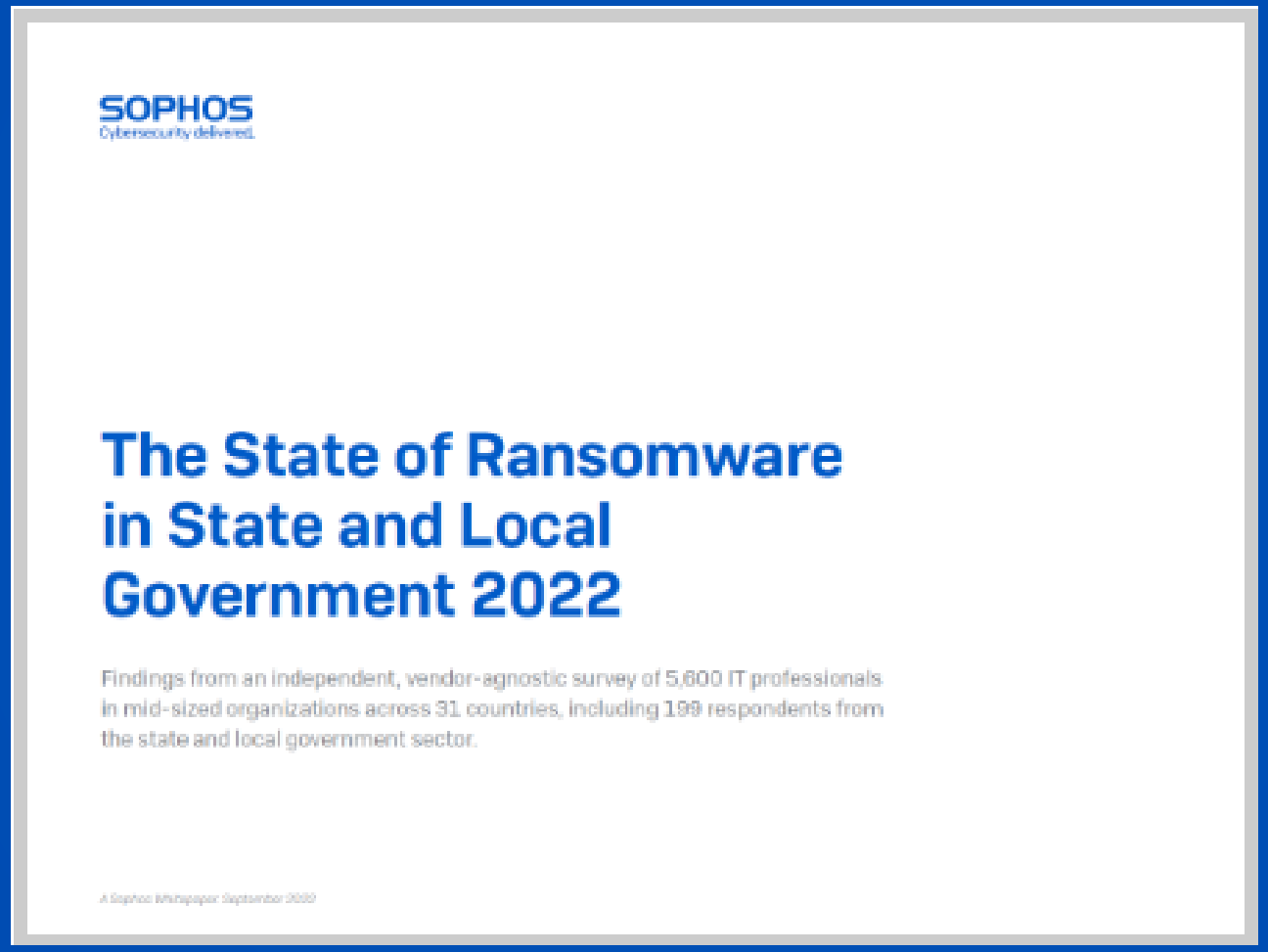
The ransomware challenge continues to grow. The proportion of organizations hit by ransomware has almost doubled in twelve months, up from 37% in 2020 to 66% in 2021. Adversaries have also become more successful at encrypting data, with 65% of attacks resulting in data encryption last year*.

Stopping ransomware requires efforts to prevent both advanced, hands-on-keyboard attacks executed by skilled adversaries as well as the growing success of the Ransomware-as-a-Service model, which significantly extends the reach of ransomware by reducing the skill level required to deploy an attack.

This guide details the top cybersecurity controls that minimize ransomware exposure and impact and how Sophos can help.

A Sophos Solution Brief. April 2022

Read the State of Ransomware in Government 2022 Report



SOPHOS

Cybersecurity delivered.