The State of Ransomware in Education 2023

Hywel Morgan (CISSP, CCSP)

19th October 2023

SOPHOS

Estimating Risk

Bungee

Scuba Diving

Sky Diving

Which has the highest risk?

Calculating Risk

RISK = FREQUENCY x IMPACT

Source Data

SOPHOS

The State of Ransomware 2023

Findings from an independent, vendor-agnostic survey of 3,000 leaders responsible for IT/cybersecurity across 14 countries, conducted in January-March 2023.

A Sophos Whitepaper. May 2023

Introduction

Sophos' annual study of the real-world ransomware experiences of IT/cybersecurity leaders makes clear the realities facing organizations in 2023. It reveals the most common root causes of attacks and shines new light on how experiences with ransomware differ based on organization revenue. The report also reveals the business and operational impact of paying the ransom to recover data rather than using backups.

About the Survey

Sophos commissioned an independent, vendor-agnostic survey of 3,000 IT/cybersecurity leaders in organizations with between 100 and 5,000 employees across 14 countries in the Americas, EMEA, and Asia Pacific. The survey was conducted between January and March 2023, and respondents were asked to respond based on their experiences over the previous year.

Within the education sector, respondents were split into lower education (catering to students up to 18 years) and higher education (for students over 18 years).

3,000
respondents

14
countries

100-5,000
employee organizations

Jan-Mar 2023
research conducted

<$10M - $5B+
annual revenue

Findings from an Independent Survey of IT Professionals

3,000
respondents

400
education respondents

100-5,000
employees

14
countries

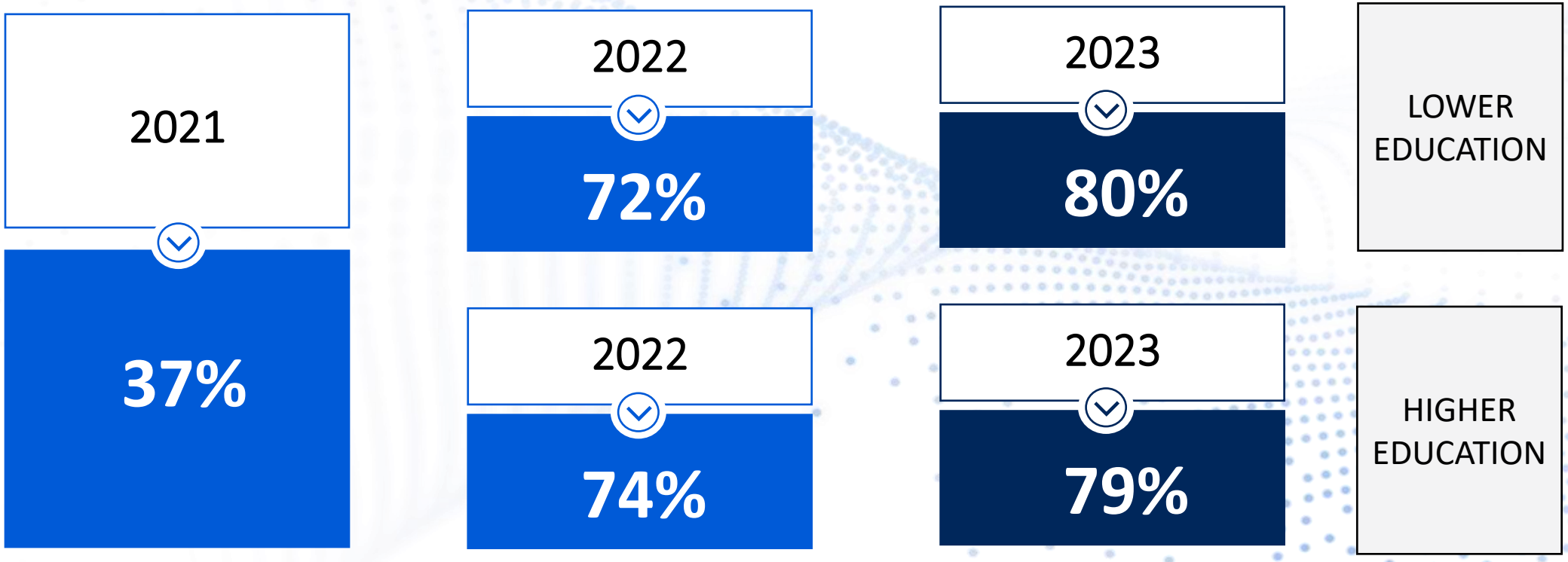
Jan-Mar 23
research conducted

SOPHOS

Frequency of Ransomware

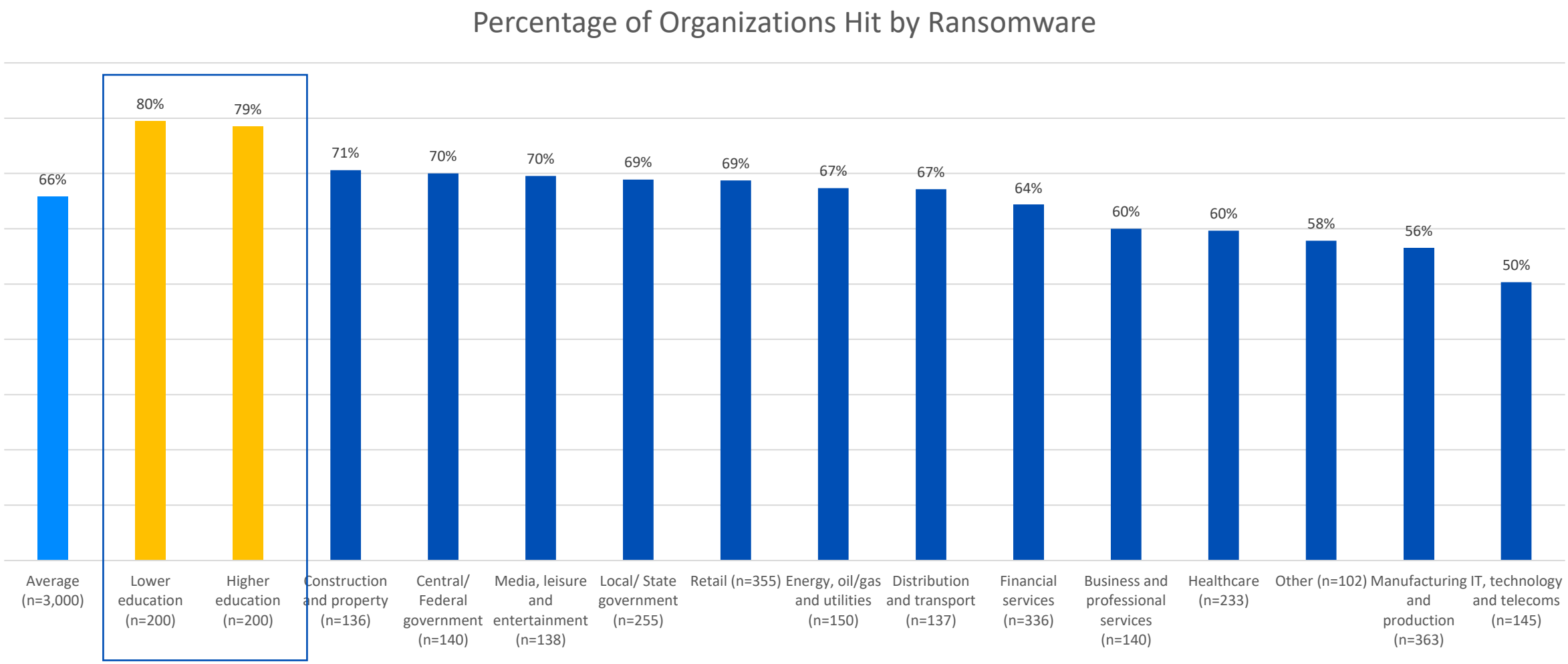
Rate of Ransomware Attacks in Education

The percentage of education organizations hit by ransomware in the last year has continued to rise



In the last year, has your organization been hit by ransomware? Yes. n=400 (2023), 440, (2022), 499 (2021)

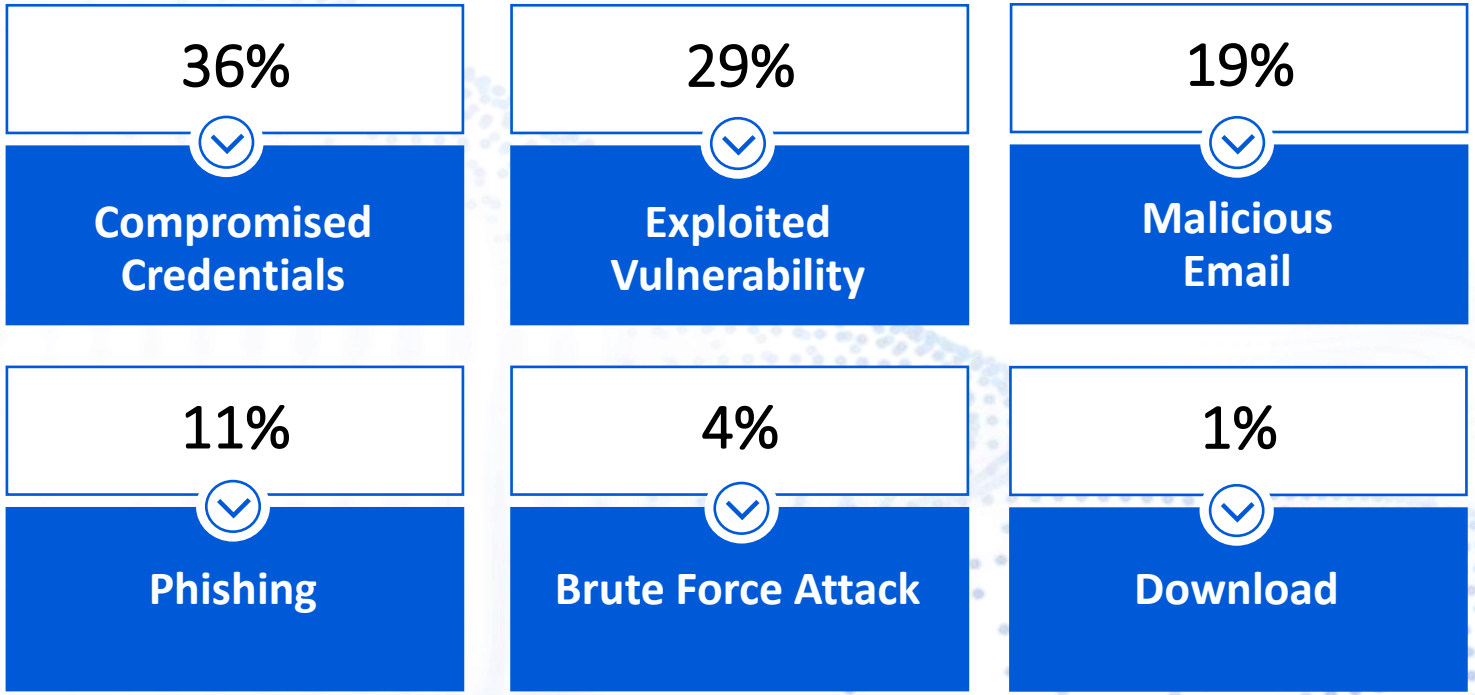
Ransomware Attacks by Industry



In the last year, has your organization been hit by ransomware? Base numbers in chart

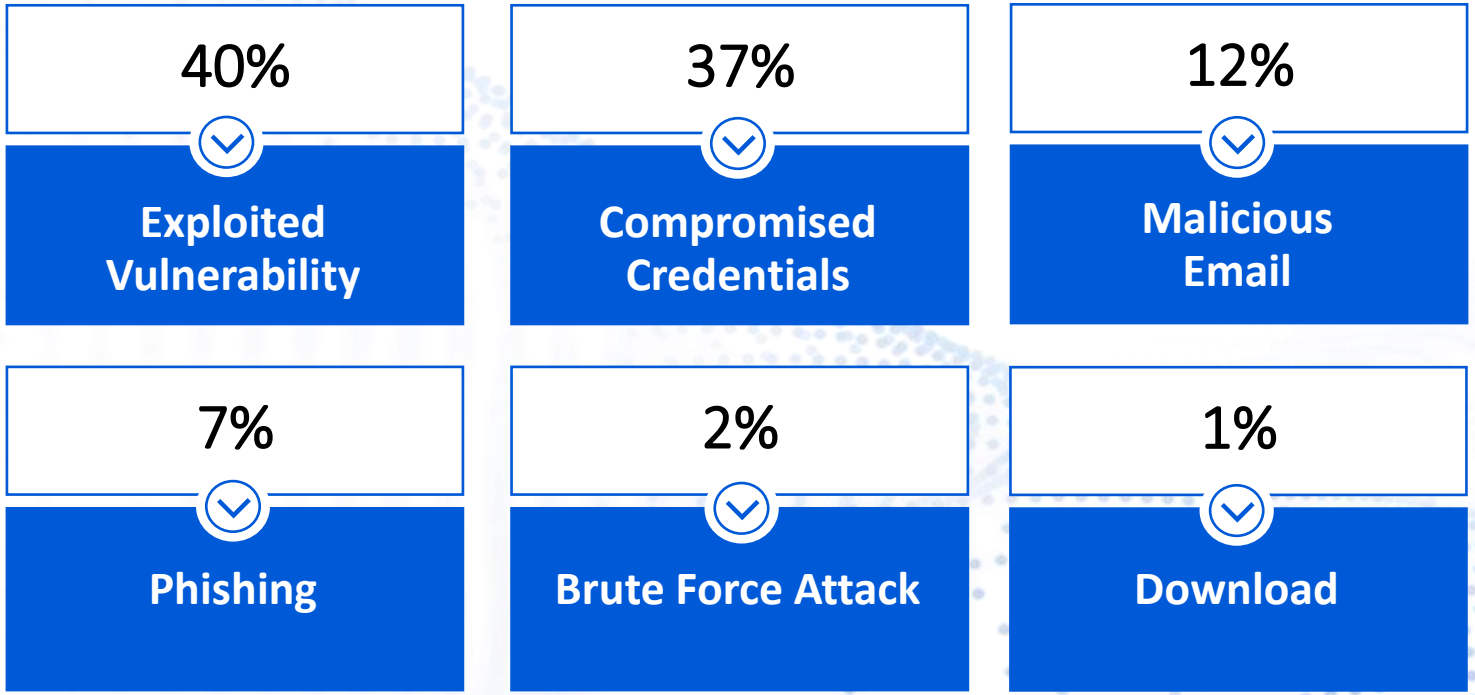
SOPHOS

Root Cause of Attack: Lower Education



Do you know the root cause of the ransomware attack your organization experienced in the last year? If you were hit more than once, think about the most significant attack (n=159 lower education organizations hit by ransomware in the last year)

Root Cause of Attack: Higher Education



Do you know the root cause of the ransomware attack your organization experienced in the last year? If you were hit more than once, think about the most significant attack (n=157 higher education organizations hit by ransomware in the last year)

SOPHOS

Compromised Credentials

- 40% of Education attacks
- 50% in other Sectors
- A similar study from the U.S. Cybersecurity and Infrastructure Security Agency (CISA), found 54% of initial access points was due to compromised credentials

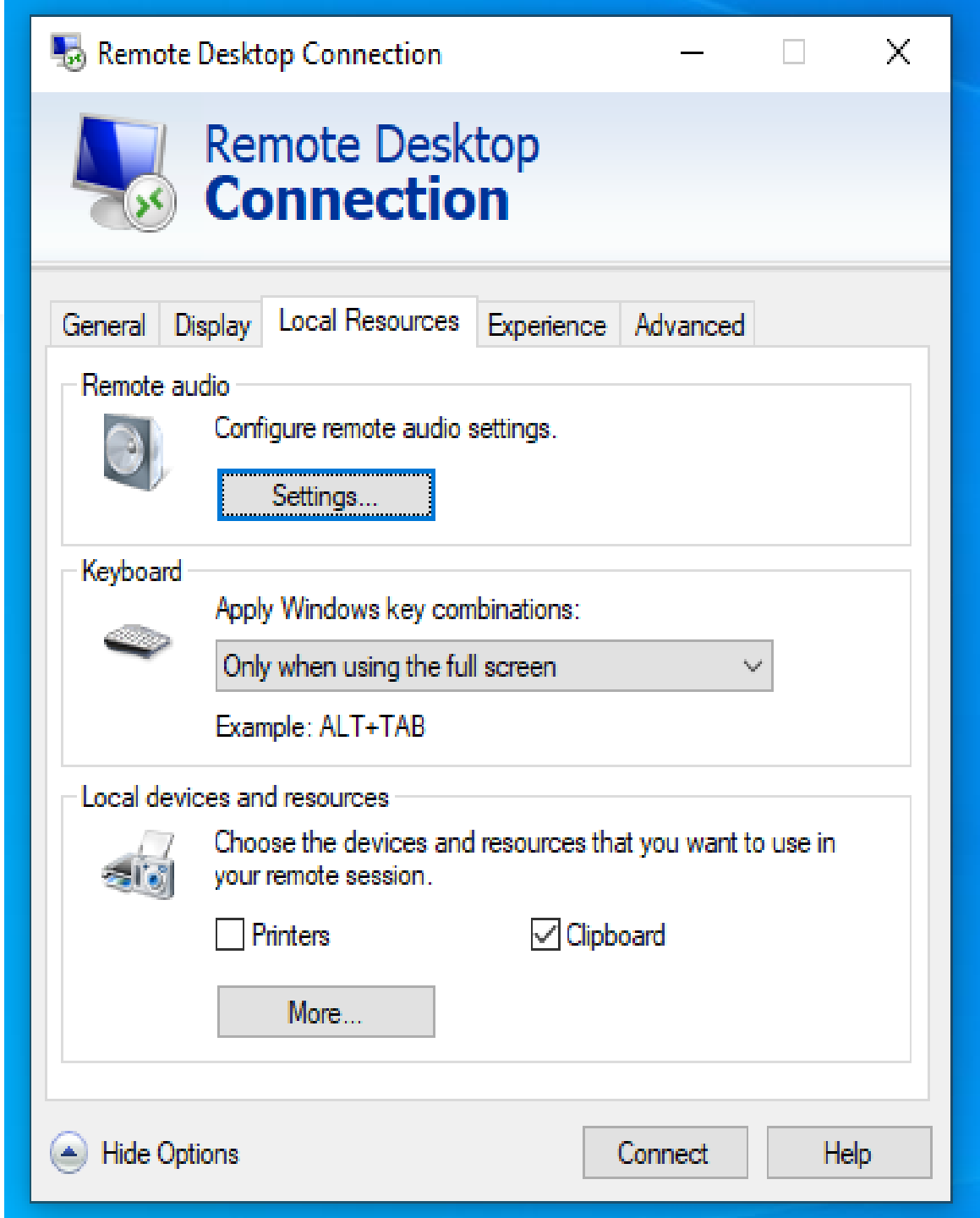
Patch and Patch Fast!

- 30-40% of attacks exploited a vulnerability in OS or App
- The U.S. Cybersecurity and Infrastructure Security Agency states:
  - Critical vulnerabilities must be remediated within **15 calendar days of initial detection**
  - High vulnerabilities must be remediated within **30 calendar days of initial detection**
- 3CX attacks all occurred on the 30th March.
- PaperCut's Two vulnerabilities took 10 and 11 days respectively
- 39% attacks use "Bring Your Own Vulnerable Driver (BYOVD)" techniques by attackers.

Remote Disaster Protocol

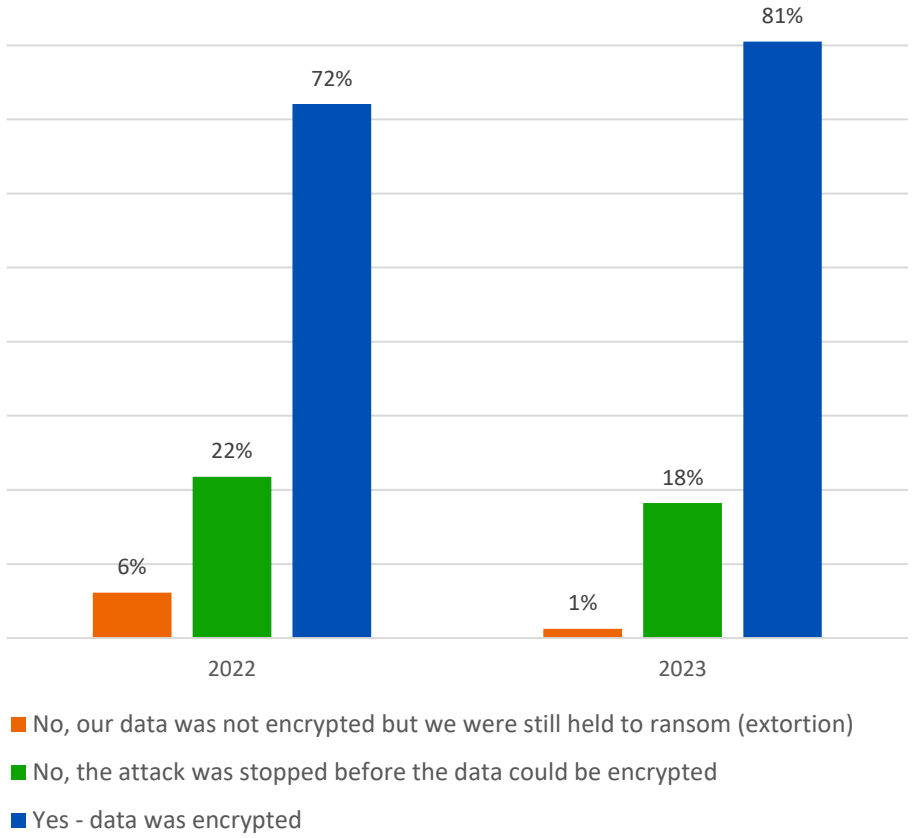
93% of attacks use Remote Desktop Protocol

- 93% (**YES 93%**) used by attackers internally within customer networks
- 18% Unprotected and exposed to the Internet for Threat Actors to walk straight in

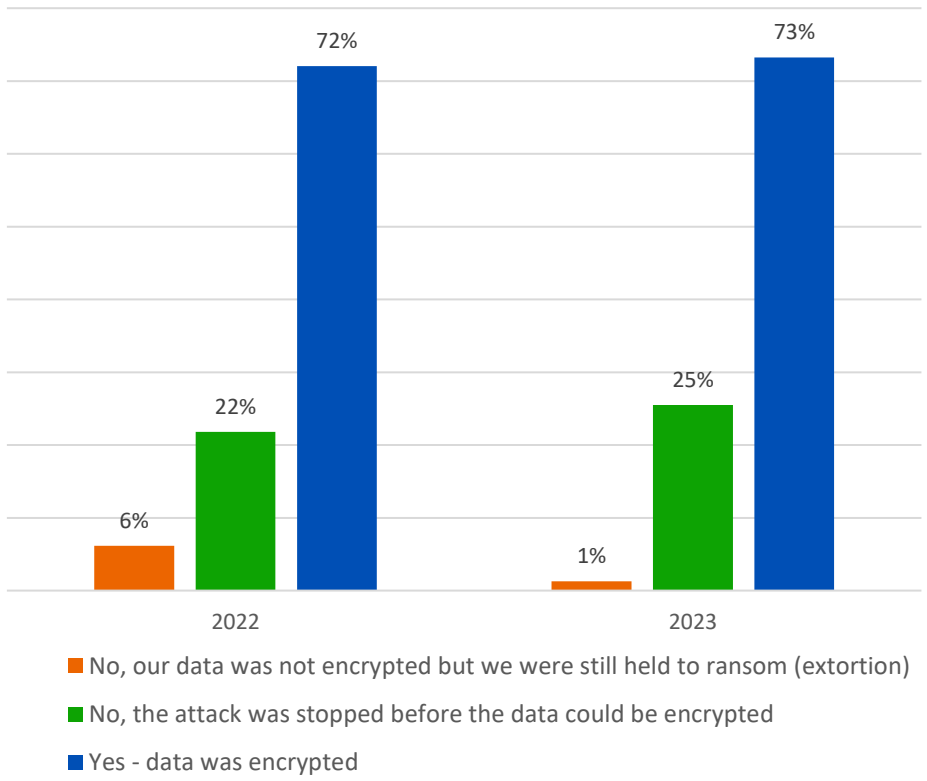


Data Encryption in Education

Lower Education



Higher Education



Did the cybercriminals succeed in encrypting your organization's data in the ransomware attack? Selection of answer options. Lower education n= 159 (2023), 179 (2022), Higher education n=157 (2023), 261 (2022)

SOPHOS

Impact of Ransomware

Data Recovery: Lower Education

Use backups to restore data	Paid the ransom and got data back	Use other means to get data back
73% (76% in 2022)	47% (45% in 2022)	2%

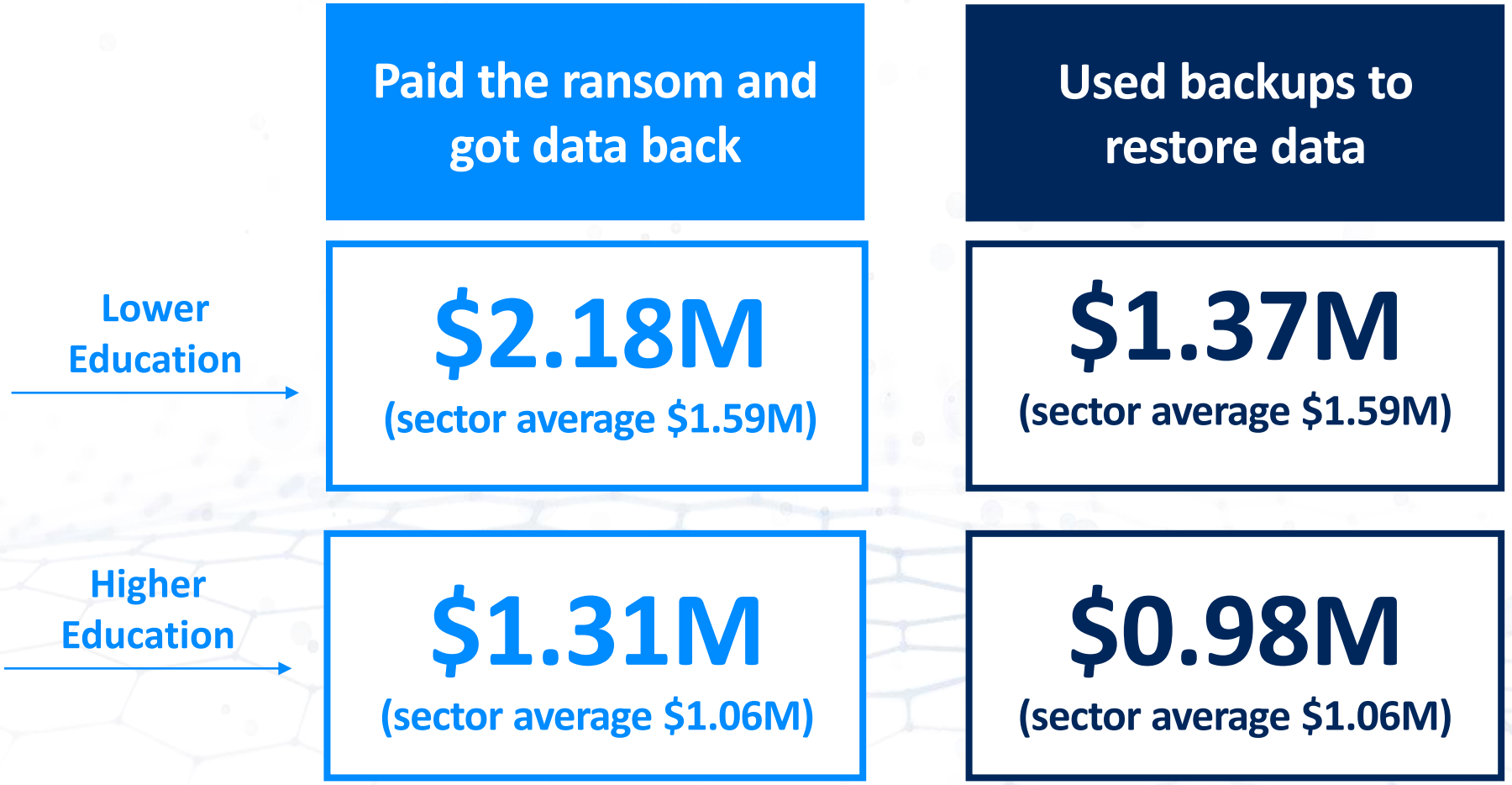
Did your organization get any data back? n=128 lower education organizations that were hit by ransomware and had data encrypted

Data Recovery: Higher Education

Use backups to restore data	Paid the ransom and got data back	Use other means to get data back
63% (70% in 2022)	56% (50% in 2022)	3%

Did your organization get any data back? n=115 higher education organizations that were hit by ransomware and had data encrypted

Recovery Cost by Data Recovery Method (Mean)



What was the approximate cost to your organization to rectify the impacts of the most significant ransomware attack (considering downtime, people time, device cost, network cost, lost opportunity etc.)? n=60 (ransom)/94 (backups) in lower ed and n=64 (ransom)/73 (backups) in higher ed

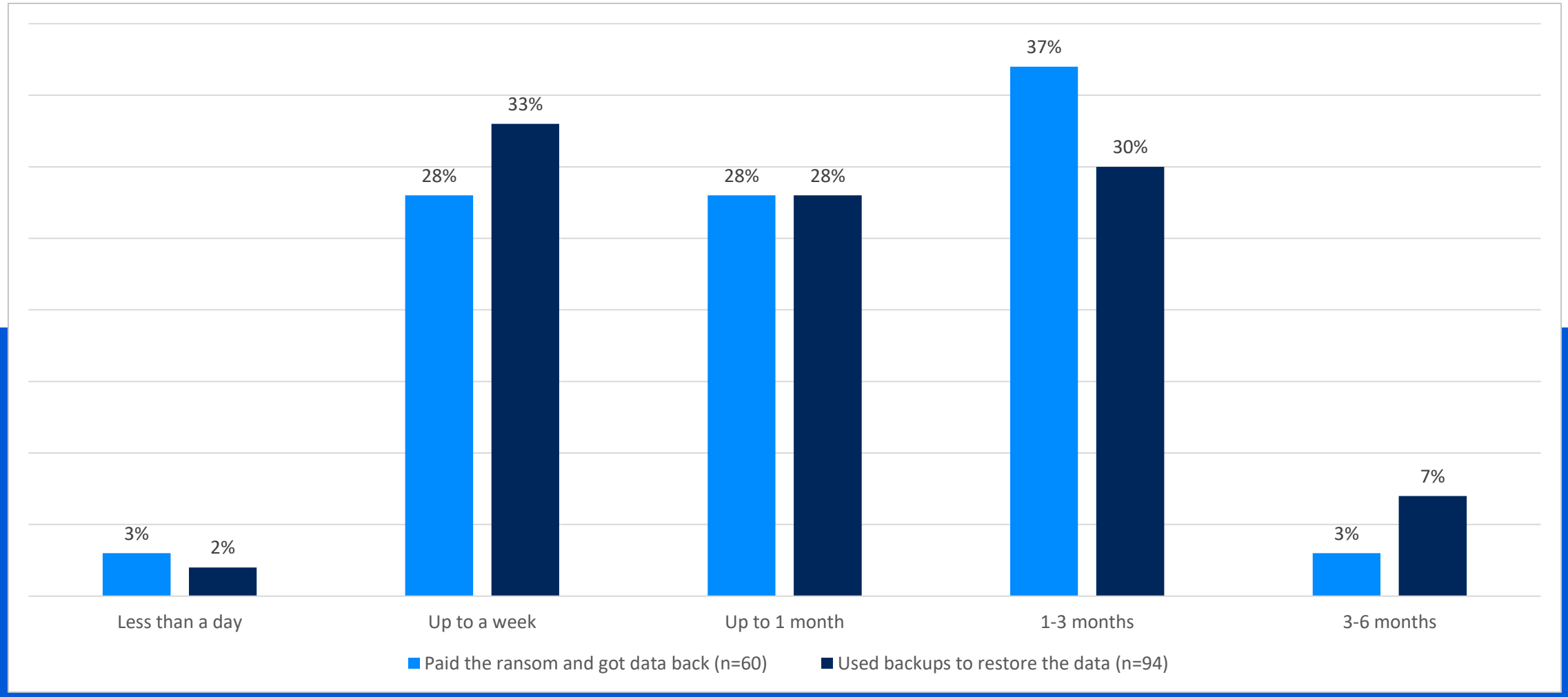
Double Dip: Ransomware + Data Theft

Percentage of ransomware attacks where data was encrypted that also had data stolen

Lower Education	Higher Education
27%	35%

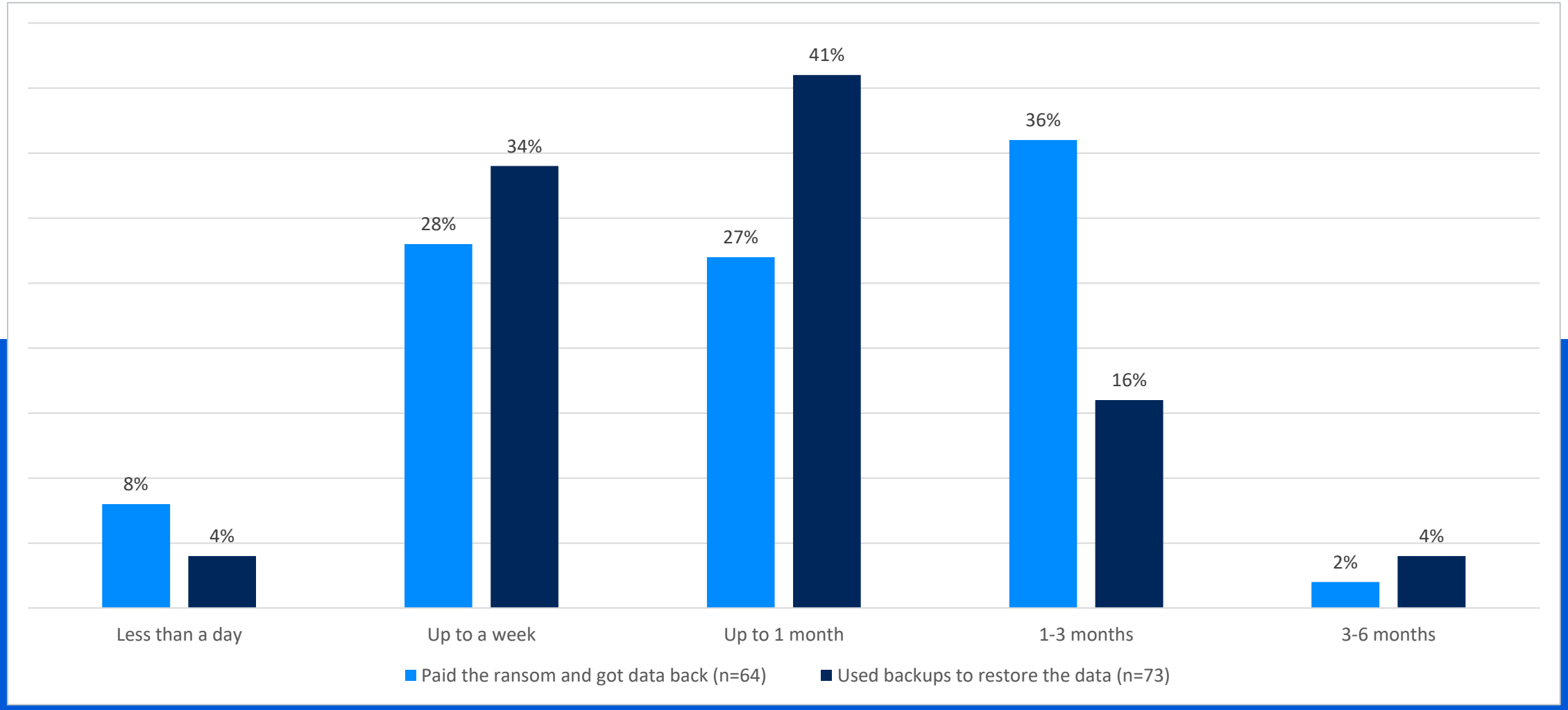
Did the cybercriminals succeed in encrypting your organization's data in the ransomware attack? Yes/Yes, and the data was also stolen n=128 (lower), 155 (higher)

Recovery Time by Data Recovery Method: Lower Education



How long did it take your organization to fully recover from the ransomware attack? Organizations that paid the ransom and/or used backups to recover data. Base numbers in chart

Recovery Time by Data Recovery Method in Higher Education



How long did it take your organization to fully recover from the ransomware attack? Organizations that paid the ransom and/or used backups to recover data. Base numbers in chart

SOPHOS

Report Summary

Education is one of the sectors most impacted by ransomware

Adversaries continue to evolve their attacks, and the data encryption rate is increasing

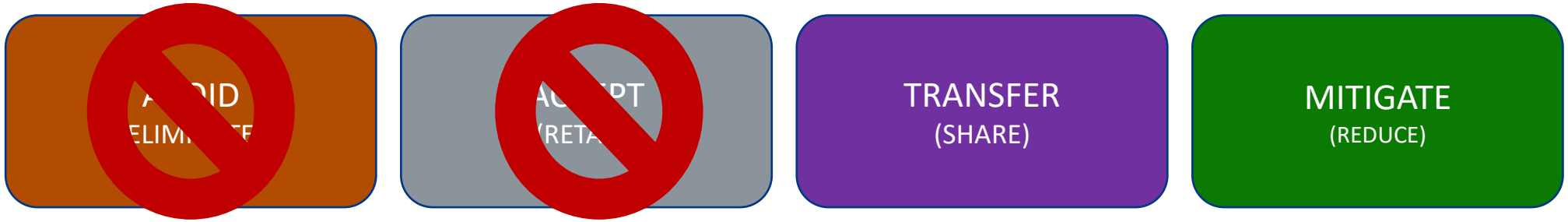
Data theft in addition to data encryption is now commonplace

The use of ransom payments for data recovery has increased in education, while backups have dropped

Ransomware has major financial and operational impacts

Recovery is cheaper if you use backups rather than paying the ransom

Risk Management Strategies



Continuous improvement recommendations

Strengthen Defensive Shields

- Protection against the most common attack vectors
- Adaptive technologies that respond automatically to an attack
- 24/7 threat detection, investigation and response

Optimize Attack Preparation

- Taking regular backup
- Practicing recovering data from backups
- Maintaining an up-to-date incident response plan

Maintain Good Security Hygiene

- Timely patching
- Use MFA
- Regularly reviewing security tool configuration
- Use your security tools and don’t ignore alerts

Sophos Can Help

Latest Adversary Behaviors

90% of ransomware attacks occur outside standard work hours

9 in 10 attacks occur outside 8am to 6pm on a weekday. 43% of attacks are launched on a Friday or Saturday.

Ransomware dwell time has almost halved since 2022

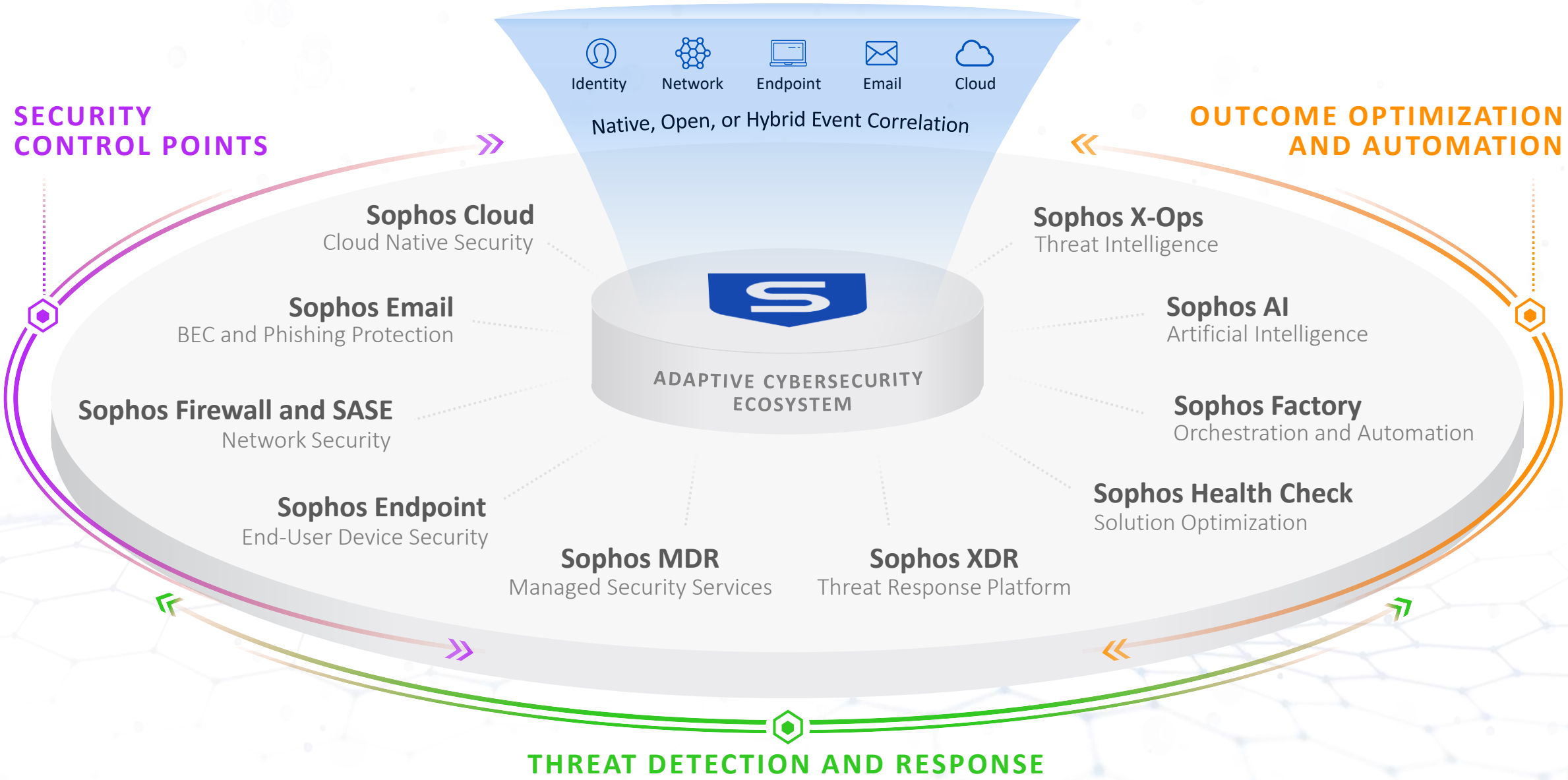
The median ransomware dwell time has fallen from 9 days in 2022 to 5 days in the first half of 2023.

Source: The 2023 Active Adversary Report for Tech Leaders, Sophos, August 2023

Changing the Story: A Two-Prong Approach

Slow Adversaries

Accelerate Defenders


Identity
Network
Endpoint
Email
Cloud
Native, Open, or Hybrid Event Correlation
SECURITY CONTROL POINTS
OUTCOME OPTIMIZATION AND AUTOMATION
Sophos Cloud
Cloud Native Security
Sophos Email
BEC and Phishing Protection
Sophos Firewall and SASE
Network Security
Sophos Endpoint
End-User Device Security
Sophos MDR
Managed Security Services
Sophos XDR
Threat Response Platform
Sophos X-Ops
Threat Intelligence
Sophos AI
Artificial Intelligence
Sophos Factory
Orchestration and Automation
Sophos Health Check
Solution Optimization
ADAPTIVE CYBERSECURITY ECOSYSTEM
THREAT DETECTION AND RESPONSE

SOPHOS

Sophos MDR: The Best Ransomware Defense

24/7 human-led threat detection and response service with extensive experience in stopping advanced ransomware attacks

Most Trusted. Highest Rated.

Sophos MDR secures **more organizations** than any other MDR vendor

The **highest rated** and **most reviewed** MDR Service on Gartner Peer Insights

No vendor has been **named a Gartner Leader** in endpoint security more times than Sophos

Meets You Where You Are

Compatible with your environment
We use our tools and 3rd party tools

Compatible with your needs
From full IR to help making decisions

Compatible with your business
Deep experience across every industry

SOPHOS

Estimating Risk

Bungee

3rd Place

1 in 500,000

Scuba Diving

1st Place

1 in 34,400

Sky Diving

2nd Place

1 in 101,083

Sophos Education Portal

https://www.sophos.com/en-us/solutions/industries/education

State of Ransomware

https://www.sophos.com/en-us/whitepaper/state-of-ransomware-in-education

SOPHOS

Cybersecurity delivered.