Cybersecurity in Education Agencies

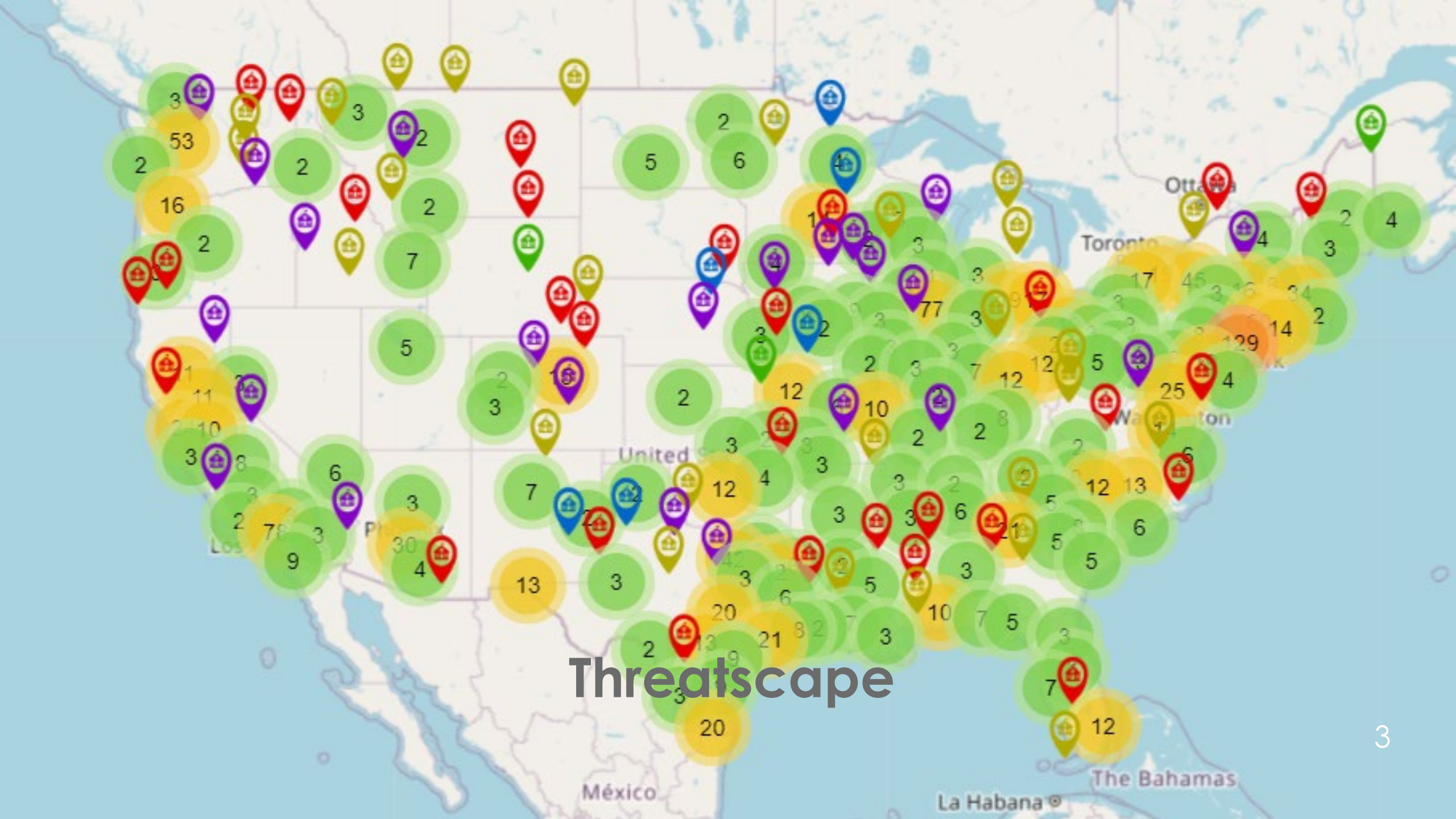
Steven Hernandez, U.S. Department of Education
Will Goodman, Boise School District (ID)

National Forum on Education Statistics

State of Cybersecurity

- Threatscape
- Supply Chain and Vendor Security
- Actionable Steps, first things first

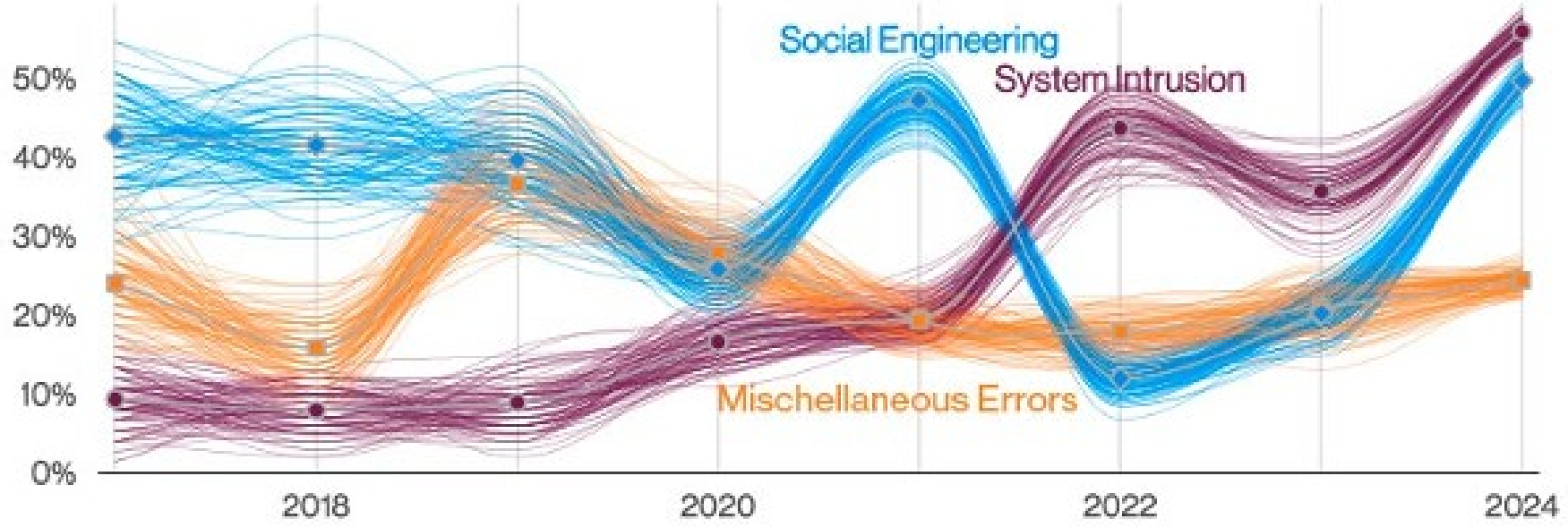
Controlled Unclassified Information (CUI)


Threatscape
Ottawa
Toronto
United States
México
The Bahamas
La Habana

State of Education Sector

- Verizon 2024 Data Breach Investigations Report (DBIR)

  Education Sector

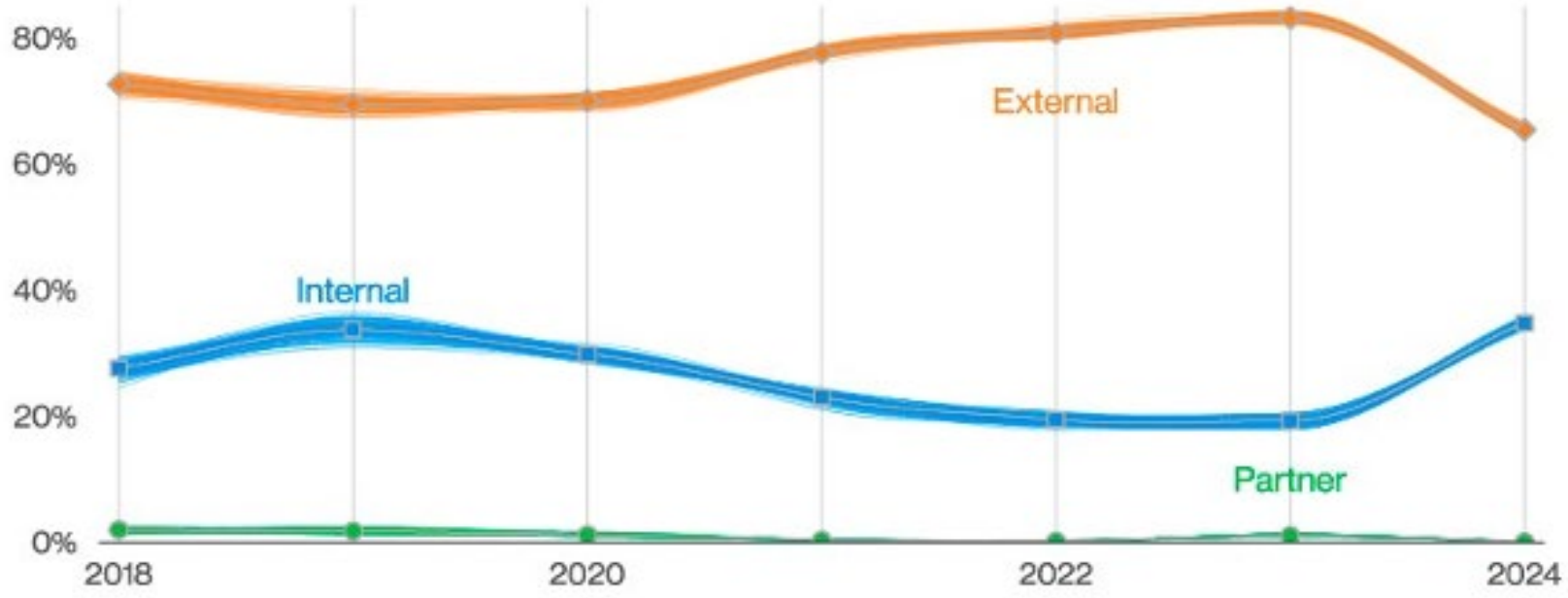


https://www.verizon.com/business/resources/reports/dbir

State of Education Sector

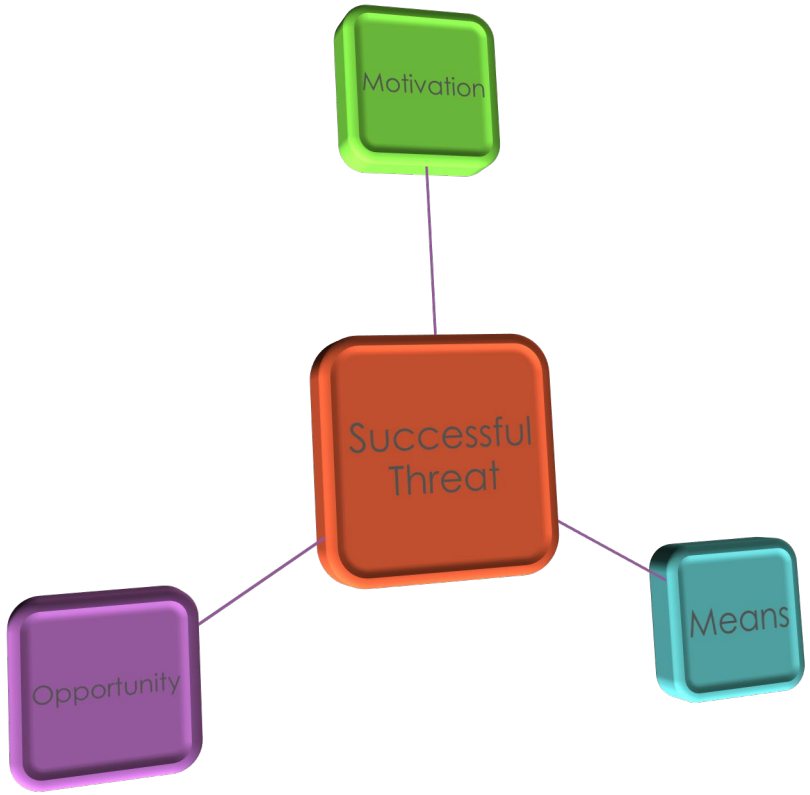
- Verizon 2024 Data Breach Investigations Report (DBIR)

  Threat Actors



https://www.verizon.com/business/resources/reports/dbir

State of Education Sector Threat Actors



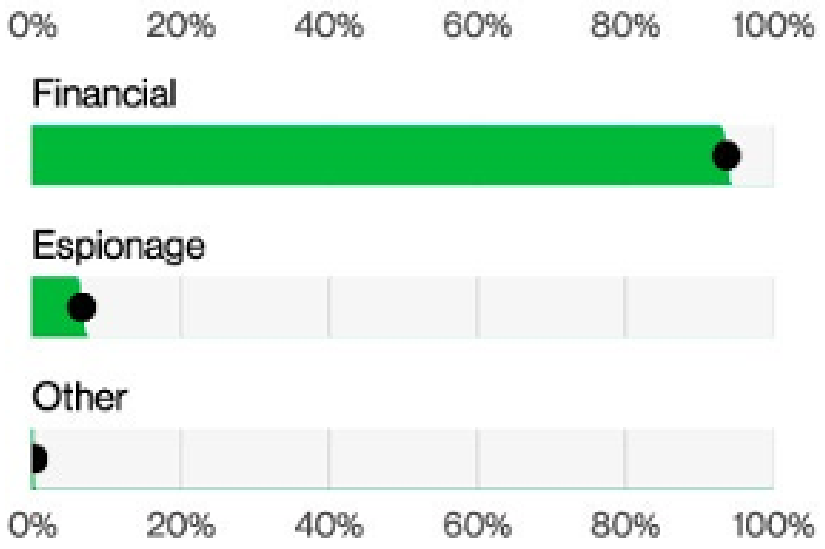


Figure 12. Threat actor motives in breaches (n=5,632)

When asked why he robbed banks, Sutton simply replied, "Because that's where the money is."
— William Sutton

https://www.verizon.com/business/resources/reports/dbir

State of Education Sector Threat Actors

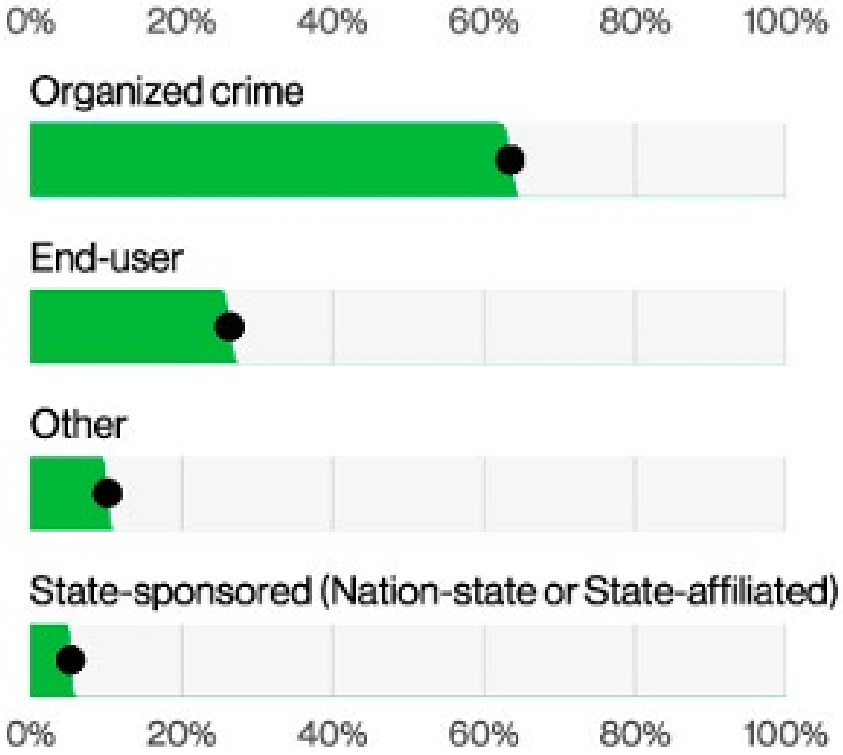
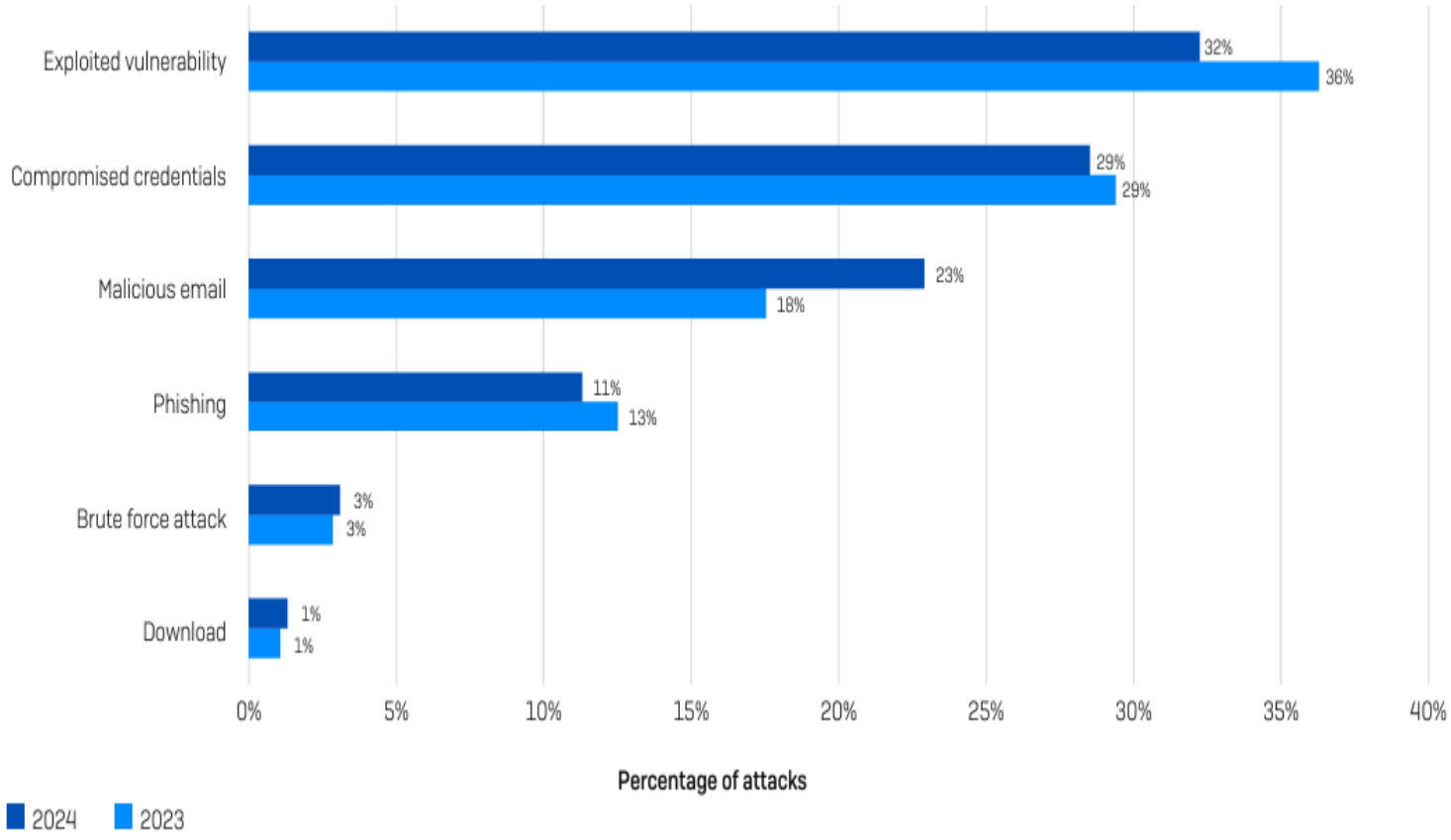


Figure 13. Threat actor varieties in breaches (n=7,921)



https://www.verizon.com/business/resources/reports/dbir

State of Education Sector

Pretexting, a form of social engineering.

"Pretexting is a form of social engineering attack in which a scammer creates a plausible scenario to bait victims into divulging sensitive information, making fraudulent payments, granting access to an account, and so on. Closely related to various types of phishing, pretexting scams are characterized by detailed situations (pretexts) and often involve impersonation as scammers work to build and manipulate victims' trust."

THINK CONARTIST! This is where your internal folks become unintentional insider threats.

https://www.zscaler.com/zpedia/what-is-pretexting

State of Education Sector

- **Roleplaying and impersonation:** Attackers may play a character such as a customer, service provider, colleague, or authority figure so the victim feels inclined to cooperate. This could include exploiting vulnerabilities in authentication processes or exploiting trusted relationships.
- **Research and reconnaissance:** Often using open, publicly available resources, attackers can gather information about a target's job and responsibilities, coworkers, personal details, and more.
- **Developing relationships:** As in any archetypal "long con," attackers can use manipulation techniques to establish credibility and trust with a target, possibly through phone calls, social media, or even face-to-face conversations.
- **Exploiting emotions:** Nothing creates urgency like uncertainty, doubt, and fear. Attackers may fabricate emergencies, one-time opportunities, and more to fool targets into taking hasty action and bypassing security measures.
- **Leveraging generative AI:** The youngest technique in this toolbox by centuries—maybe millennia—modern AI tools can help attackers rapidly create pretexts with strikingly human-like language and detail, even in languages in which they may not be proficient.

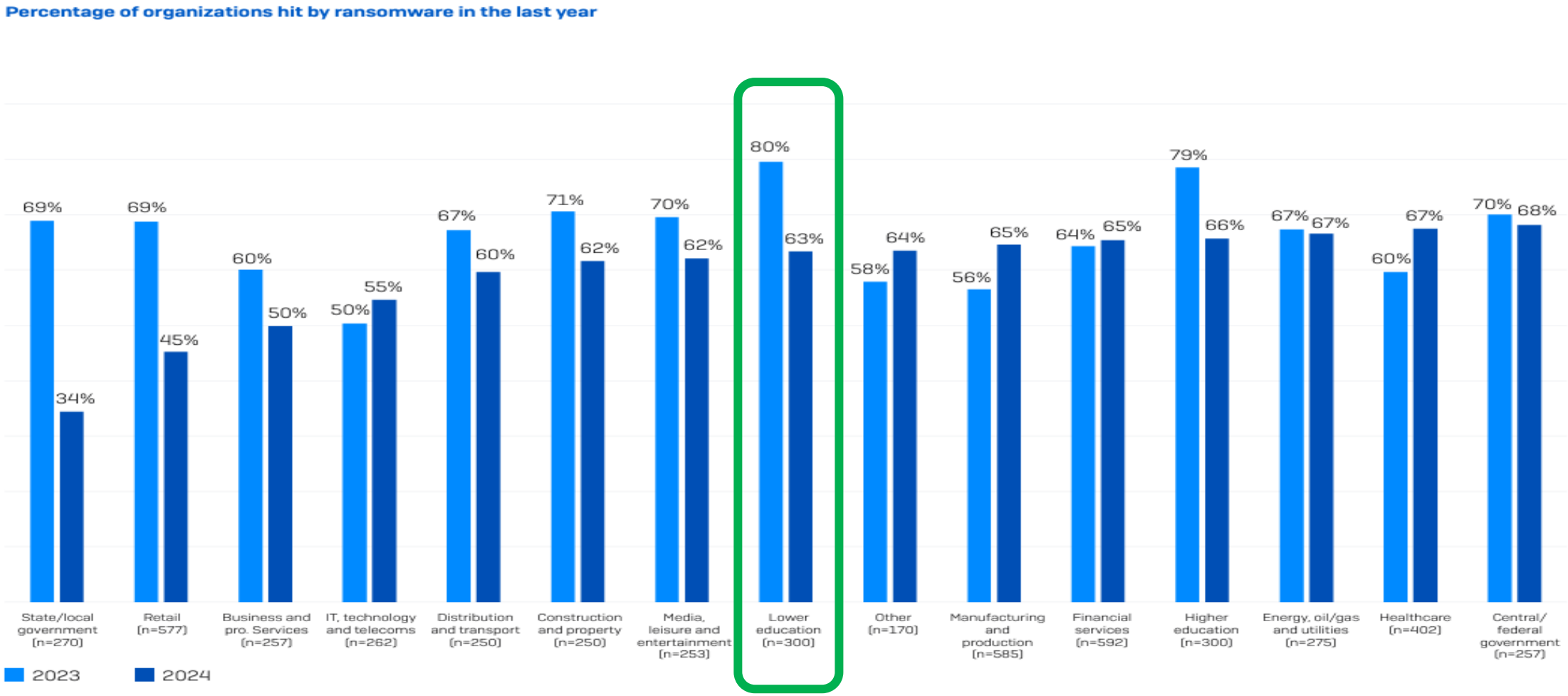
https://www.zscaler.com/zpedia/what-is-pretexting

State of Education Sector

- The education sector no longer reports the two highest rates of attack, coming in at 66% (*higher education*) and 63% (*lower education*) this year vs. 79% and 80% respectively last year

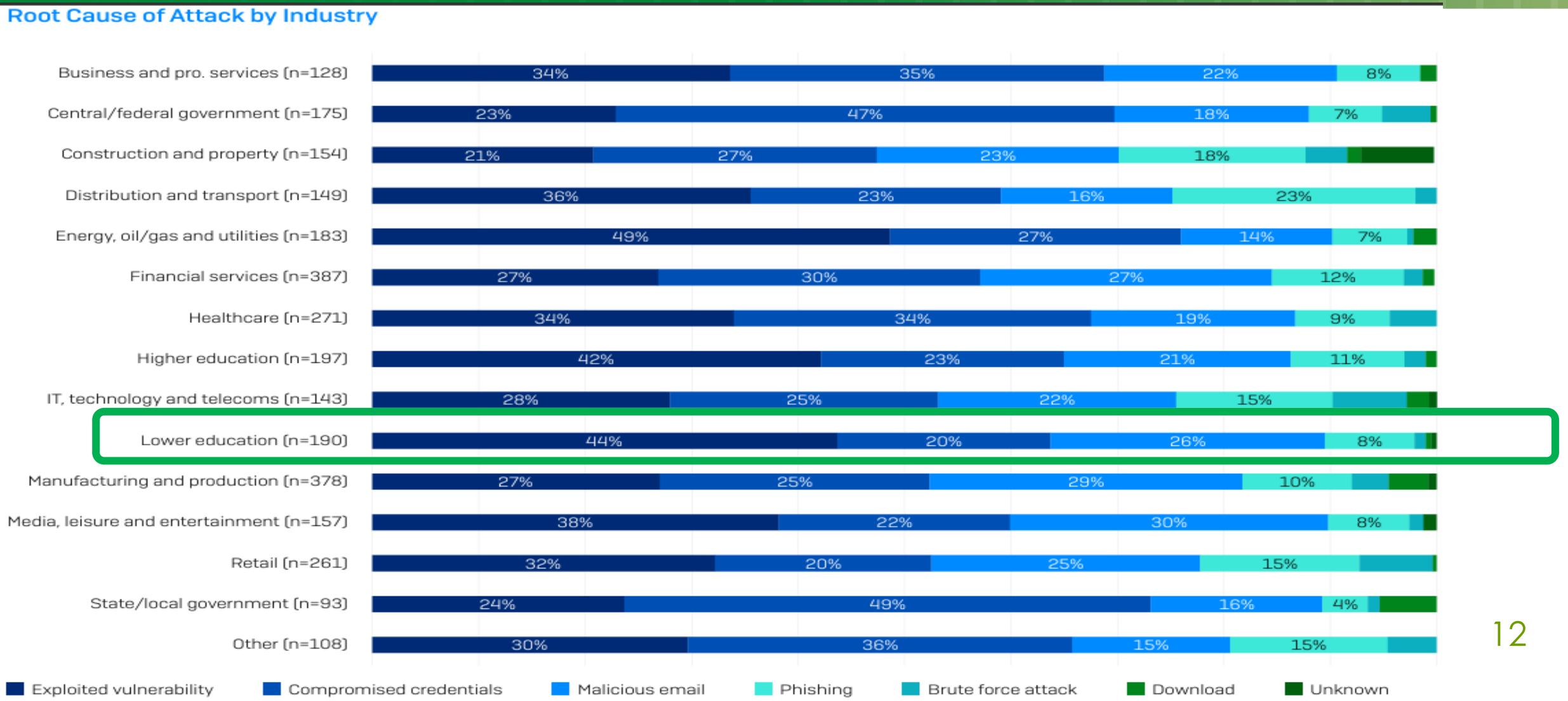
https://www.sophos.com/en-us/content/state-of-ransomware

State of Education Sector

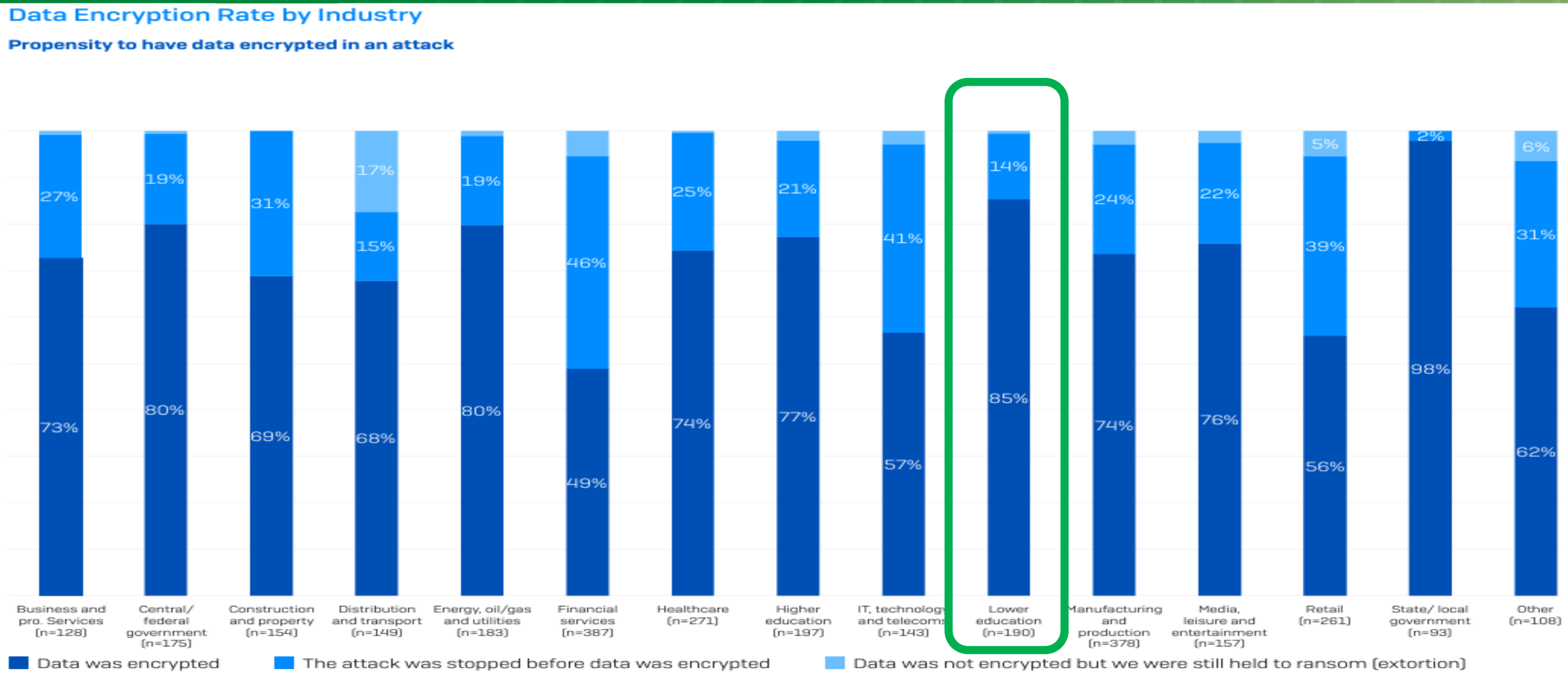


https://www.sophos.com/en-us/content/state-of-ransomware

State of Education Sector

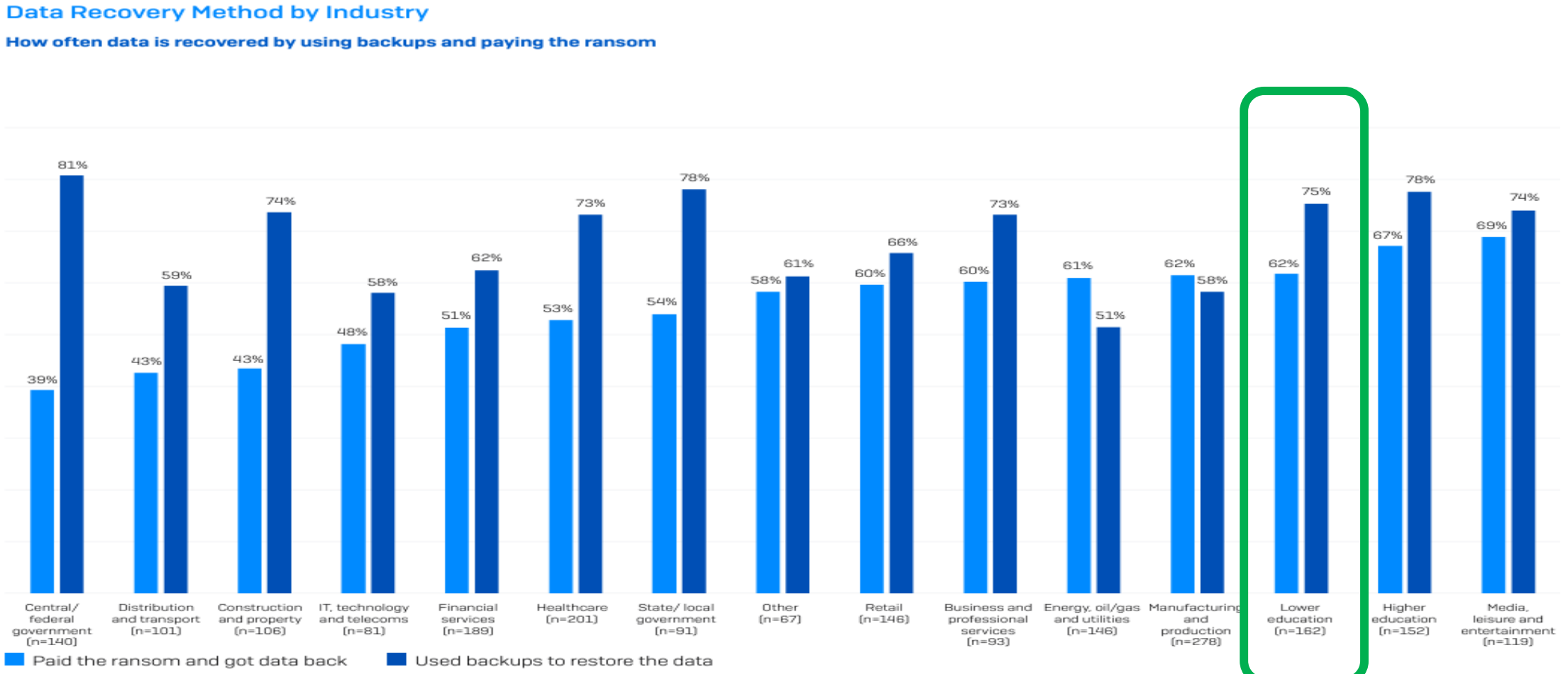


State of Education Sector



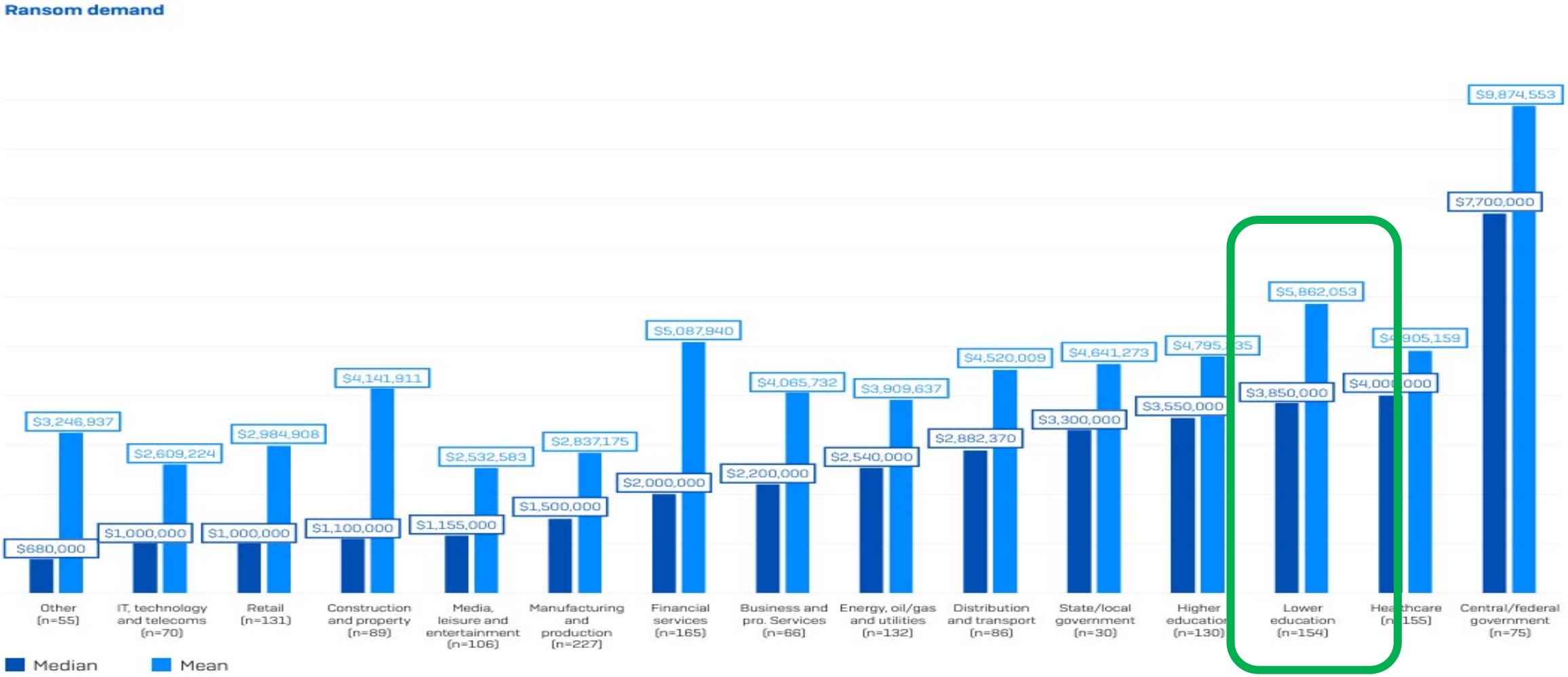
https://www.sophos.com/en-us/content/state-of-ransomware

State of Education Sector



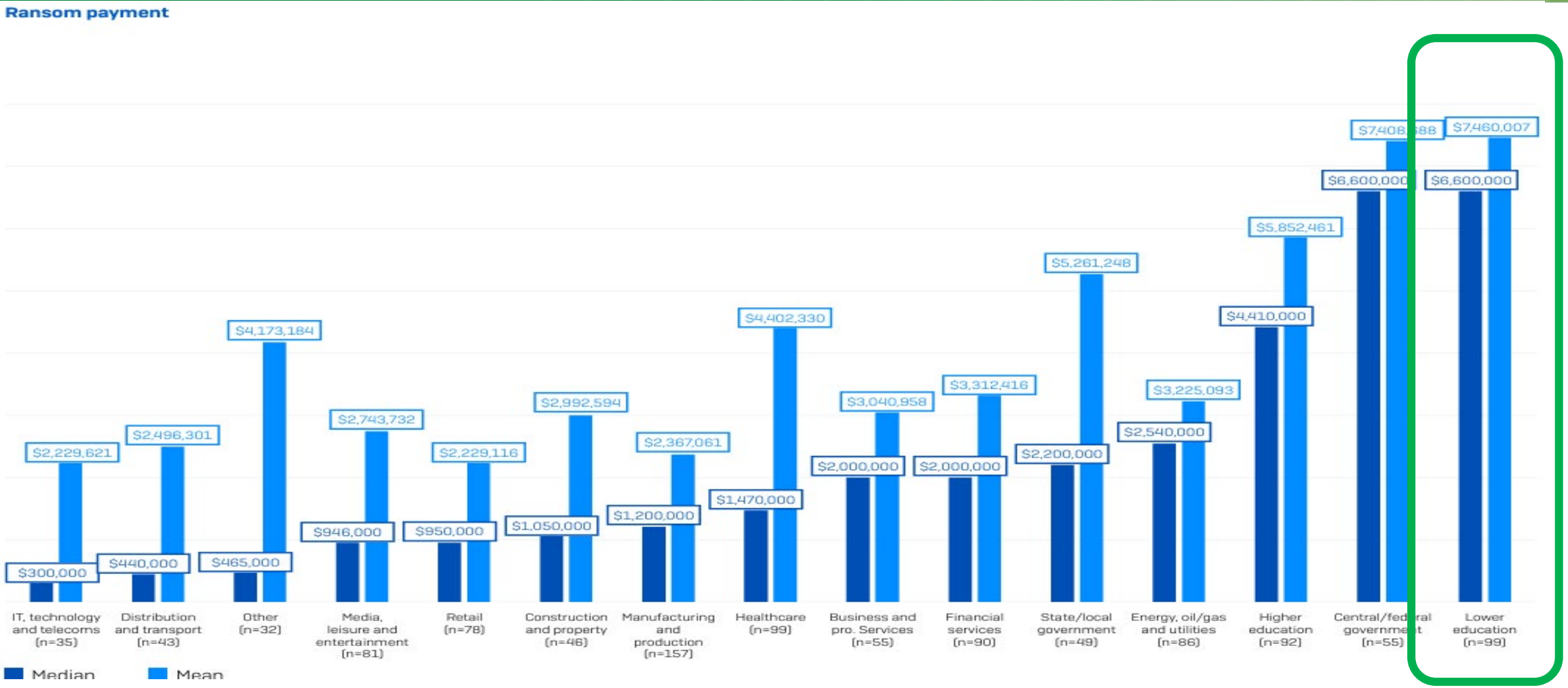
https://www.sophos.com/en-us/content/state-of-ransomware

State of Education Sector



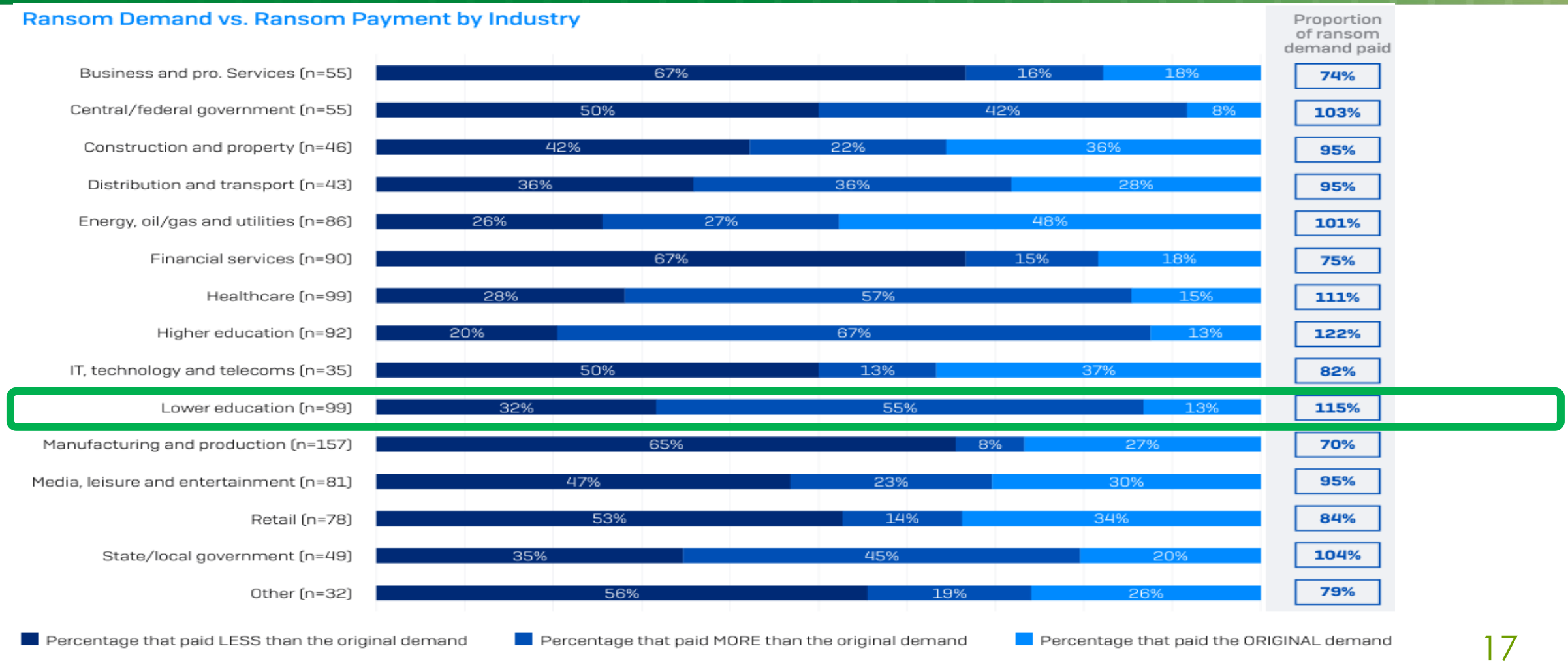
https://www.sophos.com/en-us/content/state-of-ransomware

State of Education Sector



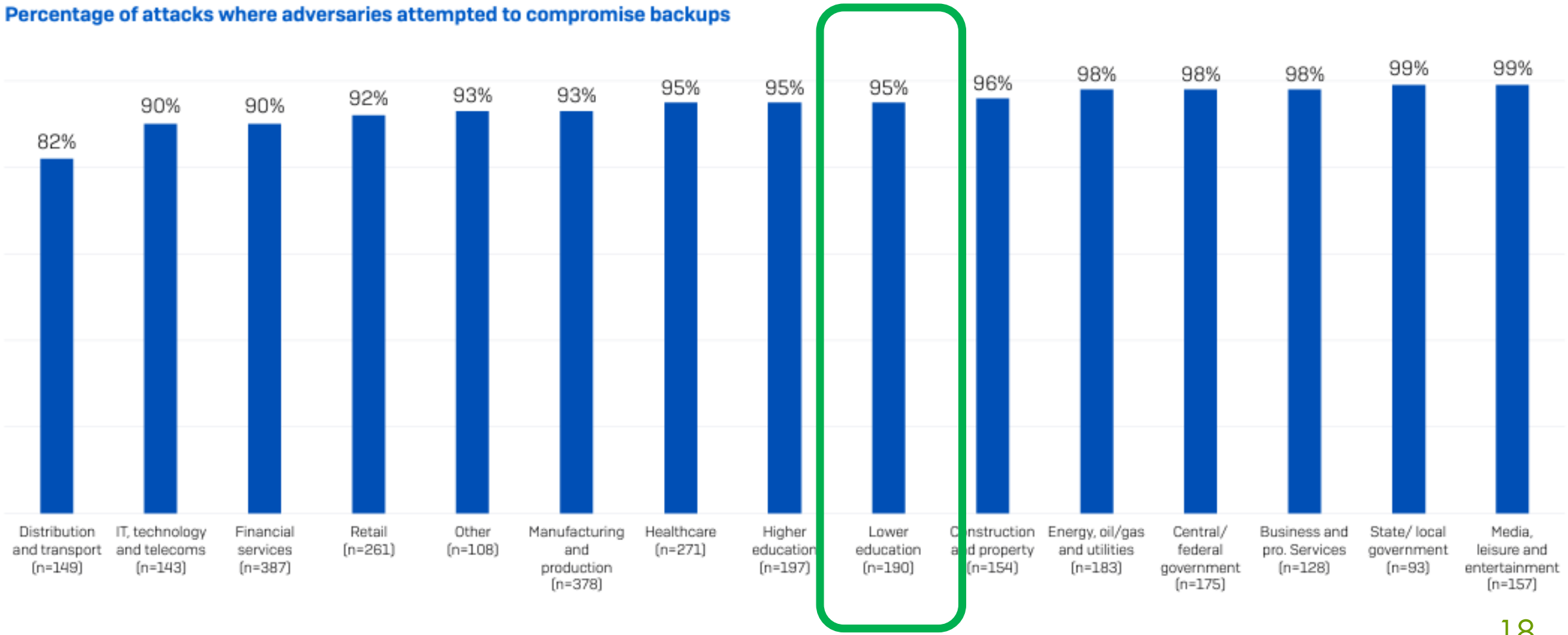
https://www.sophos.com/en-us/content/state-of-ransomware

State of Education Sector



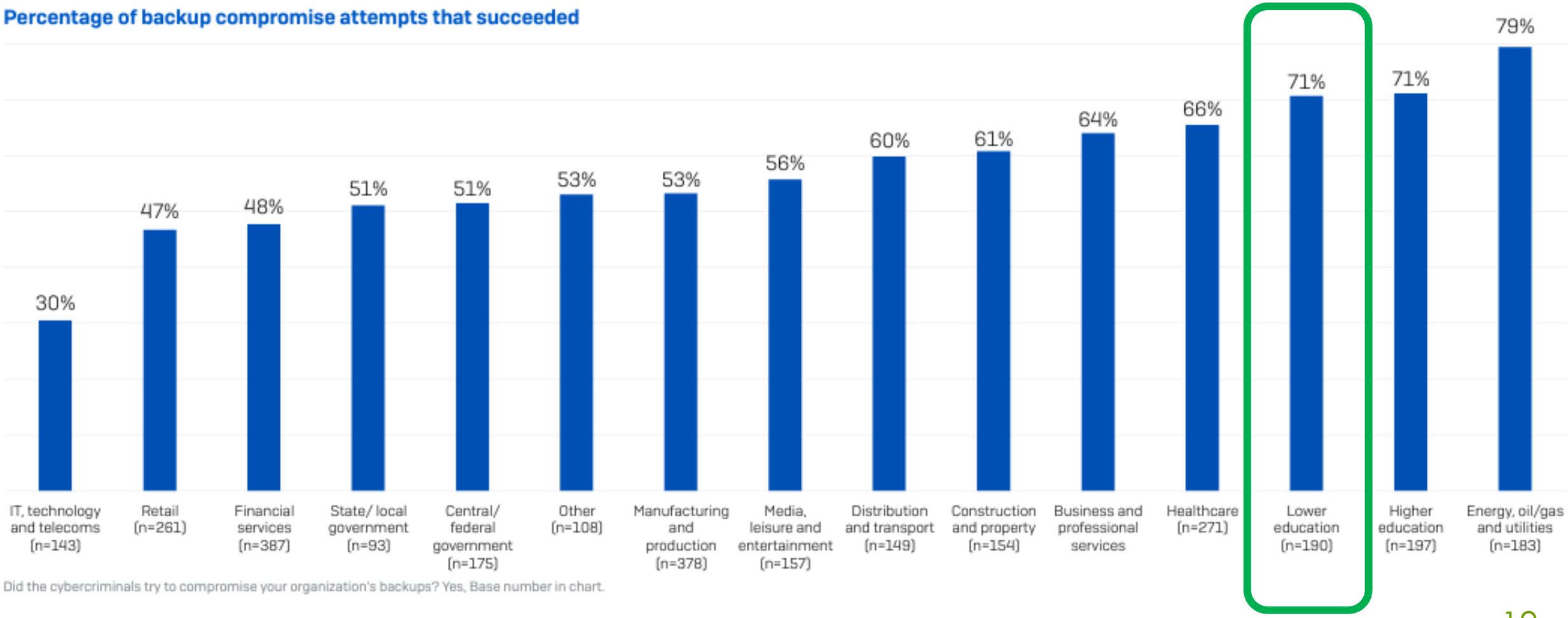
https://www.sophos.com/en-us/content/state-of-ransomware

State of Education Sector



https://www.sophos.com/en-us/content/state-of-ransomware

State of Education Sector



https://www.sophos.com/en-us/content/state-of-ransomware

Third Party Exploitation

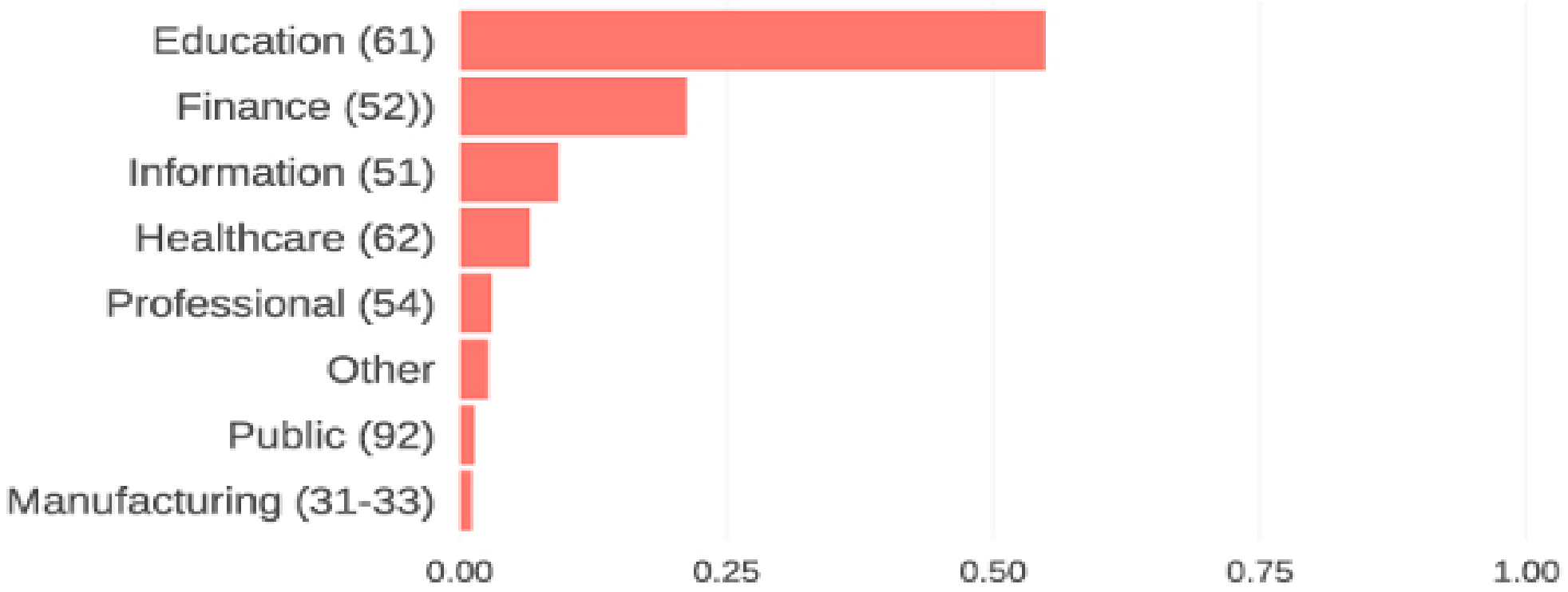


Figure 32. Top industries found in the MOVEit breach notification dataset (n=1,567)

https://www.verizon.com/business/resources/reports/dbir

Focus Areas

1. Multifactor authentication
    a. Phishing resistant authentication for privileged accounts.
2. Encryption for data at rest and in transit
3. Logging and analysis (OMB M-21-31 is a great reference if looking for a place to start!)

https://www.verizon.com/business/resources/reports/dbir

Helpful Federal Resources

- US Department of Education
  - https://studentprivacy.ed.gov/
  - https://rems.ed.gov
- FBI
  - Internet Crime Compliant Center (https://www.ic3.gov/default.aspx)
  - Local Field Offices (Establish a relationship sooner than later!) (https://www.fbi.gov/contact-us/field-offices)
  - Infragard (https://www.infragard.org/)
- Secret Service Field Offices (http://www.secretservice.gov/field_offices.shtml)
  - Electronic Crimes Task Forces (ECTFs) (United States Secret Service)
  - https://www.secretservice.gov/sites/default/files/reports/2020-12/Preparing%20for%20a%20Cyber%20Incident%20-%20An%20Introductory%20Guide%20v%201.1.pdf

Helpful Federal Resources

- DOJ Best Practices for Victim Response and Reporting of Cyber Incidents
  - https://www.justice.gov/sites/default/files/opa/speeches/attachments/2015/04/29/criminal_division_guidance_on_best_practices_for_victim_response_and_reporting_cyber_incidents.pdf
- NSA's Top Ten Cybersecurity Mitigation Strategies
  - csi-nsas-top10-cybersecurity-mitigation-strategies.pdf
- United States General Services Administration FedRAMP Program
  - https://www.fedramp.gov/training/
- Not Federal ☺ StateRAMP
  - https://stateramp.org/faqs/

Helpful Federal Resources

Cyber Infrastructure and Security Agency

- Request information about the service(s) you are interested in by emailing ncats_info@hq.dhs.gov.
- All services are available at no cost to federal agencies, state and local governments, critical infrastructure, and private organizations generally.

Cyber Hygiene: Vulnerability Scanning helps secure your internet-facing systems from weak configuration and known vulnerabilities, and encourages the adoption of modern security best practices. DHS performs regular network and vulnerability scans and delivers a weekly report for your action. Once initiated, this service is mostly automated and requires little direct interaction. After we receive the required paperwork for Cyber Hygiene, our scans will start within 72 hours and you'll begin receiving reports within two weeks.

Cyber Hygiene Services | CISA

A **CISA Reviewed industry resources:**

Free Cybersecurity Services and Tools | CISA

Overview

- Brief overview of the Idaho State Department of Education and Boise School District (ID)
  - Idaho State Board of Education and State Department of Education
  - Districts and Schools
    - Idaho – 181 Districts and Charter Schools, 935 Schools
    - Boise – 51 Schools
  - Enrollments – Idaho - ~313,000, Boise - ~23,000
  - Staff Size – Boise ~4,500
  - Idaho Code 33-133, Idaho Student Data Security Model Policy

Cybersecurity in Idaho

- 2017 Governor's Cybersecurity Task Force
  - Creation of the First Director of Information Security
  - Computing and cybersecurity facilities at INL
- 2022 Governor's Cybersecurity Task Force
  - Schools Included
  - Cyber Response and Defense Fund
- Cyberdome
- Challenges
  - Structure, Territory, Importance, Role

Training and Support

- LEAs are responsible for providing training to staff and students.
- No state funding specific for cybersecurity to LEAs.
- The Idaho Education Technology Association (IETA) provides training and has a task force (PTAC).
- Training varies based on roles.
- Training examples:
  - Phishing, URL Checking, Understanding Domains, MFA,

Preparation and Prevention

- Incident response plan, tabletop exercises, monitoring software, staff and student training.
- LEAs work together directly and through the IETA for training and support (PTAC).
- Nampa School District (ID) Breach
- Education Opportunity Resource Committee (EORC) Support

Collaboration

- EORC and IETA
- Collaborative Training
- Support from PTAC
- SEA IETA Membership
- SEA Legislative Support

Best Practices and Lessons Learned

- Staff and Student Training
- Multifactor Authentication (MFA)
- Focus on Cybersecurity
- Collaboration
- Dedicated Support

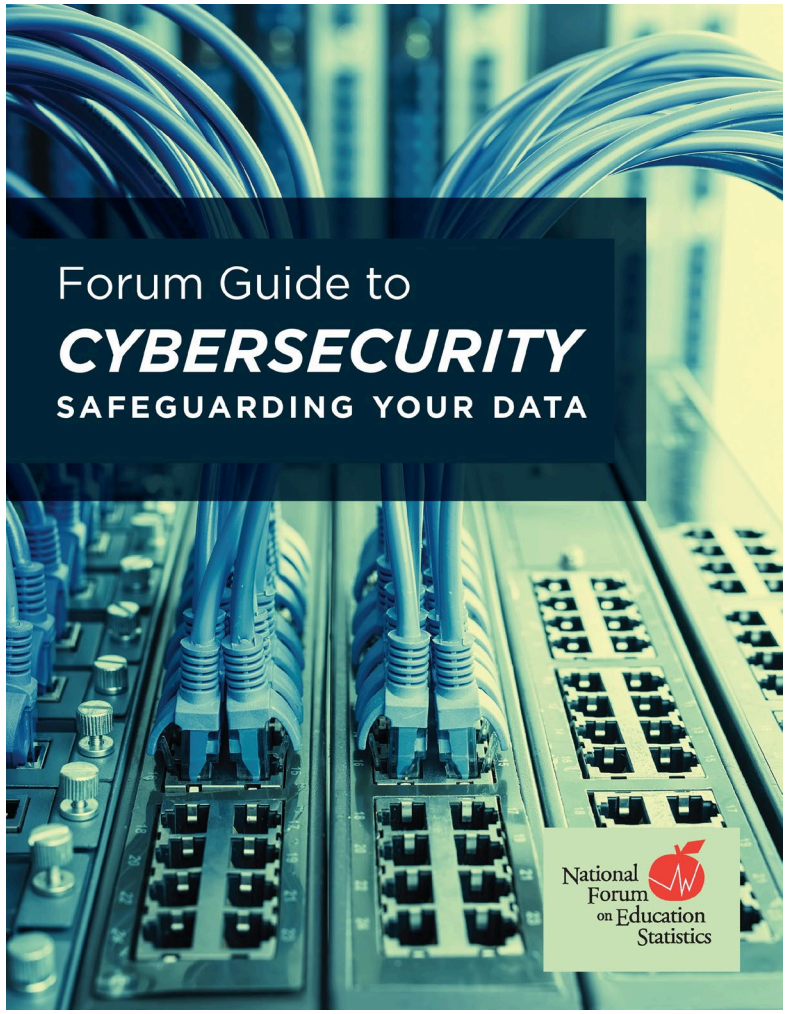
Conclusion

- Use your Resources
  - Forum Guides
  - PTAC
  - Vendor Support
  - Universal Service Administrative Company (USAC) E-Rate Program
- Collaboration
  - SEA and LEAs

Forum Guide to Cybersecurity: Safeguarding Your Data

Purpose

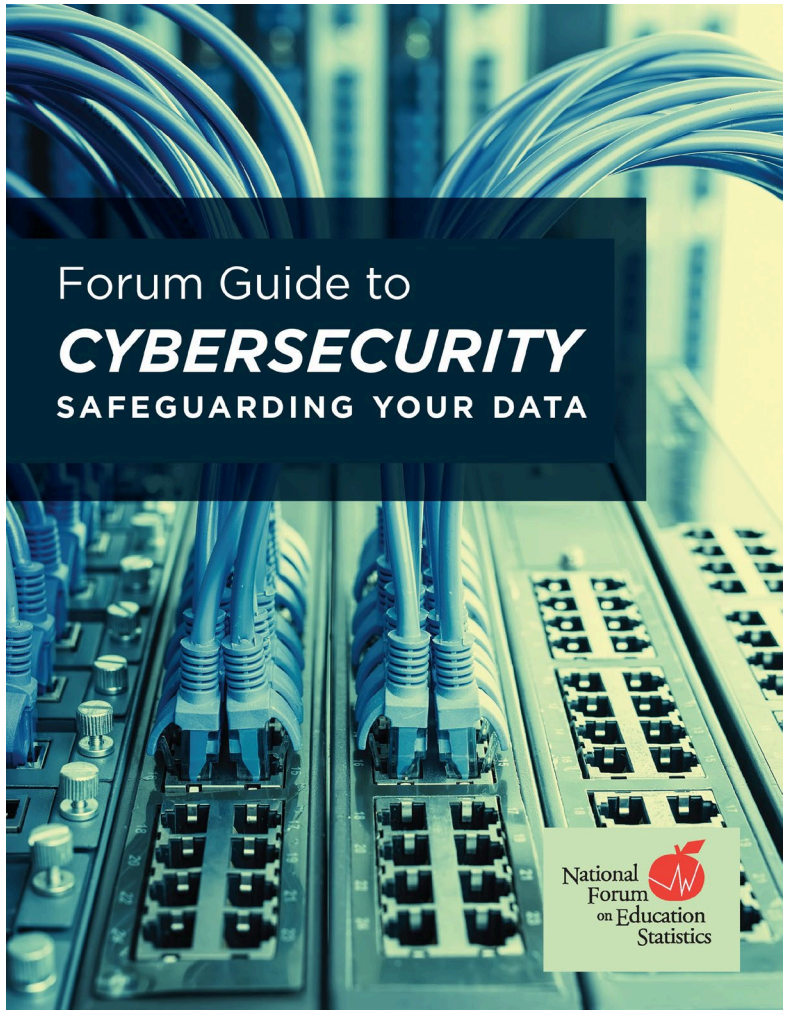
- Help education agencies prepare for, mitigate, and recover from a cybersecurity incident.
- Provide recommendations to help protect agency systems and data before, during, and after a cybersecurity incident.



Forum Guide to Cybersecurity Contents

Chapters

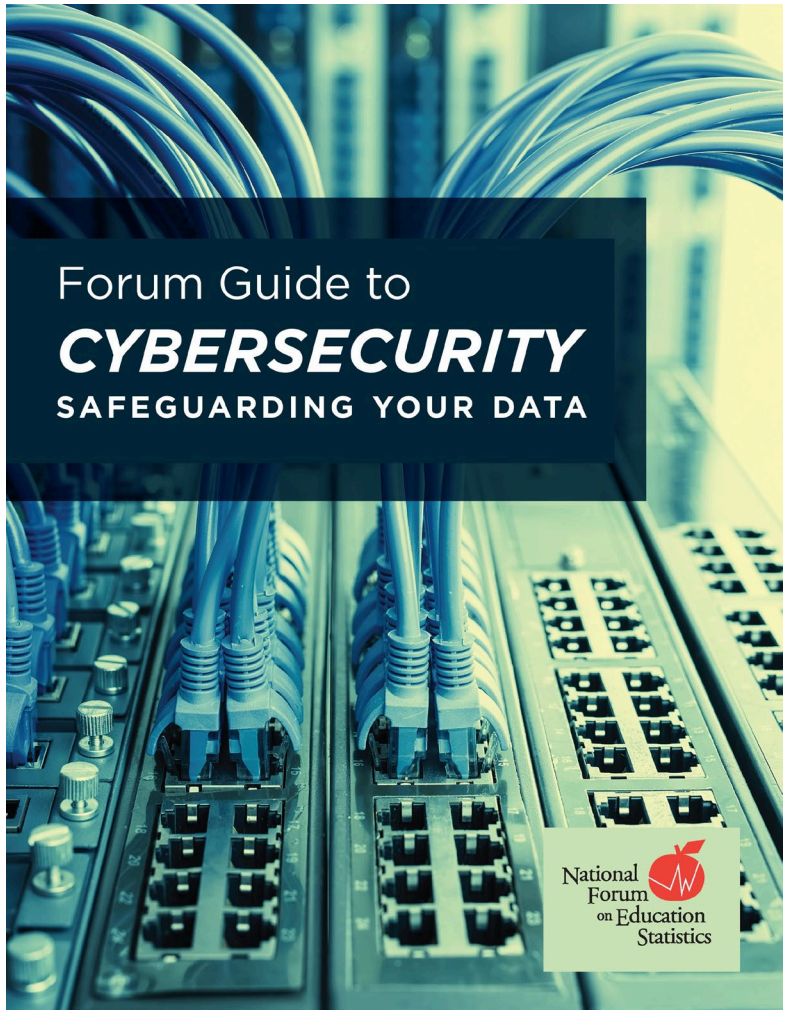
1. Cybersecurity in SEAs and LEAs
2. Before an Incident—Planning and Prevention
3. During an Incident—Mitigation
4. After an Incident—Recovery and Restoration
5. Case Studies from States and Districts



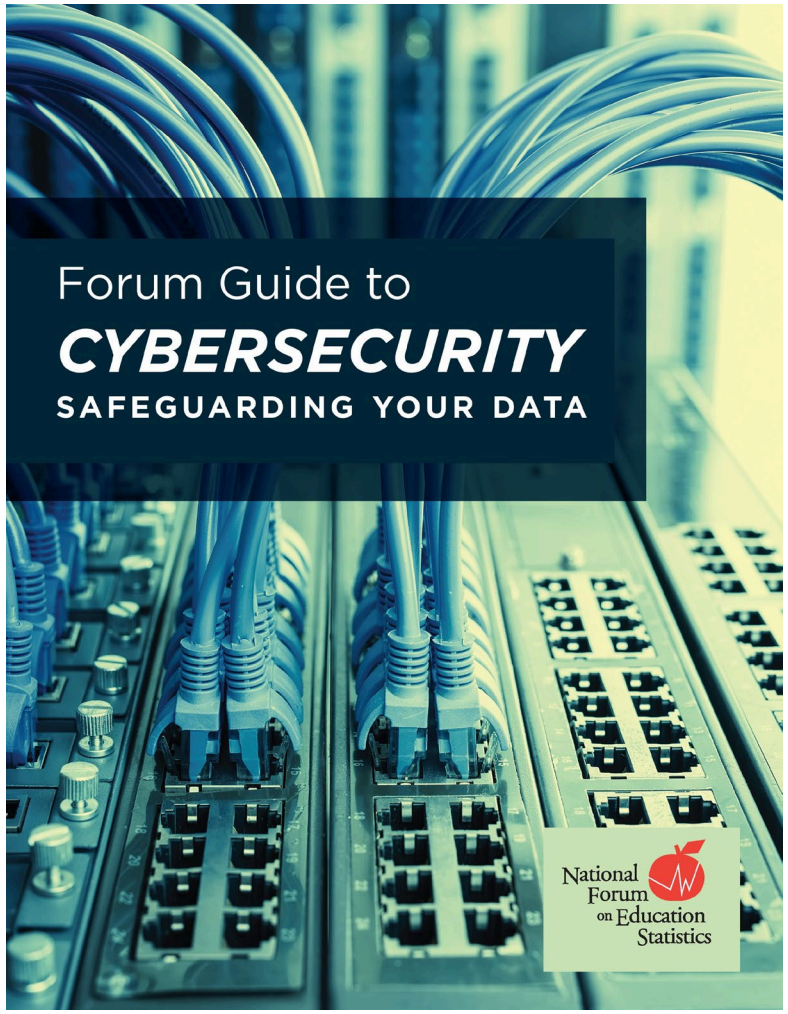
Forum Guide to Cybersecurity Case Studies

Case Studies from SEAs and LEAs:

- Developing a Data Breach Response Protocol
- Implementing a Cybersecurity Program
- Responding to a SQL Injection Attack
- Responding to a Vendor Data Breach
- Recovering from a Ransomware Attack



Questions?

Forum Guide to Cybersecurity: Safeguarding Your Data
https://nces.ed.gov/forum/pub_2020137.asp

The information and opinions published are those of the Forum and do not necessarily represent the policy or views of the National Center for Education Statistics, the Institute of Education Sciences, or the U.S. Department of Education.