Cybersecurity Landscape in 2023

NESGFOA

2023 Fall Conference

September 11, 2023

BAKER
NEWMAN
NOYES

NEW ENGLAND STATES
GOVERNMENT FINANCE OFFICERS ASSOCIATION

Thank you for hosting today!

Here with you today

BAKER NEWMAN NOYES

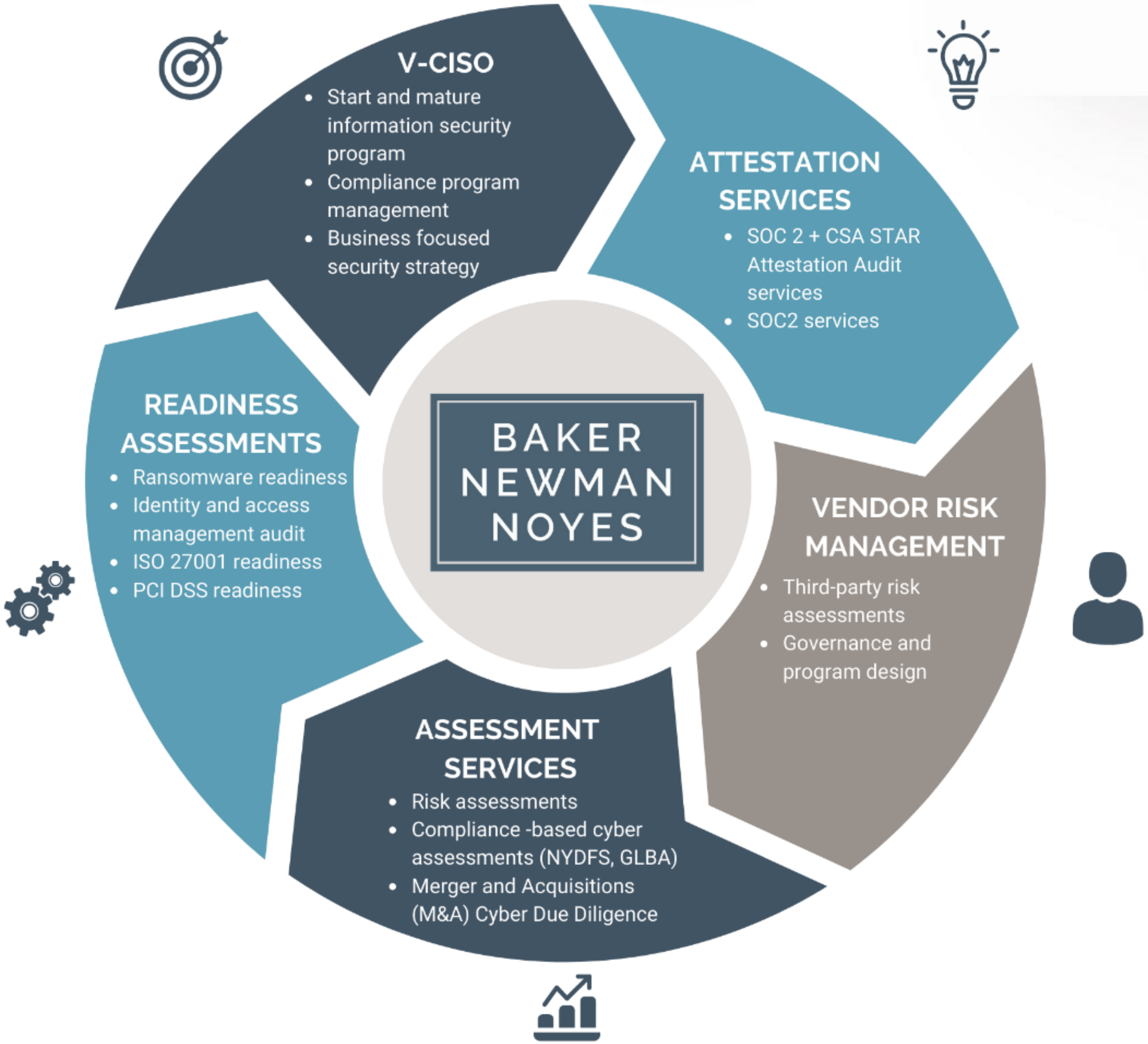
Pawel Wilczynski specializes in cyber security, risk, and IT systems assurance services. Clients turn to Pawel for help conducting cyber assessments, readiness assessments for major frameworks, standards and regulations and all things cyber. He works with a variety of clients, with a particular focus on financial and insurance institutions and the technology industry.

Pawel Wilczynski

Manager

pwilczynski@bnncpa.com

BAKER NEWMAN NOYES



V-CISO

- Start and mature information security program
- Compliance program management
- Business focused security strategy

ATTESTATION SERVICES

- SOC 2 + CSA STAR Attestation Audit services
- SOC2 services

VENDOR RISK MANAGEMENT

- Third-party risk assessments
- Governance and program design

ASSESSMENT SERVICES

- Risk assessments
- Compliance -based cyber assessments (NYDFS, GLBA)
- Merger and Acquisitions (M&A) Cyber Due Diligence

READINESS ASSESSMENTS

- Ransomware readiness
- Identity and access management audit
- ISO 27001 readiness
- PCI DSS readiness

BAKER NEWMAN NOYES

What you will hear today

- Cybersecurity landscape:
  - - Verizon DBIR highlights
  - - Current events
- How to protect your organization
- Q&A and closing

Key takeaways from the 2023 Verizon DBIR report

Key takeaways from the 2023 Verizon DBIR report

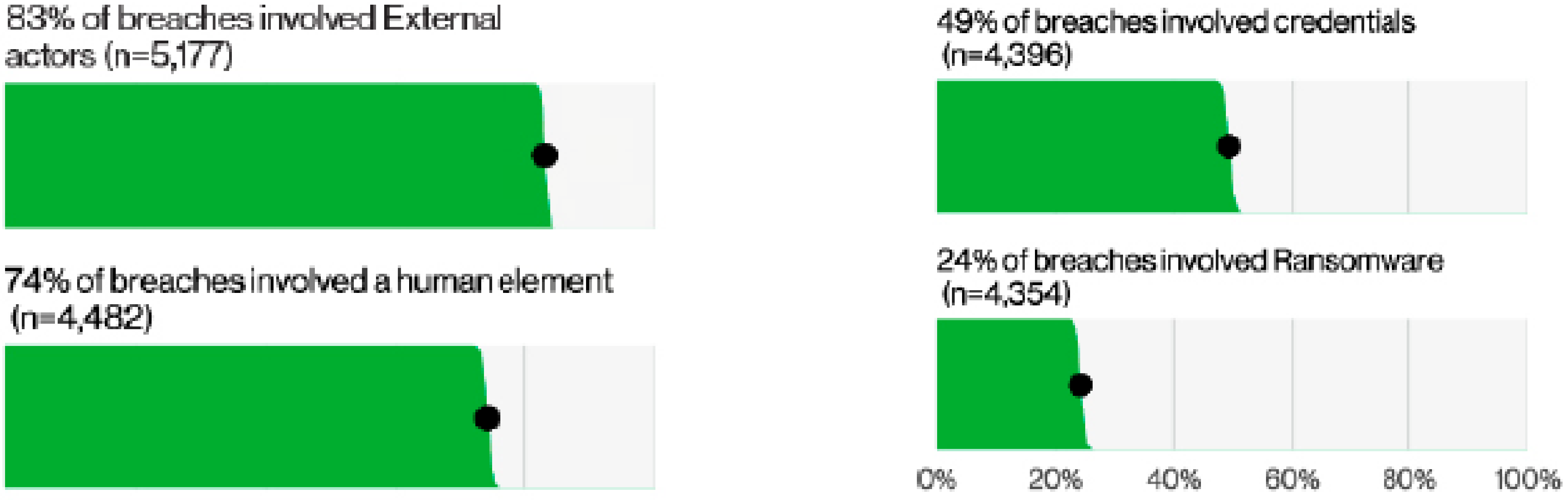
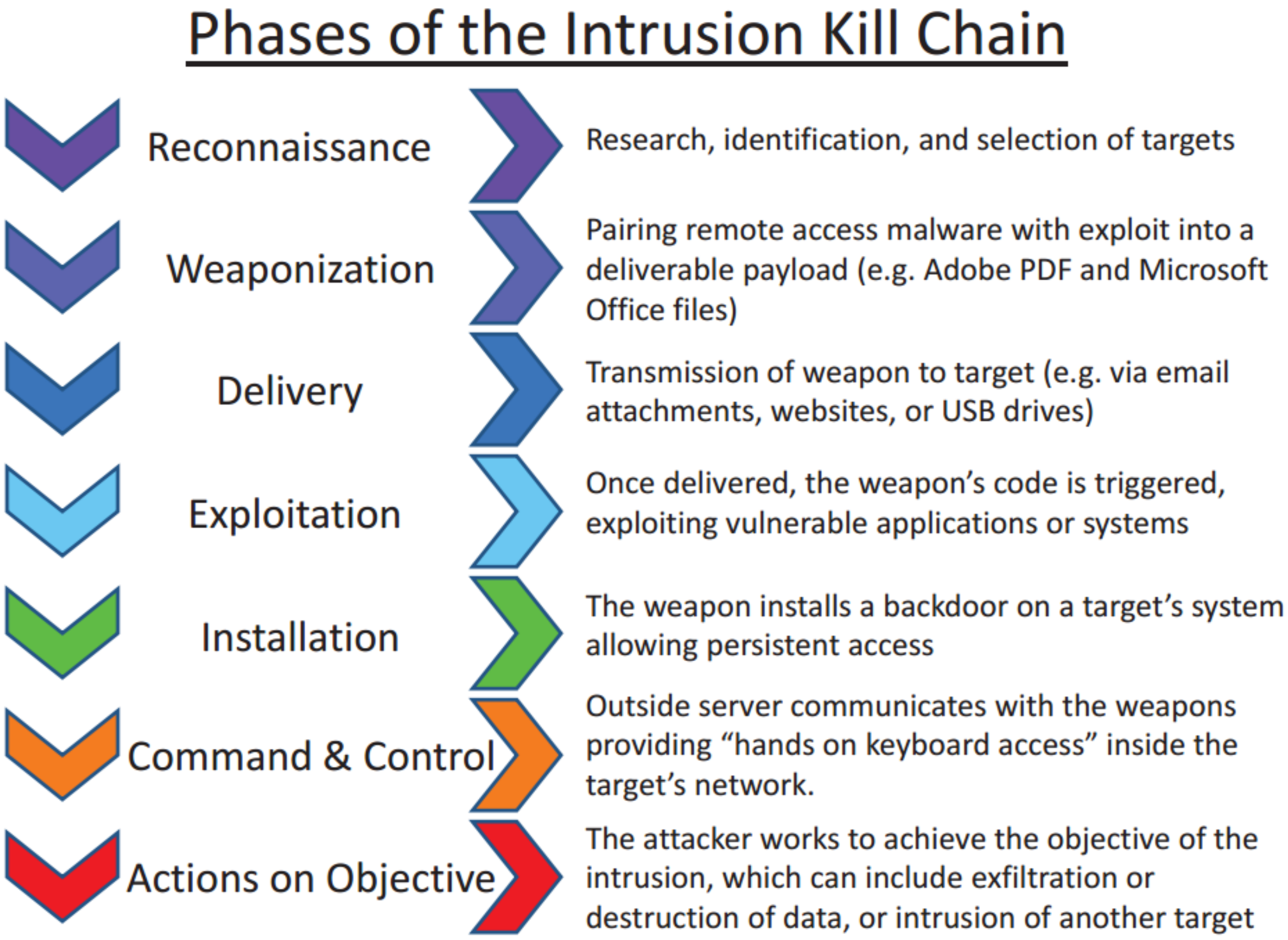


Figure 6. Select key enumerations

Key takeaways from the 2023 Verizon DBIR report

- Threat actors’ dwell time may not actually be improving – average has hovered around 85 to 100 days
- Disclosure or ransom demand happens at the last stage. Victims are reacting too late.



Phases of the Intrusion Kill Chain

Reconnaissance	Research, identification, and selection of targets
Weaponization	Pairing remote access malware with exploit into a deliverable payload (e.g. Adobe PDF and Microsoft Office files)
Delivery	Transmission of weapon to target (e.g. via email attachments, websites, or USB drives)
Exploitation	Once delivered, the weapon’s code is triggered, exploiting vulnerable applications or systems
Installation	The weapon installs a backdoor on a target’s system allowing persistent access
Command & Control	Outside server communicates with the weapons providing “hands on keyboard access” inside the target’s network.
Actions on Objective	The attacker works to achieve the objective of the intrusion, which can include exfiltration or destruction of data, or intrusion of another target

Key takeaways from the 2023 Verizon DBIR report

- System intrusion is still effective, penetration testing is still needed

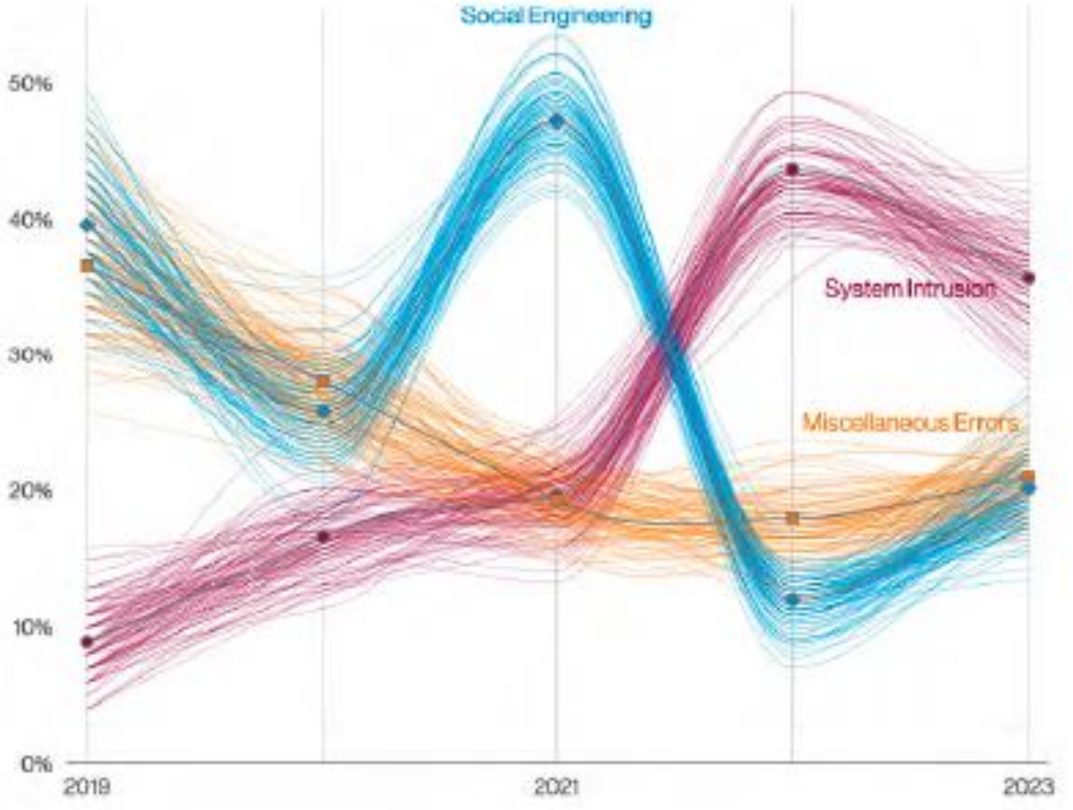


Figure 52. Patterns in Education breaches

Key takeaways from the 2023 Verizon DBIR report

- Ransomware and data theft are (still) on the rise

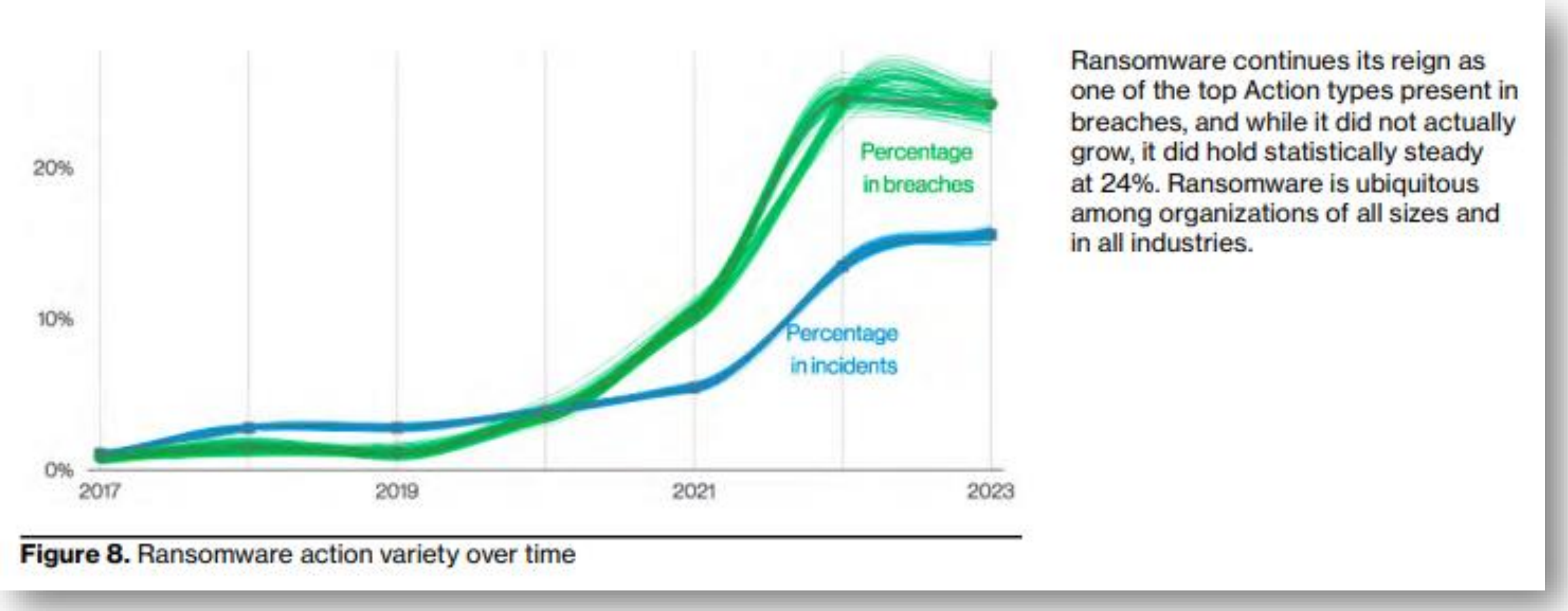


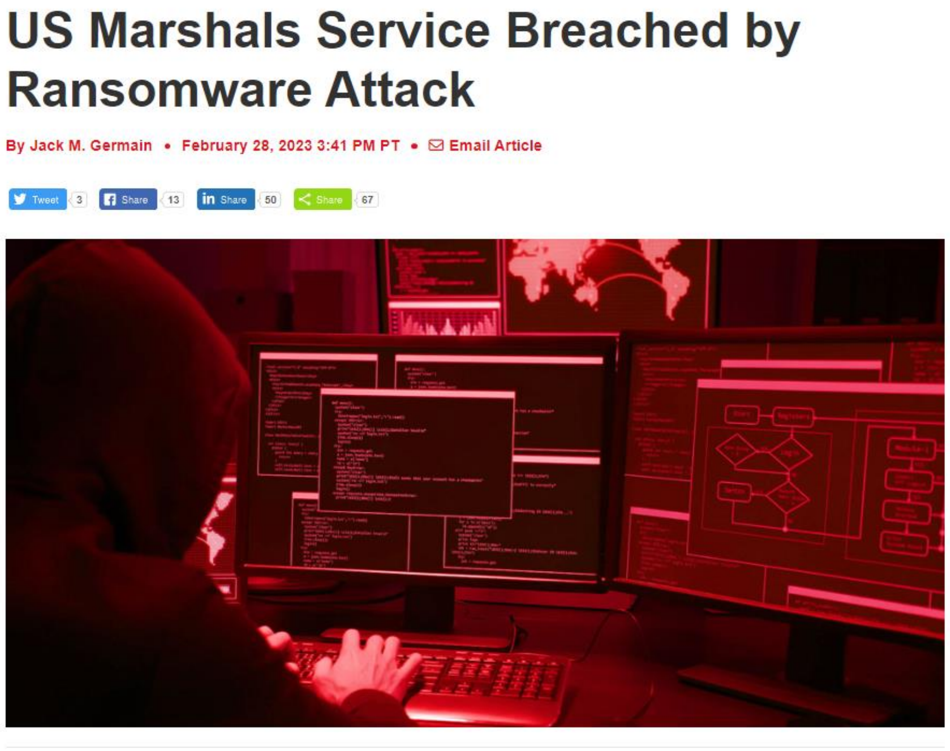
Figure 8. Ransomware action variety over time

Ransomware continues its reign as one of the top Action types present in breaches, and while it did not actually grow, it did hold statistically steady at 24%. Ransomware is ubiquitous among organizations of all sizes and in all industries.

BAKER
NEWMAN
NOYES

Current events

Current events

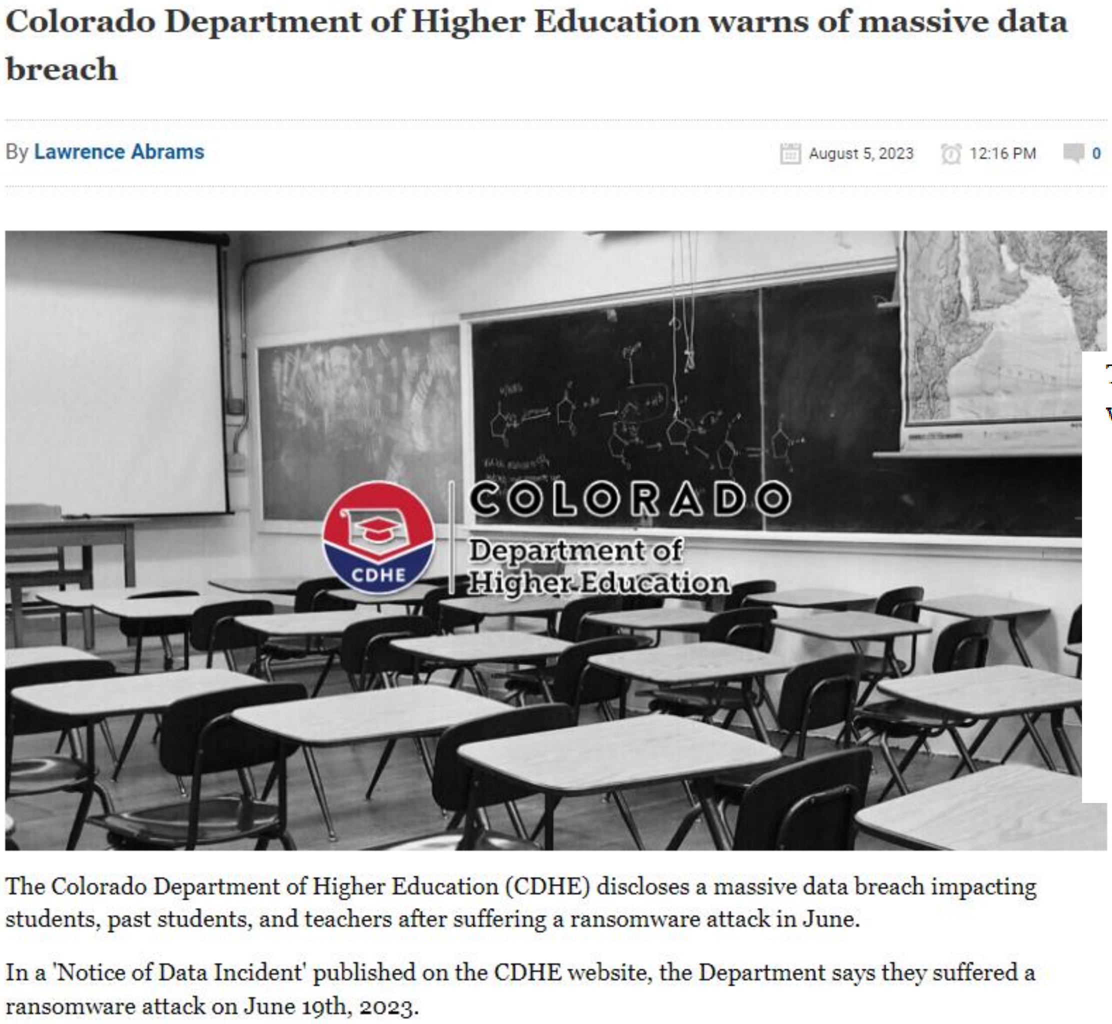


US Marshals Service Breached by Ransomware Attack

By Jack M. Germain • February 28, 2023 3:41 PM PT • Email Article

- Major breach of its computer network on February 17 that included a ransomware component
- Affected records include targets of ongoing investigations, employee personal data, and internal processes
- Data can compromise ongoing investigations and endanger the lives of law enforcement officers

Current events

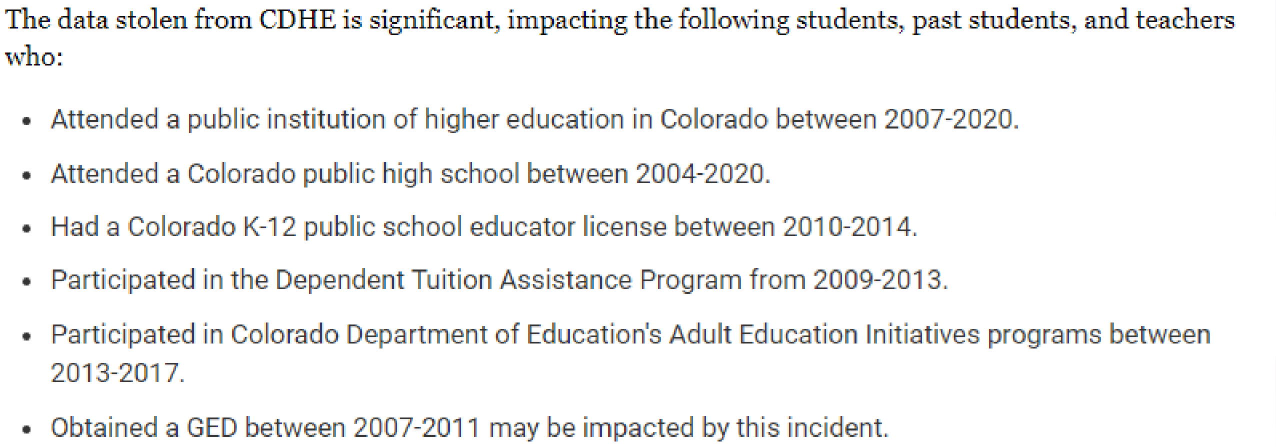


Colorado Department of Higher Education warns of massive data breach

By Lawrence Abrams August 5, 2023 12:16 PM 0

The Colorado Department of Higher Education (CDHE) discloses a massive data breach impacting students, past students, and teachers after suffering a ransomware attack in June.

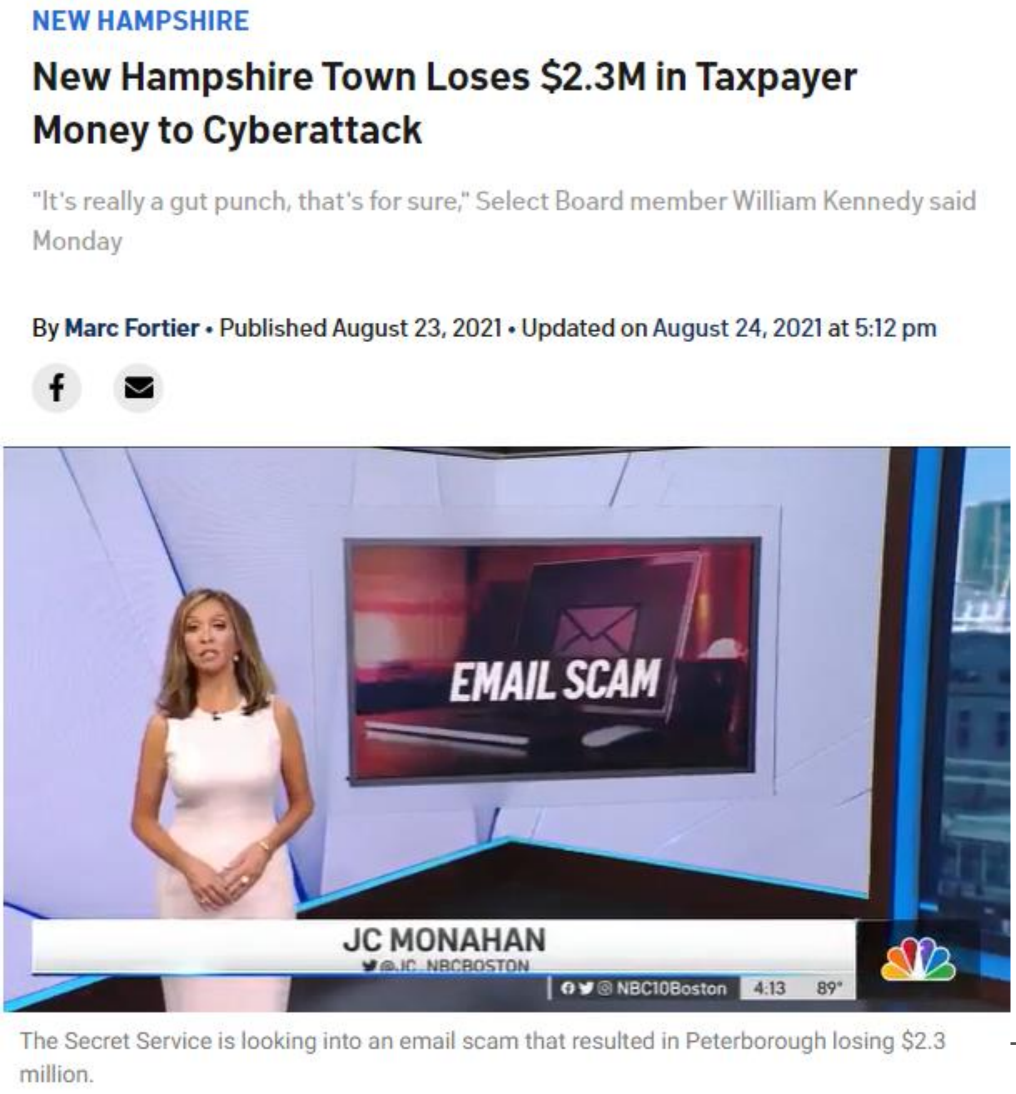
In a 'Notice of Data Incident' published on the CDHE website, the Department says they suffered a ransomware attack on June 19th, 2023.



The data stolen from CDHE is significant, impacting the following students, past students, and teachers who:

- Attended a public institution of higher education in Colorado between 2007-2020.
- Attended a Colorado public high school between 2004-2020.
- Had a Colorado K-12 public school educator license between 2010-2014.
- Participated in the Dependent Tuition Assistance Program from 2009-2013.
- Participated in Colorado Department of Education's Adult Education Initiatives programs between 2013-2017.
- Obtained a GED between 2007-2011 may be impacted by this incident.

Current events



NEW HAMPSHIRE

New Hampshire Town Loses $2.3M in Taxpayer Money to Cyberattack

"It's really a gut punch, that's for sure," Select Board member William Kennedy said Monday

By Marc Fortier • Published August 23, 2021 • Updated on August 24, 2021 at 5:12 pm

The Secret Service is looking into an email scam that resulted in Peterborough losing $2.3 million.

- The attackers used social engineering to trick town officials
- Attackers posed as school district personnel to steal $1.2M
- Attackers also posed as a contractor working on the Main street bridge project to steal $1.1M

Current events: Morgan Stanley

- Morgan Stanley hired a storage company to dispose of electronic waste
- Storage company did not wipe the drives and resold 4,900 devices with customer data on them
- Morgan Stanley fined $35 million for failing to protect customer data

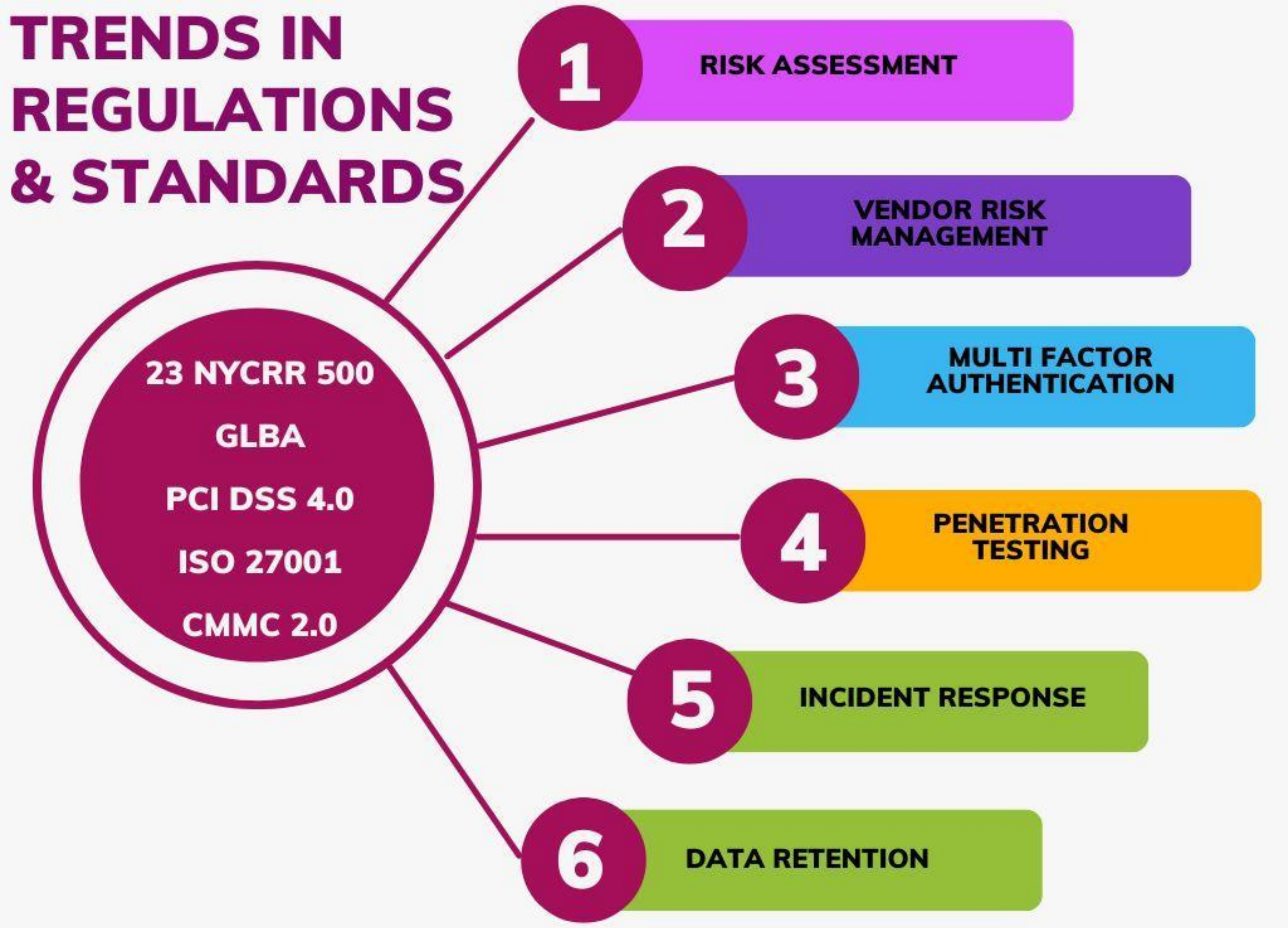
Morgan Stanley

Ransomware - Should you budget for it?

BAKER NEWMAN NOYES

Yes, but it’s not that simple!

1. Assume you’ll be hacked
2. Backup and test your backups
3. Make a decision if your company is going to pay or not
4. Incident Response is key
5. Prepare your defenses



TRENDS IN REGULATIONS & STANDARDS

23 NYCRR 500

GLBA

PCI DSS 4.0

ISO 27001

CMMC 2.0

1. RISK ASSESSMENT
2. VENDOR RISK MANAGEMENT
3. MULTI FACTOR AUTHENTICATION
4. PENETRATION TESTING
5. INCIDENT RESPONSE
6. DATA RETENTION

BAKER
NEWMAN
NOYES

How to protect your organization

How to protect your organization

- Use multi-factor authentication when available
- Utilize strong passwords (length over complexity)
- A password manager is your friend

How to protect your organization

- Update your software timely
- Backup and test your data
- Do not click on anything in an unsolicited email, text or instant message

How to protect your organization

- Have a tested incident response plan

- Stay ahead of compliance requirements

- Have prepared notifications to governing bodies in case of a breach

How to protect your business

- Stay up-to-date on common vulnerabilities affecting your vendors (and you) : Log4J
- Have a verified contact person at the vendor company you can call/email/slack any time
- Periodically assess vendors and related risks …

Conclusion

BAKER NEWMAN NOYES

- Ransomware is not slowing down
- Cyber insurance companies are more cautious than in prior years
- Choose your coverage carefully … and make sure cyber attacks are covered
- Third-party risk management is more important than ever
- Security hygiene sets solid foundations for safe business

Conclusion (continued)

- Solid asset inventory, especially internet facing – can’t protect what you don’t know exists
- User education is the key to success – be creative
- Penetration testing, vulnerability and risk assessments provide good feedback
- Consider seeking independent audits / attestations / certifications

Questions?

BAKER
NEWMAN
NOYES

Disclaimer of Liability: This publication is intended to provide general information to our clients and friends. It does not constitute accounting, tax, investment, or legal advice; nor is it intended to convey a thorough treatment of the subject matter.

Contact Us

Pawel Wilczynski

Manager, Information Systems & Risk Assurance Practice

pwilczynski@bnncpa.com

BAKER NEWMAN NOYES

bnncpa.com

PORTLAND
BOSTON | WOBURN
MANCHESTER | PORTSMOUTH

BAKER
NEWMAN
NOYES

Thank you!

THE NEW ENGLAND STATES
GOVERNMENT FINANCE OFFICERS ASSOCIATION
NESGFOA