Cybersecurity Landscape in 2023

Maine Bankers Association

2023 Bank Expo

April 26, 2023

BAKER NEWMAN NOYES

BAKER NEWMAN NOYES

MAINE BANKERS Association

Thank you for hosting today!

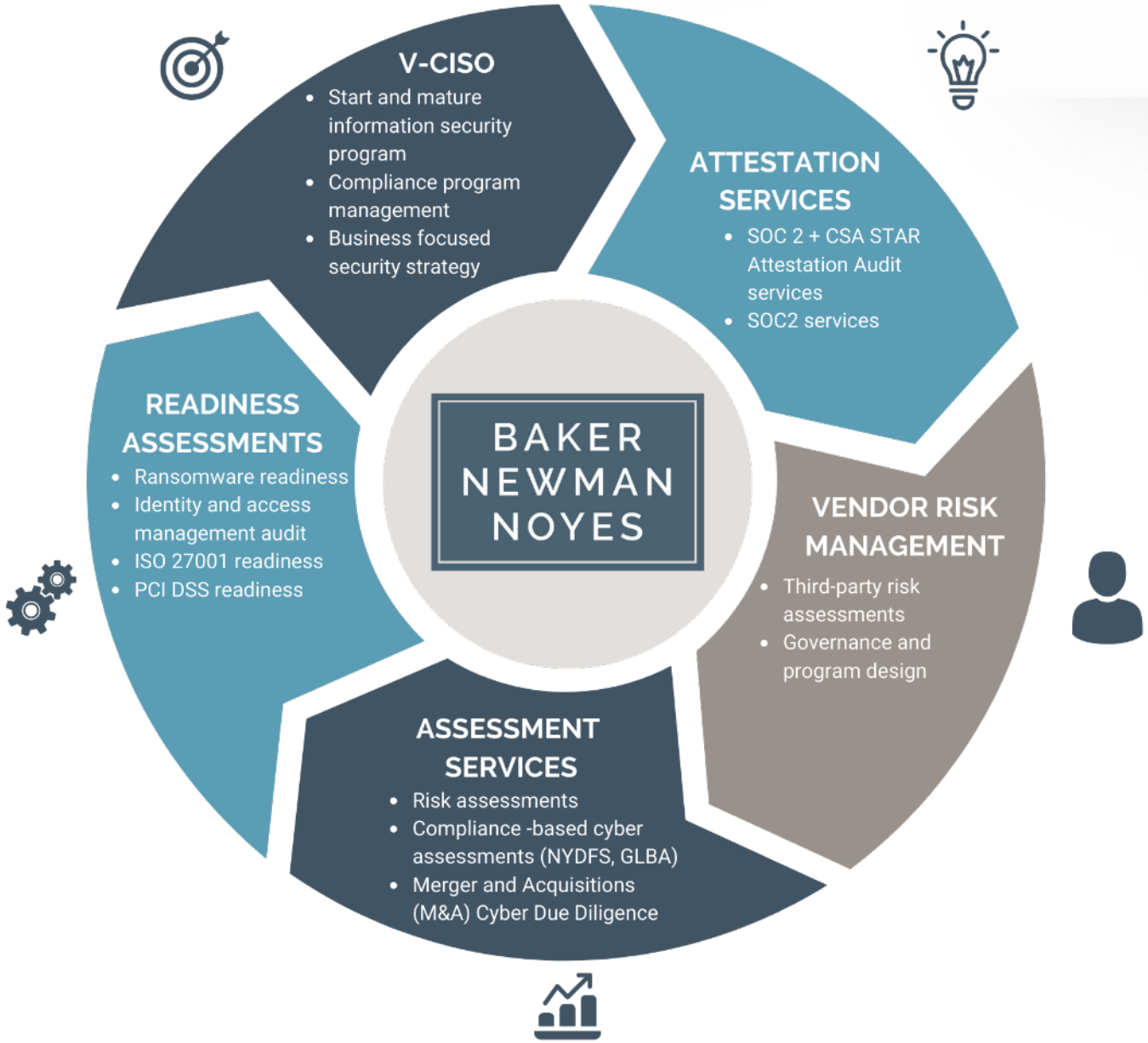
Here with you today

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

What you will hear today

BAKER NEWMAN NOYES

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

Key takeaways from the 2022 Verizon DBIR report

Key takeaways from the 2022 Verizon DBIR report

BAKER NEWMAN NOYES

- Supply chain is still top of mind and a serious threat.

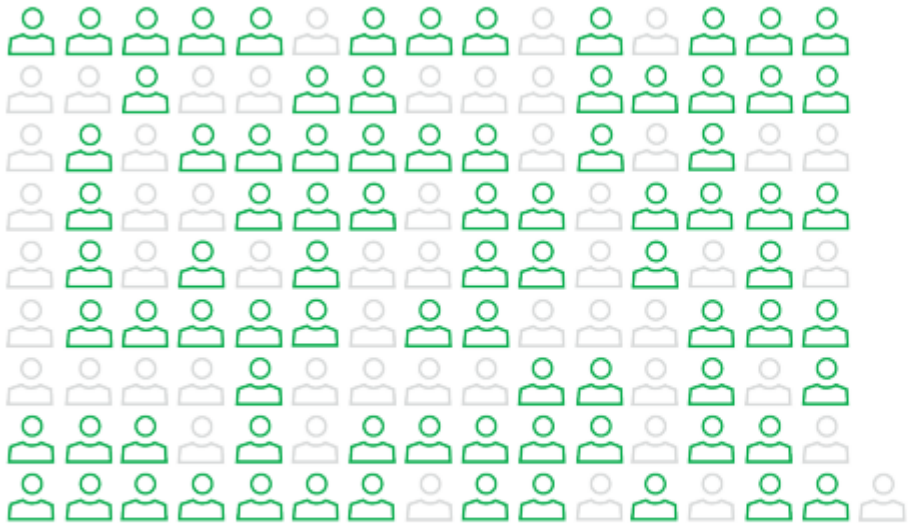


Figure 7. Partner vector in System Intrusion incidents (n=3,403)
Each glyph represents 25 incidents.

2021 illustrated how one key supply chain breach can lead to wide ranging consequences. Supply chain was responsible for 62% of System Intrusion incidents this year. Unlike a Financially motivated actor, Nation-state threat actors may skip the breach and keep the access.

Key takeaways from the 2022 Verizon DBIR report

BAKER NEWMAN NOYES

- 82% of actual breaches had a human element to them.

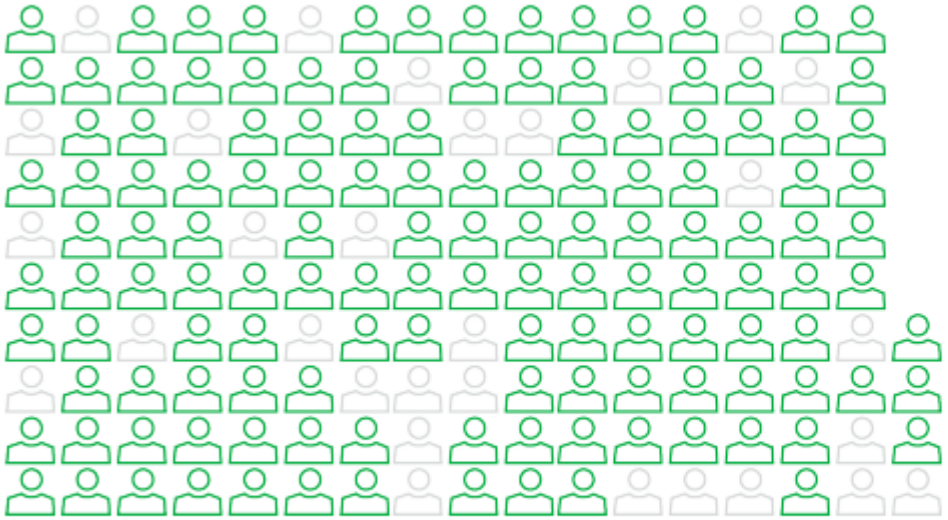


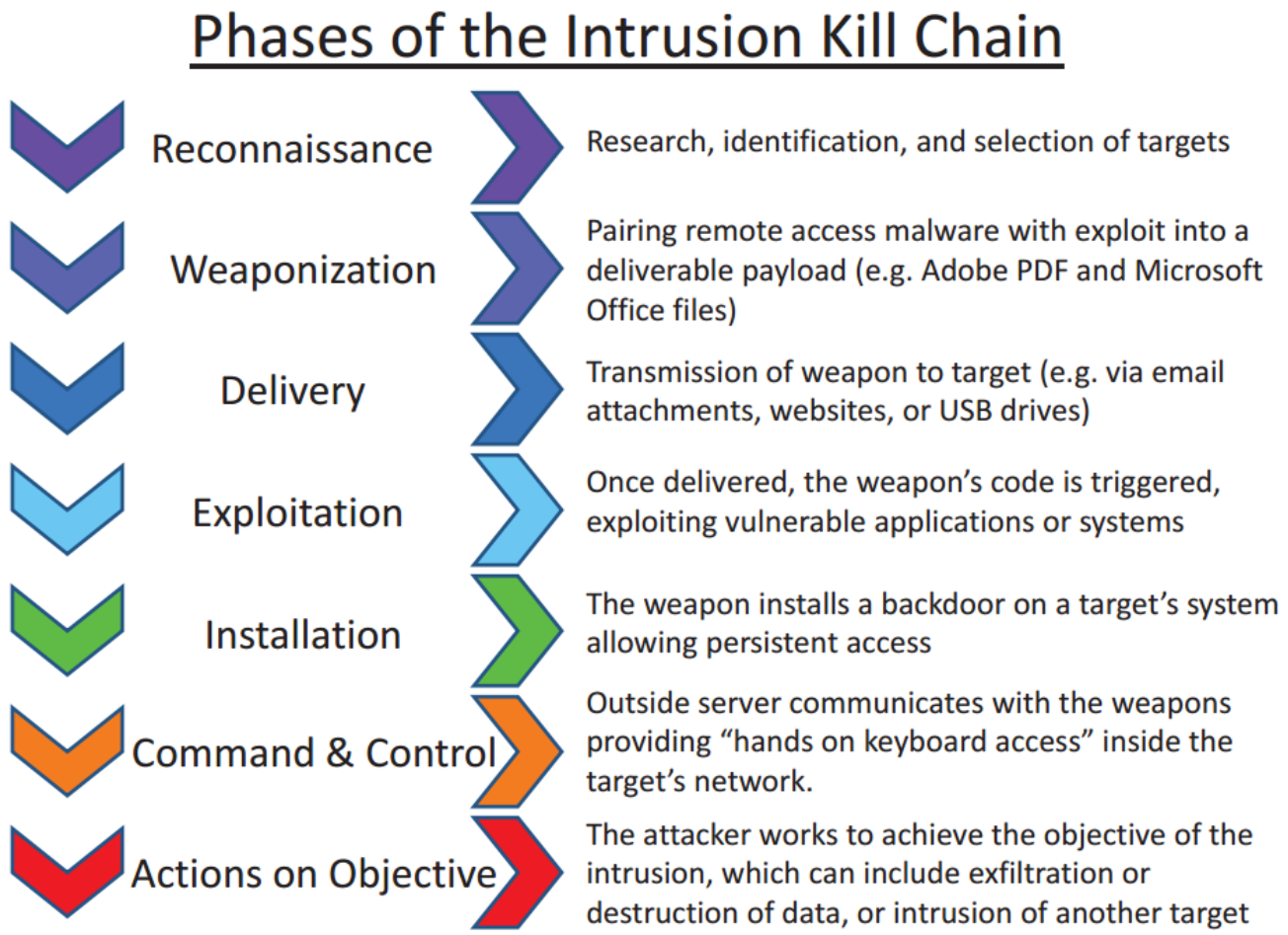
Figure 9. The human element in breaches (n=4,110)
Each glyph represents 25 breaches.

The human element continues to drive breaches. This year 82% of breaches involved the human element. Whether it is the Use of stolen credentials, Phishing, Misuse, or simply an Error, people continue to play a very large role in incidents and breaches alike.

Key takeaways from the 2022 Verizon DBIR report

BAKER NEWMAN NOYES

- 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.



Key takeaways from the 2022 Verizon DBIR report

BAKER NEWMAN NOYES

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

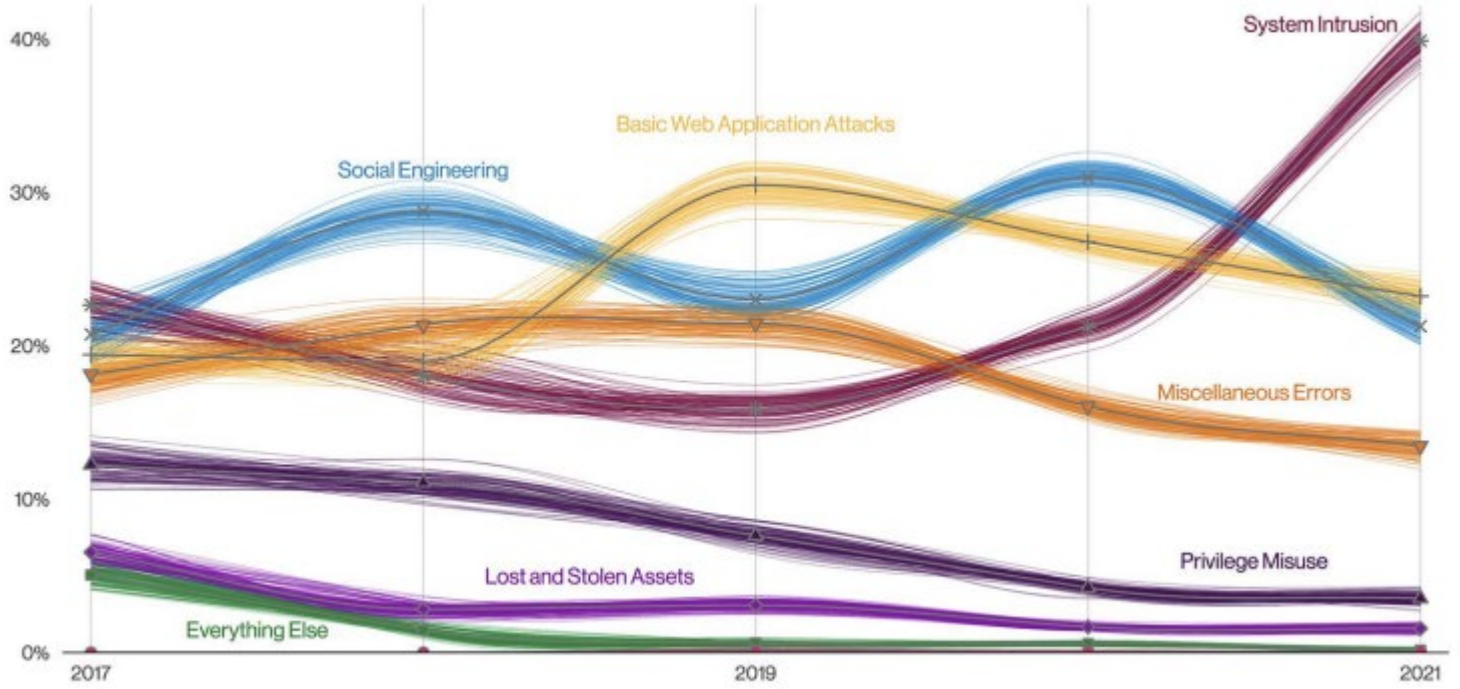


Figure 33. Patterns over time in breaches

Key takeaways from the 2022 Verizon DBIR report

BAKER NEWMAN NOYES

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

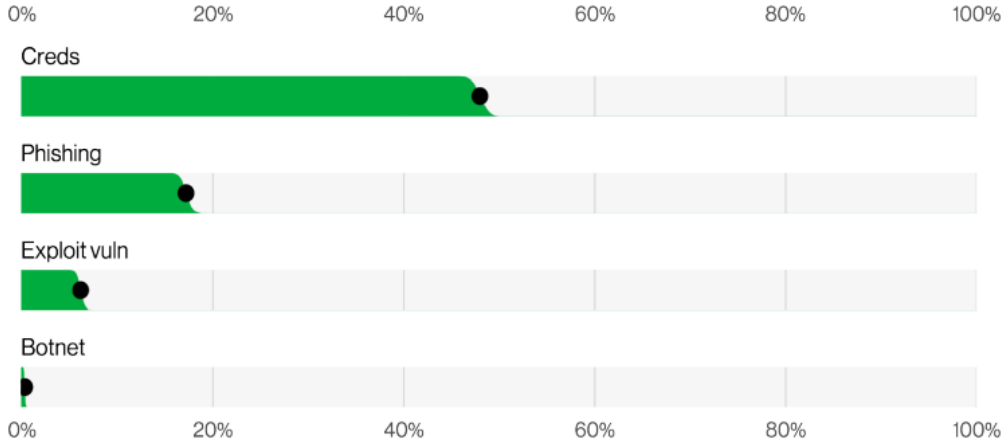


Figure 5. Select enumerations in non-Error, non-Misuse breaches (n=4,250)

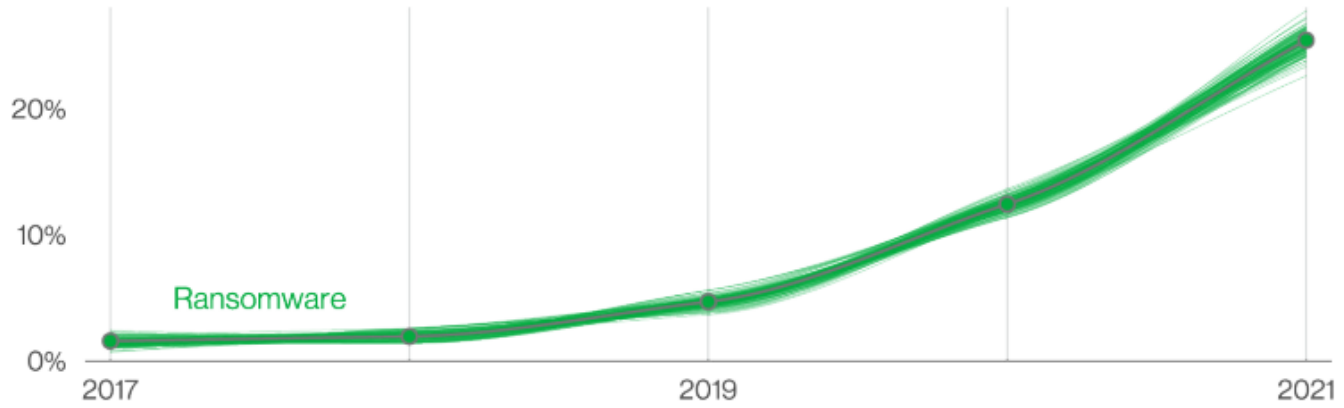
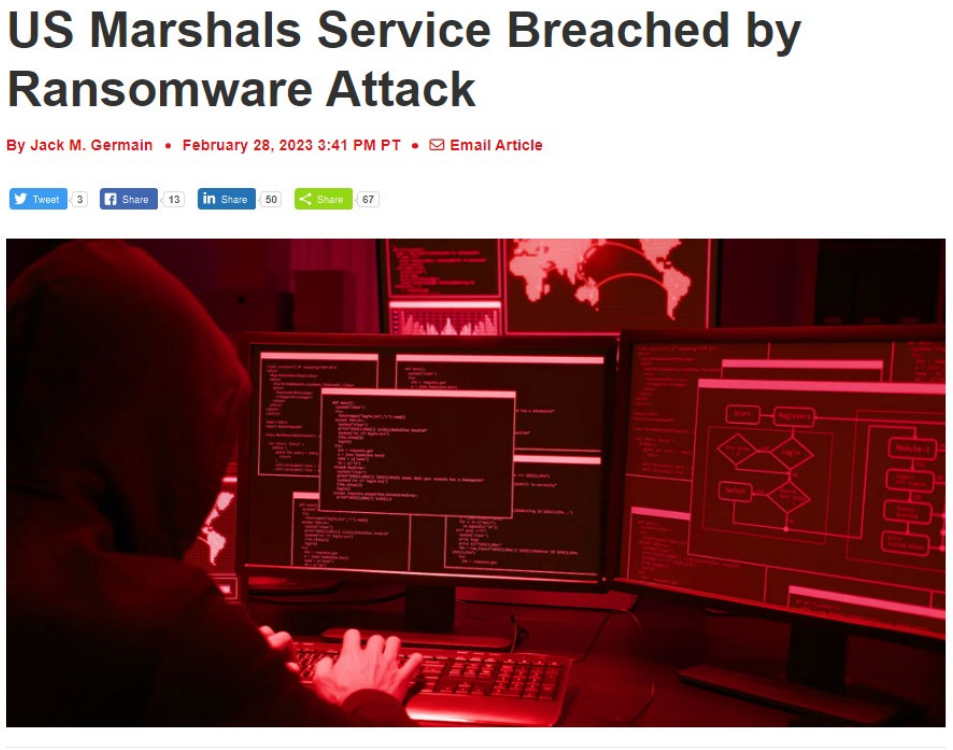


Figure 6. Ransomware over time in breaches

BAKER
NEWMAN
NOYES

Current events

Current events



- 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

BAKER NEWMAN NOYES

Dole discloses employee data breach after ransomware attack

By Sergiu Gatlan March 22, 2023 03:04 PM 0

- February 2023 ransomware attack accessed the information of an undisclosed number of employees
- Forced at the time to shut down production plants across North America

Current events

AT&T alerts 9 million customers of data breach after vendor hack

By Sergiu Gatlan March 9, 2023 12:24 PM 0

- AT&T lost information on 9 million customers
- A marketing vendor they use was hacked
- ONLY Customer Proprietary Network Information (CPNI) (no SSN)

Current events: Morgan Stanley

BAKER NEWMAN NOYES

- 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

Current events: Uber – again?

BAKER NEWMAN NOYES

- Ex Uber CISO was found guilty on charges of obstruction of the proceedings of FTC and misprision of felony in connection with the attempted cover-up of a 2016 hack at Uber
- Sets new precedence to CISOs
- Document, document, document
- CISO's role has now changed and personal liability is a reality.

Uber

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

BAKER
NEWMAN
NOYES

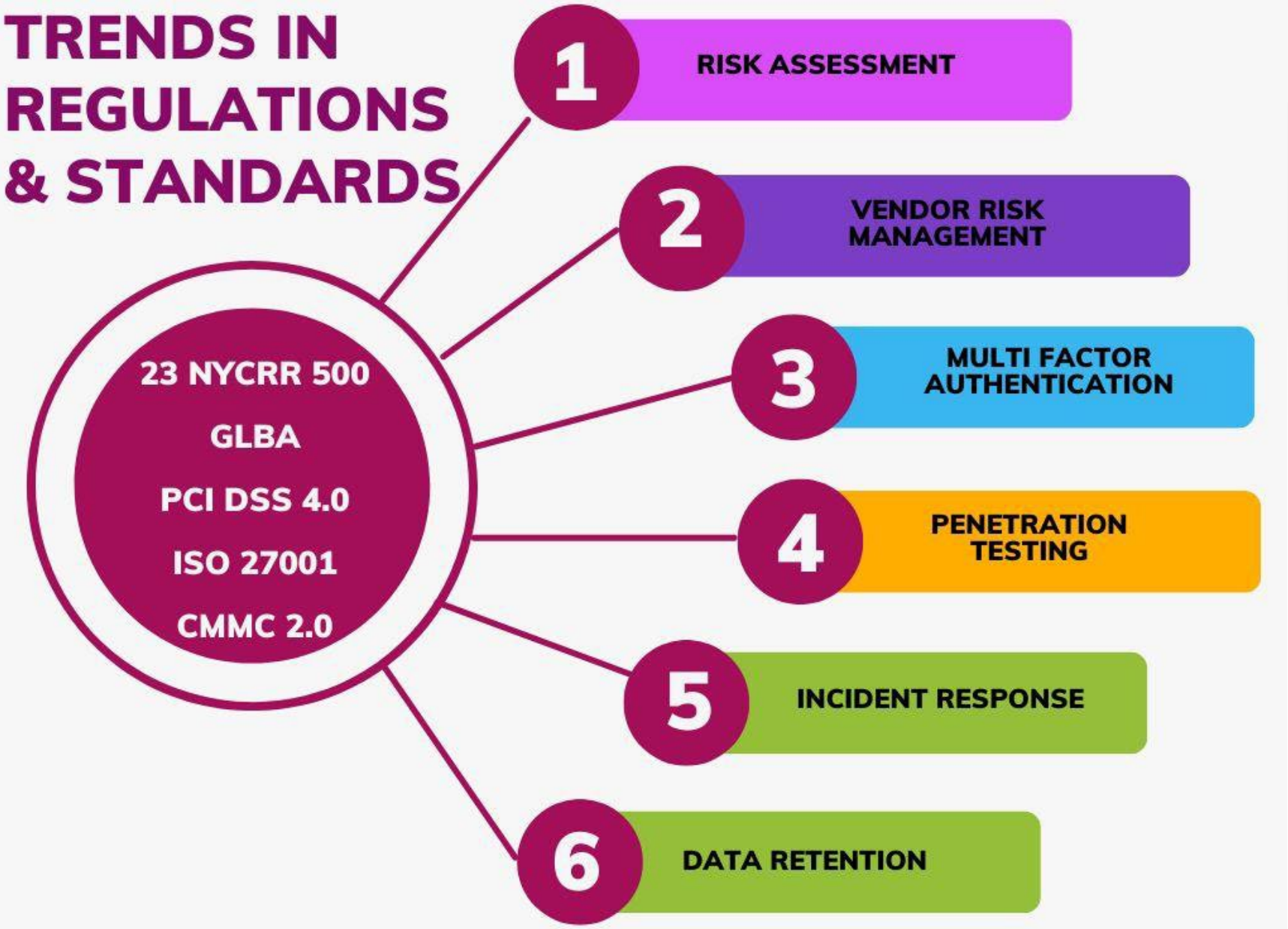
Compliance Updates

Updates in regulations and standards

BAKER NEWMAN NOYES

- Privacy – all business (GLBA)
- Banking (PCI DSS 4.0)
- Insurance (23 NYCRR 500)
- Government (CMMC 2.0)
- Security standard – all business (ISO 27001)
- Securities and Exchange Commission (SEC)

TRENDS IN REGULATIONS & STANDARDS



BAKER NEWMAN NOYES

A word on SEC updates

BAKER NEWMAN NOYES

BAKER
NEWMAN
NOYES

How to protect your bank

How to protect your bank

BAKER NEWMAN NOYES

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

How to protect your bank

BAKER NEWMAN NOYES

- 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 bank

- 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 bank

BAKER NEWMAN NOYES

- 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

- 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

Conclusion (continued)

BAKER NEWMAN NOYES

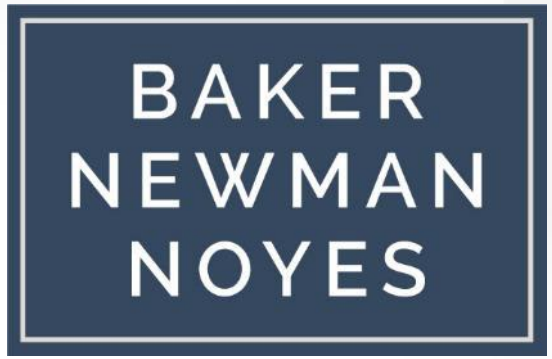
- Third-party risk management is more important than ever
- Security hygiene sets solid foundations for safe business
- Solid asset inventory, especially internet facing – can't protect what you don't know exists
- User education is the key to success – be creative

Conclusion (continued)

BAKER NEWMAN NOYES

- Updated regulations and standards have common trends: comply with one, satisfy many!
- Penetration testing, vulnerability and risk assessments provide good feedback
- Consider seeking independent audits / attestations / certifications

Questions?



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!