Mitigating Cyber Risk with Third-Party Vendors

Accounting & Business Update

October 19, 2022

BAKER NEWMAN NOYES

Here with you today

Pat Morin specializes in delivering various attestation services, including compliance examinations and SOC 1® and SOC 2® services. Pat also has specialized expertise in information technology controls, cyber security, information systems and process controls, and data extraction and analysis. He has worked with companies in a wide range of industries for over 30 years.

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.

Patrick Morin

Principal, Information Systems & Risk Assurance Practice Lead

pmorin@bnncpa.com

Pawel Wilczynski

Manager, Information Systems & Risk Assurance Practice

pwilczynski@bnncpa.com

What you will hear today

- Welcome and introductions
- Cybersecurity updates:
  - Verizon DBIR highlights
  - Current events
  - How to stay safe out there
- What is Third-Party Risk Management and why is it important?
- 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.

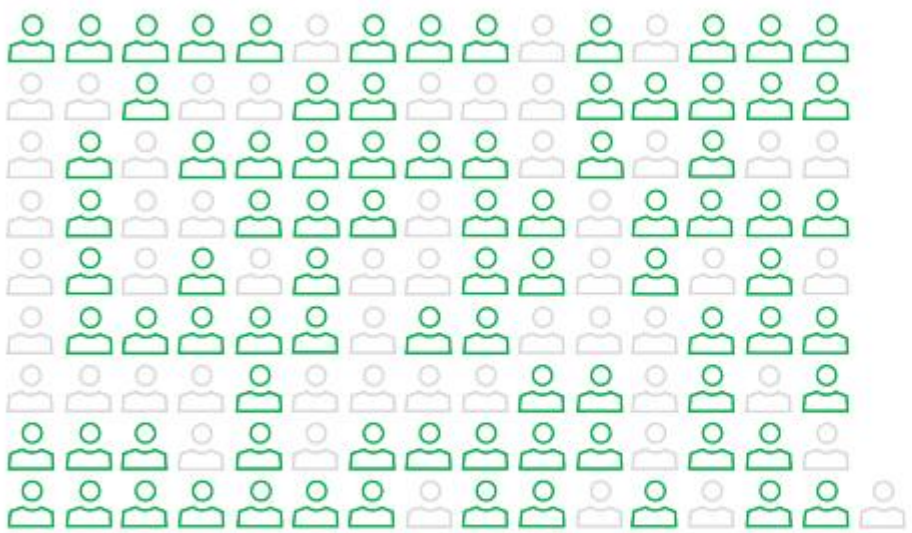


Figure 7. Partner vector in System Intrusion incidents (n=3,403)
Each glyph represents 25 incidents.

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.

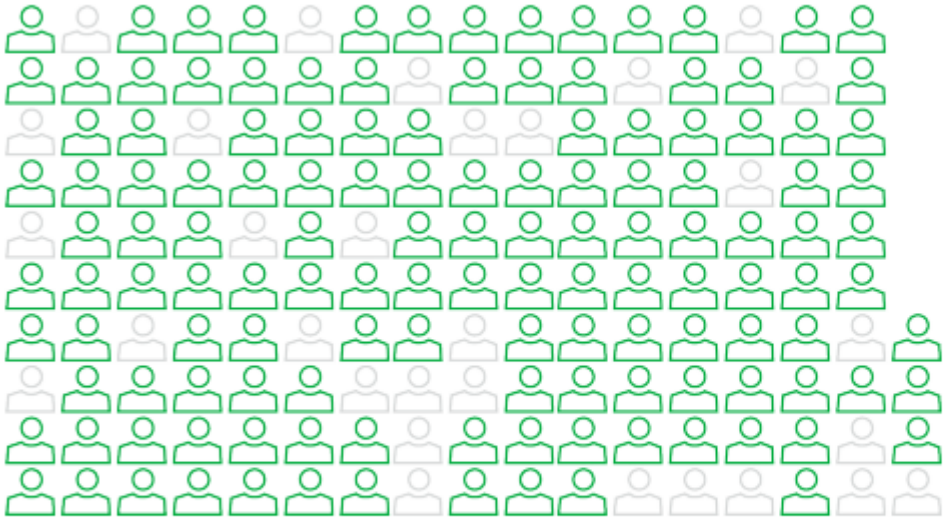


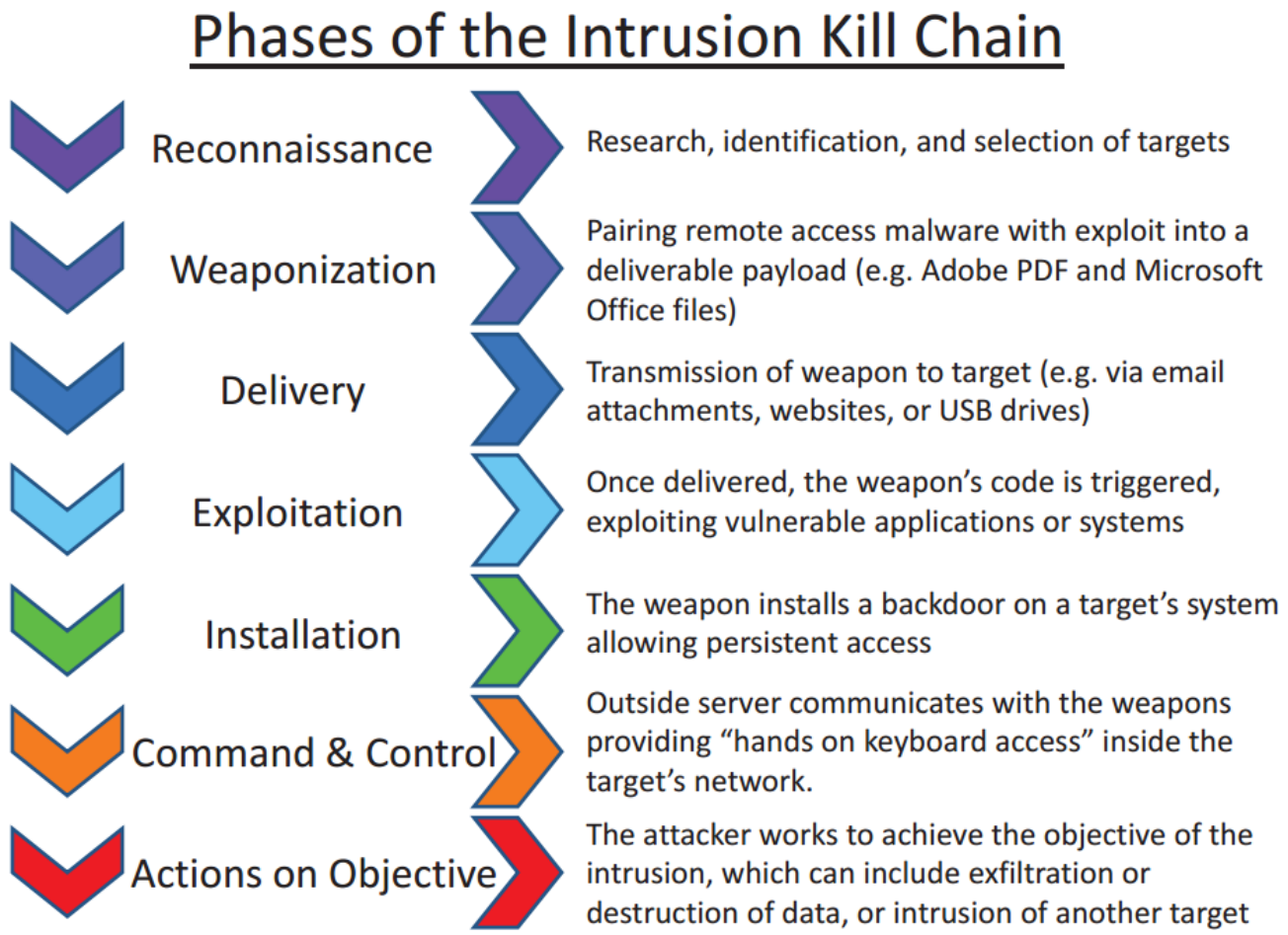
Figure 9. The human element in breaches (n=4,110)
Each glyph represents 25 breaches.

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

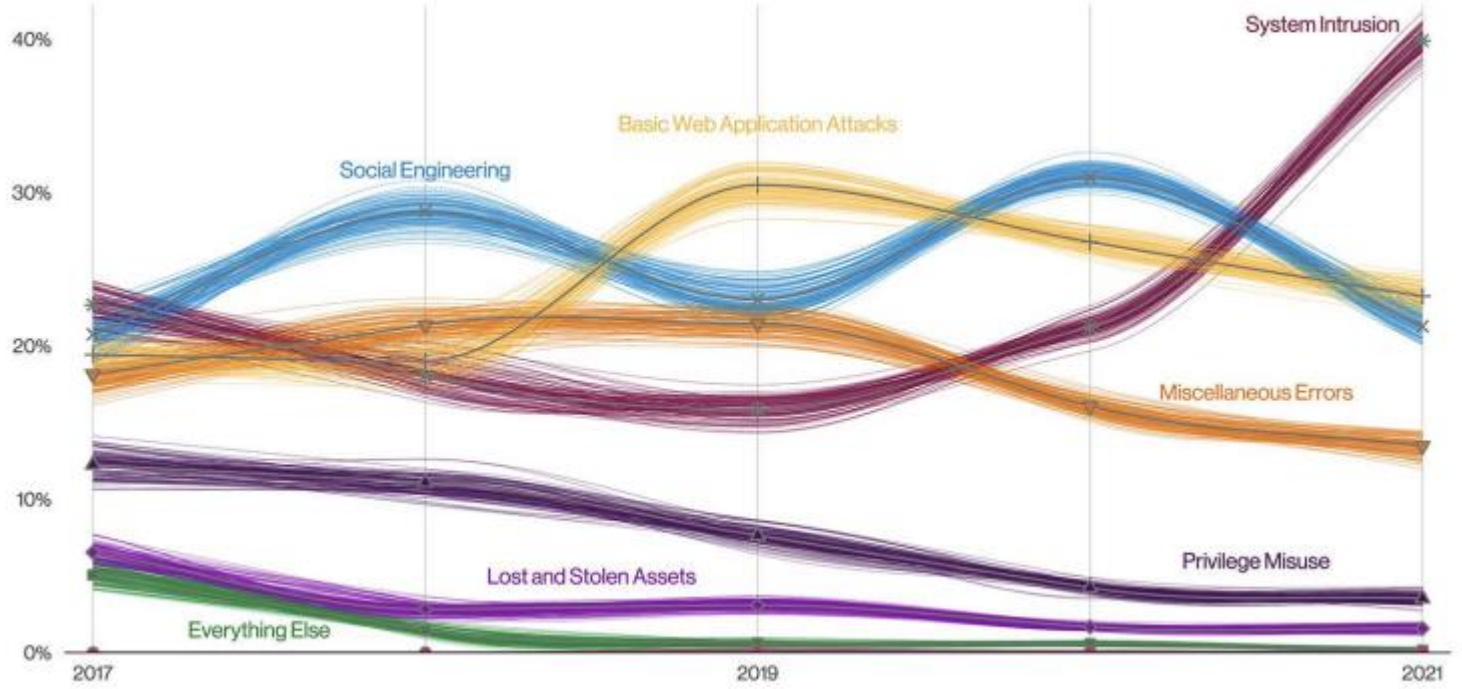


Figure 33. Patterns over time in breaches

Key takeaways from the 2022 Verizon DBIR report

BAKER NEWMAN NOYES

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

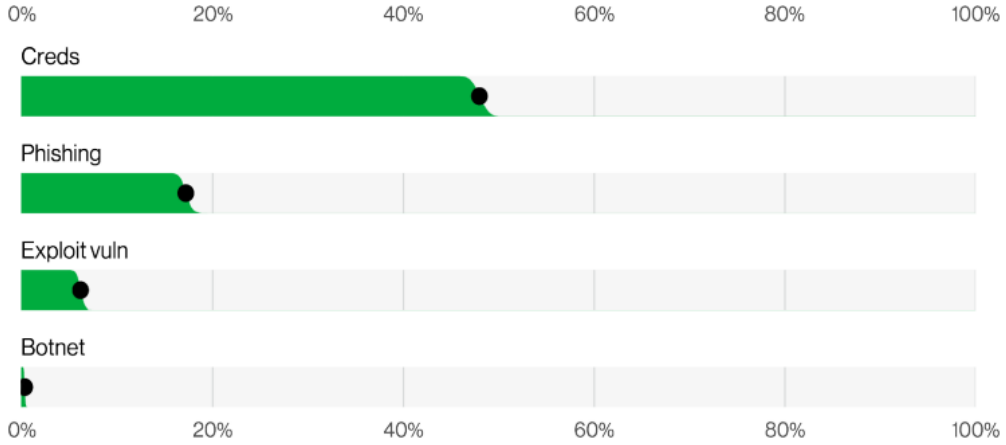


Figure 5. Select enumerations in non-Error, non-Misuse breaches (n=4,250)

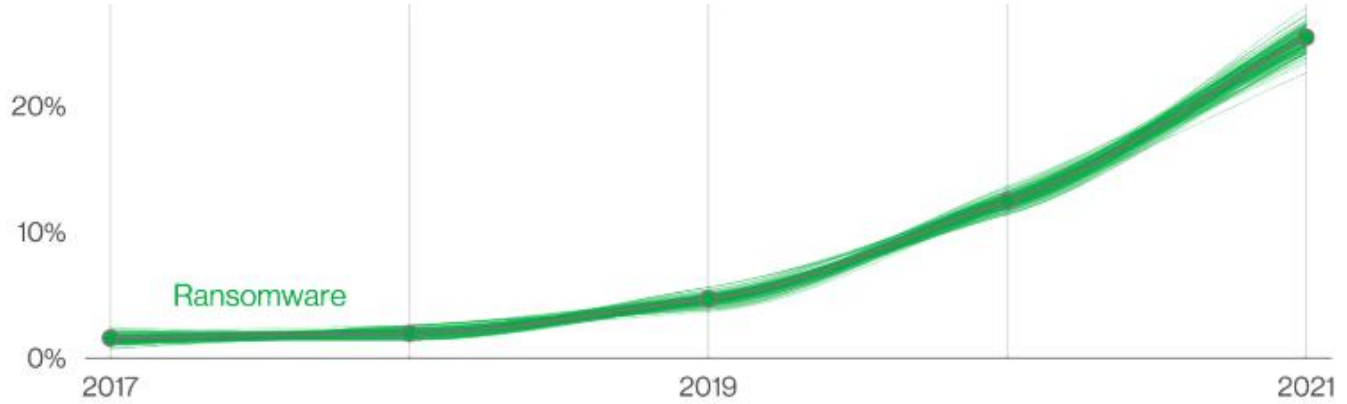


Figure 6. Ransomware over time in breaches

Current events: trending exploits

BAKER NEWMAN NOYES

- Malware in pdfs targeting Mac users
- Apple computers are not immune to the attacks
- As the market share of Macs grows, so to does the malware targeting it

Every legitimate endpoint detection and response (EDR) vendor has support for Macs, use it!

Current events

- Story Time

BAKER NEWMAN NOYES

Current events: Cisco incident - MFA

BAKER NEWMAN NOYES

- The hacker gained access to a Cisco employee's personal Gmail account
- That Gmail account had saved credentials for the Cisco VPN
- To bypass MFA, attacker used a combination of MFA push spamming and impersonating helpdesk
- After connecting to the VPN, the hackers enrolled new devices for MFA
- This allowed them to log into the network and begin moving laterally

User education is more important than ever.

Current events: Uber incident

BAKER NEWMAN NOYES

- An Uber contractor had their account compromised by an attacker.
- User accepted one of the MFA push requests, granting attacker's access to Uber's central systems
- Uber believes hacking group called Lapsus$, was responsible
- In 2022 alone Lapsus$ has breached Microsoft, Cisco, Samsung, Nvidia and Okta, among others, using similar tactics

Uber

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.

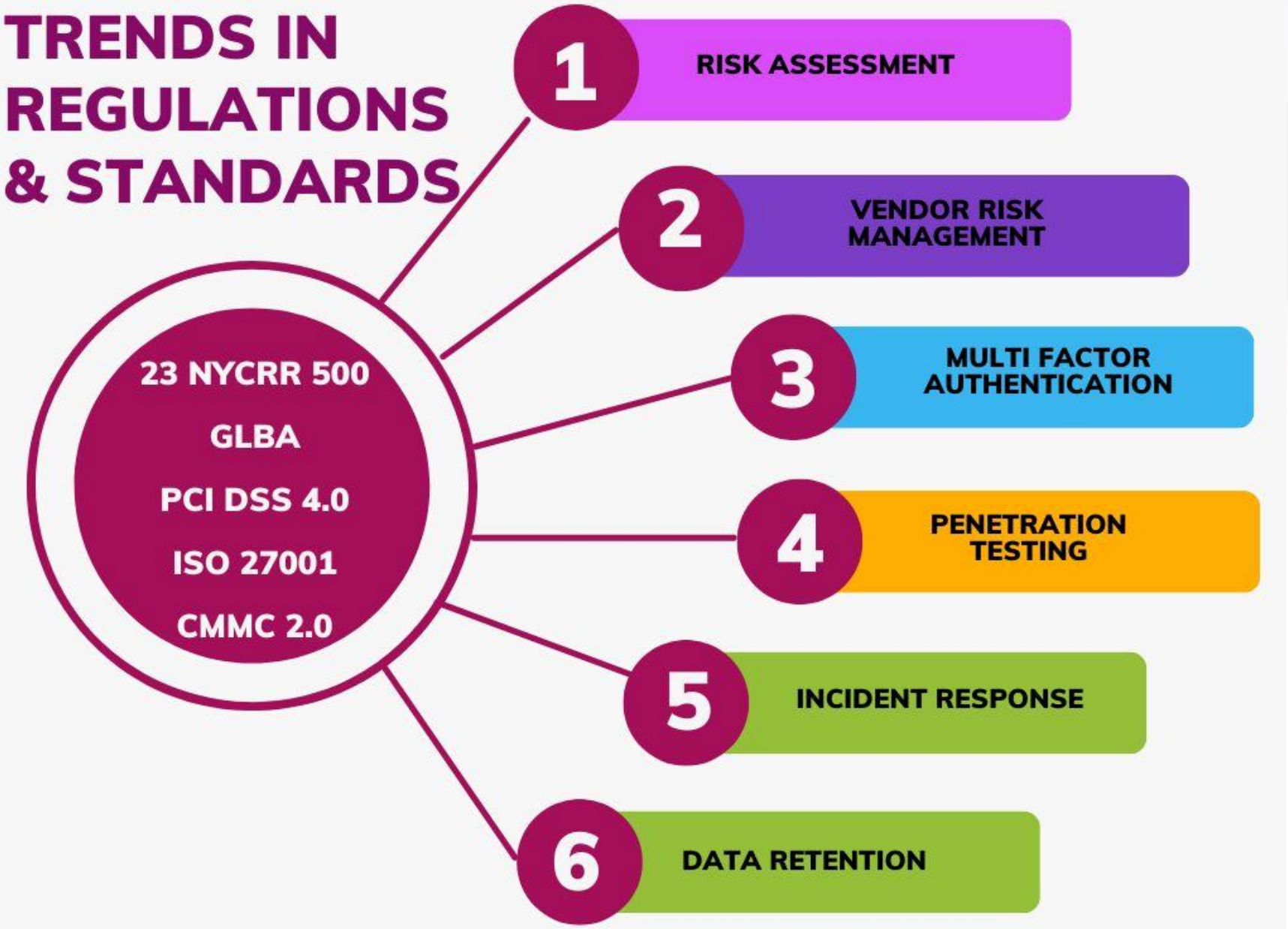
Uber

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)

TRENDS IN REGULATIONS & STANDARDS



BAKER NEWMAN NOYES

How to stay safe out there

BAKER NEWMAN NOYES

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

How to stay safe out there

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 stay safe out there

- Be smart about selecting vendors
- Assess security controls, technology and expertise to properly manage your sensitive data
- Review the contract, including terms, renewals, required service levels, and termination requirements and **right to audit**!

How to stay safe out there

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 risk …

Third-party risk management

BAKER NEWMAN NOYES

What is Third-Party Risk Management and why is it important?

Why the risk exists?

What exactly is the risk?

What can you do about it?

How can you assess the risk?

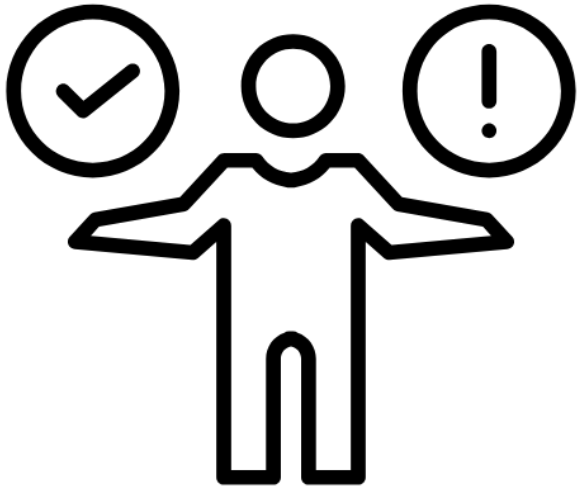
What if the risk is too great?

What is third-party risk management?

BAKER NEWMAN NOYES

- Third-Party Risk Management discipline focuses on identifying and mitigating risks associated with third-parties.

*Third-Party encompasses suppliers, vendors and service providers



Why is third-party risk management important

BAKER NEWMAN NOYES

Third-Party Risk Management enables you to:

- Track security controls and manage risk mitigation efforts
- Hold vendors accountable
- Understand how data flows and who has access
- Onboard only vendors who meet your organization’s security standards
- Comply with relevant regulations and industry requirements

Why the risk exists

- Businesses cannot afford to hire, train, and retain specialized talent and needed infrastructure
- Third-party vendors handle parts of the business
- Companies, across all spectrums of sizes and industries, outsource systems and applications

What is the risk

BAKER NEWMAN NOYES

- Third-party vendors handle, process, and store customers' personal information and other sensitive data
- Some third-party vendors are critical enough for daily operations' success
- Third-party vendors are a threat vector (Kaseya, SolarWinds, OKTA)
- Compliance risk

What you can do about it

BAKER NEWMAN NOYES

- Gain better understanding of third-party vendor security posture
- Vet vendors' security during the selection process
- Do not overlook the security assessment prior to signing-on the new vendor
- Existing vendors should be evaluated for risk at renewal or on periodic basis
- Consider seeking independent audits / attestations / certifications

How to assess the risk

BAKER NEWMAN NOYES

Steps for a successful third-party risk assessment include:

- Communicate with your third-party vendor why the risk assessment is being conducted
- Identify inherent risks
- Evaluate the controls in place that address risks
- Assess residual risk against your company's risk appetite
- Communicate with your third-party vendor if any of the risks fall outside risk appetite

What if the risk is too great

BAKER NEWMAN NOYES

- Unidentified risks, cannot be mitigated!
- If the risk doesn’t fit within risk appetite, there are two options:
  - Work with the vendor on a remediation plan
  - Off board the vendor (or do not sign a contract)

Conclusion

BAKER NEWMAN NOYES

- Third Party Risk Management is more important than ever!
- Security hygiene sets solid foundations for safe business!
- User education is the key to success – be creative!
- 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?

BAKER NEWMAN NOYES

Contact Us

Patrick Morin

Principal, Information Systems &
Risk Assurance Practice Lead

pmorin@bnncpa.com

Pawel Wilczynski

Manager, Information Systems &
Risk Assurance Practice

pwilczynski@bnncpa.com

BAKER NEWMAN NOYES

PORTLAND
BOSTON | WOBURN
MANCHESTER | PORTSMOUTH

BAKER
NEWMAN
NOYES

Thank You!