venminder
AN NCONTRACTS COMPANY

Creating Safe and Secure Third-Party Partnerships

September 18, 2024

PRESENTED BY

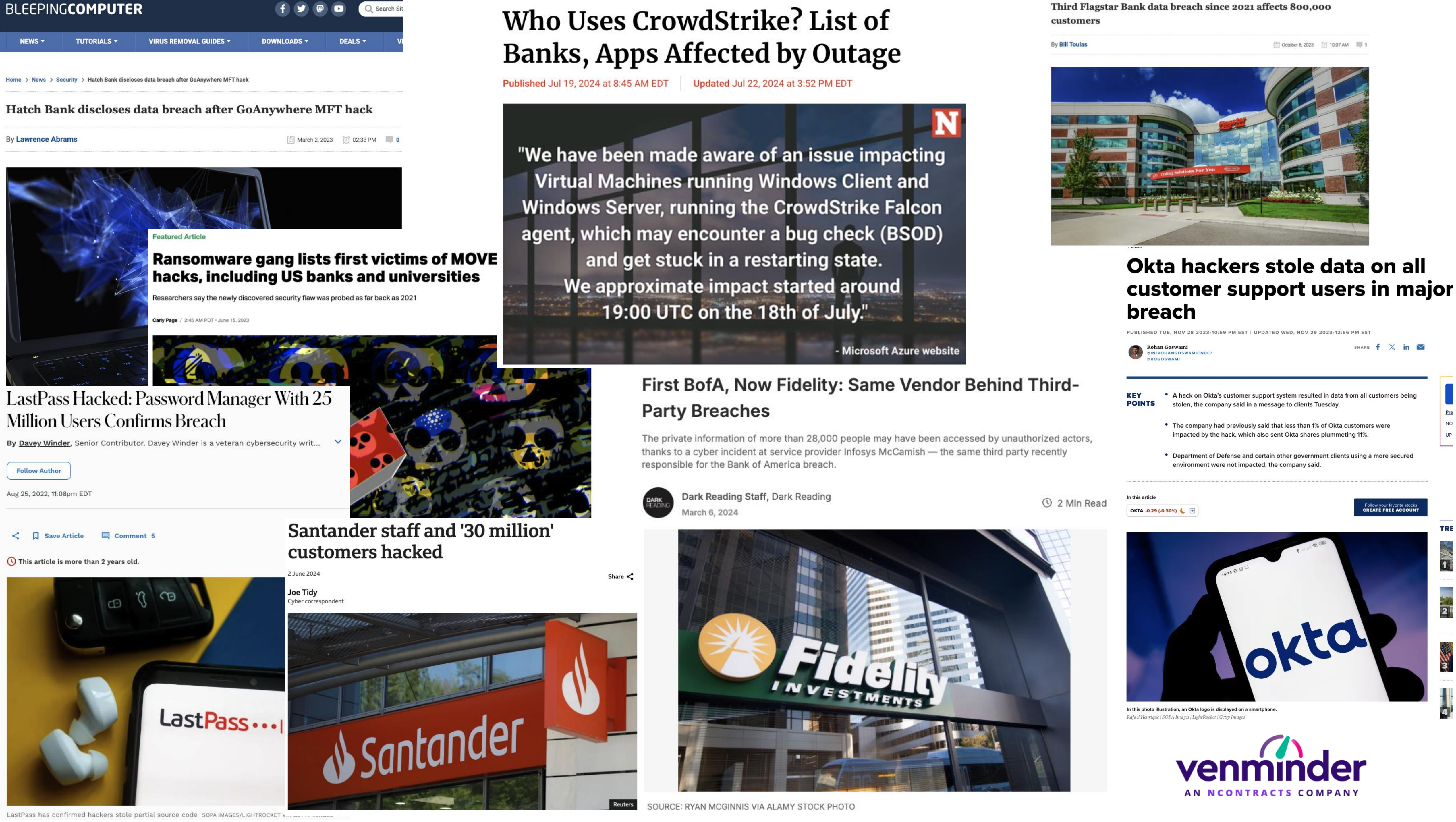
Aaron Kirkpatrick

Chief Information Security Officer
Venminder

Session Agenda

1. Understanding why we are here
2. Assessing risk from multiple angles
3. Reviewing vendor control documentation
4. What happens when your vendors aren’t perfect
5. Key takeaways

Why Talk About Cybersecurity Risks Introduced by Third Parties?



Hatch Bank discloses data breach after GoAnywhere MFT hack

By Lawrence Abrams March 2, 2023 02:33 PM 0

Featured Article

Ransomware gang lists first victims of MOVE hacks, including US banks and universities

Researchers say the newly discovered security flaw was probed as far back as 2021

Carly Page / 2:45 AM PDT • June 15, 2023

LastPass Hacked: Password Manager With 25 Million Users Confirms Breach

By Davey Winder, Senior Contributor. Davey Winder is a veteran cybersecurity writ...

Aug 25, 2022, 11:08pm EDT

This article is more than 2 years old.

LastPass has confirmed hackers stole partial source code SOPA IMAGES/LIGHTROCKET VIA GETTY IMAGES

Santander staff and '30 million' customers hacked

2 June 2024

Joe Tidy
Cyber correspondent

Reuters

Who Uses CrowdStrike? List of Banks, Apps Affected by Outage

Published Jul 19, 2024 at 8:45 AM EDT | Updated Jul 22, 2024 at 3:52 PM EDT

"We have been made aware of an issue impacting Virtual Machines running Windows Client and Windows Server, running the CrowdStrike Falcon agent, which may encounter a bug check (BSOD) and get stuck in a restarting state. We approximate impact started around 19:00 UTC on the 18th of July."

- Microsoft Azure website

First BofA, Now Fidelity: Same Vendor Behind Third-Party Breaches

The private information of more than 28,000 people may have been accessed by unauthorized actors, thanks to a cyber incident at service provider Infosys McCamish — the same third party recently responsible for the Bank of America breach.

Dark Reading Staff, Dark Reading
March 6, 2024
2 Min Read

SOURCE: RYAN MCGINNIS VIA ALAMY STOCK PHOTO

Third Flagstar Bank data breach since 2021 affects 800,000 customers

By Bill Toulas October 8, 2023 10:07 AM 1

Okta hackers stole data on all customer support users in major breach

PUBLISHED TUE, NOV 28 2023-10:59 PM EST | UPDATED WED, NOV 29 2023-12:56 PM EST

Rohan Goswami
@IN/ROHANGOSWAMICNBC/
@ROGOSWAMI

KEY POINTS

- A hack on Okta's customer support system resulted in data from all customers being stolen, the company said in a message to clients Tuesday.
- The company had previously said that less than 1% of Okta customers were impacted by the hack, which also sent Okta shares plummeting 11%.
- Department of Defense and certain other government clients using a more secured environment were not impacted, the company said.

In this article

OKTA -0.29 (-0.30%)

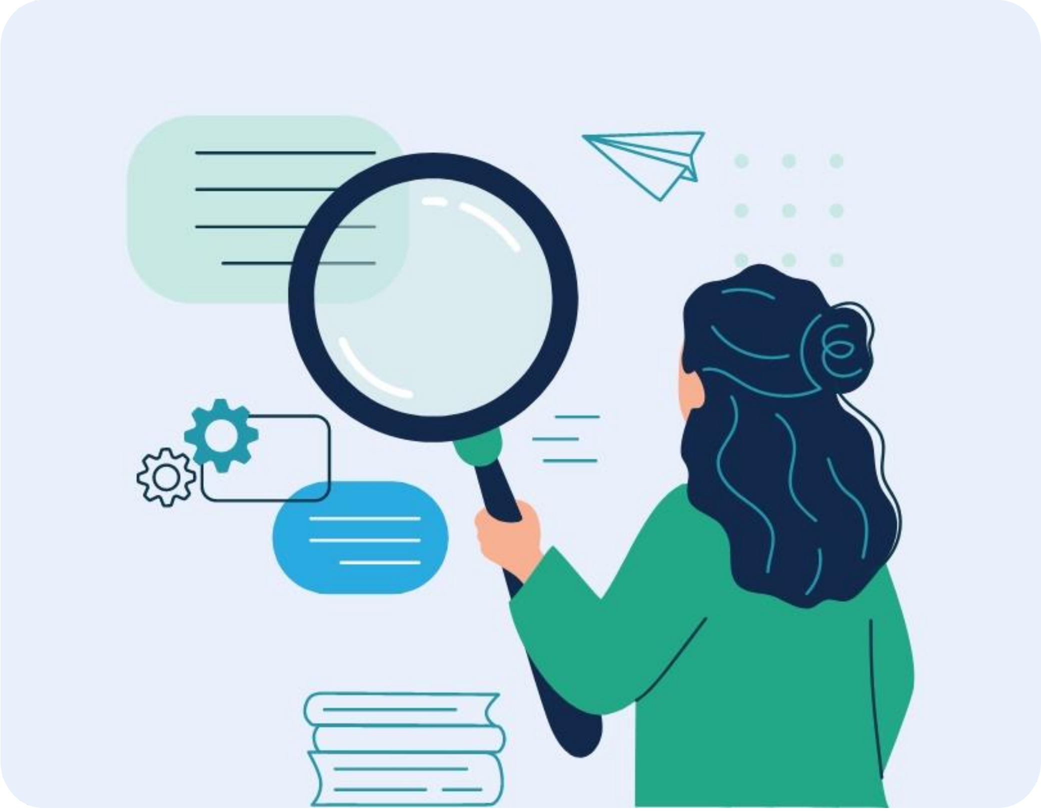
In this photo illustration, an Okta logo is displayed on a smartphone.
Rafael Henrique | SOPA Images | LightRocket | Getty Images

venminder
AN NCONTRACTS COMPANY

We Just Send a Request to All of Our Vendors… Right?

Know the Scope – Vendor Inventory

- You can’t protect what you don’t know exists
- Key data points to enable reporting



We Send the Requests Now… Right!?

Know the Scope – Understand Inherent Risks

- Using any vendor to outsource a function presents risks
    - They also may mitigate other risks
- Understand the type of risk
- Use internal vendor profile data
- Use internal inherent risk assessments
- Understand how to mitigate those risks
    - Internal controls
    - Vendor controls (Later!)

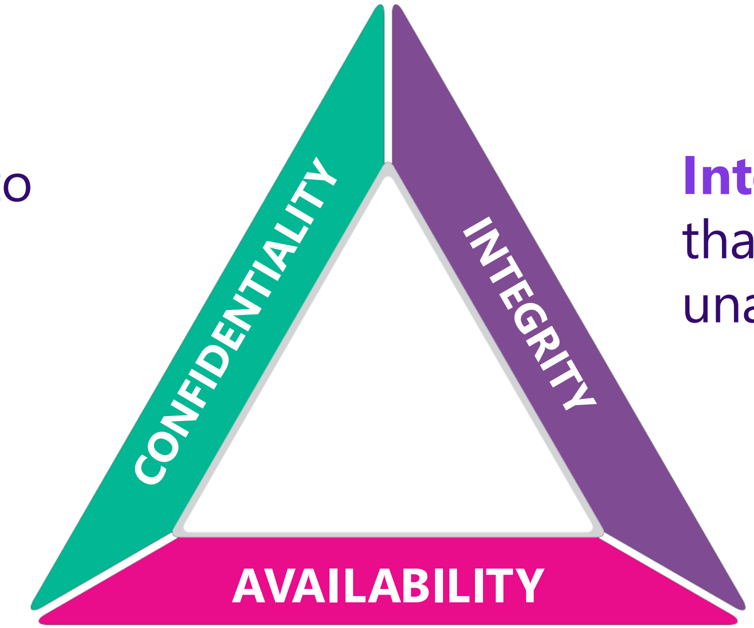
Know the Scope – Determine Priority

- Using inherent risk results, prioritize your due diligence and ongoing monitoring:
  - Consumer data/sensitive data **(Confidentiality)**
  - Transactional data **(Integrity)**
  - Customer or operations impact if unavailable **(Availability)**
- Use this prioritization and identified risks for efficiency and effectiveness:
  - Assess your resources, timelines/cadence, and requirements
- Create your plan

The CIA Information Security Triad

Cybersecurity is based on the CIA information security triad that encompasses:

Confidentiality – seeks to prevent unauthorized disclosure of information

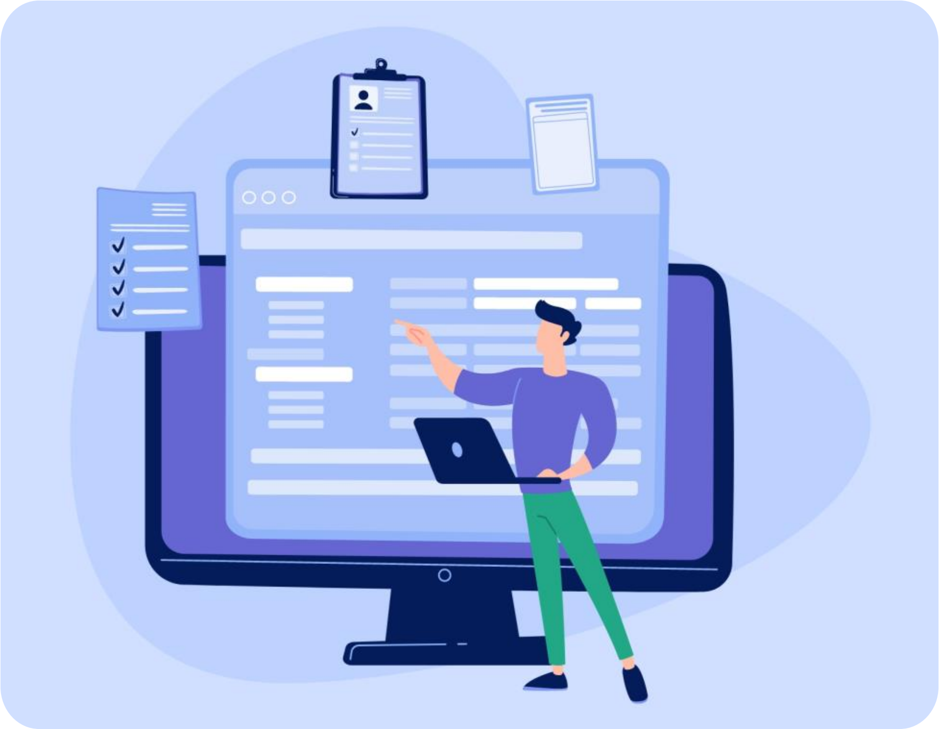


Integrity – seeks to ensure that data isn't modified by unauthorized means

Availability – ensures that information is available when needed and only to authorized personnel

Know Your Internal Facing Requirements

- Understand your internal operations commitments:
  - Service Level Agreements (SLA)
  - Recovery Time Objectives (RTO)
  - Recovery Point Objectives (RPO)
- How will you monitor those?



We STILL Haven’t Sent Those Requests!

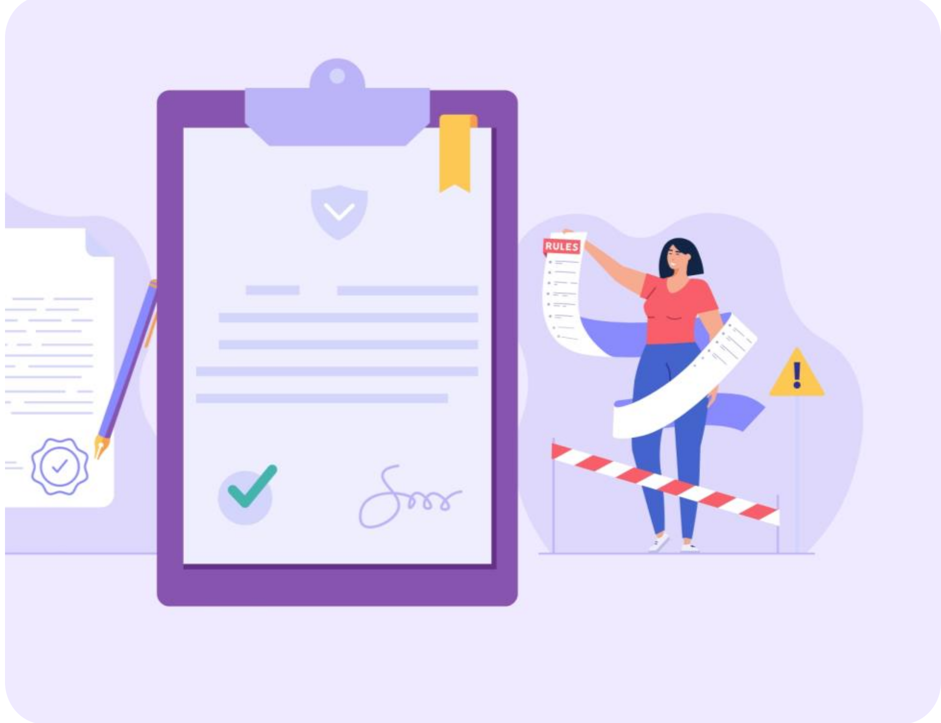
Know Your Internal Facing Requirements
CONTINUED

- Data Transfer (Encryption)
- Large Transactions (Separation of Duties)
- Privacy (Notices, Data Subject Access Request (DSAR), data flow, etc.)
- Sensitive Data (Identity and Access Management, referred to as IAM)

Trust Me… We’re ALMOST Ready to Send Our Requests!

Realistic Expectations

- You WILL NOT identify every vulnerable part of your vendor
- You're doing an important process to prove your due diligence
- You struggle to improve your own practices; you aren’t likely to impact your vendor’s



What Should You Do? It Depends…

- What are your drivers?
  - Internal (We want to be secure!)
  - External (Regulations. It's the Law…)
- What's my budget?
- Where are you starting from?
  - How mature is my TPRM process?
  - How much can we actually handle?
  - What are we going to do with vendor responses?

Understand What You're Getting Into

- Knowledge is power… knowing is dangerous:
  - Applicable, identified, unconfirmed vulnerabilities which may lead to a risk, need confirmation. Do you have the resources to follow up?
  - Create an efficient process to document and assess.

When Should You Assess Vendor Cybersecurity?

ONBOARDING:

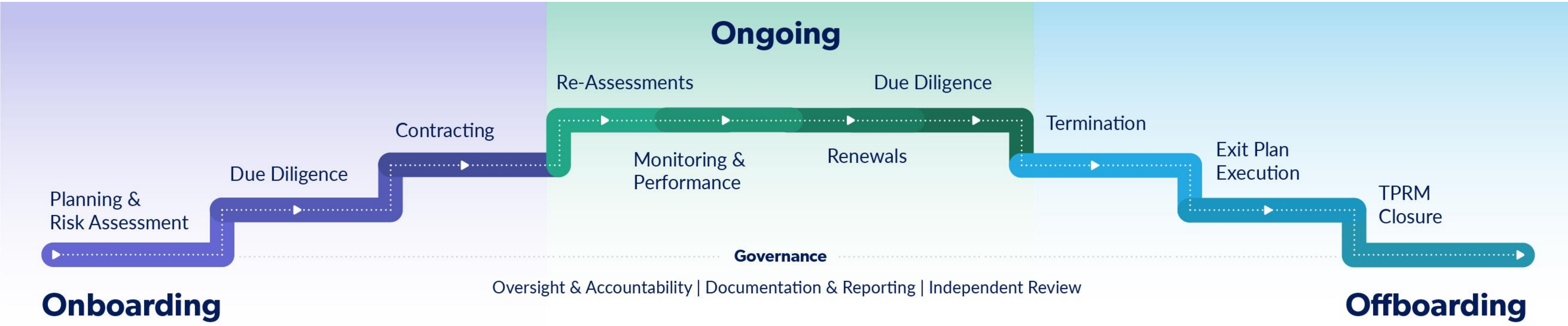
During the Planning & Risk Assessment and Due Diligence steps

ONGOING:

During the Re-Assessments, Monitoring & Performance, Renewals, and Due Diligence steps

OFFBOARDING:

During the Termination, Exit Plan Execution, and TPRM Closure



venminder
AN NCONTRACTS COMPANY

Offboarding Interlude

- Don’t be the organization that has to report to their customers that an incident at a third party that you don't even use anymore exposed their data.
- Post-contract data deletion/certificate of destruction.

So Many Options for Due Diligence

- Right-size it for your organization and have realistic expectations of the vendor:
  - Information Gathering
  - Initial/Ongoing Monitoring (Cyber, Privacy, Financial, Reputation, ESG, etc.)
  - Questionnaires (So many options!)
  - Documentation Review (So many variations)
  - Virtual/On-Site Visits (Do we do these post-COVID?)

Privacy Laws

To date, 19 states have passed comprehensive privacy laws.

1. **California**: 2 of them
   - ✓ California Consumer Protection Act (CCPA) | *Went into effect: January 2020*
   - ✓ California Privacy Rights Act (CPRA) | *Went into effect: January 2023*
2. **Virginia:** Virginia Consumer Data Protection Act (CDPA) | *Went into effect: January 2023*
3. **Colorado:** Colorado Privacy Act (CPA) | *Went into effect: July 2023*
4. **Connecticut:** Connecticut Data Privacy Act | *Went into effect: July 2023*
5. **Utah:** Utah Consumer Privacy Act | *Went into effect: December 2023*
6. **Oregon:** Oregon Consumer Privacy Act | *Went into effect: July 1, 2024*
7. **Texas:** Texas Data Privacy and Security Act | *Went into effect: July 1, 2024*
8. **Montana:** Montana Consumer Data Privacy Act | *Effective October 1, 2024*
9. **Delaware:** Delaware Personal Data Privacy Act | *Effective January 1, 2025*
10. **Iowa:** Iowa Consumer Data Protection Act | *Effective January 1, 2025*
11. **Nebraska:** Nebraska Data Privacy Act | *Effective January 1, 2025*
12. **New Hampshire:** New Hampshire Privacy Act | *Effective January 1, 2025*
13. **New Jersey:** New Jersey Privacy Act | *Effective January 15, 2025*
14. **Tennessee:** Tennessee Information Protection Act | *Effective July 1, 2025*
15. **Minnesota:** Minnesota Consumer Data Privacy Act | *Effective July 31, 2025*
16. **Maryland:** Maryland Online Data Protection Act | *Effective October 1, 2025*
17. **Indiana:** Indiana Consumer Data Protection Act | *Effective January 1, 2026*
18. **Kentucky:** Kentucky Consumer Data Protection Act | *Effective January 1, 2026*
19. **Rhode Island:** Rhode Island Data Transparency and Privacy Protection Act | *Effective January 1, 2026*

So Many Options for Due Diligence – Good and Bad

Information Gathering

Good:

- Easy (Hopefully)
- Gather context of the solutions intended use/environment

Bad:

- Limited to the basics

So Many Options for Due Diligence – Good and Bad

Initial/Ongoing Monitoring (Cyber, Privacy, Financial, Reputation, ESG, etc.)

Good:

- Easy to obtain
- Relatively inexpensive

Bad:

- What do you do when it’s bad? Have a plan!

So Many Options for Due Diligence – Good and Bad

Questionnaires (So many options! You are not “special”.)

Good:

- Standardized approach for tiers of vendors (One questionnaire, unless tiered, doesn't rule all).
- Already options created to choose from! (SIG, Google VSAQ, CSA CAIQ, HECVAT, etc.)

Bad:

- What do you do when they won’t complete?
- What are you going to do when they respond negatively?

So Many Options for Due Diligence – Good and Bad

Documentation Review (So many variations)

Good

- Semi-standardized approach for tiers of vendors.
- Documentation should already exist, so it should be quick.

Bad

- You never know what you're going to get.
- Few follow an international standard for content.
- Is a 200-page Information Security Policy better than a two page one?
- Table of contents vs full policy.

So Many Options for Due Diligence – Good and Bad

Virtual/On-Site Visits (Do we do these post-COVID?)

Good

- Nothing replaces face-to-face discussions or visual inspections.

Bad

- Resource expensive (Time, travel costs)
- Limited applicability (Critical, physical infrastructure, etc.)

Now You Can Send the Requests!

What Should You Look At?

- Legal and entity-level controls
- Governance controls
- Plans
- Technical controls

Remember, as you review what to look at, right-size your review!

Categories of Documents That Should Be Reviewed: Legal and Entity-Level

In general, you'll want to obtain evidence that your vendor possesses the following documents and can provide evidence of:

- Confidentiality agreements
- Mutual non-disclosure agreements
- Employee background checks
- Security awareness training
- Cyber insurance

Categories of Documents That Should Be Reviewed: Governance

It’s important to identify the following topics within the cybersecurity policy relevant to your organization:

- Information security
- Access management
- Vulnerability management
- Encryption
- Privacy
- Data classification
- Third-party vendor risk management

Categories of Documents That Should Be Reviewed: Plans

These documents should reveal the details of how the vendor handles the following:

- Incident management
- Incident response
- Disaster Recovery
- Business Continuity

Plans should also include testing results!

Categories of Documents That Should Be Reviewed: Technical Controls and Processes

Documents listed prior and questionnaires may include key technical controls for review:

- Penetration test overviews
- Social engineering exercises
- Encryption at rest and in transit
- Multifactor authentication
- Event monitoring and alerting
- Patching cadence

What Vendors’ Cybersecurity Should Be Assessed and By Whom

What type of vendors should be assessed?

- All critical, moderate, and high-risk vendors
- Any vendors that access, process, transmit, or store your data

Who at your organization should assess the results?

- Third-party risk manager with the internal stakeholder and internal/external audit team

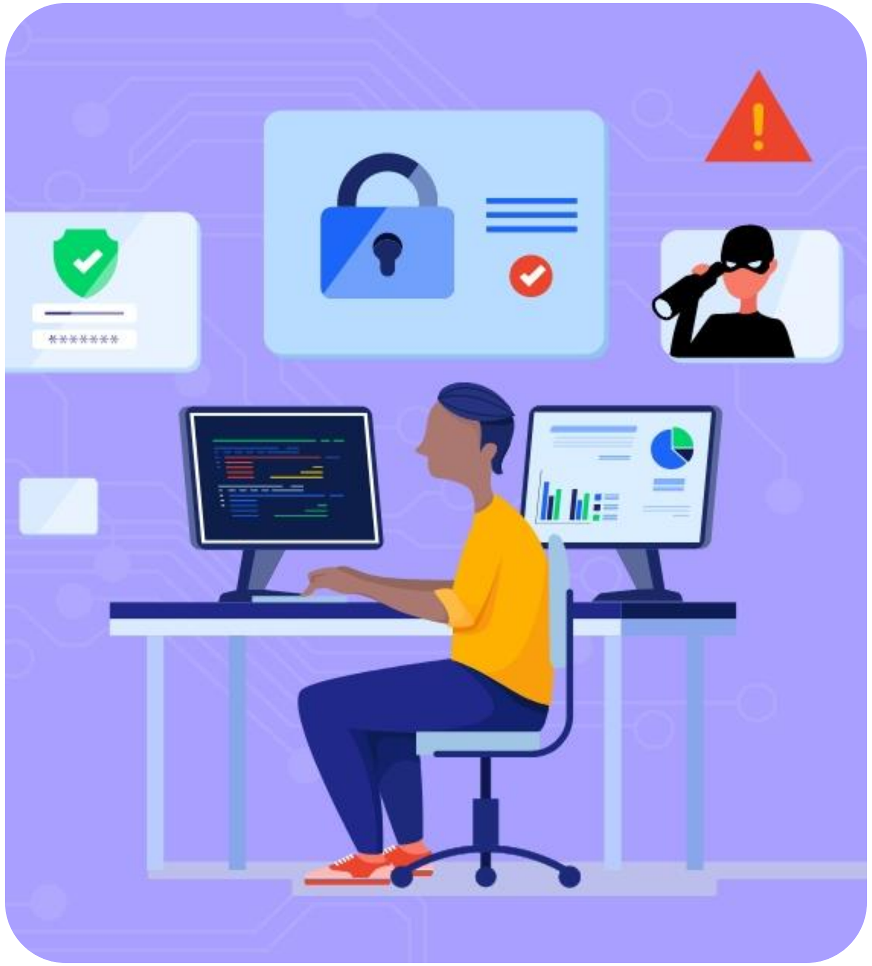
What type of qualifications should that person have?

- Broad background in information security and risk management or an experienced information security professional

Vendor Cybersecurity Posture

IS YOUR VENDOR PREPARED TO PREVENT, DETECT, AND RESPOND TO A CYBERSECURITY ISSUE?

- Identify the cyber threats your vendor could present and take proactive steps to mitigate potential areas of weakness
- Ensure you determine if your vendor (and your organizations and customers' data) will be secure
- Review if your vendor is prepared to prevent, detect, and respond to a cybersecurity issue



What If There Are Red Flags

Replacing a vendor is expensive

- Remaining contract duration
- Removal and implementation efforts
- Business friction (user pushback, user training, etc.)

Do you have compensating controls?

- Limit data retention/type of data in scope
- Periodic data exports

Collaborate with the vendor

- Plan of Action and Milestones (POAM)

Explore alternatives

Mitigating controls

- Insurance, but can you rely on it?

Red Flags to Look Out For

1. Inadequate or lack of testing
2. Lack of security policies and documentation
3. Incidents and breaches in the past
4. Lack of vendor management and security procedures around their vendors
5. Insufficient logical access management/user training
6. Insufficient security protocols/unremediated vulnerabilities

Why It’s Important

Enables risk mitigation by allowing you to:

- Influence the vendor to strengthen their controls
- Supplement their controls with controls of your own
- Make a decision on whether you should stay with the vendor

It’s a hot button issue for all external assessors!

- It’s often required that you demonstrate you’re taking proactive steps to identify and mitigate potential areas of weakness with your vendors
- You’re expected to cover the CIA Information Security Triad

TPRM Has Many Hats – Collaboration Is Key

- You can’t do it all alone, effectively
- Work with legal, procurement, contracting, privacy, infosec, risk, compliance, operations, and product owners

Protection Inside Vendor Contracts

- Accessibility to the vendor’s cyber policies and procedures
- Independent testing requirements
- Frequency and availability of test results
- Recovery times
- Backup responsibilities
- Cyber resilience
- Management of third-party/outsourced business continuity
- Breach/disruption notification

How to Report and Justify

Know Your Vendor Population:

- Which tiers/types are you reviewing?
- Which would you like to also review?
  - Report on a goal towards that
- What is your cadence?
  - Is it appropriate?
  - Are you able to keep up?
- How many vendors have material deficiencies?
  - Costs associated to mitigate or remediate?
    - Additional internal control, moving to a different plan, etc.
    - Resources spent researching, implementing, and monitoring those controls

How Much Will It Cost To:

- Violate your SLA for uptime
- Perform forensic analysis and technical remediation
- Provide credit monitoring for your consumers
- Restore your reputation

Key Takeaways

1. Make sure you know who to review and when
2. Know your own organization's requirements and controls
3. Have the right expectations and understanding
4. Ensure you have the right people doing the review
5. Understand what data you are trying to protect
6. Always include notification and audit language in your contracts
7. Be as proactive as you can, but be ready to be reactive
8. Right-size your program
9. Collaborate with legal, procurement, SMEs, contracting, and product owners

venminder
AN NCONTRACTS COMPANY

venminder

AN NCONTRACTS COMPANY

THANK YOU

Questions & Answers

POST A QUESTION:
www.thirdpartythinktank.com

THIRD PARTY thinktank
Powered by Venminder

EMAIL US:
resources@venminder.com

FOLLOW US:
@venminder

venminder
AN NCONTRACTS COMPANY