IT'S STILL YOUR FAULT

Understanding and managing vendor risk

TINA BODE, CISA, COBIT, CRISC, ITIL (F), LSSGB, PROSCI® CCP

BerryDunn

AGENDA

1 WHAT IS VENDOR MANAGEMENT?

2 RISKS WITH OUTSOURCING

3 COMPONENTS OF A VENDOR MANAGEMENT PROGRAM

WHAT IS VENDOR MANAGEMENT?

Vendor management is a discipline that enables organizations to control costs, drive service excellence and mitigate risks to gain increased value from their vendors throughout the deal life cycle.

This enables organizations to optimally **develop**, **manage** and control vendor contracts, relationships and performance for the efficient delivery of contracted products and services. This can help clients **meet business objectives**, **minimize potential business disruption**, **avoid deal and delivery failure**, and ensure more-sustainable multi-sourcing, while driving the most value from their vendors.

HTTPS://WWW.GARTNER.COM/

VENDORS INTRODUCE NEW RISK

- Significant growth in the use of third-parties as it allows you to focus on core operations
- All vendors pose risk, especially technology vendors
- Cloud Computing and Software as a Service (SaaS) providers – now host, manage, process, and support your data
- You are still responsible for your data and understanding risk

VENDORS INTRODUCE NEW RISK

- Downtime risk – You're without that service
- Perception risk – Your customers may not know it's a third-party service (branded as yours)
- Financial risk – What if they go out of business? How do they impact your bottom line?
- Compliance risk – How do their actions affect you?
- Recovery and backup risk – Will you be able to access the data they host?

A startup dissolved overnight and laid off its 400 employees via email with no warning

In the middle of the night, a startup that had raised $5.5 million dissolved and disappeared. It deleted its Twitter accounts, Facebook pages, and Google+ profile. It changed its website to say it was "pausing operations."

The message on Zirtual's site now.
Zirtual

Saks Fifth Avenue and Lord & Taylor

(Hudson's Bay Company)
Exposed records: 5,000,000
Reported April 2018

A well-known ring of cybercriminals obtained **more than five million credit and debit card numbers from customers** of Saks Fifth Avenue and Lord & Taylor by implanting software into an unsecure point of sale system in-store, siphoning card numbers and information since May of 2017.

Mopping up after your vendor's data breach

Ten states are reacting to the data breach which occurred at AJLA-TS. The cause? The human, an application misconfiguration error.

Applebee's

Exposed records: Unknown
Reported January 2018

Malware was discovered on point of sales systems at more than 160 Applebee's restaurants, exposing credit card information collected from unknowing diners.

Our CEO, Fred Kneip, weighed in with Threatpoast, stating, "We're seeing more of these types of breaches happening... it's an industry wide problem as more retailers look to an ecosystem of providers to bring in third party systems like point of sale and inventory management solutions. As of today a lot of stores are playing catch up with security, and it can take months or years to realize that compromises have happened on third party systems."

BestBuy, Sears, Kmart, Delta

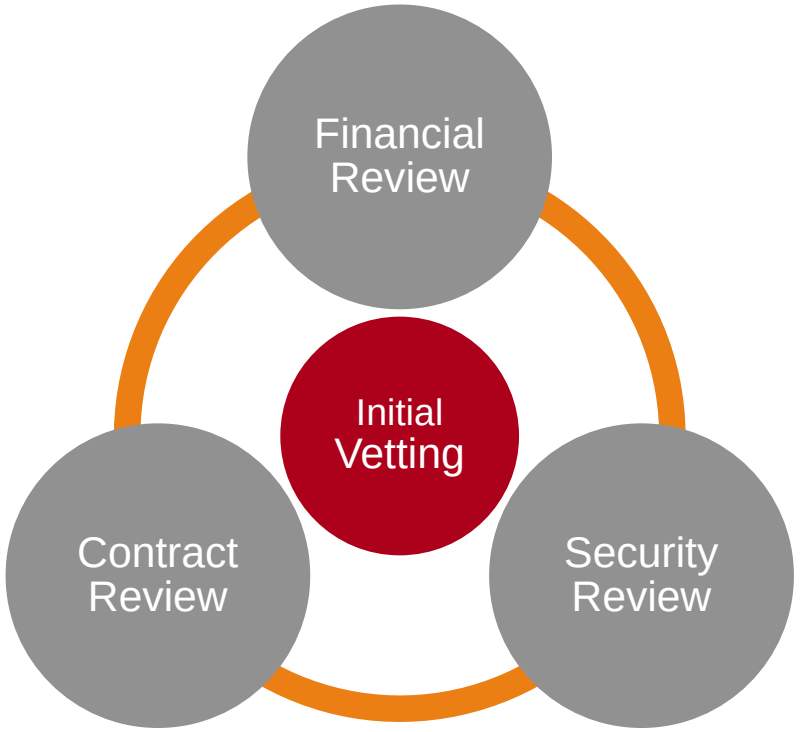
Exposed records: unknown
Reported April & May 2018

Electronics, home goods, mom jeans, and air travel – these companies don't have much in common – except for a big weak link. [24]7.ai, a chat and customer services vendor for many brand names, was hacked via malware, compromising credit card information, addresses, CVV numbers, card expiration dates, and other personal data across multiple customer groups. **Hundreds of thousands of customers were affected per company hacked.**

DOES YOUR ORGANIZATION HAVE A VENDOR MANAGEMENT PROGRAM?

WHO IS RESPONSIBLE FOR VENDOR MANAGEMENT?

- Vendor Management is an organizational-wide effort
- “Owners” should be assigned to each vendor
- There should be a centralized vendor management coordinator/manager
- The Board should be kept apprised of both risk and of the vendor management program
- Vendor Management happens twice: Initial Vetting and Ongoing



Onboarding allows you the opportunity to communicate and set expectations. If it's not in the contract, it won't be done.

- May need to use subject matter experts
- Concerns should be addressed before moving forward
- Identify the potential risk of the vendor

CRITICAL OR HIGH RISK

- Vendor provides a critical service (you couldn't operate without them)
- Vendor has direct access to facilities or systems
- Vendor hosts confidential or personal information

MODERATE RISK

- Vendor provides an important service (you could operate without them, but would cause stress)
- Vendor has limited access to facilities or systems
- Vendor does not host or have access to confidential or PII information

LOW RISK

- Vendor provides a non-critical service (you could operate without them with minimal impact)
- Vendor has no access to facilities or systems
- Vendor has no access to data

High Effort ⟷ **Limited Effort**

Vendor Management begins when a contract is signed.

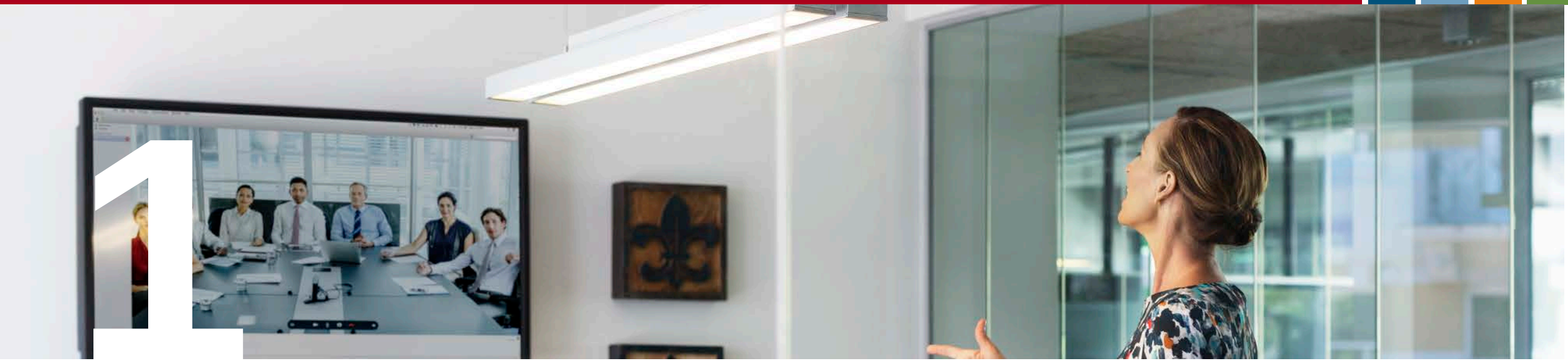
It is NOT a one-time process.
It is on-going.

1 IDENTIFY — Work with all departments in the organization and develop an inventory of third-parties used

2 RISK RANK — Identify the risk and impact of each vendor to your organization

3 MONITOR — Conduct annual due diligence based on the level of risk

4 REPORT — Report on results of monitoring to the Board annually



IDENTIFY

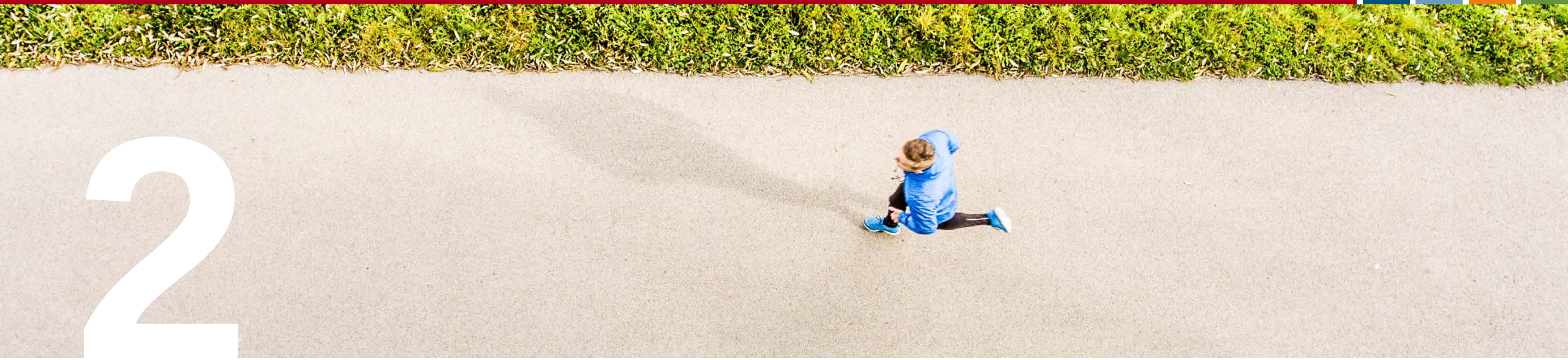
Create a Vendor Inventory:

- Vendor's name
- Contact information of primary contact
- Services/goods provided
- Your organization's vendor "owner"
- Department the vendor contracts with
- Contract terms (length of contract, pricing)
- Any special requirements

If an IT vendor or provider:

- Name and version of software or hardware used/purchased
- If product is hosted in the cloud
- If the product has any customization for you
- Indicate if there is any support provided with contract
- Are upgrades included? How often?

ONE PERSON SHOULD BE ASSIGNED RESPONSIBILITY FOR MAINTAINING AND UPDATING THE VENDOR INVENTORY



2

RISK RANK

- Risk ranking vendors allows you to establish an understanding of the vendor’s importance in your organization.
- Risk rankings also establish a standard and consistent expectation for due diligence procedures.

CRITICAL OR HIGH RISK

- Vendor provides a critical service (you couldn't operate without them)
- Vendor has direct access to facilities or systems
- Vendor hosts confidential or personal information

MODERATE RISK

- Vendor provides an important service (you could operate without them, but would cause stress)
- Vendor has limited access to facilities or systems
- Vendor does not host or have access to confidential or PII information

LOW RISK

- Vendor provides a non-critical service (you could operate without them with minimal impact)
- Vendor has no access to facilities or systems
- Vendor has no access to data

High Effort ⟵ ⟶ **Limited Effort**

3

MONITOR

Critical/High Risk Vendor: Full vetting upon hire. Annual due diligence review.

Moderate Risk Vendor: Full vetting upon hire. Bi-annual due diligence review.

Low Risk Vendor: Some vetting upon hire. Due diligence review upon contract renewal.

CRITICAL VENDOR EXAMPLE

INITIAL VETTING

- Have legal or contracting review contract language
- Are Service Level Agreements in Place? Do they meet your expectations?
- Insurance review – get certificates
- IT Questionnaire/review or System and Organization Controls (SOC) audit report review
- Financial Statement and ratio review
- Reference checks
- Background check
- Consider a “Right to Audit” clause in your contracts

ANNUAL REVIEW

- IT Questionnaire/review or SOC audit report review
- Financial review
- Insurance review
- User access review

A NOTE ON SOC EXAMS

- SOC Exams are audits done conducted by Certified Public Accountants (CPAs)
- Report on Internal Controls of a service organization
- Type 1 – as of a specific date
- Type 2 – effectiveness throughout a period of time
- Opinion – qualified (bad) or unqualified (good)
- Your financial auditors may ask for these as well (part of their risk assessment)
- Should receive an annual report
- Considered the best way to report to customers

SOC 1 EXAMINATIONS

- SOC 1 exams report on internal controls over financial reporting.
- Vendors who process transaction for you, or on your behalf

SOC 2 EXAMINATIONS

- SOC 2 exams report on the Trust Service Criteria, mapped to the COSO Principles
- Focus on Security, Availability, Processing Integrity, Confidentiality, and Privacy
- Vendors such as SaaS, managed services providers, data centers

A NOTE ON SOC EXAMS

USER CONTROL CONSIDERATIONS

- Controls that a service organization includes in SOC report
- These are controls that you should have in place at your organization to complete the control cycle
- You should test these and document those tests and evidence

SUBSERVICE USER CONTROLS

- AICPA requires service organizations to document and describe any third-parties they may use that impact you
- Declares the controls those third-parties are responsible for
- Allows you to understand who is responsible for what
- You may determine that you need to conduct due diligence procedures on the sub-service organization because it significantly impacts your organization

IF A SOC EXAM IS NOT AVAILABLE

- Request the vendor complete an IT Questionnaire
- Many third-party organizations offer useable tools – EDUCAUSE tool, ISACA, NIST, SANS Top 20
- May also request supporting documents – “please send me your IT Security Policy”

FINANCIAL REVIEW

- Request financial statements and compare results year over year
- Review footnotes that describe any big events
- Going concern risk
- Key accounting ratios (liquidity, profitability, asset turnover, financial leverage)

ARE YOU DOING ANY OF THIS CURRENTLY?

4

REPORT

EACH VENDOR SHOULD HAVE A FILE OR USE SOFTWARE TO TRACK:

- Contract
- SLA
- Risk assessment
- Documentation requested/reviewed
- Any relevant audit reports (SOC, financial, etc.)
- Memos, SOC review checklists, ratios
- Documented concerns or issues

REPORT ON:

- Results of review for high-risk vendors
- Concerns from audit reports (bad opinion)
- Particular findings that may impact your organization
- Follow-up activities with the vendor
- Any concerns should be discussed/decided by the Board

SHIFTING BOARD RESPONSIBILITIES

- 2018 SEC Requirements
    - Disclosure of cybersecurity risks and incidents
    - Oversight of cybersecurity and risk
- Cybersecurity and vendor management often go together
- Changes may require additional cybersecurity expertise on Boards
- Likely to become requirements elsewhere (ex: GLBA for higher education)

QUESTIONS?

TINA BODE
Manager
tbode@berrydunn.com
207.541.2253