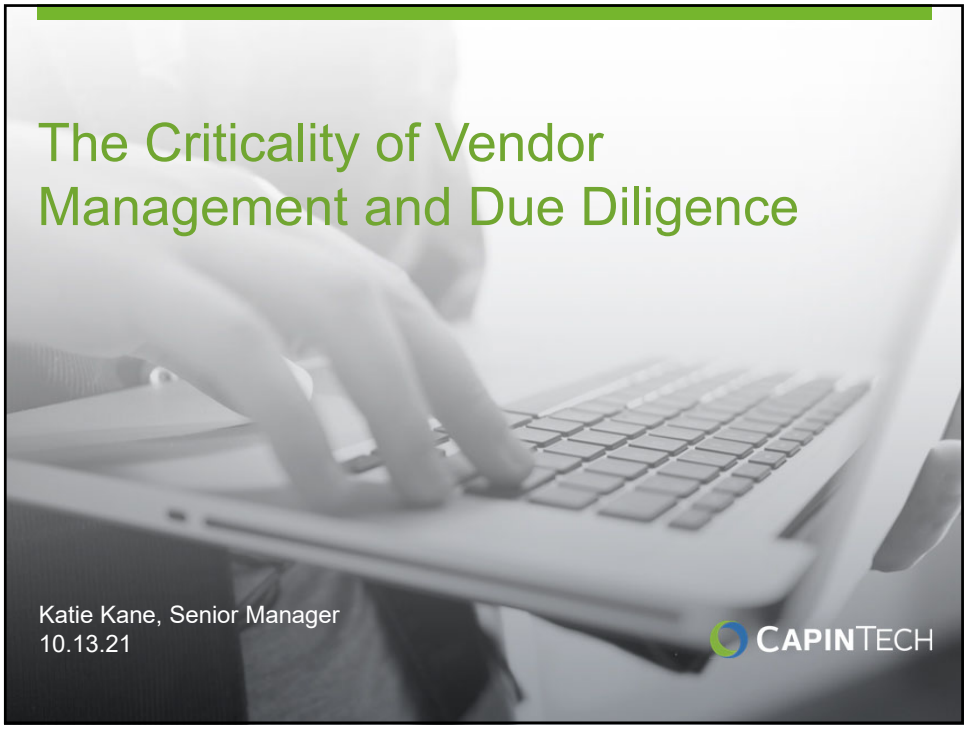
The Criticality of Vendor Management and Due Diligence



Katie Kane, Senior Manager
10.13.21

CAPINTECH

1

The content of this presentation, whether communicated in writing or verbally by partners, employees, or representatives of Capin Crouse LLP, is provided solely for educational purposes. This presentation is not intended to provide legal, accounting, investment, or fiduciary advice. Please contact your attorney, accountant, or other professional advisor to discuss the application of this material to your particular facts and circumstances.

2

Polling Question 1

Do you want CPE?

3

Why Is Vendor Management Important?

CAPINTECH

4

Why Is Vendor Management Important?

- Location of data
- Ensure appropriate vendor security controls
- Mitigation of risks
- Breaches related to vendor security deficiencies
- Monitoring of services

zoom April 2020

- Video conferencing service
- Credential-stuffing attack
- Over 500,000 accounts were found for sale on the dark web and hacker forums
  - Email addresses, passwords, personal meeting URLs and host keys

GoDaddy

May 2020

- Web hosting site
- Unauthorized third party granted access to login credentials
  - Usernames and passwords exposed
  - Approximately 28,000 customers impacted

Cognizant

April 2020

- IT managed services company
- Ransomware attack resulted in compromise of names, SSNs, TINs, financial account information, DL numbers, and passport information
- Some customers experienced service disruptions
- Impacted work-from-home setups and provisioning of laptops

Vertafore — November 2020

- Insurance software firm
- Data breach resulting in compromise of personal data and DL numbers of over 27 million Texas residents
- Data stored in unsecured external storage service
  - Human error
  - Led to data being accessed without authorization

9

solarwinds — December 2020

- IT management solutions provider
- Entered a backdoor in the SolarWinds software, causing SolarWinds Orion business software updates to distribute malware
- SolarWinds told customers to upgrade immediately
- Attacks thought to have begun as far back as October 2019, when the breach of SolarWinds occurred

10

UBIQUITI NETWORKS

January 2021

- Network devices and IoT vendor
- Unauthorized access to database through third-party cloud provider
- Reported that an undisclosed number of records were affected (whistleblower indicated otherwise)
- Not certain that user data was exposed
  - Potentially names, email addresses, hashed/salted passwords, addresses, phone numbers

11

Exchange

March 2021

- Widely utilized email platform
- Four flaws granted access to 30k+ U.S.-based organizations
- Range from small businesses to city governments
- Total remote control of affected systems

12

April 2021

- Credit reporting agency
- Breach caused by an unsecured application programming interface (API)
- Exposed names, DOBs, and mailing addresses of millions of Americans

13

July 2021

- IT solutions developer
- Supply chain ransomware attack
- Leveraged vulnerability in VSA software and pushed out an automated, fake, malicious update (Kaseya VSA Agent Hot-fix)
- Impacted managed service providers (MSPs)… and their customers (small/midsize)
- SaaS customers not impacted

14

SPRINGHILL MEDICAL CENTER
Treating You Like Family

July 2019

- Mobile, AL hospital
- Ransomware attack led to the compromise of numerous electronic systems, including fetal monitoring systems
- Resulted in the medical staff not having timely notification of fetal monitoring results

15

How to Implement a Successful Vendor Management Program

CAPINTECH

16

Polling Question 2

Have you implemented a vendor management program in your organization?

17

What Does Implementation Look Like?

- Develop an overarching strategy
- Perform initial due diligence
- Perform risk assessment of existing vendors
- Develop ongoing oversight
- Ensure appropriate management oversight

18

Initial Due Diligence

CAPINTECH

19

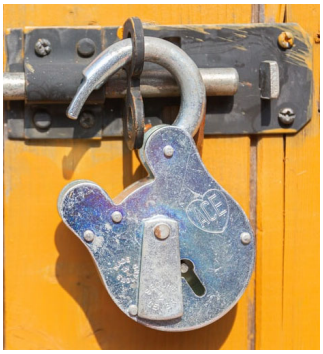
Initial Due Diligence

- Perform risk assessment
- Understand how relationship fits into strategic plan
- Perform cost-benefit analysis
- Perform review of critical areas
- Review contract
- Outline contingency plans for transition

20

Risk Assessment

- Human element and staff exposure to sensitive data
- User access controls
- Brute force attacks
- Remote access
- Data location and security
- Identify mitigating controls



Risk Assessment

- Some considerations for cloud services providers:
  - Commingling of data
  - Ownership of data
  - Deconversioning (can you get your data?)

Review of Critical Areas

- Financial stability
- Security controls (e.g., policies, security audit reports, vulnerability assessments)
- Business continuity, disaster recovery, incident response, pandemic planning and testing
- Cyber insurance

Review of Critical Areas

- Cyber threat prevention
- Foreign data considerations
- Vendor management
- Compliance and licensing information
- Complaint resolution

Polling Question 3

Do you consider the third parties of your vendors when vetting new vendors or performing ongoing reviews of existing vendors?

Contract Review and Negotiation

- Breach notification
- Information security
- Confidentiality
- Services provided
- Language to mitigate risk
  - If they refuse it, what is the risk to you?

Management Oversight and Approval

- Prior to execution:
  - Presentation of risk assessment
  - Presentation of review or critical areas
  - Obtain management approval
- Contract execution
- Implementation

27

Existing Vendor Relationships

CAPINTECH

28

Existing Vendor Relationships

- Risk-rate each relationship
- Define frequency and content of reviews
- Request documentation from vendors
- Review and assess
- Summarize and report to management

Who to Include?

- Perform an inventory of all vendors utilized
  - Survey different departmental users
  - Review listing of vendor contracts
  - Review listing of vendors from Accounts Payable
  - Review systems included in annual user access review

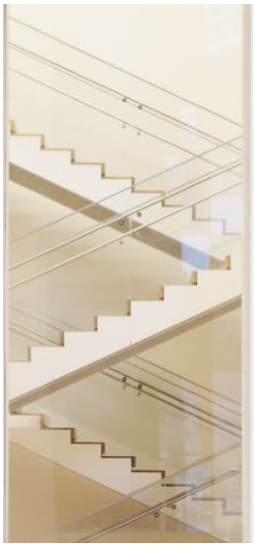
Who to Include?

- Hosted applications (e.g., accounting, customer/donor database systems)
- Website hosting
- Online backup host
- Hosted email and email encryption
- Network support or MSP
- Foreign-based vendors

31

Define Risk-Rating Criteria

- Develop multiple tiers
  - Critical vs. significant vs. non-critical
- Consider several factors
  - Criticality of the relationship to operations
  - Sensitivity of the data hosted, managed, or accessed



32

Questions to Determine Criticality

- What would happen if the vendor stopped providing services unexpectedly?
- What level of access does the vendor have, and how sensitive is the information?
- Where is the data hosted — in the United States or in a foreign country?

Questions to Determine Criticality

- Does the vendor have any access to the network or physical locations containing sensitive information?
- Is the service provided complex in nature?
- Are there heightened risks with the nature of the service provided?

When to Review

- Critical vendors – annually
- Others – based on criticality and risk
  - Ex: significant – every other year
  - Ex: non-critical – every 3 years

35

What to Review?

- Critical vendors should have the most extensive review
- Review of significant vendors and non-critical vendors will depend on the level of service provided and the risk level presented to the organization

36

Areas to Review

- Financial stability
- Security controls (e.g., policies, security audit reports, vulnerability assessments)
- Business continuity, disaster recovery, incident response, pandemic planning and testing
- Cyber insurance

37

Areas to Review

- Cyber threat prevention
- Foreign data considerations
- Vendor management
- Compliance and licensing information
- Complaint resolution

38

Review and Assess

- Review and assess documentation obtained
- Ensure controls and practices are in line with established organization standards
- If documentation not provided, determine if risk levels are within the organization's risk appetite

39

Summarize and Report to Management

- Summarize review and identify areas of weakness
- Include details of information not provided
- Recommendation for continuation, modification, monitoring, termination, etc.
- Present to board or relevant management

40

Polling Question 4

After what we discussed today, do you feel like you have a good handle on vendor management and due diligence?

41

Join Us for Our Next Cyber Series Webcast

Data Management: Developing a Strategy for Success
Wednesday, November 10
1:00 – 2:00 p.m. EST

Learn more at capincrouse.com

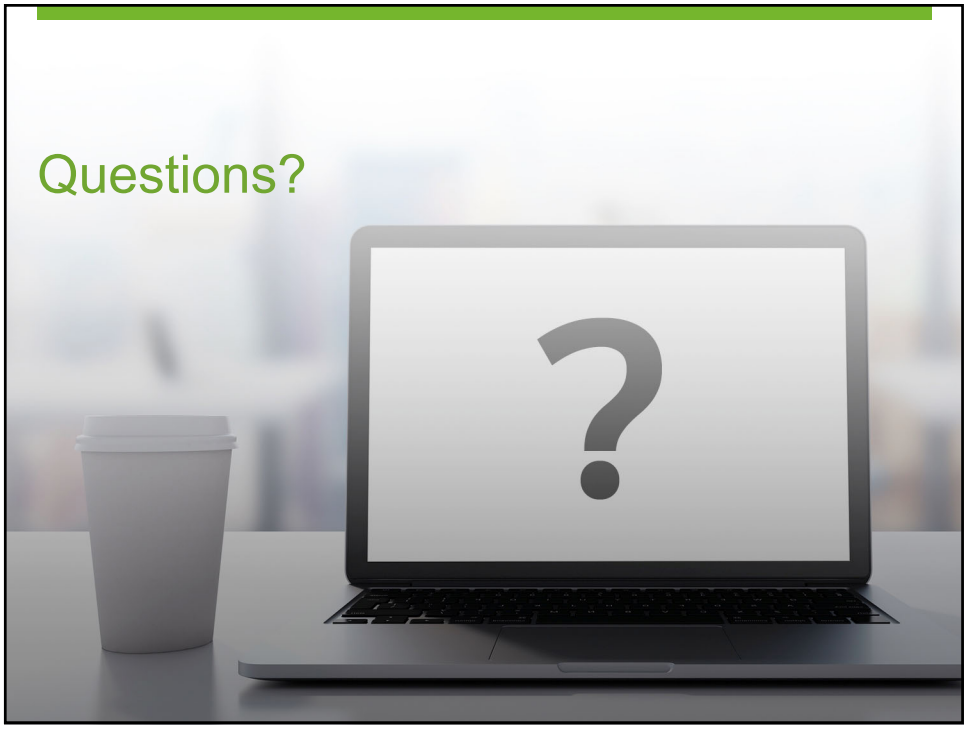
42

You Could Win a Free CapinTech Cyber Checkup!

- Receive one entry for each 2021 CapinTech Cyber Series webcast you:
  - Attend live, or
  - Watch the recording of within one week of the webcast date
- Winner announced in December

43

Questions?



44

Thanks!

Katie Kane, CISSP, CISA, CISM
Senior Manager

kkane@capincrouse.com

505.50.CAPIN ext. 2007

CAPINTECH