

WHOSE BREACH IS IT ANYWAY?



Kelly Miller
Managing Director
Cybersecurity & Data Privacy Communications
FTI Consulting



Fran Faircloth
Partner
Ropes & Gray

Quick Warm-Up



How many third party breaches can we name?

Why Third-Party Breaches Are So Complicated



You didn't cause the breach, but you're in the headlines



Vendor relationships are legal and operational tangles



Disclosure duties vs. PR damage rarely align



Examples: MOVEit, Drift/Salesloft, AI chat tools

Risk Roulette

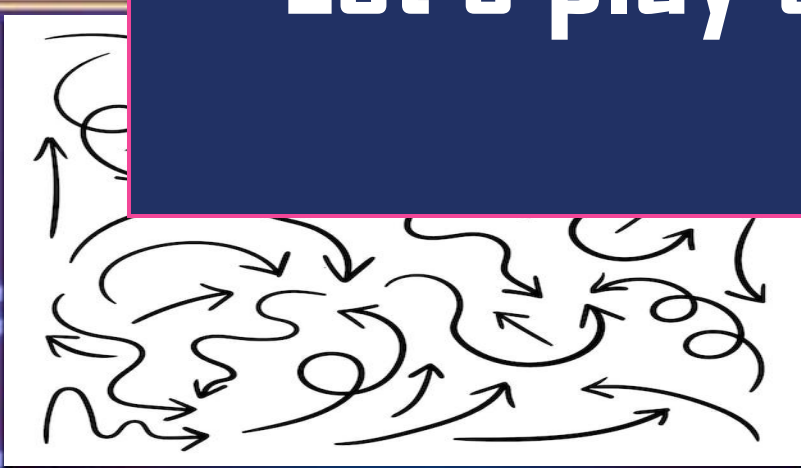


GAME
START

Media Mad Libs



Let's play some games!



Clause or Chaos



Is it Material?

Risk Roulette



Risk Roulette



Risk Roulette #1: The Data Transfer Debacle

Software Provider: FileFrigate

Vendor: DataNest Solutions

End Client: MetroCity Transit

- FileFrigate is a cloud-based secure file transfer tool used by thousands of vendors to shuttle sensitive data like employee records and benefits info. One of its longtime customers, **DataNest Solutions**, a third-party data processor that handles retirement and benefits administration for public-sector employers, was quietly using FileFrigate behind the scenes.
- When the ransomware group **ZIPn0Mercy** exploited a zero-day vulnerability in FileFrigate, they accessed large volumes of data held by DataNest, including names, SSNs, and benefits info for government employees at **MetroCity Transit**, a regional transit authority.

Time to vote!

Risk Roulette



Risk Roulette #2: The Chatbot Conundrum

Software Provider: ConvoCraft
Vendor: AutoReach
End Client: Glowbeam Skincare

- ConvoCraft is an AI-powered customer engagement platform: think website chatbots, follow-up automation, and sales team integration. One of its partners, **AutoReach**, builds customer acquisition tools for e-commerce brands using ConvoCraft's APIs to sync real-time user data, chats, and lead profiles.
- Last week, a misconfigured update in ConvoCraft's backend (exploited by the hacktivist group **ChatLeakerz**) exposed chat logs, contact info, and sales intel from multiple brands *without* AutoReach or its clients being immediately notified.
- One of those clients, **Glowbeam Skincare**, had recently launched a buzzy new product and had dozens of celebrity customers and influencers using the chatbot. Within 48 hours, screenshots of sensitive customer exchanges (including refund requests and private contact details) hit Reddit and were picked up by beauty bloggers and gossip accounts.

Time to vote!

Key Takeaway

Legal ≠ Narrative Ownership

You don't need to be breached to be blamed

Media **MAD LIBS**®

How to Avoid Communications from Sounding Like a Mad Lib

- Legalese vs Fluff
- Unwinding complicated vendor relationships
- Templates are not your friend
- Think of all your audiences

Cyber Crisis Mad Libs

Dear _____, we regret to inform you that our company has recently experienced a
NOUN
_____ cyberattack. We are working tirelessly to resolve this issue and protect your
ADJECTIVE
_____. Our team of experts, led by our _____, is investigating the breach and
NOUN PLURAL THIRD PARTY
implementing enhanced security measures to prevent future _____. We appreciate your
NOUN
patience and understanding during this _____ time. Rest assured, we are committed to
ADJECTIVE
maintaining the safety and integrity of your _____ as we navigate through this crisis
STAKEHOLDER
together.

Media **MAD** **LIBS**® #1

“Mochrie Hospital detected unauthorized access to our patient communication system, ColinConnect .

We activated our incident response protocols, eliminated the chance of any sustained access to customer data, and fully mitigated the issue within 50 minutes. We notified law enforcement.

The personal information in question did not include sensitive health information. We encourage customers to remain vigilant against potential phishing attempts and to avoid clicking on suspicious links.”

Thought Starters:

1. Which words open legal risk?
2. What assumptions are being made about risk to individuals?
3. What’s missing for the reader to truly assess the impact?

Media **MAD** **LIBS**® #2

“Our vendor, PointlessPay Systems, recently informed us of a cybersecurity issue that may have affected certain employee data. Please know that this incident occurred within PointlessPay Systems’ environment - not ours! Please direct all questions to them.”

Thought Starters:

1. Does distancing yourself from a vendor help in this situation?
2. How might this language land with affected individuals?

Media **MAD** **LIBS**® **#3**

“We recently became aware that an unauthorized third party accessed a limited amount of customer data through one of our service providers, DrewDeductions. The issue has been contained. Out of an abundance of caution, we are resetting customer passwords and enhancing monitoring. There is currently no evidence that the information was misused, and we believe the risk to customers is low. We do not anticipate further updates on this matter.”

Thought Starters:

1. What should this organization know before they use phrases like “limited amount of customer data” or “risk to customers is low?”
2. What happens if new facts emerge tomorrow?
3. How could you reframe this to maintain credibility without oversharing?

Media **MAD** **LIBS**® #4

“At YesAnd AI, trust and our customers' data is our top priority. We recently learned of a potential cybersecurity incident involving one of our valued third-party partners, ZipZap CRM. While the issue did not originate within our systems, we are actively collaborating with ZipZap CRM to ensure the highest standards of data stewardship are maintained. We remain committed to transparency and excellence as we continue delivering unparalleled service to our customers.”

Thought Starters:

1. What phrases scream “PR spin” or try to over-reassure without substance?
2. Where’s the concrete detail?
3. How many buzzwords can one paragraph hold?

Key Takeaway

Say it Straight but Smart



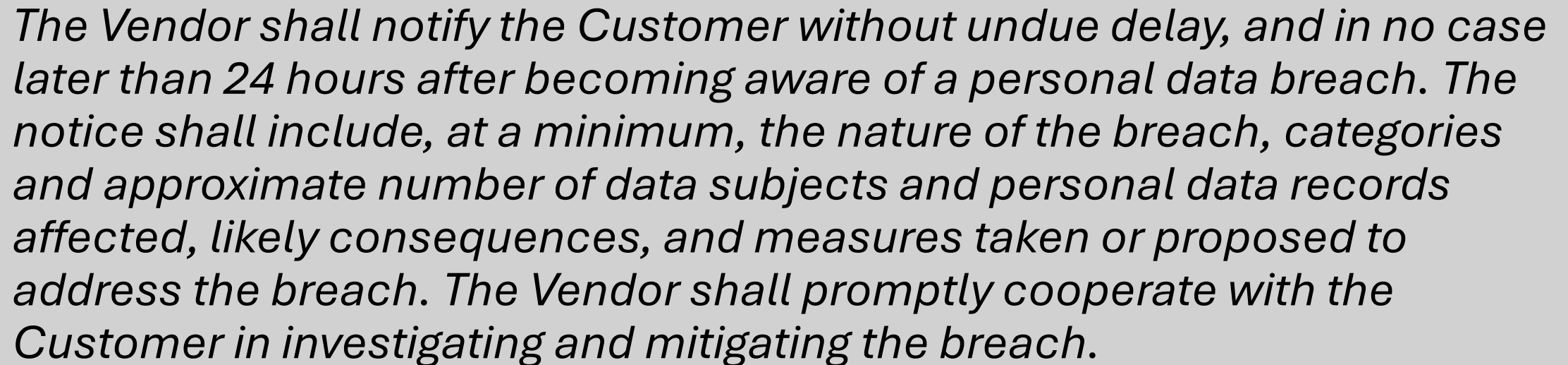
Clause

or



CHAOS

Is this clause solid or sketchy?



The Vendor shall notify the Customer without undue delay, and in no case later than 24 hours after becoming aware of a personal data breach. The notice shall include, at a minimum, the nature of the breach, categories and approximate number of data subjects and personal data records affected, likely consequences, and measures taken or proposed to address the breach. The Vendor shall promptly cooperate with the Customer in investigating and mitigating the breach.



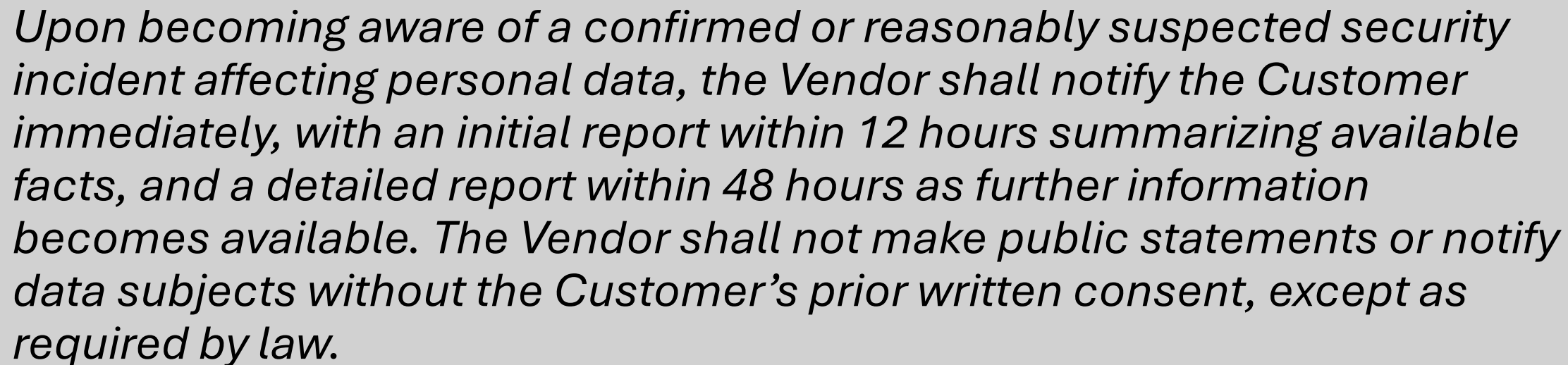
Clause

or



CHAOS

Is this clause solid or sketchy?



Upon becoming aware of a confirmed or reasonably suspected security incident affecting personal data, the Vendor shall notify the Customer immediately, with an initial report within 12 hours summarizing available facts, and a detailed report within 48 hours as further information becomes available. The Vendor shall not make public statements or notify data subjects without the Customer's prior written consent, except as required by law.



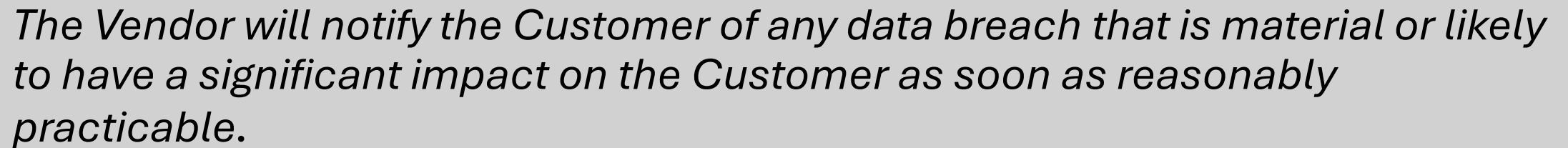
Clause

or



CHAOS

Is this clause solid or sketchy?



The Vendor will notify the Customer of any data breach that is material or likely to have a significant impact on the Customer as soon as reasonably practicable.



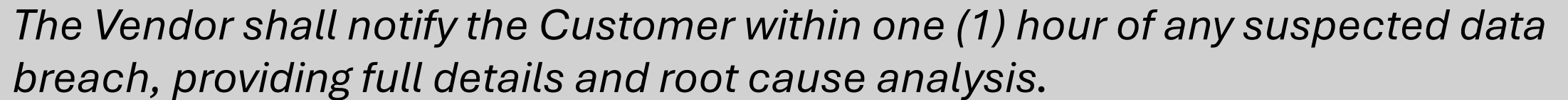
Clause

or



CHAOS

Is this clause solid or sketchy?



The Vendor shall notify the Customer within one (1) hour of any suspected data breach, providing full details and root cause analysis.

Key Takeaway

Contracts Need Real-World Thinking

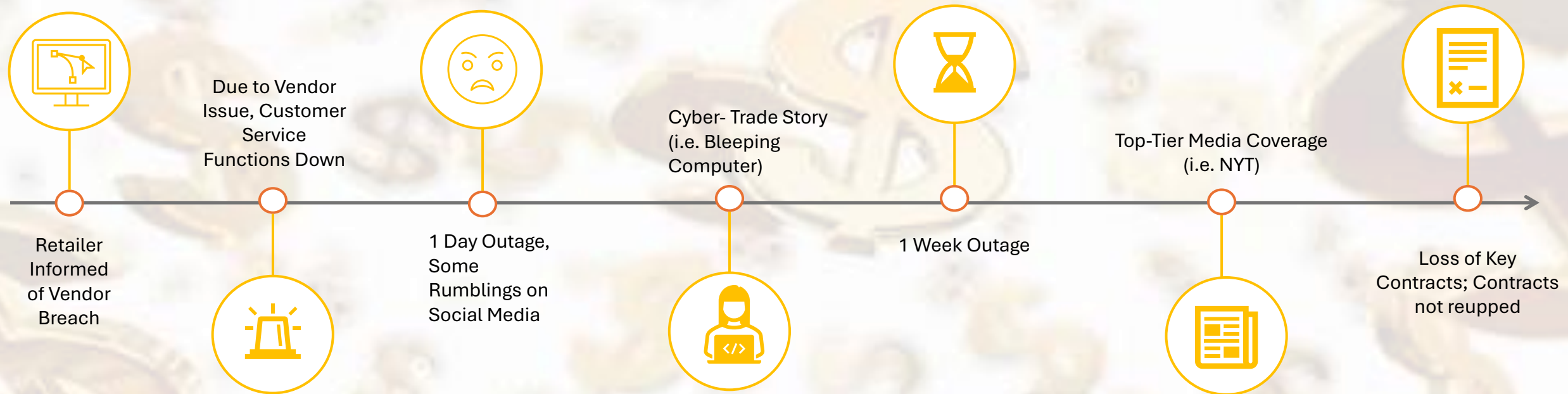
- Translate legal timelines into ops & comms workflows
- Push for breach response clauses that define roles & timing
- Avoid “notify promptly” vagueness

Is it Material?



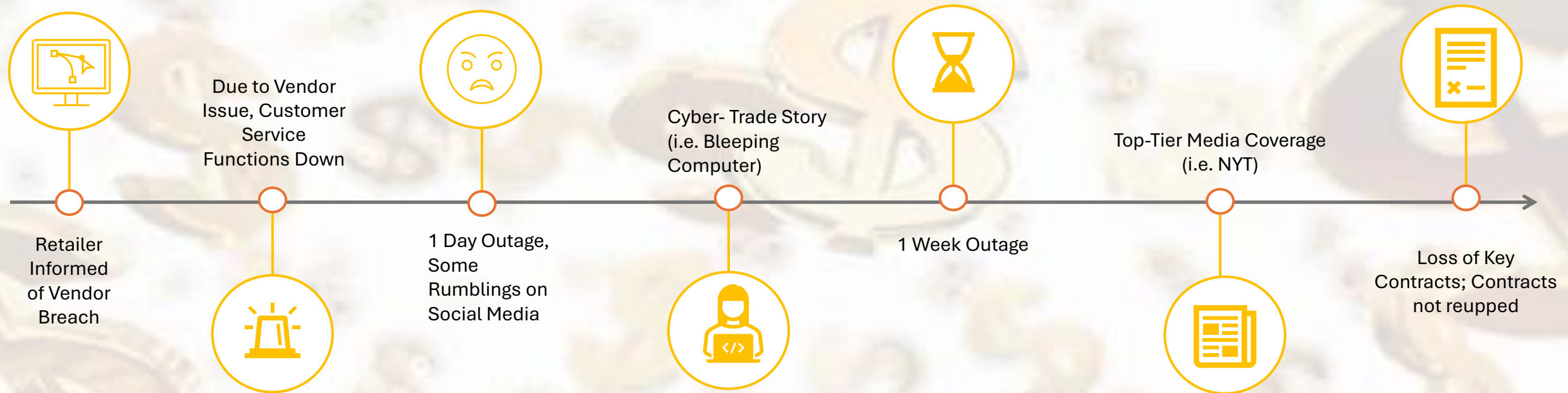
Retailer Faces Customer Support Vendor Outage

An online retailer is informed of an outage by the AI-powered chat bot that handles its primary customer service functions. Any customer trying to make a return runs into long wait-times as the team returns to manual processes.



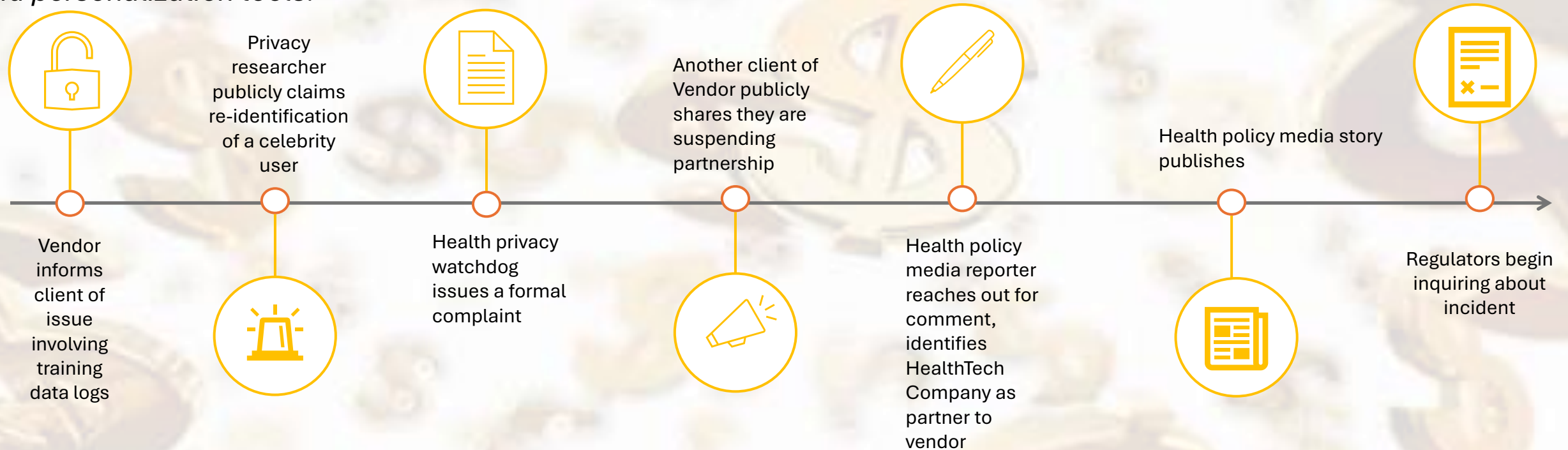
Aviation Distributor Faces Logistics Vendor Outage

An aviation supplier is informed by the vendor they rely on for logistics support is completely down. Without this software, they can only fulfil 10% of their usual shipments.



HealthTech Startup Faces Analytics Vendor Incident


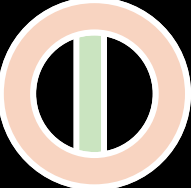

A HealthTech company is informed that its AI analytics vendor (used to process anonymized patient behavior and engagement data) may have experienced a data incident. The data powers product features, reporting to pharma clients, and personalization tools.



Key Takeaway

Legal Materiality \neq Business Crisis

Final Takeaways

- 
- 
- 
1. You don't have to be breached to be blamed
 2. Risk Domains (legal, ops, comms) are rarely blamed
 3. Prep now: Contracts, escalation paths, messaging

Questions?

