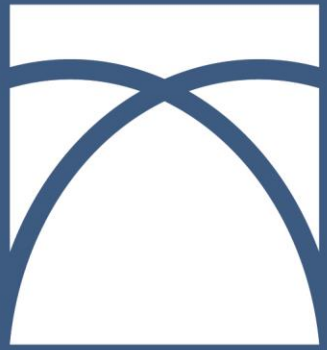


IAPP GLOBAL PRIVACY SUMMIT 2017

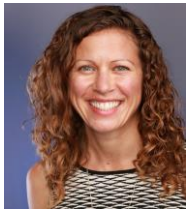
April 19, 2017

KEYS TO MANAGING PRIVACY AND SECURITY RISK IN B2B/VENDOR CONTRACTS

April 19, 2017

#GPS17

SPEAKERS



Jeanne M. Sheahan
Senior Corporate Counsel, Privacy & Regulatory
Groupon, Inc.

Cara Dearman
Assistant General Counsel, eCommerce, Member Programs and Privacy
Sears Holdings Corporation

Paul Otto, Moderator
Senior Associate
Hogan Lovells US LLP

The views presented in these slides and expressed during this panel are the personal views of the panelists and should not be attributed to their employers.

#GPS17

INTRODUCTION

- Many factors affect privacy and security negotiations with vendors:
  - Sophistication of counterparty
  - Sensitivity of the vendor's service
  - Relative bargaining power
- These considerations are relevant whenever vendors have access to:
  - Confidential, proprietary, or otherwise sensitive business information
  - Regulated information (PII, PCI, PHI, GDPR)

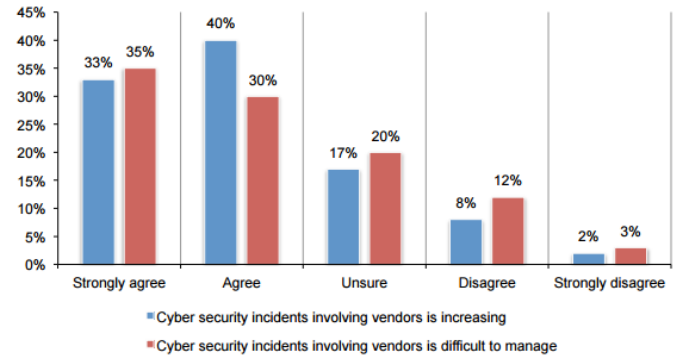
CASE STUDY — TARGET

- Bottom line: data security depends on the weakest link in the chain
- Vendor (refrigeration, heating, and air conditioning subcontractor) suffered its own breach; thieves stole VPN credentials the vendor used to connect to Target's network
- Consequences: 40M cards compromised, PII of up to 110M people exposed, ~$250M in expenses (or ~$160M after insurance)

SPECIFIC RISKS

- Breaches
  - Breach at vendor
  - Breach at vendor's subcontractor or agent
  - Breach at your company caused by your vendor or its agent
- Reputational Risk / Customer Trust

Figure 3. Cybersecurity incidents are increasing and difficult to manage



Source: Ponemon Institute Research Report, "Data Risk in the Third-Party Ecosystem" (Apr. 2016)

SPECIFIC RISKS

- Regulatory Exposure
  - Privacy Shield
    - Contract must limit processing to the term of the data subject's consent and hold third parties to the same standards promised by the certified organization
  - GDPR (effective May 2018)
    - 72 hour breach notification requirement to DPAs
  - U.S. Federal Trade Commission
    - Section 5 Unfairness/Deception Authority
  - U.S. state laws and regulations
    - E.g., Massachusetts data security regulations

COSTS

- Breaches / Cyber Attacks
  - Notification expenses
  - Outside legal, forensics, and PR
  - Investigations and litigation costs
  - Loss of reputation and trust
- Regulatory Exposure
  - GDPR / Privacy Shield liability
  - FTC / State AG settlements
  - PCI DSS

WHAT CAN BE DONE?

YOUR OWN DUE DILIGENCE

Goal: develop a nuanced understanding of vendor-specific risks to address via the contract

- NDAs
- Sources: Google / Twitter / LinkedIn / State reports
  - Breaches? Suspected security incidents? Fraud?
  - FTC or other regulatory enforcement?
- Wikipedia / Investor Sites
  - Company age? History? Capitalization? Sophistication?

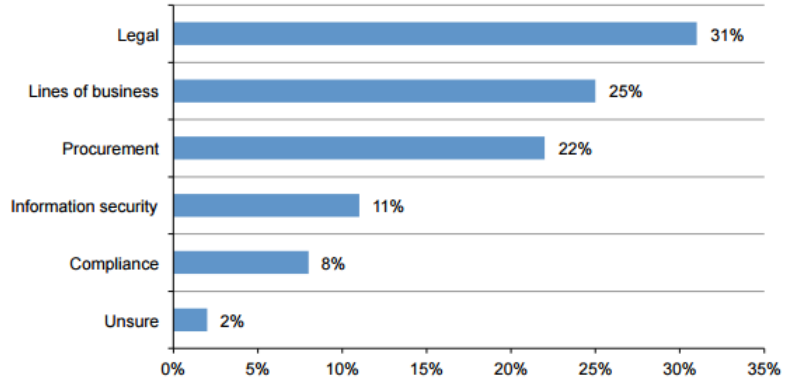
DUE DILIGENCE QUESTIONS

- Location, Location, Location
  - Where… is PII processed? are servers located?
  - What EU data transfer mechanisms do you use?
- Regulatory and Certifications
  - What sectoral / country-specific laws apply? How do you comply?
  - Which orgs do you self-certify to? Any certifications?
- Insurance
  - What cyber coverage do you have?
  - Is your data covered / excluded?

DUE DILIGENCE QUESTIONS

- Security Diligence Tips
  - Use questionnaires
  - Ask questions relevant to your company
  - Involve your InfoSec folks

Figure 7. Which department or function is responsible for ensuring that appropriate privacy and security language is included in all vendor contracts?



Source: Ponemon Institute Research Report, "Data Risk in the Third-Party Ecosystem" (Apr. 2016)

DUE DILIGENCE QUESTIONS

- Security Questions
  - Privacy and security measures in place
  - Confirm formal policies
  - Disaster recovery and business continuity
  - Compliance monitoring and reporting
  - Incident reporting (any prior breaches?)
  - Security measures for data in transit / at rest
  - Role-based access controls

CONTRACT PROVISIONS — DEFINITIONS

- "Security Incident"
  - Actual or suspected disclosure, loss, or unauthorized access of confidential data, including personal data caused by vendor or agents and their employees
- "Personnel" — screen & train personnel to be hired
- "Subcontractors"
  - Must abide by same data security provisions
  - Vendor liable for third party breach

CONTRACT PROVISIONS — REPS & WARRANTIES

- No Defects
  - Products / software free from viruses, defects, malware, etc. that may affect performance of any product
- Compliance With Laws
  - Vendor has obtained appropriate notices, consents, & privacy policy complies with applicable laws
  - Each party agrees to comply with international data transfer regulations
  - Vendor guarantees that data is collected, accessed, used, stored, processed, disposed of, and disclosed in compliance with applicable laws, self regulatory schemes and contract

CONTRACT PROVISIONS — REPS & WARRANTIES

- Security Safeguards
  - Administrative, physical and technical safeguards; at least industry standard
- Material Change Notices
  - Notification if material change to architecture, privacy, or security measures
- Training
  - Stringent hiring and training requirements (background checks)
- Prohibition on Commingling Data
  - Separate your company's data from other companies' data

CONTRACT PROVISIONS — REPS & WARRANTIES

- Physical Security
  - Deploy physical security systems
- Use Limitations
  - Restrictions on onward data transfers
- Duty of Care
  - Confidentiality; use for purposes of agreement (restrictions on use, sale, renting, transferring, analyzing, distributing, disclosing); no disclosure, even to affiliates, without written consent
- Government Requests
  - Best efforts to notify; responsible and liable

CONTRACT PROVISIONS — OTHER KEY TERMS

- Use of Data
  - Vendors agree to use data for agreed upon purpose
  - Limit access to those who need it
  - Can't sell, rent, or lease data
- Audit Rights
  - Company may audit vendor with reasonable notice
  - Vendor is obligated to remediate within a given timeframe
- Certificates
  - Vendor delivers copies of relevant certifications or audits

CONTRACT PROVISIONS — OTHER KEY TERMS

- Confidentiality
  - Vendor will not disclose confidential data
  - Obligation to train employees & agents on limited access and appropriate security
  - Transfer data in encrypted format
- Termination
  - Who keeps the data after contract term?
  - Vendor will destroy / return data following termination of contract or upon request in a reasonable period of time
- Insurance
  - Mandatory cyber coverage – beware exclusions!

CONTRACT PROVISIONS — OTHER KEY TERMS

- Security Incidents
  - Notification of known or suspected incident in specified time (~24 hours), even if not required by law
  - Clear chain of command after discovery of breach
  - Cooperation in the event of a breach
  - Right to control response, defense, settlement
  - Evidence preservation
  - Vendor to pay all legally required fines, penalties, costs, including costs of notification, credit monitoring, lawsuits, regulatory investigations, etc.
  - Vendor will indemnify for third party claims
  - Vendor report (specify contents)

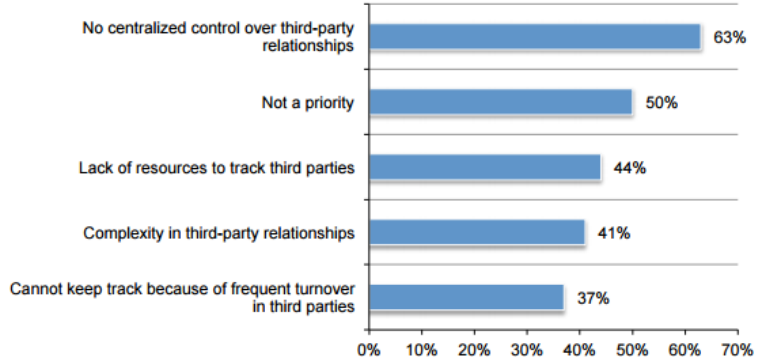
CONTRACT PROVISIONS — OTHER KEY TERMS

- Damages and Limitations of Liability
  - Unlimited liability for data breach and related costs (described in detail)
  - Unlimited liability for privacy failures, including class actions, state AG actions, regulatory fines, etc.
- Indemnification
  - Indemnification for privacy and security failures
  - Defense for not only lawsuits arising from privacy or security failures, but government / regulatory investigations as well

EXISTING VENDORS

- Not just for new vendors!
- Map your data
- Helps you prioritize key contracts and uncover risk

Figure 10. Reasons companies do not have a comprehensive inventory of all third parties
More than one response permitted



Source: Ponemon Institute Research Report, "Data Risk in the Third-Party Ecosystem" (Apr. 2016)

#GPS17

HOW DID THINGS GO?
(WE REALLY WANT TO KNOW)

Did you enjoy this session? Is there any way we could make it better? Let us know by filling out a speaker evaluation.

- Start by opening the IAPP Events mobile app
- Select this session and tap “Click the following link for speaker evaluations”
- Once you’ve answered all three questions, tap “Done” and you’re all set
- Thank you!