Cybersecurity & Privacy

Cyber Hot Topics: Vendor Management

Paige M. Boshell

September 20, 2017

Agenda

Vendor cyber risk

- Managing cyber risk through the lifecycle of the customer/vendor relationship
  - Due diligence of potential vendors
  - Negotiating the critical contract provisions
  - Managing the customer/vendor relationship

Questions

Bradley

Vendor Risk Management is a Hot Topic

- Vendor Risk is one of the largest drivers of data breaches
  - Focus on third party service relationships is increasing
  - Continued targeting of financial institutions and healthcare providers; increased targeting of smaller companies
  - 90% of organizations have been compromised in some fashion
  - 76% of data breaches resulted from a vendor which introduced the security deficiencies that were exploited.
  - Only 24% require vendors to comply with baseline security procedures.
- Target, Home Depot, Miller Coors

Takeaway: Beware the smaller breaches; beware the unsophisticated vendor.

Bradley

Lifecycle Approach to Vendor Risk

- An effective risk management process throughout the lifecycle of the relationship includes:
  - Planning
  - Due diligence
  - Third-party selection
  - Contract negotiation
  - Ongoing monitoring
  - Oversight & accountability
  - Documentation & reporting
  - Independent reviews –regulators, SOC2, PCI
  - Termination and transition

Bradley

Risk Assessment

- Identify crown jewels
- Identify access vectors
- Identify systems access

Bradley

Key Issues to Assess

- What is the vendor's experience and expertise?
- What is the overall "health" of the vendor?
  - What is the vendor's financial condition?
  - Does the vendor have a strong management structure? Is there key man risk?
  - Are the vendor's standards, policies and procedures adequate?
  - What are the vendor's security protocols?
  - Does the vendor have adequate insurance coverage?
- What is the risk profile of the vendor relationship?
  - Access to sensitive data?
  - Mission-critical processes?
- Balance the cost of investigation with the cyber risk

Miller Coors Suit

- $100 million suit for breach of contract
- MillerCoors wanted to implement SAP software for ERP (enterprise resource planning)
- Software = SAP; blueprints for customizations = Deloitte; vendor for customizations and implementation = HCL Tech (existing MC vendor)
- (1) software development contract (2) project implementation contract
- Series of work orders under existing and unrelated MSA
- Series of delays, problems; scope creep
- Go Live: 8 critical severity defects; 47 high severity defects; 1000s of defects detected in follow-up
- MC sued
- HCL countersued: info and staffing failures; inadequacy of understanding and resources; management failures; scope creep
- *Takeaway:* Deal-specific contracts with all expectations completely and objectively stated.

Bradley

Vendor Contractual Risks and Flashpoints

- Customer as original data owner will be sued first. And, held accountable.
- Hold harmless and indemnification provisions with vendors:
  - Often can include limiting and exclusionary language:
    - Caps on indemnification amounts
    - Exclusions for certain types of data breaches
  - No protection if vendor becomes insolvent or goes into bankruptcy
  - No protection if vendor decides not to honor the agreement

Takeaway: Risks that cannot be mitigated entirely by contract should be mitigated otherwise. Consider asking for specific contract terms in RFP.

Contract Negotiations – Terms to Consider

- **Warranties and Indemnities**
- Separate IP?
- Separate data breach?
- Industry standards and best practices
- **Limitation of Liability**
  - Actual, direct damages
  - Exclusion of indirect damages
  - Multiple liability caps (e.g., separate, exclusive cap for data breaches)
  - Risk/revenue analysis

Contract Negotiations – Terms to Consider

- Ongoing Monitoring / Oversight & Accountability
  - Periodic business reviews (e.g., quarterly/annual)
  - Governance structure(s) (e.g., technology review committee)
  - Incident management process
  - Service level standards
  - Standardized information gathering (SIG) questionnaire
  - SOC1/SOC2 reports
  - Audit rights (frequency, costs, third party, deficiencies)

Contract Negotiations – Terms to Consider

- Data Ownership, Use & Disclosure
  - Data classification – IP, customer, PHI, NPI
  - Ownership rights to data/information
  - Permitted uses or disclosures
  - Data retention and disposal
- Privacy & Security

-Confidentiality/NDA

-Comprehensive information security program

  - Governing information security policy
  - Appropriate security measures to comply with regulations & guidelines
  - Requirements to notify for security breaches

Bradley

Contract Negotiations – Terms to Consider

- Subcontracting
- Audit Rights / Independent Reviews
- Termination Rights (Agreement)
  - For cause
  - For convenience
  - Financial condition (insolvency, receivership, bankruptcy, assignment of assets for creditors)
  - Prohibited assignment or delegation
  - Address transition, deconversion costs
- Dispute Resolution
  - Informal process (e.g., escalation to executives)
  - Formal process (e.g., mediation/arbitration)
- Insurance
  - Types of coverage (e.g., professional liability (E&O), cyber liability/security & privacy)
  - Insurer/carrier rating

Insurance as Risk Mitigant

- Cyber Liability Insurance does not cover all exposures to cyber risk.
  - Intellectual property, Reputation, System Improvement

  First person v. third person

- Some forms of cyber risk are actually covered under a Crime policy.
  - Corporate Account Takeover, Funds Transfer Fraud, Social Engineering
  - Loss of data v. loss of funds

Takeaway: Losses are too large to just insure. Other mitigants should be considered. Cyber insurance coverages should be reviewed regularly and each time that significant additional risk is posed.

Monitoring the Vendor

- Dedicate sufficient staff with the necessary expertise, authority, and accountability to monitor the relationship
- As-needed reporting
- Training and awareness
- Independent reviews
- Regularly scheduled checkups

Takeaway: Mitigation is ongoing and continuous.

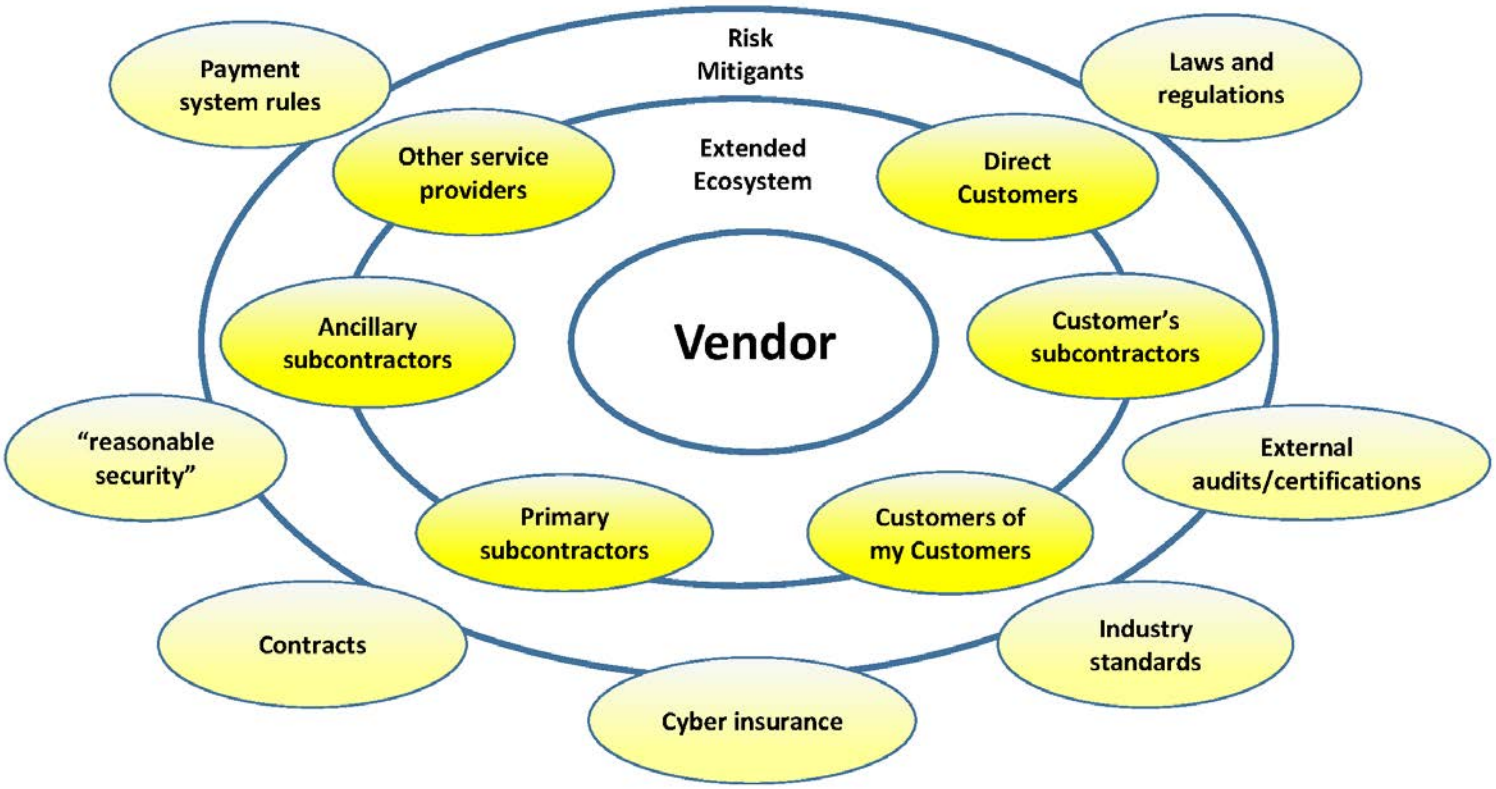
Bradley

Vendor Risk in Cybersecurity Ecosystem

- Cybersecurity should be considered as part of an enterprise risk framework.
  - What are the key risks?
  - What is the organization doing to mitigate cybersecurity risks?
  - Who are the responsible business owners for managing these risks?
  - How are these risks monitored?
  - What internal controls are in place?
- Failure to properly manage vendor relationships can have significant impact:
  - Transactional risk
  - Reputational risk
  - Legal and compliance risk

Bradley

Vendor Ecosystem



Bradley

Questions?

- Paige M. Boshell
- pboshell@bradley.com
- (205) 521-8639

Bradley