The Vendor Threat

“At least 56% of respondents experienced a third party data breach in 2017, a 7% increase from 2016”

2017 Data Risk in the Third Party Ecosystem Study from Ponemon Institute
### Vendors as Threat Vectors

- Increasing vendor reliance for critical operations
  - Payroll, IT outsourcing, etc.
- Vendors are not “external”
  - Critical access to company infrastructure
  - Movement of data and confidential information
  - Real-time integrations with vendors
- Vendor’s vendors

### Vendor Risks

- Financial risks
- Location risk
- Business continuity and time to recovery risks
- Operational risks (quality, cost, performance, capacity)

### Contract Goals

- Risk Identification
- Mitigation
- Transfer
**Diligence - Areas of Concern**

- Base Controls
- Application Controls
- Cloud Security
- Infrastructure Controls
- Physical Security
- Backup & Recovery
- Electronic Transfer
- Privacy Management
- Physical Transfer
- Decommissioning & Destruction
- Physical "Paper" Management
- External Party Management

**Confidentiality**

- What is Confidential Information?
- What are obligations?
- How long do obligations last?
- What are subpoena procedures?

**Key Contractual Concerns**

- Vendor Business and Location
- Data Access and Segregation
- Personnel Issues
- Audit
- Data Security
- Breach Response
- Disaster Recovery and Business Continuity
- Data Sharing
- Insurance
- Laws and Regulations
- Privacy
Customer Privacy Concerns

- Identify nature and categories of data
- Limit use and processing of data
- Limits on transfer of data
- Adherence to data protection laws
- Model contracts
- Flow-down provisions
- Termination

Data Breach Response and Notification

- Notification requirements
- Notice requirements
- Who pays?
### Downstream Obligations (e.g. subcontractors)

- Disclosure of subcontractors
- Adhere to vendor obligations
- Vendor indemnification
- Personnel management

---

### Termination and Data Destruction

- Transition
- Certify destruction
- Compliance concerns

---

### Warranties, Representation, and Indemnity

**Warranties:**
- Enacted, and maintains an info. sec. program
- Confidentiality obligations
- Software and/or services are free of security defects
Warranties, Representation, and Indemnity

Limitations:
• 3x the contract value
• Liquidated damages

Indemnification:
• Data breaches
  • E.g.: Third party damages
• Breach of confidentiality obligations
• Breach of warranties

Insurance
Basic “Cyber” or “Tech” Insurance

First Party Coverages
- Data Breach
- Network Security
- Computer Crime
- Computer Fraud & FTF

Third-Party Coverages
- Data Restoration
- Network Interruption
- Extortion
- Third-Party Liability
- Cyber Terrorism
- Management Expenses
- Identity Theft

Network Security
Tech E&O

Insurance

First Party Insurance and Third Party Insurance

Cyber Security

Insurance

Cyber Security Coverage Checklist - v1.1

Your Coverage Summary:
- Cyber Network, Security, and Information Loss
- Cyber Errors, Omissions, and Defective Acts
- Cyber Communications and Media Liability
- Cyber Extortion
- Cyber Terrorism
- Management Expenses
- Identity Theft

Custom Insurance Coverage Checklist is based on answers you provided about if

Guide when shopping for insurance and talking to agents. It is not

with your insurance agent for professional insurance advice.
Basic “Cyber” or “Tech” Insurance

Choosing the Right Specialty Data Breach Policy

- The types of data included in the coverage.
- Forensic Investigation Costs.
- Whether coverage is provided for data in the hands of third parties.
- Regulatory coverage.
- Business Interruption Coverage.
- Remediation coverages, including “Crisis Management,” “Credit Monitoring,” and “Public Relations Expenses.”
- Limits and control.
- Exclusions and retroactive dates.
Q/A

Thank You!

• Nick Merker
  • Nicholas.Merker@icemiller.com
  • (317) 236 - 2337