Information Security in Contracts and Cyber-Liability Insurance

HCCA Indianapolis Regional Conference 2018
Nick Merker, CISSP, CIPT
Partner, Ice Miller LLP

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
Vendor Originating Threats

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

Risk Identification and Assessment / Information Security Standard
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

Limitations:
• 3x the contract value
• Liquidated damages
Warranties, Representation, and Indemnity

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

Insurance
Insurance

First Party Insurance and Third Party Insurance

Insurance

Cyber Security
Custom Insurance Coverage Checklist - v1.1

Your Coverage Summary
- Cyber Network, Security, and Information
- Cyber Errors, Omissions, and Wrongful Acts
- Cyber Communications and Media Liability
- Cyber Extortion Threat
- Cyber Terrorism
- Cyber Incident Management Expenses
- Identity Theft

Your Business
- You
- Your
- You
Basic “Cyber” or “Tech” Insurance

Third-Party Coverages

- Tech E&O
- Network Security
- Data Breach

First-Party Coverages

- Computer Crime
- Computer Fraud & FTF
- Data Restoration
- Network Interruption
- Extortion

Data Breach

Network Security

Tech E&O

Computer Crime

Computer Fraud & FTF

icemiller.com
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.

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.
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.
Basic “Cyber” or “Tech” Insurance

Third-Party Coverages
- Tech E&O
- Network Security
- Data Breach
- Computer Crime
- Computer Fraud & FTF

First-Party Coverages
- Data Restoration
- Network Interruption
- Extortion
Basic “Cyber” or “Tech” Insurance

Third-Party Coverages
- Tech E&O
- Network Security
- Data Breach
- Computer Crime
- Computer Fraud & FTF

First-Party Coverages
- Data Restoration
- Network Interruption
- Extortion

THINK IN TERMS OF “LOSS” NOT “CAUSE”
Basic “Cyber” or “Tech” Insurance

Third-Party Coverages

**COVERAGE**
We will pay for loss of funds resulting directly from a fraudulently induced transfer causing the funds to be transferred from your premises or banking premises to a person, entity, place or account outside of your control.

**LIMIT OF INSURANCE AND DEDUCTIBLE**
The Limit of Insurance and Deductible Amounts are shown in the Declarations.

**DEFINITIONS**
As used in this Insurance Agreement only:

a. **Fraudulently induced transfer** means:
   A transfer resulting from a payment order transmitted from you to a financial institution, or a check drawn by you, made in good faith reliance upon an electronic, facsimile, telephone or written instruction received by you from a person purporting to be an employee, your customer, a vendor or an owner establishing or changing the method, destination or account for payments to such employee, customer, vendor or owner that was in fact transmitted to you by someone impersonating the employee, customer, vendor or owner.

b. **Vendor** means any entity or person that provides or has provided goods or services to you pursuant to a preexisting agreement.

c. **Funds** means money and securities.

d. **Employee** means any natural person:
   1. While in your service or for 20 days after termination of service; and
   2. Whom you compensate directly by salary, wages or commissions; and
   3. Whom you have the right to direct and control while performing services for you.

e. **Owner** means a natural person having an ownership interest in you.

Insurance Requirements in Contracts
Q/A

Thank You!

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