

Information Security in Contracts and Cyber-Liability Insurance



HCCA Indianapolis Regional Conference 2018

Nick Merker, CISSP, CIPT
Partner, Ice Miller LLP



icemiller.com

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



icemiller.com

Vendor Originating Threats



icemiller.com

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



IceMiller®
LEGAL COUNSEL

icemiller.com

Vendor Risks

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



IceMiller®
LEGAL COUNSEL

icemiller.com

Contract Goals

- Risk Identification
- Mitigation
- Transfer



IceMiller®
LEGAL COUNSEL

icemiller.com

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



icemiller.com

Confidentiality

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



icemiller.com

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



icemiller.com

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



IceMiller
LEGAL COUNSEL

icemiller.com

Data Breach Response and Notification

- Notification requirements
- Notice requirements
- Who pays?



IceMiller
LEGAL COUNSEL

icemiller.com

Downstream Obligations (e.g. subcontractors)

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

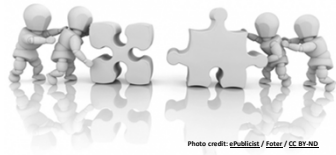


Photo credit: gshulick / iStock / iC.Miller

IceMiller
LEGAL COUNSEL

icemiller.com

Termination and Data Destruction

- Transition
- Certify destruction
- Compliance concerns



IceMiller
LEGAL COUNSEL

icemiller.com

Warranties, Representation, and Indemnity

Warranties:

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

IceMiller
LEGAL COUNSEL

icemiller.com

Warranties, Representation, and Indemnity

Limitations:

- 3x the contract value
- Liquidated damages



icemiller.com

Warranties, Representation, and Indemnity

Indemnification:

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



icemiller.com

Insurance



icemiller.com

Insurance

First Party Insurance and **Third Party Insurance**

IceMiller
LEGAL COUNSEL

icemiller.com

Insurance

Cyber Security Custom Insurance Coverage Checklist - v1.1

This coverage checklist is based on answers you provided about your business and is intended to be a guide when shopping for insurance and talking to agents. It is for informational purposes only and should be used with your insurance agent for professional insurance advice.

Your Coverage Summary

- Cyber Network, Security, and Information
- Cyber Errors, Omissions, and Wrongful Acts
- Cyber Communications and Media Liability
- Cyber Extortion Threat
- Cyber Terrorism
- Crisis Management Expenses
- Data Breach and Identity Theft

Your Business

- You are a sole proprietor
- You are a partner
- You are an S-corporation
- You are a C-corporation
- You are a non-profit
- You are a government contractor
- You are a contractor
- You are a manufacturer
- You are a retailer
- You are a service provider
- You are a professional
- You are a financial institution
- You are a health care provider
- You are a government agency
- You are a public utility
- You are a transportation provider
- You are a telecommunications provider
- You are a media organization
- You are a research organization
- You are a non-governmental organization
- You are a government contractor
- You are a contractor
- You are a manufacturer
- You are a retailer
- You are a service provider
- You are a professional
- You are a financial institution
- You are a health care provider
- You are a government agency
- You are a public utility
- You are a transportation provider
- You are a telecommunications provider
- You are a media organization
- You are a research organization
- You are a non-governmental organization

IceMiller
LEGAL COUNSEL

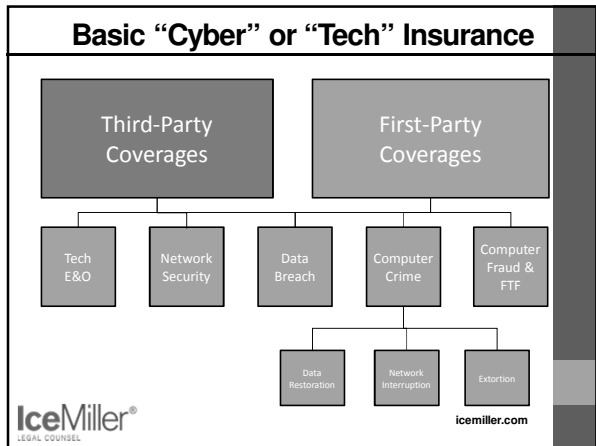
icemiller.com

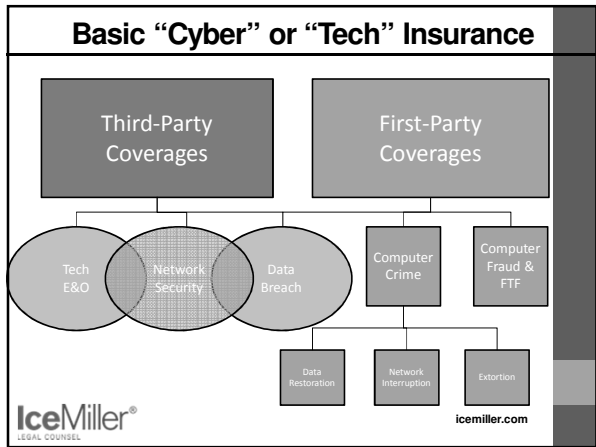
Basic "Cyber" or "Tech" Insurance

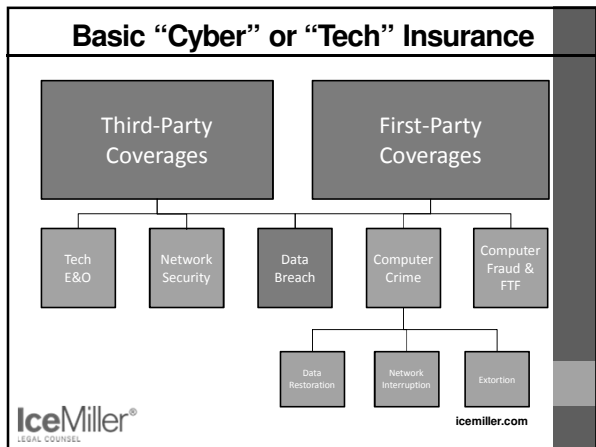
Third-Party Coverages		First-Party Coverages		
Tech E&O	Network Security	Data Breach	Computer Crime	Computer Fraud & FTF
			Data Restoration	Network Interruption
				Extortion

IceMiller
LEGAL COUNSEL

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.

IceMiller®
LEGAL COUNSEL

icemiller.com

Restoration

Interruption

Exclusion

uter
&

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.

IceMiller®
LEGAL COUNSEL

icemiller.com

Restoration

Interruption

Exclusion

uter
&

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.

IceMiller®
LEGAL COUNSEL

icemiller.com

Restoration

Interruption

Exclusion

uter
&

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.

Restoration Interruption Extortion

IceMiller®
LEGAL COUNSEL

icemiller.com

Basic “Cyber” or “Tech” Insurance

Choosing the Right Specialty Data Breach Policy

This policy does not apply to claims, losses or damages directly or indirectly arising out of or based upon or in consequence of, resulting from, or in any way involving...regardless of any other cause of event contributing concurrently...

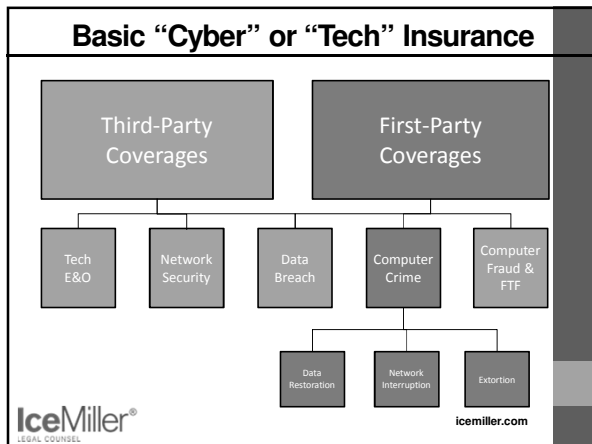
- [1] Failure in design, manufacture, workmanship, materials, architecture or configuration of [your] computer system...
- [2] Failure to ensure that [your computer system] is protected to industry standards...
- [3] any widespread dispersal of a computer virus that is not directed specifically at [your] computer system...
- [4] wear and tear, gradual deterioration, drop in performance or obsolescence of [your computer system]...
- [or] [5] inherent defects in [computer hardware or software] supplied by a third party...

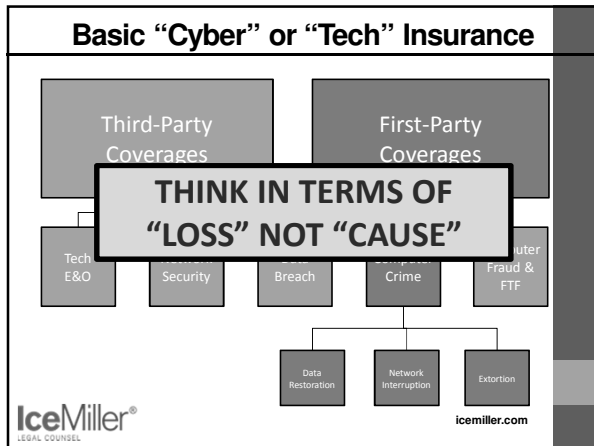
Restoration Interruption Extortion

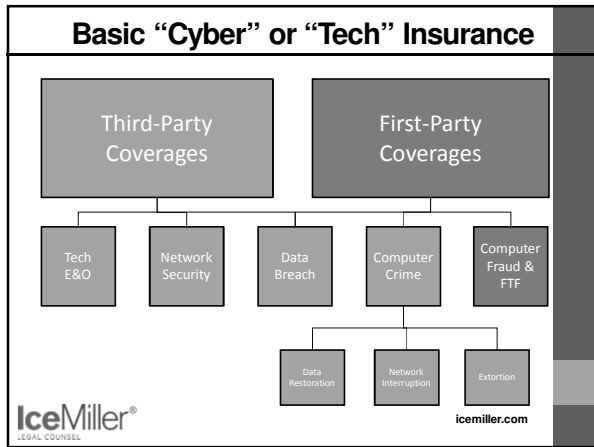
IceMiller®
LEGAL COUNSEL

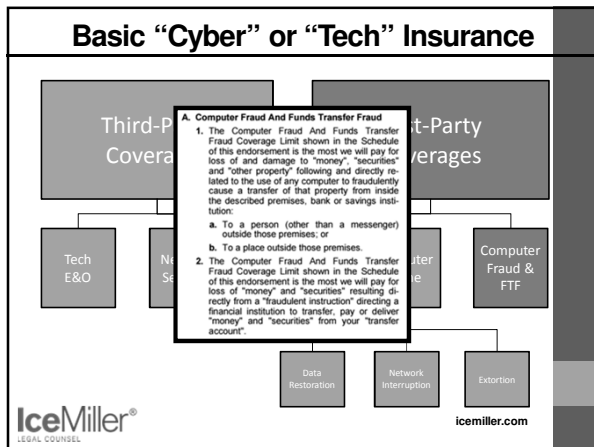
icemiller.com

Basic “Cyber” or “Tech” Insurance









Basic "Cyber" or "Tech" Insurance

Third Party + Party Ages

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 Amount are shown in the Declarations.

DEFINITIONS
As used in this Insuring 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, telefacsimile, 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 without your knowledge or consent and without the knowledge or consent of 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 30 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.

Computer Fraud & FTF

Extortion

icemiller.com

IceMiller
LEGAL COUNSEL

Basic "Cyber" or "Tech" Insurance

Third Party + Party Ages

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 Amount are shown in the Declarations.

DEFINITIONS
As used in this Insuring 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, telefacsimile, 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 without your knowledge or consent and without the knowledge or consent of 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 30 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.

Computer Fraud & FTF


Extortion

Social Engineering

icemiller.com

IceMiller
LEGAL COUNSEL

Insurance Requirements in Contracts



icemiller.com

IceMiller
LEGAL COUNSEL

Q/A



IceMiller[®]
LEGAL COUNSEL

icemiller.com

Thank You!

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

IceMiller[®]
LEGAL COUNSEL

icemiller.com
