

DATA CENTER WEEK 2025

Fortifying Data Centers: Navigating Data Privacy and Breach Insurance

Presenters



Vivek Chopra



Bradley Dlatt

Agenda



Why Insurance Matters

Potential Claims Likely to Arise Out of a Data Breach or Data Privacy Claim

Insurance Policies That May Respond

Other Risks Posed By Data Center Operation and Potential Coverage

Loss Management Strategies

Why Insurance Matters

Companies spend millions of dollars annually on premiums. Policies, however, are **assets**, not liabilities.

Corporate risk managers and in-house counsel often do not have the time or resources to understand what they are buying, even when being advised by a broker.

Insurers are slow to adapt policies to the risks in the marketplace; multiple endorsements to request or choose from.

Insurance brokers are key but do not closely review policy language.

Why Insurance Matters

Insurance companies make money in part because their customers leave it on the table. For example:

- Failure to have procedures in place to review subpoenas, demand letters or lawsuits for potential coverage
- Failure to provide timely notice of a potentially covered claim
- Failure to cooperate with an insurer by providing requested information
- Failure to scrutinize an insurer's denial of coverage

Potential Claims Likely to Arise Out of a Data Breach

First Party Claims

Theft and Fraud

Investigation Costs

Cyberextortion

Computer Data Loss
and Restoration

Business
Interruption/Supply
Chain Interruption

Property Damage

Crisis
Management/Public
Relations

Third Party Claims

Regulatory Claims

Credit and Fraud Monitoring

Common Law Privacy Claims

Statutory Privacy and Consumer Protection Claims

D&O/Shareholder Claims

Types of Policies That May Respond to a Breach

Cyber Risk/Cyberliability



Policies are written on a
“claims made” basis



Strict reporting requirements



Most Cyber Risk Policies are
modular, meaning that they
provide multiple forms of
potentially applicable
coverage

"First-Party" Coverage

- Losses due to destroyed or damaged data; data restoration
- Business Interruption
- Physical Damage
- Extortion demands

"Third-Party" Coverage

- Privacy Liability
- Unauthorized disclosure of confidential information
- Costs to investigate breaches, satisfy notification obligations, defend against regulatory proceedings

Cyber Risk/Cyberliability

“Security Event” or “Privacy Event” Coverage

- Most likely to be implicated by a breach
- “Security Event” = failure or violation of a computer system which results in unauthorized access to or use of information, DOS attacks, or receipt/transmission of malicious code
- “Privacy Event” = loss related to the release of confidential or protected information
- Also covers loss related to failure to notify the appropriate individuals of such events where required by law





Key question: Definition of
“computer system”

What is the scope of the definition?
Who owns, manages, or controls the
system that was breached?



Particularly important when outside vendors are involved

Network Interruption Coverage

- Similar to business interruption – focused on lost income
- Triggered after computer networks are compromised for a specified period of time

Event Management Coverage – after a breach, covers:

- Public relations/crisis management costs
- Investigatory costs
- Notification costs
- Restoring, recreating, or recollecting lost data

Cyber Risk/Cyberliability

- Professional Services Liability Coverage
 - Third-party claims arising out of “Wrongful Act” – i.e., error or omission in the performance of professional services
 - E.g., performing technology services, services leading to invasion of privacy, financial loss through online impersonation
- Cyber Extortion Coverage
 - Money paid to end a security/privacy threat

Cyber Risk/Cyberliability

Cyberterrorism Coverage

- Security breach or disruption combined with intention to cause harm or intimidation in an effort to further a social, ideological, religious, or political objective

Regulatory Actions

- Costs to defend any regulatory action or investigation by a governmental or regulatory body in the aftermath of a breach

Identity Theft

Social Engineering Coverage

- Threat comes from outside entity working its way into your employee's confidences

What does it cover?

- “Bodily injury” or “property damage”; or
- “Personal and advertising injury”
 - Generally requires “publication” of the information

Caused by an “Occurrence”

- What counts as an “occurrence” varies by policy definitions and jurisdiction

Commercial General Liability



Most likely to respond where there is physical damage in connection with the breach



Potentially Applicable Exclusions

Cyber liability

“Privacy Violations”

Intentional Conduct

Errors & Omissions (Professional Liability)



Can be purchased within Cyber Risk Policy or separately. Often an opportunity to purchase specific data privacy liability coverage, which would be most likely to respond to a breach.



Claims-made coverage



Covers claims against an insured arising out of “wrongful acts” committed in conduct of “professional services”

“Wrongful acts” typically focus on negligent errors or omissions

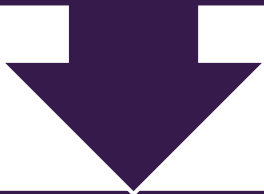
“Professional services” are tailored to your business

Claims-made coverage

Typically covers three “sides”

- Side A – direct coverage for directors’ and officers’ individual liability that corporation has not indemnified
- Side B – reimbursement coverage to organization for indemnifying directors and officers
- Side C – coverage to corporation for liability arising out of specific claims filed against company (typically securities claims and shareholder suits)

May be implicated in aftermath of a breach as investigation uncovers what decisions were or were not made by the company to deter, prepare for, and/or respond to a data breach



In addition to shareholders and securities claims, D&O policies may cover, among other things:

Responses to civil or criminal subpoenas

Government or regulatory investigations

Special litigation committee costs

Claims-made coverage

May respond to loss arising out of:

- “Employee dishonesty”
- Computer fraud or theft
- Data extraction
- Investigations related to crime or theft

Other Risks Posed By Data Center Operation and Potential Coverage

Federal Evaluation of Data Center Risks

"Data centers are **complex environments** with a number of external dependencies and internal equipment, any of which could cause downtime in multiple ways. Availability and uptime can be impacted by events such as **environmental factors**, natural disasters, **power and equipment failures**, and maintenance activities. Understanding the frequency and likelihood of these risks to availability is critical to managing them. Agencies must adopt the ongoing use of appropriate risk management frameworks to identify these risks and assess their likelihood."

Clare Martorana, Federal Chief Information Officer, Memorandum for the Heads of Executive Departments and Agencies on "Implementation Guidance for the Federal Data Center Enhancement Act" (M-25-03) (January 13, 2025), at 5.

Enviromental Risk: Property Insurance

- Scope of Coverage: First-party property policies protect a policyholder's place of operations and inventory and provide coverage for lost or damaged property.
 - “All Risk” vs. “Named Peril”
- Specific Cyber Protections for Property
- Business Interruption
 - Direct
 - Contingent (e.g. energy supplier)
- Extra expense

Enviromental Risk: Builder's Risk



Property coverage (including business interruption and extra expense) for property during course of construction



Options to "wrap" into Owner or Contractor Controlled Insurance Programs (OCIP or CCIP)

Loss Management Strategies

Loss Management Strategies

Build	Build the right team
Keep	Keep good records (policy copies, COIs, correspondence)
Audit	Audit your policies: always be negotiating
Report	Report claims promptly <ul style="list-style-type: none">• Never assume your broker has done this for you
Determine	Determine how to best tell your story
Protect	Protect privilege

*Perkins
Coie*