Contract Insurance Requirements for Breach Exposures
Session Introduction

Been there, Done that!

2012
Dangerous Data – And the Nightmare Continues

2013
Beached, Breeched or Besieged – Dealing with Data Security

2014
Point – Counterpoint: Cyber Liability

The PowerPoint presentations of these three sessions are available to members at www.strima.org.
Once you sign in as a member, see the Conference Education section on the home page.

Session Assumptions!
Our Presenters Today

Lauren Gorte
Vice President, Underwriting Manager
ACE USA

Zach Scheublein
Vice President
Aon Financial Services Group
How Can Risk Managers Protect Their Organization

Evaluate Third-Party Providers

Vendors, suppliers, consultants, IT providers and a range of other third parties have occasion to access various types of confidential State information.

A risk assessment should be conducted for each third-party provider and, depending on the type of data being shared, additional steps should be considered to prevent security breaches.

Risk managers should evaluate a range of questions including:
How Can Risk Managers Protect Their State

- Are data and network security standards equivalent to yours?
- How does the provider erect security walls between data from different customers?
- Who will have access to the information and is encryption possible?
- Will customers be notified that their information will be stored in a cloud?
- Does the cloud provider have its own adequate insurance coverage (possibly requesting that your organization be named as an “additional insured”)?
- Is some information simply too sensitive to turn over to a third party?
- How will you monitor access (tracking and privilege user access)?
- Risk versus Reward – cost effective and potentially heightened security vs. increased exposure/negative contractual terms
How Can Risk Managers Protect Their State

Evaluate Third-Party Providers

Third parties should, at a minimum, be expected to accept inclusion of language in which they warrant that they are in compliance with applicable laws relating to information privacy and security.

Contracts should contain indemnification provisions that commit the third-party providers to indemnify you should a security or privacy breach occur.
Vendor Insurance – Should you require it?

For IT vendor agreements - when is it necessary to have Cyber insurance?

Requiring vendors to carry Cyber insurance is increasingly common in service contracts. However, the need to include this requirement does involve a number of factors.

Questions to ask include:
- What services are the vendors providing?
- Will the vendor directly touch or have access to PII/PHI?
- What can go wrong?
- What costs and damages would your organization incur should the vendor have a breach?
Vendor Insurance – Should you require it?

- How many PII/PHI records are involved?
- What is the value of the contract? Big? Tiny?
- Do they have the financial strength to meet their indemnity obligations?
- Who is responsible for notification? Do you want your vendor controlling the notification process for your clients?
  - Forensics & Subrogation
Vendor Insurance – General

For IT vendor agreements –
When is it necessary to have Cyber insurance?

- Important to note that while these are general guidelines - there is no automatic answer and often insurance requirements will have to be tailored to the specific situation.

- While asking for "perfect" insurance language would seem to make sense from your State’s perspective, many smaller vendors will struggle to meet certain requirements due to size, sophistication and cost. Rigid imposition of rules may lead to contract language impasses and difficulty in securing vendors.

- It is also important to remember, that the reason to require vendors to carry Cyber coverage is to provide a financial backstop to the vendors indemnity obligations. They do not have to utilize their insurance to pay damages and, therefore, while it is a good idea to have a standard requirement, it does not always make sense to require coverage.
Here is the language we recommend to our clients for use in their contracts with technology services vendors. We suggest including the language in red if the vendor will have access to Personally Identifiable Information.

**Errors & Omissions/Professional Liability /Cyber Insurance**, in an amount not less than $X,000,000 per claim and annual aggregate, covering all acts, errors, omissions, negligence, and including infringement of intellectual property (except patent and trade secret) in the performance of services for XXX or on behalf of XXX hereunder. Vendor’s policy will provide for Data Security & Privacy “Cyber” coverage (including coverage for unauthorized access and use, failure of security, breach of confidential information, of privacy perils, as well as breach mitigation costs and regulatory coverage). Such insurance shall be maintained in force at all times during the term of the agreement and for a period of two years thereafter for services completed during the term of the agreement. XXX shall be given at least 30 days notice of the cancellation or expiration of the aforementioned insurance for any reason.

Our suggestion is to start with the aforementioned language and to let the vendor explain to you why they should not need to evidence cover.
This is a big area of misunderstanding. For most IT vendors - even those who touch PII - this is really a Liability issue that will constitute an Errors & Omissions claim alleging failure to protect PII in the course of performing services to clients.

There is a misconception among organizations that by outsourcing their data to a third-party vendor they have effectively transferred the risk in the event of a data breach. This is not the case, as the organization that is outsourcing data collection, hosting, processing, transmission or storage is still the ‘data owner’ from a regulatory perspective and thus the liabilities can not be effectively transferred contractually.
If there is a data breach that is caused by a vendor's mistake, it is still ultimately the 'data owner’s' responsibility. The notification and offering of credit monitoring services will be the responsibility of the data owner entity.

The entity will then go after the vendor asserting its contractual right to be indemnified and, if necessary, in court by bringing both a tort and contracts claim. In theory, the vendor’s E&O/Cyber policy should respond.

In assisting our clients with insurance requirements, we suggest language that requires evidence of both types of policies for these types of vendors.
Requirements for Security Obligations.
- Require vendor to maintain an information security program and at a minimum require them to follow your policies and procedures, encrypt data, etc.

Requirements for Audit and Compliance Provisions
- You should have right to audit vendor; vendor should supply you with audits performed by third parties.
Vendor Insurance - IT Specific – Risk Transfer

Subcontracting and Other Protections
- Approval rights, subs obligated to comply with same obligations, restriction on vendor location, obligations to remove your data and how.

Cyber Incident Response
- Notification within X hours, investigate and report, remediate, updates, cooperation, control of response if customer data.

- These restrictions can be difficult to impose and monitor (especially cloud companies)
Vendor Insurance - Limits

What limit to ask for is a common question.

- The limit amount is dependent upon the services provided, the size of the vendor and the size of the contract.

- Some clients create vendor level matrices – type of service, size of contract, size of vendor, do they touch PII, etc. to set suggested limits.

- Start with $5M requirement for all vendors and then move up or down depending upon the terms of the transaction.
Example - A large contract with a start-up cloud computing company that will host your customer data probably requires that the vendor carry large limits. In many cases, this is an economics discussion with the vendor. For example, if you aren't paying them much and you require a large limit for E&O coverage, the extra cost may make the contract unprofitable.
Vendor Insurance - Limits

State Examples
And their Pros and Cons

Disclaimer
Not created, reviewed, approved or otherwise evaluated by our speakers or their respective companies!
Vendor Insurance - Limits

State Example - New Jersey Approach

Developed an internal
Risk Management Matrix to Determine Liability for IT projects

Step One – Developed Criteria

• **Technology** (type, implementation plan, testing, & impact to users)
• **Interfaces** (complexity within app, interfaces with other apps or systems)
• **Political visibility** (state liability, stakeholder input, mandates)
• **Resources** (contractor experience, time to implement, cost control, how much State staff availability and skills to support)
• **Funding** (cost, timeframe, certainty of timeframe)
• **Project Management** (Compliance with State OIT, plan, requirements, documentation, collaboration with stakeholders)
Vendor Insurance - Limits

State Example - New Jersey Approach

Step Two –
Assigned criteria and related points for low, moderate, high and unknown risks for each of the related criteria and their factors discussed in step one

Step Three – Then points were assigned for
LOW RISK (23-64 points)
MODERATE RISK (65-95 points)
HIGH RISK (96-138 points)
Step Four – Developed a scoring guide for limits to require:

<table>
<thead>
<tr>
<th>Total Score</th>
<th>CGL</th>
<th>E&amp;O/Cyber</th>
<th>THREAT</th>
</tr>
</thead>
<tbody>
<tr>
<td>23-36</td>
<td>1X</td>
<td>1X</td>
<td>LOW RISK</td>
</tr>
<tr>
<td>37-50</td>
<td>2X</td>
<td>2X</td>
<td></td>
</tr>
<tr>
<td>51-64</td>
<td>3X</td>
<td>3X</td>
<td>MODERATE RISK</td>
</tr>
<tr>
<td>65-78</td>
<td>4X</td>
<td>4X</td>
<td></td>
</tr>
<tr>
<td>78-81</td>
<td>5X</td>
<td>5X</td>
<td></td>
</tr>
<tr>
<td>82-95</td>
<td>6X</td>
<td>6X</td>
<td></td>
</tr>
<tr>
<td>96-109</td>
<td>7X</td>
<td>7X</td>
<td>HIGH RISK</td>
</tr>
<tr>
<td>110-123</td>
<td>8X</td>
<td>8X</td>
<td></td>
</tr>
<tr>
<td>124-137</td>
<td>9X</td>
<td>9X</td>
<td></td>
</tr>
<tr>
<td>137-138</td>
<td>10X</td>
<td>10X</td>
<td></td>
</tr>
</tbody>
</table>

High - MUST contact Risk management
**Vendor Insurance - Limits**

**State Example – Maine**

This document is used for all Information Technology contracts of any dollar amount.

<table>
<thead>
<tr>
<th>Number of PII Records</th>
<th>Insurance per Occurrence</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 through 3,000</td>
<td>$400,000 *</td>
</tr>
<tr>
<td>3,001 through 100,000</td>
<td>$1,000,000</td>
</tr>
<tr>
<td>100,001 through 1,000,000</td>
<td>$5,000,000</td>
</tr>
<tr>
<td>Greater than 1,000,000</td>
<td>$10,000,000</td>
</tr>
</tbody>
</table>

* Maine Tort Claims Act Limit
Vendor Insurance -
Additional Insured / Notice of Cancellation

The requirements to:

(1) be named an “additional insured” and

(2) that the organization receive 30 days notice of cancellation from the carrier.

Can cause problems for vendors and do not provide a huge benefit to your organization.
Vendor Insurance -
Additional Insured / Notice of Cancellation

Some E&O/Cyber policies have language that allows the Insured to automatically add “additional insureds” when required by contract. But many do not and it becomes a headache for the vendor to go back and add every client to their policy.

In addition, if not done properly it can cause more harm than good (insured vs. insured exclusions, ‘data-owner’ notification requirements, primary, non-contributory language, etc.).

It is the rare instance where your organization would want the ability to notice claims under another policy (let alone having the ability to properly do so) or have a third-party vendor communicate to your customers/employees in the wake of a data breach.
Remember –

You may be outsourcing your operations
BUT
You are NOT outsourcing your liabilities!