MARSH JLT SPECIALTY

INSIGHTS | MAY 2020

Writing Clear Contracts for Cyber Risk Transfer

Picture the scene: Your company outsources its digital marketing – including management of the customer relationship management system with the personal details of thousands of customers – to a startup. The terms and conditions are agreed, and both parties are happy with the negotiated contract.

Months later, your customers' data is compromised while being handled by the startup.

Who is liable, and to what extent? Who will handle the incident's aftermath? Whose insurance should cover the losses? Does the startup have suitable insurance to cover costs? And, if so, does your company have the contractual right to recover? During a cyber incident, the answer to such questions is not always clear.

Amid contractual negotiations over price and service levels, questions of cybersecurity, liability, and insurance can easily slip through the cracks. A lack of contractual clarity can result in later disputes over liability, who/or which insurer should cover the costs, and which company should manage the incident.

This is why effective contractual risk transfer is a key element in negotiations before an event occurs.

Who takes the risk?

Ensuring you're not held responsible for mistakes or errors made by a vendor can provide critical business protection. A contract that clearly and specifically spells out which party is responsible in the event of a cyber loss – before work begins – could save your company time and expense in the event of litigation, and also help to improve crisis management following an incident.

This is particularly relevant for companies exploring outsourcing contracts – for example, if outsourcing to the cloud – or professional services companies providing digital services.

MARSH

The optimum outcome is to fully transfer risk with an adequate financial backstop, although this is not always realistic. Questions affecting the outcome of contractual risk transfer include:

- Who is the vendor? Are they a large or small company; a market leader or one hungry for your business?
- What is the industry? Some industries are more advanced than others on contractual language or have accepted standards around indemnification.
- Size of the contract? It's often easier to ask for more protection on a big deal than a small one.
- What services are being provided? Is the vendor handling your data? Is their service mission-critical? What happens if they make a mistake?
- What is the nature of the relationship?
- Whose contract form is it, the vendor's or yours?
- Are there any carve-outs or negligence standards? Liability caps are common in many contracts (for example, liability capped at fees earned in the past six months), and can devalue indemnity and insurance limit requirements.

Insurance provisions

It's routine to require your vendor to carry insurance for the risks they face that could affect service, including motor, property, general liability, and employer's liability coverage. In professional or technology service contracts, professional liability is also standard, and increasingly so is cyber insurance.

Insurance requirements should dovetail contractual requirements and careful analysis of your trading partner. Requiring your vendor to carry insurance ensures it has the financial wherewithal to support its indemnity obligations. For example, there is no point a vendor accepting unlimited liability for any losses relating to data breaches if it does not have adequate capital, via its balance sheet or insurance, to cover the losses.

Requiring cyber coverage may also increase the likelihood that the vendor has been through a cyber insurance due diligence process, meaning underwriters have evaluated their risks and risk management maturity. In other words, it reduces the chance of them being a "bad risk".

So what insurance should you require your vendors to have?

Typically, errors and omissions (E&O) or professional liability insurance provides vendors with coverage for a failure of their services. Meanwhile, cyber coverage addresses cyber security issues with their network or disclosure of private information.

E&O is required if the vendor provides a service, and the policy must cover negligence more generally. Most companies that need E&O insurance will bundle the liability elements of cyber coverage into their E&O policy, so one policy may satisfy both requirements.

If the concern is a data breach due to a vendor handling your data, then either E&O or cyber may work, depending upon policy language. For caution's sake, it can make sense to require both, and many tech services companies buy these coverages together.

Setting limits

Companies often start with a standard request (£2 million, £5 million, £10 million, and so on), which depends on their size and the size of the typical vendor contract by revenue. Often, the value of a specific vendor contract will provide guidance on the level of risk and appropriate limit. Other factors to consider include:

- What are the potential damages if something goes wrong?
- Is the vendor providing a mission-critical or minor routine service?
- Who is the vendor? A multinational with £50 billion in revenue or a start-up with three employees working out of the garage? Limits should be realistic, proportional, and commercially feasible.
- Is the vendor touching personally identifiable information?
- Has the vendor successfully capped its liability? For example, if they have fully capped liability at £2 million, is there reason to require £10 million of insurance?

Contract language

Being named as an "additional insured" (AI) has less value in E&O/cyber claims, although it is common in other contractually required lines. It would enable an entity to access a policy – and trigger breach cost payments – which would be beneficial in data-breach claims where the named insured provides services to the AI and causes the breach.

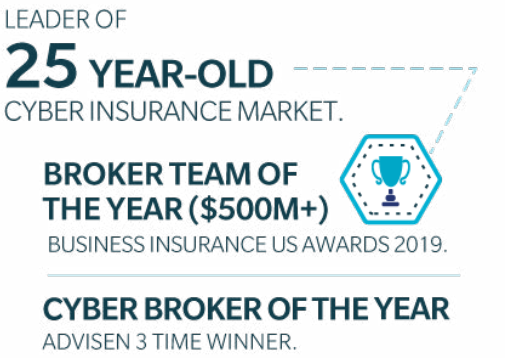
However, it would be unclear who would pay the retention or manage the process, and who would coordinate with the insurer. Being added as an AI can actually cause problems for the AI, if done incorrectly. For example, almost all policies contain an insured vs. insured exclusion, which could end up barring coverage for an E&O claim. Other insurance language could also be used to avoid coverage if the AI has its own policy.

Another consideration is whether to ask for a "right-to-audit" clause from vendors.

Contracts with vendors that touch your client or confidential information should require them to protect the data they handle. Increasingly, contractual language is more than the standard "provide appropriate security controls". Forward-thinking companies often require standards that can include: segregation of data, limitations on where the data can be housed geographically, and detailed requirements as to security practices.

Right-to-audit language typically allows you to review your vendor's security practices and procedures, although you are not generally required to do so. This allows you to identify, and then eliminate, risky vendors; supports your compliance obligations; and strengthens your security practices and procedures. Like all contracts, your ability to secure this contractual right will depend on the terms of the deal. But the request is becoming more common among larger companies with considerable amounts of personally identifiable information, which outsource some or all of their data management services.

It's as true today as ever that when you outsource services, you do not outsource liability. Clearly establishing indemnity and insurance provisions during contract negotiations with vendors, however, helps to manage cyber liability if a claim does arise.



For more information on how to address cyber liability exposures arising from contract risk, contact your Marsh representative, send an email to cyber.risk@marsh.com, or contact:

SARAH STEPHENS
Head of Cyber Practice, International
+44 (0)207 558 3548
sarah.stephens@marsh.com