In-depth analysis: Business interruption in the cyber domain

Published 1 September 2016

While the potential exposures are stark, business interruption is a relatively untested area of cyber insurance, where wordings need to keep pace with both changing exposures and customer needs.

A cyber attack or operational IT failure denying an organisation access to its electronic systems can cause major disruption, with potentially serious financial and reputational consequences. Following a data breach, an organisation can also suffer loss of production, sales and customers as networks and websites are taken offline and repaired.

“Organisations face both operational exposures and information risk in this digital age,” says Hans Allnutt, Partner at DAC Beachcroft. “Never before have organisations held so much data and been able to do so much with it. There is also an unprecedented reliance on IT systems and networks.

“Whether it is a malicious attack or an IT glitch, organisations are increasingly aware of the threat of disruption from a cyber incident. The publicised incidents of cyber related disruptions have increased in recent years. The financial loss and costs of such incidents would typically have been indemnifiable under standalone cyber insurance policies had a policy been in place,” he says.

Standalone cyber insurance was initially developed to cover third-party liabilities and first-party costs arising from a data breach, a role it appears to be fulfilling quite successfully in the US, where demand is greater. However, in the absence of wholesale mandatory breach notification laws outside the US, there has been greater interest in broader cyber coverages to meet a wider range of cyber exposures, most notably business interruption. More and more insurers are now willing to offer such cover, and limits have been increasing, while demand from customers is said to be growing.

Same but different

Cyber business interruption is a relatively untested area for insurers. While experience can be transferred from business interruption in the physical domain, cyber business interruption exhibits some important differences.

Business interruption cover that is offered by standalone cyber insurance policies is largely derived from property damage business interruption cover, and as such follows the same basic concepts. Business interruption cover typically aims to indemnify loss of profit or revenue, as well as increased cost of working and the costs of mitigating losses. There will then be some adjustment of the claim to allow for other external factors – such as fluctuations in market conditions or prices – that may mitigate the loss.

However, there are fundamental differences in the character of cyber losses and the interplay with policy wordings. Cyber business interruption claims are also potentially more complex and less tangible, and will often require different skills to quantify and adjust.

“Insurers are very much in uncharted territory when it comes to cyber business interruption and are to some degree relying on the experience of physical business interruption claims,” says Ben Hobby, a Partner at international forensic accountants RGL Forensics.

“The challenge is to understand the nature of cyber business interruption and how it differs from physical business interruption. It’s easy to conceptualise a physical peril, but with cyber we are dealing with the intangible, where it is much harder to understand the impact,” he says.

Mega Play case study

A fictitious online gaming firm is hit by a distributed denial of service (DDoS) attack. Measures taken to repel the attack by a third-party service provider responsible for the site’s caching rules result in a data breach revealing customer account details. The site is taken offline for four days while the problem is fixed, with Mega Play claiming financial losses, reputational damage and loss of customers.

This case study illustrates some key legal and forensic accounting issues when adjusting a cyber business interruption claim. For example, it is first necessary to establish the cause of the interruption according to the policy wording.

Depending on the policy wording, the cause of the interruption could be the DDoS attack giving rise to the subsequent events –

including the breach caused by changes to the caching rules. However, the third-party service provider's response to the attack, and resulting breach, could be considered a separate cause, and potentially outside the scope of cyber insurance cover which indemnifies only cyber attacks.

"Unlike property damage, where cover is usually all risk, cyber policy language tends to refer to a specific event that gives rise to a significant loss," according to Chris Wilkes, Partner at DAC Beachcroft.

In this scenario, Mega Play was also concerned with losing customers and subscribers and therefore willing to offer promotions to reduce customer churn. Depending on policy language, such payments could be viewed as mitigation costs and insurable as part of cyber business interruption cover.

Establishing cause

There are a number of key factors that need to be considered when underwriting and settling cyber business interruption claims. In particular, the nature of the loss can make it challenging to establish the cause of loss and quantify the impact on the business.

One of the starkest and most obvious differences with cyber business interruption is the lack of a physical cause. In the physical insurance domain, business interruption is triggered by a property damage event but in a cyber world it can be far more challenging to evidence a virtual cause and quantify losses.

"When moving from the physical world to the digital, there are a number of factors that underwriters and brokers need to consider, such as the cause of the disruption, its impact on the business and what can be done to mitigate it," says Chris Wilkes, Partner at DAC Beachcroft. "The chief difference with cyber interruption is the absence of physical damage. This is a simple point, but one that is often overlooked."

Deductibles and waiting periods

Another big difference between cyber and physical business interruption is the duration of disruption and the repair period, and how this relates to policy wordings.

Business interruption wordings will typically apply a financial deductible or a time-based waiting period before the insurance indemnity will respond – this element of self-insurance leaves the insured to deal with smaller claims. Insurers also will limit the period of indemnity (that is, the number of days, months or years of interruption for which the policy will pay for losses).

For property business interruption the period of indemnity is likely to be relatively long, reflecting the time it takes to repair equipment or rebuild property – the average time to repair a building following a fire can be 12–36 months.

Yet time is short in a cyber event. "With cyber business interruption we are looking at much shorter periods of disruption, perhaps hours or days, and a maximum cover period of three to four months. Underwriters and insureds should consider whether this is long enough," says Kevin Harding, a Partner at RGL Forensics.

At present, waiting periods for cyber policies are typically around 6–12 hours, but an online retailer, for example, could rack up very large losses in a 12-hour period of disruption. If its policy includes a six-hour waiting period, a substantial loss of sales could fall within the deductible.

In such cases it may be that a financial deductible will be more appropriate than a waiting period. The suitability of waiting periods versus financial deductibles is expected to be an area for future debate as cyber insurance products develop.

"Underwriters will want flexibility. But they will also need to satisfy themselves that a monetary deductible is reasonable in the context of the insured and the type of incidents they may face. It all comes back to understanding the insured's business to ensure that those situations are appropriately dealt with," says Wilkes.

External factors

Shorter periods of disruption have implications to be considered when quantifying the financial impact of a cyber event on a business.

As with property business interruption, cyber business interruption claims are subject to adjustment for external factors, such as industry or market trends. For example, if an online retail website goes down, the loss of sales will depend on the exact time of the outage – sales may be lower or higher, for example, on certain holidays or weekends.

Shorter periods of disruption may make it harder to separate actual business interruption from other factors, such as those affecting the performance of the business or external trends. "Despite shorter periods of disruption, external factors and trends will still be an issue for cyber claims. In fact, when the interruption is so short, there may be discussions as to whether an insured has actually lost sales depending on the type of business," says Harding.

There may also be instances where the initial disruption and repair time is just a few days, but where the financial damage continues for many months or years. In a recent example, a company suffered a 12-hour website outage. Despite sales returning to normal relatively quickly, the company was able to show an ongoing reduction in profits due to the loss of new customer signups during the interruption.

Given that new customers typically stayed with the site for three to four years, the impact of the loss went well beyond the 12 hours in which the website was down. However, the policy only indemnified financial losses for up to three months following the disruption.

Insuring reputation
An area of debate within the cyber insurance market is the insurability of reputational damage. It is arguable that cyber business interruption operates to insure some of the financial effects of reputational damage, including the impact on market share and loss of customers. In the property world, a wellmanaged disruption can shore up customer loyalty, but in the cyber domain, customers may be less supportive, at least where there are alternative suppliers.

Reputational impact is a striking feature of cyber losses and potentially an even more significant driver for business interruption losses than in property. For example, concerns for data security following a breach could deter new customers or affect existing customer contract renewal rates, and these exposures may be insured within the business interruption wordings of cyber policies.

The relevance of reputational damage to cyber business interruption means that careful consideration needs to be given to how a reduction in revenue is calculated and protected by insurance.

What's the aggregate?
As cyber insurance evolves, insurers are having to balance the demands of customers for wider coverages against scant claims history and exposures to systemic risks and aggregation concerns.

For example, supply chain and contingent business interruption risk is particularly challenging to assess and underwrite, with potentially enormous concentrations of risk in the world's cyber network infrastructure. An incident at a major internet or cloud services provider, or a security flaw in a systemic software product, could result in a huge accumulation risk for the insurance industry.

The insurance industry is taking steps to get a better handle on cyber business interruption risk, developing tools to model exposures and partnering with IT security firms to assess risks. Financial regulators have also recently begun to investigate these exposures, asking firms to conduct realistic disaster scenarios to assess their capital adequacy and reinsurance arrangements.

"Actuarial developments will help insurers better understand cyber exposure, including the cause and effect of cyber business interruption. But these developments in exposure will need to be matched with developments in policy wordings," says Allnutt.

"Demand for cyber business interruption is expected to increase, but insurers are having to work from the ground up, in developing appropriate cover," he adds. "As the market evolves, insurers will need to look at the scope of cover they offer very carefully from an actuarial and wording perspective. This is a big challenge. Wordings have yet to be tested in court and there is still only limited actuarial and claims experience for large cyber business interruption losses."

Authors

Hans Allnutt
London - Walbrook
+44 (0) 20 7894 6925
hallnutt@dacbeachcroft.com

Chris Wilkes
London - Walbrook
+44 (0)20 7894 6844
cwilkes@dacbeachcroft.com