IUA OF LONDON
INTERNATIONAL UNDERWRITING ASSOCIATION

Cyber Insurance & Business Interruption

July 2018

A report from the IUA's Cyber Underwriting Group in association with RGL Forensics

RGL Forensics

Table of Contents

Introduction

I am pleased to introduce this International Underwriting Association report Cyber Insurance and Business Interruption.

The continued education of businesses about the cyber risk exposures is an essential task, both at an operational risk management level and in the boardroom. The IUA's Cyber Underwriting Group's Policy Positions Paper has previously highlighted the role that national authorities, insurers and brokers must all play in this process. If they are to obtain suitable security for this increasingly important business risk, then firms must have easy access to information on the status of cyber insurance markets and the available coverage options.

As part of this education process, it is necessary to carefully consider and analyse the pros and cons of existing cyber risk products and extensions to more traditional classes of business – identifying possible problem areas, gaps in coverage and uncertainties. With this in mind our Group is looking to actively engage with market participants and will be using this report to do so.

The document highlights how business interruption cover may respond to cyber risks when compared to more traditional classes of business, such as property insurance and provides examples illustrating some of the nuances involved. It is intended to enable a better understanding of the ways in which a client may be exposed to business interruption and the effect of the forms of cover available under a cyber policy. It does not attempt to answer all questions which may arise, but it should assist market professionals in identifying potential pitfalls and to choose appropriate policy wordings.

This report from the Cyber Underwriting Group would not have been possible without the contribution of the members who proposed the concept and drafted the content and the input of other group members who reviewed it. I would like to extend my thanks on behalf of the committee to those involved in the production of this report.

Matthew Hogg

Chairman of the IUA Cyber Underwriting Group.

Cyber Insurance & Business Interruption

Why Is Business Interruption Relevant To Cyber?

Companies are becoming increasingly reliant on their IT systems to store and process the data that is critical to the continued operation of their business. Historically, companies may have considered cyber to be related to risks associated with data breaches caused by external hackers. Consequently, those companies that did not host confidential data may not have considered themselves to be exposed to a significant cyber risk.

However, cyber refers to anything "computer related", including computer breakdowns or failures, not just malicious attacks. For example, the system outage suffered by British Airways in May 2017 was caused by either an employee or contractor error. This caused the cancellation of flights which impacted approximately 75,000 passengers, resulting in a projected business interruption loss of £80m1[1] .

The WannaCry and Petya/NotPetya ransomware attacks in May and June 2017, which were aimed at computers running Microsoft Windows, also show that cyber-attacks, when they occur, can be indiscriminate and not necessarily targeted towards a specific entity. The consumer goods company, Reckitt Benckiser, has reported an estimated sales loss of £110m as a consequence of the Petya/NotPetya attack[2] .

In this increasingly digital age, organisations rely heavily on their IT systems and networks in many aspects of their business, e.g. storage of key operational data, generating and making sales, automating the production system, or for communication. A failure in any of these services can cause major disruption and hinder the ability of the business to operate as normal, potentially resulting in a significant financial loss. Companies may also suffer indirectly as a result of incidents at their key suppliers or customers.

[1] http://www.bbc.co.uk/news/business-40285288

[2] https://www.ft.com/content/ef641e2e-6214-11e7-8814-0ac7eb84e5f1?mhq5j=e3

Purpose of Business Interruption Insurance

In essence, business interruption insurance covers the profit and loss account of a company, in the same way that property insurance covers buildings and equipment. The intention of this insurance, therefore, is to return the policyholder's profit and loss account to what it would have been, had the insured event not occurred.

In property damage policies, the business interruption coverage is automatically triggered when there is damage to property covered by the policy. The policy will then pay for business interruption losses that flow directly from the damage.

Currently, business interruption in cyber policies tends to be a standalone extension, the triggers for which are separately defined in the policy wording. It should therefore be noted that even though a company may have coverage for a particular type of cyber loss, e.g. the legal costs arising from a data breach, it does not automatically follow that the resulting loss of profits directly caused by that event will also be covered.

Cyber Business Interruption Insurance

For the business interruption section of a cyber policy to be triggered, the majority of current policies require there to be disruption to, or a failure of, the company's IT system or network. This usually requires there to be some degradation in network performance, this degradation being the cause of any interruption to commercial operations.

In general terms, business interruption cover is available for the following cyber triggers:

- Unauthorised use of or access to the network;
- Denial of service attack or denial of access, including ransomware;
- Receipt or transmission of malicious code, including viruses;
- Damage, loss or theft of data, including confidential data;
- Cyber extortion;
- Reputation harm following a cyber event;
- Administrative or operational errors;
- System failure;
- Internal power outage, caused by an external hacker or other operational issue.

It is important to note that the above triggers are not all included in every policy that is currently available. Companies therefore need to ensure that they have identified all of their cyber business interruption risks and that the policy to be bought fully addresses these risks.

Period of Loss

The period of loss in property policies is generally known as the Maximum Indemnity Period. This is specified in the policy and all losses that flow directly from the event will be covered up until the end of this period.

However, the period of loss in cyber policies is generally split as follows:

- Period of restoration, i.e. the time taken before the company's systems are returned to normal operations. This period is usually capped in the policy at between 60 to 120 days.
- Period of extended coverage that commences after the end of the period of restoration. This period provides additional cover for the company in the event that it takes longer for sales to return to their pre-incident level and is usually capped at between 90 and 120 days.

In reality, the impact to the business rarely ends when systems are restored. For example, if a manufacturing business suffers a ransomware attack that impacts its industrial control systems, production is likely to cease while the ransomware is dealt with. However, losses are unlikely to end when the system has been restored, as a) it will take time for production volumes to return to pre-incident levels such that sales losses may continue and b) the manufacturer will then seek to catch up its lost production and, hence, some of the lost sales. This is likely to occur by running additional production shifts or by extending working hours, with the consequential increase in standard and overtime labour costs.

Alternatively, if an online gift retailer suffers a DDoS attack and its website is unavailable, even for a matter of hours, its customers will likely go to another retailer offering similar products for similar prices, rather than waiting for the problem to be resolved. That represents a lost sale for the affected retailer during the period of restoration. It may then take time to get that customer back, who may think of the alternative retailer first for their next purchase. Depending on the timing of this next purchase, this represents a potential loss of sales during the period of extended coverage.

However, this change in customer allegiance may not occur if there isn't a close substitute for the products that the affected retailer sells. For example, after the Sony PlayStation hack of 2011, gamers may have wanted to transfer their business to Microsoft's Xbox platform, but were prevented from doing so by the cost of purchasing the alternative hardware.

While all cyber business interruption policies provide cover for the period of restoration, not all will include a period of extended coverage. What the above therefore highlights is the need for companies, as part of their analysis of cyber risks, to consider the impact on operations of these risks crystallising and the likely duration of this impact. Consideration can then be given to ensuring that the expected periods of interruption match the maximum period of loss provided by the cyber policy.

Basis of Measurement of Cyber Business Interruption Loss

As set out previously, business interruption insurance is concerned with the profit and loss account. The table below shows the expected, i.e. but for the incident, and actual, i.e. post incident, profit and loss accounts in respect of a cyber event.

Description	Expected But For Incident	Actual	Variance
	£'000		
Sales	250	125	125
Variable costs	(100)	(50)	(50)
Gross Profit **Rate of gross profit**	**150** **60%**	**75** **60%**	**75** **60%**
Fixed overheads	(80)	(70)	(10)
Net profit before increased costs of working	**70**	**5**	**65**
Increased costs of working	0	(15)	15
Net profit	70	(10)	80

As can be seen from the table, the company has suffered a loss of £80,000.

The business interruption wording in cyber policies generally adopts one of two approaches to valuing this loss of profit:

1) Loss of gross profit

2) Net profit plus continuing fixed costs

The majority of current cyber wordings currently use the latter of the above two approaches. However, the gross profit approach, which is common practice in UK property policies, is becoming more common in cyber policies written in the London market.

While there are these two approaches to calculating a business interruption loss, it is important to note that the calculations for each approach will result in the same answer, as is shown in the table below.

Loss of Gross Profit	
Description	**Total**
	£'000
Loss of sales Rate of gross profit	125 60%
Loss of gross profit Increased costs of working Savings in fixed overheads	**75** 15 (10)
Total loss	**80**

Net Profit Plus Continuing Fixed Costs	
Description	**Total**
	£'000
Expected net profit Less: Actual net profit before increased costs of working	70 (5)
Loss of net profit before increased costs Increased costs of working	**65** 15
Total loss	**80**

With regard to the Net Profit wording, it is usual for this to include the requirement that any reduction in net profit is attributable to a reduction in revenues that are a direct consequence of the incident. Given this caveat, and the fact that both approaches result in the same answer, it is more likely for calculations of loss to be prepared using the loss of gross profit approach.

This will therefore require consideration of the loss of revenue.

Calculating the Loss of Revenue

In the case of a property loss, the period of interruption can last a couple of months, if not a couple of years. Historic monthly revenue can therefore be used to identify trends over the medium to long term which are then used to calculate what revenue would have been, but for the incident.

Monthly revenue data is less appropriate in cyber as loss periods are generally measured in days, therefore requiring the use of daily, not

monthly data. However, consideration still needs to be given to the correct base period to calculate expected revenue.

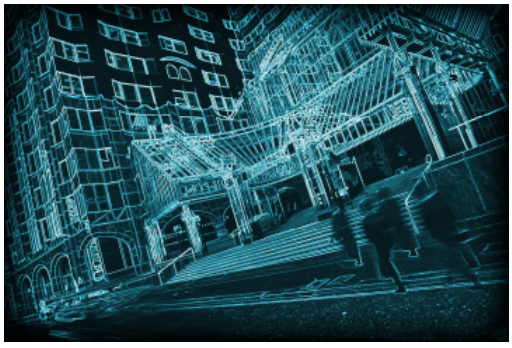
For example, if an online retailer suffers an incident over a weekend, then consideration will need to be given to whether the business generates higher sales at a weekend than during the week. If it does, then weekend sales in the period immediately before and after the incident will need to be reviewed as part of the calculation of expected revenue. If not, then average daily sales may be a more appropriate basis of measurement.

However, if the incident occurs during a peak sales period, Black Friday for example, then pre and post incident sales may not be an appropriate barometer as they are likely to be outside the peak period. In this example, consideration will need to be given to a) the extent of the uplift in sales that has been generated in similar previous peak sales periods and b) the ability of the company to accurately forecast sales in these peak periods. It may also be possible to obtain market data for the relevant period which can also be used to help inform any calculation.

Depending on the nature of the incident and the extent of any competition in that particular retail sector, there may be an extended period of loss, resulting from the fact that customers may not return immediately once the systems are restored. The extent of this loss can be measured by reviewing pre and post incident operational data, such as the volume of website traffic, the conversion ratio of website visits to sales and the average value of each sale transaction.

The above highlights the need to understand a) the business and how and when it generates revenue and b) the specific trading circumstances that existed at the time of the incident. As a consequence of this, each and every loss calculation will be different, as it will need to take into account the specific characteristics of the business impacted by the incident, as well as those of the incident itself.

While any calculation of loss of profit will ultimately use financial data, the above commentary also highlights the need to use other non-financial or operational data as part of preparing any calculation. Most importantly, it emphasises the need to work with the insured entity to ensure that all issues that will influence a calculation are appropriately identified and considered.



Calculating the Total Loss

While daily information will be required to calculate the loss of revenue, it is likely that the monthly management accounts can be used to derive the rate of gross profit. However, consideration will need to be given as to the extent that this fluctuates due to changing trading conditions, as well as general trends. For example, if the incident occurs during a period of discounting, such as Black Friday, then an average rate of gross profit calculated over a longer period of time that includes normal trading may not be appropriate. As with revenue, this highlights the need to engage with the insured entity to understand the business.

The majority of cyber policies provide cover for additional expenses, which are often described as follows:

- Additional expenses;
- Operational expenses;
- Increased costs of working; or
- Interruption expenses.

Irrespective of their title, this section of the policy provides cover for costs incurred by the Insured to either assist a) in continuing normal operations or b) in mitigating and/or reducing the loss of sales. These costs can usually be evidenced by way of invoice. However, where these costs are additional overhead expenses, such as overtime, a review of pre and post incident costs will be required. As with revenue, this review will need to be based on daily, not monthly data.

Some cyber policies, just as with property, require that these increased costs of working are economic, i.e. for every £1 spent, the loss of gross profit is reduced by a similar or greater amount. Analysis will therefore be required to consider the timing of this additional expenditure and when the benefit of this expenditure is realised, which will then need to be compared to the insured period of loss. Early engagement with the insured entity can therefore usually assist in reviewing any loss mitigation strategy.

As to fixed overheads, such as management payroll and property costs, it is unlikely that these will have altered as a consequence of a cyber event, as the interruption period for this type of incident will usually be short in duration. However, if the incident had resulted in a reduction in overheads, then any saving would need to be deducted from the business interruption calculation.

Waiting Periods and Deductibles

Historically, the cyber market has used both waiting periods and monetary based deductibles in its business interruption policies. However, both have their advantages and disadvantages.

The waiting period is set to ensure that attritional losses, or normal operational issues, are not covered under the policy. A company will usually have enough information to show the average period of any short outages that it experiences. Similarly, insurers will have information from their own claims experience. On this basis, a waiting period, say 12 hours, for the policy is agreed.

However, not all Insured's will have revenue data on an hourly basis. This then causes an issue in calculating the losses in the waiting period itself. For example, an incident occurs at an online retailer at 1700, whose cyber policy has a 12-hour waiting period. The retailer advises that the majority of its daily business is transacted between 1600 and 2300, i.e. a 7- hour period, but it does not have the transactional data with which to support this. When adjusting the claim, is it appropriate to a) take an hourly average based on daily sales, knowing that this will be understated when compared to actual hourly sales in the period immediately after the incident or b) exclude losses for the date of incident itself, assuming that losses between midnight and 0500, i.e. the end of the waiting period, will be minimal?

Either of the above approaches to dealing with losses in the waiting period will be imprecise, albeit the monetary value of this imprecision will vary from insured to insured and from claim to claim. It is this type of issue, therefore, that increases the attractiveness of a monetary deductible.

However, when setting the monetary deductible, insurers will still need to understand the potential value of any loss that may occur in the first 12 hours, say, to ensure that the deductible value is set appropriately.

To address the above issues, some cyber policies have introduced a franchise deductible, where if an incident continues beyond a set period, say 12 hours, then the full loss from when the interruption commenced will be covered. Losses where the interruption is for a duration of less than this set period will continue to not be covered.

However, this approach will mean that there is no contribution from the Insured to the overall losses suffered, as there is under a waiting period and monetary deductible. In addition, where a franchise deductible is used, it is likely that insurers will require that the insured undertake their best endeavours to resolve the incident as promptly as possible.

Given the above, there is no right or wrong approach to waiting periods and deductibles. On that basis, insurers and insureds need to work together to establish the best approach for the insured's own particular business.

Measuring the Period of Interruption

The process of identifying the trigger for the purpose of the cyber policy will depend on the type of incident the company endures. However, irrespective of whether the incident results from a DDoS or a system failure, for example, it is important to understand what represents the normal level of network performance.

On this basis, system logs are essential for both establishing when an incident has occurred and when network operations have returned to normal. These logs are normally monitored by a separate application that ingests logs from multiple platforms and provides a dashboard overview of the network's "health status".

However, if logging is not enabled, then this identification and measurement can be difficult due to the following:

- System performance will be subjective and will vary, depending on whether this is considered from a user or administrator perspective. For example, if the user sees that the system is running slowly, they may report a system interruption, when, in fact, the system is underperforming due to resource allocation issues rather than a systemic incident.
- The system may shutdown or halt for a reason that is unknown to the user, administrators or developers. It may be the case that the system is simply processing a substantial amount of data and will eventually catch back up.

In addition, log data may not be retained for a period longer than a month, for example, such that there could be inadequate data available to determine what constitutes normal operations and, therefore, when the period of interruption commences.

Given the above, when reviewing the types of events that may trigger a cyber policy, both insurers and insureds need to consider a) what system performance information is available, b) the period of time for which this information is retained and c) how this can be analysed to determine what represents "business as usual".

Contingent Cyber Business Interruption

In the physical world, supply chains can be long and complicated, as well as spanning multiple continents. Consequently, property damage at a key supplier or customer can be just as detrimental to a company as damage to its own property. Contingent business interruption coverage has been available as part of property policies for a number of years so as to address this type of risk.

Just as physical damage can disrupt a supply chain, so can a cyber event. The global shipping company, Maersk, was a victim of the Petya/NotPetya attack in June 2017, which meant that it was unable to

dock and unload containers at some of its 76 ports worldwide[3] . This had the consequential effect of causing disruption to those companies awaiting delivery of the products and materials held on those vessels that were unable to dock.

This type of issue is not limited to cyber risks within the physical supply chain. For example, Amazon Web Services suffered an outage in February 2017 due to human error. This not only interrupted its own services, but also took down a large number of company websites for approximately four hours. It has been estimated that this single event caused business interruption losses of between $150m and $160m to S&P 500 companies and a further $160m of losses to US financial institutions[4].

The impact of this type of incident on a single company will be greater if a number of its suppliers within its own supply chain use the same cloud or outsourced services provider, given that a greater proportion of the supply chain will be disrupted. The above incident therefore illustrates how one event can impact multiple companies. It is therefore critical that companies consider all cyber risks within their own supply chain to ensure that these types of contingent business interruption risks are identified.

Contingent business interruption insurance is currently available in the cyber market, usually with sub-limits, under the following types of cover:

- Cloud providers/IT service providers;
- Outsourced service providers;
- Named providers; and
- Any provider of any service with whom there is a contract between the Insured and the third party.

However, as with property, this section of the policy will usually only respond if the cyber event at the supplier would have triggered the company's own cyber insurance if they had been the victim of the same event.

This is usually straightforward in the property market as fire and flood events, for example, are widely reported and can be easily identified. However, this may be less straightforward in the event of a cyber incident, as the supplier may not be willing to share the full facts of the incident. Companies may therefore wish to consider the wording of their supply agreements and how information regarding cyber events are shared, given the impact that this may have on cyber business interruption insurance.

---

[3] https://www.ft.com/content/b8432fc4-60c1-11e7-91a7-502f7ee26895?mhq5j=e3
[4] http://www.datacenterknowledge.com/archives/2017/03/02/aws-outage-that-broke-the-internetcaused-by-mistyped-command/

Summary

It is clear that the cyber risks faced by a business can be complex. The business interruption consequences of a cyber incident can also be significant. It is therefore crucial that companies fully explore the possible ways in which cyber events could affect their business and therefore identify the key operational risks.

As cyber is a relatively new and ever developing area of insurance, policy coverage and wordings can vary considerably. It is therefore important for companies to compare these wordings to their key risks to ensure that the coverage that is bought meets the needs of the business.

Given that cyber business interruption coverage is not standard across the market, a three-way conversation between the company, their broker and underwriters will assist in ensuring that the cover that is purchased will respond appropriately in the event of a loss.

Published by:

The International Underwriting Association of London Limited

In association with

RGL Forensics

Dashwood

69 Old Broad Street

London, EC2M 1QS

With special thanks to Ben Hobby, RGL Forensics, who wrote the report and Matthew Hogg, Chairman of the IUA Cyber Underwriting Committee who proposed the scope of the report.

International Underwriting Association

1 Minster Court
Mincing Lane
London
EC3R 7AA

Tel 020 7617 4444
Email info@iua.co.uk
Web www.iua.co.uk
Twitter @IUAofLondon

The International Underwriting Association of London (IUA) is the focal representative and market organisation for non-Lloyd's international and wholesale insurance and reinsurance companies operating in the London Market. It exists to promote and enhance the business environment for international insurance and reinsurance companies operating in or through London.