Cyber Risks and Insurance

An Introduction to Cross Class Cyber Liabilities

January 2016

IUA OF LONDON
INTERNATIONAL UNDERWRITING ASSOCIATION

NORTON ROSE FULBRIGHT

Report Details

Published by:

International Underwriting Association of London Limited

1 Minster Court

Mincing Lane

London EC3R 7AA

United Kingdom

Telephone +44 (0)20 7617 4444

Email: info@iua.co.uk

In Association with Norton Rose Fulbright LLP:

Ffion Flockhart	Partner
Steven Hadwin	Associate
Charlie Weston-Simons	Senior Associate
Chris Zavos	Partner

First Published: January 2016

Cyber Risk and Insurance – An Introduction to Cross Class Cyber Liabilities

Table of Contents (hyperlinked)

Cyber Risk and Insurance – An Introduction to Cross Class Liabilities

The Purpose of this Paper

This paper is an analysis of whether conventional lines of insurance might provide cover in respect of the ever-expanding scope of cyber risk which is now faced by organisations in a broad range of locations and industry sectors.

Following a brief introduction into what is meant by 'cyber risk', the paper uses a number of possible factual cyber risk scenarios in order to explore the extent to which conventional lines of insurance may provide cover.

As part of the analysis, reference is also made to the exclusions commonly found in conventional lines of insurance and the extent to which they exclude the scope of cyber risks facing insureds.

The paper concludes with an analysis of the cyber insurance market and in particular, how separate cyber insurance cover (by way of extensions in existing insurance policies, drop-down cover or comprehensive standalone cyber insurance policies) might respond to fill the gaps in cover where conventional lines of insurance do not respond or where exclusions preclude cover for cyber risks.

What is Cyber Risk?

Cyber risk has been described as the "*biggest, most systemic risk*" facing the insurance market in the last half century. It essentially encompasses any risk arising out of the use of technology and data and, in this digital age, affects virtually every organisation around the world.

The risks captured under the cyber umbrella are both first-party and third-party in nature, ranging from cyber extortion to regulatory investigations and, in extreme cases, death or bodily injury.

In terms of scale, statistics suggest that the number of cyber incidents in 2014 reached a daily average of 117,339, with 81% of large businesses and 60% of small businesses suffering a cyber security breach – almost double the figures for the previous year. From a costs perspective, it is now estimated that cyber risks cost businesses some $400 billion every year.[1]

---

[1] Information taken from PwC's 'The Global State of Information Security® Survey 2015' HERE and Cybersecurity Ventures 'Cybersecurity Market Report' HERE

High-profile adverse cyber incidents – such as the recent data breaches at large US retailers and online businesses, as well as the recent issues affecting businesses such as the TalkTalk Group and Morrisons in the UK – demonstrate how cyber risk can have a fundamental impact on organisations in a broad range of sectors. Recent studies have also analysed the enormous losses which could result from a catastrophic, systemic cyber loss – such as an adverse cyber incident affecting the provision of essential utilities to areas of high population and economic activity.[2]

Legislators worldwide are also taking an increasing interest in this area, which is leading to organisations being required to meet higher standards than ever in terms of their cyber risk management. A prominent example of this is the proposed EU General Data Protection Regulation (GDPR), which will make organisations which process the personal data of EU residents potentially subject to fines of up to 4% of their global annual turnover if they breach their data protection obligations. The Regulation will also provide greater rights for data subjects, more extensive data breach notification provisions and, in certain circumstances, requires companies to appoint a Data Protection Officer.

The risk of litigation arising from the misuse of data is also growing in a number of jurisdictions. The implementation of the GDPR, coupled with heightened litigation risk, is expected to increase demand for separate cyber insurance cover. A recent study predicted that this process will lead to the global cyber insurance market growing to $20bn in premium by 2025.[3]

It is also an increasing boardroom concern, given the potential personal liability that directors and officers may attract from the failure to put measures in place to manage the growing cyber risks faced by their organisation properly. Some high-profile data breaches have already led to shareholder class actions being brought against company boards for breach of duty – this trend seems set to continue with the growing expectation that cyber risk will be managed at board level.

The Future of Cyber Risk

Cyber risk is growing in prominence in a number of respects. As well as the forthcoming legislative changes under the proposed GDPR, which will have a significant impact on the cyber liability profile of a broad range of organisations, a number of recent developments highlight the growing prominence of cyber risk.

---

[2] See for example, 'Promoting UK Cyber Prosperity: Public-Private Cyber-Catastrophe Reinsurance' HERE (A Long Finance report prepared by Z/Yen Group Co-sponsored by APM Group).

[3] Taken from the 'A Guide to Cyber Risk' Allianz Global Corporate & Specialty, HERE.

In addition to legislative change, regulators are paying close attention to the management of cyber risk and how it affects the operation of the insurance market. The Prudential Regulation Authority (PRA) has recently launched a probe into the cyber risk preparedness of insurers. This reflects the risk position of insurers who, as well as having to manage their own cyber risk position, are taking on much of the cyber risk which is faced by their insureds by underwriting cyber business.

Further details on legal and regulatory developments affecting the cyber risk landscape are set out later in this paper.

How is Cyber risk currently understood by Insureds and Insurers?

Despite the increasing media coverage on the cyber risk that organisations now face, understanding of what cyber risk encompasses and how it can be mitigated remains in a developmental phase. For example, there is a tendency to treat cyber risk as being synonymous with malicious hacking. While hacking is of course an important source of cyber risk, it is worth noting that the majority of cyber incidents reported to insurers are the result of accidental acts or omissions.

The effects of cyber risk are also often underestimated. As demonstrated in this paper, the range of possible losses arising from a cyber incident is broad and can include damage to physical property, bodily injury and reputational damage – as well as more obvious types of loss such as loss of data and business interruption.

From an insurance perspective, many insureds still take the view that their existing forms of cover will respond to the full range of cyber risks they face. However, the overall scope of cover available under conventional lines of insurance often means that gaps in cover might arise where cyber risks are concerned. Standalone cyber insurance, as well as extensions or drop-down cover that are used to enhance the cover provided in conventional lines of insurance, are aiming to address these gaps. If the trend in the US is any indicator of the likely trend elsewhere, these additional protections for cyber risk are set to grow in prominence as cyber risk continues to expand.

Data privacy law in Europe – a state of flux

A key aspect of the evolving cyber risk landscape is the on-going development of data privacy law in Europe, which is seeing organisations face greater liability risks in relation to the use of data than was previously the case.

The implementation of the GDPR will have broad implications for data protection law in Europe. Stricter rules will be imposed on data controllers in relation to data subject consent, data profiling, data handling and compliance. These rules will be enforced by reference to aggressive mandatory reporting requirements and potentially heavy penalties for contravention.[4]

However, legislative reform is only one aspect of the changing legal and regulatory landscape in Europe when it comes to data protection. Other legal developments suggest a shift towards greater risks of legal and regulatory liability being imposed on companies for matters related to data privacy and cyber risk more generally.

In England & Wales for example, a recent Court of Appeal judgment in the ongoing case of Vidal-Hall et al v Google[5] has potentially broadened the circumstances in which companies can face liability arising out of data privacy issues in two ways. First, the judgment established that tortious claims for misuse of private information can be brought in the English Courts. Second, the judgement made important findings on the damages to which data subjects may be entitled if they consider their data is misused. Under s13 of the Data Protection Act 1998, individuals who suffer damage by reason of any contravention, by a data controller, of any of the requirements of the Data Protection Act are entitled to compensation from the data controller for that damage. The judgement held that the scope of "damage" in this context was not limited to pecuniary loss. This means that damages may be awarded in cases of this nature for non-tangible loss including emotional distress resulting from the misuse of private information.

The Court of Justice of the European Union's recent decision in Schrems[6] saw the US / EU "Safe Harbor Framework" – a set of guidelines which simplified the process of transporting personal data from the EU to the US in a way which was legally compliant – being declared invalid. The effect of this decision is that organisations can no longer rely on the existing Safe Harbor framework as a legal ground for exporting personal data to the US. Instead, organisations will need to seek to justify transfers of data on alternative grounds, such as the use of model data protection clauses when dealing with data subjects or reliance on specific derogations from the general requirement that adequate data protection has been provided. It appears, however, that

---

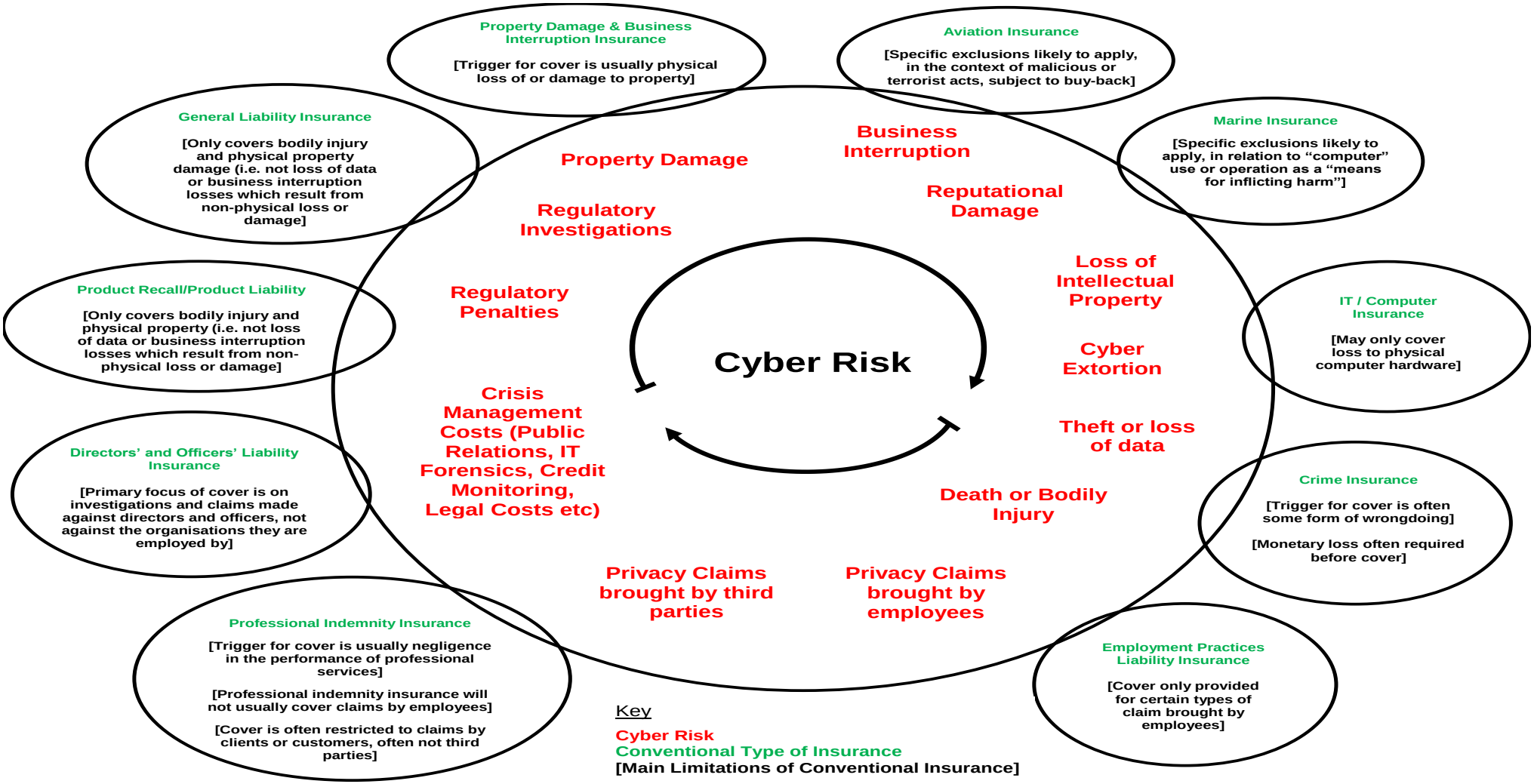
4 See HERE for further details of the EU work on data protection, including a precis of the latest proposals which were agreed by the European Parliament, the Council and the Commission in December 2015.

5 [2014] EWHC 13 (QB), judgement HERE.

6 Judgement of the Court (Grand Chamber) of 6 October 2015 (request for a preliminary ruling from the High Court (Ireland)) — Maximillian Schrems v Data Protection Commissioner (Case C-362/14).

the *Schrems* decision has also cast doubt over the adequacy of some of these alternative forms of protection. While steps are being taken to agree and implement “Safe Harbor 2.0” - a revised version of the previous framework which would satisfy EU law requirements and would allow organisations to rely on the framework once again - there is presently a degree of uncertainty over whether organisations that transfer data from the EU to the US can fully comply with their data protection obligations. This could leave those organisations exposed to regulatory investigations and / or penalties. Claims may also be brought by data subjects, who may have rights under national law to claim compensation as a result of the organisation breaching its legislative obligations in relation to data protection. While data protection regulators are not expected to pursue organisations that previously relied on the Safe Harbor framework aggressively, the fact remains that, for now at least, organisations transferring data from the EU to the US face a greater regulatory liability risk than was previously the case.

Cyber Risks and the cover provided by traditional lines of Insurance



The Scenarios – Executive Summary

Conventional insurance

- The Scenarios set out in the paper demonstrate that conventional lines of insurance may sometimes, directly or indirectly, provide cover for certain cyber risks. Insurers and insureds may not be fully aware of the scope of cyber risk which is being underwritten in these lines of insurance. See, for example, the D&O and Professional Indemnity scenarios.

- The scope of insuring agreements and triggers for cover in some conventional lines of insurance mean that cover might not be provided in respect of cyber-related perils, in circumstances where there may be an expectation that cover would be provided. See, for example, the Property Damage and Business Interruption scenarios.

- Exclusions that are commonly used in relation to a number of lines of insurance may operate to preclude cover for some cyber-related perils. Key examples of these exclusions include CL380 (see the Marine Hull, Energy and Marine Cargo scenarios) and AVN48B (in relation to the Aviation scenario). Other exclusions which are not specifically aimed at cyber-related perils may also preclude cover, as demonstrated by the Terrorism, General Liability and Crime scenarios – a number of exclusions can be found below.

Cover for Cyber risks

- Cyber-related perils present a broad range of first party risks such as property damage, business interruption, theft or loss of data and rectifications costs, as well as a range of third-party liability risks such as the risks of litigation and regulatory investigations.

- Cyber-specific wordings and products may be an effective means of 'filling the gaps' in cover which exist in conventional lines of insurance in respect of this broad risk landscape. See the summary of the cyber insurance market for more details.

The Scenarios – The Legal Position on Exclusions

Conventional insurance and exclusions affecting coverage of cyber risk

The applicability of exclusions in conventional lines of insurance – be they specific cyber risk exclusions or otherwise – is an important aspect of this paper and a key consideration when analysing when cyber risks will be covered under conventional insurances.

In many circumstances and as will be seen from the various scenarios in this paper, cyber risk may be one of a number of causes of a loss. These causes may be specifically covered under a particular insurance policy, not specifically covered or specifically excluded.

It is therefore worth summarising the general position under English law in circumstances where cyber risk is one of a number of causes of loss. It is an important principle of English insurance law that an insurer will only be liable for losses proximately caused by the peril covered by the policy. “Proximate cause” in this context refers to the dominant, effective or operative cause of the loss.

It is possible for there to be multiple proximate causes of a loss which operate concurrently. An important issue is therefore whether an insurer will be liable in circumstances where not all of the proximate causes of a loss relate to perils that an insurer is underwriting. In these circumstances, the current position as a matter of English law is generally as follows:

- Where there are two proximate causes of loss, one of which is specifically covered and the other is neither specifically covered nor specifically excluded, the insurer will in principle be liable for the loss.

- Where there are two proximate causes of loss, one of which is specifically covered and the other is specifically excluded, the insurer can rely on the exclusion in relation to the entire loss.

This paper considers the position under English law as it stands today and not as may be amended by the coming into force of the Insurance Act 2015 in August 2016. In particular, in considering the scenarios below, it should be remembered that the Act will (unless insureds / insurers are able to and do contract out of it) change English law in relation to the remedies available to insurers where there has been a breach of the insured’s duty to make a fair presentation of the risk, in relation to the effect of breach of warranty and concerning the extent to which insurers can rely upon non-compliance with certain policy terms and conditions (which may extend to exclusions).

Scenario – Marine Hull

Facts

Two vessels are insured against marine risks in the London market under English law policies incorporating ITC-Hulls (01/10/83) and the Institute Cyber Attack Exclusion clause (10/11/03 – CL380) (**CL380**).

Vessel A is trading and uses ECDIS (Electronic Chart Display & Information System), which is updated via the internet. Vessel B is laid up in a recognised anchorage and complies with applicable lay-up requirements. Vessel A sails into the anchorage and strikes Vessel B. On investigation, it transpires that the anchorage had been shown on the ECDIS chart until updated via the internet, two weeks prior to the collision. The update had deleted the reference on the chart to the anchorage by reason of a malicious code or software programme inadvertently loaded with the update. The officer on watch had not sailed in that area previously and had not been keeping a proper lookout. Subsequent investigation reveals the presence of the malicious code or software programme but is unable to identify the source of the code/programme or its author. There is no evidence to suggest that the author of the code/programme was a terrorist or acting from a political motive (see clause 24.2 of ITC-Hulls).

Analysis

The coverage position – subject to CL380 - is broadly as follows:

a) Vessel A has a claim for damage to the vessel caused by a peril of the sea and/or crew negligence (subject to issues around unseaworthiness (s39(5) Marine Insurance Act 1906) around crew competence and the due diligence proviso in relation to the crew negligence peril) and for an indemnity in respect of 3/4ths collision liability, if liable at law for the collision; and

b) Vessel B has a claim for damage to the vessel caused by a peril of the sea.

How does CL380 impact the above?

The key issues are whether the H&M insurers of Vessel A could, if they so wished, seek to rely on CL380 in response to the claim. At the very least, the collision was indirectly caused by or contributed to or arose from the use of a malicious code or software programme – arguably a "*cyber-attack*". The opening words of CL380 are very broad and displace the usual rule that insurers need to show that the malicious code or software programme was the proximate cause of the loss. It would be sufficient for the insurers to show that they were a remote cause of the loss.

The issue then arises whether insurers need to show that the code was "*malicious*" or simply a "*non-malicious*" software programme. Either way, insurers would need to show it was used or operated as a "*means for inflicting harm*".

There is no case law which assists in understanding what is meant by these words. On the face of it, "*as a means*" suggests that the purpose is to achieve harm – in other words a means to an end.

The word "*inflict*" suggests a deliberate act – i.e. intention – which is consistent with the "*cyber-attack*" heading to the clause. However, it is uncertain whether, for the purposes of the clause, insurers would need to show that there was an intention to harm the assured or whether it is simply an intention to inflict harm. CL380 is silent on whether an intention to inflict harm on the assured is required. An intention to inflict harm – without targeting any particular victim – may be sufficient. It seems inherent in the use of a "malicious code" that the author may not know where the code will end up or whether the security safeguards at the end user will prevent it from being effective. But can the same be said of a "*non-malicious*" software programme?

In this context, "*harm*" is wider than loss or damage and has been broadly construed in a criminal context (see R v Lewys Martin [2013] EWCA Crim 1420) under the Computer Misuse Act 1990: "*it is of little moment to the victims of such crimes that the offender may be motivated by bravado … rather than by financial gain. The capacity for harm is very great either way*". On that basis, "*malware*" or "*malicious code*" might of themselves be treated as a "*means for inflicting harm*" - but a defective software programme – which produced unexpected results – would not so qualify.

It is doubtful whether a code can itself be "*malicious*", as opposed to a code created with malicious intent. In a marine context "*malicious*" means "*spite, or ill-will, or the like*" (see the *Mandarin Star* [1969] 1 Lloyd's Rep 293). It was considered again in the Grecia Express [2002] EWHC 203, where, following the Malicious Damage Act 1861, the Court held that the words "*any person acting maliciously*", "*cover casual or random vandalism and do not require proof that the person concerned had the purpose of injuring the assured or even knew the identity of the assured*". This was followed in the North Star [2005] EWHC 665 and the B Atlantic [2014] EWHC 4133. Although these cases concern the peril of "*any person acting maliciously*", it is at least arguable that they also apply to the meaning of "*malicious*" in the context of an exclusion – such that identifying the perpetrator or the perpetrator's intent is not necessary for the exclusion to apply.

That said, in a non-marine case (Tektrol v International Insurance Co of Hannover [2005] EWCA Civ 845), the Court of Appeal held that an exclusion in respect of "*erasure, loss, distortion or corruption of information on computer systems … caused deliberately by rioters, strikers, locked-out workers, persons taking part in labour disturbances or civil commotion or malicious persons*"

only applied where the assured was specifically targeted. Buxton LJ put it this way: "*the clause does not extend to interferences by such people that are not directed at the computer systems, etc, used by the insured at the premises. If the insurer wished to exclude all damage caused however indirectly by a computer hacker he needed to place that exclusion in a separate clause, and not refer to malicious persons in the same terms as rioters or locked-out workers*."

It seems likely that CL380 would not be so limited, given it is a stand-alone provision.

Summary (for both the Energy and Cargo scenarios)

It is plainly arguable that any claim by Vessel A would be precluded by the terms of CL380, notwithstanding that an insured peril has operated.

It is also arguable that any claim by Vessel B would similarly be precluded or at least that the position is uncertain, in circumstances where Vessel B appears entirely innocent.

Scenario – Marine Energy & Cargo

Energy

Facts

A mobile offshore drilling unit is insured against all risks of loss or damage (including war risks) under an operating policy incorporating CL380.

The unit relies on a computer-controlled DPS (dynamic positioning system) to fix itself over the drill site. The system is remotely accessible through the internet for monitoring purposes. In adverse weather, the unit suffers a loss of dynamic positioning control causing it to move off the drill site, resulting in damage to the risers and subsequent release of drilling fluids. On investigation, it is discovered that the DPS was targeted by hackers, who had disabled it at the time of the adverse weather.

Analysis

The coverage position –- subject to CL380 - is broadly that there has been fortuitous loss and damage, amongst other things, to the risers. However, the same issues arise under CL380 as in the marine hull scenario.

Additional observations which are specific to this scenario include:

a) the disabling of the DPS at the very least contributed to the damage to the risers, thus potentially bringing any claim within the broad opening words of CL380;

b) the adverse weather may have been an operative peril too; as discussed previously in this paper, where a loss is proximately caused by two competing perils, one of which is covered and the other excluded, then, if the exclusion applies, it will prevail; and

c) if a computer was used to disable the DPS then the issue arises whether, in order successfully to establish that the exclusion applies, insurers would need to identify the hackers. It is arguable that CL380 does not require such identification, provided that the insurers can establish that the loss arose from *"the use or operation"* of a computer *"as a means for inflicting harm"*.

Marine Cargo

Facts

A consignment of a new model mobile phone destined for a launch in London is stored at a container terminal, mid-transit. The shipment is insured for transit and storage risks against all risks under the Institute Cargo clauses (A) and Institute War and Institute Strikes clauses. The policy incorporates CL380 (un-amended).

The port has a computerised container tracking system. This is targeted by hackers who install password capture devices and are subsequently able to infiltrate the IT systems of the container terminal. Hackers identify the container with the mobile phone consignment and generate new dispatch codes causing the container to be shipped to another destination, and the consignment is lost.

Analysis

Prima facie, there is cover for theft under the Institute Cargo Clauses (A). Again, the issues arising on the application of CL380 (un-amended) are similar to those in the Marine Hull scenario. The hacking of the tracking system at the very least "contributed to" the theft and involved the "use or operation of a computer …as a means for inflicting harm". It may not be necessary for insurers seeking to rely on CL380 in these circumstances to identify the thieves.

However, in cargo policies in particular, it is very common to find that CL380 is amended to reduce its scope, such that the amended CL380 does not apply where the use or operation of a computer (and so on) "facilitates" the theft or taking of insured property. On the scenario above, under an amended CL380 provision, there would not be grounds for relying upon the cyber exclusion.

Summary

In both the Energy and Marine Cargo scenarios, it certainly appears arguable that CL380 would apply so as to preclude cover under Energy and Marine Cargo policies.

Again, the requirement of a "*malicious act*" is important to the application of the exclusion.

Scenario - Aviation

Facts

An aircraft is insured for property and certain liability risks under AVN1D (or AVN1C, also commonly used). The principal cover is against physical loss or damage, subject to exclusions under AVN48B (see the appendix to this paper for the full text of the exclusion). It provides "*this Policy does not cover claims caused by … any malicious act or act of sabotage*". These risks are subject to write back under the provisions of one of the AVN52 clauses and separate sub-limits[7].

Air traffic control is hacked in the country in whose airspace the aircraft is flying. The hackers use air traffic control to re-route the aircraft intending to keep the aircraft in the air until it runs out of fuel. This necessitates an emergency landing at another airport. The emergency landing causes damage to the aircraft, damage to a number of other aircraft on the ground at the airport and personal injury to passengers.

There is no evidence that the hackers were acting for political or ideological purposes although the hacking does appear to have been perpetrated deliberately. An indemnity is sought under the insurance policy in relation to all losses resulting from the incident.

Analysis

On the face of it, there is cover under AVN1D (or 1C) for the physical damage to the aircraft and liability for bodily injury and property damage to passengers and third parties. However, should the AVN1D (or 1C) underwriters establish that the hacking was "*malicious*", then claims may be excluded under AVN48B.

The exclusion of *"any malicious act*" is not limited to acts on board the aircraft and for the reasons provided under the marine scenario, the deliberate hacking of air traffic control may qualify as malicious (even if the perpetrators cannot be identified or it cannot be shown that this insured was targeted). However, risks of "*malicious acts*" are covered under the war covers and subject to the possibility of an aggregate limit of three times the top hull value under the war covers, the distinction may not ultimately be significant in this context (putting to one side difficulties as to which policy should respond).

The distinction with CL380 is that the scope of the "*malicious acts*" exclusion under AVN48B is narrower. The broad opening words (*"directly or indirectly caused by or contributed to by or*

[7] The suite of AVN52 clauses can be accessed HERE and HERE.

arising from") found in CL380 are not replicated in AVN48B. It would be incumbent on insurers in this context to show that the, or a competing, proximate cause of the loss was a "*malicious act*".

Summary

The application of AVN48B may prelude this specific cover if it can be shown that the hackers were acting maliciously, but the scope of AVN48B in terms of proximate cause and "non-malicious" computer use is considerably narrower than CL380.

Scenario - Directors and Officers Liability Insurance

Facts

The board of directors of a listed company is covered by a D&O insurance policy which is generally market standard in terms of scope of cover and applicable exclusions. A director of the company loses a laptop containing the details of two million customers. At the time the laptop was lost, the director was using it off-site to upload photographs of a recent vacation.

The director seeks legal advice and, as a result, a notification of the lost customer details is made to the Information Commissioner's Office in the UK (the ICO). The ICO advises the company to notify its customers without delay and, in the course of doing so, news that the laptop has been lost is leaked to the press. Severe reputational damage is caused and the company's share value decreases.

The company's shareholders bring an action against the directors (the **Shareholder Action**) on the basis that, in failing to implement adequate cyber security measures that could have prevented the loss from arising, the board members breached their statutory duties. A number of customers also threaten legal action against the company as well as the individual director at fault for breach of privacy (the **Privacy Action**).

The directors make a claim under the company's D&O policy, seeking to recover:

(i) the legal costs associated with notifying the ICO and the company's customers (the **Notification Costs**); and
(ii) the costs of defending both the Shareholder Action and the Privacy Action.

Analysis - Coverage

In general terms, D&O policies cover the costs, expenses and liabilities incurred by (or on behalf of) directors and officers as a result of claims made against those individuals by third parties or regulatory investigations into the conduct of those individuals.

The first question to ask in the context of this scenario is whether the directors are "insureds" under the Policy. In principle, they ought to fall within this definition, subject to one possible caveat in relation to the director at fault. The caveat is that the D&O policy may only respond when individuals are acting in their insured capacity – i.e. in their capacity as directors. As such, while each member of the board is likely to fall within the definition of "*insured*" for the purposes of the Shareholder Action (on the basis that such action relates to the general failure to put in place adequate cyber security measures), the position may not be as straightforward in relation to the director at fault in the context of the threatened Privacy Action. Arguably, that director was not

acting in his insured capacity at the time the laptop was lost and, as a result, coverage may not be available.

The next question to consider is the extent to which a typical D&O insuring clause responds to the losses for which recovery is sought in this particular scenario.

The trigger for cover usually depends on the definition of "*claim*", which can vary in scope from policy to policy. The definition of "*claim*" is likely to include the Shareholder Action and also the threatened Privacy Action. While regulatory proceedings or investigations may also fall within the definition of "claim" (or may otherwise appear in a separate insuring clause), the notification, which was made voluntarily to the ICO, is unlikely to constitute a regulatory proceeding or investigation for these purposes. Even if the notification itself did fall within the relevant definition, the Notification Costs are more likely to be met by the company rather than the individual directors. While the company itself may well be an "*insured*" under the D&O policy in certain respects (e.g. "Side B" cover, where the company is reimbursed for any indemnity it provides to a director in respect of that director's liability), the company is not likely to be covered for its own losses or liabilities, at least not of this nature.

Accordingly, the Notification Costs are unlikely to be covered. However, to the extent that the ICO or any other regulator launches a formal investigation into the systems and controls of the company (e.g. regarding IT security), the costs incurred by the directors in co-operating with the regulator's enquiries are likely to fall for cover under the D&O policy.

As for the directors' costs of defending the Shareholder Action, these ought to fall within the insuring clause, as should any relief ultimately awarded by the court. The same should be the case in relation to the Privacy Action, subject to the caveat above in relation to the director at fault if he was found not to be acting in his insured capacity.

Exclusions

D&O policies do not generally incorporate specific exclusions relating to cyber risk.

However, D&O policies do often exclude claims brought by one insured against another under an "*Insured v Insured*" exclusion. As shareholder derivative actions are strictly speaking brought in the name of the company (which is likely to fall within the scope of the definition of "*insured*" for these purposes), this exclusion may be relevant. Insured v Insured exclusions do however vary in scope and frequently contain a carve-back of cover for shareholder derivative actions.

Standard policy exclusions may also apply if the directors have committed deliberate wrongdoing. A finding of wrongdoing may, in these circumstances, trigger a right for the insurer to be

reimbursed for any defence costs advanced to the relevant director or officer in relation to the particular claim.

Furthermore, if the regulator were to become involved, any subsequent fine may also be expressly excluded (or may otherwise be uninsurable by law).

Summary

Cover is likely to be available to insured directors in respect of the Shareholder Action and the Privacy Action, subject to the usual policy exclusions for deliberate wrongdoing and insurability.

The limitations relating to insured capacity create a potential coverage issue for the director threatened by the Privacy Action.

Scenario - Professional Indemnity

Facts

A professional services firm (the **Firm**) is insured under a professional indemnity insurance programme which is broadly market-standard in terms of scope of cover and exclusions.

The Firm erroneously compromises confidential data relating to a client, who is a high-profile individual. The Firm lost the data by emailing electronic documents containing sensitive information belonging to that client to the wrong email recipient. The intention was to send the data to the client, but an employee of the Firm used an incorrect email address.

The client becomes aware of these events and sues the Firm in contract and in tort for negligence and misuse of private information (the **Litigation**). The Information Commissioner's Office (**ICO**) becomes aware of the matter and begins an investigation (the **Investigation**).

The employee whose error led to the data being lost is dismissed by the Firm. That employee makes a Data Subject Access Request pursuant to the Data Protection Act 1998 in order to obtain copies of all information that the Firm holds on him, with a view to contesting his dismissal (the **Data Subject Access Request**). The employee had worked at the Firm for many years and the volume of information held by the Firm in relation to him is vast.

The Firm seeks an indemnity under its professional indemnity insurance programme for (i) the costs of defending the Litigation and any damages award made in relation to it; (ii) the costs of dealing with the Investigation and any regulatory penalties imposed in relation to it; and (iii) the costs of dealing with and responding to the Data Subject Access Request.

Analysis - Coverage

In general terms, professional indemnity policies cover the costs, expenses and liabilities incurred by an organisation (or any individual insured within that organisation) arising from claims alleging negligence and/or certain other types of wrongdoing in the performance of professional services.

In relation to the Litigation:

a) The claim being brought alleges negligence on the part of the Firm as well as misuse of private information. This is likely to fall within the definition of "Claim" in the professional indemnity policy, which typically includes formal allegations of wrongdoing made against the insured in the conduct of its business.

b) The allegations of negligence and misuse of private information relate to the performance of professional services carried out by the Firm, since it appears that the documents were being sent to the client as part of the services which the Firm was providing.

This means that, in principle, cover is likely to be available in respect of the costs of defending the Litigation as well as in respect of any damages award made in it.

In relation to the Investigation:

the actions of the regulator may also fall within the definition of "*Claim*" in the policy or be covered under a separate element of cover for regulatory investigations. This means that cover is also likely to be available in principle in relation to the costs of dealing with the Investigation. Whether cover is available for any fines or penalties ultimately imposed by the ICO will depend on whether there is an exclusion for fines and penalties in the policy wording. In addition, if a fine or penalty is imposed for intentional, reckless or negligent conduct, the fine or penalty may not be insurable as a matter of law, essentially for reasons of public policy.

In relation to the Data Subject Access Request:

a) it is unlikely that the Data Subject Access Request would fall within the definition of "Claim" since it does not constitute a demand or proceeding brought against the Firm or an insured individual – rather, it is a request for information under the Data Protection Act 1998; and

b) the request does not appear to arise out of the firm's provision of professional services as it has been made by a former employee rather than a customer or client.

It therefore seems unlikely that cover will be available in respect of costs which the Firm incurs in dealing with and responding to the Data Subject Access Request. These costs are likely to be significant given the employee has worked at the Firm for many years and the volume of information which the Firm held on him was vast.

Exclusions

Professional indemnity policies generally do not incorporate any specific exclusions relating to cyber risk. The main coverage issues therefore relate to the scope of cover provided under the policy's insuring agreements, as described above.

Summary

Cover may well be available in respect of the Litigation and the Investigation, although the insurability of fines and penalties arising out of the Investigation is questionable. Cover in respect of the Data Subject Access Request is unlikely to be available.

Scenario – Property Damage and Business Interruption

Facts

A manufacturer is insured under a property damage and business interruption (**PDBI**) insurance programme which is broadly market-standard in terms of scope of cover and exclusions.

The manufacturing equipment at an insured factory is controlled by software which is corrupted by malicious code. The corruption of the software causes the manufacturing equipment to break down, which means that no production occurs in the factory for a period of 36 hours (the **Incident**).

The manufacturing equipment at the factory uses large volumes of corrosive liquid chemicals in its manufacturing processes. Following the Incident, the malicious code causes the equipment to discharge liquid chemicals in the factory building in a way which causes substantial physical damage to the building and its contents and forces the factory to cease production for a number of weeks (the **Factory Damage**). The Factory Damage includes the destruction of a number of servers containing valuable data which had been created as a result of extensive research and development.

The manufacturer seeks an indemnity under its PDBI Insurance programme for (i) business interruption losses caused by the Incident; and (ii) property damage and business interruption loss caused by the Factory Damage (including the loss incurred as a result of the destruction of the data which was stored on the servers).

Analysis

In general terms, PDBI policies cover:

(a) physical loss or damage to insured property and contents. The insured property is likely to include the manufacturer's factory and therefore the manufacturing equipment in it; and

(b) cover for business interruption loss, which is contingent on direct physical loss or damage to the insured property.

In relation to the claim for business interruption loss caused by the Incident, the trigger for such loss was the malicious code. Given that no "physical" damage was caused to the equipment, business interruption cover is unlikely to be triggered in respect of the Incident. While not binding in England & Wales, recent authority from New Zealand which the English courts may find persuasive has reaffirmed that, where the physical condition of the equipment has not been impaired, a requirement of physical loss or damage will not have been satisfied (see, in particular, Kraal v Earthquake Commission [2014] NZHC 919).

Exclusions

Most PDBI policies exclude cover for "*insured loss… resulting from the loss, damage, destruction, distortion, erasure, corruption or alteration of electronic data*". The value of the lost data and related restoration costs are therefore unlikely to be covered. In addition, if the lost data is a contributing cause to the business interruption costs caused by the Factory Damage, the manufacturer may find it difficult to recover its losses in light of the electronic data exclusion, given that the business interruption costs would most likely be seen as "*resulting from the loss, damage, destruction, distortion, erasure, corruption or alteration of electronic data".*

As an aside, many PDBI policies contain an environmental exclusion which may apply so as to preclude cover in relation to the Property Damage which was caused by the chemicals.

Summary

As the Incident did not involve direct physical loss or damage to insured property, cover is unlikely to be available.

Cover may be *prima facie* available for the Factory Damage, although this is likely to be precluded at least to some extent if an exclusion for lost electronic data is included in the policy.

Scenario – Terrorism

Facts

A manufacturer is insured under a terrorism insurance policy which is broadly market-standard in terms of scope of cover and exclusions.

A number of computer viruses were created several years ago by a group acting for ideological purposes. The viruses have the effect of disabling temperature control mechanisms in software-operated machinery. These viruses affected millions of personal computers around the world, including that of an employee of the manufacturer. The employee routinely used a USB key to transfer documents from his personal computer to his employer's computer systems.

The employee, acting without any malicious intent or knowledge of the computer viruses, infected the computer systems of the manufacturer by using the USB key at work. The viruses disabled all temperature control systems in the manufacturing facility, leading to a fire which destroyed large parts of the facility.

The manufacturer therefore seeks an indemnity on its terrorism policy for the property damage caused by the fire, on the basis that the computer viruses were created for ideological purposes. The manufacturer cannot seek an indemnity under its property damage and business interruption policy as cover is excluded under a widely-drafted terrorism exclusion.

Analysis

Market-standard terrorism policies indemnify the insured against loss which arises from physical loss or damage to the insured premises and contents, where the physical loss or damage arises from an act of terrorism, political violence and/or sabotage, or a resulting fire. It follows that, in order to recover under this type of policy, the insured must demonstrate that one of these perils is the "proximate cause" of its loss. As described earlier in this paper, "proximate cause" is essentially the dominant, effective or operative cause of the loss.

While the release of computer viruses created for ideological purposes would almost certainly qualify as an act of terrorism, it is clear that the manufacturer's computer systems would not have been infected without the intervention of the manufacturer's employee. In these circumstances, the act of terrorism may not have been the proximate cause of the policyholder's losses; the more likely analysis being that the employee's actions amount to a cause from a new and independent source.

Exclusions

Market-standard terrorism policies typically exclude loss arising as a result of physical loss or damage caused by "*attacks by electronic means*", such as computer hacking or the introduction of a computer virus.

Therefore, even if the manufacturer is able to prove its case on proximate cause, its losses are likely to be excluded.

Summary

While the losses incurred by the manufacturer appear likely *prima facie* to fall within the scope of cover provided under the policy subject to the manufacturer being able to establish that an insured peril is the proximate cause of the loss, a broad exclusion for attacks by electronic means would, if such an exclusion appears in the policy wording, be likely to preclude cover.

Scenario – General Liability

Facts

A transport operator is insured under a general liability insurance programme which is broadly market-standard in terms of scope of cover and exclusions. Due to a malfunction of software systems, a train carrying several hundred passengers operated by the transport operator comes to a halt mid-way through a journey. The malfunction causes air conditioning systems to fail, leading to dangerously high temperatures inside the train. All passengers and staff are unable to leave the train for a number of hours.

After the incident, a number of claims are brought against the transport operator by members of the staff and passengers. These claims relate to:

(i) physical and mental injury caused by the conditions on the train which resulted from the malfunction; and
(ii) the delay caused by the malfunction.

The transport operator seeks an indemnity under its general liability insurance programme for liabilities which it has to members of the staff and passengers.

Analysis - Coverage[8]

Cover is generally provided under general liability policies for liabilities arising from personal injury caused to third parties in the conduct of the insured transport operator's business.

The final requirement of this type of cover is probably the simplest in this scenario - given that the losses have arisen from an incident which occurred on a train being operated by the insured transport operator, the losses appear to have been incurred in the conduct of the company's business.

---

8 Though beyond the scope of this particular scenario, General Liability policies (both Public Liability and Employers' Liability) will often provide an extension to cover potential liabilities under the Data Protection Act 1998, particularly Section 2 of that Act relating to the treatment of sensitive data. Further, some insurers (though probably not a majority) also provide cover for anxiety or distress arising from the data breach and defence costs arising from the DPA breach.

In terms of whether the liabilities arise from personal injury, this is a definition which will most likely include bodily injury to passengers and staff. Definitions of "*bodily injury*" are often broad and are likely to encompass mental as well as physical injury.

Sums which the insured is legally liable to pay in respect of this "*bodily injury*" – and the costs of defending demands or proceedings brought in respect of that "*bodily injury*" – may therefore fall within the scope of general liability cover. More expansive definitions of "*bodily injury*" or "*personal injury*" in general liability policies may also encompass the concept of wrongful detainment or false detention.

It may be arguable (although is far from clear) that this may incorporate within the scope of cover any amounts which the insured is legally liable to pay as a result of the delays caused to passengers and staff, on the basis that the delay amounted to wrongful detainment or false detention. However, absent any intention on the part of the transport operator to detain the relevant individuals, it may be difficult to establish that this is the case. In any event, pure financial loss caused to passengers or to the transport operator as a result of the delay is unlikely to fall within the scope of cover provided under a general liability policy.

Exclusions

While it appears that the main losses claimed will likely fall within the insuring clause, it is important to note that general liability policies frequently contain an electronic data exclusion – which will exclude cover for damages arising out of the loss of, loss of use of, damage to, corruption of, inability to access or inability to manipulate electronic data. It appears that liability would "arise out of" the software malfunction in that the malfunction was essentially the proximate clause of the losses incurred by the transport operator (applying the reasoning of the judge in *British Waterways v Royal & Sun Alliance Insurance* [2012] EWHC 460 (Comm) in interpreting the phrase "arising out of" in the context of policy exclusions). The malfunction of the software system may therefore fall within this exclusion.

As an aside, general liability policies also usually contain exclusions for obligations which an insured has under any workers' compensation law or as a result of employers' liability. These exclusions are likely to preclude cover for liability to staff members.

Summary

It seems likely that any claim by the insured would be precluded by the terms of an electronic data exclusion in the general liability wording, notwithstanding that an insured peril has occurred. The use of such an exclusion is common in general liability policies.

Scenario – Crime

Facts

A bank is insured under a crime and fidelity insurance programme which incorporates comprehensive cover for specie loss and which is broadly market-standard in terms of scope of cover and exclusions.

The bank is the victim of a targeted cyber-attack which has the effect of causing all security at the bank's vaults to fail mechanically. The cyber-attack succeeded because the IT security systems which were in place at the bank had not been subject to a required software update – something of which the bank's data security team had been made aware. In this regard, the bank gives a warranty in the policy wording that its IT systems are regularly updated and are fully operational.

USD 200 million in specie is stolen from the bank's vault during the period in which security at the vault is disabled. The bank seeks an indemnity under its crime and fidelity programme in respect of this loss.

Analysis – Coverage

Crime and fidelity policies generally cover the insured for first-party loss directly caused by certain types of wrongdoing by employees and third parties. Such policies often provide cover for theft of specie. Cover is also likely to be provided for loss that results directly from computer misuse – which would most likely include a cyber-attack. "Computer misuse" is generally a broad definition incorporating a range of wrongdoing involving the use of computers or data, which would most likely include a targeted cyber-attack of the type described above.

Exclusions

Crime and fidelity insurance policies do not, as a rule, contain specific cyber risk exclusions. However, there are a number of exclusions which commonly appear in crime policies that may preclude cover in the circumstances set out above.

The first is a common exclusion for mechanical failure. Exclusions of this nature generally exclude cover for loss resulting from, or related to, any mechanical failure or electrical disturbance. This would most likely exclude loss that results from the failure of the security system at the bank's vaults.

A complicating factor in relation to this exclusion is that, in this scenario, there are a number of competing potential causes of the loss – specifically the cyber-attack, the mechanical failure of the vaults and the theft of specie itself. As discussed earlier in this paper, where there are a

number of proximate causes of loss, one or more of which is excluded, a claim will be excluded in full if the insured loss would not have been incurred without the operation of the excluded peril. Here, it seems likely that the loss would not have been incurred without the mechanical failure of the vaults. In these circumstances, a mechanical failure exclusion would apply to exclude the claim as a whole.

In addition, as with a number of other lines of insurance, crime insurance policies will generally exclude loss arising from matters known to the insured prior to the inception of the policy. If the insured (or at least individuals operating within the insured) were aware of the issues with the bank's IT security systems before the policy incepted, insurers may have an argument that losses arising from those issues are excluded.

Breach of warranty?

It appears possible that, in not updating the bank's software, the bank is in breach of the warranty given in the policy in relation to its IT systems. If this is the case, the insurer will (under the current law at least) have a right to terminate the policy from the date of the breach of the warranty, which would mean that the insured would be precluded from recovering its loss arising from this scenario. Warranties of this nature may become more common in policy wordings of this type, given the increasing importance of cyber risk management which is incumbent on insureds.

Summary

Theft of the specie should, *prima facie*, be covered under the crime policy, either by way of straightforward theft cover or under cover for computer misuse. However, standard policy exclusions (such as the mechanical failure exclusion) which have no direct relation to cyber risk may operate so as to exclude the loss as a whole. Finally, cover may be precluded – and policy liability terminated - on the basis of a breach of warranty on the part of the insured in this scenario.

Systemic Cyber Risks

The scenarios discussed in this paper are specific in nature – they refer to particular incidents causing particular losses, which may or may not be covered under particular conventional lines of insurance.

The possibility of more systemic cyber risks – that is to say, cyber risks that cause a broad range of potentially insured losses – is also an issue which the insurance market is considering. The prospect of a systemic cyber risk leading to significant insured losses across the insurance market has not yet been realised, but is perhaps becoming a realistic prospect in the context of today's evolving cyber risk landscape.

Consider, for example, the hacking of the key data infrastructure of a port that operates the navigational and logistical aspects of the port's operations. Such a hacking could lead to a range of losses, including loss of or damage to vessels, loss of or damage to cargo, physical damage to the port itself, business interruption losses and / or bodily injury. Loss or damage of this type would most likely trigger claims on, for example:

a) Marine hull and marine cargo policies;
b) Property damage and business interruption policies; and
c) General liability policies,

taken out by a number of stakeholders (including the port companies and their service providers, vessel owners and operators, logistics companies and other parties using the port's services). Such a broad range of exposures could have a significant impact on the insurance market.

Though cyber risks throw up distinct challenges for underwriters, the application of policies to specific losses - a single aircraft or vessel for example – remain well understood by practitioners and generally within their day-to-day underwriting parameters. However, the possibility of systemic losses – an entire port's warehouses or fleet of aircraft or loss of Air Traffic Control at an airport for example - arising from a cyber loss requires careful analysis. More widely, regulators are also monitoring how the market addresses cyber risks and potential for accumulated losses which perhaps go beyond the normal underwriting expectations at the outset of the policy.

To mitigate the insurance market's exposures, insurers should bear in mind the effective use of exclusions and limits in the policies they are underwriting. Obviously, a continued focus on effective risk management is required.

The Cyber Insurance Market

Cyber Insurance – a brief history

The idea of “cyber insurance”, taking the form of either a standalone cover or as an enhancement to conventional lines of insurance, first emerged around 20 years ago, primarily in the US. The initial purpose of this insurance was to insure business interruption and damage to data exposures brought on by the dot-com bubble.

Take-up was, at that time, limited. However, with the growth and the development of the internet and other internal and external networks (including payment networks) concerns over vulnerabilities increased.

The turning point for much of cyber insurance business today emanates from a very specific exposure relating to the breach of personally identifiable information. A legal change in California, enacted in 2002, pushed regulation to place responsibilities upon:

“*a person or business that conducts business in California, that owns or licenses computerized data that includes personal information, as defined, to disclose in specified ways, any breach of the security of the data, as defined, to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person*”.

In substance, this legislation imposed obligations on those handling data to disclose adverse cyber incidents to the authorities and to those affected. Similar legislative change in a large number of US States has been the primary driver for the cyber insurance market as we know it.

This legislative approach is in the process of being adopted in the EU via the proposed GDPR, the implementation of which is expected to act as a catalyst for take-up of separate cyber-specific cover in Europe, which to date has been relatively low.

However, contemporary cyber policies, as well as extensions or drop-down cover provided in conventional insurances, provide cover which is much broader than the costs and liabilities associated with mandatory reporting of adverse cyber incidents. Cyber cover has evolved to reflect the expanding cyber risk landscape. This process of evolution will no doubt continue as the technological and legal / regulatory positions develop. What looks like cyber insurance today may change significantly in the future, but the same link to technology dependency and the exposures they bring will continue as might other exposures relating to data. This means that cyber cover tends to be broad in scope, further detail on which is given later in this paper.

Given the broad scope of cover available in the cyber insurance market, it seems logical that cyber insurance will, to some extent, become seen as a means of 'filling the gaps' which conventional insurances leave open in relation to cyber-related perils, some of which are identified in the scenarios set out above.

What might wordings cover

At present, forms of cyber insurance are many and varied, but typically include cover for loss arising from:

- Damage to Digital Assets (data and programmes)
- Non-physical business interruption and extra expense
- Cyber extortion
- Privacy Liability
- Confidentiality Liability
- IT Liability
- Regulatory fines, costs and expenses
- Crisis Management (mitigation) costs, including notification expenses, forensic expenses, public relations costs, credit monitoring and other assistance costs.

Some cyber wordings, but by no means all, will also provide cover in respect of:

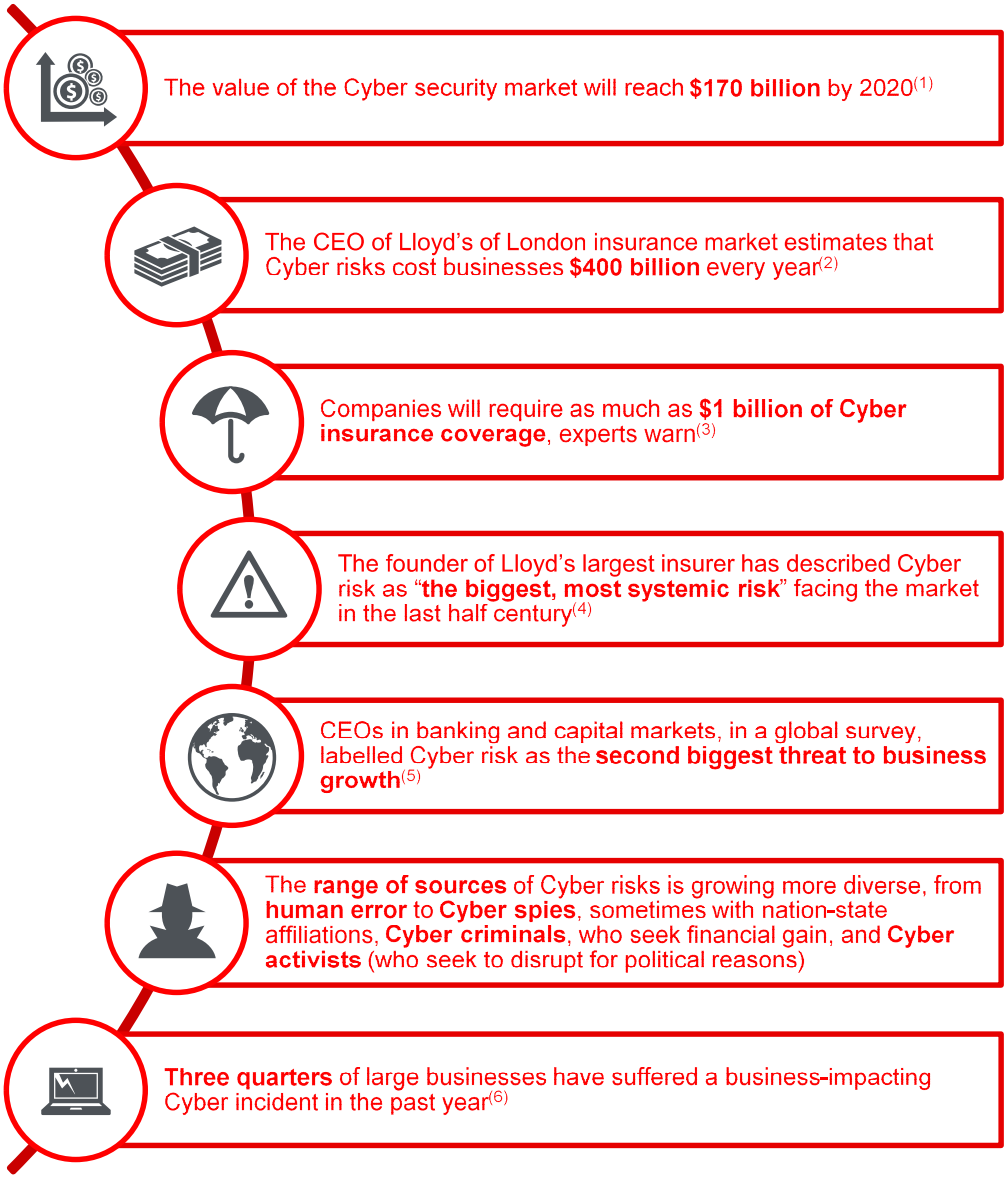
- Theft of monies/crime
- Business interruption
- Property damage (including in relation to the 'internet of things')
- Errors & omissions and Professional Indemnity Cover
- Media liability (online or multi-media) for intellectual property, defamation and other liabilities.

Cyber wordings will generally provide cover for losses arising from a broad range of events, including:

- Accidental damage or destruction
- Administrative or operational mistakes by employees or third parties
- Computer Crime, computer attacks and wrongdoing by employees
- Full system failure.

Cyber cover will not generally be limited by exclusions of the type described in the conventional insurance scenarios. Cyber cover is therefore well-placed to 'fill the gaps' in cover which will be experienced by a broad range of organisations.

Cyber Risks – Key Facts



NORTON ROSE FULBRIGHT

(1) MarketsandMarkets, 'Cyber Security Market', June 2015
(2) Fortune, 'Lloyd's CEO: Cyber attacks cost companies $400 billion every year', 23 January 2015
(3) Financial Times, 'Cyber attack risk requires $1bn of insurance cover, companies warned', 18 February 2015
(4) Financial Times, 'Cyber risks too big to cover', 5 February 2015
(5) CBR Online, 'Cyber risk spooks financiers as attacks escalate', 17 February 2015
(6) HM Government, Information Security Breaches Survey, 2015 (p.6)

Recent Cyber incidents

US supermarket chain Target was attacked in December 2013. The credit and debit card records of approximately 40 million customers across the USA were stolen, as well as the personal information of around 70 million people.[1]

Sony Pictures Entertainment Inc. was attacked in November 2014. Over 200GB of data were exposed, including personal information about employees and their salaries, e-mails between employees, and previously unreleased films.[2]

Anthem, a US healthcare insurance firm. admitted in February 2015 that it was hit by a "very sophisticated" cyber attack that accessed databases containing information (including names, birth dates, medical and social security IDs, and addresses) on 80 million customers.[3]

The US Office of Personnel Management admitted in June 2015 that it had been the subject of an attack from March 2014 onwards, losing the records of up to 21.5 million people, including social security numbers and security clearance information.[4]

In July 2015, extra-marital dating website Ashley Madison was hacked, with all of its customer data stolen, as well as the emails of the CEO and the company board. All of this user data was released by August 2015.[5]

In August 2015, Carphone Warehouse was subject to a cyber attack on its website which exposed details of up to 2.4 million customers, which also included 90,000 credit card records.[6]

In October 2015, almost 157,000 TalkTalk customers had their personal details hacked. The data included bank account numbers and sort codes.[7]

NORTON ROSE FULBRIGHT

[1]http://www.forbes.com/sites/maggiemcgrath/2014/01/10/target-data-breach-spilled-info-on-as-many-as-70-million-customers/

[2] http://uk.businessinsider.com/the-sony-hackers-still-have-a-massive-amount-of-data-that-hasnt-been-leaked-yet-2014-12?r=US&IR=T;
http://www.bbc.co.uk/news/entertainment-arts-30512032

[3] http://ww2.cfo.com/risk-management/2015/02/anthem-discloses-sophisticated-cyber-attack/

[4] http://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html

[5] http://www.theguardian.com/technology/2015/aug/19/ashley-madisons-hacked-customer-files-posted-online-as-threatened-say-reports

[6] http://news.sky.com/story/1532547/millions-hit-by-carphone-warehouse-cyber-attack

[7] http://www.bbc.co.uk/news/business-347431858

Cyber risk mitigation steps for insureds

Appointing a Chief Information Officer at board level ensures that information security policy and issues are dealt with at the highest level.

Penetration testing by a professional security company will test the insured's security arrangements, identify vulnerabilities, and suggest improvements.

The insured should have a robust, detailed Cyber Incident Response Plan, which provides vital certainty of procedure following an incident.

The Government-backed Cyber Essentials certification provides evidence that the insured's business complies with Cyber best practice to insurers, customers and other stakeholders.

The insured should provide its employees and other technology-users with an up-to-date and accessible IT policy to help mitigate risk.

Regular IT and risk-awareness training for staff is an important element of Cyber security.

Prioritising Cyber security at a board level will help develop a culture where Cyber security is everyone's responsibility, and not just an IT issue.

NORTON ROSE FULBRIGHT

Model Cyber Related Policy Clauses

INSTITUTE CYBER ATTACK EXCLUSION CLAUSE

1.1 Subject only to clause 1.2 below, in no case shall this insurance over loss damage liability or expense directly or indirectly caused by or contributed to by or arising from the use or operation, as a means for inflicting harm, of any computer, computer system, computer software programme, malicious code, computer virus or process or any other electronic system.

1.2 Where this clause is endorsed on policies covering risks of war, civil war, revolution, rebellion, insurrection, or civil strife arising therefrom, or any hostile act by or against a belligerent power, or terrorism or any person acting from a political motive, Clause 1.1 shall not operate to exclude losses (which would otherwise be covered) arising from the use of any computer, computer system or computer software programme or any other electronic system in the launch and/or guidance system and/or firing mechanism of any weapon or missile.

10/11/03
CL380

Terrorism Insurance Physical Loss or Physical Damage Wording

This Policy does not insure against:

Loss or damage by electronic means including but not limited to computer hacking or the introduction of any form of computer virus or corrupting or unauthorised instructions or code or the use of any electromagnetic weapon.

This exclusion shall not operate to exclude losses (which would otherwise be covered under this Policy) arising from the use of any computer, computer system or computer software programme or any other electronic system in the launch and/or guidance system and/or firing mechanism of any weapon or missile.

(LMA3030, Exclusion 9)

WAR, HI-JACKING AND OTHER PERILS EXCLUSION CLAUSE

(AVIATION)

This Policy does not cover claims caused by

(a) War, invasion, acts of foreign enemies, hostilities (whether war be declared or not), civil war, rebellion, revolution, insurrection, martial law, military or usurped power or attempts at usurpation of power.

(b) Any hostile detonation of any weapon of war employing atomic or nuclear fission and/or fusion or other like reaction or radioactive force or matter.

(c) Strikes, riots, civil commotions or labour disturbances.

(d) Any act of one or more persons, whether or not agents of a sovereign Power, for political or terrorist purposes and whether the loss or damage resulting therefrom is accidental or intentional.

(e) Any malicious act or act of sabotage.

(f) Confiscation, nationalisation, seizure, restraint, detention, appropriation, requisition for title or use by or under the order of any Government (whether civil military or de facto) or public or local authority.

(g) Hi-jacking or any unlawful seizure or wrongful exercise of control of the Aircraft or crew in Flight (including any attempt at such seizure or control) made by any person or persons on board the Aircraft acting without the consent of the Insured.

Furthermore this Policy does not cover claims arising whilst the Aircraft is outside the control of the Insured by reason of any of the above perils. The Aircraft shall be deemed to have been restored to the control of the Insured on the safe return of the Aircraft to the Insured at an airfield not excluded by the geographical limits of this Policy, and entirely suitable for the operation of the Aircraft (such safe return shall require that the Aircraft be parked with engines shut down and under no duress).

AVN 48B 1.10.96

ELECTRONIC DATA ENDORSEMENT A

1. Electronic Data Exclusion

Notwithstanding any provision to the contrary within the Policy or any endorsement thereto, it is understood and agreed as follows:

(a) This Policy does not insure loss, damage, destruction, distortion, erasure, corruption or alteration of ELECTRONIC DATA from any cause whatsoever (including but not limited to COMPUTER VIRUS) or loss of use, reduction in functionality, cost, expense of whatsoever nature resulting therefrom, regardless of any other cause or event contributing concurrently or in any other sequence to the loss.

ELECTRONIC DATA means facts, concepts and information converted to a form useable for communications, interpretation or processing by electronic and electromechanical data processing or electronically controlled equipment and includes programmes, software and other coded instructions for the processing and manipulation of data or the direction and manipulation of such equipment.

COMPUTER VIRUS means a set of corrupting, harmful or otherwise unauthorised instructions or code including a set of maliciously introduced unauthorised instructions or code, programmatic or otherwise, that propagate themselves through a computer system or network of whatsoever nature. COMPUTER VIRUS includes but is not limited to 'Trojan Horses', 'worms' and 'time or logic bombs'.

(b) However, in the event that a peril listed below results from any of the matters described in paragraph (a) above, this Policy, subject to all its terms, conditions and exclusions, will cover physical damage occurring during the Policy period to property insured by this Policy directly caused by such listed peril.

Listed Perils
Fire
Explosion

2. Electronic Data Processing Media Valuation

Notwithstanding any provision to the contrary within the Policy or any endorsement thereto, it is understood and agreed as follows:

Should electronic data processing media insured by this Policy suffer physical loss or damage insured by this Policy, then the basis of valuation shall be the cost to repair, replace or restore such media to the condition that existed immediately prior to such loss or damage, including the cost of reproducing any ELECTRONIC DATA contained thereon, providing such media is repaired, replaced or restored. Such cost of reproduction shall include all reasonable and necessary amounts, not to exceed {Response} any one loss, incurred by the Assured in recreating, gathering and assembling such ELECTRONIC DATA. If the media is not repaired, replaced or restored the basis of valuation shall be the cost of the blank media. However this Policy does not insure any amount pertaining to the value of such ELECTRONIC DATA to the Assured or any other party, even if such ELECTRONIC DATA cannot be recreated, gathered or assembled.

25/01/01
NMA2914

ELECTRONIC DATA ENDORSEMENT B

1. Electronic Data Exclusion

Notwithstanding any provision to the contrary within the Policy or any endorsement thereto, it is understood and agreed as follows:

(a) This Policy does not insure loss, damage, destruction, distortion, erasure, corruption or alteration of ELECTRONIC DATA from any cause whatsoever (including but not limited to COMPUTER VIRUS) or loss of use, reduction in functionality, cost, expense of whatsoever nature resulting therefrom, regardless of any other cause or event contributing concurrently or in any other sequence to the loss.

ELECTRONIC DATA means facts, concepts and information converted to a form useable for communications, interpretation or processing by electronic and electromechanical data processing or electronically controlled equipment and includes programmes, software and other coded instructions for the processing and manipulation of data or the direction and manipulation of such equipment.

COMPUTER VIRUS means a set of corrupting, harmful or otherwise unauthorised instructions or code including a set of maliciously introduced unauthorised instructions or code, programmatic or otherwise, that propagate themselves through a computer system or network of whatsoever nature. COMPUTER VIRUS includes but is not limited to 'Trojan Horses', 'worms' and 'time or logic bombs'.

(b) However, in the event that a peril listed below results from any of the matters described in paragraph (a) above, this Policy, subject to all its terms, conditions and exclusions, will cover physical damage occurring during the Policy period to property insured by this Policy directly caused by such listed peril.

Listed Perils

Fire

Explosion

2. Electronic Data Processing Media Valuation

Notwithstanding any provision to the contrary within the Policy or any endorsement thereto, it is understood and agreed as follows:

Should electronic data processing media insured by this Policy suffer physical loss or damage insured by this Policy, then the basis of valuation shall be the cost of the blank media plus the costs of copying the ELECTRONIC DATA from back-up or from originals of a previous generation. These costs will not include research and engineering nor any costs of recreating, gathering or assembling such ELECTRONIC DATA. If the media is not repaired, replaced or restored the basis of valuation shall be the cost of the blank media. However this Policy does not insure any amount pertaining to the value of such ELECTRONIC DATA to the Assured or any other party, even if such ELECTRONIC DATA cannot be recreated, gathered or assembled.

25/01/01
NMA2915

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.