Silent cyber: Can you hear it?

With events such as the WannaCry ransomware attack of 2017, which has been classified as a cyber catastrophe event, a number of silent cyber issues have developed into very public property policy coverage disputes. Lyndsey Bauer, Partner at Paragon, provides an overview of silent cyber and the responses that insureds should take going forward.

I. OVERVIEW

What is silent cyber?
Because cyber risk is now a pervasive threat to all operating entities, it impacts practically every line of commercial insurance. Yet, it remains unaddressed in many lines of insurance.

The lack of clarity in some standard property and casualty policies can lead to confusion or misunderstanding about coverage for cyber risks. Simultaneously, an insurer covering a loss it had not contemplated can jeopardise its credit rating and/or financial solvency. We refer to these potential cyber exposures as 'silent' cyber or 'non-affirmative' cyber.

Is silence desirable or not?
Silence provides an argument for cover, but such coverage cannot be relied upon. The coverage outcome is uncertain and the situation would likely evolve into a legal dispute. An insurer, in aggregate, may pay one loss it does not believe is covered before amending its forms. Silence may provide a short-term win, but that really is only delaying the inevitable and, ultimately, too much uncertainty will no doubt be distressing when a claim is to be made.

Silence therefore leads some companies to believe that they have adequate cover for cyber risk when they do not. Non-affirmative language within a traditional insurance policy may also be subject to differing interpretation by insurers, which could lead to legal disputes.

Silent cyber is resulting in claims being made which insurers have not underwritten nor charged for. This silence is more about slow insurance product development, rather than a reflection of insurer appetite.

Potential arguments for denying cover
a. The basis of insurability
For a loss to be insurable, it must relate to a definite and measurable risk. Without information, an insurance company can neither produce a reasonable benefit amount nor a premium cost. If submission materials do not address cyber risk or risk management; the risk has not been measured and would therefore not meet this requirement.

The loss must also be fortuitous – it must have occurred due to chance. It has to be the result of an unintended action and has to be unexpected in its exact timing and impact. Unless an organisation were to intentionally leave cyber risk unmanaged, cyber loss will likely meet this criteria.

An insurable loss should not be catastrophic in nature. Catastrophic loss refers to two kinds of risk.

One of those is where the risk is so large that the premium would be inefficient or where no insurer could hope to pay for the loss. Silent cyber could fall into this category.

Another is where the catastrophic risk involves an unpredictably large loss of value that is not anticipated by either the insurer or the policyholder. Silent cyber has likely not been underwritten; therefore, the risk is not anticipated by the insurer and may not meet this requirement.

Exclusions can typically be found across most policies for catastrophic events such as floods, pollution, nuclear, war and terrorism. However, cyber events as triggers for loss are not explicitly included or excluded. Often, cyber exclusionary language within the policy is ambiguous or absent altogether.

b. Obligations under the Insurance Act of 2015: A loss not underwritten is not insured
The Insurance Act of 2015 affects the way in which business is underwritten and placed. It also changes the remedies of insurers for non-disclosure and misrepresentation, breach of warranty and fraudulent claims.

The assured required to make a fair presentation of the risk. This represents a fundamental shift from the doctrine of "utmost good faith" (enshrined in section 17 of the Marine Insurance Act of 1906 (MIA)). That is not a new concept – in fact, there is an element of going 'back to the future'.

The Insurance Act of 2015 creates a positive duty of inquiry for the insurer. Also, an assured is not required to disclose information that an insurer already knows (Section 5 (1)); or information that it ought to know (Section 5 (2)); or information that it is presumed to know (Section 5 (3)). As is the case now, an insurer will also be presumed to know things that are common knowledge.

Cyber risk is a known risk – however, no one but the company itself would know better about its exposure to cyber risk. The underwriter should ask the insured about its exposures, but likewise, there is a duty on the insured to present cyber risk and risk management to the underwriters.

Why is silent cyber an issue now?
In a large part, silent cyber has become an issue recently due to events such as the WannaCry, Petya and NotPetya attacks in 2017, which has been classified as a cyber catastrophe event. Consequently, the focus of the insurance and reinsurance industry has shifted from potential large professional lines cyber-related losses to the potential impact on the property market, through both affirmative and non-affirmative cyber losses.

According to Property Claim Services (PCS), the total industry loss from the Petya/NotPetya cyber-attacks has now surpassed $3 billion (£2.3 billion). Of these losses, 90% were driven by silent cyber impacts, while the rest stemmed from affirmative losses.

A number of silent cyber issues developed into very public property policy coverage disputes, such as the case of the US food company Mondelez, which sued its insurer, alleging that it was wrongfully denied a claim under a property insurance policy for losses incurred in 2017's NotPetya malware attack. In that case, the argument for silent cyber coverage was undermined by a war exclusion clause.

Regulators and global insurers have sought to deal with non-affirmative cyber risks and exposures within property and casualty (P&C) insurance portfolios. In the UK, the agenda on this issue has been driven by the Prudential Regulation Authority (PRA) and Lloyd's of London.

In a letter to all UK insurers issued in January 2019, the PRA stated that they must have "action plans to reduce the unintended exposure that can be caused by non-affirmative cyber cover". Later that year, Lloyd's issued a market bulletin mandating that all policies need to be clear on whether coverage is provided for losses caused by a cyber event, in order to eliminate silent cyber exposure. This was to be achieved by either excluding from or affirmatively covering the exposure in all P&C policies by 1 January 2020, commencing with First Party Property Insurance in this initial phase of the mandate.

Further bolstering these mandates, rating agencies have cited the failure to manage these exposures as liable for consideration as ratings criteria. It is expected that the European Insurance and Occupational Pensions Authority will issue a similar message.

Possible responses from insurer
Insurers are acting to clarify their coverage intent regarding cyber, often because of requirements from regulators. Some insurers have done so by defining cyber risk and then excluding it from non-cyber policies. Others are introducing new policy language and underwriting guidelines. Yet others, such as Lloyd's of London, are requiring insurers to expressly include or exclude cyber risk in their traditional lines policy wordings.

Any change to policy language impacts cover, which means that it is very unlikely that you will be able to renew as expiring.

However, many of the proposed cyber endorsements on traditional P&C policies have been inconsistent or simply too broad. For example, some of such endorsements exclude loss stemming from previously covered physical perils, merely for the reason that technology use was involved in the chain of causation. Many proposed wordings by insurers continue to sidestep the fact that technology is central to business operations across all sectors today.

A one-size-fits-all approach does not work. Each insurer may interpret the guidance differently or will have a different appetite for cyber risk. They may each have different requirements and priorities too.

It is inevitable that your coverage is going to change – it is only a matter of how much it will change.

Policyholder options
You can try to reject the endorsement. Bear in mind, though, that this might result in the insurer accepting this as a non-renewal.

If you intend to reject the endorsement, you should do this well in advance of the policy expiration. You will be surprised how many clients try to leverage the removal of the exclusion with an order to bind – only to find they are left with a choice to buy the insurance with the exclusion or go uninsured. Give yourself, and your broker, time to find alternatives.

There may be others who will take a different view, but with the Financial Conduct Authority (FCA) and the rating agencies also interested in this, it would seem to be an unlikely route. If you reject the exclusion, you may end up without any coverage; most, if not all insurers will not intentionally run afoul of regulations. If you reject the exclusion, you may end up buying the affirmative coverage endorsement or not placing business without addressing non-affirmative cyber.

That leaves you with the option of accepting the exclusion or shopping around for alternative solutions. You may encounter reduced competition as a result of trying to secure affirmative cover, this can result in higher premiums and may present a challenge for building big towers.

II. RESPONDING TO SILENT CYBER TODAY

The nature of insurance

The triggers of many insurance products are based on how the event happened – whether it was internal or external, whether it was an unintentional or intentional act.

Insurance products also cover specific types of loss, whether first party or where it pertains to liability, breaches of duty, contracts, regulation. Standard insurance policies therefore tend to respond to one or two of the quadrants in **Figure 1**.

The nature of cyber risk, however, challenges traditional insurance. Before you can address the impact of silent cyber, you would first need to understand the parameters of your current insurance. Where does your current coverage start and end? Are there insurable cyber gaps?

A cyber exclusion will not change the basic parameters of existing cover, but may inadvertently undermine it.

Meanwhile, affirmative cyber will not expand the basic parameters of existing cover, but may limit it.

In this section, we will look at some examples of insurance policies and apply some sample exclusionary language.

Crime insurance

Before addressing the market response to silent cyber, it is worth recapping what crime insurance sets out to do.

Crime insurance covers the insured's direct financial loss resulting from a criminal act, whether committed by dishonest employees or external fraudsters. Typically, crime is written on a named perils basis for first-party loss.

My view is that loss of money, securities or other property through criminal acts should be covered by crime insurance. This is where the experience resides – in underwriting and in claim settlement. But outdated wordings leave significant gaps before any exclusions are added. You would therefore want to move away from named period crime cover where you can.

A 'direct' fraud happens when a hacker penetrates a company's systems and wires money to a fraudulent account, thereby leading to a direct loss.

There is no coverage for indirect losses, and some forms do not offer coverage for liability for claims arising out of the direct loss of client money under your control. There may not be cover for an employee being socially engineered, on the basis that there may have been no "computer crime" as defined in the policy, and the employee may not have been acting dishonesty nor beyond their authority. There is also almost certainly no crime policy coverage for your client being socially engineered into paying a false invoice which they believed was from you. An underwriter cannot underwriter your customers' internal controls.

So, crime exclusion calls for some attention before we can evaluate how to address the cyber exclusion.

Crime insurance exclusion

Consider the following sample crime insurance exclusion wording:

> *... For loss or costs directly or indirectly caused by or contributed to by or arising from the use or operation of any computer, computer system, computer software programme, computer process or any other electronic system.*

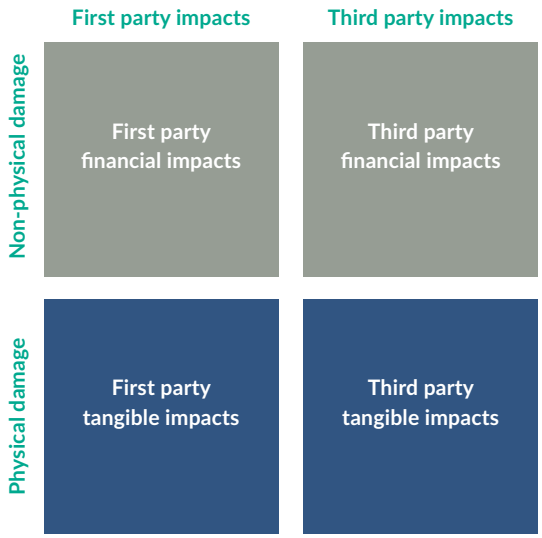

Figure 1: The nature of insurance policies.
Source: Paragon

This exclusion wording is very broad, stating that all loss arising out of the use of computers is excluded. If strictly interpreted, it could undermine the entire basis of the coverage. You can negotiate on the language used. There is no specific mandatory version to be used, except that the underwriters have to address non-affirmative cyber – you can work with the underwriters on how they do that.

As the crime market is tied to criminal intent, more acceptable language would include a carve-back that the exclusion shall not apply with the intent to cause harm or it could perhaps be limited to excluding direct loss arising from a cyber incident. A cyber incident should be defined in alignment with your cyber policy, if purchased.

D&O exclusion
Consider the following sample crime insurance exclusion wording:

> *… For any loss arising from the use of a computer system, network or loss of data.*

This exclusion wording is also very broad, as with the above wording from a crime exclusion clause, and could similarly undermine the entire basis of the coverage.

In the context of a D&O policy, you could perhaps accept a fall-back to claims arising out of wrongful acts alleged against a director or officer in their capacity as such, to ensure you are at least providing defence costs for an insured person required at a GDPR (or other privacy) investigation.

Likewise, you should ensure that the D&O exclusion under a cyber policy aligns with what is affirmatively covered by the D&O policy.

Marine affirmative cover
The Lloyd's Market Association (LMA) has offered sample language to exclude and affirm cyber cover. LMA 5403 is the affirmative grant, which it offers by excluding all loss arising from cyber risk and carving back what it intends to cover. LMA 5403 excludes:

> *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, computer process or any other electronic system.*

Again, this is not a mandatory version – each insurer may choose its preferred language. You would of course be able to negotiate the wording with your insurers, but I think this wording makes a reasonable effort. It is putting the risk in a basket, which the insurer can then attempt to underwrite around.

I like the language "as a means of inflicting harm", because it removes tricky language that requires the "intent to cause the insured harm".

Before you accept this endorsement, you should obviously ask some coverage questions:

- Does a cyber event need to be deemed an act of war or terrorism to trigger cover?
- How is that defined?
- Is this broadly a "malicious" event carve-back?
- Where is coverage from non-malicious acts (negligence)?

If the insured buys cyber insurance, it would interact with this language through the "Other Insurance" clause. Cyber policies are in excess to other insurance if the other insurance is written more specific to the loss incurred.

If the affirmative endorsement attaches to a marine policy, then the cyber policy is excess only if the marine policy covers war and terrorism, and political violence. Obviously, the cyber policy would provide coverage subject to its own terms and conditions.

Most cyber policies exclude tangible losses.

Property affirmative cover
The LMA 5400 is a two-part exclusion that applies to "cyber loss" and "data loss" with carve-backs. It excludes:

> *Cyber Loss other than physical loss or physical damage to property insured under this Policy caused by any ensuing fire or explosion which directly results from a Cyber Incident, unless that Cyber Incident is caused by, contributed to by, resulting from, arising out of or in connection with a Cyber Act including, but not limited to, any action taken in controlling, preventing, suppressing or remediating any Cyber Act.*

and

> *Loss, damage, liability, claim, cost, expense of whatsoever nature directly or indirectly caused by, contributed to by, resulting from, arising out of or in connection with any loss of use, reduction in functionality, repair, replacement, restoration or reproduction of any Data, including any amount pertaining to the value of such Data, unless Data Processing Media owned or operated by the Insured, should such suffer physical loss or physical damage insured by this Policy, then this Policy will cover the cost to repair or replace the Data Processing Media itself plus the costs of copying the Data from back-up or from originals of a previous generation.*

Like marine policy, it is an example of affirmative language in the form of an exclusion with a

carve-back. The definition of cyber loss is broad, encompassing first-party and third-party costs, and including loss remediation efforts to stop the attack. Therefore, it is a blanket exclusion. The carve-back allows for physical damage to property caused by fire or explosion, where the proximate cause was a cyber incident but not a cyber act.

Before you accept this endorsement, you should obviously ask some coverage questions:

- "Computer Systems" broadly refers to communication networks. Are industrial controls or more mechanical-based automated systems covered?

- Does the property policy only cover damage from fire or explosion? If not, why is the carve-back limited to these perils?

I personally prefer the marine market approach, which puts the risk into a category and allows the insurer the chance to underwrite the risk. This LMA 5400 affirmative cover endorsement, however, does not go as far as we might have expected. A "cyber act" means malicious cyber activity, including social engineering. Providing cover a fire following a cyber event is useful, but overheating or bricking would be even more useful.

The property 'affirmative' cover effectively puts all cyber-related BI/EE to the cyber market, along with data restoration. The cyber market may exclude physical damage other than bricking of communications devices.

Again, this is not a mandatory version; each insurer may use its own language and you are of course able to negotiate with your insurer.

Exclusions and endorsements: General takeaways
Increased reliance on connectivity blurs the line between physical and cyber risk, this means you probably already have coverage 'gaps' in your portfolio – consistent with the parameters of your existing insurance and as a result of the risk not being fully addressed in insurance policy language.

The move to address silent cyber has resulted in two trends that the risk manager needs to navigate:

1. Overly broad exclusions

2. Affirmative language that is limiting by triggering coverage on how the event happened – that is, was it malicious or not malicious?

Obviously, the acceptance of an exclusion highlights that something is not covered. But silence is not certainty of coverage.

The good news and the bad news is that cyber risk – silent or otherwise – is not addressed consistently in the broader P&C market, including within cyber insurance. This means that if there is coverage that your firm has identified as a priority, you can likely find coverage for it. It may be negotiated with existing insurers or can be created for a premium, and will depend on the submission materials made available.

We saw this when Employment Practices Liability (EPL) cover was excluded from D&O policies and a new product was developed to cover the risk. The market has always evolved and still does.

Each organisation needs to identify whether the loss of uncertain cover flags an issue for it and whether it needs to seek certainty of coverage.

What is cyber insurance?
Cyber insurance is available to cover organisations for certain first-party and third-party exposures arising from various cyber perils, therefore, offering affirmative cover. But there is no standard cyber policy. **Figure 2** shows common core coverages across the cyber market.

It is very important to note that some policies are written to respond to DATA DISCLOSURE (privacy) Injury only. This type of cover may be less expensive than the alternatives but would not suit a business that is not responsible for the confidentiality of personal information.

Many will respond more broadly to damage arising from NETWORK EVENTS (security). There are variations on this, which can have a malicious act trigger (internal or external), a negligent systems operations trigger and, in some cases, also a "unplanned system outage trigger".

All will respond to the insured's privacy liability, whether or not that arises from third-party vendors. Some will provide business interruption cover when this is caused to the insured by third-party vendors.

What can the policyholder do?
Understand that your coverage will change. What that means to each insured will vary.

Fortunately, there are insurers who are willing to offer significant coverage. You may be able to negotiate affirmative cover with insurers or seek alternative risk transfer products, as in the cyber market, and there is always a market willing to develop manuscript policies to address specific gaps.

What you need to do is give yourself as much time as you can and to think conservatively – think of these renewals less in terms of 'what you can get' and more in terms of 'what you can keep'.

This is happening in an already challenging marketplace. Many insurers across product lines are pushing for premium rate adequacy, and renewals

Incident response: To determine what happened, how to repair the damage, to reduce downtime and to meet privacy regulatory requirements.

Extortion: Costs such as ransom payments and IT forensic expenses.

Lawsuits and Private regulatory investigations: This includes legal fees associated with a breach of confidentiality, legal settlements and also regulatory fines where insureable.

Business losses: Monetary losses experienced by network downtime or cyber incident, data loss recovery, cyber rannsom payments and costs involved in managing a crisis, including PR services.

Figure 2: Insurance for economic or legal costs, arising from data disclosure and/or network events.
Source: Paragon

are taking longer to complete. But even without the hardening market, it would have been very unlikely that you will be able to secure "coverage as expiring" at "premium as expiring" as markets move to address silent cyber risk.

Your organisation will need to determine its own specific renewal priority – whether that is programme limits, premium spend or coverage. Living with an exclusion will be the path of least resistance, enabling least pressure on available limits or renewal pricing, but will highlight coverages you do not have. You can almost certainly find a way to address any gaps with underwriting information and for premium.

Insureds and their brokers will need to work closely together to identify coverage at risk and plan from there.

If coverage is the priority, you and your broker will need a strategy to align coverage across your portfolio. This will add yet more time to the process, especially due to the prevalence of inconsistent definitions and inconsistent triggers (event versus consequence).

Whichever is your priority, collecting the information required by the underwriters will take time. There are many cyber risk stakeholders in your organisation whose feedback will be required in order to make a fair presentation of risk. You may need to lock in the availability of the C-suite members to present to the market.

Presenting the risk to the market or markets will also take time. Standard renewals are taking longer, in part due to Covid-19, but also because underwriters are requiring more information and because the market is hardening, and more market feedback is being sought and therefore needs to be reviewed.

III. SUMMARY

Insurers and regulators are taking action to address the risk of silent cyber. Policy language is evolving and that is impacting coverage. Insureds can lose the argument for coverage. Besides being untested, the drafted language could also overreach.

Policyholders face the challenges of getting inconsistent responses from their insurers, inadvertent loss of intended coverage and programme gaps.

Finally, insureds should prepare for renewal – they should develop a strategy, identify renewal priorities, approach the market with C-suite support and always review feedback.