Cyber Insurance - Understanding Coverage, Curtailments and Exclusions

P. Umesh
Consultant – Liability Insurance

"There are only two types of companies: those that have been hacked and those that will be. Even that is merging into one category: those that have been hacked and will be again." - Robert Mueller, III, FBI Director, 2012.

Cyber attacks are a fact of life companies have to learn to live with. Companies need to build in appropriate standards, protocols, processes and firewalls to reduce the possibility of an attack or at least soften its impact on their balance sheets.

Cyber attack is an attempt by hackers to damage or destroy a computer network or system or exploit its vulnerabilities. It means unauthorised access, unauthorised use or transmission of a computer virus which alters, copies, misappropriates, corrupts, destroys, disrupts, deletes or damages the organisation's computer system causing losses to the victim organisation and/ or may result in Failure of Security or Denial of Service. Cyber attacks may lead to disclosure of confidential data, corruption or loss of an organisation's systems or data, corruption or loss of third party systems or data thereby resulting in significant third party liability as also regulatory actions. These attacks may also cause damage to companies' own reputation and business interruption besides inviting regulatory interventions and actions. Cyber attacks may result in losses of various kinds to the victim organization. According a report from Cybersecurity Ventures, cybercrime will cost the world $6 trillion annually by 2021up from $3 trillion in 2015. Much has been written about frequency and severity of various types of losses resulting from cyber attacks. While best practices and processes are the first line of defence, they may not always prevent attacks and resultants losses.

Cyber incident ranks as the top risk ahead of supply chain interruption, changes in legislation and natural catastrophes etc. for companies globally as per "Allianz Risk Barometer 2020".

Cyber attack is an attempt by hackers to damage or destroy a computer network or system or exploit its vulnerabilities. It means unauthorised access, unauthorised use or transmission of a computer virus which alters, copies, misappropriates, corrupts, destroys, disrupts, deletes or damages the organisation's computer system causing losses to the victim organisation and/ or may result in Failure of Security or Denial of Service. Cyber attacks may lead to disclosure of confidential data, corruption or loss of an organisation's systems or data, corruption or loss of third party systems or data thereby resulting in significant third party liability as also regulatory actions.

This is the context in which cyber insurance plays a significant role.When cyber insurance was introduced in the 1990s, the primary attention was on covering data breach exposures in response to regulations framed by authorities in USA and Europe. Later, when business operations started getting more digital and the influence of information technology became all pervasive, insurers started offering wider coverage.

COVERAGE:

Broadly, cyber Insurance provides coverage in respect of the following.

- **Regulatory actions:** Investigation costs, defence costs and awards, *fines and penalties imposed by a regulator(*allowed depending upon admissibility of the same in various jurisdictions).
- **Crisis management costs:** Public relation costs, investigation costs, customer notification,

credit monitoring costs and extortion payments.

- **Liability claims:** Defence costs, awards and out of court settlements.
- **First Party losses:** Forensic costs, data restoration costs and business interruption losses.

Cyber risk permeates all classes of insurance across various industries. A cyber event can trigger losses across many lines of insurance - property damage and business interruption resulting from computer systems failure/ virus under property insurance, siphoning money through phishing under crime insurance, product liability/ product recalls from security vulnerabilities under product liability/ recall insurance, breach of contract/ negligence claims under E&O insurance and for managerial failure under D&O insurance. Against this background, given that cyber exposures have significantly increased in India and globally resulting in uptake of cyber insurance covers, it is necessary to review some of the cyber insurance policy curtailments that restrict or reduce coverage and exclusions listed as such.

POLICY PROVISIONS CURTAILING COVERAGE:

Coverage to subsidiaries: When a parent company and its subsidiaries are covered under one policy, it is not that coverageunder all sections is automatically available to the subsidiaries. Cover may apply only to certain exposures like breach of data protection law or an act. Insureds need to understand this restriction and if possible try to negotiate cover as required.

Changes in the risk: If material changes in the risk are not informed to insurers, policy rights may get prejudiced. There may be changes in the fund transfer protocol, changes in the business continuity planning and access control for remote access. It is necessary to seek continuity of coverage by informing insurers about the changes lest coverage remains a mirage. Need for this notification to insurers has become more pronounced after Covid 19 lockdown when work from home has become a norm and other processes also had to undergo significant change.

Failure to maintain minimum required practices/ update systems: Some insurance policies exclude claims when the standards and procedures are not maintained as mentioned in the policy. Similarly, there could be stipulation about testing standards or audits at specified intervals. Impact of these stipulations needs to be understood carefully. There are hard lessons to learn from the case Columbia Casualty Co. v. Cottage Health System. While the stipulations are necessary to maintain the risk at the same level throughout the policy period, it is advisable to restrict the applicability of the exclusion to material changes so that coverage does not become illusory.

Phishing attacks: In the normal course, phishing attack claimsare not in the realm of cyber insurance. They fall under crime insurance. Insurers may not automatically offer cover for phishing attacks under cyber insurance. When they offer coverage, they may subject it to a sub limit. Restrictions imposed by the insurer in this matter also need to be understood.

Network interruption: While losses resulting from network interruptions are covered, problems arise when coverage is restricted to insured's own network, given the fact many activities are outsourced as a result of which third party network also becomes relevant. This necessitates extending coverage in respect of interruptions to third party network also.

Computer System: Normally coverage is provided to those systems which are provided by the company for exclusive and secure usage for the purpose of its business. This may deny coverage when employees use their own computers while working from home which is more prevalent now, in the post Covid19 world or when insured's employees bring in their own devices under BYOD schemes. These restrictions need appropriate amendments to ensure coverage.

Termination of policy: Sometimes a provision is found in the policy that the insurer may terminate the cover, if the existence of certain covers under policy is revealed to some persons. This may create problems to the insured sparticularly when the information is revealed inadvertently or under pressure. While ideally the policy has to be made non-cancellable, Insureds should at least seek to restrict the termination provision only if revelation is deliberate.

Business interruption: Coverage here normally refers to the interruption to the computer systems and the time taken to restore them ignoring

interruption to the operations on the shop floor which is relevant. It is necessary to get the cover till the time the business operations are back to normal. Otherwise, insureds should know that there is coverage only for the period till Information Technology(IT) systems become fully functional. Various components covered also need to be known. Ignorance cannot grant any coverage.

Merchant Service payments: Sometimes coverage is reduced or eliminated for certain amounts by narration in definitions or by listing it as an exclusion- e.g. payments the insured is responsible for under a merchant services agreement. This may create a coverage gap.PF Chang's China Bistro Inc v Federal Insurance Co is a case in point.

EXCLUSIONS:

Every insurance policy has exclusions. The purpose of an exclusion is to eliminate or restrict coverage. While the ideal thing is to get all exclusions at one place, it does not happen that way. Exclusions are listed in multiple places – general exclusions, specific exclusions, definitions, conditions and also endorsements.

Prior acts exclusion: In the normal course, coverage is not available for acts prior to the policy inception date. But, globally insurers do offer cyber insurance covers on claim discovery basis meaning there would not be any exclusion for acts prior to inception of the policy. It is therefore advisable to negotiate the policy on claim discovery basis with no retroactive date.

Intentional Acts: As in the case with most insurance policies, intentional and dishonest acts are excluded from the coverage. But, it is necessary to subject this exclusion to final adjudication.

Non-compliance losses: This exclusion takes away cover when the insured fails to implement steps suggested by insurer or their representative. Distinction needs to be made between recommendatory and mandatory steps so that it does not result in blanket removal of cover.

Bodily injury/property damage (BIPD) : This exclusion is found in all cyber insurance policies. Any loss arising out of, based upon or attributable to bodily injury or property damage is generally excluded under a cyber insurance. In view of the recent trend of non cyber insurance policies like CGL excluding cyber losses, one needs to ensure that the BIPD does not fall in a no man's land.

War & Terrorism: Food and beverage conglomerate Mondelez International became a victim of the Not Petya ransomware attack in June 2017. It filed a claim to the tune of USD 100 million with Zurich Insurance for losses attributed to the Not Petya cyber attack. This claim was repudiated based on the policy's war exclusion by the insurer. Mondelez case is the first case where an insurance company has invoked the exclusion to decline coverage for a cyber-attack. This created a situation where an exclusion has snatched coverage for one of the main risks the coverage was bought for. It is therefore necessary to understand the implications of the exclusion relating war and terrorism and get dispelled any doubts before buying the cover.

Absolute Exclusions:

Exclusions can be "Absolute" exclusions and "For" exclusions. Absolute exclusions eliminate coverage completely for claims irrespective of whether they are directly or remotely connected to the primary nature of exclusion. These mostly relate to specific events like Pollution, Pandemic or Cyber attacks etc.These have always been a matter of concern. But, following the recent upsurge in event triggered claims, whether it is cyber risks or Covid 19, absolute exclusions are beginning to find place in many policies and it has become necessary to review the policy document with a fine tooth comb to understand the irimpact. Absolute exclusions may negate coverage in an unexpected manner. Even insurers could not escape the unexpected outcome, as can be seen from the following excerpt from an IRMI article "Beware of "Absolute" Insurance Policy Wording" .

"The insurer issued a pollution liability policy to one of its Insureds. The insured was sued by a third party for pollution, and the insurer, in turn, denied coverage. Following the denial, the insured sued the insurer, alleging bad faith. Yet, because the insurer's own insurance company E&O liability policy contained an "absolute" pollution exclusion, coverage for the bad faith lawsuit against the insurer was denied. This was despite the fact that the insurance company was not the polluter and, ironically, the insurer's premium volume received for writing pollution liability coverage was used (in part) to

calculate its premium when purchasing its E&O policy! Such language - to at least one attorney's delight-is being upheld by courts with increasing frequency."

When an exclusion cannot be avoided, insurance buyers should negotiate to reduce the fallout of absolute exclusions by getting the exclusions tied to their (Insured's) primary acts. Additionally, carve back of coverage can also be sought – for aspects like defence costs and derivative suits etc. Absolute exclusions deleting coverage for claims "for, based upon, arising from, in consequence of, or related to, directly or indirectly" should ideally be resisted. Wording that exclude coverage only "for" the claims, ought to be the preferred option.

It may be noted that in India, any exclusion imposed by insurer has to be in conformity with the "Guidelines on Product Filing Procedures for General Insurance Products" issued by Insurance Regulatory and Development Authority of India (IRDAI). Relevant provisions as mentioned in CHAPTER II GUIDING PRINCIPLES FOR PRODUCT DESIGN AND RATING are as under:

6. Product Development

(g) The design of insurance product should take care of Policyholders' reasonable expectations. Insurance product design should ensure transparency and clarity in wordings, terms, coverage, exclusions and conditions in order to devise a fair and balanced risk transfer mechanism through insurance.

(l) The terms and conditions of cover shall be fair between the insurer and the insured. The conditions and warranties should be reasonable and capable of compliance and in conformity with various laws, regulations, guidelines and circulars. The exclusions should not limit cover to an extent that the value and intent of insurance is lost.

All exclusions need to be filed with the regulator as a part of the filing procedure.

While buying cyber insurance, it is necessary to align it with other covers of the company broadly undertaking the following steps to make the insurance programme truly responsive:

- Cyber exposure analysis in terms of severity and frequency under various lines of insurance taking the help of the specialists.
- Understand current coverage and exclusions under various insurance policies.
- Identify the gaps/uninsured cyber risk.
- Identify classes which need inclusion of cyber coverage.
- Work with insurance intermediaries/ carriers and try to achieve ideal balance between premium and coverage.
- Continuously monitor developments because of the dynamic nature of the subject including new exposures like thermal scanning of employees and visitors and work on course correction in terms of risk management measures as also appropriate insurance coverage.

Insurance is neither the primary nor the only line of defence. It is complimentary to the best practices and best processes. That cyber insurance is critical in the risk management armoury of a company and it is a complex product are not in doubt. Complications arise because of multiple wordings. There is a need to understand nuances and finer points. What kind of a policy and from which carrier it is bought matters.

Insurance is neither the primary nor the only line of defence. It is complimentary to the best practices and best processes. That cyber insurance is critical in the risk management armoury of a company and it is a complex product are not in doubt. Complications arise because of multiple wordings. There is a need to understand nuances and finer points. What kind of a policy and from which carrier it is bought matters.

There should not be any illusion that it is possible to cover all exposures under an insurance policy. It is not. Hence, it is necessary to know what is covered, what is curtailed and what is excluded. Well

informed decision making matters.

P. Umesh

Consultant - Liability Insurance

p.umesh@liabilityinsurancepractice.com

www.liabilityinsurancepractice.com

References:

- Cybercrime damage costs may double due to Coronavirus (COVID-19) outbreak https://www.prnewswire.com/news-releases/cybercrime-damage-costs-may-double-due-to-coronavirus-covid-19-outbreak-301027007.html
- Allianz Risk Barometer 2020 – Identifying The Major Business Risks For 2020 https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2020.pdf
- Columbia Casualty v. Cottage Health System, i.e. when your cyber-insurance is not what it seems https://www.technethics.com/blog/columbia-casualty-v-cottage-health-system-i-e-when-your-cyber-insurance-is-not-what-it-seems/
- Cyber-insurance: merchant pays almost $2 million in assessment fees.https://www.internationallawoffice.com/Newsletters/Insurance/USA/Mendes-Mount-LLP/Cyber-insurance-merchant-pays-almost-2-million-in-assessment-fees
- Mondelez's action against its insurer reveals potential issues in cyber insurance https://www.insurancebusinessmag.com/asia/news/cyber/mondelezs-action-against-its-insurer-reveals-potential-issues-in-cyber-insurance-164052.aspx
- Beware of "Absolute" Insurance Policy Wording https://www.irmi.com/articles/expert-commentary/beware-of-absolute-insurance-policy-wording