NCIGF | National Conference of Insurance Guaranty Funds

Considerations for Insolvency Practitioners presented with Cyber Security Claims

I. Introduction

Cyber security insurance coverage is trending into the admitted market. Consequently, NCIGF anticipates the insurance insolvency resolution system will be presented with claims and other issues related to this coverage. These policy obligations may flow both from standalone cyber policies, endorsements, or from coverages that may be found to exist in commercial general liability and other lines of business typically written for business entities. For this reason, policymakers need to determine how such coverages will be handled should an insurer writing this business become insolvent. While each jurisdiction will need to decide whether, and within what parameters, cyber claims will be covered, we offer for consideration and guidance the attached amendments to the NAIC Property and Casualty Insurance Guaranty Association Act (NAIC Model 540). Policy makers should also consider how such claims will be handled before guaranty funds and associations (hereinafter "guaranty funds") are triggered – for example in a rehabilitation proceeding. Likewise, current insolvency processes and transition to the guaranty funds will need to be changed and enhanced to deal with this unique line of business and especially its demanding claims administration standards. For the purpose of this discussion, we offer the following information:

II. Key Cyber Insurance Facts and Characteristics

1) Cybersecurity ("Cyber") Insurance is a generalized term that covers a range of first-party and third-party policy coverages and benefits. While a policy could include various triggers, typically policy coverage is implicated by an unauthorized access to a computer system and/or by unauthorized access to or use of private or confidential information. Examples could include ransomware, malware, theft or loss of a device, improper disclosure of protected information, and more.

2) Policies often offer a policyholder as a policy benefit the opportunity to engage service providers to investigate a suspected infiltration, to give legal advice about a policyholder's regulatory or statutory reporting and notification obligations, to send notifications, and to give benefits to affected persons, such as credit monitoring. There may be coverage for the services of a ransomware negotiator and for a ransom paid in response to cyber extortion. The policies often include coverages directed to recovering or recreating data or access to data compromised by the incident. They may also afford business interruption coverage. In addition, policies generally provide liability coverage, including the provision of a defense, triggered by specific types of allegations or claims. Some policies contain e-crime coverages

such as social engineering losses, fraudulent instruction losses, etc.

3) There are currently no standardized Cyber Insurance policy forms, but the sample policies we have examined do have many characteristics of P&C insurance. While many descriptions of Cyber Insurance, such as those written by brokers and others promoting such insurance, do not convey this underlying reality, Cyber Insurance policies are similar to other conventional insurance coverage. Some of these similarities are described below.

4) Although Cyber policy forms are not standardized (in contrast to ISO forms, for example), there are trends toward certain common characteristics in these policies, including the following:

   a) Most, if not all, policies are written on a claims-made basis.
   b) Most typically, these policies have aggregate limits, with a current trend toward lower limits.
   c) Often there are sub-limits applicable to certain types of coverage.
   d) Amounts expended under the policy, including defense costs, typically erode the aggregate limits and, where applicable, appropriate sub-limits.
   e) Policies generally include retentions or deductibles to be borne by the policyholder, although a retention may be zero for some coverages, with a current trend toward higher retentions or deductibles.
   f) Generally, policies define all claims or losses arising from the same incident to be a single claim or loss.
   g) Some policies require a policyholder to use incident response (breach response) service providers from a preapproved list of vendors. Others may require prior mutual agreement to the retention of a particular service provider. As to defense counsel under a liability insuring agreement, prior mutual agreement is commonly required.
   h) Policies may vary, including by insuring agreement, as to whether an insurer reimburses a policyholder (meaning the policyholder pays in the first instance) or pays on behalf of a policyholder.

5) Coverages are modular and will vary significantly, even among policies issued by a specific insurer.

6) The range of services paid for by or on behalf of the policyholder are varied and novel as compared to traditional P&C products. The insurer is typically very active in identifying service provider options for the policyholder to consider engaging in terms of appropriate legal representation (including notification obligations), cyber forensic services and other ancillary services needed for regulatory compliance.

7) Another defining characteristic of Cyber Insurance is the required timeline for the insurer's response in the event of a triggering incident. Ideally, a policyholder's first notice of loss is given as soon as possible upon discovery, an insurer's response also must be very quick, and

any appropriate contact with breach counsel, computer forensics, and cyber extortion services vendors is arranged within a short time and with urgency. In summary, the timeline for responding to and servicing the claim is extremely short compared to typical property & casualty claims.

8) A significant benefit of the bargain for some policyholders, particularly small and middle market businesses, is obtaining the insurer's expertise in providing the policyholder access to qualified service providers to engage for the investigation of a cyber intrusion and breach response tactics, as well as legally evaluating and assisting with the complex regulatory compliance often required in such circumstances.

9) Cyber Insurance often covers ransomware extortion payments, even though United States policy strongly discourages such payments. Such payments have potential implications for compliance with OFAC (Office of Foreign Asset Control), sanctions, and perhaps other laws. We understand, however, that insurers do sometimes negotiate and pay such fees. There are also troubling trends shown in the data with implication for this coverage discussion: smaller companies are most frequently victimized by ransomware. We believe this coverage will need to be carefully evaluated in the discussions about Cyber Insurance.

10) The market for Cyber Insurance is dynamic and growing. While larger policyholders often have stand-alone Cyber Insurance policies, for some smaller insureds, Cyber Insurance coverage is more likely to be endorsed on to some other kind of policy, such as a CGL(Commercial General Liability), BOP(Business Owner's Policy), or Professional Liability policy. That said, there are also stand-alone policies for smaller insureds and that approach appears to be expanding. There are also some smaller specialty insurers that write Cyber Insurance coverages in the middle and main street markets.

11) Premium reporting for Cyber Insurance is somewhat uncertain because it is not its own line or classification. This appears to be changing, but the publicly available historical premium and experience data is limited. In general, however, and putting surplus lines Cyber Insurance aside, we believe that premiums for admitted Cyber Insurance generally are currently reported within the guaranty fund's assessable lines. This is an important distinction.

12) Cyber liability claims may also arise from CGL, medical malpractice, legal malpractice, and other commercial lines, sometimes referred to as "silent cyber" coverage.

III. Issues to Consider

Insolvency practitioners should consider the following issues:

1. What are appropriate guaranty fund limits if a jurisdiction decides to cover cyber claims?

While industry loss reporting for Cyber Insurance is not formally administered as such by a rating or advisory agency, the available voluntarily reported data indicates generally that the average claim for small and medium size businesses under these policies would fall within the claim cap (see attached 2021 claims study report). The claims costs for 2020 were materially higher than prior years. It is difficult to predict the future threat landscape and thus future claims costs, as the escalation in attacks is being met with a variety of defensive and mitigation strategies. At this juncture, however, the typical guaranty fund claims caps of $300,000-$500,000 should provide reasonably adequate coverage for most small and medium size businesses in most states. The statutory amendments offered in our revisions to the NAIC Model Act call for only one claim cap per incident.

2. Should the guaranty funds and receivers use vendors established in the policy to provide various services such as breach coaching, notification, forensics, etc.?

Sometimes use of certain vendors is mandated by the policy or accompanying documents. It may make sense for the receivers and guaranty funds to make use of pre-established vendors if they are still available, especially considering the short timelines in play for response on Cyber Insurance claims response. As we are all aware, however, sometimes vendor relationships can be disrupted in a liquidation context. It is thus advisable to expressly maintain the guaranty fund's statutory power to select counsel and service providers and direct the provision of legal and other services. Moreover, receivers should be prepared to address these services in a troubled company context. This issue is likely to require cooperative and innovative solutions.

3. What are considerations for amending guaranty fund acts and potentially other insolvency law that policymakers should take into account? ?

Guaranty fund laws are amended infrequently – any amendment should stand the test of time. Other typical guaranty fund provisions, such as the purpose clause, warranty exclusion, deemer provisions, and fine and penalty exclusions, should be reviewed in order to avoid conflicts with any Cyber Insurance amendments. Policymakers should also review net worth provisions embodied in many guaranty fund acts to ensure that claims payment and services provided on an expedited basis will be properly recovered from high net worth insureds as Cyber Insurance claims will require claims administration on a compressed timeline incompatible with high net worth vetting. As always and given that this coverage is also written on a surplus lines basis, it should be clear that GA coverage extends only to licensed business and does not extend to claims on surplus lines policies.

IV. Conclusion and Request for Collaboration

Finally, we ask that the NAIC and other policymaking bodies who are considering statutory amendments or other measures to address Cyber Insurance claims work with the NCIGF to develop solutions. The NCIGF Legal Committee has spent considerable time studying this

matter and the NCIGF wants to share the benefits of the knowledge acquired with the NAIC and other appropriate stakeholders in order to ensure that appropriate policy claims and claims related services for insurance consumers are not disrupted, thus upholding the insurance promise.