Insurance Resolution: Preparing for Cyber Claims

By: Tim Schotke, Chad Anderson, John Blatt

Introduction

Cybersecurity insurance ("Cyber") is a rapidly growing, relatively immature segment currently making industry headlines for emerging risks and high-stakes coverage disputes. Cyber introduces new challenges from the resolution perspective. The uniqueness of these claims calls for a specialized approach for Cyber carriers, from regulation to resolution.

While many Cyber *Liability* policies may simply reimburse for business interruption or other losses after the fact, other Cyber insurance products promise a full suite of legal, technological and regulatorily-mandated services to policyholders. Such products differ from the property and casualty policies normally handled by P&C receivers and guaranty funds which consist almost exclusively of payments for losses. For coverage to be in any way effective, it is essential that specialized services such as legal breach coaching and digital forensic analysis be delivered to the policyholder within minutes or hours of an incident being reported, rather than days or weeks.

A regulator or receiver stepping into a troubled Cyber writer may not have any experience taking in these claims and interfacing with this unfamiliar class of vendors. When such a company is liquidated, affected guaranty funds may not be prepared to expedite coverage determinations and may not have access to the information needed to process Cyber claims.

The purpose of this paper is to identify areas where the resolution system must work together to ensure an adequate level of pre-liquidation planning. Doing so will ensure that both receivers and guaranty associations are prepared when a Cyber insurance carrier enters the system. Whatever the challenges, we share a responsibility to ensure protection is delivered to the policyholders in a meaningful timeframe.

Background

Cyber insurance is growing rapidly both in the amount of coverage in force and in the number and cost of claims. The NAIC's September 12, 2019 Report on the Cybersecurity and Identity Theft Insurance Coverage Supplement (appended) indicates that for those companies that completed the Supplement to the P&C Annual Statement in 2018, approximately 500 insurance companies were selling Cyber coverage, with just over $2 billion in 2018 premiums. This is up slightly from $1.89 billion in 2017 premiums. Cyber coverage is sold as a stand-alone policy, as a bundled coverage, or as an endorsement or rider attached to an underlying insurance policy. When including premiums from endorsements and riders, the total premium for the Cyber market is much higher, at roughly $3.6 billion. This number has increased each year with no signs of slowing down.

A typical standalone Cyber policy is a complex product that provides services to policyholders in addition to payments for losses. Companies vary in the products they offer, with some allowing the policyholder to develop a customized bundle of coverage from a comprehensive menu of offerings. Elements of a Cyber policy can include:

- Claim Management – first-party costs for legal, forensic, public relations and other claims costs;
- Security & Privacy – third-party liability coverage for damages, mandatory costs, and legal defense;
- Ransom & Extortion – Ransomware and similar risks (somewhat similar to a kidnapping and ransom policy), which may include securing a ransom payment in the form of cryptocurrency;
- Business/Network Interruption;
- Regulatory – cost of compliance with public investigations and state data breach notification requirements; and
- Specialty – which includes D&O and E&O coverage, among other things.

Standardized Cyber policy language is not in use, and the policy language being used by those insurers with a lower degree of experience and expertise may not have been given adequate analysis with respect to such emerging risks as "silent coverage". Silent coverage, or "non-affirmative cyber", is the concept of losses not excluded by policy language, but potentially not anticipated by underwriters or factored into premium and coverage decisions. Policy exclusions are evolving quickly but, like the policy forms themselves, so far have not been standardized across the industry to the authors' knowledge. Given the absence of standardized policy language, there is consequently the absence of a large, shared historical experience database to assist companies in underwriting and accurately pricing these products.

Financial Reporting

Clear financial reporting of Cyber exposure by companies is necessary for insurance regulators, receivers and guaranty funds to prepare themselves to handle Cyber claims. It is our understanding that no uniform direction exists for reporting Cyber premiums to regulators on the Exhibit of Premiums and Losses ("Page 14") within the P&C Annual Statements. While we presume that standalone Cyber policies may most often be reported as General Liability, an endorsement to a preexisting policy is potentially reported in the same line as the underlying policy (perhaps as Medical Malpractice premium, as discussed below). Although regulators and receivers have greater access to confidential company information, guaranty funds typically do not have access to that information pre-liquidation and must refer to publicly available information and court filings at the time public proceedings begin against the troubled carrier. The lack of a dedicated reporting line or field for Cyber premiums written makes it difficult for funds to determine whether a company wrote Cyber insurance. For example, Galen Insurance Company sold Cyber coverage as a rider to their Medical Malpractice policies. Because these endorsements were not distinct from the primary polices on publicly available documents, there was no advance notice to the guaranty funds of any Cyber exposure.

Regulators overseeing troubled companies may want to pay particular attention to those that are selling Cyber for any of the reasons above. However, the varied methods of issuing

Cyber coverage may present challenges for regulators in deriving an accurate aggregation of all the Cyber risk assumed by a particular insurer. The aggregate risk challenge also has implications for premium reporting and solvency regulation. The Exhibit of Premiums and Losses requires insurers to report premiums by line of business and is supplemented by certain interrogatories. Currently, there is no line for reporting Cyber on the Exhibit, which makes it difficult for regulators to develop a holistic measure of a given insurer's exposure to Cyber risk. The lack of clear reporting may also hinder the ability of receivers to quickly assess the risks the company presents. Further, guaranty funds are unable to accurately predict their funding, staffing and vendor needs in the face of a possible liquidation.

The entire insurance resolution system would benefit from the creation of a separate line to report Cyber exposure. When a company becomes troubled, these reports along with any interrogatory responses could then be shared with the guaranty funds pursuant to a confidentiality agreement to ensure the funds are properly prepared for any potential Cyber claims.

Enhanced Tools for Examiners

Financial examiners are the early investigators of a troubled company. When financial examiners are in the early stages of investigating a company, it may be beneficial for them to assess the true scope of the Cyber exposure for that company. Currently, the NAIC's Financial Condition Examiners Handbook provides guidance for examiners to determine the *internal* cybersecurity risk of a company related to its own systems, but does not provide any guidance on analyzing the exposure to that company from writing Cyber policies. With a more detailed analysis of the policy provisions offered and the relationships managed by the carrier, regulators will have a clearer picture of the company's Cyber exposure and an opportunity to put appropriate safeguards in place.

The NAIC's Financial Condition Examiners Handbook and Troubled Company Handbook provide guidance to examiners and regulators. Those tools could be enhanced through the development of an analytical checklist for Cyber insurance. Example checklist questions include:

- Does the company have Cyber coverage in force? If so, what is the premium volume and amount of total exposure?
- Is the coverage sold as a stand-alone policy?
- Is the coverage sold as a rider or endorsement to another more traditional coverage? If so, which coverages are included in the underlying policy to which the rider is attached?
- What are all of the different benefits that are provided under the Cyber coverage? For example, are in-kind services provided for IT support, credit monitoring, data breach notification, and forensic analysis?
- What arrangements does the company have in place to provide in-kind services and other non-indemnity benefits under the Cyber coverage? For example, does

the company have a panel of "breach coaches" who are familiar with the company's policies and the administration of benefits provided thereunder? Does the company have a Cyber claims "hotline" for claims reporting?

- Is coverage provided for government-imposed penalties, and if so, for which levels of government? For example, will state data breach penalties, Federal HIPAA penalties, or EU GDPR penalties be covered claims?
- What are the coverage triggers that are used in the Cyber policies? Are they "occurrence" or "claims made" policies? If the Cyber business is written on a "when discovered by management" basis, will a forensic report also be necessary to determine what management knew and at what time in order to trigger coverage?
- How many different Cyber policy forms, endorsements, or riders are in force?
- Are the Cyber benefits in actuality provided by a third party or fully reinsured?
- Is Excess Cyber coverage being provided?
- What are the range of limits provided under the various Cyber coverages?
- What are the largest limits provided on a single risk, across all layers?

Answers to the aforementioned questions will not only assist regulators, but also will give receivers and guaranty funds the tools to quickly determine company liabilities and be prepared to step in quickly and provide in-kind coverage to policyholders. Effectively administering these claims will require an increased level of coordination between regulators, receivers and the guaranty funds. It will also be interesting to reconcile the responses to these questions with the information contained on the Cybersecurity and Identity Theft Insurance Coverage Supplements filed by the troubled company.

Operational Readiness

Under more traditional property and casualty policies, it has been fairly straightforward to gain insight into the type and magnitude of the claims that a guaranty fund should expect by looking at the troubled company's annual statements. For the reasons expressed above, this will be difficult to carry out for Cyber writers unless some enhancements are made to the financial reporting of Cyber coverage by companies.

It will be helpful if financial regulators are able to share with receivers and guaranty funds on a confidential basis potential Cyber exposure in a troubled company facing liquidation. The "prevention and detection of insolvency" language found in most guaranty fund statutes may allow insurance departments to confidentially share certain information about a troubled company with a guaranty fund. In some cases, a standing confidentiality agreement for this purpose may be desirable. Early warning efforts from insurance departments will be important to receivers and guaranty funds so that they can prepare to appropriately protect policyholders and claimants under this line of coverage.
If a Cyber insurer falls into receivership or liquidation, receivers and guaranty funds will be required to provide the specialized services and benefits promised under those policies.

As neither has a history of providing such services, receivers and guaranty funds will need additional lead time to analyze the Cyber contracts of the troubled company and establish contractual relationships with the same or similar vendors. It is important that guaranty funds and receivers become familiar with all aspects of handling Cyber claims, develop Cyber claims handling plans, and identify potential vendors and experts to provide the most common specialized services found as benefits in a Cyber policy.

It will be essential to the administration of a troubled Cyber insurance writer that regulators, receivers and guaranty funds collaborate early in the process to share relevant policy information, plan for retention or replacement of specialized vendors, and coordinate the handling of both existing and newly-reported claims.

Coverage and Priority Issues

Receivers and guaranty funds in each state should also consider likely points of stress when Cyber claims begin to interact with their statutes. In each state, they will need to consider coverage questions such as the proper application of claim caps and, given the compressed response timeline, an approach to "covered claim" determinations and dealing with non-covered claims. These are just a few of the issues that must be answered *before* the first challenging Cyber insolvency occurs.

Conclusion

The orderly resolution of a company that writes Cyber insurance will require tangible changes to the way our system collects and shares information. We recommend that the NAIC, IAIR and the NCIGF consider the following steps:

- Create a more transparent reporting structure by requiring Cyber premiums to be reported separately on the Exhibit of Premiums & Losses ("Page 14");
- Develop a checklist and special interrogatories for financial examiners evaluating insurers that write Cyber policies;
- Amend the Receiver's Handbook to advise early engagement, including sharing of relevant confidential information, with the guaranty funds;
- Advise receivers and guaranty funds to establish a bank of vendors to ensure in-kind services are seamlessly provided on Cyber claims during an insolvency; and
- Ask guaranty funds to examine their statutes and establish plans for expediting "covered claim" determinations for certain newly-reported Cyber claims.

There is much to be done before the state resolution system is fully prepared for the smooth resolution of an insolvent Cyber insurance carrier, but now is the time to put in the work. With cooperation, we can address these challenges and guarantee protection for the policyholders in this growing and rapidly developing segment.