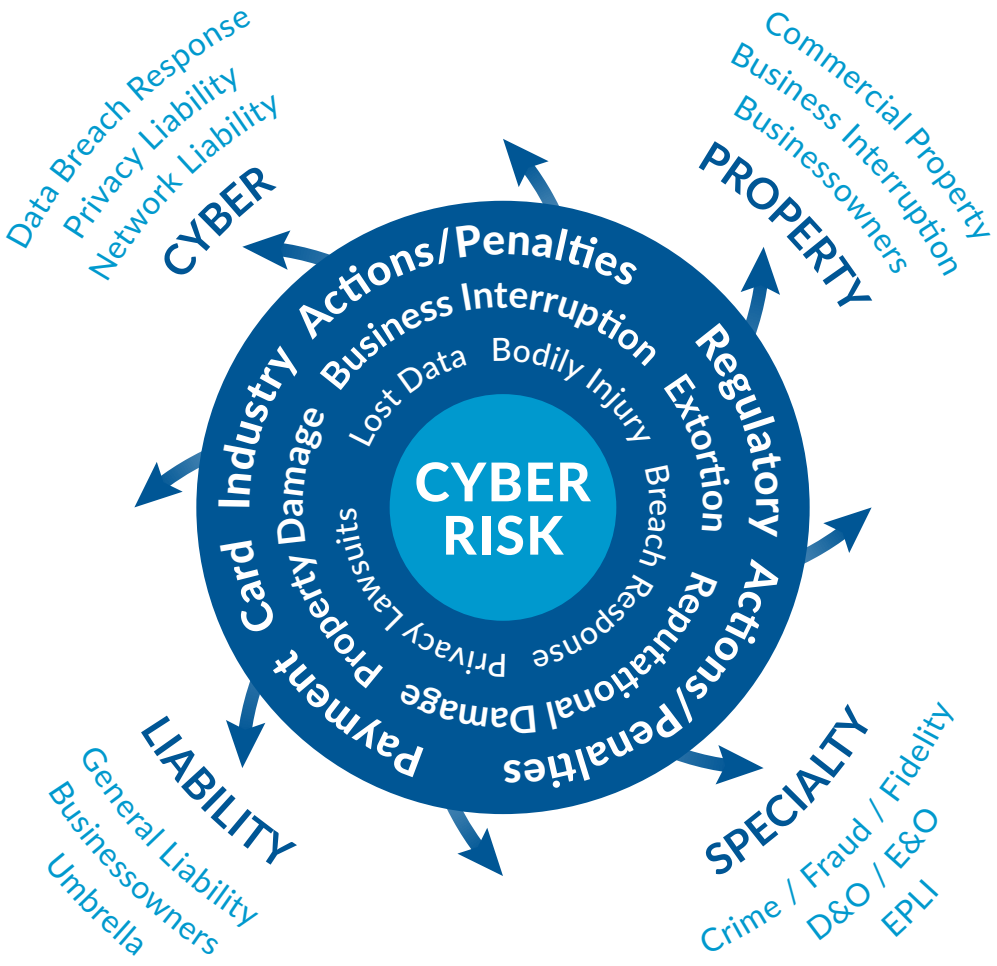
Gen Re

CYBER AND INSURANCE

Do You Know Where Your Cyber Exposure Is?



Cyber vs. Data Breach Terms

We generally use the term "Cyber" to refer to the various exposures and insurance offerings for data breaches, privacy liability, fines and penalties, network liability, extortion, business interruption, data restoration, media liability and any other coverages that an insurer may include in a Cyber policy. There is no one standard definition or policy form.

"Data Breach" is typically a subset of Cyber, and refers to the loss of or unauthorized access to private information, and related remediation obligations. Some policies in the market cover only data breach-related losses, which can mean breach response costs and/or privacy liability from a breach. Other policies extend to all or most of the Cyber coverages noted in this article.

There is truly a broad spectrum of insurance options. The scope of *your* Cyber or Data Breach insurance products will shape your exposures to any cyber event.

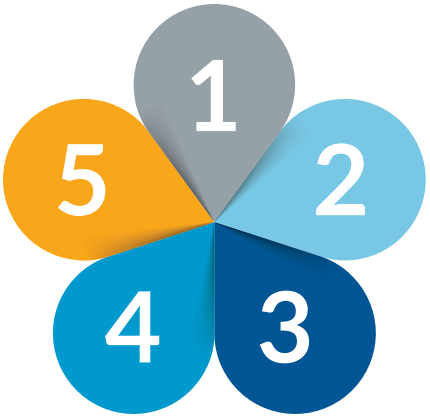
introduction

Many insurers assume Cyber exposure by underwriting specialized policies and endorsements. However, a large number of insurers are learning that they also insure Cyber risk under their traditional insurance products.

One source is explicit coverage under Cyber policies; the other is more of a "silent" coverage under other commercial policies. Whether explicit or silent, the costs can add up. *What is the sum of all this Cyber exposure?*

Rating agencies, regulators, business partners and board members are asking insurance company managers this question and expecting answers. While each constituent may have different motivations, their questions are similar. Each would like to understand how an insurer would perform following a major cyber event.

Does the insurer maintain sufficient resources and resiliency to withstand and service a major influx of claims following a significant cyber event? Will its reinsurer—and reinsurance recoverables—weather the storm?



5 questions

Insurers must first understand where and how they are covering Data Breaches and Cyber Liability in their existing property and casualty portfolios. There are five questions that should help an insurer gain an understanding of the totality of its Cyber exposure.

1. What is my exposure under traditional Commercial General Liability policies?
2. What is my exposure under Property, Crime/Fraud/Bond and other traditional first-party policies?
3. What is my exposure under specialized Cyber policies versus traditional policies?
4. How does my reinsurance address Cyber across my insurance products?
5. How will regulators, rating agencies, business partners, policyholders and board members measure my Cyber exposure and resiliency?

These are heady questions to arise out of a single court opinion on a CGL policy. However, these questions were always there. The federal court ruling, coupled with growing rating agency and regulatory scrutiny of Cyber exposure, raises the profile of Cyber exposure.

Where is my Cyber Exposure under traditional General Liability policies? What if I have an exclusion in those policies?

The recent U.S. Court of Appeals decision sparking so much discussion is *Travelers Indemnity v. Portal Healthcare Solutions*,[1] a data breach class action testing CGL coverage. The insured, a healthcare services firm, left patient data exposed on the Internet for four months. Two patients made this discovery and then filed a class action against Portal Healthcare alleging negligence and breach of warranty and contract. There was no indication that third parties had accessed the confidential information. The insured presented the lawsuit to Travelers for a defense. Portal's insurance policies covered Personal Injury arising from the "electronic publication of material" that "gives unreasonable publicity" or, in the later version, "discloses information about" a person's private life.

The question before the court was whether the insured's potential liability arose out of "Personal Injury" and, in particular, an electronic publication that satisfied the publicity or disclosure requirements in the policy. The Fourth Circuit concluded that providing access to private medical information on the Internet was a publication satisfying the policy, without the need for a third party to have actually seen or used that information. The policy form was not ISO, where the publication must "violate a person's right of privacy." However, the differences in policy language do not seem material in view of the court's decision and reasoning.

The bottom line: *There was CGL defense coverage for a data breach liability claim.*

The critical subtext: *The policy pre-dated the appearance of Bureau BOP, CGL, and CU exclusions aimed at keeping all data breach coverage out of these commercial general liability policies.*

To date, the decisions considering BOP, CGL or CU coverage for data breach loss and liability have involved policy editions in use before the introduction of mandatory "data breach" exclusions. Starting in 2013, ISO, AAIS and MSO filed exclusions to address the growing concerns about data breaches and cyber events. The intent was to make even clearer that a specific Cyber policy coverage grant would be the appropriate place to find coverage, where the exposure would also be properly rated and underwritten. ISO's version, entitled "Access or Disclosure of Confidential or Personal Information," excludes damages arising out of:

> *"any access to our disclosure of any person's or organization's confidential or personal information, including patents, trade secrets, processing methods, customer lists, financial information, credit card information, health information or any other type of nonpublic information."*[2]

Had the Portal policy been a more recent form with a Bureau or similar proprietary exclusion, it is likely that the data breach class action would not have been covered. Making personal or confidential data available on the Internet would seem to fit squarely into the "access to or disclosure of" language.

That leads to the first aha moment: If the insurer has adopted the ISO, AAIS, MSO or a similar data breach exclusion in its commercial products, its BOP, CGL or CU exposure from such a breach should be limited. Has your company adopted a bureau or proprietary exclusion for your BOP, CGL or CU policies? If not, the *Portal Healthcare* decision should be a wake-up call.

The decision does not mean that coverage will be found for all data breach liability claims. The outcome would depend on the facts of the breach and the law of the jurisdiction. For example, the New York trial judge in the Sony PlayStation litigation ruled that there was no CGL coverage because a criminal hacker published the personal information, not the insured.[3] The decisions are still sparse, and until a body of law has developed on the "publication" question, insurers are left with uncertainty and litigation risk on policies without the exclusion.[4] (See page 6 for more.)

This much is certain: If an insurer wishes to exclude liability from data breaches, an explicit bureau or proprietary exclusion for "access to or disclosure of" confidential information should work better than remaining silent. Without the exclusion, coverage is possible and in some jurisdictions likely.

Aligning Primary CGL and Umbrella

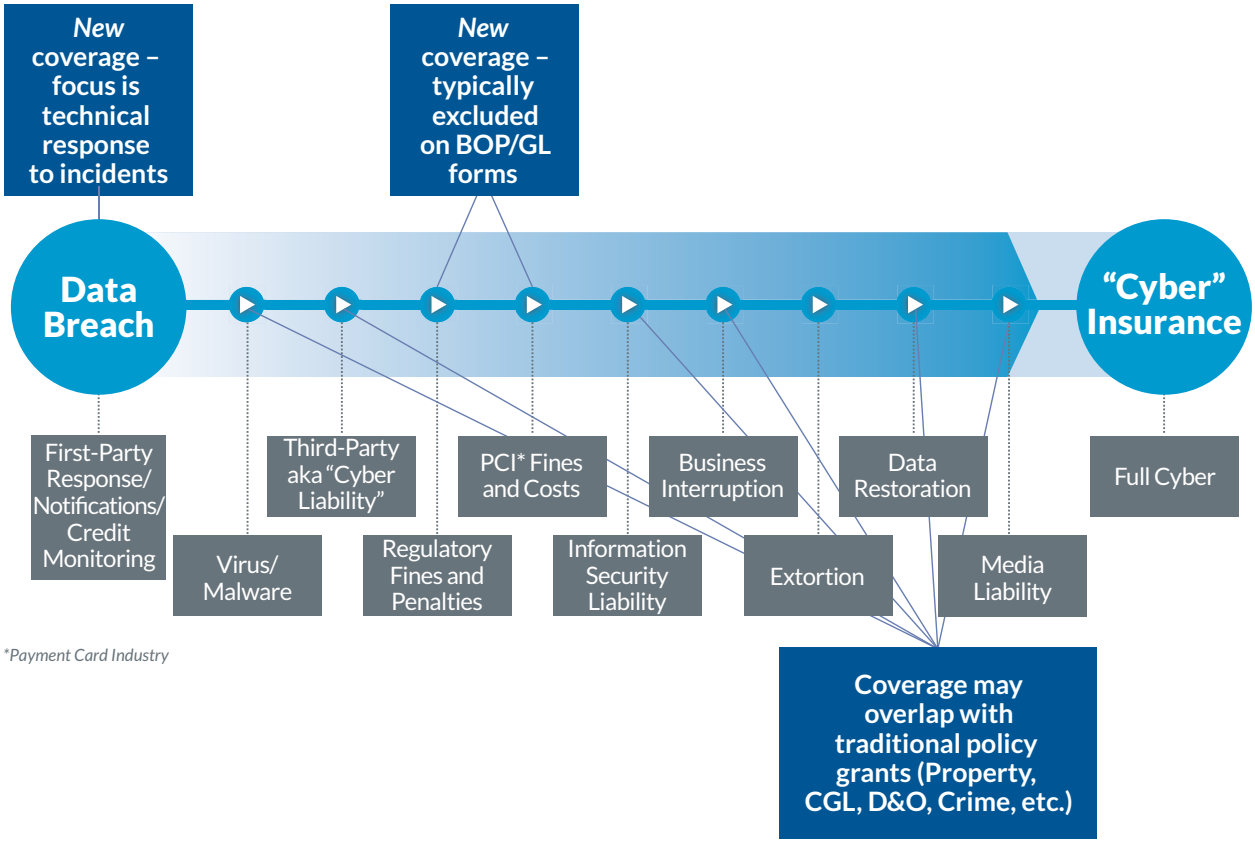
It would be remiss to not mention the importance of aligning primary and commercial umbrella policies for cyber exposures. Unintended drop-down scenarios can be prevented by addressing these issues:

- If the insurer writes the primary and umbrella, do both forms have a Data Breach exclusion? Is it the same Data Breach exclusion?
- If the insurer writes an umbrella over a different company's primary, does the umbrella insurer know if there is an exclusion in the primary? Is the language consistent?

Fortunately, all the bureaus have BOP, GL and CU exclusions available. The question is whether insurers are using—and aligning—all of them.

Cyber Coverage Spectrum

New Coverage/Overlapping Coverage



Was There GL Insurance Coverage for the Data Breach?

A sampling of court decisions shows a split in view. **All rulings pre-date recent bureau Data Breach exclusions.** Here is how the courts answered the question on the specific facts and policy language:

No: Theft of credit card information from the computer network was not Property Damage because the policy excluded "electronic data" and stated it was not tangible property. *RVST Holdings v. Main Street America Assurance*, 2016 N.Y. App. Div. LEXIS 1205.

Yes: Personal information left accessible on the Internet was a publication under Personal Injury provisions of a GL policy. *Travelers Indem. V. Portal Healthcare Solutions*, 2016 U.S. App. LEXIS 6554 (unpub.)

No: Lost tapes with employee personal information that fell off of a truck in transit were not a publication violating a right to privacy without evidence that they were accessed and or caused loss to the employees. *Recall Total Information Management v. Federal Ins.*, 2015 Conn. LEXIS 150.

Yes: Computer frozen by virus in vendor's software resulted in "loss of use of tangible property" because, unlike data, a computer was tangible property under the policy. *Eyeblaster v. Federal Ins. Co.*, 2010 U.S. App. LEXIS 15152 (Note that the policy in question did not appear to contain an Electronic Data exclusion).

No: Mere access to personal data by hackers was a publication, but Personal Injury coverage only applied to violation of privacy by the insured and not by third-party hackers. *Zurich American Ins. v. Sony*, 2014 N.Y. Misc. LEXIS 5141.

2 Would my Property policy pay for a cyber event? What other lines of insurance could be the source of Cyber coverage in my book?

Other policies may come into play in a data breach or cyber event, not just the liability coverage in commercial forms. ***Even with the data breach exclusion in GL, BOP and CU products***, a Cyber claim may trigger some amount of traditional coverage. As is always true, the specific language of the insurance policy and facts of the claim will determine if and how much coverage exists.

- **Property—Physical Damage.** The major exposure involves a cyber attack triggering a covered peril that damages physical property or sets into motion events that cause physical damage to property. Consider when a hacker turns off temperature controls on machinery and a fire erupts. Was there direct physical damage from a covered cause? In some situations, the typical property policy covers the fire loss. An exception, depending on state law, may arise for hacking that is classified as terrorism. Most carriers are by now aware of the significant exposures and claim challenges in even discovering whether a cyber attack was involved in a physical loss.

- **Property—Additional Coverage.** There are several sources of data breach and Cyber coverage in ISO's Commercial Property (CPP) and BOP policies, albeit subject to sublimits. ISO revised its Commercial Property forms in 2002 and its BOP forms in 2006 in response to a court decision finding first party coverage for loss from the inability to access electronic data. The Bureaus went on to exclude Electronic Data, but gave limited protection back in a sublimit. These ISO provisions or similar alternatives are important to determining how the Cyber policy or coverage endorsement will respond.

  - ***Electronic Data Coverage***—*Additional Coverages: The "cost to replace or restore 'electronic data' which has been destroyed or corrupted by a 'Covered Cause of Loss'"* is covered up to $10,000 in the aggregate under the ISO BOP ($2,500 in the CPP). The provision specifies that "*a computer virus, harmful code or similar instruction*" is a Covered Cause of Loss. An exception to this data damage coverage is for intentional acts by employees and vendors. Many insurers offer ISO or proprietary enhancements increasing the sublimits and/or scope of coverage for damage to or loss of electronic data.

  - ***Interruption of Computer Operations***—*Additional Coverages: If operations are suspended by "an interruption in computer operations due to the destruction or corruption of 'electronic data,'"* an additional $10,000 in the aggregate under the ISO BOP ($2,500 in the CPP) is available for lost business income and extra expense. The same language applying coverage to a computer virus and harmful code (malware), as well as the exception for intentional employee and vendor acts, applies to this additional coverage.

  - ***Valuable Papers and Records***—*Coverage Extensions:* As a counterpart to electronic data destruction, this section provides up to $10,000 ($2,500 in the CPP) to recreate lost or stolen paper. Unlike the Additional Coverages above, this coverage limit applies on a per occurrence basis.

- **Crime, Computer Fraud and Fidelity Bonds.** In some instances of fraudulent access to systems to take money or other valuables, a crime or similar policy can be a source of coverage. There are, however, often policy limitations that could preclude coverage, e.g., for theft being "direct" (covered) versus "indirect" (excluded). As with other insurance coverage issues, the question of causation and state causation law came into play in the recent *State Bank v. Bancinsure* case involving social engineering and a Financial Institution bond.[5] In this case, malware residing on an employee's computer, combined with an employee error, had allowed a hacker to transfer funds from the insured's bank into a foreign account. The insurer pointed to several exclusions for loss caused directly or indirectly by employees, or that compromised confidential information. Minnesota recognizes the "concurrent causation doctrine" and looks to the efficient proximate cause of loss. The Eighth Circuit appellate court first held that the "directly or indirectly" language was not sufficiently clear to circumvent the concurrent causation doctrine. It went on to find that computer systems fraud was the "efficient proximate cause" of the loss, not employee error or other excluded actions.

  Causation rules have influenced other court decisions finding coverage.[6] More court decisions are expected soon where "phishing" or other social engineering claims test coverage when employees were tricked into transferring funds to criminals. The New York litigation in *Medidata Solutions Inc. v. Federal Insurance Company*[7] is one to watch for the question of whether the computer crime and fraud coverage applies when an employee transferred funds, rather than the money being taken by the criminal as in the *State Bank* case. Many bonds now have exclusions for the loss of personal or confidential information. That will help insurers in some loss scenarios, but as *State Bank* indicates, not all of the cyber scenarios.

- **Employment Practices Liability Insurance—Invasion of Privacy.** An insured business is also a workplace, and breaches of certain data can affect employees as well as customers. When employee personal data is the subject of a breach, employers could be hit with a claim for violation of privacy.

  The ISO EPLI policy defines "wrongful act" to include "libel, slander, invasion of privacy, defamation or humiliation." Most EPLI forms in the market are proprietary, and the language will vary. Many will cover an "oral or written publication" of material that violates a right of privacy, and the question of what constitutes a "publication" could arise here as well. We have not yet seen any coverage decisions in the EPLI context. At present, the ISO EPLI policy does not contain any "data breach exclusion." The rationale for using an exclusion would be the same as for GL or BOP: Data Breach and Cyber Liability are best handled under a policy designed for that exposure.

The bottom line: Many insurers are likely to have Cyber exposure from more than one product.

The critical subtext: Depending on the claim facts and form language, insurers may have exposure under traditional commercial policies in addition to that under their specialized Cyber policies.

Getting a handle on that total exposure requires a comprehensive policy review with underwriters, legal, claims and other professionals in the company. If you are writing Cyber policies, or plan to, a review of those forms is in order. To truly evaluate your Cyber and other coverage from a breach or attack, you need to understand how these covers work *individually and together*.

Note: Since most insurers in the SME (small/medium-sized enterprises) space do not issue D&O and/or E&O policies, we do not dwell on those coverages in this article.

3 What is my exposure under specialized Cyber policies versus traditional policies?

For insurers not issuing explicit Cyber policies, the coverage inquiry ends with traditional policies. For those that write explicit Cyber-related coverage, whether stand-alone or by endorsement, a significant source of exposure remains. After a Cyber event, insurers might look here first for obligations and that would be a natural step. It is just not the only step. In addition to the traditional covers, insurers need to evaluate the scope of coverage, limits and sublimits in their Cyber policies. The Cyber insurance marketplace offers a wide spectrum of coverages and little standardization.

How much loss is covered by your Cyber policy? Is your policy first-party only for breach response costs, or does it include privacy liability and network liability to third parties? Do you include protection for government or industry fines and penalties?

Some provisions critical to exposure are not so obvious. For example, is coverage "primary" or "excess over other insurance? The "which policy pays first" or "which policy pays it all" question is usually answered by reference to "Other Insurance" conditions or, in some cases, Exclusions. In general, traditional ISO commercial policies are "primary" and pay first. If the Cyber policy is also primary, the insurers share the loss according to the method indicated. What if the Cyber policy says something different?

Some Cyber policies in the small business market make Cyber coverage "excess of other insurance." With this language, the insurer must reference other policies to sort out the ultimate place and amount of coverage. If a data privacy claim tests traditional GL coverage in a state without case law, or with a ruling like that in *Portal Healthcare Solutions*, the traditional liability policy could pay its limits before the Cyber policy ever kicks in. A similar outcome could result for first-party electronic data damage and business interruption losses.

Disputes over "who pays first" are a mainstay of coverage attorneys. In the case of Cyber, the issues are further complicated by the newness of Cyber forms. Will two or more forms become the subject of declaratory judgment (DJ) actions over coverage?

Cyber policies do not operate in their own exclusive silo. When a cyber event occurs, insurers need to take a broad look across their products and policies to find where the losses should go. This exercise is not just for their own obligations, but for another important reason: Reinsurance.

POINTS TO CONSIDER

- ✔ Limits and Sublimits
- ✔ Scope of Policy—Data Breach vs. Cyber
- ✔ "Excess Over Other Insurance"—Condition or Exclusion
- ✔ Other Policy Terms and Conditions

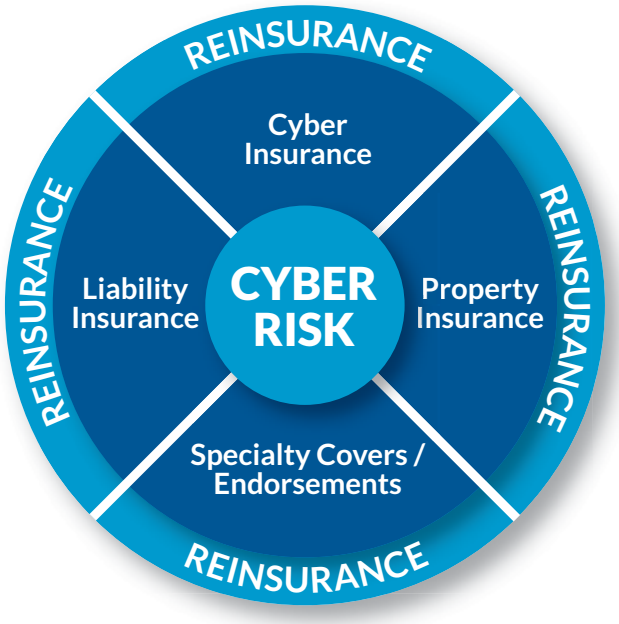
4 What are my reinsurance recoverables across the insurance products?

This analysis moves from insurance coverage to the implications of insurance coverage. More often than not, an insurer has very different reinsurance protection for its traditional commercial and specialized Cyber products.

In the SME (small/medium-sized enterprises) marketplace today, chances are that losses under the Cyber policy are 100% reinsured. In contrast, losses under traditional commercial policies are probably less than 100% reinsured, due to large retentions or sharing in the risk. Depending on where and how the loss is covered, the insurer could collect 100% or little to nothing. That makes the "where is it covered and who pays first" questions critical to determining an insurer's net exposure from a cyber event. As a *general* rule, insurers recover more if losses flow to the Cyber policy.

If the Cyber policy is primary, the insurer could recover 100% of the loss under the policy and, if adequate, there would be no loss, or shared loss, under traditional policies. If the Cyber policy is excess of other insurance, the answer could be different. If the claim has coverage under the traditional policy, the BOP, GL, property or other insurer pays first, and the loss flows through that reinsurance program subject to retentions and/or risk sharing. Even for a "Cyber" loss, the insurer could have significant net exposure depending on what the policies say and which reinsurance program is triggered.

In some scenarios the calculations are relatively simple. If the claim involves a data breach triggering forensics and notifications, for example, the Cyber policy is probably the only source of protection and 100% reinsurance is available. Breach Response costs are a "new" coverage not generally found in traditional policies. However, if a privacy lawsuit follows like the one in *Portal Healthcare* or the BOP picks up damage to electronic data, the coverage answer is not so simple or clear.



? Which reinsurance agreement(s) apply?

What is the retention?

What is the reinsured share?

5 How will insurance regulators, rating agencies and boards, among others, measure my Cyber exposure and resiliency?

If you have not yet asked these insurance and reinsurance coverage questions about your Cyber exposure, you can bet that regulators and rating agencies will. It does not matter that you have had no Cyber losses yet, or that you think the likelihood of a systemic cyber event is very low. Your regulators, rating agencies, boards and business partners could think otherwise. They see an increasingly hostile world and expect that insurers will be tested by cyber attacks. It is their job to see that you are up to the task.

The four R's—**reputation, regulators, rating agencies and resiliency**—are front and center for insurers with Cyber exposure. The drumbeat from these constituencies keeps growing louder:

- NAIC is moving to adopt model laws on cybersecurity.
- Some insurance departments are already using the NAIC drafts with their domestic carriers in the examination process.
- New York's Department of Financial Services issued recommendations for insurance company cybersecurity practices and policies, and other regulators may follow their lead.
- A.M. Best's SRQ directs insurers to report Cyber policies and premium as well as limits for the 25 largest policyholders, adding that "additional Cyber risk policy information may be requested."
- Fitch published a Cyber report warning that Cyber exposure is already embedded in existing policies and that significant accumulations could result.
- ISO issued a Cyber data call and is likely to fine-tune its products.
- Congress enacted the Cyber Information Sharing law that will ultimately lead to reasonable expectations around the standard of care to protect against and recover from cyber events.

> "If you cannot adequately demonstrate resiliency to cyber events, for practical purposes, you don't have it."

As Fitch noted, insurers are being asked to assess exposure of "events that are feared but not yet experienced in reality."[8] How will insurers show they have done the comprehensive analysis expected by these constituencies? If you cannot adequately demonstrate resiliency to cyber events, for practical purposes, you don't have it.

The answer to the resiliency question starts with knowing the answers to the basic coverage questions we posed for your Cyber and Commercial policies. ■

Endnotes

1 *Travelers Indemnity Co. of America v. Portal Healthcare Solutions*, 2016 U.S. App. LEXIS 6554 (unpublished); U.S. Court of Appeals for the Fourth Circuit affirmed published federal district court decision from Virginia.

2 ISO CG 21 06 05 14, BP 15 04 05 14 and CU 21 86 05 14.

3 *Zurich American Ins. v. Sony*, 2014 N.Y. Misc. LEXIS 5141.

4 See The Meaning of "Publication" in the Electronic World—From Data Collection to Data Breaches, by Josh Mooney, White and Williams, in Gen Re *Policy Wording Matters* (December 2015).

5 *State Bank v. BancInsure*, 2016 U.S. App. LEXIS 9235.

6 *Retail Ventures v. National Union Fire*, 2012 U.S. App. LEXIS 17850 (6th Circuit applied Ohio law to find coverage under "blanket crime policy" when hacker stole credit cards data).

7 *Medidata Solutions v. Federal Ins.*, No. 15-cv-907 (S.D.N.Y. filed Feb. 6, 2015).

8 Fitch Ratings, *Global Cyber Insurance Update: Expanding Threats Amplify Underwriting Opportunity, Loss Potential* (2016).

Do you know where your Cyber exposure is?

Gen Re devotes a lot of time and resources to answering these questions, and can help you get a better picture of your Cyber exposures. If you need help evaluating your products for Cyber coverage, let us know.

Gen Re

genre.com