CLM 2018 Cyber Summit
October 10-11, 2018
New York City

Silent and Endorsed Cyber Coverage

While a robust cyber insurance market has developed over the past decade, issues have periodically arisen concerning whether non-cyber insurance policies respond to cyber events and any resulting damages. This issue has largely been resolved in the context of commercial general liability policies, but policyholders have continued to push for cyber event coverage under non-cyber insurance policies. For example, management liability, professional liability, property, and crime policies are a few of the policies under which policyholders have sought coverage for cyber events. This narrative discusses the background concerning silent cyber coverage, recent case law, and the future of cyber coverage under policies that are not currently intended to cover those risks.

I. Silent Cyber Coverage Past and Present

With emerging risks come questions regarding the availability of coverage under various policies. This was certainly the case with early cyber events, which saw policyholders seeking coverage under non-cyber policies for damages arising from a cyber event.

Initially, coverage for cyber losses under commercial general liability policies was frequently disputed, but has since been largely resolved by case law and the addition of endorsements precluding coverage for a cyber event. (*See Zurich American Insurance Company v. Sony Corporation of America, et al.*, Index Number: 651982/2011 (N.Y. Sup. Ct. Feb. 21, 2014)(finding that a third party criminal cyber attack does not trigger Coverage B); *see also* ISO Endorsements CG 21 06 05 14 and CG 21 07 05 14). However, initial coverage disputes did not always end in uniform decisions.

Compare the result in *Sony* (*i.e.*, no coverage) to the decision in *Tamm v. Hartford Fire Ins. Co.*, 16 Mass.L.Rptr. (Mass. Super. Ct. 2003), wherein the Massachusetts court found that a duty to defend was triggered based on allegations that an ex-employee threatened to distribute private information by email.

While *Sony* and *Tamm* addressed coverage under Coverage B, the Minnesota Court of Appeals' decision in *Retail Systems, Inc. v. CNA Insurance Co.,* 469 N.W. 2d 735 (Minn. Ct. App. 1991) dealt with Coverage A. In *Retail Systems*, coverage was found under a CGL policy for information contained on a data tape that was lost. The court held that the data on the lost data tape had value and was integrated with the tangible properties of the tape. (*See also Eyeblaster, Inc. v. Fed. Ins. Co.*, 613 F .3D 797 (8th Cir. 2010)(finding coverage because loss of use of tangible property occurred when the underlying claimant visited the insured's website resulting in the loss of use of claimant's computer even though it was not physically damaged.)

While some courts have found in favor of coverage under CGL policies for electronic data, there are many decisions finding that there is no coverage. (S*ee America Online, Inc. v. St. Paul Mercury Ins. Co.*, 347 F .3s 89 (4th Cir. 2003)(finding that there was no coverage for software that corrupted a customer's software because software does not qualify as tangible property.)) However, the appearance of a lack of consistency among courts may be part of what is driving policyholders to attempt to find coverage under insurance policies that were never intended to cover cyber risks. This is especially true of policyholders that have failed to secure separate cyber coverage.

One line of insurance that has seen an uptick recently in the number of coverage disputes for cyber events are crime policies. The Second Circuit's decision in *Medidata Sols. Inc. v. Fed. Ins. Co.*, 2018 U.S. App. LEXIS 18376 (2d Cir 2018), highlights the potential for silent cyber coverage under non-cyber policies. The court noted that an executive's spoofed emails directed Medidata employees to transfer funds, which was completed the same day. The court found that the spoofing attack was the proximate cause of Medidata's losses, and that while Medidata employees had to take action to effectuate the transfer, it was not enough to sever the cause (the spoofed email) from the loss (the transferred funds). (*See also Am. Tooling Ctr., Inc. v. Travelers Cas. & Sur. Co. of Am.*, 2018 U.S. App. LEXIS 19208 (6th Cir 2018)(finding in favor of coverage because the computer fraud directly caused the insured's direct loss.))

Contrast the *Medidata* decision with the decision in *Pestmaster Services, Inc. v. Travelers Casualty & Surety Co. of America*, 656 F. App'x 332, 333 (9th Cir. 2016), which found no coverage under a crime policy. Pestmaster had hired Priority 1 Resource Group to handle its payroll tax services and granted Priority 1 electronic access to its bank account. Priority 1 was then authorized to transfer funds out of Pestmaster's bank account into its own account, and

from there it was to pay Pestmaster's payroll taxes. The fraud occurred when Priority 1 failed to pay the taxes and kept the money instead. The difference in *Pestmaster* was that Priority 1's use of a computer was legitimate, and the fraudulent act did not involve a computer.

The industry will also see third party claims arise from increased spoofing that professionals fail to detect. There is the potential for these types of matters not being the result of a security failure or data breach, meaning claims may not fall within the insuring agreement of a cyber policy and could possibly trigger coverage under errors and omissions policies.

Property insurance is yet another area that may provide silent cyber coverage in the event a cyber attack results in property damage or business interruption. Recognizing the scope of the liability presented by cyber events, many insurers are limiting coverage to decrease their exposures. For example, one carrier has sought to eliminate bodily injury coverage for property claims arising out of a cyber event.

When it comes to property policies, policyholders should have their broker perform a gap analysis to determine whether there are damages that will not be covered by a cyber policy, but may be covered by a property policy. Some items that may factor into the analysis are equipment replacement (hardware), electronic data reconstruction and replacement (software), and business interruption. Hardware replacement and property damage require direct physical loss or damage which a property policy should typically cover. However, property policies can now provide non-physical coverage for data recovery and business interruption, which may have some overlap with a policyholder's cyber policy. Because of the potential for overlap, claims adjusters should be asking about property coverage when processing cyber claims that have property damage or business interruption components.

II. Cyber Coverage By Endorsement and Its Limitations

Given the unique risks presented by cyber events, underwriters, policyholders and brokers frequently work together to ensure that the cyber risks faced by a particular insured are managed as best as possible. Manuscripted policies and endorsements are employed to cater to the particular risks faced by an insured, but they are also utilized to provide coverage that falls within an insurer's underwriting limitations.

Manuscripted policies and endorsements enable insurers and policyholders to customize coverage for a particular insured, but the importance of the wording utilized cannot be understated. While many lines of insurance employ language that has been addressed by the courts, manuscripted policies and endorsement can deviate from tried and tested wording. In

those instances, it is important for all of the parties involved that clear and well-defined language be employed so that disputes can be minimized.

If the intent is for a policy not to cover cyber risks, but the policy's insuring agreement raises questions as to whether there may be silent cyber coverage, one method of limiting cyber related risks is to either exclude coverage altogether or offer a sublimit for cyber risks. By offering a sublimit, losses arising from cyber risks are covered but capped at a nominal amount, thus eliminating the need to dispute whether or not a policy provides silent cyber coverage.

Insurers are now increasingly offering bodily injury and property damage coverage by endorsement. On the other hand, some insurers are limiting their exposure by subliming phishing, telephone and spoofing exposures to $100,000, while others still make full limits available. Utilizing a broker to compare the coverage offered by insurers and the resulting premium is highly advisable in a market that is continually changing.

III. Identifying Policies That May Respond to a Cyber Event

Following a cyber event, members of a policyholder's organization are understandably preoccupied with dealing with the fallout and may not be focused on potential coverage. The importance of a risk manager and/or broker at this time cannot be understated. Not only will they compare the facts underlying the cyber event to policies that are intended to respond, but they will also be able to evaluate whether any other policy could potentially provide silent cyber coverage.

A thorough analysis of each policy's terms, conditions and exclusions is required before any notification is provided to the insurance carrier. This is especially important when policyholders seek coverage under policies that are not underwritten with the intent of covering cyber risks. Blindly noticing carriers following cyber events can lead to a waste of both the policyholder's and insurers resources. It can also unnecessarily result in a hardening of positions that can affect relationships and increase costs.

IV. Managing the Cost of a Cyber Event

As mentioned above, in the aftermath of a cyber event, policyholders are more focused on responding to the event than notifying their carrier. While cyber policies may permit a policyholder to incur costs without first obtaining consent, many other policies do not permit the insured to incur any costs without the prior written consent of the insurer. In addition, the issue of pre-notice costs may be a more significant issue when it comes to cyber events because

of the high expense of vendors and legal counsel that are retained in the days following a cyber event.

In the event a non-cyber policy responds to a cyber event, some costs incurred in responding to the cyber event may fall within the policy's definition of damages, while other costs will not be eligible for reimbursement. A threshold issue when it comes to costs is the level of detail provided concerning the services provided. A frequent source of friction between policyholders and insurers are invoices from vendors and legal counsel that lacks specificity as to the nature and purpose of the services provided.

Another issue that may arise as a result of silent cyber coverage is language that requires expenses be reasonable and necessary. While some costs incurred as a result of a cyber event are commonly covered under cyber policies that may not be the case under policies that have silent cyber coverage. Extra expenses, reputation protection, upfront credit monitoring, and notification costs are examples of costs that are likely not covered under non-cyber policies.

Similarly, if defense costs for third party claims are covered under a policy that has silent cyber coverage, it could potentially create an allocation issue between a cyber policy and a duty to defend non-cyber policy. Many cyber policies provide for the reimbursement of legal fees for counsel selected and retained by the policyholder. In some cases, the rates that a cyber carrier will reimburse are higher than those that are acceptable under a non-cyber policy, which frequently have panel counsel assigned to represent the policyholder's interests. Resolving the issue of the disparity between amounts covered between cyber and non-cyber policies can lead to disputes and underwriters should consider addressing this issue in their policies.

V. Conclusion

While every industry faces the risks presented by cyber events, some policyholders are either underinsured or lack a cyber policy altogether. In those situations, policyholders may be inclined to seek coverage for the significant costs associated with cyber events under whatever policies they have in place. In some instances they are able to secure coverage for some or all of the resulting damages, but when policies that were not intended to cover cyber risks are found to provide silent cyber coverage, the industry is quick to respond and either preclude coverage for future cyber events or adjust the coverage provided with a corresponding increase in premium.