2015 CLM Annual Conference
Palm Desert

"Holistic View of Cyber and Data Privacy"

Presenters: Sarah Abrams, *Markel Service, Incorporated*
Brian Bassett, *Traub Lieberman Straus & Shrewsberry LLP*
Joe DePaul, *Willis*
Cathleen Kelly Rebar, *Stewart Bernstiel Rebar & Smith*
Brian Robb, *CNA Insurance*

I. Cyber/Data Privacy – *What Coverage do you Need?*

Most companies do not realize that traditional insurance coverage does not cover most data privacy related events.

Understanding what your business is, who your customers are and where you operate are fundamental questions that need answering before you begin exploring the coverage elements of cyber insurance.

Am I a hospital system or managed care provider operating in 5, 45 states? Do I process student applications from individuals in 10 states and internationally? Am I accepting payments at my sporting goods locations off and online? Do I allow my residents to pay for their motor vehicle violations online, how about taxes? Am I a small financial institution with personal and business accounts? Am I a provider of technology services? Am I a multi-billion dollar public company with customers in the US, Europe, dealing with multiple vendors, with seasonal exposures?

Wow, that is a lot to think about. But, these are the things a company and the management team/board of directors must understand as they move forward into this brave new world of cyber risk, where anything can happen, and where the best laid incident response plans can be wiped out in a second.

The data is at the heart of the problem. Ensuring that you have identified your data, you have categorized and organized your data, and you have put an information governance program in place are critical. Where is the data? Questions you should be thinking about constantly, and which you will need to answer when your world implodes. The answer to this question will either save you millions of dollars or will cost you millions of dollars.

Why do I need cyber insurance anyway? As an organization, you have the responsibility to peel away the onion and understand what your risks and exposures are. In addition, if there is a way to mitigate the financial loss that will overtake your company, and there was a solution that could have eliminated or prevented this loss, did you explore it? Did you ask the right

questions about coverage, do you understand who your peers are and what they may be buying? Looking into the trends, determining what the best mitigating program that may be available to you is important. Otherwise, the question will be, have we budgeted for such a loss? And, why didn't we hedge our bet? Cyber insurance is not 100% of the answer, but I would argue that it is pretty darn close.

II. Breach: *One size does not fit all? Or does it?*

A certain standard of care has evolved with respect to the primary steps taken in response to a data privacy event. However, those steps are not necessarily the right steps, in the right order for every data privacy event. There are many critical considerations to review before deciding what exactly needs to be done in any given circumstance.

Traditionally, the prototypical response to a data privacy event includes the immediate appointment of experienced counsel to begin the attorney/client relationship. From there the selection of a third-party vendor in forensic investigation is made. Data is reviewed and distilled to establish a list of potentially affected or affected individuals and a breach notification correspondence is drafted. Vendors are often retained in order to manage and distribute the mail notification correspondence to the affected list. If necessary a public relations company is engaged in order to assist in managing the negative public response to the very public news that a company suffered a data privacy event. In many jurisdictions, it is necessary to engage the attorney general's office and respond to inquiries regarding the steps undertaken by the company before the breach and the remediation efforts are put in place following.

However, experienced breach response counsel knows that all breaches are not created equal. For instance, Target is different than JP Morgan which is different than Sony. A small business would not be set up for, nor require the same response as a publically traded company. Professional firms would have different requirements in response to a data privacy event from a health care provider.

Also, there are laws particular to each area of business. It is important to understand how a particular breach victim is affected by the varying laws and also among the different jurisdictions. Fortunately, or unfortunately, there is no single Federal Data Breach Law. Most unfortunately, for compliance, there are 47 different state laws which depending upon where your affected individuals reside, may subject the company suffering the breach to many of those state laws. Further, health care companies/providers and business associates are subject to HIPPA and HITECH. As mentioned above, various states require a company facing a breach to involve and notify the state Attorney General's office or OCR, etc.

The issue of whether a company should conduct a pre-breach risk assessment has been the subject of debate. There are often insurance carrier incentives provided to insureds to undergo such a risk assessment. However, if a company undergoes a risk assessment and fails to follow the recommendation, the same could subject them to additional liabilities from individuals affected by a company breach.

III. Coverage: *What is covered?*

When a data privacy event happens, the first call often made is to the insurance broker, the second to the insurance carrier. These events require immediate response. But, before an adjuster can appoint breach response counsel, a decision needs to be made as to whether the insured has the appropriate coverage and whether the data privacy event is, in fact, covered.

Often we will see attempts to tender the data breach to both a professional liability policy *and* a data breach policy. Depending on the language of the policy (i.e. broad worded D&O) and the nature of the loss coverage may be triggered under both.

An adjuster needs to consider several critical questions before determining whether the insured has coverage for the reported event. Specifically, the adjuster should determine whether the policy is a standalone data breach policy with various coverage parts. Other considerations include whether this is a first party or third party claim, or possibly both. The policy needs to be reviewed to determine whether there is breach mitigation coverage. The specific event needs to be considered in light of the available coverage. For instance, with crypto-defense, the insured's data becomes encrypted and ransom is demanded for the release, or encryption key. The response to the data privacy event may be covered, but the ransom may not. It is important to consider this before advising the insured that it has data privacy event response coverage. Of significance, is whether the insured has a self-insured retention or deductible. In addition, if there is breach mitigation coverage, the insured may have significant leeway in choosing counsel to respond as well as credit monitoring services. If so, the insured should be reminded of this from the outset.

In some situations, regulatory agencies may impose civil penalties and/or fines. The policy at issue may or may not cover these fines. Also, there are certain nuances with respect to a data privacy event that may afford coverage under other policies which the insured has with the company. All aspects of the event need to be considered in order to determine all available resources for the insured to respond to the breach.

IV. Role of the Attorney

The role of the attorney depends upon the capacity in which it is retained – coverage counsel, monitoring counsel or defense counsel.

Coverage counsel should generally follow in the footsteps of the claims professional in determining the scope of coverage available for the loss. Consideration should be given to the nature of the loss, and whether it implicates third party liability coverage, first party coverage, or both. Importantly, first party coverage should be utilized to respond to a loss, not to allow the insured to upgrade its system at the insurer's expense. In a third party claim, counsel should closely scrutinize policy exclusions that may apply, including the dishonest act exclusion, prior knowledge exclusion, risk management control exclusion, and contractual liability exclusion. Counsel should also evaluate whether the policy's notice condition was complied with, and whether delayed notice prejudiced the carrier. Some policies permit the use of an examination under oath to further assess the nature of the loss and whether coverage defenses are available. Counsel and the insurer should be cautious in using that tool to evaluate coverage

As there are no reported coverage cases on standalone cyber policies, the attorney and the insurer need to be mindful that position they take could create precedent for its future handling of claims. It is important to be consistent. Counsel should obtain the insured's E&O, D&O, CGL, property, crime and K&R policies to determine whether other coverage may be available for the loss. Additionally, case law addressing similar provisions under traditional insurance products should be consulted in making a coverage determination.

Defense counsel is retained to represent the insured in responding to a breach. Counsel must be fully apprised of and ensure compliance with breach notification laws (e.g. New York, New Jersey, Texas, Florida, Georgia, California, Massachusetts, Illinois). Liability needs to be

evaluated by counsel in the context of state data security laws and federal statutes (HIPPA, HI-TECH, GLBA). Cooperation with state and federal agencies in the investigation of and response to the loss may also be required. Defense counsel should also examine whether the insured's conduct complies with the NIST framework as that may form a theory of liability asserted by counsel for claimants. Defense counsel should also work closely with the vendors retained to respond to the breach, including the breach coach, the forensic investigator, and the public relations consultant.

If claims are filed in connection with the breach, counsel's role evolves. There are certain successful legal defenses that have been raised in connection with such claims. For instance, many insureds challenge whether the claimants have standing to pursue the claim and whether the claimants suffered actual injury as a result of the breach. There are also avenues to defeat an attempt at class certification depending on the nature of the loss. Research should be conducted to determine if courts from jurisdictions nationwide have addressed liability in the context of the specific breach.

Monitoring counsel is often a hybrid of the defense and coverage counsel. These attorneys are generally retained to represent the interest of an excess carrier in large exposure cases and they do not directly represent the interests of the insured in responding to the breach. They will assess coverage for the benefit of their client, and then keep apprised of the status of any claims or breach response in an effort to insulate the excess carrier from exposure. Given the tripartite relationship, these attorneys are usually afforded the right to be informed of the status of the insured's efforts to mitigate losses and can obtain attorney-client privileged materials.

V. Segway to Litigation

How an insured responds to a breach may influence whether litigation follows. In high exposure breaches, it is a virtual certainty that litigation will ensue. However, in breaches affecting smaller organizations, a well-tailored response including mitigation, credit monitoring and remediation can assist an insured in avoiding litigation in the future.

When or if litigation follows a breach event, it is important to have a basic understanding of the legal landscape so you can counsel and guide the insured, who will undoubtedly ask questions about what will likely happen if they are sued. Certain aspects of the breach response, like offering free credit monitoring have a direct relationship to a decrease in the likelihood of subsequent litigation. Also, the type of data involved increases the probability that your insured will be sued. Mishandling of personal information as opposed to a criminal act involving hacking will increase an insureds risk of suit.

It is important to know that for suit to survive in Federal Court, a Plaintiff must show an actual injury. A series of events that will probably lead to injury will not suffice. However, Plaintiffs' counsels are pursuing other avenues to bring litigation, such as Consumer Protection Statutes, Privacy laws, misrepresentations about the strength of a privacy policy and other causes of action where proof of actual loss is required.