CLM Claims & Litigation Management Alliance™

ADVANCING ETHICS, COOPERATION AND EDUCATION

CLM 2015 Cyber Liability Summit
October 21, 2015 in New York City

The Interface of Underwriting, Claims and Counsel to Create Sustainable Insurance Products for Cyber Risk

I. The Approach to Underwriting Cyber

Difficult to Underwrite to Pick Winners vs. Losers

Underwriting cyber is relatively "new" in terms of lines of business in the insurance business. There is not a ton of historical data to rely on, and underwriting companies have a lot of work to do to enter the cyber space while building a profitable portfolio.

Determine underwriting guidelines

Underwriting teams need to thoroughly analyze the cyber landscape to determine what their strategy will be in terms of industry focus, industries they will not write, and how they will approach different segments of the business from a size perspective: Large corporate risks, middle market, small commercial, etc.

Determine decision making variables

Underwriting cyber can focus on a number of key variables where underwriters base their decision making. A combined actuarial and underwriting analysis needs to be completed to determine the right approach to this depending on the portfolio the insurance company is looking to build and based upon the opportunity the company has in the marketplace. As the landscape for cyber attacks continues to evolve, underwriters need to update their underwriting approach so they are not adversely selected against based on dated information.

Determine target segments/industries

Getting into the cyber insurance market without a clearly defined appetite and target market would not be very prudent. Different industries and segments require different approaches to underwriting and different pricing methodologies. Also, without a clearly defined strategy and appetite, brokers and insureds will likely not take you seriously as a competing market, opening the door to adverse selection.

Use Parameters to Build the Portfolio you Want

Portfolio management and steering is quite important when building a portfolio of cyber risks. As indicated in the above discussion, doing the analysis to determine the underwriting appetite and target segments is very important. Monitoring this portfolio will be valuable to ensure profitability, and will likely require deeper analysis of underlying data – "peeling back the onion."

Use data to build portfolio analytics

Actuarial analysis of the underwriting obtained in applications and through the underwriting and research process combined with claims data will be very valuable for the buildout of management information reports used to monitor and steer where the portfolio is going.

Set parameters of target portfolio

A collaboration between underwriting and actuarial teams can determine what key metrics will be used to monitor and steer the portfolio of cyber risks. The parameters can range significantly, but would likely include some of the following: industry, revenue size, number of records, historic loss ratio, limits purchased, retentions, rate on line, rate change, etc.

Monitor data and steer portfolio

The important next step is once parameters and metrics have been set, the team needs to set the process on how this information will be used and how decisions will be made using the information. Underwriting teams can think about having quarterly portfolio reviews (the frequency can be different, this is just an example), where performance versus the metrics are monitored and decisions on how to "correct" or "adjust" underwriting going forward can be taken.

Monitoring the benefits derived from the value added services to the policy

Claims services are valuable to insureds

Unlike other lines of insurance, cyber insurance offers many proactive claim services once a claim is made. The insurance carriers often have strong vendor relationships with forensic analysts, mail centers, public relations experts and other critically important service providers which provide a much added benefit to insureds who face a cyber event. Claims handlers are extremely knowledgeable in the variety of cyber events that arise and collaboration on the front end with data breach counsel can be extremely valuable with mitigating the loss to the insured whether economic or reputational.

Risk Management offerings

Risk management offerings have a unique dilemma as the benefits of such services are delayed. The companies that need the value added services only get access to them through the policy.

II. The Value of Regular Feedback Loops Between Claims And Underwriters

Perhaps even more so than other product lines, regular and meaningful communication between claims adjusters handling cyber exposures and the underwriters (and even actuaries) is critical to building a sustaining a growing cyber liability book of business. As exposures continue to change and evolve-- whether the risk classes targeted shifts or grows, or the manner in which breaches occur become more complex—such information needs to be shared to properly ensure that policies are adequately addressing the exposures for policyholders on the front lines.

Help Underwriters Ensure they are asking the right questions

As underwriters examine a risk—whether it be new business or a renewal-- having a proper understanding of the policyholder's business, how it operates, the policyholder's client base, as well as the general industry in which the policyholder does business, is imperative to providing proper coverage at an appropriate price. An internal claims department specializing in these exposures can have a very positive impact in assisting the underwriters during policy procurement.

During this process, many a times an underwriter and claims department will discuss a particular prospective risk, and formulate appropriate questions to address the business and exposures at hand. This is particularly helpful if claims is already handling a breach event or other claim for a similar sized insured in the same risk class. Further, if a claim has already presented itself for an existing policyholder, and a renewal is underway, the underwriter can gain a better understanding from claims if the policyholder has taken all appropriate and reasonable measures to mitigate against future cyber exposures.

Tailor or amend application questions

From time to time, a claims department may see a pattern or trend emerge or develop amongst its claims population which would warrant a closer examination of the policy application and the questions posed therein. This is particularly true if the answers to the questions, while responsive, may not necessarily capture the intent of the question posed-- and thus, leave the underwriter with an incomplete understanding of the true exposures facing the policyholder. Clear, focused and direct questions on the application will allow an underwriter to properly tailor the policy to address the risks at hand, and allow for everyone's expectations—the underwriter, claims, and the policyholder-- to be met when a claim is tendered to the carrier.

Provide Underwriting insight on claims scenarios

Apart from regular and meaningful communication between claims and underwriting during the policy procurement process for a particular account, regular claims roundtables with underwriting—whether on weekly, monthly or quarterly basis, is an excellent vehicle to share emerging trends and evolving law on the cyber insurance product line. Given the speed and frequency with which breach events occur in the headlines, and the ever changing decisional authority affecting claim disposition in litigation, an internal claims department in particular is best suited to relay such information with the underwriters so that they may properly adjust the broader book accordingly.

Policy Changes Can Be Made After "Unexpected Claims"

Depending on the particular policy issued to an Insured, a specialized claims team can be of great benefit to the underwriters in offering policy changes and amendments to better position the broader book while fulfilling the expectations of all involved. For example, apart from a stand-alone cyber policy, or even an endorsement of sub-limited coverage to address cyber exposures, some policies may not have been designed to cover a breach event, but in the end, may have done just that. General liability policies, director and officer policies, and even professional liability policies in recent years have been focused upon as potentially responsive to cyber exposure risks facing policyholders. On the flip side, policy changes are needed with input from a claims department when a cyber policy was intended by the underwriter to cover a particular claim as presented, but perhaps the language in the policy form arguably precluded coverage. Lastly, proposed policy changes are also warranted with input from internal claims departments as the exposures change, or the broader insurance industry broadens or narrows coverages available under the myriad of cyber policy forms available.

III. The Current State of Cyber Policies in the Market

A variety of cyber insurance policies and solutions exist in the market today. There are cutting edge forms from leading and specialty insurers, all the way to general cyber extension endorsements that may be added to a BOP policy for a main street America type of risk.

Stand-alone policies are not standardized, but insured and broker demands are starting to move the market in the same direction, making policies look more and more similar as updates and revisions occur. This trend will continue and although there will never be a standard cyber form, forms will start to look more and more alike as time passes and experience is gained.

Is the Cyber Policy Past Covering the Expected Causes of Loss?

Cyber policies continue to evolve just as the nature of cyber breaches and cyber exposures evolve. During the normal evolution of any policy, monitoring and reassessment need to take place to ensure the policy's coverages are sustainable. The forces of supply and demand in the market are helping to shape the future of cyber policies, likely in the direction of expected causes of loss, which can be sustainably priced using data and historical experience.

Catastrophic, unexpected, loss exposures will be subject to the build out of holistic multi-line aggregate covers.

Market and Insured demands are changing

The demands of insureds and the supply of the insurance market are the driving forces behind the evolution of cyber policies. There are new developments in the cyber market being announced regularly. Insurance companies partnering with technology companies to provide threat assessments as part of insurance policy services. These are great advances, but is it enough? The penetration of cyber insurance in the mid-market and small commercial space is still low, suggesting that the supply and demand in the market have not found a sweet spot per se.

Insurers are focusing on predictability and profitability

Insurers want to build a product that offers coverage for losses that can somewhat predictable with data. The experience data gives actuaries what they need to price the product with relative confidence. This would lead to a solid risk transfer insurance product, likely highly commoditized with a low level of variability in pricing around key underwriting metrics.

The predictability would keep insurance companies focused on building a portfolio that produces an underwriting profit and underwriting managements would be extremely happy. However, would this meet or solve the needs of the buyers of cyber insurance? Per the comment above, it may not. There are still companies who do not buy cyber insurance. These companies have likely evaluated the cover and felt that the value and protection provided is not worth the cost. How will the industry close the gap?

Outlook on ways the cyber policy may potentially evolve

No one has the crystal ball around how cyber policies will evolve and what they will look like in the future. Cyber policies have already been quite innovative in insurance terms, as they provide both first and third party coverages. This pushes the boundaries of historical insurance lines of businesses. The insurance market's understanding and comfort with cyber exposure will continue to evolve, likely providing broader coverage over time (perhaps fewer sublimits) but in a targeted approach that allows for predictability of expected loss.

As mentioned earlier, there is a push towards insurers partnering with technology companies and service providers to provide risk assessments for their insureds. This is a great advancement, but raises the issue about timing. In order for insurers to get a good underwriting view of an insured, it should use the assessment services as part of the underwriting process. However, the cost of this is likely to be very high. The companies that likely have a need for these services may be too small (or generate too little premium) to justify the cost. Therefore, are the services targeting the right insured segment?

One view of where cyber is going is to look at Boiler and Machinery products today. The history of boiler and machinery products was somewhat similar to cyber. Boilers were / are extremely dangerous, and the only way to be comfortable insuring them is to perform detailed

inspections and servicing of the systems. Therefore the product evolved by the likes of Hartford Steam Boiler to be a combined service and insurance product. This is one view of where cyber will end up. There is movement in this direction already with the partnerships being formed, and it is foreseeable that the service and insurance products will continue to meld into one offering, similar to boiler and machinery.

Will cyber have a similar natural evolution that EPLI experienced?

The evolution of cyber as an insurance line of business is frequently compared to the evolution of Employment Practices Liability Insurance (EPLI). When EPLI coverage came out, some insureds and industry players felt it was covered in the GL policy (this feeling exists with cyber), and that there was no need to buy an additional policy (again, similar to cyber). Insurance companies began offering EPLI extensions and endorsements with low sublimits to provide some coverage and meet insured demands while still limiting downside potential due to the new and uncertain nature of the line. This is still sounding similar to cyber today, correct? Insurers began to realize the value in the service component of the EPLI coverage form, such as HR contact numbers, access to web portals providing examples of employee handbooks, etc. Eventually, claims activity picked up in EPLI and insurers pushed insureds to buy stand-alone policies addressing solely the exposures of EPLI, and insureds wanted dedicated limits.

Many believe we are in the middle of this evolution with cyber, as parts of the EPLI story sound quite similar to where the market is with cyber today.

IV. View from Our Expert Panel: Is Cyber Insurance here to stay?

Lawyer View

Cyber insurance is here to stay, in what form remains to be seen. Currently, cyber policies provide lower limits of coverage than other types of insurance. For average businesses this will never be an issue. However, larger businesses are not capable of purchasing limits that would/could wholly protect them in the event of a cyber event. For instance, the Target breach will provide approximately 90 million dollars in insurance coverage, but the total loss to Target exceeded 252 million dollars in coverage.

The evolution of regulations for minimum standards, risk mitigation, quantifiable cost data and data collection on paid claims will dictate cyber insurance products of the future. Whether the coverage will provide wide sweeping exclusions, lower limits, or high premiums is the question mark.

Claims View

Cyber insurance is certainly here to stay. Unlike some who have pondered whether cyber insurance is 'the next Y2K'— judging by the repeated data breaches taking place and our societies' ever increasing reliance upon technology, data collection, and seamless sharing of information through the cloud and otherwise, the claims will continue to grow and evolve and

require those carriers with internal claims departments with the necessary technical, legal and coverage expertise to adjust and grow accordingly. Further, the continued globalization of business and policyholders will further create complexities for the insurance market and legal environment within which these exposures are addressed by claims departments.

Underwriting View

Cyber is here to stay for sure. It is in the interest of the insurance industry, and buyers, to have a specialized product dedicated to covering losses stemming from cyber attacks. The shape and form of cyber insurance may change, and no one has the crystal ball to determine how the product will evolve. Insureds are likely to continue to become smarter buyers with better data and better underwriting information available for a solid assessment to be made. Underwriters will develop better models, and use big data to more accurately assess cyber exposure and more accurately price coverage for such exposure. It is an exciting time for the insurance industry from this perspective.

Reinsurance View

Cyber insurance is here to stay, but what the policy looks like in the future, and what coverages are provided, are not clear at this point. Insurance companies are pleased that the cyber line of business is a way to generate growth in insurance spend in a time where prices are soft in other lines of business. For this reason, it is likely that cyber will continue as a stand-along line of business. What the policy ultimately looks like and how it is priced are still to be refined. Earlier in our discussion we compared cyber to boiler and machinery products, and there is a strong view that in the future, the service component of cyber policies will be as important and a key piece of the final product sold in the market.

Insurers will also improve metrics used to monitor and steer their portfolios and feel comfortable with expected losses the policies have been priced for. The unexpected, however, will be a challenge, specifically the aggregation and accumulation concerns around a major cyber event or an event that impacts multiple lines of business. This is an area the reinsurance industry will need to address so it can provide clients the reinsurance support that is most valuable going forward.

V. Supply and Demand Discussion: Are buyers satisfied with the insurance product?

Cyber-attacks affect or can affect any industry. As cybercriminal tactics become more advanced the years to come will show an increase in data privacy events. As a result, cyber liability insurance is as important as property and liability insurance to a business' overall corporate insurance program. Despite this, many businesses still forego cyber coverage. As far as insurance goes, the cyber insurance market is still under-sold in comparison to other markets, especially among smaller businesses. Statistics reveal that cyber insurance has barely cracked the surface for smaller businesses. While debatable, the lower rate of cyber policies for small to mid-sized businesses is thought related to the lack of federal and state regulations, a general

lack of understanding of cyber-related business continuity risks, and false sense of security in existing cyber security.

Do Insureds feel there is Value in the Cyber Policy Purchased?

With the above backdrop, the answer is simple. If a business has a need to invoke its policy, the overwhelming response of the insured is that the policy was of great value. Most businesses have under estimated the expense of the response to a data privacy event and have a false impression of what constitutes a breach and of their requirement to investigate and effectively rule out those events which may constitute a breach.

The very first phone call with an insured after they experience a possible data privacy event reveals the insured's lack of appreciation of their responsibilities in responding to the even the possibility of a breach. Once they gain an understanding of the expense and expertise required for an appropriate response, insureds with a cyber policy are among the most appreciative of policy holders.

Insurers have been innovative in developing Cyber Products

More so than other insurance sectors, carriers offering cyber policies have been offering more for less. When a cyber specific policy is at issue, coverage determinations have been more favorable to the insureds than in other sectors. In large part this is because insurers realize the huge upside potential for growth and a growing demand. More carriers are entering the market, with more cover to provide, which is increasing capacity. Statistics showed steady increases in renewal premiums for cyber policies in 2013 and 2014, but lower premiums beginning in late 2014 and into 2015. Likely because the market is saturated with product and the demand is not keeping up.

For instance, in this sector you are seeing risk mitigation as part of the insurance offering. Some carriers, are offering partnerships with technology based companies to provide monitoring services and rapid response when a cyber-attack or threat is detected. Additional innovations is policy premium rebating when an insured undertakes a risk assessment of their network or training and education with approved vendors about ways to protect PII within the insured's business. Carbon Black has a product on the market for some time that tracks similar to a black box, the system events so that if a possible data privacy event occurs, the carbon black software can definitely show what, where, when and how to provide a more isolated and focused response.

What new Innovations are needed in the Cyber Insurance business?

There are two types of potential insureds: those who have been hacked and those who do not know they have been hacked. Like an act of god, there is no way to completely avoid a cyber attack. The best and only option is to mitigate its impact. Acquiring insurance for this imminent future event is marketed by the insurance industry as necessary.

Traditional insurance is based on calculated risk. For instance, costs of a breach will be less than the collected premiums in a given year. In the cyber arena, there is a lack of

calculations and the foreseeable costs are still somewhat unknown. Over time the data will evolve and shape the cost and the offerings to better align the insurance carrier to balance the risk.

At present, the sales approach to cyber insurance is selling product to offset a real and unavoidable event. Risk mitigation whether it be state of the art firewalls, malware detection, vulnerability assessments or threat detection software is part of the offering, but the real value of that mitigation on the cost side is unknown. The risk mitigation is being discussed for one reason: to demonstrate why the insurance is needed, but little quantifiable data has been collected to establish how the risk mitigation products or services actually reduce the financial impact of a breach.

New products are emerging like Risk Calibrator offered by CXOWARE a software company that helps to quantify the costs benefit of risk mitigation and resultant effects of a cyber event. Risk Calibrator offers a quantifiable risk assessment of a business using Factor Analysis of Information Risk (FAIR). It calculates the costs of the business effects of a breach. It is expected that the insurance industry will codify these risks (covered losses) into similar tools to calculate what type, and how much cyber investment is needed in a given area. The effect will be in the premium and coverage.

Also Universities like Carnegie Mellon are teaching an alternative approach to business management of cyber risk. In fact, they are teaching Chief Information Security Officers to approach cyber from a risk based approach versus the formal checklist driven compliance methodology. The net effect is predicted as a shift in pricing, delivery, coverage and benefits to mitigation.

Also, insurance company innovations will address the new and unforeseen vulnerabilities of The Internet of Things. The Internet of Things, is the name for technology that is not new but has now reached critical mass. It is the use of embedded sensors in daily objects, machines, and even our own bodies to transfer data to a network. For instance, heart monitors, home security devices, gps, traffic monitoring devices, etc. This connectivity, so to speak, provides new vulnerabilities that may not be contemplated under existing policies. For instance, possible hacking involving smart car technology that causes bodily injury or property damage. Underwriters will need to consider this when crafting policies to meet the risk.