IADC COMMITTEE NEWSLETTER

CORPORATE COUNSEL

January 2018

IN THIS ISSUE

Corporate Counsel face increasing work from their client. The most significant area of work has to do with cyberattack/events and the need to establish effective insurance to deal with those occurrences. IADC programs have highlighted the issue on different occasions throughout the last few years. Corporate Counsel are at the forefront of efforts to establish effective general insurance coverage regarding these events for all commercial activities. This article deals with the complex process of negotiating and acquiring cyberattack/event insurance coverage and the role of Corporate Counsel in that endeavor.

Corporate Counsel Perspectives on Cybersecurity Insurance Procurement

ABOUT THE AUTHOR

Joseph F. Speelman is currently serving as General Counsel for a private, Swiss based energy information group. He has directed successful defense efforts against Public Nuisance lead paint litigation in 15 states, gaining defense verdicts in those states including achieving a defense verdict before the state of Rhode Island Supreme Court that reversed a lower court trial verdict and rendered a defense verdict by the high court. He can be reached at jfspeelman49@gmail.com.

ABOUT THE COMMITTEE

The Corporate Counsel Committee is composed of in-house counsel and others who, although in private practice, serve as general counsel for corporate clients. The Committee provides its members with educational programs and networking opportunities to address common concerns of corporate counsel. It also works to ensure that the IADC and its committees, through their work and offerings, meet the needs of corporate counsel. Learn more about the Committee at www.iadclaw.org. To contribute a newsletter article contact:

Joseph F. Speelman
Vice Chair of Publications
Petro-Logistics S.A.
jfspeelman49@gmail.com

During the Annual Meeting of the IADC in Quebec City this year, an early morning insurance sponsored committee presentation on cyber security provided a very sobering view of the difficulties some companies were experiencing when seeking insurance coverage for cybersecurity or cyberattack situations associated with covering the companies' business related risks. The view of the panelists, which included coverage counsel and brokers, was to the effect that most policies being procured specifically for cyber risks, were virtually useless because of the manner in which such policies were written. Those present during the meeting almost uniformly commented on the usefulness of the presentation and the need to get such information to IADC members generally. (**The Cyber Insurance Broker Conundrum. 7:30 am, Tuesday, July 11, 2017)**

Cybersecurity is perhaps the most constant and pressing concern for Corporate Counsel and their clients in today's business environment. It will become an even greater risk issue for business counsel and leaders in the near future. Cyberattacks continue to increase in number, complexity, costs, and size throughout the international business community. The risks fall into a few, deceptively simple categories: denial of service, theft of confidential information, theft of confidential and sensitive business and financial information, and theft of accounts and money.

IADC Leads the Way on Cyber Risks

The IADC has played a significant and early role in highlighting the existence and growing concern of the risks of cyber events to companies and their counsel during the International Corporate Counsel College in Paris, France by sponsoring on November 14, 2013 a major program entitled **"Cyber Risks – E-Privacy"** dealing with Cyber security risks to Corporations. The program featured law enforcement officials, insurance counsel, and corporate counsel describing the developing issues and how governments and companies were beginning to respond to the problem. The idea for the program came from an analysis by IADC members of the Association of Corporate Counsel (ACC) daily legal report (ACC Newsstand) during the first half of 2012. That analysis, based upon article topics, demonstrated that corporate counsel were writing and expressing their concern about cyber security issues in an alarming and increasing level. Over a 200% increase in articles, items, and written material on the subject had occurred in only a six month period. No other topic even came close to such a significant number.

Since the above events, the issue, and the problems associated with it, have exploded across all international business; large, medium and even small entities. Corporate Counsel find themselves, as they should be, at the center of their client's reaction to and actions regarding these issues. The costs associated with cyber events are growing and governments and customers are insisting upon additional protection from the results of such events. Companies that deal with the handling, storage, or maintenance of customer financial information face significant and growing risks of liability

associated with cyber attack/event damages.

Insurance Issues Begin to Predominate

Corporate counsel and their clients are in the process of seeking insurance coverage for specific cyberattack associated risks. The reason for this is the emerging fact that most insurance companies who issue general liability insurance and business related insurance coverage policies to large companies have, effectively, limited their existing coverage responsibilities under general business liability insurance policies for cyber attack liability through policy limitations, modifications, interpretations or, in some instances through the cancellation of such existing policies.

The business of selling and buying business related insurance is an old and generally well understood process between insurers and their potential clients. It is a competitive business and those involved in the process are comfortable with the process and the results. What we are facing with cyberattack/event related insurance is a major paradigm shift in the insurance process. New insurance policies are being created by the insurers. As a result, a new type of insurance with a new and very dynamic risk factor has arisen and it has become a "tricky" process for both insured and insurers. The standard policies do not apply and the reliance of standard clauses, risk limiting factors and risk size no longer control the negotiation. Corporate counsel are at the forefront of this process. This is a new type of insurance. Labels, coverage, and the details of those policies vary dramatically from one insurer and insurance product to the next. This is a new area of insurance. "Standard" coverage simply does not exist. Wise corporate counsel should understand that what they are involved in is RISK assessment, evaluation, and ultimately mitigation of a new and not well understood risk.

Negotiations, discussions, and evaluations of insurance company offerings are becoming much more direct, formal, and potentially adversarial in nature. Corporate counsel must provide a direct leadership role for their client in this process. What may have in the past been a rather "chummy", friendly and low key discussion or negotiation with an existing insurance provider is now a much more formal, wide ranging, direct and "testy" negotiation with a number of insurance providers in which corporations seek the best and most effective policy at a reasonable price. The role of Corporate Counsel becomes central to these discussions. No agreed upon blocks of standard insurance language. Each paragraph will be reviewed, understood and a negotiated understanding of what the language means and the resulting coverage levels, range, and overall extent will be formally negotiated, understood and agreed to by both parties with written agreements between the parties to those effects. A classic corporate counsel role and environment. If done properly. **(Managing Cyber Risks: Tips for Purchasing Insurance that Works for your Business, Omid Safa, James S. Carter, and Jared Zola, Pratt's Privacy and Cyber Security Law Report, Vol 3, Number 4, May 2017.)**

What Corporate Counsel Must Accomplish

The Corporate Counsel must form a Risk Assessment Team for the specific purpose of evaluating the full extent and nature of cyberattacks/events and related occurrences and their impact on all aspects of the company. The team should include representatives from IT, Security, Insurance, operations, Accounting at a minimum. Corporate counsel must lead this effort because of the direct relationship to risks, contractual negotiations (insurance), and the need to ensure privilege will attach to communications internally and with brokers representing the company. Further, a formal and constant communication between the risk team and corporate leadership must be maintained and, of course, must be privileged.

The risks in Cyberattacks are generally in two categories: **1st party risks**, such as investigation costs, remediation costs, notification costs, financial and credit issues and always to be anticipated are public relations costs and the expenses related to internet defense of the company. **3rd party losses,** claims and litigation brought by third parties including customers, individuals, and generally parties alleging damage or harm through the company as a result of the cyber event. The 1st party risks generally occur immediately and, because of the insurance situation, will form the potential for the parties to establish how the claim process will proceed and, as to insurance carriers, might be their effort to limit the extent of coverage they have for the entire event. It will be important to realize that the third party claims, although not yet filed or generally understood, may well be the largest part of the overall incident costs, and therefore, the size of the potential claims against an existing insurance policy.

The initial insurance claim process can be a treacherous period as the existing insurance carriers may seek to cause an "under oath" claim evaluation with the company at an early stage. This can be a contentious situation requiring corporate counsel, company leadership, and coverage counsel to work closely to avoid reducing the coverage responsibility of the carrier as a result of actions, or inactions of the company, either real or perhaps "suggested" during the evaluation.

The insurance claims process is a very complex situation and becomes more so in the event of a large potential claim event. Communications between the insured (company) and the insurer (insurance company) must always be monitored or controlled directly by Corporate Counsel and, as appropriate, outside coverage counsel. Often, an "accommodation" offered by the insurer actually ends up reducing coverage levels or extent and caps the costs for the insurer. Corporate Counsel must ensure the company's communications to brokers and other contractors regarding policy negotiations be maintained as privileged. Some jurisdictions make this more difficult than others. The access of brokers and others to the privilege communications and attorney-client work product must be limited during the claim process.

Corporate Response Plan Coordination

Most companies have emergency Response Plans set up to provide process and guidance during a variety of emergencies from weather issues, national emergencies, force majeure events as well as including cyberattack/events. It is ABSOLUTELY ESSENTIAL that Corporate Counsel fully coordinate all aspects of a Cyberattack/event insurance policy with the company Emergency Response Plan so that the plan does not compel or provide for action by the company that might jeopardize in any fashion the coverage or applicability of the insurance policy to a cyber related event. This is a critical issue of internal coordination and communication that Corporate Counsel, as leaders in risk management, must ensure is dealt with properly. **(Supra, Safa etal, Cyber Security Law Report, Vol 3, Number 5, June 2017.)**

During the initial stages of dealing with a cyberattack/event, the company will invariably be faced with unanticipated costs or potential expenditures. These type of costs must be anticipated, if at all possible, and should be pre-negotiated as to rates and response efforts with not only the vendors but also with the insurance carriers so that such costs do not present an issue during the initiate claim evaluation stage of the coverage. As an aside, I am sure you will not be surprised to learn that pre-negotiated rates tend to be smaller that those a company is confronted with AFTER an event has occurred. As well, having those costs identified prior to agreement on the insurance coverage limits the ability of the carrier to use them as a challenge to coverage. The insurance policy should have sufficient language to allow truly unanticipated but essential costs if necessary.

Large Versus Small or Smaller Companies

Much of this article seems to presume a certain, rather large size to a company being faced with the risks discussed above. In reality, many companies are affected by Cyber events that are quite small. The level of attention and detail remain as set out above. Often the "team" size called for in risk assessment and related matters may be two or three people covering each and all of the areas of concern. Small companies have fewer employees and contractors but the functions; accounting, legal, security, IT etc, all still exist. They are generally covered by one or two senior individuals. Relax. That makes many things much easier and quicker. It is essential the process be adhered to but there is no required amount of time or energy to expend on these processes. Some companies have many attorneys that are corporate counsel, many companies have one or two such individuals. The thought process is the same but much quicker. Outside counsel can play a significant role for a small company but, caveat, they must be "in the shoes" of the corporate counsel in those situations.

We live and work in difficult times. So be it. The role of Corporate Counsel is growing in all types of companies. Rise to the tasks.

Be careful out there.

Past Committee Newsletters

Visit the Committee's newsletter archive online at www.iadclaw.org to read other articles published by the Committee. Prior articles include:

OCTOBER 2017
A Tidal Wave of Public Nuisance Law Suits across the US Involving Opioid Litigation
James K. Holder and Joseph F. Speelman

SEPTEMBER2017
What Next Rough Beast….The Second Coming of Nuisance Law Litigation
Joseph F. Speelman

DECEMBER 2016
Please Call Again: The Supreme Court Declines to Rein in TCPA Litigation
W. Jason Rankin and Charles N. Insler

NOVEMBER 2016
No Harm, but Still a Foul? Application of the Supreme Court's Punitive Damages Jurisprudence to Actions Seeking Statutory Damages
Jeffrey A. Holmstrand

OCTOBER 2016
Drone Law and Drone Regulation: A Primer
Lem Montgomery

APRIL 2016
Proportionality and Reasonableness: Using the 2015 FRCP Amendments to Rein in Discovery
Martin J. Healy and Joseph D. Fanning