CyberRiskPartners

415 Madison Avenue, 15th Fl.
New York, NY 10017
1.646.673.8511

CyberRiskPartners, LLC Responses to Dept. of Commerce Notice of Inquiry

Regarding CyberSecurity, Innovation and the Internet Economy
30 Sept 2010

CyberRiskPartners,LLC has determined, based upon our review of the Dept. of Commerce NOI, that our specialties are aligned to comment specifically on questions (P) – (U)

Our thoughts below are based on two allied assumptions

1. the optimal financial outcome of any entity is to completely avoid a cyber event
2. physical cyber resilience at any cost cannot protect with 100% certainty any entity from experiencing a cyber event

While there is growth in the adoption of cyber insurance, a compelling economic case for large scale Underwriting of cyber risk insurance, apparently, has not been made.

Please see our responses below

(P) What role could/should public policy play, if any, in the development of a cyber-risk measurement framework that would be useful in developing insurance products?

We think that public policy should play as little role as possible in the development of a cyber-risk measurement framework in developing insurance products. Insurance products already exist, though whether these products are effective still can be debated. The difficulty in establishing more effective and transparent insurance products is the present low level of acknowledgement by participants in the clouds, both vendors and users, that the moment that an entity becomes a carrier of data, that entity has an implied liability resulting solely from the potential that you might lose the data. Hence, ultimately the real metrics in quantifying the amount and breath of the liability will be derived from a simple formula. The formula is based on how long an entity has the data of a 3rd party and what data was under their province. As the technology industry is already geared to measure time, the ability to do so as it relates to cyber risk already exists. Hence the more meaningful enigma at present is how to quantify the liability. In this instance, it is really just a case of ongoing education of cloud users and cloud providers to create a greater acknowledgement that building financial resiliency is necessary through the engagement of companies that are experts in the field of risk transference by developing value ranges for specific types of data sets (i.e. a credit card theft would not have the same liability to an entity when compared to a lost medical file). As the US contains, arguably, the most sophisticated financial engineers in the world, the infrastructure to facilitate cyber risk is already in place and the driving engine should then be creating greater customer demand for risk transfer products that address the "What If" scenarios. Generating customer demand will be a function of several catalysts to include cloud vendors acknowledging their implied liabilities, customers of the clouds demanding some sort of assurance of their respective cloud vendor to demonstrate financial resilience and /or a BIG event. Under this thread of thinking, the tools are already in place to

facilitate greater momentum in the creation of a deeper cyber risk transfer market that would be filled not just by insurance products but also hedging strategies that can also be developed as financial cyber-risk mitigation processes. In an indirect way though, the public accounting arena will definitively play a large role in the future in terms of how to get presently unseen, or, at a minimum, unacknowledged liabilities to show up on a respective company's balance sheet. Additionally, as more data is lost and repercussions of such begin to echo louder in the court system, the ability to narrow the band of quantifying the implied liabilities resulting from a decision to carry data will only be enhanced in the future. The US is a world leader in technology, financial engineering and through its insurance industry boasts an infrastructure in place to disperse risk, regardless the type. Hence, to original point, we think public policy on this matter would only serve severely to dampen momentum.

(Q) In the face of growing risk from the increasing volume of cyber threats and vulnerabilities, what data can be made available to companies to support decisions regarding protection through the purchase of insurance products or investing more in CyberSecurity protection controls?

At present, we have been formulating a database to capture all publicly known events. While the immediate information is helpful in terms of being able to establish a band-with for specific data breaches, the data should be considered ever evolving as a data breach today might not yield a liability until some time in the future. For example, if a medical file is lost today, the liability might not be recognized until some time after that the medical record is used in a nefarious way, or until such time, that the medical record's owner suffers some harm from such use (this ultimately will be decided in the courts). It is our belief that as more participants enter into the risk transfer market, all participants (cloud vendors, cloud providers, insurance companies, risk transfer specialists, etc….) should begin to see their overall cyber risk profile go down over time given more entities from all industries are now sharing the risk. Hence, the absolute dollar spend for security and intelligence will go up – it will have to. Ultimately, there needs to be more catalyst events to move the market significantly, but in the interim, we contend that using what we know to educate is a reasonable starting point. The acceleration of the data collection and the continuing evolution of the data set could be greatly enhanced by cloud vendors and cloud users being more open about breaches that they experience, yet do not make it into the public domain. The insurance, accounting and financial analysis industries ultimately will serve as primary accelerants to making the growth of the cyber risk transfer market in terms of demanding complete transparency on all cyber risk matters. We do not think that any one data collection point, nor tool, is the answer. Rather, in the most efficient market, those entities that understand the risks through more accurate quantification of such will do better than those that do not. That is the inherent driver.

(R) If companies were able to predictably limit financial risk through specific cyber-insurance coverage at a reliably predictable cost, how would this affect investment in cyber-security programs and infrastructure?

Our solution is the response to the question, which is outlined in our business plan.

CyberRisk Partners

415 Madison Avenue, 15th Fl.
New York, NY 10017
1.646.673.8511

(S) To what extent might insurance providers create incentives or requirements for such investment?

At present there seems to be little incentives for entities to be completely forthcoming regarding security breaches given the lack of market and/or government requirements to do so. The trend appears that negative cyber events only make it into the public domain when it appears an event comes with the potential of a possible negative financial outcome. There is a pool of data that is not being collected and ultimately analyzed as there is no motivation to do so until such time that the breach manifests itself as a potential financial loss. An entity is motivated toward this behavior as the tail of the breach is an unknown liability until such time that it MIGHT manifest itself. Until that time, the logical argument an entity can make is we will worry about it if we have to and as we are not sure what it might cost later and is presently not costing anything, why create the perception that the breach in fact does constitute a liability, whether that is a cash outflow or a liability entry on their balance sheet which would have a negative impact on an entity's profit/loss statement. Overcoming this inertia ultimately will be reliant on creating cyber risk transfer demand, which we believe is inevitable

(T) In the absence of empirical data to quantify losses from certain types of cyber incidents, what criteria could be used to most accurately and effectively determine premium costs?

More effective measurement of damage and harm can be drawn upon by involving the end-user and/or owner of the data. When one approaches the end user/data owner to quantify the individual's *perceived* Cyberliability losses that would result from a data leak, one begins to narrow the bandwidth of quantification as to what the perceived economic data loss that is sustained, ultimately represents.

(U) What, if any, quantitative relationship can be established between investment in security controls and the cost of insurance?

Pursuant to our research within our proprietary CyberFactors™ database regarding measurement of cyber exposures vs. realized, actual losses - our view sustains that no quantitative relationship can be drawn between investment in security controls and cost of insurance, as simply measuring security controls does not capture all the cyber risk variables that currently exist.

We don't dispute the question, we are simply stating that one cannot take a multi-dimensional equation and solve it with a two-dimensional approach.