GUY CARPENTER

Business Roundtable Address on Cyber Security and Reinsurance

Homeland Security Task Force
December 13, 2001
Washington, DC


Harry Oellrich

The Business Roundtable, an association of chief executive officers of leading U.S. corporations, recently invited Guy Carpenter's Harrison D. Oellrich to speak to their task force on homeland security. The Roundtable is selective in the issues it studies; with a principal criterion being the impact the problem will have on the economic well-being of the nation. Working in task forces on specific issues, the chief executives direct research, supervise preparation of position papers, recommend policy, and lobby Congress and the Administration on select issues.

In essence, The Business Roundtable believes that its potential for effectiveness is based on the fact that it draws on CEOs directly and personally, and presents government with reasoned alternatives and positive suggestions.

Harry Oellrich: Good morning, it's good to be with you here today. A simple salutation, perhaps, but one which has taken on an entirely new perspective since the September 11 terrorist attacks on the Pentagon and World Trade Center. Guy Carpenter had its home office staff of over 700 in Two World Trade, the south tower, and our primary insurance colleagues at Marsh, Inc. had a major presence across the plaza in One World Trade, the north tower. On that beautiful morning, the kind aviators refer to as "severe clear", I was in my office. I was also in the March 1993 bombing, so yes, it is indeed very good to be here with you this morning!

Having experienced so much in these two attacks, I cannot overemphasize the importance of working collaboratively with the government to do everything within our collective power to thwart further attacks. As we have heard in this morning's "threat briefs" by members of the White House staff and the law enforcement and intelligence communities, attacks against various components of our critical infrastructure can be of either a physical or digital nature. If we are not protected against such attacks, the potential for devastation increases exponentially.

During the next few minutes, I will attempt to provide a short overview of the importance of reinsurance to the insurability of emerging Internet exposures. Reinsurance, to many of you, is probably a term that you have come across only occasionally, if at all. However, it can be the key driving force behind the availability and affordability of coverage for your organizations and, therefore, protection against various threats to the very viability of your enterprises. Let's begin with a little level-setting.

All insurers, from the most modest single-county mutual insurer, right up to the largest multi-national stock company, require and therefore purchase various reinsurances. For example, AIG and Chubb are both major clients of Guy Carpenter. Both of these clients need to purchase protections to mitigate exposures from the underwriting of their respective network security products, the AIG netAdvantage[SM] Suite and CyberSecurity by Chubb[SM] for Financial Institutions.

At the end of the day, all reinsurance is purchased to provide the insurer with one or more of the following benefits: capacity, stability, financing and/or catastrophe protection. Reinsurance is either sold by reinsurance companies or reinsurance departments of insurance companies throughout the world. Some of the more prominent reinsurers you might be familiar with include Lloyd's of London, General Re, American Re, Munich Re and Swiss Re.

In recent years, as the exposures associated with cyberspace have proliferated, insurers – and especially reinsurers – have become increasingly concerned that, because these very sophisticated exposures were not fully contemplated, they cannot be successfully underwritten. This is particularly an issue within the context of traditional "bricks and mortar" property and casualty policy forms. Some specific risks associated with this space include:

- Damage, theft, or disclosure of electronic information;
- Loss of service;
- Lack of authentication, repudiation of agreements because of a lack of valid confirmation;
- Computer fraud;
- Privacy violations;
- Legal and regulatory uncertainty; and
- Intellectual property, content, and advertising infringement

A major difference between these emerging risks and traditional property and casualty exposures is that many of these risks are intangible. If a company's confidential electronic information is disclosed, lost, stolen, destroyed, or corrupted, the impact on earnings and even share price can occur within hours, not days or weeks.

The recognition that these exposures are very different further fuels reinsurers' concerns that the ceding companies they support are unable to sufficiently quantify, underwrite,

and price for them, especially when a part of existing policies. Consequently, reinsurers are in the process of mandating that loss from certain new exposures, most notably viruses, worms, etc., will be tightly controlled, if not entirely excluded within the traditional portfolios they reinsure. This process was well underway even prior to the attacks on the World Trade Center and Pentagon, and will be realized as insurers and their reinsurers negotiate to renew their reinsurance agreements, called "treaties", over the next 12 months. The knock-on impact of this to business is that coverage for these exposures is being dramatically curtailed – if not totally eliminated – from their existing property and casualty policies as we speak.

As companies grapple with severely limited access to coverage through their traditional insurance products, a new generation of insurance products focusing solely and specifically on these exposures has been developed. Beginning with the development of Marsh, Inc.'s Net Secure™ product, the AIG netAdvantage℠ Suite and Chubb's CyberSecurity by Chubb℠ for Financial Institutions, products have been developed to provide specific solutions to businesses that engage in e-commerce. Since they are stand-alone products, they enable underwriters to individually assess, underwrite, and price each client's unique Internet exposures.

Consequently, it has become absolutely critical for a company to have a comprehensive security plan in place prior to going on-line. Redundancies in key systems and well thought-out action and recovery plans are vital to the mitigation of damage and economic loss in the event of an attack. Additionally, security assessments, which are conducted by independent third parties and are required prior to coverage under the new generation of stand-alone network security products such as the AIG netAdvantage℠ Suite and CyberSecurity by Chubb℠ for Financial Institutions, are a valuable tool for uncovering and addressing weaknesses in a firm's network security protocols.

And here again, reinsurance becomes critical. As with most new product offerings, insurers look to reinsurers to support their efforts in developing new products through the implementation of agreements designed to share the risks being insured. An extensive due diligence process by reinsurers with their ceding company to scrutinize the new product offering ensues, which allows more time for both the insurer and reinsurer to more closely examine the new product. As this process unfolds for these new products, insurers and reinsurers became aware of specific and potentially catastrophic exposure that had to be dealt with in order for this much-needed marketplace to develop.

In order for insurers to provide a lasting solution to businesses' need for protection against these emerging exposures, it became necessary for both insurers and reinsurers to address the potential for multiple losses arising from a single Internet attack. For instance, an attack directed simultaneously against many businesses in a given sector or

across several sectors could, if successful, seriously affect insurers, reinsurers and our economy in much the same way as a natural disaster such as a hurricane or an earthquake would affect the "bricks and mortar" world. This exposure, which we have nicknamed "cyber hurricane", must be addressed in order for a working marketplace for these exposures to develop and mature.

This, in turn, leads us to how our friends in government can perhaps assist. Insurers and reinsurers have invested a tremendous amount of time and resources over the last decade in an effort to quantify, through the use of sophisticated probabilistic and deterministic modeling, their actual expected losses. These losses can be quantified in relation to either their existing or a theoretical portfolio of risks in just about any real or hypothetical loss scenario, be it an earthquake, windstorm, or other physical peril. Having convinced themselves that they can thus construct a portfolio of business from which they can expect an acceptable exposure to loss from any one of these natural perils, enter these cyber exposures which initially appear to subvert their newfound ability to make accurate predictions.

The Internet is viewed with great concern by the industry, and on the surface at least it is so unique that it cannot be modeled in this ground-breaking way. Whereas natural perils losses occur in a specific geographical location, the Internet is both everywhere and nowhere and its perils are neither fully identified nor defined. Historical data needed to populate models for bricks and mortar property catastrophe exposures is plentiful, while historical data to build and run models for these new cyber exposures is virtually non-existent. In fact, many past attacks have never been reported at all because companies are fearful of sharing information about cyber crime and attack – their customer reputations can be seriously damaged if on-line transactions are perceived as insecure.

With credible data and a way to model exposures, there is every opportunity to build a substantive and sustainable reinsurance marketplace to support these exposures for insurers and their clients. To the extent that government has collected and manipulated data in this area, if made accessible, this data and its modeling can be used to jump-start insurers and reinsurers dealing with cyber exposures.

In summation, what does all of this mean to the various interests in this room?

1. Many businesses relying on their traditional property and liability policies are likely to find themselves with extremely limited, or even a complete lack of insurance protection for several significant emerging Internet exposures. This will likely occur while use of the Internet as a channel of distribution is increasing dramatically for the companies themselves.
2. Businesses must have comprehensive security and recovery plans in place to handle a cyber attack, to help mitigate the impact a future attack could have,

and to qualify for coverage under new stand-alone policies being offered in the marketplace to fill these coverage gaps.

3. Stand-alone solutions for providing such coverage have been developed and are currently being refined by Marsh, Inc., AIG, Chubb and others to meet this need, but will need to have reinsurance support to be able to adequately meet future demand.
4. In order to help ensure that adequate reinsurance support is available to meet this need, new reinsurance products, data and models must be developed to enable insurers and reinsurers to quantify their aggregate exposures.

Finally, from a personal perspective, I would like to close by mentioning how truly impressed I am with how quickly all of us, after the extraordinary events and nearly unimaginable challenges of the past three months, have, as individuals, as families, as businesses, and as a nation, rebounded and gotten back to doing what we do in our lives! If we can work collaboratively on critical issues such as this in the future, and concentrate on the truly valuable things in life, I have no doubt that our children will see a brighter, safer future.

_____

Since 1979, Harry Oellrich has been a key contributor to Guy Carpenter's success. A Managing Director at Guy Carpenter, Harry was recently elected Managing Director of Marsh, Inc. Even prior to September 11, he has been working closely with the White House and other governmental entities to understand complex issues such as infrastructure interdependencies and actuarial data needed to support new areas of risk transfer. He can be reached via e-mail at harrison.d.oellrich@guycarp.com

TOP