GUY CARPENTER

Harry Oellrich *is a Managing Director at Guy Carpenter.*

Internet-Related Business Risk
Part One

The rapid development of a wholly new electronic marketplace has created the need for companies doing business there to protect themselves from exposures that were never contemplated in a bricks and mortar world. Forrester Research, in an article recently published in the LA Times, was quoted as saying that business-to-business Internet commerce will increase to $1.3 trillion by the year 2003, from $43 billion last year. Consequently, insurers and their reinsurers are faced with a growing increasing need to understand and respond to the emerging risks associated with this movement to a digital economy.

Guy Carpenter Views talks with Harry Oellrich, a Guy Carpenter Managing Director, about the evolution of Internet-related business risks and some of the innovative solutions that are being developed to respond to these risks. Harry is presently responsible for several large clients within the global accounts department in New York. Additionally, he is a member of the firm's Professional Liability Initiative and Professional Liability Practice and is coordinating its e-commerce reinsurance activities.

Topics At A Glance:

The Evolution of Internet-Related Business Risks

Guy Carpenter Views: What are some of the specific risks, both first and third party, that are associated with using the Internet in the course of business? How are these risks different from those that exist in the material world?

Harry Oellrich: Moving from a material to a digital world clearly changes existing risk, but there is a lack of definition and quantification of these new cyber risks and little historical data available with which to calibrate them. Companies will not share information about their experiences with cyber crime and cyber attacks, because their reputation could be seriously damaged if the public feels that trading with them electronically is not secure. Therefore, the only losses that we are likely to hear about are just the tip of the iceberg.

Specific risks emerging from doing business in cyberspace include:

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

A major difference between these emerging risks and traditional property and casualty exposures is that many such 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.

GCV: Can you describe some of the recent cyber crimes that have highlighted the need to effectively address these risks?

HO: In recent months, we have been inundated by media coverage of cyber attacks. In this year alone, there have been seemingly endless stories about the introduction of various "viruses" via the Internet, some causing little more than annoyance, others having more destructive consequences. In February, a series of highly publicized Distributed Disruption of Service (DDOS) attacks occurred, taking down several very well-known e-business sites for varying periods. Additionally, there was at least one extortion attempt, where a hacker threatened, then actually carried out his threat, to release a company's customer lists and their personal information if he wasn't paid a sum of money.

GCV: In your opinion, how important is it for companies to have a security plan in place before going on the Internet? What are some of the other security measures companies can use to protect their proprietary information?

HO: There is no question that it is absolutely critical for a company to have a very 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 a problem. In addition, coverage under some of the new e-commerce insurance products, such as AIG's "NetAdvantage Security+" and Marsh's "NetSecure," requires security assessments that look closely at the prospective insured's security and recovery plans.

Coverage Under Traditional Policies

GCV: Can coverage for Internet-related risks be found under any traditional policies?

HO: The answer to this question is tricky. At this point, I would respond with a tentative maybe.

Clearly, cyber risks were not contemplated when existing property and casualty policies were first developed. Consequently, litigation will almost certainly take place to determine what protection, if any, is granted under these policies.

However, traditional policies, which were designed to protect physical assets against perils such as earthquakes and hurricanes, will likely not protect information or reputation assets against such cyber perils as denial of service or theft of information.

GCV: What are some of the common problems (e.g., definitions and exclusions) with traditional policies with regard to the coverage of Internet perils?

HO: Because traditional policies clearly never contemplated these unique perils, they will not fit neatly within existing definitions and exclusions.

For instance, with respect to first-party coverage, traditional property policies generally cover only physical damage caused by perils such as fire and windstorm. Additionally, traditional property and crime policies cover only tangible property. They do not cover intangible assets and information assets, for example, customer lists, customer information, and competitor information.

Similarly, with respect to third-party coverage, general liability policies typically provide coverage for bodily injury and property damage arising from an accident or occurrence. Nothing in these traditional coverages responds specifically to claims arising from a cyber attack against a company's computer system or from transmission of a computer virus to third parties. The disclosure of private or confidential information is also typically not addressed.

There are a number of other common problems related to the ability of traditional policies to address Internet exposures, such as:

- Companies may not have errors and omissions coverage, or, if they do, such coverage contains a security breach exclusion.
- Advertising injury coverage under a general liability policy does not completely address intellectual property infringement, content, and advertising offenses committed over the Internet.
- Under many property policies, business interruption/extra expense is triggered only if there is direct physical loss.
- Intellectual property stored electronically is valued as "data."
- Crime policies contain confusing exclusions and limitations with respect to employee dishonesty and computer fraud.
- Policy coverage may not be global.

Modifying Existing Policies To Respond To Internet Risks

GCV: Are insurers modifying traditional policies to either clarify their intent to include Internet exposures or explicitly limit coverage? Which policies are most affected by these modifications?

HO: I am not aware of any instances in which companies have modified existing policy language to either reflect or exclude coverage for these new exposures. The unveiling of products such as NetSecure and NetAdvantage Security+, which do explicitly protect against these exposures and can be purchased to either supplement traditional policies or as first-line policies, would not have occurred if Internet risks were viewed as being covered elsewhere.

If modifications to existing policies are to be implemented, the policies that would likely come under scrutiny are the traditional property, general liability, and crime forms, as well as some errors & omissions policies.

A substantial opportunity exists for insurance companies and brokers to address these recently identified and evolving exposures by developing innovative products.

Mr. Oellrich will discuss some of these new products, as well as Guy Carpenter's role in this market, in Part Two of this interview.

A managing Director of Guy Carpenter, **Harrison D. Oellrich** is responsible for several large clients within the Global Accounts Department.

Mr. Oellrich began his career with Guy Carpenter in 1979 and has negotiated and placed a wide variety of property and casualty reinsurances for several of Guy Carpenter's most prestigious clients during his nearly 20 years with the firm.

A graduate of Hofstra University, he earned a BA in Political Science and an MBA with a concentration in Management while studying there. He can be reached via e-mail by contacting marketing@guycarp.com

TOP