



Besieged by Cyber Liability?

By Neil Kransdorf and Steven Dyson

Web sites, online services, e-mail and software programs have created vast new industries whose clients demand that insurance coverage is in place prior to awarding contracts.

Aside from creating new business opportunities, these complex technologies present new exposures to companies that are not covered by standard miscellaneous professional liability and/or commercial general liability policies. In addition, trends of increased computer virus and third-party hacking activity, post 9/11, means that exposures are multiplying far faster than most companies keep up with. How does an agent convert these complex issues into simple terms that a customer can understand?

First, cyber liability exposures or more accurately described as technology, media and professional services (TMPS) exposures and liabilities are not routinely understood by insurance professionals or insured's. The understanding of common terms is an essential building block to gaining expertise. This will position you to better understand your client's business, their customers, competitors and potential risk exposures.

Second, a working knowledge of the sources of TMPS claims is very helpful to determine whether or not a company needs to purchase a TMPS policy. This will provide you with the armor to endure and successfully survive the typical questions like... Why do I need this policy? A client may bring suit against a company for a number of different allegations, including:

- an error or omission,
- intellectual property (i.e. copyright/trademark infringement, trade name),
- breach of contract,
- negligence in the performance of professional services,
- failure to render professional services and personal injury (i.e. liable/slander, defamation, and invasion of privacy),
- breach of security (i.e. virus, hacker, unauthorized access), and misrepresentation.

Being able to relate these situations to your customer's business and citing examples is usually a positive experience for both you and your customer.

For example, let's say you're meeting with a company that provides information technology consulting services. The company provides consulting services to help clients improve Web site performance, maintenance, service offerings and return on investment. If the company advises a client to move their Web site to a new hosting facility and there are major service interruptions during the process, the company can be sued for breach of contract and misrepresentation. In the meantime, if the company lists the client on their Web site as a reference without their permission, the client could allege copyright/trademark infringement.

Third, an appreciation for trends and statistics concerning risk and exposures helps to validate the vulnerabilities that companies are dealing with today, and into the future.

Studies show that virus attacks, unauthorized computer access, a.k.a. "hacking" is on the rise, some with significant consequences, while others are a small nuisance. Either way, the outcome(s) can be unpredictable, which makes stopping them a challenge, however, an absolutely necessary task as they could potentially impair a company's obligations to third parties.

How real is this threat? You can answer this question yourself. The "2002" Computer Crime and Security Survey" can help to validate these trends. The survey is based on responses from 503 U.S. companies and

concludes that the threat of security breaches continues to escalate and that financial losses are mounting. For example, "99 percent of respondents detected computer security breaches within the last 12 months, and 88 percent acknowledged financial losses due to computer breaches." There is a siege on network administrators today by worms, bugs, viruses and who knows what else.

As these professionals are tracking down these pests they may remain blind to a whole group of other nasty intruders. The list of risks and exposures are growing faster than budgets or staffs can keep pace with. Making sure that all of these risk exposures are adequately covered is no simple task.

Now that we have described the playing field in terms of the many risk exposures its time to discuss the coverage game plan.

As TMPS exposures evolve so are insurance policies that cover them. The trend with CGL policies is to specifically exclude any cyber liability exposures.

For example, CGL policies won't provide coverage for intentional torts, or intellectual property claims, such as copyright infringement, trade secret infringement or trademark infringement, under the coverage for bodily injury or property damage liability. A MPL policy will only cover the risk exposure associated with negligence in the performance of professional services and specifically excludes the intellectual property and breach of security exposures. Some MPL policies will add these coverage's by endorsement but coverage under the policy still needs to be triggered by a wrongful act which, does not usually happen for intellectual property and breach of security claims. The TMPS policy replaces the MPL policy and fills the gaps of the CGL policy.

As companies become more dependent on the Internet, online services, e-mail and other complex technologies, they are clearly increasing their risk exposures.

In today's evolving information technology arena, technology and media professionals face many new hazards and potential pitfalls that were not even envisioned a few years ago.

A TMPS policy can address the needs of companies to protect against financial loss associated with all of these exposures.

A good TMPS policy combines professional errors and omissions coverage with coverage for media and intellectual property liabilities within a single policy, including coverage for the company's electronic activities, as well as the gathering and dissemination of media materials online or in any other media form.

Kransdorf is an executive vice president with E-Risk Services, with over 10 years of experience in professional liability products. He is also the COO of the company. Dyson is an executive vice president with E-Risk Services, with more than 16 years of experience in underwriting, sales and marketing of management liability and health & welfare insurance. He is the chief marketing officer for E-Risk.