



Cyber Liability: A World Wide Web of Risk

By Robert G. O'Shea, Jr.

As evolving technology facilitates an increased usage of the internet, almost all companies face a breadth of liability issues they may never have experienced before. Although companies use technology and the internet in various ways, the exposures are generically referred to as "cyber liability". Whether companies advertise or conduct electronic commerce (e-commerce) on the internet, own, design, develop or consult on websites, or act as a host or internet service provider, it is important to understand the exposures presented and the insurance risk-transfer programs now available to address them.

Background

Companies increasing their reliance on computer networks for data and business continuity simultaneously increase their vulnerability to loss. In 2003, computer viruses and hackers together caused an estimated \$16 billion in damages according to American International Group's eBusiness Risk Solutions. Although many attacks emanate from non-traditional sources, a recent survey by the Computer Security Institute (CSI) illustrates computer crime threats come from both inside and outside a

company's electronic perimeter (e.g. employees).

Other computer related loss exposures to be considered include loss of data due to power outages or the improper storage and safeguarding of sensitive customer and website visitor data (i.e. dates of birth, PINs, credit card, drivers license and Social Security numbers), as well as costs associated in restoring the public's confidence when these losses occur.

Effective risk management programs generally require companies that have internet exposures install formal security processes and systems to protect themselves from attacks from third parties (i.e. "hackers"), including disgruntled employees. These measures should be tested regularly by competent outside firms to certify their effectiveness (for both vulnerability and penetration levels). Ernst & Young's "Global Information Security Survey 2003," revealed that 90 percent of 1,400 organizations surveyed recognize that information security is of high importance and 78 percent identify risk reduction as the major influence on their information security spending. Despite this concern, surprisingly over one third

of these organizations said their ability to determine whether their systems were under attack was inadequate while also acknowledging they were inadequate in their ability to respond to incidents. Two-thirds said they weren't compliant with applicable security regulations.

Many wrongly expect that as security systems and safety techniques become more effective and universally applied, they will help reduce the exposure and incidences of loss, ultimately reducing the costs of risk transfer. But, there are other issues involved.

An important consideration is the widening legal aspects. Specifically,

- the unique global characteristics of the internet presents many new legal exposures/risks that fall outside the scope of traditional insurance policy coverage;
- there is a greater recognition of the value of intellectual property entities are not only looking to protect, but exploit;
- international and local laws, multi-jurisdictional disputes and technical issues will continue to greatly affect many companies as never before;
- many local and international jurisdictions are invoking laws geared toward protecting an individual's identity, requiring company's full compliance; and
- there is greater difficulty in assessing damages.

Adam H. Fleischer, an insurance litigator with the firm Bates & Carey (Chicago) said, "cyber liabilities are the slip-and-fall exposures of the next millennium." To further help develop their risk management program, companies need to evaluate their respective exposures, assess their appetite for risk and compare them to the level of protection afforded under existing insurance programs. They would also be well served in exploring the breadth of coverage insurance markets now offer to enhance the effectiveness of their risk management program.

Swiss Reinsurance's study, entitled "The Impact of E-Business on the Insurance Industry: Pressure to Adapt -- Chance to Reinvent" released in 2000, divided e-commerce risks into two categories; technical and liability. On the technical side, computers remain vulnerable and susceptible to technical faults that disrupt the production process, resulting in losses. Examples of this include programming errors, software performance or the failure of your work to perform as warranted within your contract.

Sometimes for discussion purposes, included within this realm are security issues, including unauthorized access to or theft of data or e-business activities, unauthorized e-commerce transactions, computer viruses or "denial of service" attacks.

With respect to liability, electronic commerce accommodates millions of transactions. Such use and volume of the internet increases opportunities for crime

and opens new frontiers for errors, omissions, libel and trademark violations. Cyber liability torts will differ from traditional predecessors in several ways, including the types of intellectual property claims, the complexity of the claims and multi-jurisdictional issues, all of which also serve to increase defense expenses. As the magnitude of torts increase, the number of claims and their related defense expenses will rise, exponentially.

Traditional Insurance is Inadequate

“Traditional” standard property and commercial general liability (CGL) insurance covering “tangible property” does not adequately address cyber risks (e.g. attacks or network security failure, programming errors, contract performance disputes or other Professional Liability exposures). In fact, to eliminate past coverage uncertainties, the newest standard Insurance Services Office (ISO) general liability forms specifically exclude data or other network security risks (“cyber-exposures”).

Arguments such as whether cyber torts constitute “advertising” within the meaning of traditional “media liability” policies can also be used to support the theory that these policies are inadequate. These policies may respond to “traditional” personal injury and copyright claims, but most likely will not address E&O exposures related to electronic delivery systems.

Recognition of these new exposures has led the insurance industry to develop “e-commerce” or “cyber liability” insurance policies. Insurers initially offered coverage via modified traditional commercial general liability, property, media liability or errors & omissions liability policies to address these risks. Later, as underwriters became more familiar with risks and their loss

potential, forerunner policies known as “network computer liability” evolved into the various specific cyber liability policies available today.

Driving this metamorphosis was the increasing use of the internet as a commercial tool. Companies began to contractually require their vendors to obtain some form of network security insurance to protect them from accidental or criminal loss which increase the demand for broader insurance.

Cyber Risk Policies

Today’s policies can be underwritten on either a “package” or a stand-alone basis, depending on the company’s size. Stand-alone programs for larger risks are available on a modular or menu-driven framework and are generally tailored to the company’s specific exposures. Insureds can purchase several or all of the coverage parts available, designed to address liabilities ranging from errors and omissions from the technology and internet side, network security exposures, virus transmissions, as well as media Intellectual Property exposures, all on a global basis. Some policies have also been expanded to provide “Cyber Extortion” coverage to address the threat of damage or misuse of an insured’s computer system, electronic data or website by outside parties.

Cyber liability programs generally cover both first-party and third-party liability, including:

Errors and Omissions – coverage for defense costs, settlements, judgments (and sometimes punitive damages) or other financial loss resulting from a broad range of computer systems (internet media) and information

related professional services provided to customers, such as:

- Breach of privacy due to theft of data (e.g. credit cards, financial or health related data),
- Security failure causing network systems to be unavailable to third parties,
- Inadvertent transmission of a computer virus or other liabilities resulting from a computer attack,
- Rendering/failing to render Internet Professional Services, and
- Intellectual Property risks such as advertising injury or personal injury from allegations including libel, trade libel, slander, defamation, copyright or trademark infringement, plagiarism or other “media” activities on the company’s web site.

Business Interruption – covers loss of business income as a result of an attack on a company’s network that limits the ability to conduct business, such as a denial-of-service computer attack. Coverage also includes extra expense, forensic expenses and dependent business interruption.

Cyber Extortion – covers the “settlement” of an extortion threat against a company’s network, as well as the cost of hiring a security firm to track down and negotiate with extortionists.

Public Relations – covers financial costs associated with restoring public confidence.

Criminal Rewards – covers the cost of posting a criminal reward fund for

information leading to the arrest and conviction of the cyber criminal who attacked the company’s computer systems.

Cyber Terrorism – covers those terrorist acts covered by the Terrorism Risk Insurance Act of 2002 and, in some cases, may be further extended to terrorist acts beyond those contemplated in the Act.

Identity Theft – coverage for misuse of information provides access to an identity theft call center in the event of stolen customer or employee personal information.

There are several insurance market leaders that will write this coverage for large US based firms. Others, including U.S., London, European and Bermuda based markets will support these leaders to develop programs requiring significant capacity.

Cyber Liability Loss Scenarios

In many instances, companies that experience claims make every attempt to settle large losses. They also tend to keep this information confidential and away from public scrutiny because they deem it to be a matter of reputation and business continuity.

With respects to computer crime, in 2003, the FBI reported that less than 40 percent of companies that had experienced at least one computer intrusion reported the incident(s) to law enforcement. For these reasons, it is very difficult to provide actual historical cyber liability and cyber crime claims information.

However, the following loss scenarios highlight common situations companies face:

- A virus attacks your computer system leaving your company unable to fill customer e-commerce orders for an entire month. Your company loses a significant amount of revenue over this time span, but the inability to fill customer orders cost your larger customers revenue because they rely on your company to supply critical parts. They sue your company to recoup their losses.
- Your company web site is secure but a virus attacks the e-mail system. Your company employee transmits the virus to your customers and they sue for the cost of “cleaning up” their own computer network.
- Hackers break into your customer database and steal vital customer information. A customer’s identity is stolen and they sue your company for damages.
- Your system allowed hackers to gain access to personal data of your customers stored on your system in a country that just recently passed privacy laws that now hold your company responsible for any and all damages incurred. Thousands of customers are affected and will likely sue.
- There is no clear “error or omission”, but your customer is not satisfied with the end result of the publication (your product) and brings a claim to obtain a

different result to avoid paying your fee. Your company looks to insurance to pick up the legal expenses to defend the claim.

- A customer alleges your company negligently staffed a project and rendered their system unusable. They sue for loss of revenues as well as breach of contract.
- Malicious employees misuse information provided by e-customers.
- A celebrity sues your company for “fair market value” for improperly using their name and photo on the website, which can be accessed globally.

Conclusion

Technology continues to change businesses, its applicable risk exposures and the need for companies to protect themselves and their customers. Regardless of whether it’s B2B or B2C, web page design or hosting, today most companies are best advised to consider protecting themselves by purchasing some form of cyber liability coverage. It can be asserted that if your company has a computer system or a web site, you need cyber liability protection to address your exposures. Companies should review their insurance to determine whether coverage clearly applies to their particular operations. We also recommend this issue be discussed with your insurance broker and attorney if there are any questions or concerns.

Revolutionary

Beecher Carlson is revolutionary. We're an integrated commercial insurance and risk management brokerage that leverages a unique combination of advanced analytics, technology tools and years of industry expertise to assess and model risks in a way that provides clients the right solution, every time. For more information about the services we provide, call 800-657-0243 or visit www.beechercarlson.com.

Robert G. O'Shea is a Vice President at Beecher Carlson's Executive Liability Practice in New York. He has over twenty seven years of experience in the insurance industry, with a particular expertise in developing insurance solutions for Professional Liability and Errors & Omissions exposures.

Prior to joining Beecher Carlson, Bob served as a Senior Vice President at Marsh Inc. He can be reached at roshea@bechercarlson.com

Disclaimer

This publication is for informational purposes only. It is not a guarantee of coverage and should not be used as a substitute for an individualized assessment of one's need for insurance or alternative risk services. Nor should it be relied upon as legal advice, which should only be rendered by a competent attorney familiar with the facts and circumstances of a particular matter.

© 2005 Beecher Carlson Holdings, Inc.
All Rights Reserved.