

BUSINESS INSURANCE IN THE AGE OF E-COMMERCE

Meredith Blake Martin, Esq.
Astrachan Gunst & Thomas, P.C.

Does your company use the Internet during the course of your business operations? Do you accept orders or emails from your website, or emails through your company's website? Do your employees use email to communicate internally or externally? Does your company provide IT services? If you answered "yes" to any of these questions, you are at risk for a computer virus which may destroy business data and/or equipment, such as PCs, hard drives, and disk drives. If your business involves *providing* computer programming or other IT services to customers, you are at risk for infecting customers with a computer virus and may, consequently, become liable for their loss of data and/or equipment. Importantly, *you may not be insured for this risk* under either a first party or third party business insurance policy.

In 2001, the Insurance Services Office, Inc. ("ISO") changed the language of the standard form commercial general liability policy to expressly exclude electronic data from "property damage" coverage. The majority of business liability insurance policies currently being written, therefore, either expressly exclude losses of electronic data, or deny coverage for losses caused by a computer virus on the basis of a narrow definition of "physical loss or damage" or "property damage." In other words, a general business insurance policy likely will not cover losses caused by malicious code unless hardware, or physical computer components, is damaged in addition to data corruption. This type of physical damage may be difficult to prove, and courts have generally been unwilling to extend coverage on this basis, as the distinction between data corruption and physical damage to computer equipment appears to be an illusory one. The bottom line: most insurers never intend to cover computer virus loss under property insurance policies, and will routinely deny coverage for this type of claim.

At first blush, a computer virus may appear to be a minor inconvenience. Your website may become inoperable for a period of time, or your company's email system may not function in the short term. Consider, however, a circumstance in which the computer virus renders numerous PCs or other hardware components inoperable; repair can easily cost hundreds of thousands of dollars. Consider loss of income, costs to repair and restore damaged systems, public relations costs (particularly if you are an IT company), loss of information or data not properly stored, and stolen or corrupted data due to unauthorized access. Specific claims have included the following:

- An employee dials into the company network remotely, introducing a virus into the company's network, which virus was ultimately transmitted to software being installed

on products sold by the company; by the time the virus was discovered, the insured had to shut down the assembly line, remediate the problem, and address the infected products at a total loss of approximately \$15 million.

- A hacker steals and publishes customer credit card information from an online retailer, causing approximately \$2 million in loss of income and third party damages.
- A hacker overwhelms websites with seemingly legitimate requests for data, causing loss of income of approximately \$1 million.
- A disgruntled employee downloads malicious code onto firm's network, publishing confidential client information and destroying applications.
- A third party seeks damages from the developer of an application for an error or omission in the code which causes third party to sustain losses.

While virtually all businesses have some exposure to this type of loss by virtue of simple use of the Internet and/or email during the normal course of business operations, the companies most at risk are those which transact business online or provide computer-related services.

Insurance coverage issues aside, every business should have certain precautions in place, including installation of anti-virus software, firewalls and intrusion detection software, and implementation of security policies. Companies should also consider allocating this type of risk by contract, as appropriate.

In assessing how to insure your company's e-business risk, there are several choices: self-insurance; a general business liability insurance policy (possibly with an endorsement covering electronic data losses); and/or a stand-alone e-business or cyber liability policy (which may provide the added benefit of an insurer's duty to defend). Consider carefully which of your company's operations depends on computer programs, the volume and importance of the company's transactions via the Internet, what company data is stored electronically, and whether the business involves providing software or related services to customers. Be sure to understand the scope of coverage and exclusions afforded by your current business policy, and consider the availability of stand-alone policies to address your specific e-commerce insurance needs. An ounce of prevention *now* is worth a pound of cure; the frequency and severity of this type of claim only continues to increase with the growth of electronic commerce and communication.