

Critical Computer Assets May Be Exposed to Risk by Gaps in Business Insurance Coverage

By Cathy Kiselyak Austin and Melissa Skylas

Are computer and web-based data systems important to your business? For almost all companies today the answer clearly is yes. But what is less clear, however, is how to manage computer systems and Internet risk effectively and to insure against potentially catastrophic exposures.

The expanding scope of technology has raised many insurance coverage issues as courts, insurers and policyholders contend with the unique risks posed by computer data and the Internet. It is increasingly doubtful that these risks can be adequately insured under the typical business insurance policy, in light of recent conflicting court decisions regarding insurance coverage for information systems and data and the proposed exclusion of electronic data and software from the standard Comprehensive General Liability (“CGL”) form. In consequence, insurance carriers are developing new products to supplement traditional coverage and cover these exposures.

To manage computer-related risk effectively, it is important to be aware of recent legal developments and the policy changes that carriers are planning for 2002.

Conflicting Court Decisions

Policyholders seeking coverage for destroyed computer data and loss of computer functionality under CGL policies have battled their insurers in court, with mixed results. In a seminal case in April 2000, the U.S. District Court for the District of Arizona held for the policyholder. In *American Guarantee & Liability Ins. Co. v. Ingram Micro, Inc.*,¹ the court found that a temporary power outage that caused the loss of computer data was indeed physical damage, covered under the company’s CGL policy.

Ingram Micro, a wholesale distributor of microcomputer products, relied on a single, worldwide computer network to run its business. In December 1998, Ingram’s data center suf-

fered a power outage that erased all programming information from the random access memory of its computers, requiring them to be manually reprogrammed. When Ingram filed a claim for the resulting business and service interruptions, American denied coverage, asserting that the computer system had not been “physically damaged” because it was still able to perform its intended functions. Ingram’s policy insured against “all risks of direct physical loss or damage from any cause, howsoever or wheresoever occurring” for “real and personal property.” Upon denial of the claim, Ingram filed suit, arguing that its computers had suffered physical damage through their loss of use and functionality. The court agreed, finding that “physical damage” is “not restricted to the physical destruction or harm of computer circuitry but includes loss of access, loss of use, and loss of functionality.”

More recently, however, in *State Auto Property & Casualty Ins. Co. v. Midwest Computers & More*, the U.S. District Court for the Western District of Oklahoma found computer data not to be tangible property and therefore not covered under a business owner’s liability policy.² In a suit against Midwest Computers, a computer sales and service firm, the plaintiffs alleged that Midwest’s negligent computer repair work had deprived them of the use of their computers and destroyed extensive amounts of business information stored on their hard drives. Midwest filed a claim with its insurer, State Auto, who denied coverage and sought a declaratory judgment that its policy did not cover the claim.

The court had to decide whether the computer data allegedly destroyed by Midwest’s acts was “tangible property” under the policy. Upon examining the ordinary meaning of the term “tangible,” the court found it to mean the ability to be “perceived, especially by touch; palpable; capable of being precisely identified or realized by the mind.” The court determined that none of these definitions describes computer data stored on a disk or tape, and found the data to be intangible and not covered by the policy. However, relying on the same

interpretation of the term “tangible,” the court did find that loss of the use of the computers constituted “property damage” under the policy.

Policy Changes on the Horizon

In an effort to reduce the exposure to property insurers, the Insurance Services Office (“ISO”), an industry group that sets underwriting standards for 1,500 property-casualty insurers and agents, is developing several significant changes to the standard forms used by underwriters. These changes would clearly place the risk of data loss and many Internet-related risks outside the coverage grant of traditional policies, forcing businesses that rely on computer technology to cover their exposure by purchasing one of the new policies designed to address technology risks.

In 2002, the ISO plans to add the following clarifying language to the definition of “property damage” in its standard CGL form:

“For the purposes of this insurance, electronic data is not tangible property. As used in this definition electronic data means information, facts or programs stored as or on, created or used on, or transmitted to or from computer software, including systems and applications software, hard or floppy disks, CD-ROMS, tapes, drives, cells, data processing devices or any other media which are used with electronically controlled equipment.”

A similar exclusion is planned for the ISO Building and Personal Property Coverage Form and the ISO Business Income (and Extra Expense) Coverage Form. However, the ISO has drafted coverage extensions that would allow insureds to purchase coverage for the cost of replacing lost or damaged data and for losses resulting from a suspension of operations caused by loss or damage to electronic media and data. The ISO also intends to develop a new “Electronic Data Liability Coverage Form,” which would provide coverage for consequential damage to data arising from an occurrence that causes physical injury to tangible property, but excludes direct damage to data.

In addition, “Electronic Vandalism” and “Denial of Service Attack” exclusions will be added to property policies to exclude coverage for damage caused by intentional alteration of computer media and data, a virus or other malicious code that disrupts the normal operation of computer equipment, or malicious direction of a high volume of inquiries to web site or e-mail destinations that limits legitimate access.

These changes to traditional policies will mean that insureds will no longer be able to rely on them for protection from the potentially large Internet-related loss and defense expense exposures arising from direct damage to the data of others and from claims for the infringement of patented and copyrighted materials.

New Insurance Products

While industry groups are responding to coverage uncertainties with changes to their standard forms, insurance carriers have reacted by generating new specialized policies to fill the gaps. These new products are specifically designed to provide coverage for the risks posed by businesses’ increasing reliance on information systems and the Internet. For example, a number of insurers now offer hacker/virus policies providing both first and third party coverage. Other policies offer broad e-commerce coverage and incorporate errors and omissions and media liability features. Also, endorsements to existing programs are being developed to cover losses related to damaged electronic data, as well as extended coverage for intellectual property infringement.

Many of these new policies contain unique features and requirements, perhaps in response to heightened consciousness about security and the costs of litigation. For example, one new policy that insures against loss of data integrity and system availability requires the insured to provide system backups, change passwords regularly, record log-ins, and install intrusion detection equipment as additional security measures supplementary to coverage.

Some insurers offer a worldwide claim coverage feature, where the policy is explicitly written to cover all possible exposure in cyberspace. Finally, insurers are also marketing abatement coverage, which often includes legal expenses incurred in bringing suits for any third party copyright, patent, and trademark infringement that began during the policy period.

Taking Action

We recommend that businesses address their technology coverage issues by taking the following measures:

- Analyze current insurance policies for possible gaps in coverage with respect to computer, data, or Internet-based losses. Periodically repeat this analysis as part of regular risk management due diligence.

- Consult a risk management or insurance consultant, in addition to the business's regular broker, to determine if specialized policies are needed to protect against computer-related losses (e.g., Business Interruption, Internet Professional Liability, Electronic Errors & Omissions, or Intellectual Property Infringement Protection policies). Policies like these can cover the exposure gaps of standard Comprehensive General Liability policies.
- If a loss is experienced due to computer failure, lost data, denial of service attacks, or Internet-based problems, file a claim under all applicable insurance policies. Even if the insurers deny coverage initially, part or all of the losses may be recovered by pursuing the claims through the judicial process.

At the present time, both the courts and insurance companies are struggling to apply old policy language to the new web-based economy. As technology exposures continue to develop and insurance companies rewrite their policies and create new ones, it is important for companies to be aware of emerging issues and to take measures to minimize potential gaps in insurance coverage. Thus, Internet and technology specific coverage must be part of risk management for computer-dependent businesses to effectively cover their exposure to losses related to critical computer and data assets and Internet activities.

* * * *

The authors wish to thank Jim Lopiccio of Arthur J. Gallagher & Co. for his invaluable assistance with respect to the insurance matters addressed in this memorandum.

¹ CIV 99-185, 2000 U.S. Dist. LEXIS 7299, (D. Az. April 19, 2000).

² 147 F. Supp.2d 1113 (W.D. Ok. 2001).

* * * *

If you have any questions regarding the article, please contact Cathy Kiselyak Austin via telephone at (312) 245-8429 or e-mail at caustin@gcd.com.

TECHNOLOGY / CYBERLAW DEPARTMENT

Cathy Kiselyak Austin (312) 245-8429
caustin@gcd.com

Darren S. Cahr (312) 245-8505
dcahr@gcd.com

Karen A. Erikson (312) 245-8528
kerikson@gcd.com

Edwin A. Getz (312) 245-8475
 [egetz@gcd.com](mailto: egetz@gcd.com)

Philip J. Havers (312) 245-8761
phavers@gcd.com

Michelle A. Kaiser (312) 245-8786
mkaiser@gcd.com

Ira Kalina (312) 245-8590
ikalina@gcd.com

Melissa Skylas (312) 245-8884
mskylas@gcd.com

Liisa M. Thomas (312) 245-8494
lthomas@gcd.com

Priscilla A. Walter (312) 245-8442
pwalter@gcd.com