



**THE RISK  
MANAGEMENT  
LETTER**

This article is excerpted from The Risk Management Letter (ISSN 1070-0102), a publication of Warren, McVeigh & Griffin, Inc., independent risk management consultants.

The Risk Management Letter focuses on important news and information for professionals involved with risk and insurance issues.

Warren, McVeigh & Griffin, Inc.  
1420 Bristol Street North  
Suite 220  
Newport Beach, CA 92660  
Tel 949/752-1058  
Fax 949/955-1929

[www.griffincom.com](http://www.griffincom.com)

©Warren, McVeigh & Griffin, Inc. Reproduction of all or part of The Risk Management Letter may be made only with permission of the publisher.

## **Gaps In Traditional Coverage, Part 1: The Need For Network Security Insurance**

*The loss, destruction, or abstraction of intangible electronic data or data transmission via a network can create potentially crippling exposures to loss for many organizations. Although standard insurance may cover some of the risks of loss, what actually constitutes a loss is not always clear. Numerous other exclusions and limitations can totally eviscerate any coverage an insured thought they might have had. This is the first in a series of articles examining the limitations of conventional insurance policies when it comes to electronic data and what you need to do to protect yourself.*

*Volume 25, Issue 2 (2004)*

**By Paul E. Paray**

Imagine you are buckled in and driving down a country road in a new car armed with anti-lock brakes, head and torso side air bags, load-shifting protection, and a pendulum B-pillar side-impact protection structure. As you usually do, you drive at a reasonable speed and have complied with all state and local driving requirements. Even though you chose the best technology to protect your safety and have complied with all common law and statutory duties, you still get into an accident. Thankfully, insurance will fully protect you, your car, and the truck driver who hit you.

Now imagine you are the senior partner of a large law firm. You head up the committee that voted to adopt the firm's current network security policy. Your security team passed complete background checks. All firewalls and patches are current. Anti-virus definitions are updated daily and servers are monitored 24/7 for security breaches. Notwithstanding these technology safeguards, a disgruntled former employee was still able to circumvent anti-virus protection and download malicious code onto the firm's network and onto the network of certain clients. The code launched confidential information into the public domain and destroyed critical corporate applications, resulting in substantial third-party claims and a first-party loss. Do you have insurance to cover these claims? The answer may surprise you.

Fitting network security risks into traditional insurance coverages is like pushing the proverbial square peg into a round hole. For example, in the above hypothetical, first-party property insurance would likely not cover the claim given that the destroyed data is not "tangible property." Courts have reasoned that the loss of intangible assets such as electronic data, financial information, trade secrets, customer information, and competitive information cannot satisfy the "direct physical loss" requirement. And, because there is no automatic coverage for third-party property, the client's data that was destroyed in this hypothetical would probably not be covered.

The typical commercial general liability (CGL) policy covers only bodily injury and damage to tangible property, not loss of intangible data. As well, although most of the damages resulting from a network security breach are economic in nature, purely economic loss is generally not covered under a CGL policy. Depending on where the law firm's clients were located, there also may be another question as to available coverage. This follows because notwithstanding the fact that a network security risk may be global in nature, a CGL policy's coverage territory generally is limited to North America.

Although courts have been on both sides of the lynchpin "intangible property" issue, the weight of authority has been to interpret property and CGL policies to not cover data and software »

destruction. For example, in *America Online, Inc. v. St. Paul Mercury Insurance Company*,<sup>1</sup> the Court of Appeals for the Fourth Circuit was faced with an insurer that denied coverage because the damages claimed in various class actions did not arise out of “tangible property damage” as defined by the relevant provisions of the applicable policy. The underlying complaints alleged that AOL’s Version 5.0 access software altered the customers’ existing software, disrupted their network connections, caused them loss of stored data, and caused their operating systems to crash. AOL’s main argument was that “because software involves the arrangement of atoms on computer disks, software has a physical property and, on that basis, the complaints’ allegations of damage to software allege ‘physical damage to tangible property.’”<sup>2</sup>

In rejecting AOL’s argument, the Court reasoned that “the conclusion that physical magnetic material on the hard drive is tangible property is quite separate from the question of whether the data, information, and instructions, which are codified in a binary language for storage on the hard drive, are tangible property.” As an illustrative tool, the Court provided the reader with a helpful analogy:

*[W]hen the combination to a combination lock is forgotten or changed, the lock becomes useless, but the lock is not physically damaged. With the retrieval or resetting of the combination—the idea—the lock can be used again. This loss or alteration of the combination may be a useful metaphor for damage to software and data in a computer. With damage to software, whether it be by reconfiguration or loss of instructions, the computer may become inoperable. But the hardware is not damaged.... It is not damage to the physical components of the computer or the lock, i.e., to those components that have “physical substance apparent to the senses.”<sup>3</sup>*

Similarly, in *Ward General Insurance Services, Inc. v. The Employers Fire Insurance Co.*,<sup>4</sup> a California appellate court determined that a first-party property policy did not cover the loss of stored computer data that was not also accompanied by the loss or destruction of the storage medium. The court ruled

plaintiff’s loss of its database, with its consequent economic loss, but with no loss of or damage to tangible property, was not a “direct physical loss of or damage to” covered property.

Those few cases that have held property or CGL coverage exists for loss of data have distinct facts or rely on circular reasoning. For example, in *Lambrecht & Associates, Inc. v. State Farm Lloyds*,<sup>5</sup> the plaintiff sought coverage from State Farm Lloyds for a hacking incident under a business insurance policy. The claim was to recover costs arising out of the loss of computer data and the related loss of business income. In that case, however, the physical damage caused to the computer system required plaintiff to replace its server and purchase a new operating system and other prepackaged

software. Also, in addition to the coverage enumerated in the general provisions of the policy, plaintiff purchased additional valuable papers and records coverage which was stated in an “Extension of Coverage” endorsement to be as follows:

*Valuable Papers and Records. We will pay your expense to research, replace or restore the lost information on valuable papers and records, including those which exist on electronic or magnetic media, for which duplicates do not exist.*

In finding that coverage existed, the court avoided discussing “the physical nature of the data itself and the debate as to whether or not it can be dissolved into a quantitative mass or is entirely transcendental.”<sup>6</sup> Instead, the court focused on the destruction of the very tangible computer server and the language in the Extension of Coverage endorsement.

Given that in the foreseeable future insureds will continue to face legal uncertainty when seeking coverage for a loss of data claim, the most effective means of dealing with such uncertainty is to buy network security insurance. There are a number of insurers offering such specialized coverage and brokers have been busy educating their clients about the differences between these marketed products. Security technologist and author Bruce Schneier said it best: “Sooner or later, the insurance industry will sell everyone anti-hacking policies. It will be unthinkable not to have one. And then we’ll start seeing good security rewarded in the marketplace.”<sup>7</sup> »

**Although courts have been split on the “intangible property” issue, the weight of authority finds that CGL policies do not cover data and software destruction.**

#### NOTES

<sup>1</sup> *America Online, Inc. v. St. Paul Mercury Insurance Company*, 347 F.3d 89 (4th Cir. 2003).

<sup>2</sup> *Id.*


<sup>3</sup> *Id.*

<sup>4</sup> *Ward General Insurance Services, Inc. v. The Employers Fire Insurance Co.*, 114 Cal. App. 4th 548, 7 Cal. Rptr. 3d 844 (Cal. App. 2003).

<sup>5</sup> *Lambrecht & Associates, Inc. v. State Farm Lloyds*, 119 S.W.3d 16 (Tex. App. 2003).

<sup>6</sup> *Id.*

<sup>7</sup> *Information Security*, February 2001. See also *Wall Street Journal*, February 24, 2004, “Despite High-Profile Attacks, Web Security Remains Shaky” (“[I]nsurance can do a lot of good for the security field. It will make management cognizant that if they spend on prevention, they can spend a lot less on the cure.”).

In the way good drivers riding safety-conscious cars are rewarded with both safer roads and lower insurance premiums, the entrance of network security insurance into the marketplace will bring about similar benefits. The actual risk management of network security, including the significance of implementing security practices suggested during the underwriting process, is the subject of the second of this two-part article on network security insurance. 

*Paul E. Paray is the Assistant Regional Underwriting Manager for AIG eBusiness Risk Solutions (AIG eBRS), a unit of the property and casualty insurance subsidiaries of American International Group, Inc. (AIG). He currently manages the New York region for AIG eBRS and can be reached at paul.paray@aig.com. The views expressed in this article by the author are his own and do not necessarily represent those of AIG or any of its subsidiaries, business units, or affiliates.*