My Computer Won't Work: First-Party Insurance Coverage for Cyber Losses

By: Jonathan R. Gross and Victor J. Jacobellis

Introduction

We live in a world where businesses are computer dependent — employees require a computer to perform their jobs; business transactions are conducted via computer systems; and company records, customer information and company work-product are now electronically stored across computer networks instead of in file cabinets. There is no doubt computer technology has improved the way we do business, both internally and with customers. Computer dependency, however, has created a new realm of cyber risks, many of which traditional property insurance, even with a computer coverage endorsement, is not crafted to cover. This article focuses on how courts have applied the coverage afforded under traditional property policies to cyber losses and, to a limited extent, new first-party cyber insurance coverages.

Just What Is a Cyber Loss Anyway?

There is no specific definition of what a "cyber risk" is or what type of loss constitutes a "cyber loss." Generally speaking, a cyber loss can refer to any loss associated with the use of electronic equipment, computers, information technology, or virtual reality. Gregory D. Podolak, *Insurance for Cyber Risks: A Comprehensive Analysis of the Evolving Exposure, Today's Litigation, and Tomorrow's Challenges*, 33 Quinnipiac L. Rev. 369, 371 (2015). The event that often comes to mind when thinking of a cyber loss is a data breach resulting in the theft of company and customer information. An example of a data breach is the 2013 Target data breach that compromised credit card and banking card information for 40 million shoppers and cost Target almost $150 million. Dan Kedmey, *Target Expects $148 Million Loss from Data Breach*, Time, August 6, 2014. These losses are becoming more and more common. As FBI Director Robert Mueller aptly stated, "there are only two types of companies, those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again." Roberta D. Anderson, *Viruses, Trojans, and Spyware, Oh My! The Yellowbrick Road to Coverage in the Land of Internet Oz*, Tort and Trial Practice Law Journal (49:2), Winter 2014, p. 535.

A data breach is not the only cyber event a company is at risk of suffering. Other events that can cause a cyber loss include the injection of a virus into a computer network, loss of electronic data or disruption in the operation of computer systems. Often times the occurrence of one cyber event can lead to another cyber event. For example, the injection of a virus into a computer can trigger the loss of data or disrupt an entire network's operation. The losses and expenses associated with such events can include the cost to replace hardware, the cost to replace software and data, the loss of business income that occurs while a computer network is not operating, and extra expenses incurred to return the business to normal operation as quickly as possible.

When a cyber loss occurs, business income losses and extra expenses incurred can far outweigh the cost to repair or replace physically damaged property. An example of this is a law firm that experiences the failure of a hard drive server resulting in the loss of access to the computer network for a few days. The cost to replace the damaged hard drive may only be $1,500; this is a minor expense in comparison to the loss of billable hours.

Cyber Losses Under a Traditional Property Policy: Fitting the Square Peg into a Round Hole

The risks related to a modern day cyber loss did not exist when property insurance was first being developed. In late seventeenth century London, merchants, bankers, and ship owners gathered in a coffee house owned by Mr. Edward Lloyd where they agreed to share the risks of marine ventures among themselves. 2 Admiralty & Mar. Law § 19-1 (5th ed.). It was from the risks of the sea and the need for protection to owners of ships and cargoes that marine, and eventually property, insurance was born. *Unkelsbee v. Homestead Fire Ins. Co. of Baltimore,* 41

A.2d 168, 170-71 (D.C. 1945). Early marine policies insured against extraordinary and unusual perils that vessels did not reasonably expect to encounter such as shipwreck, foundering, stranding, collision, and damage resulting from violent wind and waves or damage from heavy weather. Am. Jur. 2d, Insurance § 641. Accordingly, in order to recover under insurance, actual tangible property was required to have been damaged or lost. Marine insurance policies did not contemplate insuring against the loss of information.

These types of marine losses became the basis for how coverage is provided in a typical modern day property insurance policy. A typical first-party property policy states an insurer "will pay for direct physical loss of or damage to Covered Property at the premises described in the Declarations caused by or resulting from any Covered Cause of Loss." Businessowners Coverage Form, Miller's Standard Insurance Policies Annotated, ¶ 1-1A1 (7 Ed. 2013). In order to recover for a business income loss, "the suspension [of business operations] must be caused by direct physical loss of or damage to property." Businessowners Coverage Form, Miller's Standard Insurance Policies Annotated, ¶ 1A5f1b (7 Ed. 2013). Under extra expense coverage, the extra expense "must be caused by or result from a Covered Cause of Loss." Businessowners Coverage Form, Miller's Standard Insurance Policies Annotated, ¶ 1A5g1a (7 Ed. 2013).

When it comes to cyber losses under a traditional property policy, the threshold question is whether physical loss or damage has occurred. For example, is electronically stored data property that can be physically lost or damaged? Is there direct physical loss or damage when a computer virus causes electronic data to be lost, but there is no actual physical damage to any computer, server or equipment, *i.e.*, is lost data alone a physical loss? Or, what if there is a power surge that causes an online retailer's computer network to turn off for three hours resulting in millions of dollars in lost sales, even though there is no actual physical damage to a computer system and its components? Different courts have answered these questions in different ways. The majority of courts have required that there be damage to a tangible component of a computer or network in order for there to be coverage. Other courts have broadly construed the term "physical loss and damage" to encompass the loss of use of a computer or data.

Cases Narrowly Construing "Physical Loss and Damage" to Apply Only to Tangible Property

Some courts, when analyzing coverage for "physical loss or damages," have required that there be physical damage to a tangible item. One of the first cases to analyze this issue was *America Online, Inc. v. St. Paul Mercury Ins. Co.*, 347 F.3d 89 (4th Cir. 2003). Although this case involved a general liability policy, the court analyzed whether electronic data was tangible property and whether the loss of use of a computer, in and of itself, constituted damage to tangible property. This matter was a class action lawsuit against America Online ("AOL") where the plaintiffs claimed the installation of AOL software altered existing software on plaintiffs' computers, disrupted the plaintiffs' computer network connections, caused the loss of stored data on the plaintiffs' computers and caused plaintiffs' computer operating systems to crash. *Id.* at 91-92.

AOL argued there was physical damage to tangible property because computer software involves the arrangement of atoms on computer drives and, therefore, software has a physical property. *Id.* at 92. St. Paul, on the other hand, asserted computer software and data are not tangible property because software and data are nothing more than ideas that happen to be stored in electronic form. *Id.* The court sided with St. Paul. In doing so, it first noted that a computer drive, which is a physical magnetic medium to store information, is separate from the data, software, programming information and instructions stored on the computer drive. The court, taking a technical approach, found that "data, information and instructions used in a computer are codified into a binary language and the binary language is processed by the computer." "Thus, if a hard drive were physically scarred or scratched so that it could no longer properly record data, information or instructions, then the damage would be physical, affecting the medium for storage of the data. But if the arrangement of the data or information stored on the hard drive were to become disordered or the instructions were to come into conflict with each other, the physical capabilities and properties of the hard drive would not be affected. Such disordering or conflicting instructions would amount to damage to the data and information and to the instructions (*i.e.*, the software) but not to the hard drive." *Id.* at 95.

By analogy, the court reasoned, "when the combination to a combination lock is forgotten or changed, the lock becomes useless, but the lock is not physically damaged. With the retrieval of or resetting the combination—the idea—the lock can be used again…. With damage to software, whether it be by reconfiguration or loss of instructions, the computer may become inoperable. But the hardware is not damaged. The switches continue to function to receive instructions and the data and information developed on the computer can still be preserved on the hard drive. While the loss of the idea represented by the *configuration* of the computer switches or the *combination* for the lock might amount to damage, such damage is intangible property. It is not the damage to the physical components of the computer or lock, *i.e.*, to those components that have 'physical substance apparent to the senses.'" *Id.* at 96.

In *Eyeblaster, Inc. v. Federal Ins. Co.*, 613 F.3d 797 (8th Cir. 2009), the court took a similar approach in narrowly construing what constituted physical loss and damage. Like *AOL*, this case also involved a liability policy, but the focus was the insurance policy's coverage for "physical injury to tangible property." Eyeblaster provided online advertising services. The plaintiff filed suit against Eyeblaster alleging an Eyeblaster spyware program caused his computer to freeze up, caused data pertaining to his unfinished tax returns to disappear, caused pop-up ads to appear, hijacked his web browser's communication with web sites, slowed his computer's performance and caused his computer to crash. *Id.* at 799-800. One of the issues before the court was whether the plaintiff's complaint contained any allegations for damage to tangible property. The court, relying on *AOL*, held the claimed damage, *i.e.*, the operation of plaintiff's computer, did not constitute "physical damage to tangible property" and damage to the computer's hardware was required to trigger coverage.

The leading first-party property case is *Ward General Ins. Servs., Inc. v. Employers Fire Ins. Co.*, 114 Cal. App. 4th 548 (2003), involving a claim for data loss under a traditional property policy. The *Ward* court also took a narrow approach in determining if electronic data constitutes tangible property. In this case, human error caused the insured's computer database to crash, resulting in the loss of data necessary for business operations. The crash did not cause any damage to the hardware on which lost data was stored. The insured spent over $50,000 to restore the lost information, suffered a business income loss of over $200,000, and submitted a claim under its businessowners policy for these costs. *Id.* at 550-51.

The *Ward* court considered whether electronic data was tangible property, and the sole issue before the court was whether the loss of electronically stored data, when there is no accompanying damage to any tangible parts of the computer system, constituted direct physical loss or damage. In order to answer this question, the court examined the plain and ordinary meaning of the word "physical," defined as "having material existence" and "perceptible especially through the senses and subject to the law of nature." The court then looked to the definition of material, defined as "capable of being perceived especially by the sense of touch." On the basis of these definitions, the court said "with confidence that the loss of the [insured's] database does not qualify as 'direct physical loss,' *unless* the database has material existence, formed out of tangible matter, and is perceptible to the sense of touch."

The court then examined the nature of a database. It defined "data" as "factual or numerical 'information'" and "database" as a large collection of organized data and concluded the "loss of a database is the loss of organized information." *Id.* at 556.

The court's conclusion, based on this analysis, was that there was no loss of or damage to physical property and, therefore, no "direct physical loss of or damage to" covered property. In coming to its decision, the court reasoned that it failed to see how "data" or "information" can have a material existence, be formed out of tangible matter, or be perceptible to the sense of touch. And although data is stored on a physical medium, *e.g.*, a magnetic disc or tape, the information itself is intangible. Even though the insured lost stored information, it did not lose the tangible material of the storage medium, which was still capable of storing information. *Id.*

Metro Brokers, Inc. v. Transportation Ins. Co. (No. 1:12-CV-3010-0DE) 2013 WL 7117840 (N.D. Ga. Nov. 21, 2013), demonstrates a creative, yet unsuccessful, argument through which an insured sought coverage for a cyber loss involving a fraudulent electronic transfer of money. In this case, Metro Brokers had money stolen when thieves logged onto its bank account and used the bank's Automated Clearing House System ("ACH") to make payments from Metro's bank account. Metro submitted a claim for the money stolen through ACH payments under its business property policy's "Forgery and Alteration" coverage. Under this coverage, the insurer agreed to pay for any loss resulting from forgery in any check, draft, promissory note, bill of exchange, or similar written promise to pay money by anyone acting as you or your agent. The coverage included the forgery of an electronic signature. *Id.* at *2. Metro claimed there was coverage because its electronic signature was forged to make the ACH payment. *Id.* at *3. Although Metro's claim was inventive, the court nonetheless found there was no coverage because the forgery and alteration coverage clearly applied only to losses pertaining to promises to pay contained on written instruments, making the ACH payment outside the scope of coverage. *Id.* at *5.

Cases Broadly Construing Data Loss and the Loss of Computer Use as "Physical Loss and Damage"

Some courts have broadly construed what constitutes physical loss and damage when a cyber loss occurs to find coverage under a traditional property insurance policy. One of the first cases finding coverage for a cyber loss under a traditional property policy is the unpublished, but often cited, case, *American Guarantee & Liability Ins. Co. v Ingram Micro, Inc.* (No. 99-185 TUC ACM) 2000 WL 726789 (D. Ariz. April 18, 2000). In this case, the court did not focus on whether or not information stored on a computer was tangible property. Instead, this court found "physical loss and damage" was not restricted to the physical destruction or harm to computer circuitry. The court chose to broadly define "physical loss and damage" to include loss of access, loss of use and loss of functionality to computer systems when stored information on a computer was lost. In this case, the insured, Ingram Micro, was a wholesale distributor of microcomputer products. All of Ingram Micro's sales were processed through a computer network known as Impulse. *Id* at *1. A power outage caused all of Impulse's programming information to be erased, causing Impulse to became inoperable and all of Ingram Micro's computers to not function for eight hours. *Id.* at *1-2.

Ingram Micro made a claim for business income losses caused by the power outage under an American Guarantee business property policy. The only issue before the court was whether the power outage caused direct physical loss or damage to Ingram Micro's computer system. *Id.* at *1. American Guarantee admitted the power outage affected Impulse's ability to function. American Guarantee argued, however, Ingram Micro's computer system was not "physically damaged" because the system's ability to function remained intact and was still able to receive the input of programming information that had been erased, which allowed the system to operate properly again. Ingram Micro, on the other hand, argued "physical damage" includes loss of use and functionality and, therefore, the fact the computer system could accept information and eventually operated as the system did before the loss did not mean the computer system had not been "physically damaged."

The court sided with Ingram Micro's broader definition of "physical damage." *Id.* at *2. The court concluded the loss of use and functionality of the computer system in and of itself constituted "physical damage." It based this conclusion upon an examination of the U.S. and several states' penal codes addressing cybercrimes. The court held that penal codes'

relevance was significant because law makers around the country have determined that when a computer's data is unavailable, there is damage; and when a computer's software or network is altered, there is damage. The court found that restricting coverage to actual "physical damage" to the computer system components, as American Guarantee suggested, would be archaic. *Id.* at *3.

In *Southeast Mental Health Center, Inc. v. Pacific Ins. Co., Ltd.*, 439 F. Supp. 2d 831 (W.D. Tenn. 2006), it was found, under the principles of *Ingram Micro*, that the loss of computer data constituted physical damage under a business property policy. In this case, a storm caused Southeast Mental Health Center, the insured, to lose power causing a data loss. *Southeast Mental Health Center*, 439 F. Supp. 2d at 834-35. The insured subsequently submitted a claim for the recovery of the lost data, which was denied on the basis that the data loss did not constitute "physical loss and damage" because the actual computer on which the data loss occurred was not damaged. The court, citing *Ingram Micro*, found the data loss was "physical loss and damage" because the lost data affected the computer system's ability to operate. *Id.* at 837-38.

Coverage for a cyber loss was more recently considered in another unpublished case, *Landmark American Inc. Co. v. Gulf Coast Analytical Labs., Inc.* (No. 10-809) 2012 WL 1094761 (M.D. La. March 30, 2012). This case specifically addressed whether electronic data is physical, *i.e.,* tangible property, or nonphysical in nature, *i.e.*, not tangible property, and, therefore, whether the loss of electronic data constituted "physical loss and damage." *Id.* at *3. The insured, Gulf Coast, suffered a computer server failure that caused its electronic data to be corrupted and permanently unusable. The data loss caused Gulf Coast to lose over $1 million in business income and it expended over $100,000 to recover the data. Gulf Coast submitted a claim to Landmark for the losses and Landmark claimed electronic data is not tangible property and, hence, not susceptible to physical loss and damage. Landmark further argued that electronic data can be subject to coverage only if the associated hardware is damaged and causes a loss of electronic data. Gulf Coast, on the other hand, argued electronic data was physical in nature because data was physically disrupted when the computer server failed. *Id.* at *1.

The court sided with Gulf Coast and held electronic data was physical in nature and the loss of electronic data constituted physical loss and damage under the insurance policy. Applying Louisiana law, the court noted tangibility is not a defining feature of physicality. The court reasoned that although electronic data is not tangible, it is still physical because it can be observed and altered through human action. It further found Gulf Coast's electronic data "has physical existence, takes up space on the tape, disc or hard drive, makes physical things happen, and can be perceived by the senses." *Id.* at *4.

Coverage Under a Cyber Policy

In order to meet the demand for protection from a cyber loss, insurance companies have added a variety of coverage extensions for cyber risks to their existing business property policies and have begun to create new specialty cyber insurance policies designed to address these risks. This is still a new and developing area of coverage and there is no typical cyber risk policy. Some policies extend coverage to the loss of data or software from different specified causes of loss. Such policies often also offer coverage for the loss of business income from a cyber loss and the expenses incurred to restore lost data. 2 Computer Software § 9:49 (West 2015). Policies may also provide coverage for losses associated with a data breach, including: (1) the cost to investigate forensically a data privacy or cybersecurity incident; (2) attorney costs for the review and determination of whether data privacy laws were violated; (3) the cost to send letters notifying customers or at risk individuals about a data breach, incident in accordance with statutes and regulations; (4) the cost of credit or fraud monitoring for affected individuals; and (5) the cost of complying with a regulatory investigation in connection with a data privacy incident. Scott Godes, *Managing Cybersecurity Risks in the Ever-Changing Cyber Insurance Law Environment*, Understanding Developments in Cyberspace Law, 2015 Edition, Leading Lawyers on Analyzing Recent Trends, Case Laws, and Legal Strategies Affecting the Internet Landscape, August 2015, at 1. There is also a wide range of coverage that may be provided under a cyber loss policy and the terms and conditions in such a policy may often vary from insurer to insurer and may even vary in different policies issued by the same insurer.

Since cyber coverages are relatively new, there are only a limited number of cases addressing them. The case law concerning cyber policies and the courts' opinions, consequently, are reflective of the specific policy language concerning coverage and the application of the policy to the facts. This is a good reminder that most evaluations of coverage under a cyber policy should focus on the policy at issue and the facts of the loss.

Retail Ventures, Inc. v. National Union Fire Ins. Co. of Pittsburgh, Pa., 691 F.3d 821 (6th Cir. 2012), involved a claim made under a special coverage entitled "Computer & Funds Transfer Coverage." This coverage protected against any loss resulting from the theft of any insured property by computer fraud. Computer fraud included the act of wrongfully converting assets through a computer system and insured property included the theft of property held by the insured in any capacity. *Id.* at 827. This coverage contained an exclusion for any loss of proprietary information, trade secrets, confidential processing methods, or other confidential information of any kind. *Id.* at 832. The insured, which operated retail shoe stores, DSW, had a data breach by hackers who accessed DSW's computers and downloaded credit card and checking account information of more than 1.4 million DSW customers. DSW made a claim under its "Computer & Funds Transfer Coverage" for investigative costs it incurred in connection with the data breach and amounts it reimbursed customers for fraudulent transfers made with their financial information. *Id*.

The parties agreed the data breach was theft of insured property under the "Computer & Funds Transfer Coverage." The insurer, however, claimed there was no coverage for the loss under the policy's exclusion for loss of proprietary information, trade secrets, confidential processing methods, or other confidential information of any kind. *Id.* at 832. The court disagreed and found the exclusion did not apply and there was coverage. The court first found customer information was not proprietary since the information was held by the customers' financial institutions and because the customers provided their financial information to merchants. It further held the customers' financial information was neither a "trade secret," found to mean information used in the insured's business, nor a "confidential processing method," found to mean a secret process or technique used in the insured's business. Finally, the court held the catchall phrase "other confidential information of any kind" could only refer to the insured's own confidential information because it was part of a sequence pertaining to the insured's secret information and not the secret information of the insured's customers. *Id.* at 833-34.

In *Lambrecht & Assoc., Inc. v. State Farm Lloyds*, 119 S.W.3d 16 (Tex. App. 2003), the insured was found to have coverage under its policy for its business income loss and extra expense the insured incurred after a virus shut its computer systems down and damaged its software and data. The policy specifically stated it would pay for accidental direct physical loss to electronic media and records, defined to include storage media, electronic data, storage media and the data stored on such media. *Id.* at 25. State Farm Lloyds argued the injection of the virus was not accidental and there was no coverage for the damages that resulted from the virus. The court disagreed and held the injection of the virus and the resulting damage was an unexpected and unusual occurrence and was, from the insured's view, unexpected. *Id.* at 21. State Farm also contended that an exclusion pertaining to electronic data losses caused by an error in programming applied to losses caused by the virus, but the court held the injection of a virus was not an error in programming. *Id.* at 25.

Conclusion

The advancement of cyber risks and policy forms to address those risks are still in the early stages of development. How the courts will address cyber loss coverage disputes will likely be on a case by case basis according to the specific facts of the loss and the particular language of the applicable insurance policy.

Mr. Gross is the managing partner of, and **Mr. Jacobellis** special counsel in, the California office of the firm.

This article accompanied a presentation Mr. Gross gave at the Defense Research Institute's "Insurance Coverage and Claims Institute Seminar" on April 7, 2016 in Chicago.