KAUFMAN DOLOWICH VOLUCK
www.kdvlaw.com

Business Interruption Claims for Cyber-Related Losses

Authors:

Avery A. Dial, *Partner*
Co-Chair, Data Privacy & Cybersecurity Practice Group

Eric B. Stern, *Partner*
Co-Chair, Data Privacy & Cybersecurity Practice Group

May 18, 2020

KAUFMAN DOLOWICH VOLUCK

ATTORNEYS AT LAW

Business Interruption Claims for Cyber-Related Losses

Property Insurance Policy

Typically, the standard Commercial Property Policy form provides coverage for "actual loss of Business Income" sustained due to the "necessary suspension of your operations during the period of restoration," and suspension of operations must be caused by "direct physical loss of or damage to property."

Courts have reached different conclusions on whether cyber-losses constitute "physical loss." Some courts have held that "physical damage" is not limited to physical destruction or harm but rather also includes "lack of access, loss of use, and loss of functionality." *Am. Guarantee v. Ingram*, 2000 U.S. Dist. LEXIS 7299 (D. Ariz. 2000); *NMS Services, Inc. v. The Hartford*, 62 Fed. Appx. 511 (4th Cir. 2003) (Court held that there was coverage under a business property policy for an insured's loss of business and costs to restore records lost when a former employee hacked into the insured's network); *Southeast Mental Health Center Inc. v. Pacific Ins. Co. Ltd.,* 439 F. Supp. 2d 831 (W.D. Tenn. 2006) (Insured proved necessary direct physical loss where the insured's pharmacy computer data was corrupted due to a power outage).

Further, some courts have held that a policy that covers only physical damage to property would not cover the loss of critical data inadvertently wiped out because the lost information was not tangible. *Ward General v. Employers Fire,* 7 Cal. Rptr. 3d 844 (Cal. Ct. App. 2003); *Am. Online v. St. Paul Mercury Ins.*, 207 F. Supp. 2d 459 (E. D. Va. 2002) (Court held that CGL Policy did not cover costs to defend AOL against lawsuits alleging that AOL software damaged customers' computers because such lawsuits did not involve "physical damage" to "tangible property"); *Seagate v. St. Paul Fire,* 11 F. Supp. 2d 1150 (N.D. Ca. 1998) (Insured sought coverage under a CGL policy for lawsuit based on damage to consumer's computer data caused by defective disk drives sold by the insured. Court held that there was no coverage because the alleged damage to data was not physical damage to tangible property).

In *State Auto Property & Casualty Insurance Co. v. Midwest Computers & More,* 147 F. Supp. 2d 1113 (W.D. Okla. 2001), the court held that damage to "tangible property" had occurred under the terms of the policy because "a computer is clearly tangible property." Id. at 1116.However, the subject policy's "your work" exclusion applied to bar coverage for the claims.

Of course, specific policy language will create different outcomes. For example, in *National Ink and Stitch, LLC v. State Auto Property and Casualty Insurance Co.*, 2020 WL 374460 (D. MD. 2020) the subject policy contained an endorsement that expressly included data and software as covered property. Accordingly, the court found coverage based upon "physical loss" being decreased functionality of the computer system and "software" and "data" being defined as covered property.

If there is physical damage caused as part of the cyber-loss, then there is probably coverage. However, absent real-world physical damage, whether there is coverage is left up to the court's interpretation of the policy to overlook or broadly interpret the "tangible property" requirement.

As related to the potential impact of the Covid-19 related losses – although there is no factual basis, at this point, to support an argument that cyber-related business interruption was caused primarily by the pandemic – there is a split in jurisdictions, as discussed above, about whether the loss qualifies as a covered business interruption loss absent tangible physical damage to the system.

Coverage For Cyber-Loss Due To The Increase Of Employees Working from Home

The largest risk caused by the Covid-19 pandemic is the risk caused by insured-employees working from home in significantly larger numbers than any insurer or insured could have anticipated when issuing or setting a premium for a cyber-policy.

The central language in a policy that will likely control coverage for a cyber-loss suffered by the insured due to an intrusion into the employee's computer or system is the policy's definition of a covered "computer system."

Most policies' definition of "computer system" includes electronic, wireless, web, or similar systems used to process and store "data" or information. However, as it relates to coverage for computer systems at an employee's home, policies differ, in relevant part, in the scope of the coverage based on the connectivity between Named Insured and the personal system.

The greater the level of ownership and control over the system used at insured-employee's home, the more likely that coverage for an intrusion would apply. Issues regarding the place of entry into the system for the intrusion and the Named Insured's ownership, operation and control of such place of entry, and the specific policy language will determine whether there is coverage for an at home date-intrusion.

Many policies will also contain exclusions for a lack of proper security or an insured's failure to adhere to protections contained in the insured's application for coverage. To the extent such an exclusion exists on a cyber-policy it is important for insureds to review the security at their employee's home and remind employees of the steps that need to be taken to properly secure their system.

KAUFMAN DOLOWICH VOLUCK
ATTORNEYS AT LAW

Cyber policies may also limit coverage to intrusions into the insured's programs and systems. To that end, an employee working at home may use the insured-owned hardware and systems for personal purposes. To the extent an intrusion is made through a program or system that allows access to the insured's data, coverage for such an event may be excluded.

There are a host of different coverages and scenarios that may be contemplated as a result of Covid-19. Insureds and insurers should review their policies and claims must be analyzed on a case-by-case basis. .

Stand-Alone Cyber-Policy

Unlike Commercial General Liability or Commercial Property Policies, each Cyber Liability Insurance Policy differs and there is no standard form. Therefore, every "cyber" policy form is unique and deserving of a careful review. However, regardless of the form, an insured must still prove that there was a covered cause of loss and further, link the cyber event to the claimed business interruption.

Cyber events increasingly cause business interruption loss across all lines of industries – including manufacturers, construction companies, banks, and health care providers. Indeed, business Interruption loss does not have to result from a "hack" or social engineering, it may result from routine technical failures or human error.

Coverage triggers for business interruption are not uniform across cyber policies. The first element to determining coverage is identifying the alleged cause of the cyber-interruption. As we analyze Covid-19-related business interruption, insureds and insurers need to be aware of triggers that may occur as a result of the Covid-19-shutdown, such as whether coverage is triggered by non-malicious acts or other governmental acts.

As it impacts Covid-19-related losses, although there is no factual reason to believe that there is cyber-related business interruption caused primarily by the pandemic, to the extent the insured can draw a causative link between the forced shut-down of businesses and a cyber-event to cause business interruption, insureds and insurers should review their specific policy to see if such event is covered.

About Kaufman Dolowich & Voluck LLP

KDV is a nationally recognized, AV-rated® law firm serving the business community in a number of practice areas. Originally founded over 33 years ago as a boutique labor and employment law firm, KDV has established a strong reputation in areas of commercial litigation, directors and officers liability (D&O), all matters involving financial institutions, professional liability coverage and defense, and insurance coverage and litigation. The firm's attorneys are seasoned legal practitioners and litigators who place clients first, think like business people, and provide viable, innovative solutions.

Mansfield Rule™ Certified 2019 Powered by DIVERSITYLAB

Offices

NEW YORK

Woodbury (Long Island)
135 Crossways Park Drive, Suite 201
Woodbury, NY 11797-2005
Tel: (516) 681-1100
Fax: (516) 681-1101

New York City
40 Exchange Place, 20th Floor
New York, NY 10005
Tel: (212) 485-9600
Fax: (212) 485-9700

NEW JERSEY

Hackensack
25 Main Street, Suite 500
Hackensack, NJ 07601
Tel: (201) 488-6655
Fax: (201) 488-6652

PENNSYLVANIA

Blue Bell (Philadelphia Metro)
1777 Sentry Parkway West
VEVA 17, Suite 100
Blue Bell, PA 19422-2227
Tel: (215) 461-1100
Fax: (215) 461-1300

Philadelphia
Four Penn Center
1600 John F. Kennedy Blvd., Ste 1030
Philadephia, PA 19103
Tel: (215) 501-7002
Fax: (215) 405-2973

FLORIDA

Fort Lauderdale
One Financial Plaza
100 SE 3rd Avenue, Suite 1500
Ft. Lauderdale, FL 33394
Tel: (954) 712-7442
Fax: (888) 464-7982

Orlando
301 E. Pine Street, Suite 840
Orlando, FL 32801
Tel: (407) 789-0230
Fax: (888) 502-6353

ILLINOIS

Chicago
135 So. LaSalle St., Suite 2100
Chicago, IL 60603
Tel: (312) 759-1400, (312) 646-6744
Fax: (312) 759-0402

CALIFORNIA

Los Angeles
11755 Wilshire Blvd., Suite 2400
Los Angeles, CA 90025-1519
Tel: (310) 775-6511
Fax: (310) 575-9720

San Francisco
425 California Street, Suite 2100
San Francisco, CA 94104-2206
Tel: (415) 926-7600
Fax: (415) 926-7601

Sonoma
193 Sonoma Highway, Suite 100
Sonoma, CA 95476
Tel: (707) 509-5260
Fax: (707) 509-5261