2019 Annual Conference
March 13 -15 2019
Orlando, FL

Cyber Coverage Under Non-Cyber Policies: Cases, Wordings and Predictions

I. Why non-cyber policies will be pursued in cyber claims

A. Most American businesses lack cyber insurance

Recent statistics indicate that only 33% of domestic businesses carry cyber insurance and that up to 67% of small and mid-sized businesses in the United States are not even aware that cyber insurance exists. Many companies cite the confusing nature of cyber coverage as the primary reason that they choose to forgo purchasing cyber insurance. To further complicate matters, a large number of applications for cyber policies are rejected by underwriters due to the applicant's inadequate cyber security testing and audit procedures and the applicant's inadequate cyber incident response plan. As a result, a large portion of American businesses lack cyber insurance coverage.

B. Coverage under cyber policies varies greatly

Cyber policies are not written on standard forms and the coverages provided among various insurers has varied widely. Upwards of 50 insurers now offer cyber coverages under multiple products and with varying sublimit. Moreover, coverages are changing on a regular basis due to the evolving nature of cyber-attacks and the constant advancement of technology. Despite these facts, typical coverages under cyber policies include both first-party and third-party coverage for such items as data breaches, unauthorized disclosure of personal identifying information, notification of affected parties, cyber extortion, data loss or destruction, and electronic media liability.

C. Losses from cyber events can be significant

Losses for a cyber even can be extraordinary, often exceeding the available limits of any given cyber policy. For example, the Ponemon Institute's 2017 Cost of Data study found that organizations took, on average, 191 days to identify a data breach**.** The same

study found that the average total cost of a data breach was $3.62 million. A large portion of the cost of any data breach is the lost productivity of employees while IT systems are down. Moreover, the reputational damage to any business can be significant.

II. Non-cyber coverages which are looked to for cyber coverage

A. Commercial General Liability Policies

Commercial general liability policies are the most commonly available coverage for American small to mid-sized businesses. As a result, in the event of a cyber loss, many insureds seek to recover all, or a portion of their loss, under commercial general lability policies. While coverage under commercial general liability policies is highly dependent of the facts of each case, a number of cases turn on whether a loss was "physical damage to tangible property" and, thereby, met the definition of property damage.

Other cases have involved an analysis of whether there is coverage under a commercial general liability policy's coverage grant for personal (or reputational) injury. These cases often turn on whether the policyholder can establish that there was "publication" of material that violated a person's right to privacy.

Even if a cyber claim is potentially covered under a commercial general liability policy, many first-party losses will probably not be covered. These losses can include IT forensic costs, customer notification costs, and business interruption losses. Furthermore, many commercial general liability carriers are adding exclusions to specifically eliminate coverage for cyber losses.

B. Professional Liability/E&O Coverages

Non-standard wordings and less common guiding case authority can give maneuvering room to businesses seeking coverage. Employee dishonesty coverage in these policies may give coverage for intentional acts, such as some cyber acts. In addition, a defense obligation might attach in employee dishonesty coverages, where a final adjudication of dishonest acts is sometimes required to void coverage. These provisions might require an insurer to defend a cyber claim through trial, even if indemnity coverage does not attach.

Claims for coverage for cyber losses under errors and omissions policies are much less common than under commercial general liability policies. Like commercial general liability policies, however, errors and omissions policies will typically only provide coverage, if any, for third-party liability and not first-party losses. Cases will often analyze whether the underlying complaint has alleged a "wrongful act" on the

part of the policyholder as insurers will often argue that the relevant wrongful conduct was intentional.

C. Crime Policies

A number of courts have found coverage for cyber claims under commercial crime policies. As cyber-attacks are often intentional acts done for criminal gain, there is often an argument that a commercial crime policy will cover all, or a portion of, a loss for a cyber-attack. Cases analyzing coverage under a crime policy often focus on whether human error or computer fraud caused the policyholder's loss. These cases often focus on policy language requiring that the loss result "directly from the fraud." For example, courts have evaluated (and often found) coverage under crime policies for cases in which the policyholder incurred losses resulting from fraudulent transaction instructions. These cases look at whether the loss was incurred due to the use of a computer or due to human dishonesty and error.

D. Property Policies

Another fertile source of coverage for cyber claims under non-cyber policies are first-party property policies. Like the policies discussed about, coverage under property policies often turns on whether the cyber loss triggers the policies insuring agreement. With property policies, that debate often leads to an evaluation of whether the damage to the policyholder constituted "direct physical loss or damage." In a number of cases, courts have examined whether electronic data is "physical." In very general terms, courts have found that electronic data has a physical existence, in that it takes up space on hard drives. Other courts have found that, because computers can be reprogrammed with new data, no loss occurred.

III. Suggested Cases where coverage is sought, and sometimes found

Cyber claims are not going to go away and small to mid-sized businesses are not likely to begin purchasing cyber policies in large quantities. As a result, claims for cyber losses under non-cyber policies will be prevalent. While insurers will likely continue to add exclusions and narrow policy language to avoid covering cyber losses under traditional policy coverages, the law of unintended consequences may result in policyholders finding coverage for cyber losses where coverage was not intended to exist. For example, "advertising injury" coverage was first added to commercial general liability policies in 1973, almost a decade before the advent of the internet. Yet, policyholders have successfully triggered coverage for cyber losses under advertising injury coverage grants. Cyber claims may evolve faster than insurance wordings intended to address them.

A. Commercial General Liability (CGL):

Eyeblaster, Inc. v. Federal Ins. Co., 613 F.2d 797, 802 (8th Cir. 2010); Insured's loss of ability to use its computer system after hack was property damage under standard form GL policy.

Ciber, Inc. v. Federal Ins. Co., 2018 W.L. 1203157 U.S.D.C. (Colorado 2018); *Eyeblaster* distinguished; software system which worked improperly did not constitute property damage under CGL policy, because computer system itself was not rendered non-functional.

B. Crime:

Interactive Communications Int'l, Inc. v. Great American Ins. Co., 731 Fed. Appx. 929 (11th Cir. 2018); scam involving multiple redemptions of chips loaded on debit cards held not covered within the meaning of computer fraud policy, as loss did not result "directly from the fraud".

C. Errors and Omissions:

Doctor's Direct Ins. Inc. v. Bochenek, 38 N.E.2d 116 (App. – Illinois 2015); alleged violation of Telephone Consumer Protection Act by sending unsolicited text cosmetic surgery advertisements to cell phones were not "privacy wrongful acts", within meaning of cyber claims endorsement to professional liability policy.

D. Commercial Crime:

Principle Solutions Group, LLC v. Ironshore Indemnity, Inc., 2016 W.L. 4618761 (U.S.D.C. – Georgia 2016); policy language on crime policy provided coverage for loss resulting from fraudulent transaction instructions held ambiguous and construed in insured's favor.

IV. A Cautionary Tale: The government may sue your company for poor cyber security.

FTC v. Wyndham Worldwide Corp., 10 F.Supp.3d 602 (U.S.D.C. – New Jersey 2014); Federal Trade Commission had standing to sue Wyndham for "failure to maintain reasonable and appropriate data security for consumers' sensitive personal information".