ALFA International
THE GLOBAL LEGAL NETWORK

2022 Insurance & Professional Liability Seminar

June 22-24, 2022

THE EVOLUTION OF CYBER COVERAGE

Teresa M. Young
Moderator
BROWN & JAMES, P.C.
St. Louis, Missouri
tyoung@bjpc.com

Alex P. Tilling
LEAKE & ANDERSSON, LLP
New Orleans, Louisiana
atilling@leakeandersson.com

THE EVOUTION OF CYBER COVERAGE

A. A brief history of cyber coverage.

a. Cyber coverage can be traced back to Errors and Omissions (E&O policies) issued to technology companies.

These initial cyber coverages were usually added to E&O policies as "network security" or "internet liability" coverage.

i. 1990s

The earliest cyber liability insurance generally consisted of policies covering online media or errors in data processing. These policies excluded first-party coverage and included exemptions for rogue employees, regulatory claims, and fines and penalties.

ii. 2000s

Insurers expanded cyber coverage to include unauthorized access to systems, network security, destruction or loss of data, and computer viruses. They also began to include first-party coverage for cyber business interruption, extortion, and network asset damage.

iii. 2003

In 2003, California enacted the Security Breach and Information Act. The Act required a California business or state agency to notify any resident whose unencrypted personal information was accessed or acquired by an unauthorized person. Many other states followed suit. As a result, insurers began to offer first-party coverage for IT forensics and information security, public relations, credit monitoring and customer notifications, as well as third-party coverage for regulatory defense and fines and penalties.

b. The landscape of cyber coverage began to change as insurance companies attempted to exclude cyber coverage from their policies.

i. 2001

Until 1996, commercial general liability (CGL) and commercial crime policies included coverage for "computer fraud," which was only available by endorsement. In 2001, the Insurance Services Office, Inc. (ISO) changed the standard policy definition of "property damage" to mean "physical injury to

tangible property," and the phrase "electronic data is not tangible property" was added.[1]

ii. 2014

New cyber exclusions went into effect, excluding damages arising out of access to, or disclosure of Personally Identifying Information (PII) and the "loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data."[2]

B. Cyber coverage today.

a. Current issues in cyber coverage.

i. Risk evaluation

There is little to no historical or actuarial data to evaluate the risk of a cyber attack.

Damages from cyber attacks are often intangible and hard to quantify. For example, a company may suffer a loss of goodwill due to a data breach exposing clients' PII.

ii. Lack of standardization

There is no standard cyber policy form, and therefore, cyber policies are often highly customized.

b. Common cyber risks.[3]

- Identity theft as a result of security breaches.
- Business interruption from unauthorized network access.
- Damage to data records.
- Theft of digital assets, such as customer lists, trade secrets, and other electronic business assets.
- Introduction of malware.

---

[1] Virginia N. Roddy, *Expanding Risks, Growing Market: Cyber Insurance Today*, 59 No. 10 DRI For Def. 80. (2017).
[2] Danielle Gilmore & David Armillei, *The Future is Now: The First Wave of Cyber Insurance Litigation Commences, and the Groundwork is Laid for the Coming Storm, in* INSURANCE LAW 2016: TOP LAWYERS ON TRENDS AND KEY STRATEGIES FOR THE UPCOMING YEAR, 2016 WL 1089828, at *2 (2016).
[3] Roddy, *supra*.

- Human error leading to inadvertent disclosure of sensitive information.
- Cost of credit-monitoring services for those affected by a security breach.
- Lawsuits alleging trademark or copyright infringement.

c. National Association of Insurance Commissioners ("NAIC") has drafted an Insurance Data Security Model Law.

The model law seeks to establish data security standards for regulators and insurers to mitigate the potential damage of a data breach.

To date, the model law had been adopted and has gone into effect in eighteen states. Maryland and Kentucky also recently adopted the law, and it will go into effect in both states by next year.

C. Obtaining cyber coverage under non-cyber policies.

a. Silent Cyber

"Silent cyber" coverage is potential cyber exposure under traditional property and liability insurance policies which are not expressly covered or excluded

b. Issues in coverage litigation.

i. "Property damage"

Most courts have found that "data" does not constitute "tangible property" within a CGL policy's definition of "property damage."[4]

Some courts have found that stored data that is "magnetically encoded on a segment [] hard disk" constitutes "tangible property" capable of being damaged.[5]

ii. "Personal and advertising injury"

Courts generally agree that a data breach constitutes a violation of a person's "right of privacy" within a CGL policy's definition of "personal and advertising injury."

However, the main issue that is being addressed within the courts is what constitutes "publication."[6] For example, a data breach in which third-party hackers gain access to customers PII may not constitute "publication" because, to

[4] *America Online, Inc. v. St. Paul Mercury Ins. Co.*, 347 F.3d 89 (4th Cir. 2003).
[5] *See London-Sire Records, Inc. v. John Doe*, 542 F.Supp.2d 153 (D. Mass. 2008); *see also Capitol Records, LLC v. ReDigi, Inc.*, 934 F.Supp.2d 640 (S.D.N.Y. 2013); *NMS Servs. Inc. v. The Hartford*, 62 F. App'x 511 (4th Cir. 2002).
[6] *See Innovak Int'l, Inc. v. Hanover Ins. Co.*, 280 F. Supp. 3d 1340 (M.D. Fla. 2017).

the extent the information is actually "published" and not just accessed by the third party, the publication must be made by the insured itself rather than by the third party.