Managing Cyber Risks

Insurance Coverage Issues Relating to Cyber Security Exposures

Thomas G. Drennan, Partner

(312) 428-2728

tom.drennan@dinsmore.com

September 15, 2016

Outline:

- Types of Cyber Risks
- Insurance Coverage Issues Under “Traditional” Policies
- Insurance Coverage Issues Under “Cyber Risk” Policies

Types of Cyber Risks

Types of Cyber Risks:

- Liability:
  - Responding to allegations of negligent acts, errors, omissions in providing technology-related services to others
  - Responding to allegations that a network security failure resulted in the stealing, or inadvertent disclosure, of private or sensitive information
  - Responding to allegations that a cyber-security event resulted in defamation, copyright or trademark infringement, or invasion of privacy
  - Responding to regulatory or other governmental investigations relating to a cyber-security event

Types of Cyber Risks:

- First-Party:
  - Costs incurred in responding to a cyber-security event, including investigative, forensic, public relation, notification, and other costs
  - Business interruption losses
  - Costs incurred in restoring and/or recreating electronic data following a cyber-security event
  - Cyber extortion
  - Reputational damage
  - Theft of valuable digital assets, including customer lists and trade secrets

Coverage Issues Under General Liability and Other "Traditional" Types of Insurance Policies

Main Issues/Recent Trends

- Commercial General Liability (CGL) Policies:
  - Normally written on ISO forms
  - Could the loss involve “bodily injury” or “property damage” (Coverage A) or “**personal injury**” or “advertising injury” (Coverage B)?
    - Analysis as to whether the loss involves “property damage” may turn on whether the damages property is “tangible.” *See*, *e.g.*, *Am. Online, Inc. v. St. Paul Mercury Ins. Co.*, 347 F.3d 89 (4th Cir. 2003) (Court rejected the insured’s argument that data was tangible because it consisted of small electromagnets visible under a microscope)

Main Issues/Recent Trends

- Commercial General Liability (CGL) Policies:
  - ISO began in 2012 to publish endorsements seeking to limit or eliminate coverage for cyber risks under CGL policies
    - Through modified definitions and/or exclusions

Main Issues/Recent Trends

- Property Policies:
  - Most property policies insure only against *physical* loss
  - Some courts have held that "physical damage" is *not* restricted to the physical destruction or harm of computer circuitry, but includes loss of access, loss of use, and loss of functionality. *See*, *e.g.*, *Am. Guar. & Liab. Ins. Co. v. Ingram Micro, Inc.*, 2000 WL 726789, 2000 U.S. Dist. LEXIS 7299 (D. Ariz. 2000); *NMS Servs. V. Hartford*, 2003 U.S. App. LEXIS 7442 (4th Cir. 2003)

Main Issues/Recent Trends

- Property Policies:
  - However, other courts have questioned that reasoning, and ruled otherwise. *See*, *e.g.*, *Ward Gen. Ins. Servs., Inc. v. Employers Fire Ins. Co.*, 114 Cal. App. 4th 548, 7 Ca. Rptr. 3d 844 (Cal. App. 2003) (Plaintiff's loss of database and information was not a direct physical loss or damage to covered property, as the information itself did not have a material existence, and is not formed from tangible matter nor perceptible to the sense of touch); *State Auto Prop. & Cas. Ins. Co. v. Midwest Computers & More*, 147 F.Supp.2d 1112 (W.D. Okla. 2001) (Although court found coverage on other grounds, it held that computer data itself can't be touched, held or sensed by the human mind, and has no physical substance)

Main Issues/Recent Trends

- Other Types of "Traditional" Policies:
  - Although the analysis will vary depending on the nature of the claim and the specific policy language, it is possible (though unlikely) that coverage for cyber-related claims may be available under other types of "traditional" insurance policies, such as:
    - Professional Liability (Errors & Omissions) policies - *See*, *e.g.*, *Eyeblaster, Inc. v. Fed. Ins. Co.*, 613 F.3d 797 (8th Cir. 2010) (finding duty to defend under technology errors and omissions policy); *St. Paul Fire & Marine Ins. Co. v. Compaq Comput. Corp.*, 539 F.3d 809 (8th Cir. 2008)

Main Issues/Recent Trends

- Other Types of "Traditional" Policies:
  - Directors & Officers Liability policies – *See*, *e.g.*, *First Bank of Del., Inc. v. Fid. & Deposit Co. of Md.*, 2013 Del. Super. LEXIS 465 (Del. Super. Ct. 2013) (finding coverage for losses from data breach under "Electronic Risk Liability" coverage part)
  - Crime and fidelity policies – *See*, *e.g.*, *Retail Ventures, Inc. v. Nat'l Union Fire Ins. Co.*, 691 F.3d 821 (6th Cir. 2012) (finding coverage for $6.8 million in damages caused by a hacking incident under a computer fraud rider to a crime policy)

Recent Decisions Involving Cyber Risks and "Traditional" Insurance Policies

Recall Total Info. Mgmt. v. Fed. Ins. Co., 147 Conn. App. 450, 83 A.3d 664 (Conn. App. 2014); *affirmed* 317 Conn. 46, 115 A.3d 458 (2015)

- IBM contracted with Recall to store computer tapes containing "personally identifiable information" (or PII) of IBM employees. Recall subcontracted with a transportation company to transport the tapes to its facility. During the transport, the cart containing the tapes fell out of the back of the van near a highway exit ramp, and many of the tapes were removed from the roadside by an unknown person.

Recent Decisions Involving Cyber Risks and "Traditional" Insurance Policies

Recall Total Info. Mgmt. v. Fed. Ins. Co., 147 Conn. App. 450, 83 A.3d 664 (Conn. App. 2014); *affirmed* 317 Conn. 46, 115 A.3d 458 (2015)

- IBM ultimately spent more than $6 million in notifying the affected employees, setting up a call center, and providing credit monitoring services, and charged the amount to Recall. Recall settled with the transportation company, who assigned its rights to any insurance proceeds to Recall.
- Coverage issue was whether Coverage B of a CGL policy should provide coverage, and specifically whether the loss involved "oral or written publication, in any manner, of material that violates a person's right of privacy"

Recent Decisions Involving Cyber Risks and "Traditional" Insurance Policies

Recall Total Info. Mgmt. v. Fed. Ins. Co., 147 Conn. App. 450, 83 A.3d 664 (Conn. App. 2014); *affirmed* 317 Conn. 46, 115 A.3d 458 (2015)

- The court held that there was no coverage because there was no "publication," since there was no evidence that the information on the tapes had been accessed or disseminated

Recent Decisions Involving Cyber Risks and "Traditional" Insurance Policies

Zurich Am. Ins. V. Sony Corp. of Am., Index No. 651982/2011 (N.Y. Sup. Ct. 2014)

- Trial court granted summary judgment to Zurich and Mitsui Sumitomo Insurance Company of America
- The issue was whether acts by third-party hackers constitute "oral or written publication, in any manner, of material that violates a person's right of privacy"
- The trial court held that they did not, and therefore there was no coverage under the policies issued by Zurich and MSI
- While on appeal, case settled

Recent Decisions Involving Cyber Risks and "Traditional" Insurance Policies

L.A. Lakers, Inc. v. Fed. Ins. Co., 2015 U.S. Dist. LEXIS 62159 (C.D. Cal. April 17, 2015)

- Underlying claim involved a putative class action, in which the lead plaintiff sought damages and injunctive relief pursuant to the Telephone Consumer Protection Act ("TCPA"). The plaintiff alleged that in 2013, while attending a Lakers game, he acted on the Lakers' solicitation to send a text message that would be posted on the arena's scoreboard during the game, and that the Lakers then used his cellular number to send an unsolicited text message in order to solicit business.

Recent Decisions Involving Cyber Risks and "Traditional" Insurance Policies

L.A. Lakers, Inc. v. Fed. Ins. Co., 2015 U.S. Dist. LEXIS 62159 (C.D. Cal. April 17, 2015)

- In the ensuing coverage litigation, the court granted the insurer's motion for summary judgment, finding that under the Directors & Officers policy at issue, the exclusion for any claim "based upon, arising from, or in consequence of libel, slander, oral or written publication of defamatory or disparaging material, invasion of privacy, wrongful entry, eviction, false arrest, false imprisonment, malicious prosecution, malicious use or abuse of process, assault, battery, or loss of consortium" applied to preclude coverage.

Recent Decisions Involving Cyber Risks and "Traditional" Insurance Policies

Travelers Indem. Co. of Am. v. Portal Healthcare Solutions, LLC, 35 F.Supp.3d 765 (E.D. Va. August 7, 2014); *affirmed* 2016 U.S. App. LEXIS 6554 (4th Cir. April 11, 2016)

- The underlying class action lawsuit involved allegations that the insured posted confidential medical records on the internet, making the records available to anyone who searched for a patient's name and clicked on the first result
- The Federal District Court held that: 1) making confidential medical records publicly accessible via an internet search does fall within the plain meaning of "publication"; and 2) posting confidential medical records online without security restriction gives "unreasonable publicity" to, and "disclosure" of information about, patients' private lives

Recent Decisions Involving Cyber Risks and "Traditional" Insurance Policies

Travelers Indem. Co. of Am. v. Portal Healthcare Solutions, LLC, 35 F.Supp.3d 765 (E.D. Va. August 7, 2014); *affirmed* 2016 U.S. App. LEXIS 6554 (4th Cir. April 11, 2016)

- As a result, the Federal District Court held that Travelers was obligated to defend the insured
- On appeal, the 4th Circuit affirmed

Recent Decisions Involving Cyber Risks and "Traditional" Insurance Policies

Cooper Indus. v. Nat'l Union Fire Ins. Co., 2016 U.S. Dist. LEXIS 80342 (S.D. Tex. June 21, 2016)

- Arose out of losses sustained by the insured from its investment in a Ponzi scheme, and the insurer's denial of coverage under a commercial crime policy
- The policy at issue had a limit of $10 million, and stated "we will pay for loss of or damage to 'funds' and 'other property' resulting directly from fraudulent or dishonest acts committed by an 'employee', whether identified or not, acting alone or in collusion with other persons"

Recent Decisions Involving Cyber Risks and "Traditional" Insurance Policies

Cooper Indus. v. Nat'l Union Fire Ins. Co., 2016 U.S. Dist. LEXIS 80342 (S.D. Tex. June 21, 2016)

- The policy also stated that "the property covered under this policy is limited to property: (1) that you own or lease; or (2) that you hold for others whether or not you are legally liable for the loss of such property"
- The court held that because the insured had loaned the funds to the investment advisor prior to the loss, it did not own the funds within the meaning of the policy

Recent Decisions Involving Cyber Risks and "Traditional" Insurance Policies

Maxum Indemnity Co. v. Long Beach Escrow Corp., Case No. 2:16-CV-05907, filed on August 8, 2016 in the Central District of California

- Case recently filed in order to determine the insurer's rights and obligations under a Professional Liability Coverage Form (Non-Medical) policy issued to Long Beach Escrow
- In the underlying action, the plaintiffs allege that one of their principal's email was hacked into and taken control of by unidentified individuals or entities
- The hackers allegedly sent an email to Long Beach Escrow, requesting three withdrawals from the plaintiffs' account totaling over $250,000

Recent Decisions Involving Cyber Risks and "Traditional" Insurance Policies

Maxum Indemnity Co. v. Long Beach Escrow Corp., Case No. 2:16-CV-05907, filed on August 8, 2016 in the Central District of California

- The plaintiffs allege that Long Beach Escrow wired over $250,000 to the hackers' accounts without communicating directly with the plaintiffs either by telephone or facsimile, and that it is standard industry practice to use two different communication forums when confirming transaction requests
- Maxum issued to Long Beach Escrow a professional liability policy with a policy limit of $1 million

Recent Decisions Involving Cyber Risks and "Traditional" Insurance Policies

Maxum Indemnity Co. v. Long Beach Escrow Corp., Case No. 2:16-CV-05907, filed on August 8, 2016 in the Central District of California

- Maxum alleges that coverage is precluded by: 1) a Funds Exclusion, and 2) a Fiduciary Duty Exclusion

The Advent of Cyber Risk Insurance, and Recent Case Law Interpreting Cyber Policies

The Advent of Cyber Risk Insurance

- Cyber coverage is relatively new, and is offered by approximately 30 - 60 insurers, including many of the largest and well known property and casualty carriers
- Policies go by many different names (“cyber,” “information security,” “network” or “privacy” to name a few), and there is little uniformity among policies
- Most cyber risk policies offer some combination of first-party and third-party (liability) coverage
- Cyber coverage may also be sold in conjunction with other coverages including, for example, professional liability, directors & officers, or media coverage

The Advent of Cyber Risk Insurance

- Features **may** include:
  - A number of separate grants of coverage, including data loss, business interruption, privacy notification, credit monitoring, reputational response, cyber extortion, forensics and regulatory investigation response
  - “Claims made” rather than “occurrence based”
  - Limitations on the definition of “damages”
  - Sublimits for specific types of cyber risk
  - No coverage for “intentional,” criminal or fraudulent conduct
  - Exclusion for claims resulting from acts of war or terrorism
  - Other exclusions

Recent Decisions Involving Cyber Policies

New Hotel Monteleone, LLC v. Certain Underwriters at Lloyd's London, Case No. 15-11711, filed in Orleans Parish, LA on December 10, 2015

- On or about October 17, 2014, Hotel Monteleone discovered that it may have experienced a cyberattack, and as a result of the security breach, payment card numbers were allegedly compromised and were no longer confidential
- Hotel Monteleone had procured a CyberPro insurance policy, with a policy limit of $3 million, issued by Ascent through a Lloyd's Syndicate
- According to the petition, Ascent relied on an endorsement to the policy, titled "Payment Card Industry Fines or Penalties Endorsement," to assert that a $200,000 sublimit applied to the loss
- Hotel Monteleone also sued the insurance broker

Recent Decisions Involving Cyber Policies

New Hotel Monteleone, LLC v. Certain Underwriters at Lloyd's London, Case No. 15-11711, filed in Orleans Parish, LA on December 10, 2015

- The lawsuit was later jointly dismissed

Recent Decisions Involving Cyber Policies

Travelers Prop. & Cas. Co. of Am. v. Federal Recovery Services, Inc., Case No. 2:14-CV-170, U.S. District Court for the District of Utah

- The defendants, which are in the business of providing processing, storage, transmission, and other handling of electronic data for its customers, procured from Travelers a CyberFirst Technology Errors and Omissions Liability Form Policy
- In the underlying lawsuit, the defendants were accused of intentionally withholding customer payment and account data from a fitness company it had contracted with
- The policy provided coverage for “errors and omissions,” and defined the term “errors and omissions wrongful act” as “any error, omission or negligent act”

Recent Decisions Involving Cyber Policies

Travelers Prop. & Cas. Co. of Am. v. Federal Recovery Services, Inc., Case No. 2:14-CV-170, U.S. District Court for the District of Utah

- By order dated May 11, 2015, and reiterated in an order issued on January 12, 2016, the court ruled that Travelers did not have a duty to defend the insureds because the underlying complaint alleged only intentional conduct

Recent Decisions Involving Cyber Policies

P.F. Chang's China Bistro, Inc. v. Fed. Ins. Co., Case No. CV-15-01322-PHX-SMM, U.S. District Court for the District of Arizona

- Federal issued to P.F. Chang's corporate parent a CyberSecurity by Chubb Policy
- P.F. Chang's had entered into a Master Service Agreement with Bank of America Merchant Services ("BAMS"), under which P.F. Chang's would deliver its customers' credit card payment information to BAMS, which would then settle the transaction through an automated clearinghouse
- On June 10, 2014, P.F. Chang's learned that computer hackers had obtained and posted on the Internet approximately 60,000 credit card numbers belonging to its customers

Recent Decisions Involving Cyber Policies

P.F. Chang's China Bistro, Inc. v. Fed. Ins. Co., Case No. CV-15-01322-PHX-SMM, U.S. District Court for the District of Arizona

- As of May 26, 2016, Federal had reimbursed P.F. Chang's over $1.7 million for costs incurred as a result of the security compromise
- Following the data breach, MasterCard imposed on BAMS a Fraud Recovery Assessment totaling over $1.9 million (separate from the $1.7 million already reimbursed by Federal), which BAMS passed on to P.F. Chang's. P.F. Chang's tendered those amounts to Federal, which denied coverage. P.F. Chang's then filed suit, seeking recovery of those costs from Federal.
- The main coverage issue was whether BAMS suffered a "privacy injury," which gave rise to P.F. Chang's liability

Recent Decisions Involving Cyber Policies

P.F. Chang's China Bistro, Inc. v. Fed. Ins. Co., Case No. CV-15-01322-PHX-SMM, U.S. District Court for the District of Arizona

- The court held that BAMS had not suffered a "privacy injury," because the customers' information that was the subject of the data breach was not part of BAMS' "record," but rather the "record" of the issuing banks

Recent Decisions Involving Cyber Policies

InComm Holdings, Inc. v. Great American Ins. Co., Civil Action No. 1:15-cv-02671-WSD, filed in the U.S. District Court for the Northern District of Georgia

- In May of 2014, InComm discovered an unauthorized exploitation of its computer system that processes transactions for InComm's Vanilla Reload Network. Apparently, fraudsters manipulated InComm's Integrated Voice Response (IVR) system in a manner that allowed them to illegally redeem funds from a single Vanilla Reload prepaid chit multiple times, resulting in a loss to InComm of over $11.4 million.
- InComm sought coverage under a Crime Protection Policy issued by Great American. Great American allegedly denied coverage.

Recent Decisions Involving Cyber Policies

InComm Holdings, Inc. v. Great American Ins. Co., Civil Action No. 1:15-cv-02671-WSD, filed in the U.S. District Court for the Northern District of Georgia

- On July 15, 2016, InComm filed a Motion for Summary Judgment
- Further briefs have been filed, and Great American recently sought leave to file a Sur-Reply in Opposition to InComm's Motion for Partial Summary Judgment
- One coverage issue relates to whether the loss resulted from "computer fraud" (there are others)
- The case is being followed with interest

Thomas G. Drennan, Partner
(312) 428-2728
tom.drennan@dinsmore.com

Let's *Accomplish* more.℠ Together.