DORSEY always ahead

Minnesota Legal Conference on Privacy and Data Security: Cybersecurity Insurance

July 23, 2019

Katie C. Pfeifer
Dorsey & Whitney LLP
Pfeifer.Katie@Dorsey.com
(612) 340-2600

Cyber Incidents

- Common
  - Identity Theft Resource Center, Monthly Breach Report December 2018 – 89 breaches with 945,735 records exposed
- Can Be Costly
  - Average cost of data breach (U.S.): $7.91 million (2018 Ponemon)
  - Average cost of data breach for each record (U.S.): $233 (2018 Ponemon)
  - Average number of records at issue per breach (U.S.): 31,500 (2018 Ponemon)

Who Will Pay the Bill? Insurance As One Tool In Risk Management

- Understand Risk, Magnitude of Exposure
- Traditional Policies Provide Some Coverage
- Cyber Policies Available
- Couple With Non-Insurance Risk Management

DORSEY always ahead

Part I:
Fitting a Round Peg in a Square Hole

Finding Coverage for Cyber Losses in Traditional Insurance Policies

DORSEY always ahead

Can you make it work?

DORSEY always ahead

Traditional Policies

- Cyber policies exist and may provide coverage for the loss or theft of data
- Not all insureds have those policies
- And not all cyber policies provide (enough) coverage in the event of a claim
- When there is a loss or theft of data or information, may try to find coverage under other policies

DORSEY always ahead

First Party Claims

- Claim by the insured
- Seeking recovery for its own losses
- Usually a loss of use of property because of damage or destruction

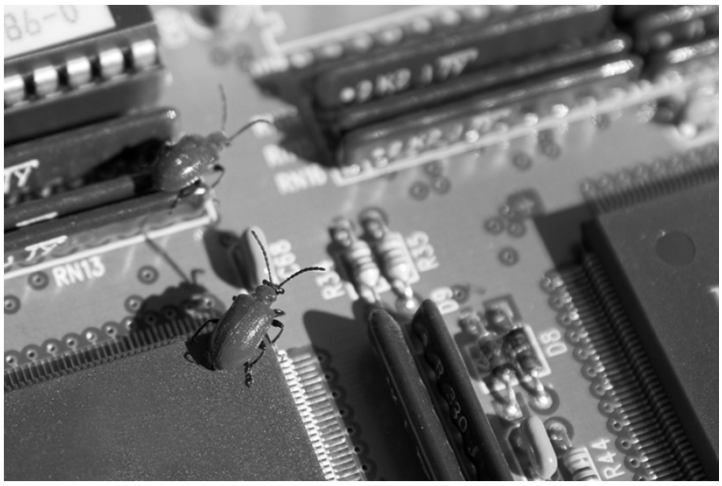
DORSEY always ahead

First Party Cyber Losses

- Replacing corrupt data
- Labor costs of re-entering data
- Loss of stolen property
- Cost of replacing inoperable systems
- Loss of income / administrative costs (business interruption)
- Cost of extortion
- Investigation / notification
- Regulatory costs of reporting, paying fines, challenging the fines, etc.

DORSEY always ahead

Property Insurance: A Bug in the System



DORSEY always ahead

Property Coverage

- Damage to property
- "Direct **physical** loss of or damage to" covered property
- Physical injury to **tangible property**, including all resulting loss of use of that property and also loss of use of tangible property that is not physically injured

DORSEY always ahead

Is electronic data tangible property?

DORSEY always ahead

Importance

- Deciding whether data is “tangible property” is important in both claims by an insured (first party) and claims against an insured (third party)
- The issue comes up in both property insurance claims and CGL claims
- The case law under both types of claims is relevant

DORSEY always ahead

History

- Decisions in the 1980s dodged the issue
- When the courts began to actually address the question in the early 1990s, they seemed to answer "yes"
- A Minnesota court compared tape to motion picture film and found that data was tangible property because it was "integrated completely with the physical property of the tape" (*Retail Sys., Inc. v. CNA Ins. Cos.*, 469 N.W.2d 735 (Minn. Ct. App. 1991))
- *See also Landmark Am. Ins. Co. v. Gulf Coast Analytical Labs*, 2012 U.S. Dist. LEXIS 45184 (M.D. La. Mar. 26, 2012) (in case involving hard drive failure leading to corruption of data, concluding that because the "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" that there was "direct, physical 'loss or damage'")

DORSEY always ahead

Developments

- Position shifting
- Courts have found that data is not tangible property because it has no physical substance
- While stored in a physical form on a computer's hard drive, software and data amounted to the loss of an abstract idea, logic, instruction, or information (*Am. Online, Inc. v. St. Paul Mercury Ins. Co.*, 347 F.3d 89 (4th Cir. 2003))
  - *See also Ward Gen. Ins. Servs., Inc. v. Emp'rs Fire Ins. Co.*, 114 Cal. App.4th 548 (Cal. Ct. App. 2003) (finding no coverage for database crash (i.e., loss of organized information), as database was not physical)

DORSEY always ahead

Current Positions

- Data is information
- Data is therefore not “tangible property”

DORSEY always ahead

But wait…

DORSEY always ahead

There May Be Coverage

- Data is information
- But issues like damage to software or a virus may have other consequences
- Some courts have found that, when a computer fails or works slowly, there is damage to tangible property
- That is, loss of use of the computer is damage to tangible property

DORSEY always ahead

Analyzing the Claim

- In any claim under a property insurance policy, the first step should involve identifying the type of damages claimed
- If there is no claim of damage to hardware, there likely will be no coverage

DORSEY always ahead

Crime Insurance

DORSEY always ahead

Computer Fraud

- Crime, or fidelity, insurance policies usually provide coverage for employee theft and fraud, **including computer fraud**
- Insurer will pay for loss of, or damage to, money, securities, and other property resulting directly from the use of any computer to fraudulently transfer that property from inside the premises or bank to a person or place outside the premises

DORSEY always ahead

Property

- The coverage, again, is for property
- The same issues in defining property can apply here

DORSEY always ahead

Is the loss a "direct" loss?

- If an employee takes money from the cash register, that is a direct loss
- But a loss that results from a 3rd party may not be
- A crime policy will probably not cover a data breach resulting in theft of a customer's personal information (credit card numbers, etc.)

DORSEY always ahead

Use of a Computer

DORSEY always ahead

What sort of computer use is required?

- What if the loss was a fraudulent scheme involving communication by email instead of in person or by phone?
- As more business is done with email (and more phone lines run through computers), can be an important question
- Courts are split

DORSEY always ahead

Yes: Any Use is Enough

- *State Bank of Bellingham v. BancInsure, Inc.*, 2014 U.S. Dist. LEXIS 136849 (D. Minn. Sept. 29, 2014)
  - Fidelity bond matter; conclusion that coverage applies if the data breach is a foreseeable and natural consequence of the computer use
  - Insured defrauded out of nearly $500,000 after computer hacker installed a virus on the insured's computer that allowed hacker to initiate unauthorized financial transactions
  - Case turned on what the "efficient and proximate cause" of the loss was: court decided not the employee's conduct (excluded conduct) in downloading a virus from an email
  - Court summarized: "without the fraudster's actions, there would have been no loss even if all of the other circumstances existed"

DORSEY always ahead

25

Yes: Any Use is Enough (con't)

- *Owens, Schine & Nicola, P.C. v. Travelers Cas. & Sur. Co. of Am.*, 2010 Conn. Super. LEXIS 2386 (Conn. Super. Ct. Sept. 17, 2010), *vacated by stipulation of the parties* 2012 Conn. Super. LEXIS 5053 (Conn. Super Ct. Apr. 18, 2012)
  - Fraud communicated by email (request for assistance to a law firm for a collections matter)
  - Insurer argued the claimed loss was not "directly caused by a computer fraud" and that intended coverage was for hacking
  - The court disagreed: "use of a computer" was ambiguous

DORSEY always ahead

Yes: Any Use is Enough (con't)

- *Am. Tooling Center, Inc. v. Travelers Cas. & Sur. Co. of Am.*, 895 F.3d 455 (6th Cir. 2018)
  - Fraud by social engineering
  - Concluded summary judgment appropriate for insured, arising out of fraudulent transfers of money: "it was not necessary for the computer to fraudulently cause the transfer of funds
  - Rather, impersonator sent fraudulent emails using a computer, and the emails fraudulently caused the insured to transfer the money to the impersonator
- *Medidate Sols., Inc. v. Fed. Ins. Co.*, 268 F. Supp.3d 471 (S.D.N.Y. 2017) (concluding insured demonstrated its losses were a "direct cause of a computer violation" where insured's employees "only initiated the transfer as a direct cause of the thief sending spoof[ed] emails posing as [insured's] president")

DORSEY always ahead

No: There must be more than just regular or incidental use

- *Universal Am. Corp. v. Nat'l Union Fire Ins. Co. of Pittsburgh, Pa*, 25 N.Y.3d 675, 683 (N.Y. 2015)
  - Coverage "applies to losses incurred from unauthorized access to [the insured's] computer system, and not to losses resulting from fraudulent content submitted to the computer system by authorized users"
- *Apache Corp. v. Great Am. Ins. Co.*, 662 Fed. Appx. 252, 258 (5th Cir. 2016)
  - Agreeing with insurer that loss was not covered because it did not "result directly from the use of any computer to fraudulently cause a transfer"; "the 'computer use' was an email with instructions to change a vendor's payment information" but "the email was part of the scheme" and "merely incidental to the occurrence of the authorized transfer of money")

DORSEY always ahead

Look Closely

DORSEY always ahead

Policy Language

- In crime insurance claims, the specific policy language, if any, defining “use of a computer” will likely determine if coverage exists under the facts of the case
- But, assuming language is not iron clad, can likely find case law to support coverage or not

DORSEY always ahead

Third Party Claims

- Third party losses are losses caused (allegedly) by the insured's negligence and sustained by third parties who then bring a claim against the insured
- In cyber cases, third party losses are usually losses that result when someone accesses the insured's electronic data and destroys it, damages it, or steals the information of some third party when that information is in the care and control of the insured

DORSEY always ahead

Types of Loss

- Theft of personal information
- Transmission of a computer virus from the insured's system to some third party's system
- Exclusion of an authorized third party from accessing the insured's computer system
- Failing to give notice of an intrusion or theft to a third party in violation of statutes, regulations, or contractual terms

DORSEY always ahead

Immediate vs. Future

- Claims may be immediate: a 3rd party's loss of data, recovery expenses, costs to replace inoperable computers or systems, etc.
- Claims may be for potential future losses: identity theft repair and monitoring

DORSEY always ahead

Broad Coverage?

DORSEY always ahead

Commercial General Liability

- Big area for 3rd party claims
- CGL policies are broad liability policies with many subparts
- The terms of the policies typically follow the standard Insurance Services Office (ISO) policies
- The most common sections that are triggered are Coverage A and Coverage B

DORSEY always ahead

Coverage A

- The insurer will pay those sums the insured becomes legally obligated to pay as damages because of bodily injury or property damage
- A bodily injury claim may not be typical yet, although perhaps more potential for such claims than in years past because of the Internet of Things (IoT)
  - The interconnection of devices (other than typical devices such as computers and smartphones) to the Internet
  - Cars, refrigerators, thermostats (Nest)
  - 50 billion devices connected to the Internet by the year 2020
- Claims for emotional distress are also theoretically possible

DORSEY always ahead

Second verse, same as the first…

DORSEY always ahead

…Property Damage

- Coverage A claims thus far are almost always claims for property damage
- The analysis looks like a first party property damage issue – does the loss actually involve damage to tangible property?
- Again, the trend is to find that data is not tangible property, so the claims must involve more than just data
  - *See, e.g.*, *Seagate Tech., Inc. v. St. Paul Fire & Marine Ins. Co.*, 11 F. Supp.2d 1150 (N.D. Cal. 1998) (in case regarding allegations against Seagate that disk drives were failing, because the complaint did not allege that components of the host computer, other than the disk drives, suffered damage, the loss of data by itself was not "physical damage to tangible property")

DORSEY always ahead

Language Change

- ISO changed the definition of "property damage" in 2001
  - The definition now states that "electronic data is not tangible property"
- And, in 2004, ISO added an exclusion (Exclusion P)
  - The policy does not cover "[d]amages arising out of the loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data"
  - But, in 2013, there was a language change that confirms coverage for damages for bodily injury due to the loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data

DORSEY always ahead

Coverage B

- Personal and advertising injury, which includes "publication, in any manner, of material that violates a person's right of privacy"
- Claims under this provision typically involve alleged damages due to the theft of personal information from a large company, like the well-publicized data breaches involving Yahoo, Target, Sony, and others

DORSEY always ahead

Exclusions

- Several exclusions may apply
  - Intentional/Criminal acts
  - Knowing violation
  - Intellectual property

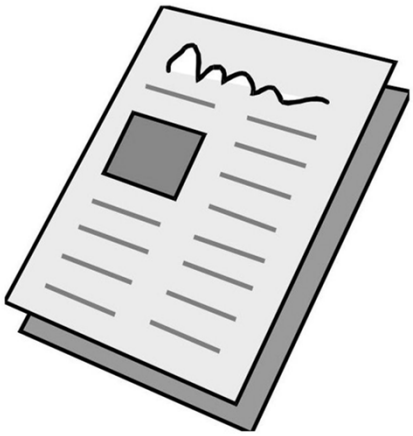
DORSEY always ahead

"Right of Privacy"

- Some courts have required that the 3rd party actual make a claim for invasion of privacy
- Minnesota does not have that requirement
  - *Owners Ins. Co. v. European Auto Works, Inc.*, 695 F.3d 814, 820 (8th Cir. 2012) (concluding that coverage can extend to seclusion based torts that involve intruding on another's solitude, as well as secrecy-based torts such as those directed at disclosure of information)

DORSEY always ahead

Publication



DORSEY always ahead

What Constitutes Publication?

- Often biggest question under Coverage B
- Definition of publication not limited to cyber cases
- Many courts require that “publication” involve a wide-spread distribution
- But others have found publication in a more restricted group of recipients

DORSEY always ahead

Is a data breach a publication?

- Fact-dependent
- In a case alleging theft, use, and possible sale of personal information, Ohio court found support for the claim that publication took place
  - *Galaria v. Nationwide Mut. Ins. Co.*, 998 F. Supp.2d 646, 658 (S.D. Ohio 2014), *rev'd on other grounds* 663 Fed. Appx. 384 (6th Cir. 2016))

DORSEY always ahead

Is a data breach a publication? (con't)

- *Recall Total Info. Mgmt., Inc. v. Fed. Ins. Co.*, 83 A.3d 664 (Conn. App. Ct. 2014): "The plaintiffs have failed to cite any evidence that the information was published and thereby failed to take their allegation beyond the realm of speculation."
- *Burton v. MAPCO Express, Inc.*, 47 F. Supp.3d 1279 (N.D. Ala. 2014): "Mr. Burton offers no legal basis for his claim that a theft of data from a merchant constitutes communication of the information stolen to the public. Without such disclosure to the public at large, there is no tort."

DORSEY always ahead

Publication by Whom?

- In *Zurich Am. Ins. Co. v. Sony Corp. of Am.*, 2014 N.Y. Misc. LEXIS 5141 (N.Y. Sup. Ct. Feb. 21, 2014), the insurer argued that Coverage B applied to the purposeful and intentional acts of the insured, not to acts by third parties
- The judge ruled from the bench, finding that there was a publication, but that coverage only applied to the extent that Sony, not the hackers, was responsible for the publication
- The case was appealed, but (after oral argument) the parties settled
- *See also Innovak Int'l, Inc. v. Hanover Ins. Co.*, 280 F. Supp.3d 1340 (M.D. Fla. 2017) (summary judgment in favor of insurer; no duty to defend under Coverage B because of no allegation of publication, directly or indirectly, by insured)

DORSEY always ahead

ISO Change

- As with Coverage A, CGL policies are beginning to change terms to prevent claims based on the theft of electronic data
- A 2013 endorsement to the standard ISO form removes coverage for publication of material that violates a person's right of privacy from the definition of personal and advertising injury under Coverage B
- That change, and other similar changes, will likely limit claims by insureds under their CGL policies for data breaches

DORSEY always ahead

Finding Coverage for Management Errors

- Directors and Officers Liability (D&O)
- Errors and Omissions Liability (E&O)

DORSEY always ahead

Shareholder Complaints

- For example, in light of their highly publicized data breaches, shareholders of Target and Sony brought claims against the directors and officers of the companies, alleging that managers failed to implement internal controls to protect personal information, and that such failures breached a fiduciary duty owed to investors
- Claims of that nature may prove difficult to establish, *see Palkon v. Holmes*, 2014 U.S. Dist. LEXIS 148799 (D.N.J. Oct. 20, 2014); *see also David v. Steinhafel,* 14-cv-203, Order (D. Minn. July 7, 2016) (dismissing derivative suits arising out of Target data breach, following SLC investigation)
  - Defense costs and perhaps indemnification (if necessary) may be covered under D & O policies

DORSEY always ahead

Language

- These policies (especially D&O policies) are not as standard as CGL policies and so the specific policy language may be determinative

DORSEY always ahead

Part II:

A Round(er) Hole For A Round Peg

Cyber-Specific Coverages

DORSEY always ahead

Cyber-Specific Policies

- Many insurance companies offer some type of cyber-specific coverage
- Danger though: No standard cyber-policy form in the industry
  - Insurers getting into the market; need to proceed with caution as to the insurer's knowledge and experience
  - Insurers creating their own policy forms, with coverage that can differ significantly from form to form
- Cyber-specific policies are often "attached" to other policies
  - *E.g.*, an E&O policy might contain cyber-specific endorsements
  - Better option generally is a stand-alone policy BUT
    - Ala carte menu: many different types of coverage available

DORSEY always ahead

Cyber-Specific Policies

- Like "traditional" policies, cyber-policies are designed to cover:
  - First Party Claims
  - Third Party Claims

DORSEY always ahead

First Party Claims

- **Theft and Fraud** – destruction or loss of the policyholder's data due to criminal / fraudulent cyber event
- **Forensic Investigation** – assess and stop a cyber event
- **Notification Costs –** costs of notifying victims of cyber-event
- **Crisis Management** – costs of public relations or management services

DORSEY always ahead

First Party Claims

- **Business Interruption** – lost income and related costs suffered by the policyholder
- **Extortion** – investigation of threats and "payments" to extortionists
- **Computer Loss and Data Restoration** – damage to or loss of use of computer-related assets, including retrieving and restoring data
- **Regulatory Response** – response to governmental inquiry relating to cyber-event

DORSEY always ahead

Third Party Claims

- **Litigation/Regulatory Liability** – liability and defense in third-party / government action (e.g., losses because of denial or delays of access to business systems or costs associated with regulatory proceedings resulting from a cyber incident)
- **Media Liability** – damages due to copyright infringement, misappropriation of trade secrets, defamation, or invasion of privacy relating to publication of affected material
- **Privacy liability –** liability relating to privacy claims (e.g., damage payable for unauthorized disclosure, use, or destruction of information or PII)
- **NDA** / **Confidentiality** – liability relating to confidential corporate information

DORSEY always ahead

A Host of Options

DORSEY always ahead

58

Types of Cyber Insurance

- Privacy and Crisis Management
- Computer Program and Electronic Data Restoration Expenses
- Network Business Interruption
- Cyber Extortion
- Network Security and Privacy Liability (could include information security and privacy liability, regulatory defense and penalties, and payment card industry fees and penalties)
- Enterprise and Internet Media
- Whether imbedded within or separate: coverage for computer fraud, funds transfer fraud, or social engineering / fraudulent instruction

DORSEY always ahead

Example Insuring Agreement

- Policy language example (Privacy and Crisis Management):
  - Insuring Clause: The Insurer shall pay all Loss, in excess of the applicable Retention, less the applicable Coinsurance percentage that an Insured incurs solely as a result of an alleged Security Failure or Privacy Event that has actually occurred or is reasonably believed by such Insured and the Insurer to have occurred.
  - Definition of Security Failure: failure or violation of the security of a Computer System, including, without limitation, that which results in or fails to mitigate any unauthorized access, unauthorized use, denial of service attack or receipt or transmission of a malicious code
  - Definition of Privacy Event: any failure to protect Confidential Information including, without limitation, that which results in an identity theft or other wrongful emulation of the identity of an individual or corporation

DORSEY always ahead

Example Insuring Agreement

- Policy language example (Network Security and Privacy Liability):
  - Insuring Clause: The Insurer shall pay on an Insured's behalf all Loss in excess of the applicable Retention that such Insured is legally obligated to pay resulting from a Claim alleging a Security Failure or a Privacy Event.
  - Definition of Security Failure:
    - failure or violation of the security of Computer System …
    - physical theft of hardware controlled by a Company …
    - failure to disclose an event referenced above in violation of any Security Breach Notice Law
  - Definition of Privacy Event:
    - any failure to protect Confidential Information, without limitation, that which results in an identity theft or other wrongful emulation of the identity of an individual or corporation;
    - failure to disclose an event referenced above in violation of any Security Breach Notice Law; or
    - violation of any federal, state, foreign or local privacy statute alleged in connection with a Claim for compensatory damages, judgments, settlements, pre-judgment …

DORSEY always ahead

Example Insuring Agreement

- Policy language example (Network Business Interruption):
  - Insuring Language: The Insurer shall pay all Loss in excess of the Remaining Retention that an Insured incurs after the Waiting Hours Period and solely as a result of a Security Failure.
  - Definition of Security Failure: means a failure or violation of the security of a Computer System, including, without limitation, that which results in or fails to mitigate any unauthorized access, unauthorized use, denial of service attack or receipt or transmission of a malicious code
  - Definition of Computer System: means any computer hardware, software, or any components thereof that are under the ownership, operation or control of a Company or an Outside Provider, or leased by a Company, and linked together

DORSEY always ahead

Example Insuring Agreement

- Policy language example (Cyber Extortion):
  - Insuring Clause: The Insurer shall pay all Loss in excess of the applicable Retention that an Insured incurs solely as a result of a Security Threat.
  - Definition of Security Threat: means any threat or connected series of threats to commit an intentional attack against a Computer System for the purpose of demanding money, securities or other tangible or intangible property of value from an Insured

DORSEY always ahead

Definition of Data

- For policy covering data restoration or replacement, definition of data is key
  - Typically includes PII
  - Should also include non-PII confidential data: trade secrets, proprietary business information, and other confidential non-PII information a particular business handles
  - May also include non-electronic data: will want to ensure no coverage gap (compare other policies)

DORSEY always ahead

64

Scope of Covered Losses

- Questions to Ask:
  - PCI fees included?
  - Social Engineering Fraud?
  - Data Loss from Physical Breaches (e.g., theft of / loss of laptops, smart phones)?
  - Data Loss from Storage with a Third-Party Storage or Cloud Vendor?
  - BYOD Coverage?

DORSEY always ahead

65

Other Important Considerations

- Consultancy Services
  - Forensic firms
  - Crisis management / public relation firms
  - Law firms
- Sublimits
- Retroactive Date
  - Data breaches / cyber events can result from incidents that took place well in the past
- Warranties and Incorporation of Application Materials

DORSEY always ahead

66

Other Important Considerations

- Dishonesty / Criminal / Intentional Acts Exclusion (but severability generally applies)
- Contractual Liability Exclusion
  - PCI consequences
  - *P.F. Chang's China Bistro, Inc. v. Fed. Ins. Co.*, 2016 U.S. Dist. LEXIS 70749 (D. Az. May 26, 2016) (concluding no coverage for PCI fees and assessments because insured had voluntarily agreed to indemnify other party, and there was no evidence that insured would have had to do so absent its agreement)

DORSEY always ahead

Other Important Considerations

- Location Restrictions
  - Data is global
- War / Terrorism Exclusions
- Failure to Follow Minimum Required Practices / Failure to Follow Minimum Accepted Practices
  - *Columbia Cas. Co. v. Cottage Health Sys.*, No. 2:16-cv-03759 (C. Dist. Cal.)

DORSEY always ahead

Insurance As One Tool In Risk Management

- Understand Risk, Magnitude of Exposure
  - Information and Operations
- Traditional Policies Provide Some Coverage
- Cyber Policies Are Available
  - Underwriting Can Be Extensive
  - Applications Matter
  - Details Matter
- Couple With Non-Insurance Risk Management
  - Security programs, policies and procedures
  - Data retention / storage attention
  - Readiness exercises
  - Contractual risk management (indemnification)

DORSEY always ahead

Questions?

Katie C. Pfeifer
Dorsey & Whitney LLP
(612) 340-2600
Pfeifer.katie@dorsey.com

DORSEY always ahead