

# Insurance Coverage for Cyber Liability

Tarron L. Gartner-Ilai  
Carrie T. Carter

24th Annual Insurance Symposium

April 7, 2017

Cityplace

2711 N. Haskell Ave.

Dallas Texas 75204

© 2017 This paper and/or presentation provides information on general legal issues. It is not intended to provide advice on any specific legal matter or factual situation, and should not be construed as defining Cooper and Scully, P.C.'s position in a particular situation. Each case must be evaluated on its own facts. This information is not intended to create, and receipt of it does not constitute, an attorney-client relationship. Readers should not act on this information without receiving professional legal counsel.

Cooper & Scully  
*A Professional Corporation*

# What is Cyber Liability?

Cyber liability is the risk that information obtained through conducting business over the internet, other networks, or through the use of electronic storage technology will be compromised.

- First party liability occurs when your own information is breached.
- Third party liability occurs when the compromised information is disseminated to a third party.

```
C:\Documents and Settings\run
```

# Who's at Risk?

Neiman Marcus

Scottrade



Anthem. 

SONY

 Experian<sup>SM</sup>

Cooper & Scully  
A Professional Corporation

# The Usual Suspects

- Organized Crime
- Hackers
- Rogue Employees
- Stalkers
- Human error
- You
  - Lost or stolen devices
  - Weak passwords or repeated use of the same passwords

# The Fall Out

- Business interruption
- Logistics and expense of data recovery
- Public relations (short term)
- Crisis management
- Legal fines and penalties
- Civil liability
- Reputation (long term)

# Possible sources of Coverage: the CGL: Coverage A

- “Bodily injury”
  - Mental anguish without physical manifestation is not “bodily injury”  
*Zurich Am. Ins. Co. v. Nokia, Inc.*, 268 S.W.3d 487 (Tex. 2008).
  
- “Property damage”
  - Since 2001 CGL policies states:
  - “For purposes of this insurance, electronic data is not tangible property. As used in this definition, electronic data means information, facts or programs stored as or on, created or used on, or transmitted to or from computer software, including systems and applications software, hard or floppy disks, CD-ROMS, tapes, drives, cells, data processing devices, or any other medial which are used with electronically controlled equipment”

# Possible sources of Coverage: the CGL: Coverage B

- Personal and Advertising Injury
  - “Personal injury” includes defamation and publication of material that violates a right of privacy
    - Employee blogging (defamation)
    - Rouge employee data theft (if published and violates right of privacy)
  - “Advertising injury”
    - Data breach, if it results in theft of IP and later used in insured’s “advertising activities” (customer lists)



# Possible sources of Coverage: the CGL: Coverage B

- *Zurich American Ins. Co. v. Sony Corp. of Am.*, 127 A.D.3d 662 (N.Y. Sup. 2015)
  - The theft of Personally identifiable information regarding Play Station users is not a “publication” for purposes of “personal and advertising injury” coverage unless insured actually commits the offending act.
- *Recall Total Info. Mgmt. v. Federal Ins. Co.* 83 A.3d 664 (Ct. App. – Connecticut 2014)
  - Loss of 130 tapes containing employment related data is not a publication of material that violates a persons right of privacy absent evidence that anyone accessed the tapes.

# Possible sources of coverage: Commercial Property

- Does data loss or breach constitute direct physical loss of, or damage to, “covered property”?
  - The answer may depend on the difference between data versus loss of servers, hard drives, or other hardware.
- Business Interruption?
  - Depends on whether the peril is covered to begin with.

# Possible sources of coverage

- Employee Dishonesty/Crime
- E&O and D&O
  - Is a cyber attack a “loss event?”
  - Exclusions for loss of electronic data
  - May depend on definition of “professional services” in policy
  - Exclusions for fraudulent, malicious, criminal, dishonest acts

# Cyber Policy

- First Party Claims – unauthorized access to system or network
  - E-Theft or vandalism of proprietary or financial business data or information
    - Misappropriation
    - Damaged software or hardware caused by a virus or malware
    - E-signature
  - E-Threat - ransom
  - Business interruption damages
  - Regulatory fines and expenses
  - Expenses for upgrading software
  - Costs to restore stolen data
  - Damage to reputation
  - Crisis Management
  - Notification Expense

# Possible sources of coverage: Cyber Policy

## Third Party Claims

- Disclosure Injury for unauthorized access to information resulting from a cyber attack into a system
- Reputational Injury because of disparagement or invasion of privacy resulting from cyber activities
- Content Injury because of actual or alleged infringement of service mark, trade mark, slogan, symbol or title resulting from cyber activities
- Conduit Injury because a system cannot be used or is impaired resulting from a cyber attack or unauthorized access (DOS)
- Impaired Access Injury sustained by a customer authorized to access the system who is unable to do so as a result of fraudulent access

# New ISO Endorsements Effective May 1, 2014

- CG 00 01 04 13 – Electronic Data Exclusion:
  - p. Electronic data

Damages arising out of the loss of, loss of use of, damage to, corruption of, inability to access or inability to manipulate electronic data.

However, this exclusion does not apply to liability for damages because of "bodily injury."

As used in this exclusion, electronic data means information, facts or programs stored as or on, created or used on, or transmitted to or from computer software, including systems and applications software, hard or floppy disks, CD-ROMS, tapes, drives, cells, data processing devices or any other media which are used with electronically controlled equipment.

**QUESTIONS?**