The Nuts & Bolts of Cyber & Privacy Insurance Today

Thursday, February 28, 2013, 2:45 p.m.

Angela R. Elbert
Partner
Neal Gerber & Eisenberg, LLP
Chicago, Ill.

Angela R. Elbert, partner, Neal Gerber & Eisenberg, LLP, counsels clients on complex risk management and insurance issues and helps them obtain the maximum recovery possible when claims arise. She focuses her practice on advising organizations and boards of directors on a wide variety of risk management issues including indemnification agreements, financial insolvency concerns, and insurance aspects of corporate transactions and other business contracts. She has significant experience in handling complex insurance coverage litigation as well as other commercial litigation and mediations and arbitrations with an emphasis on representing policyholders nationwide in insurance coverage disputes involving virtually every line of insurance. Based upon interviews with her clients and peers, Angela has been described as “fantastic” and a “leading light” whose “breadth of knowledge is matched only by her commendable work ethic,” according to “Chambers USA: America’s Leading Lawyers for Business.”

Session Description:
This session will provide an overview on the nuts and bolts of today’s cyber and privacy risks. The presentation will include a general background of why you should care about these issues, the basic regulatory requirements and framework, the hole insurers perceive in cyber and privacy coverage in CGL policies, and the basics of a cyber and privacy policy.
Top Three Session Ideas
Tools or tips you learned from this session and can apply back at the office.

1. ________________________________________________

2. ________________________________________________

3. ________________________________________________
The Nuts & Bolts of Cyber & Privacy Insurance Today

Session Outline

Overview
- Background: Why You Should Care
- Recent Examples
- Key Causes of Loss
- Costs for Loss Generally
- Agenda

Regulatory Requirements
- Increasing & Varied Landscape
- Federal Law?
- SEC Guidance
- State Laws
- International Scope
- Disclaimer/Warning!

Cyber & Privacy Coverage in CGL Policies
- Historical CGL Policies
- CGL Coverage for Cyber Claims
- "Property Damage" Coverage for Data Losses
- 2001 CGL Policy Amended: Electronic Data is Not "Tangible Property"
- Loss of Use Damages Caused by Software as "Property Damage" Under 2001 CGL Policy
- "Electronic Data" Exclusion Added to 2004 CGL Policy
- Cyber Liability as "Personal Injury"
- Personal Injury Coverage for Telephone Consumer Protection Act of 1991 ("TCPA") Claims
- Person Injury Coverage for Fair Credit Reporting Act of 1970 ("FCRA") Claims
- GL Exclusions for Cyber Liability
- Post-2004 Cyber Liability Endorsements
- CGL Exclusions for "Personal and Advertising Injury" Coverage for Privacy Claims

Cyber & Privacy Insurance Policy
- Backdrop: What is it?
- Type of Coverage Cyber Can Provide
- Who Chooses Third Party Vendors?
- Cyber Sublimits
- Common Cyber Exclusions
- Cyber Policies Overview
- Cyber Insurance Overview
- Cyber Claims?

Underwriting Best Practices

Questions & Answers
Background: Why You Should Care

- Incidents of cyber crime, terrorism and “hactivism” (taking revenge on perceived slights) are rampant today
- Privacy Rights Clearinghouse reported that since 2005 more than 534 million personal records have been compromised
- In 2011, 273 breaches were reported involving 22M sensitive personal records (101M email address records from Sony)
- World Economic Forum’s Global Risks 2012 report, reported cyber attacks as 4th most worrisome risk, behind economic fears and concerns over rising greenhouse gas emissions
- Data security is most prevalent concern for GCs and BODs
Recent Examples

- 2nd largest data breach in U.S. history -- Sony shut down PlayStation online network for a month in 2011 with $200M estimated price tag
- Citigroup targeted in June 2011 by hackers who stole account information from 360,000+ credit card customers
- Other recent cyber attacks reported by:
  - South Carolina Department of Revenue
  - Global Payments
  - Zappos
  - Senate, CIA
  - Fox News Tweet Account (Obama is dead hoax)
  - RSA Security (SecurID tokens) + Lockheed Martin Corp.
  - Bank of America
  - Google (Government employee Gmail accounts in China)
  - PBS (Tupac Shakur alive in New Zealand hoax)

Key Causes of Loss

- Computer hacking/viruses
- Human Error
  - Lost/Stolen laptops, media, smartphone, iPads, backup tapes
  - Improper disposal
  - Employee misuse
  - Vendor negligence
Costs for Loss Generally

- $214/record (3/8/2011 Ponemon Study)
- $7.2M/incident
  - $1-4/person, notification costs
  - $5/call, call center costs
  - $10-50/person, credit monitoring

Discussing Today

1. Regulatory requirements currently governing data breaches
2. Coverage for cyber and privacy related liability under general liability insurance
3. What does a cyber policy cover anyway?
4. Underwriting best practices
REGULATORY REQUIREMENTS

Increasing & Varied Landscape

- Currently no over-arching U.S. federal law mandating data protection or loss notification to regulators or individuals
- Instead there are ad hoc federal and state consumer privacy laws and regulations that are industry based and may contradict
  - i.e. HIPAA, TCPA, FCRA, CAN-SPAM, FACTA, Song Beverly Act
  - Most states require breach notification (not KY, NM, SD, AL)
Federal Law??

- In 2011, over 50 cyber related bills were introduced, including one proposed by Obama.

  Common traits:
  - harsher penalties for computer criminals – adding cyber offenses to RICO, synchronizes computer crime with other crime and sets mandatory minimum prison sentences for cyber intrusions
  - apply to organizations that handle PII of at least 10,000 individuals a year
  - notification required within 60 days
  - pre-empt state laws
  - makes Department of Homeland Security as gatekeeper for cyber security and FTC gatekeeper for data notification

SEC Guidance


  - It “fundamentally changes the way companies will address cyber security in the 21st century”
  - Requires public companies to disclose material cyber risks if they “are among the most significant factors that make an investment in the company speculative or risky”
  - Also Requires disclosure of relevant insurance
States Laws

- States laws vary – how, whom and when to notify. See [www.nymity.com](http://www.nymity.com)
  - CA recently passed an amendment to its regulations, raising the bar on data breaches, that went into effect 1/1/12 (SB24).
  - MA laws very broad and far reaching – require written information security proposal, up to $5,000 per violation
  - 20 states maintain Data Disposal Laws regulating how data destroyed; 30 states have regulations on use/store/protect SSNs

- **State laws make it clear that responsibility lies with company that collected and stored data**

- AGs have broad enforcement powers similar to FTC under state laws – investigate/file suits, order fines/penalties, enforce federal laws (i.e. HIPAA/HITECH), and they have used them

International Scope

- **EU 1995 Data Protection Act** provides personal data should not be processed except in limited circumstances

- However, few international countries currently have breach notice requirements (Japan, Germany). Landscape is shifting:
  - EU e-Privacy Directive 12/09 includes mandatory breach notification, security policy, restricted access to personal data (as of 5/11)
  - 2/12 EU Proposed Directive
What follows is written from a policyholder lawyer’s perspective who:
- counsels policyholders on the need for buying cyber coverage
- negotiates cyber coverage with insurers on behalf of policyholder clients
- negotiates and litigates claims when disputes arise on behalf of policyholders

While you may not agree, it may help you think about your policies to know this perspective
Historical CGL Policies

- Historically known as “comprehensive” general liability
- Known to cover every business liability risk that was not specifically excluded
- Insurers have paid out many claims relating to liabilities they say they never intended to cover and didn’t charge premium for:
  - Asbestos
  - Environmental
  - Intellectual Property
  - Cyber
- Over the years, CGL policy has been narrowed in some ways and newer policies have been written to specifically exclude risks that were previously found to be included in coverage.

CGL Coverage for Cyber Claims

- In general, a commercial general liability (“CGL”) policy provides liability coverage for damages because of:
  - bodily injury or property damage caused by an occurrence (accident); and
  - “Personal and advertising injury” defined as “injury” arising out of certain enumerated offenses, including violation of privacy rights.
- Industry-wide, standardized CGL policy language.
- Amendments to policy definitions of “property damage” and “personal and advertising injury” have limited coverage for cyber or data-related claims.
“Property Damage” Coverage for Data Losses

- Prior to 2001, CGL policies defined “property damage” as follows:
  12. "Property damage" means:
    a. Physical injury to tangible property, including all resulting loss of use of that property. All such loss of use shall be deemed to occur at the time of the physical injury that caused it; or
    b. Loss of use of tangible property that is not physically injured. All such loss shall be deemed to occur at the time of the "occurrence" that caused it.

ISO Form No. CG 00 01 11 88 (emphasis added)

2001 CGL Policy Amended:
Electronic Data is not “Tangible Property”

17. “Property damage” means:
   * * * * *
   For the 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 media which are used with electronically controlled equipment.

ISO Form No. CG 00 01 10 01.
Loss of Use Damages Caused by Software as “Property Damage” under 2001 CGL Policy

- “Loss of use” of tangible property resulting from damage to intangible data or software could be covered
  
  - See, e.g. Eyeblaster, Inc. v. Federal Insurance Co., 613 F.3d 797 (8th Cir. 2010) (coverage for physical injury to computer hardware such as freeze-up (loss of use) caused by spyware)

- Complex, fact-specific issues regarding applicability of “impaired property” exclusion and “property damage” definition

“Electronic Data” Exclusion Added to 2004 CGL Policy

2. Exclusions
   
   This insurance does not apply to:
   *
   *
   *
   *
   *

   q. 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.
      
      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.

ISO Form No. CG 00 01 12 04
Cyber Liability as “Personal Injury”

- 1985 CGL policy defined “personal injury” as follows:
  “Personal injury” means injury, other than “bodily injury,”
  arising out of one or more of the following offenses:
  * * * * *
  Oral or written publication of material that
  violates a person's right of privacy;

ISO Form No. CG 00 01 11 85

- Policy does not define “injury”

Personal Injury Coverage for Telephone Consumer Protection Act of 1991 (“TCPA”) Claims

- The TCPA prohibits “use [of] any telephone facsimile machine, computer, or other device to send an unsolicited advertisement to a telephone facsimile machine.” 47 U.S.C. § 227(b)(1)(C)

- Courts are split on whether sending unsolicited advertisements is “[o]ral or written publication. . . of material that violates a person's right of privacy.”
Personal Injury Coverage for Fair Credit Reporting Act of 1970 (“FCRA”) Claims

- FCRA claims typically involve a consumer alleging that a business has obtained his or her credit information and used that information for purposes not authorized by FCRA
- Several courts have found coverage for FCRA claims because they involved liability because of “[o]ral or written publication . . . of material that violates a person's right of privacy”

GL Exclusions for Cyber Liability

- “Exclusion – Violation of Statutes that Govern E-Mails, Fax, Phone Calls or other Methods of Sending Material or Information”
  (ISO No. CG 00 67 03 05)
- “Recording and Distribution of Material or Information in Violation of Law Exclusion”
  (ISO Form No. CG 68 05 09)
- “Information Distribution and Recording Violations Exclusion”
  (AAIS Form No. GL 1022 09 09)
Post-2004 Cyber Liability Endorsements

- Endorsements broadly eliminated coverage for bodily injury, property damage, or personal and advertising injury arising out of violations of:
  - The Telephone Consumer Protection Act (TCPA);
  - The CAN-SPAM Act of 2003;
  - The Fair Credit Reporting Act (FCRA); and
  - Any other law that “addresses, prohibits or limits the printing, dissemination, disposal, collecting, recording, sending, transmitting, communicating or distribution of material or information”

CGL Exclusions for “Personal and Advertising Injury” Coverage for Privacy Claims

q. Right of Privacy Created by Statute:

“Personal and advertising injury” arising out of a person’s right of privacy created by any state or federal act

However, this exclusion does not apply to liability for damages that the insured would have in the absence of such state or federal act
Backdrop: What is it?

- With other (non cyber) policy lines narrowing coverage relating to internet or privacy claims (i.e. GL fights relating to coverage for Song Beverly Act privacy claims)
- Only 33% of companies currently buy cyber
- Business is booming -- $1 billion market
  - Capacity is strong -- $350M
  - Double-digit premium growth-volume in 2012
  - Compared to EPLI market at $1.4 billion (but cyber around only half as long)
  - $800 in 2011 – up 25% according to Betterly’s 2012 Cyber/Privacy Ins. Market Survey
Type of Coverage Cyber Can Provide

- Third Party Liability – Defense/indemnity relating to:
  - Media Liability/Website Media Content
    - Internet related defamation, intellectual property violation
  - Information, Security and Privacy –
    - theft, loss, unauthorized disclosure of personally identifiable information ("PII");
    - alterations, corruption, destruction, deletion or damage to data
  - Network Security – breach of network security
- Regulatory Action – defense and penalties relating to breach of laws associated with control and use of PII
- Notification and Credit Monitoring Costs – reimburse insured for costs of notification or for credit monitoring for injured people after insured’s loss of their PII

Type of Coverage Cyber Can Provide

- First Party Business Interruption Loss – relating to a network attack (often excluded from property policy)
- Cyber/Network extortion – reimburse insured amounts paid to avert a credible threat to commit or continue a network attack against the insured or to disclose PII for the purpose of obtaining payment
- Crisis Event Management – Public relations costs in dealing with restoring public confidence in insured following material covered event
- Data Forensic/Privacy Breach Response Expenses – reimburse insured for the expenses to determine the cause, source and extent of a network attack following a data breach and possibly fix it
Who Chooses Third Party Vendors?

- Policies generally fall into one of two camps:
  - Those that allow policyholders to choose vendors
  - Those that provide policyholders with a pre-chosen team of vendors
- Vendors include:
  - PR
  - Forensic Investigators
  - Lawyers
- Policyholders often choose what policy to buy based on a match of philosophy as to this issue

Cyber Sublimits

- Cyber Liability limits tend to allow for full aggregate limits
- Policyholders have expressed concern over lower sublimits provided on other Cyber coverages
  - policyholders are counseled to pay close attention here because some issues can be quite costly (i.e. notification and monitoring costs, data forensic costs) and they are looking for higher sublimits or full limits
Common Cyber Exclusions

- Trend appears to be moving toward less exclusions
- Common Exclusions today:
  - Mostly Uninsurable Acts
    - Intentional Bad Acts (if proven)
    - Prior Acts/Prior or Pending Litigation
    - Breach of Contract
    - Anti-Trust
    - War
    - Patent law violation and some other specific IP exclusions
    - Insured v. insured claim
  - Acts Covered by other Policies
    - Pollution/Nuclear
    - Bodily Injury/Property Damage
    - Discrimination/FLSA
    - ERISA
    - D&O/E&O Claim

Common Cyber Exclusions

- Other Exclusions to Pay Close Attn for:
  - Failure of utility service or infrastructure, including internet service
  - Expiration or withdrawal of technical support by software vendor
  - Violation of TCPA or similar federal or state law
  - Failure of software vendor to distribute a patch or other remedy for defect or vulnerability in the software vendor provided, when such defect was known by vendor
  - RICO Claim
  - FTC Claim
  - Wrongful Collection of Data
  - Bad Acts by former or current employees
  - Laptop Exclusion!!!!
Cyber Policies Overview

- A lot of capacity in cyber market
- Biggest growth area for insurers
- Many insurers trying to establish themselves
- Policy coverages differ widely from carrier to carrier
- Room to negotiate terms, price, coverages

Cyber Insurance Overview

- Claims are becoming more and more likely
- Carriers are offering stand alone cyber and seeking to avoid cyber & privacy coverage under other policies
- For those not yet buying cyber insurance, they need to be cognizant that they are self-insuring
- Eventually virtually every company will buy this coverage – starting at low limits and building
Cyber Claims?

- NetDiligence 2012 Study of Payouts (for claims filed between 2009-11) found:
  - PII and PHI most exposed
  - Average claim $3.7M (but skewed because of one large $76M claim)
  - $200,000 typical loss cost
  - Third-Party damages largest component
- Clear that if carriers want to sell more cyber insurance they will need to pay out on claims

Underwriting Best Practices

- Require, incentivize or help policyholders do the following:
  - Put Written Policies and Procedures in Place
    - Strong Password/Encryption Data Requirements
    - Controlling Access – Know Your Data, Minimize and Map it
    - Put Data Breach Protocol in Place
    - Prepare a WISP (written information security plan)
  - Provide Regular Employee Training
  - Suggest that policyholders require vendors to contractually indemnify policyholder and have primary cyber/privacy coverage in place:
    - With required minimum limits
    - Specifies coverages it must include
    - Adding policyholder as an additional insured
  - Encourage monitoring, particularly of data vendors
Question & Answer

Contact Information

Angela R. Elbert, Esq.
Partner
Neal, Gerber & Eisenberg LLP
2 N. LaSalle, Ste. 1700
Chicago, IL 60602
aelbert@ngelaw.com
(312) 269-5995
www.ngelaw.com