Insurance coverage for data breaches, denial-of-service attacks, and cybersecurity events

Scott Godes | Richard Bortnick | Jennifer Smith | William Um | Hon. Carl West
Insurance coverage for data breaches, denial-of-service attacks, and cybersecurity events

Scott N. Godes
Dickstein Shapiro LLP
1825 I Street, NW
Washington, DC 20006
Tel.: (202) 420-3369
godess@dicksteinshapiro.com

corporateinsuranceblog.com
twitter.com/insurancecvg
linkedin.com/in/scottgodes

About the Firm  Dickstein Shapiro LLP, founded in 1953, is internationally recognized for its work with clients, from start-ups to Fortune 500 corporations. Dickstein Shapiro is U.S. News & World Report’s “Law Firm of the Year” for Insurance Law for 2011-2012.
Cozen O'Connor, founded in 1970, delivers legal services on an integrated and global basis, with 575 attorneys in 22 cities and two continents. Their lawyers counsel clients on their most sophisticated legal matters in all areas of corporate and regulatory law as well as litigation.

Richard J. Bortnick
Cozen O'Connor
1900 Market Street
Philadelphia, PA 19103
Tel.: (215) 665-2093
rbortnick@cozen.com

cyberinquirer.com
twitter.com/cyberinquirer
linkedin.com/pub/richard-j-bortnick/1/690/143
Lockton, founded in 1966, is the world’s largest privately owned, independent insurance brokerage firm. Clients across the globe count on Lockton for risk management, insurance and employee benefits. Lockton personnel tailor solutions to the unique needs of each company, organization, and individual just about anywhere. Their long-term relationships with underwriters around the world allow them to structure and negotiate comprehensive coverage at the best price possible.

Jennifer G. Smith
Lockton Companies, LLC
Vice President, Senior Client Advisor, Global Technology & Privacy Practice
1110 Vermont Ave., NW, Suite 700
Washington, DC 20005
Tel: (202) 414-2604
jsmith@lockton.com
	twitter.com/insurancegirldc
linkedin.com/pub/jennifer-g-smith/3/71a/261

About the Firm

Insurance coverage for data breaches, denial-of-service attacks, and cybersecurity events
Hunton & Williams, founded in 1901, represents clients across the full spectrum of industries that make up today's global economy, from manufacturers, financial institutions, retailers, healthcare companies and professional-services providers, to businesses and academic institutions developing renewable energy resources and new technology solutions.

Insurance coverage for data breaches, denial-of-service attacks, and cybersecurity events

William T. Um
Hunton & Williams LLP
550 South Hope Street, Suite 2000
Los Angeles, CA 90071
Tel: (213) 532-2175
wum@hunton.com

linkedin.com/pub/william-um/3/885/780
Insurance coverage for data breaches, denial-of-service attacks, and cybersecurity events

Judge West started his judicial career as a judge of the Los Angeles Municipal Court (1994-1996). From April 2002 to February 2012, Judge West was assigned to the Complex Litigation Panel, and served as the Supervising Judge of the Complex Panel in 2010 and 2011. Judge West is a frequent panelist and lecturer on topics involving complex case management, electronic discovery, toxic torts, and various substantive and procedural topics of interest to civil judges and litigators.
Presentation Overview

1. Exposures to insureds and insurers
2. Regulatory and statutory framework
3. Data breach and privacy class actions
4. Show me the coverage!
Exposures in the areas of technology, cyber security, and privacy

- Types of cases
  - Data Breach Cases (from TJ Maxx to Sony)
  - “Zip Code” Cases (from CA to MA)
  - “Cookie” Cases (from Facebook to Google)
  - Geo-Location Tracking Cases (from iPhones to Androids)
  - Securities Exposure?

- Evolution of underlying cases
  - Establishing “damages”
  - Credit monitoring costs
  - Class action exposure
Types of First-Party Loss

- Hardware or Software Malfunction
- Data Corruption
- Denial of Service Attack
- Extortion
Types of Third-Party Claims and Liabilities

- Copyright/Trademark Infringement
- Data Privacy Breach
- Internet Media Liability (e.g., Defamation)
- Unauthorized Access/Unauthorized Use (e.g., Third Party Data Corruption, Denial of Service Attack)
- Statutory Liability (Federal and State Privacy Laws)
What Is Personal Identifiable Information?

• Depends on law at issue.
• May include any combination of the following:
  – Name; address; telephone number; electronic mail address; fingerprints; photographs or computerized images; a password; an official state or government-issued driver's license or identification card number; a government passport number; biometric data; an employer, student, or military identification number; date of birth; medical information; financial information; tax information; disability information; and zip codes.
Costs of a Data Breach

• 2010 average total cost per incident (among surveyed companies) = $2.4 million to $7.2 million, depending on whose study you read
• 2010 per record cost (among surveyed companies) = $160.00 to $320.00, depending on the cause and impact

Sources: Ponemon Institute and NetDiligence survey
1. This action seeks to redress Defendants’ intentional, willful and reckless violations of the privacy rights of more than 4.9 million individuals, whose private medical and other personal information has been publicly disclosed as a result of Defendants’ violations of the federal Administrative Procedures Act (“APA”) and the federal Privacy Act of 1974 (“Privacy Act”).
Hackers Shift Attacks to Small Firms

By GEOFFREY A. FOWLER and BEN WORTHEN

Recent hacking attacks on Sony Corp. and Lockheed Martin Corp. grabbed headlines. What happened at City Newsstand Inc. last year did not.

Unknown to owner Joe Angelastri, cyber thieves planted a software program on the cash registers at his two Chicago-area magazine shops that sent customer credit card numbers to Russia. MasterCard Inc. demanded an investigation, at Mr. Angelastri’s expense, and the whole ordeal left him out about $22,000.

His experience highlights a growing threat to small businesses. Hackers are expanding their sights beyond multinationals to include any business that stores data in electronic form. Small companies, which are making the leap to computerized systems and digital records, have now become hackers’ main target.

“Who would want to break into us?” asked Mr. Angelastri, who says the breach cut his annual profit in half. “We’re not running a bank.”

With limited resources and few technical experts on staff, small businesses generally have weak security. Cyber criminals have taken notice. In 2010, the U.S. Secret Service and Verizon Communications Inc.’s forensic analysis unit, which investigates attacks, responded to a combined 767 data breaches, up from 141 in 2009. Of those, 482, or 63%, were at companies with 100 employees or fewer. Visa Inc.
Regulatory and statutory framework

- SEC Guidelines, published October 13, 2011
- Federal and state laws require businesses to maintain adequate data security and destroy data with Personal Identifiable Information or Personal Health Information
- Notification statutes require disclosure in certain circumstances where Personal Identifiable Information or Personal Health Information has been obtained by an unauthorized third party
“appropriate disclosures may include: . . . Description of relevant insurance coverage.”
Tidal Wave of Class Actions

• Evolving causes of action and theories of recovery
• Balancing insurance and liability concerns
• Settlements and coverage issues
  – Risk of liability and reasonableness?
  – Payment of plaintiffs’ attorneys’ fees
  – Covered and non-covered claims
  – Bodily injury, property damage, or personal and advertising injury?
  – Credit monitoring?
• Herding cats
  – Multiple plaintiffs’ firms
  – Multiple actions, forums
  – Multiple insurers
Data Breach and Privacy Class Action Issues

• Standing
  – Actual case or controversy?
  – Injury?

• Damages
  – Actual damages?
  – Theoretical damages?
  – Credit monitoring and future expenses?
  – Evolving theories?

• Certification
  – Commonality?
  – Typicality?
Frequent Allegations In a Privacy Breach (Class Action) Lawsuit

- Failure to protect customer information/privacy
- Reduction in value of claimants’ PII
- Failure to notify/timely notification
- Cost to reissue payment cards/open new accounts
- Cost of fraudulent purchases
- Cost to inspect and repair computing devices
- Consumer Redress: credit monitoring/identity theft insurance
- Regulatory Actions: fines and penalties
Notable Recent Underlying Cases

• Defenses Eroding
  – *Stollenwerk v. Tri West* – alleged ID theft
  – ITERA (Identity Theft Enforcement and Restitution Act)
    – “pay an amount equal to the value of the time reasonably spent to remediate intended or actual harm”
  – *In re Hannaford Bros. Data Security Breach Litigation* – does time equal money?
  – *ChoicePoint Data Breach Settlement* – FTC: ChoicePoint paid for “time they may have spent monitoring their credit or taking other steps in response”
Notable Recent Underlying Cases

- **Claridge v. RockYou, Inc.**
  “breach of his PII has caused him to lose some ascertainable but unidentified ‘value’ and/or property right inherent in the PII.”

- **Krottner v. Starbucks Corp.**
  increased risk of identity theft constitutes an injury-in-fact
Show Me the Coverage!

• Coverage under CGL policies?
  – Bodily injury, property damage, or personal and advertising injury?
  – Credit monitoring?

• Other policies?
  – Crime
  – First party
  – EPLI
  – E&O, D&O, K/R/E, others?

• “Cyberinsurance”?
Data security: A growing liability threat

Coverage Under “Traditional” Policies

1. First-party property policies typically cover “all risk” of loss or damage to covered property. However:
   a. Some policies may have exclusions for certain causes of damage to systems; and
   b. The policy may need to be endorsed to cover computer equipment and electronic data.

2. Third-party liability policies such as Commercial General Liability (CGL) policies provide coverage to a company when it issued. Provisions in CGL policies may provide coverage for some types of lawsuits triggered by a data security breach. However:
   a. Some policies may exclude personal or advertising injury arising out of knowingly violating the rights of another and/or personal or advertising injury arising out of publication of material that violates a person’s right of privacy;
   b. Damage to personal property in the care, custody or control of the insured is usually excluded; and
   c. Some policies exclude coverage for electronic data.

3. Errors and Omissions (E&O) policies cover wrongful acts committed in the insured’s performance of professional services. However:
   a. Whether there is coverage for data security breaches depends upon the policy’s definition of the covered professional services.

4. Directors’ and Officers’ Liability (D&O) insurance provides coverage for directors and officers, and usually coverage for the entity, for wrongful acts committed in their capacity as directors and officers of the insured organization. However:
   a. Organization coverage may be limited to securities claims;
   b. D&O policies typically contain exclusions for intentional acts and property damage.

Coverage Under “Traditional” Policies

Commercial General Liability Policies

• Property Damage Coverage
• Personal and Advertising Injury Coverage
• Relevant Endorsements
  – Bodily injury extension?
  – Data coverage?
• In the late 1990s and early 2000s, courts split over whether computer data damage constituted property damage.
Some courts decided that lost computer data was “physical” with “an actual physical location . . . capable of being physically damaged and destroyed.”

Commercial General Liability Policies

Property Damage Coverage – PRO

- Like-minded courts construed “physical damage” beyond “harm of computer circuitry” to encompass “loss of access, loss of use, and loss of functionality.”

Alleged computer freezes, pop-up ads, hijacked browser, random error messages, slowed performance and crashes, and ads based on past surfing habits constitute loss of use.

• Other courts have disagreed that data is tangible camp.

Certain denial-of-service attacks cause physical destruction or alteration of network components.


- Allegations of damage to hardware, or actual evidence of such damage, should trigger property damage coverage, as the claim does not implicate software and data alone.

See, e.g., Eyeblaster, Inc. v. Federal Insurance Co., 613 F.3d 797, 801 (8th Cir. 2010)
Personal and Advertising Injury Coverage

• No property damage requirement.

Accord, e.g., Pipelayers Welfare Educ. Fund v. Westchester Fire Ins. Co., 976 F.2d 1037 (7th Cir. 1992) (policy provision for property damage did not apply to personal and advertising injury coverage, unless written specifically to encompass both coverages); Titan Holdings Syndicate, Inc. v. City of Keene, 898 F.2d 265, 270 (1st Cir. 1990) (same).
Commercial General Liability Policy

Personal and Advertising Injury Coverage

• Usually does not have an “occurrence” requirement and usually covers intentional conduct.

• **One** privacy-related claim in a cyber security or data breach-based complaint could trigger a duty to defend, and may even require coverage of the entire lawsuit.

Zurich American v. Fieldstone Mortgage

- Basis of dispute: Underlying complaint alleged that consumer credit report was accessed without claimant’s consent or permissible purpose under FCRA. Underlying complaint sought seeks statutory damages, injunctive relief, attorney's fees, litigation expenses, and cost of suit, based upon Fieldstone’s “willful[ ]” violation of FCRA.

Zurich American v. Fieldstone Mortgage

Fieldstone and Zurich disputed whether the Personal and advertising injury coverage in commercial general liability policies applied to the claim. “Personal and advertising injury” included injury “arising out of one or more” offenses, including “[o]roral or written publication, in any manner, of material that violates a person’s right of privacy.”

Zurich American v. Fieldstone Mortgage

• “Zurich argues that in order to constitute a publication, the information that violates the right to privacy must be divulged to a third party.” But “the majority [of courts] have found that the publication need not be to a third party.”

✓ Consider Zurich’s argument in the context of a hacking incident or data breach by a third party.

Personal and Advertising Injury Coverage

Netscape v. Federal Insurance (Chubb)

- Personal and advertising injury coverage applied to “claims alleging that AOL had made known to any person or organization material that violated a person’s right of privacy.”
- “Although the underlying claims against AOL were not traditional breach of privacy claims, given that coverage provisions are broadly construed, . . . the underlying complaints sufficiently alleged that AOL had intercepted and internally disseminated private online communications.”

*Netscape Communications Corp. v. Federal Insurance Co.*, 343 F. App’x 271, 272 (9th Cir. 2009).
Check your policy!

• When analyzing the scope of bodily injury coverage in the context of cyber risks, consider whether the definition of “bodily injury” has been expanded to include mental anguish, mental injury, shock, fright, or similar terms.
  – One of the class action complaints filed against Sony alleges that “plaintiff and the Class have suffered damages, including, but not limited to, . . . fear and apprehension of fraud . . . .”
Check your policy!

- Notwithstanding the property damage case law, your CGL policy may provide coverage for data losses. The Insurance Services Office, which drafts standard form CGL policies, created an “Electronic Data Liability” endorsement that provides coverage for loss and loss of use of electronic data resulting from physical injury to tangible property.

Credit Monitoring Coverage?

- Is credit monitoring covered under CGL policies?
- Will insurers argue that they are not damages “because of” bodily injury, property damage, or personal and advertising injury?
  - Consider coverage for analogous concepts, such as medical monitoring. See, e.g., Baughman v. U.S. Liab. Ins. Co., 662 F. Supp. 2d 386, 394-95 (D.N.J. 2009) (medical monitoring costs are damages because of bodily injury).
Other Sources of Coverage

Crime Policy

• Broadly crafted agreements may cover hacking, data breaches, and consumer data theft.
• Check for endorsements for computer fraud, computer theft, or other data breaches.
Other Sources of Coverage

**Crime Policy**

- Computer Funds & Transfer Fraud Endorsement in AIG Crime Policy found to cover hacking and data breach to DSW.

Other Sources of Coverage

**Crime Policy**

- Coverage for “hack, pump, and dump” scheme sought under Computer Systems Fraud Rider/Endorsement to Travelers Financial Institutions Bond.
- Settlement after policyholder won motion to compel.

Other Sources of Coverage

All Risk/First-Party Property Policies

• May provide coverage for data damage, business interruption, and contingent business interruptions due to denial-of-service attacks and data breaches.

Other Sources of Coverage

All Risk/First-Party Property Policies

• May provide coverage for loss under “valuable papers and records” section.

See, e.g., NMS Servs. Inc. v. The Hartford, 62 F. App’x 511 (4th Cir. 2003).
Other Sources of Coverage

**EPLI policies**

- May provide coverage for third-party claims by or on behalf of “Employees” alleging “invasion of privacy” for the unauthorized disclosure of confidential “Employee” information resulting from a data breach or cyber attack.

- Certain EPLI policies provide coverage for “wrongful employment acts,” defined terms that may expressly include “employment-related torts” such as “invasion of privacy” for the unauthorized disclosure of personally identifiable information under HIPAA, credit information under FCRA, criminal records, and other confidential data.
• Consider how broadly the types of “injury” and “wrongful act” are defined.
  – “Sefton alleges that Eyeblaster installed tracking cookies, Flash technology, and JavaScript on his computer, all of which are intentional acts. However, Federal can point to no evidence that doing so is intentionally wrongful.”

Other Sources of Coverage

D&O and Other Coverages

• Study the allegations against the company and other defendants, to determine whether D&O coverage applies.
  – How broadly is Entity Claim defined?
• Depending on the facts, kidnap and ransom policies, Employment Related Practices, or Data Processing policies may supply coverage.
Other Sources of Coverage

**Indemnity Agreements, Additional Insureds**

- Review agreements with vendors and contracting partners to determine whether there are indemnity agreements.
- Determine whether your company may be covered as an additional insured under another company’s policy.
Network Security / Data Risk

- What Data do you collect?
  - Personally Identifiable Info. (PII)
  - Protected Health Info. (PHI)
  - Credit Card Numbers
- Where is it?
- How well is it protected?
- How long do you keep it?
- What is a Breach?
  - Unauthorized disclosure
  - Unauthorized acquisition
  - Data compromised
Typical First-Party Coverages

- Digital Asset Expenses
- Business Interruption Income Loss and Dependent Business Interruption Income Loss Coverage
- Network Extortion Threat and Reward Payments Coverage
Typical Third-Party Coverages

- Network Security Liability Coverage
- Privacy Liability Coverage
- Media Liability Coverage
- Technology Liability Coverage
- Miscellaneous Professional Liability Coverage
Personal and Advertising Injury Coverage

- Cyber privacy claims may implicate personal and advertising injury coverage
  - Right to Privacy
  - Defamation
  - Scope of Publication
  - Social Media
  - Copyright and Trademark Issues
Thank You!

www.poweredtemplates.com