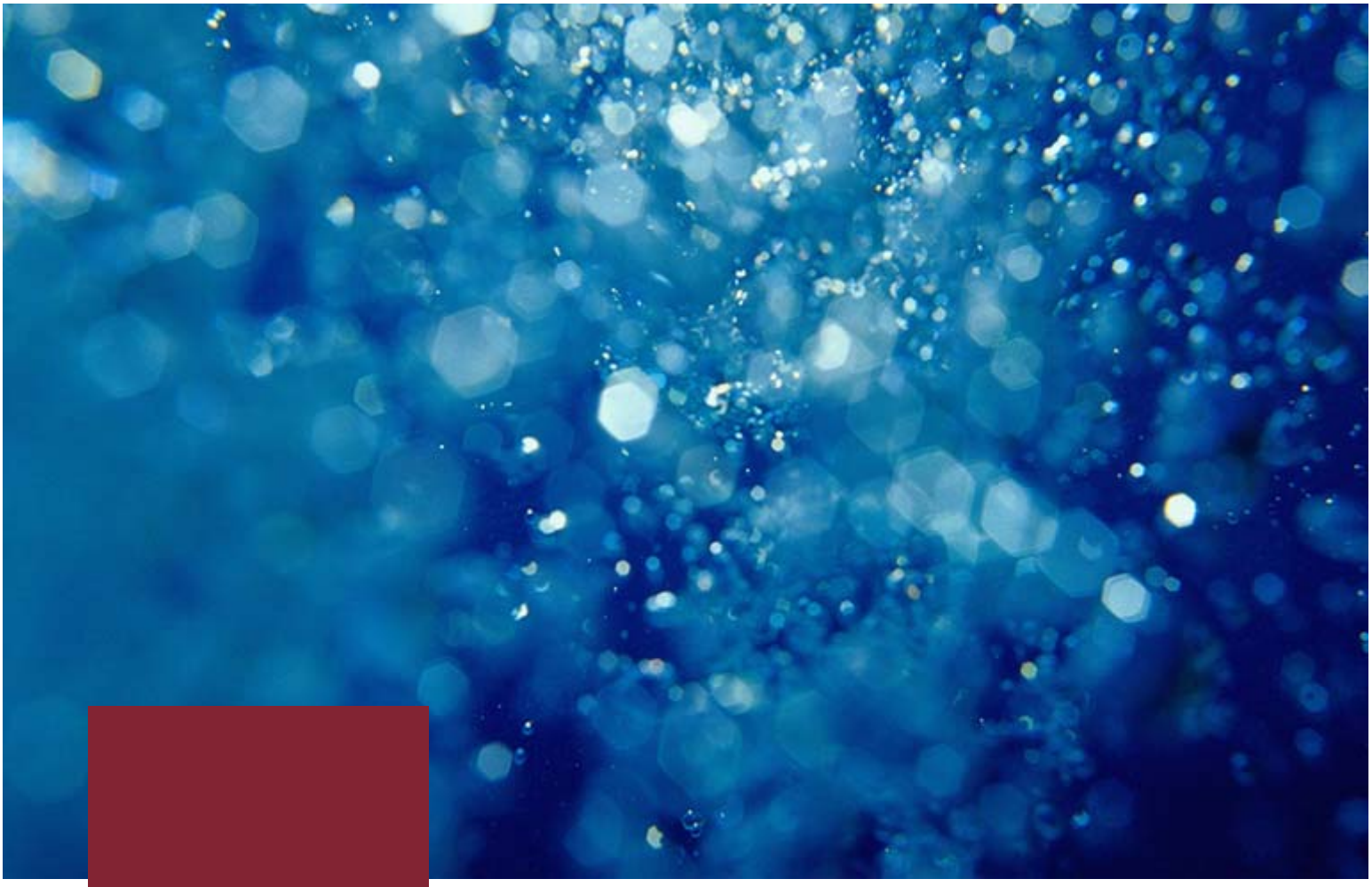


K&L GATES

K&L Gates presents:

"What Your Company Needs to Know About Cybersecurity"

Handout Materials

June 6, 2013

Our Experience

K&L GATES

OUR CYBERSECURITY AND CYBERLAW PRACTICE

Nearly every company is at cyber risk. With distributed denial of service (DDoS), data security breaches, and other attacks on the rise, addressing and mitigating cyber risk is top of mind among companies across the globe. Reports of high-profile cyber attacks make headlines almost every day and the headlines confirm the reality: cyber attacks are on the rise with unprecedented frequency, sophistication, and scale. And they are pervasive across industries and geographical boundaries.

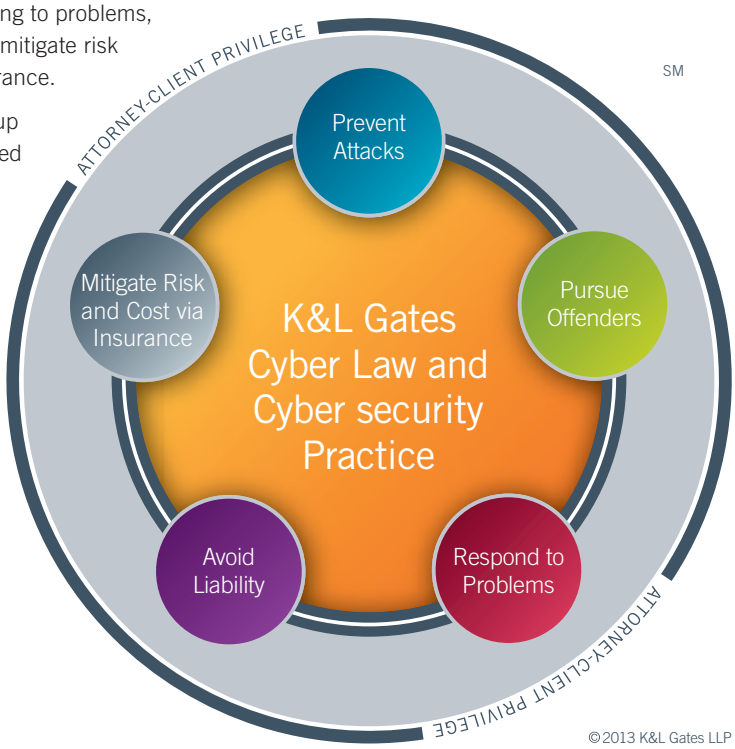
In the wake of more frequent and severe cyber incidents, the Securities and Exchange Commission (SEC) Division of Corporation Finance has issued guidance on cybersecurity disclosures under the federal securities laws and has advised that companies "should review, on an ongoing basis, the adequacy of their disclosure relating to cybersecurity risks and cyber incidents" and that appropriate disclosures may include, among other things, a"[d]escription of relevant insurance coverage."

Amid increased exposure to such risks, companies need assistance in handling security breaches and preventing future cybersecurity threats.

Our Practice

From helping clients to assess network/data security and insurance coverage prior to an attack to dealing with the aftermath of an attack, our international cybersecurity team has deep experience to assist clients with all aspects of addressing and mitigating cyber risks. Our capabilities include preventing and deterring attacks, pursuing perpetrators, responding to problems, and helping clients to mitigate risk and loss through insurance.

Our cybersecurity group includes an experienced federal policy team, cyber forensic investigators with extensive experience in successful internet tracking, a rapid response team to handle active attacks, and experienced insurance coverage counsel, among others. Our team has a unique blend of skills that span various practice areas to help clients deal with cybersecurity issues. We have experience in internet and technology law, legal and regulatory, government regulations, and insurance coverage, as well as established relationships with registrars, internet service providers (ISPs), service providers, and law enforcement.



What We Do

Managing Threats and Attacks

Our cybersecurity team helps manage Internet security and prevent cyber attacks and data breaches through a unique skill set that includes a technical lab and cyber forensic investigators, extensive experience in Internet tracking, and a rapid response team of professionals to deal with current attacks. The team also has experience working with the FBI and IT forensic consultants after attacks.

Legal and Regulatory Risk

Our team works with clients to prepare them for data breaches and minimize their potential legal exposure by drafting internal policies and procedures and contractual provisions regarding discovery, investigation, remediation, and reporting of breaches. We also investigate incidents to determine the scope of a breach and analyze what is required under applicable laws.

Government Regulation and Legislation

Our team has significant experience in government regulation and legislation related to cybersecurities crimes. For more than 20 years, we have advanced information technology issues before the U.S. administrative branch, regulatory agencies, and Congress. We work to ensure that government cybersecurity standards and mandates are industry-led and technology neutral and we have obtained legislation to broaden and strengthen U.S. criminal penalties for cyber crimes. We also led the effort to liberalize export controls on American encryption products and to prevent domestic limitations on the use of encryption.

Insurance Coverage

A complete understanding of a company's insurance program is key to maximizing protection against cyber risk. Our team is skilled in obtaining coverage for various types of cyber risks, considering the adequacy of existing insurance programs, analyzing new insurance products, and drafting and negotiating cyber insurance policy placements.

Our cybersecurity team regularly assists clients with:

- Internet safety
- Privacy, data protection, and information management
- Internal policies
- Employment issues
- Data breach responses
- Analyzing breaches
- Investigating incidents
- International data transfers
- Litigating data security breach actions
- Insurance coverage for data security breaches and other cyber risks
- Contracting with customers, service providers, and affiliates
- SEC disclosures
- Government enforcement actions
- Mergers and acquisitions

"Our team has a unique blend of skills that span various practice areas to help clients deal with cybersecurity issues."

Learn more about our cybersecurity and cyberlaw practice at klgates.com.

11820

Our Lawyers

K&L GATES

Roberta D. Anderson

Partner

Pittsburgh
T 412.355.6222
F 412.355.6501
roberta.anderson@klgates.com

OVERVIEW

Ms. Anderson is a partner in the firm's Pittsburgh office. She has significant experience in complex commercial litigation and alternative dispute resolution. Ms. Anderson concentrates her practice in insurance coverage litigation and counseling. She has represented policyholders in connection with a wide range of insurance issues and disputes arising under almost every kind of insurance coverage, including general liability, commercial property and business interruption, environmental, fidelity, fiduciary, professional liability, directors and officers (D&O), errors and omissions (E&O), employment practices liability (EPL), “cyber”-liability, political risk, fiduciary, terrorism, residual value, nuclear and other insurance coverages, and in broker liability disputes. Ms. Anderson counsels corporate policyholders on ways to maximize the value of their current and historic insurance assets.

Ms. Anderson also counsels clients on complex underwriting and risk management issues, including the drafting and negotiation of D&O, E&O, “cyber”-liability, and other insurance policy placements. She provides strategic insurance coverage advice to clients in assessing their potential risks, analyzing new insurance products and considering the adequacy of their existing insurance programs. Ms. Anderson has performed insurance due diligence for clients contemplating mergers and acquisitions concerning the adequacy of the target companies’ insurance programs. She also counsel clients on risk transfer and representation and warranty insurance in connection with corporate transactions.

Ms. Anderson has served as coverage counsel in a variety of forums, including United States federal and state courts, *ad hoc* arbitration and private mediations. She has acted as special insurance counsel in reorganization proceedings in the United States Court of Appeal for the Fifth Circuit. Ms. Anderson also has participated in arbitrations in leading national and international situses, including London, Bermuda and New York. Ms. Anderson has significant knowledge and experience relating to the London and international insurance markets.

PROFESSIONAL BACKGROUND

Ms. Anderson has published extensively on issues relating to insurance coverage, international arbitration and products liability. She currently serves on a number of editorial boards, including for the Tort Trial & Insurance Practice Law Journal (American Bar Association) and The Insurance Coverage Law Bulletin (American Lawyer Media). She also served on the editorial board of the CGL Reporter (International Risk Management Institute) from 2007 to 2010. Ms. Anderson has spoken on a variety of insurance coverage and litigation practice issues for

Roberta D. Anderson (continued)

American Bar Association (ABA) programs and various local bar association and other professional programs.

Ms. Anderson is a member of both the ABA Litigation Section and the ABA Tort and Insurance Practice Section (TIPS). She currently serves as a Co-Chair of the ABA Section of Litigation's Insurance Coverage Litigation Committee (International/London Subcommittee). She also serves as a Vice-Chair of the ABA TIPS Insurance Coverage Litigation Committee. Ms. Anderson is past Chair of the ABA TIPS Excess, Surplus Lines and Reinsurance Committee (2008-2010) and served as a member of the ABA Public Relations Special Standing Committee from 2010 to 2012.

Ms. Anderson has served as an arbitrator in the Allegheny County Court of Common Pleas, Pennsylvania

PRESENTATIONS

- "Cyber Risk And Insurance" – Insurance Coverage Training Series, September 5, 2012 (Pittsburgh, PA)
- "Finding Balance in the Shifting Sands of Insurance Coverage" – ABA Tort Trial & Insurance Practice Section's Insurance Coverage Litigation Committee's Midyear Program, February 24-26, 2011 (Phoenix AZ)
- "Nuclear-related Liabilities" – Insurance Coverage Training Series, January 7, 2009 (Pittsburgh, PA)
- "Testing the Waters: Discovering the Latest Currents in Insurance Coverage Law: Navigating Current Issues Under E&O and D&O Policies" – ABA Tort Trial & Insurance Practice Section's Insurance Coverage Litigation Committee's Midyear Program, February 28–March 1, 2008 (Marina Del Rey, CA)
- "The Battle Before the Battle: Shifting Sands of Insurance Coverage Seeking Relief from the Changing Winds of Judicial Review" – ABA Tort Trial & Insurance Practice Section's Insurance Coverage Litigation Committee's Midyear Program, February 15–17, 2007 (Tucson, AZ)
- "Challenging the Guidelines & the Carrier's Response" – LexisNexis® Mealeys™ Litigation Management Guidelines Conference, July 20-21, 2006 (New York, NY)
- "Broker Contingent Commissions Investigations" – Risk and Insurance Management Society, April 2005 (Pittsburgh, PA)
- "Getting the Most Out of Lloyd's And Equitas: Basics I: Organization And Terminology" – ABA Litigation Section's Essential Intelligence for US Coverage Lawyers™ Conference, May 14-15, 2002 (Chicago, IL)

PUBLICATIONS

- Insurance Coverage for Cyber Attacks, *The Insurance Coverage Law Bulletin*, Volume 12, Number 4, May 2013

Roberta D. Anderson (continued)

- "The Role of Insurance in the Land of Viruses, Trojans, and Spyware," *Coverage*, Volume 23, Number 1, January-February 2013
- "Key Insurance Coverage Considerations in the Wake of Superstorm Sandy," *The Insurance Coverage Law Bulletin,* Volume 11, Number 12, January 2013
- Chapter 58: USA, *The International Comparative Legal Guide to: International Arbitration*, 2012
- "Recent Developments in Insurance Coverage," 48 Tort Trial & Ins. Prac. L.J. 285, *Tort Trial & Insurance Practice Law Journal*, Fall 2012.
- Chapter 1: Utilizing Recent Case Law to Develop Effective Products Liability Class Action Strategies, *Litigating Products Liability Class Actions (Inside the Minds Series)*, Aspatore Books, November 2011
- "The Calm Before a Storm of Claims: Identifying and Preserving Insurance Coverage for Hurricane Irene-Related Losses," *The Insurance Coverage Law Bulletin*, Volume 10, Number 9, October 2011
- Losses from Hurricane Irene: Are You Covered?, *Insurance Coverage Alert*, August 30, 2011
- "ICC To Unveil New Rules of Arbitration," *Arbitration World*, August 2011
- Chapter 51: USA, *The International Comparative Legal Guide to: International Arbitration*, 2011
- "Recent Developments in Insurance Coverage Litigation," 47 Tort Trial & Ins. Prac. L.J. 297, *Tort Trial & Insurance Practice Law Journal,* Fall 2011
- " 'Cyber-Attacks': Important Insurance Coverage Considerations," *Insurance Coverage Alert*, June 30, 2011
- "Disaster in Japan: Worldwide Insurance Coverage Considerations," *Insurance Coverage Alert*, March 16, 2011
- "Recent Developments In Excess Insurance, Surplus Lines Insurance, And Reinsurance Law," 45 Tort Trial & Ins. Prac. L.J. 329, *Tort & Insurance Practice Law Journal*, Winter 2010
- "The UAE's Proposed Federal Arbitration Law," *Arbitration World*, October 2010
- "Recent Developments Concerning Dubai Ruler's Decree 57 of 2009," *Arbitration World*, May 2010
- "International Arbitration in the UAE and the Middle East Region: Recent Developments," *Arbitration World*, February 2010
- "Insurance Recovery For Dubai Credit Default Losses," *Insurance Coverage Alert*, December 11, 2009
- "Protocol of Enforcement Affords Reassurance on Enforcement of DIFC-LCIA Arbitral Awards and DIFC Judgments Beyond DIFC Boundaries," *Arbitration World*, October 2009

Roberta D. Anderson (continued)

- "Proposed Part VII Transfer of Liability on Lloyd's Policies: Considerations for Lloyd's Policyholders," *Insurance Coverage Alert*, May 22, 2009
- "Recent Pennsylvania Legislative And Judicial Developments Favor Policyholders Asserting Statutory And Common Law Bad Faith Claims," *Mealey's litigation Report: Insurance Bad Faith*, November 2007
- "Potential Business Interruption Coverage: July 18, 2007 Manhattan Steam Pipe Explosion," *Insurance Coverage Alert*, August 31, 2007
- "The Emergence of Prejudice As a Necessary Element of an Insurer's Late Notice Defense: An Analysis of NY Law," *The Insurance Coverage Law Bulletin*, August 2007
- "Pennsylvania Supreme Court Rules On Assignments," *The Insurance Coverage Law Bulletin*, February 2007
- "Proposed Equitas Transaction with Berkshire Hathaway: What Does It Mean for Lloyd's Policyholders?," *Insurance Coverage Alert*, January 2007
- "Recent Developments In Excess Insurance, Surplus Lines Insurance, and Reinsurance Law," 41 Tort Trial & Ins. Prac. L.J. 393, *Tort & Insurance Practice Law Journal*, Winter 2006
- "Insurance Coverage for Investigations and Demands of State Attorneys General," *Insurance Coverage Alert*, September 2005
- "Upheaval in the Insurance Industry: Potential Implications for Policyholders," *Practical Law Company Cross-Border*, April 2005
- "Marsh Settles Spitzer Charges For $850 Million," *Insurance Coverage Alert*, February 2005
- "A Timely Lesson From The WorldCom And Enron Settlements: Make Sure Your D&O Program Is Adequate," *Insurance Coverage Alert*, January 2005
- "Insurance Industry Bid-Rigging/Steering Scheme Allegations Demand Policyholder Attention," *Insurance Coverage Alert*, October 2004
- "Insurance Coverage For Silica Claims," *The Insurance Coverage Law Bulletin*, August 2004
- "Insurance Coverage For Inside Corporate Counsel: A Topic Of Increasing Interest," *Insurance Coverage Alert*, April 2004
- "Expanding Risk: Directors' and Officers' Coverage is Shrinking Just When People Need It Most," *Legal Times*, February 17, 2003
- "Insurance Coverage For *Mandolidis*-Type Claims," *Insurance Coverage Update*, February 2003
- "Proposed Life Insurance Employee Notification Act, *Corporate Alert*, February 2003
- "Insurance Coverage for Natural Resource Damages," *Insurance Coverage Alert*, January 2003
- "Terrorism Risk Insurance Act of 2002," *Insurance Coverage Alert*, December 2002

Roberta D. Anderson (continued)

- "*Lititz Mutual Insurance Co. v. Steely*. Pennsylvania Supreme Court Takes a Second Look at the Absolute Pollution Exclusion," *Journal of Insurance Coverage*, Summer 2002
- "Threatened Equitas Insolvency: Is The Lloyd's "Chain of Security" Really Secure?" *Journal of Insurance Coverage*, Summer 2002
- "Bankruptcy Court Rules The Babcock & Wilcox Company Solvent At Time Of Asset Transfer," *K&L Update*, Spring 2002
- "Insurance Facts Businesses Should Know In The Wake of September 11," *Journal of Investment Compliance*, Winter 2002
- "The Absolute Pollution Exclusion in Pennsylvania Post-*Madison*: Intermediate Appellate Courts Resume the Debate," *Journal of Insurance Coverage*, Autumn 2001
- "Pennsylvania High Court Hands Down Long-Awaited Sunbeam Decision" *Insurance Coverage Alert,* October 2001
- "Policy Matters: Insurance Facts of Life Every IT Leader Should Know," *Best Practices In IT Leadership*, October 2000
- "Insurance Coverage for 'Cyber-Losses,'" 35 Tort & Ins. L. J. 891, *Tort & Insurance Law Journal*, Summer 2000
- "Is it Still Possible to Litigate Against Lloyd's in Federal Court?," 34 Tort & Ins. L. J. 1065, *Tort & Insurance Law Journal*, Summer 1999
- "California High Court Hands Down Two Pro-Insurer Split Decisions on Environmental Coverage Issues: *Foster-Gardner, Inc. v. National Union Fire Insurance Co. and Aydin Corp. v. First State Insurance Co.*," *Journal of Insurance Coverage*, Winter 1999

PROFESSIONAL/CIVIC ACTIVITIES

- United Way of Allegheny County
  - United Way Tocqueville Committee (2012 to present)
  - United Way Young Leaders Group (Member, 2000 to present; Committee Member, 2001; Co-Chair, 2002; Philanthropy Sub-Committee, 2006)
  - United Way Women's Leadership Initiative (Member, 2001 to present)
  - United Way Campaign Cabinet (2002)
- Allegheny Conference on Community Development (Athena Award Program Host Committee, 2004 to 2010)
- Downtown Pittsburgh YMCA (Board of Management, 2004 to 2010; Advisory Committee, 2010 to present)
- University of Pittsburgh Law Chancellor's Circle
- University of Pittsburgh Law Fellows
- American Bar Association (Litigation and Tort and Insurance Practice Sections)

Roberta D. Anderson (continued)

- Allegheny County Bar Association (Civil Litigation Section)
- Pennsylvania Bar Association (Civil Litigation Section)
- University of Pittsburgh School of Law Murray S. Love Mock Trial Competition Judge (2011 and 2012)
- University of Pittsburgh School of Law 2008 Alumni Reunion Class Representative

ADMISSIONS

- Pennsylvania
- Supreme Court of Pennsylvania
- U.S. Courts of Appeal for the Fifth and Tenth Circuits
- U.S. District Court for the Western District of Pennsylvania
- Numerous *pro hac vice* admissions in various state and federal courts

EDUCATION

J.D., University of Pittsburgh School of Law, 1998 *(magna cum laude,* Order of the Coif; Managing Editor, *University of Pittsburgh Law Review,* Faculty Award For Excellence In Legal Scholarship; CALI Excellence for the Future Award®)

B.A., Carnegie Mellon University, 1994 (*cum laude*)

REPRESENTATIVE EXPERIENCE

Insurance Coverage Litigation and Arbitration

Ms. Anderson has significant experience in complex commercial litigation with a substantial focus on the litigation, trial, appeal, arbitration and mediation of insurance coverage disputes. Representative matters include:

- Briefed, argued and secured a precedent-setting victory on behalf of the policyholder in a landmark decision concerning insurance coverage for losses caused by a mechanical equipment failure. The suit successfully challenged the applicability of the standard-form "your work," "your product," product recall, and "impaired property" business risk exclusions that are typically contained in commercial general liability insurance policies and that are frequently relied upon by insurers. *Washington Energy Co. v. Century Sur. Co*., 407 F.Supp.2d 680 (W.D.Pa. 2005). Reported in *Risk & Insurance*, May 2006.
- Represented the policyholder in a landmark decision concerning insurance coverage for claims alleging injuries resulting from exposure to radioactive emissions from nuclear fuel processing facilities. The suit successfully challenged the insurer's approach to the "trigger of coverage" and the scope of its defense obligations. As part of the same case, a jury awarded $80 million for settlements entered into without the insurer's consent. *The*

Roberta D. Anderson (continued)

Babcock & Wilcox Company, et al. v. American Nuclear Insurers, et al., No. 1916 WDA 2001, 2002 WL 31749119 (Pa. Super. Ct. 2005), *aff'g* 51 Pa. D. & C.4th 353 (Pa. Com. Pl. 2001), *appeal denied*, 829 A.2d 350 (Pa. 2003). Reported in *Business Insurance*, December 2002.

- Represented a worldwide oil and gas exploration and production company regarding recovery under its Bermuda Form excess liability insurance policies in connection with underlying class action litigation alleging property damage relating to a Hurricane Katrina related crude oil spill at a refinery. Following the initiation of London-seated arbitration proceedings and a first partial award, the case settled favorably as to three of the four insurers. Following a final hearing on the merits, the arbitration panel ruled in favor of the policyholder on all issues.
- Represented one of the four largest U.S. bank holding companies regarding recovery under its financial institution bonds/fidelity policies in connection with a substantial employee theft loss. Following the initiation of litigation, submission of proofs of loss and successful mediation, the case settled favorably.
- Represented one of the largest U.S. diversified financial institutions regarding recovery under its vehicle residual value insurance policy. The case settled favorably on the eve of trial for a mid-nine figure recovery.
- Represented one of the world's three largest producers of aluminum regarding recovery under its general liability insurance policies in connection with underlying claims alleging property damage to boats and other seafaring vessels arising out of the distribution of an aluminum alloy.
- Represented a provider of health benefit plans regarding recovery under its excess loss mitigation insurance policies in connection with the settlement of underlying securities class action lawsuits. Following the initiation of litigation and mediation, the case settled favorably.
- Represented an energy-sector policyholder regarding recovery under its pollution insurance policy in connection with the remediation of a former nuclear fuel processing facility. Following the initiation of litigation and discovery, the case settled favorably.
- Represented a private equity investment firm regarding recovery under its professional liability insurance policy in connection with underlying litigation alleging breach of a merger agreement. Following the initiation of New York-seated arbitration proceedings, discovery and successful briefing on disputed coverage issues, the case settled favorably.
- Represented a group self-insurance fund policyholder regarding recovery under its crime/fiduciary policy in connection with a substantial employee theft loss. Following the initiation of litigation, discovery and successful briefing on disputed issues, the case settled favorably.

Insurance Coverage Counseling

Ms. Anderson has counseled policyholders in connection with a wide range of insurance issues and disputes, from disaster, environmental, products liability, asbestos, nuclear, political risk and

Roberta D. Anderson (continued)

business interruption losses to disputes arising under D&O, E&O, and fiduciary liability policies and many others. A list of representative matters is available on request.

Insurance Coverage Due Diligence

Ms. Anderson has performed insurance due diligence for clients contemplating mergers and acquisitions concerning the adequacy of the target companies' insurance programs. Representative matters include:

- Counseled an energy-sector client in assessing key coverage terms and conditions, including sufficiency of limits, of a target company's nuclear, pollution legal liability, commercial general liability and property insurance policies prior to acquisition.
- Counseled a non-profit client in assessing key coverage terms and conditions, including change-in-control, anti-assignment, cancellation provisions, and extended reporting and tail coverage options, of a target's commercial general liability, D&O, E&O, professional liability and workers' compensation/employers' liability policies prior to merger.

Insurance Coverage Negotiation and Placement

Ms. Anderson has counseled clients on complex underwriting and risk management issues, including the drafting and negotiation of D&O, E&O, "cyber"-liability, and other insurance policy and blended program placements. Representative matters include:

- Represented one of the five largest U.S. banks in structuring and negotiating the terms of its cyber insurance program.
- Represented the world's largest private operator of health care facilities in assessing and negotiating the terms of its cyber and professional liability insurance program.
- Represented a Fortune 500 retailer in assessing and negotiating the terms of its cyber insurance policies.
- Represented an online travel/entertainment client in assessing and negotiating the terms of its cyber insurance policies.
- Represented one of the world's four largest media conglomerate's in structuring and negotiating the terms of its D&O insurance program.

K&L GATES

David A. Bateman

Partner

Seattle
T 206.370.6682
F 206.370.6013
david.bateman@klgates.com

OVERVIEW

David Bateman is a trial lawyer and focuses on the cutting edge of Internet law, technology law, and intellectual property litigation. With 20 years of experience in technology and intellectual property law, David represents clients in high profile litigation matters, and provides counseling to technology clients in business deals and lobbying efforts.

David consults with clients regarding all types of cyberlaw issues, including online brand protection, digital rights management, privacy, electronic communications, and Internet commerce. A nationally recognized leader in Internet, e–commerce, and software litigation, he has been lead counsel in hundreds of lawsuits against spammers, software pirates, phishers, cybersquatters and other Internet malefactors. He is a frequent speaker on the protection of computer systems, trade secrets and intellectual property, and has designed programs for protection of trade secrets and technology.

David's litigation practice has grown in step with rapid developments in technology and e–commerce. He has worked with online retailers, wireless carriers, internet service providers, software developers and hardware manufacturers to create, protect and defend their intellectual property and technologies. He has worked cooperatively with major ISPs, industry participants, and state and federal government agencies in the battle against online consumer deception and fraud. In addition, he has defended clients in class action lawsuits and agency investigations regarding consumer complaints, technology disputes, and trademark infringement.

PRESENTATIONS

- “Fighting Cybersquatting and Phishing – A New Tool to Protect Your Customers and Brands,” Privacy & Data Security Law Journal, November 2007
- “What The Tech Industry is Doing About Phishing,” National Association of Attorneys General Conference, August 2007
- “Getting Control of Spam: Challenges and Solutions,” UW Business School, Northwest eBusiness 2005, Seattle, WA
- “Internet Update – Spam,” 19th Annual Computer & Information Law Institute, Dallas, Texas, 2004
- “Spam Law 101,” Adjunct Professor, University of Washington Law School, Seattle, WA, 2004

David A. Bateman (continued)

- “Lessons from Recent Litigation,” Doing Business Online: Electronic Marketing Conference, Seattle, WA, 2003

ADMISSIONS

- U.S. District Court for the Eastern District of Washington
- U.S. District Court for the Western District of Washington
- Washington

EDUCATION

J.D., Yale Law School, 1984

B.A., Yale University, 1980 (summa cum laude; Phi Beta Kappa)

REPRESENTATIVE WORK

- Served as lead trial lawyer in Microsoft's nationwide Internet safety and security litigation efforts, heading programmatic litigation in spam, phishing, spyware, click-fraud and malvertizing enforcement.
- Served as lead trial lawyer for major online retailers in domain name defense efforts and cybersquatting litigation.
- Filed first civil action under federal CANSPAM Act
- Obtained $3.4 million judgment against spyware distributor
- Defended software manufacturer in consumer class action alleging Computer Fraud and Abuse Act violations and spyware claims
- Represented music publishers and software manufacturers managing national, programmatic copyright infringement and piracy litigation
- Served as lead counsel for technology company in successful bench trial to protect trade secrets and enforce employee non–compete agreement
- Defended local start–up company in trade secret and non–compete litigation
- Represented national mobile phone service provider in employee theft litigation.
- Defeated class certification of anti–spam allegations brought by consumers against national retailer of copier and printer products
- Defended national insurer in class action lawsuit involving allegations relating to consumer credit insurance.
- Defended securities issuer in class action securities litigation and derivative suit. Obtained sanctions against class representative and class counsel.
- Represented ticketing agency in class action litigation brought by disappointed Michael Jackson fans.

David A. Bateman (continued)

ACHIEVEMENTS

Recognized as a Washington *Super Lawyer*, 2004-2012

K&L GATES

Bruce J. Heiman

Practice Area Leader – Policy/Regulatory

Washington, D.C.
T 202.661.3935
F 202.778.9100
bruce.heiman@klgates.com

OVERVIEW

For over 20 years, Mr. Heiman has engaged in a wide-ranging federal counseling and lobbying practice on behalf of leading clients in the computer software, information technology and telecommunications industries. He also assists a range of companies understand the laws and policies applying to their Internet and e-commerce activities. He is one of two Practice Area Leaders of K&L Gates' Policy and Regulatory Practice and serves on the firm's Management Committee.

Mr. Heiman is a recognized authority on cyber security and privacy policy issues. He was counsel to the private sector coalition that led the fight to liberalize export controls on American encryption products. He currently is working with a leading trade association to ensure that efforts to promote cyber security and protect critical information infrastructure are market-driven and industry-led.

He has been actively involved in formulating practicable privacy policies, protecting intellectual property rights, and improving the delivery of government services while preventing unfair competition with the private sector.

He has long opposed governmental regulation of the Internet and technological mandates and was instrumental in ensuring that information services and ISP's were not treated like telecommunications services and carriers (CALEA in 1994; the Telecommunications Act of 1996; the PATRIOT Act of 2001).

Mr. Heiman was profiled by *Tech Counsel* Magazine as one of the leading high-tech lobbyists in Washington and has been quoted on info-tech issues in *The Washington Post, New York Times, Wall Street Journal, National Journal, Congressional Quarterly, Legal Times* and *Tech Daily*. He has spoken to the RSA Security Conference, the ABA Committee of Corporate General Counsel and the Congressional Internet Caucus.

From 1984 to 1987, he served as legislative director and trade counsel to U.S. Senator Daniel Patrick Moynihan of New York.

PUBLICATIONS

- "Patent-Infringement Remedy Needs Supreme Court Tuneup," (with Paul Stimers), San Jose Mercury News, February 9, 2006
- "Who Steals My Name? The US and EU Response to Data Security Breach," (with Donald A. Cohn and Jonthan P. Armstrong), ACC Docket, June 2006

Bruce J. Heiman (continued)

- "Data Breach Notification and Cybersecurity Standards in the U.S. and E.U." (with Jonathan P. Armstrong), BNA International's World Internet Law Report, December 2005
- "At Risk: a Secure Net," Legal Times, week of August 14, 2000
- "Internet is Ripe for Government Intervention," Los Angeles Times, April 6, 2000

PRESENTATIONS

- "The Year of Location Privacy?", RSA Conference, San Francisco, CA, March 1, 2013
- "Cybercrime: The Identity Theft Enforcement and Restitution Act, and Beyond," RSA Conference, San Francisco, CA, April 23, 2009
- "Three Rules of Data Security," Hispanic National Bar Association Continuing Legal Education meeting, Washington, D.C., October 15, 2005
- "Cyber Security – The Right Way," Center for Strategic and International Studies Forum, January 2004
- "Cyber Security Regulation is Here!," 12th Annual RSA Security Conference, April 15, 2003
- "Cyber Security: What Consumers & Government Should Do," FTC Consumer Information Security Workshop, May 20, 2002
- "The Right Way to Promote Cyber Security," 11th Annual RSA Security Conference, February 19, 2002

ADMISSIONS

- District of Columbia

EDUCATION

J.D., Harvard Law School, 1980

M.P.P., John F. Kennedy School of Government, Harvard University, 1980

B.A., Brandeis University, 1976 (magna cum laude)

Additional Materials

Insurance Coverage Litigation
January-February 2013, Vol. 23 No. 1

ARTICLES

The Role of Insurance in the Land of Viruses, Trojans, and Spyware

By Roberta D. Anderson[1] – February 26, 2013

There's no denying that the present-day Internet, while extraordinary, is increasingly scary. Cyber attacks of various types continue to escalate across the globe. As stated by one recent commentator, "Cybercrime is raging worldwide."[2] Reports of high-profile cyber attacks make headlines almost every day. In recent weeks and months, sophisticated distributed denial-of-service attacks on at least 26 of the largest U.S. banks reportedly breached some of the nation's most advanced computer security, rendering bank websites unavailable to customers and disrupting transactions for hours at a time.[3]

The headlines confirm the reality: Cyber attacks are on the rise with unprecedented frequency, sophistication, and scale. And they are pervasive across industries and geographical boundaries.

Even though no organization is immune from cyber attacks, it is uncertain that companies are sufficiently aware of the escalating onslaught.[4] Even companies that are sufficiently aware of the problem might not be sufficiently prepared. It is abundantly clear that network security alone cannot entirely address the issue. As noted by one observer, "[t]here is no fail-safe technology that is immune to hacking. Online security will evolve as hackers and security experts work continuously to outwit each other."[5] Insurance can play a vital role. Yet, some companies may not be adequately considering the important role of insurance as part of their overall strategy to mitigate cyber risk. A recent 2012 survey conducted by global consulting firm Towers Watson reports that 72 percent of the 153 risk managers of North American companies surveyed "ha[d] not purchased network security/privacy liability policies."[6] And those companies that did purchase policies "opted for limits that were on the low end of the spectrum."[7] In addition, risk managers and in-house counsel may not be aware if, and to what extent, the company already has coverage for cyber risks under existing "traditional" insurance policies, many of which cover cyber risks.

A complete understanding of the company's insurance program is key to maximizing protection against cyber risk. Indeed, in the wake of the recent attacks, the Securities and Exchange Commission has issued guidance on cybersecurity disclosures under the federal securities laws and advises that "appropriate disclosures may include," among other things, a "[d]escription of relevant insurance coverage."[8]

In view of the cyber risks and realities, companies should carefully examine their insurance programs, evaluate what coverage already may be available, and see what

may be done to enhance the available coverage. To the extent there may be gaps in available coverage, companies should consider how those gaps can be filled, including through specialty cyber risk policies.

Cyber Criminals Seize the Day—and the Data

The past two years have seen some of the world's most sophisticated corporate giants fall victim to different types of serious cyber attacks. These attacks have included some of the largest data breaches in history[9] and affected online gaming providers, marketing services firms, retailers, the health care industry, banks, insurers, defense contractors, social networking sites, cloud storage providers, credit card processors—even sophisticated security firms.[10] The Privacy Rights Clearinghouse reports that as of January 1, 2013, 605,742,951 records have been breached in 3,539 data breaches made public since 2005.[11] The organization notes that the number . . . should be much larger" because it is "not a comprehensive compilation" and "[f]or many of the breaches listed, the number of records is unknown."[12]

The escalating cyber attacks are not limited to data breaches of course—they also include expensive distributed denial-of-service attacks, such as the recent attacks that targeted the financial services sector, and myriad other types of cyber threats, including attacks principally designed to destroy or corrupt data, and cyber extortion. The Ponemon Institute's recent *2012 Cost of Cyber Crime Study* concludes that "companies expend considerable time and resources responding to a plethora of different types of attacks."[13] According to the recent study "[c]yber attacks have become common occurrences" with the 56 organizations involved in its survey experiencing "102 [overall] successful attacks per week and 1.8 successful attacks per company per week."[14] The study notes that this represents an increase of 42 percent over the "successful attack experience" reflected in its prior August 2011 study.[15]

The problem of cyber risks is exacerbated not only by increasingly sophisticated cyber criminals and malicious code and other types of malware—which, in the case of the recent distributed denial-of-service attacks, was described as "10 times as potent as the types of denial-of-service attacks hackers have mounted in the past"[16] —but also by the reality of the modern business world, which is full of portable devices, including cell phones, laptops, iPads, USB drives, jump drives, media cards, tablets, and other devices that facilitate the loss of sensitive information.[17] The Ponemon Institute's recent *2013 State of the Endpoint* study finds that "[o]ne of the top concerns is the proliferation of personally owned mobile devices in the workplace such as smart phones and iPads" and that "data-bearing devices pose a significant security risk to their organization's networks or enterprise systems because they are not secure."[18]

Cyber Attack Costs Are on the Rise

As the incidence of cyber attacks escalates, the cost associated with attacks is also increasing. In data breach cases, for example, companies may incur substantial

expenses relating to federal and state notification requirements.[19] Companies may also face governmental and regulatory investigations, fines and penalties, and lawsuits seeking damages for lost or stolen data, invasion of privacy, misappropriation of intellectual property or confidential business information, or other consequences of a data breach. Even if not ultimately successful, such lawsuits can be extremely costly to defend. Companies also may incur significant expenses associated with retaining forensics experts and assuaging and attempting to maintain customers and curtailing damage to reputation, including by providing credit monitoring services to affected individuals and retaining public relations consultants.

In its seventh annual *Cost of Data Breach Study* published in March 2012, the Ponemon Institute noted that "data breaches continue to have serious financial consequences for organizations."[20] The study found that despite a slight decline in the average organizational cost of a data breach "from $7.2 million to $5.5 million" (and in the cost per stolen record "from $214 to $194"),[21] certain costs increased, including "[t]he costs to notify victims of the breach."[22] It also is important to note that the study does not include organizations that had data breaches involving more than 100,000 records because they "are not representative of most data breaches and including them in the study would skew the results."[23] But the incidents of large-scale breaches are on the rise. The 2011 high-profile attack on the Sony PlayStation Network alone was estimated to cost some $170 million.[24] This does not include potential compensation to claimants. Some experts say that the final tally could exceed $2 billion.[25]

Even in cyber attack cases in which sensitive information is not actually or potentially compromised, a company may experience substantial business interruption and related losses if online systems or websites are disabled by—or disabled in order to address—a cyber attack. A company also may incur damage to the company's computers, networks, and data, in addition to costs to update and fix any flaws in its security systems. These examples of potential costs and losses are far from exhaustive. The Ponemon Institute's *2012 Cyber Crime Study* found that "the average annualized cost of cyber crime for 56 organizations in [its] study is $8.9 million per year, with a range of $1.4 million to $46 million."[26] This number is up from the $8.4 million average annualized cost reflected in the 2011 survey.

It is clear that attacks and associated costs are on the rise. And insurance can play an important role in mitigating the problem.

Traditional Coverage under Commercial General Liability Policies

While some companies carry specialty insurance policies that are specifically designed to afford coverage for cyber risk, many companies have various forms of traditional insurance policies that may cover cyber risks, including commercial general liability (CGL) coverage. CGL policies generally cover the company against liability for claims alleging bodily injury and/or property damage under Coverage A and also against liability for claims alleging personal injury and/or advertising liability under Coverage B.

Although insurers typically argue that cyber risks are not intended to be covered under CGL policies (or other traditional types of insurance coverages), insureds pursuing coverage under CGL policies have met with some, albeit not universal, success as described below. Coverage in a particular case necessarily will depend on the specific facts of each case, the terms, the conditions and exclusions of each individual policy, and the applicable law.

A brewing legal dispute between Sony and one of its insurers concerning the PlayStation Network data breach highlights the challenges that companies can face in getting insurance companies to cover losses arising from cyber risks under CGL policies. In *Zurich American Insurance Co. v. Sony Corp. of America*,[27] the insurer seeks a declaration that there is no coverage under the CGL policies at issue on the basis that the underlying lawsuits arising from the cyber attacks "do not assert claims for 'bodily injury,' 'property damage,' or 'personal and advertising injury.'"[28] The Sony coverage litigation may provide additional guidance on the scope of coverage for data breaches and other cyber risks under traditional CGL policies. In the meantime, the current case law is instructive.

Potential CGL Coverage for Electronic Data as "Property" Subject to Damage

The main coverage part of the current standard form Insurance Services Office, Inc. (ISO) CGL policy form states that the insurer "will pay those sums that the insured becomes legally obligated to pay as damages because of 'bodily injury' or 'property damage'"[29] that "occurs during the policy period."[30]

One potential issue in cyber risk cases is whether the definition of "property damage" is satisfied. A standard form definition of "property damage"[31] includes "[p]hysical injury to tangible property, including all resulting loss of use of that property" and "[l]oss of use of tangible property that is not physically injured."[32] The standard form further states that the insurer "will have the right and duty to defend the insured against any 'suit'" seeking potentially covered damages.[33]

Insurers typically argue that data are not tangible property that can suffer physical injury and, therefore, are not susceptible to property damage. However, a number of courts have held that damaged or corrupted software or data are tangible property that can suffer physical injury. For example, the Court of Appeals of Minnesota in *Retail Systems, Inc. v. CNA Insurance Co.*[34] found that "data on [a] tape was of permanent value and was integrated completely with the physical property of the tape."[35] On this basis, the court held that both "the computer tape and data are tangible property"[36] and, therefore, can be the subject of covered property damage.

Consistent with the holding in *Retail Systems*, the District of Arizona in *American Guarantee & Liability Insurance Co. v. Ingram Micro, Inc.*[37] held that electronic data can suffer "physical injury":

> At a time when computer technology dominates our professional as well as personal lives, the Court must side with [the insured]'s broader definition of "physical damage." The Court finds 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.[38]

In support of its holding, the *Ingram Micro* court cited various state and federal laws that make it a crime to cause "damage" to computer hardware or data, noting that "[l]awmakers around the country have determined that when a computer's data is unavailable, there is damage; when a computer's services are interrupted, there is damage; and when a computer's software or network is altered, there is damage."[39]

Other courts likewise support an argument that data are tangible property. The decisions are not uniform, however, and some courts have held that computer data are not tangible property and therefore not susceptible to property damage. [40] A leading insurance law authority notes that the issue as to whether "computerized information is tangible property" has "not been satisfactorily resolved."[41]

One potential hurdle for insureds is that the current ISO standard form policy and other ISO standard form policies written or effective on or after December 1, 2001, expressly exclude electronic data from the definition of "property damage."[42] In addition, policies written or effective on or after December 1, 2004, expressly exclude "[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."[43]

These provisions may not vitiate coverage however. For example, the ISO Electronic Data Liability Endorsement adds electronic data back to the definition of "property damage."[44] Standard form ISO policies written or effective on or before December 1, 2001, moreover, do not except electronic data from the definition of property damage[45] and do not exclude electronic data. Even recently issued policies may not contain such exceptions or exclusions. One might reasonably presume, for example, that the Zurich policies in the Sony PlayStation coverage litigation, which as alleged were effective for the policy period beginning April 1, 2011,[46] do not contain any express exceptions or exclusions—none are raised in Zurich's complaint.

Even where a policy contains an express electronic data exclusion, moreover, some courts have found coverage. For example, the Eighth Circuit in *Eyeblaster, Inc. v. Federal Insurance Co.*[47] held that an insurer had a duty to defend a complaint alleging injury to the plaintiff's "computer, software, and data after [the plaintiff] visited [the insured's] website."[48] The plaintiff alleged that "his computer was infected with a spyware program from [the insured] on July 14, 2006, which caused his computer to immediately freeze up," and that "he lost all data on a tax return on which he was working and that he incurred many thousands of dollars of loss."[49] The plaintiff further alleged that "he ha[d] experienced the following: numerous

pop-up ads; a hijacked browser that communicates with websites other than those directed by the operator; random error messages; slowed computer performance that sometimes results in crashes; and ads oriented toward his past web viewing habits."[50] The insured's CGL policy obligated "the insurer to provide coverage for property damage caused by a covered occurrence."[51] "Property damage" was defined in the policy at issue as "physical injury to tangible property, including resulting loss of use of that property . . .; or loss of use of tangible property that is not physically injured."[52] The definition of "tangible property" excluded "any software, data or other information that is in electronic form."[53]

Notwithstanding the express exclusion, the court held that the insurer was obligated to defend because the complaint alleged "loss of use of tangible property that is not physically injured" under the second prong of the "property damage" definition:

> [The insurer] did not include a definition of "tangible property" in its General Liability policy, except to exclude "software, data or other information that is in electronic form." The plain meaning of tangible property includes computers, and the [underlying] complaint alleges repeatedly the "loss of use" of his computer. We conclude that the allegations are within the scope of the General Liability policy.[54]

As claims increase, we can expect to see more courts addressing whether such claims raise sufficient issues at least to trigger a defense obligation under the CGL Coverage A.

Potential CGL Coverage for "Publication" That Violates a "Right of Privacy"
The Personal and Advertising Injury Liability coverage section of the current standard form ISO CGL policy states that the insurer "will pay those sums that the insured becomes legally obligated to pay as damages because of 'personal and advertising injury,'[55] which is caused by an offense arising out of [the insured's] business."[56] "Personal and advertising injury" is defined in the ISO standard form policy to include a list of specifically enumerated offenses,[57] which include the offense of "[o]ral or written publication, in any manner, of material that violates a person's right of privacy."[58] Similar to Coverage A, the policy further states that the insurer "will have the right and duty to defend the insured against any 'suit.'"[59] The CGL Coverage B can indemnify and provide a defense against a wide variety of claims, including claims alleging violation of privacy rights.

Potential issues arising under Coverage B include whether there has been a "publication" that violates the claimant's "right of privacy"—both terms are left undefined in standard form ISO policies. Courts generally have construed these requirements favorably to insureds, and this coverage may afford broad coverage to companies for theft of consumer data and misuse of customer information, copyright infringement, and other types of unfair competition. For example, in *Tamm v. Hartford Fire Insurance Co.*,[60] the Superior Court of Massachusetts confirmed that the insurer had a duty to defend a lawsuit alleging, inter alia, that the insured

"access[ed] and distribut[ed] information obtained in private email accounts" and "threatened to contact a list of specific e-mail addresses for individuals. . . ."[61] The underlying lawsuit set out 10 counts against the insured, including "violations of RICO, misappropriation of trade secrets, and violations of Federal wiretapping laws," and requested that "the court restrain [the insured] from 'disclosing to any person or entity, or using in any other manner, any confidential or proprietary information or materials belonging to or wrongfully acquired from [the plaintiff] or its officers, directors, employees, attorneys, or agents.'"[62] Based on the complaint, the court easily concluded that the insurer had a duty to defend under the insurance policy:

> In order to trigger the duty to defend under the invasion of privacy language of the policy, an underlying complaint must allege two things: (1) an "oral or written publication" of (2) "materials that violate person's rights of privacy." The [underlying]complaint alleges that [the insured] accessed the private e-mail accounts of [the plaintiff] and its executives and sent these private communications and materials to several outside counsel for [the plaintiff]. The allegations of sending these private communications via e-mail to outside attorneys seemingly satisfies both prongs under the invasion of privacy clause of the policy.[63]

More recently, the Ninth Circuit upheld coverage in *Netscape Communications Corp. v. Federal Insurance Co.*[64] In that case, the underlying plaintiffs alleged that the insured's "SmartDownload [software] violated the claimants' privacy by, among other things, collecting, storing, and disclosing to Plaintiffs and their engineers claimants' Internet usage."[65] The insurance policy obligated the insurer to "pay amounts [the insured] is legally required to pay as damages for covered personal injury that … is caused by a personal injury offense," which was defined to include the offense of "[m]aking known to any person or organization written or spoken material that violates a person's right to privacy."[66] The court held that the insurer had a duty to defend, reasoning that "when [the insured] received information from SmartDownload, it was making it known to AOL by transmitting it to its parent company. Similarly, individual [insured] employees made the information known to each other by circulating files among themselves with the information gained from SmartDownload."[67] The Ninth Circuit affirmed that "the district court correctly determined that the claims against [the insured] were 'personal injury offenses' and within the policy's coverage."[68]

Again, there may be potential coverage hurdles under Coverage B. ISO standard form policies written or effective on or after December 1, 2001, contain exclusions relating to Internet-related activities that insurers may assert limit the broad grant of coverage.[69] Unless clear and unambiguous, however, any exclusions should be construed in favor of the insured pursuant to established canons of insurance policy construction.[70] Whether an exclusion applies depends on the specific exclusionary language in the policy and whether the insurer can meet its burden to demonstrate that the exclusion applies to the loss in question under applicable law.

Potential Property Policy Coverage for Injury to Covered Property

Most companies have insurance coverage that is intended to insure the company's assets. By way of example, the 2007 standard form ISO commercial property policy covers "direct physical loss of or damage to Covered Property at the premises described in the Declarations caused by or resulting from any Covered Cause of Loss."[71] Such policies may be in the form of broadly worded "all risk," "difference in conditions," "multiperil," or "inland marine" policies.

As discussed above in connection with CGL coverage, a company's ability to recover for cyber attacks under all risk property policies may turn upon whether data loss comprises physical loss of or damage to covered property.

Potential Property Policy Coverage for Business Interruption and Extra Expense

Many first-party policies also provide what are known as "time element" coverages—including "business interruption" and "extra expense" coverages—that cover loss resulting from the company's inability to conduct normal business operations. These coverages may cover business interruption resulting from a cyber attack. Business interruption coverage generally reimburses the insured for its loss of earnings or revenue resulting from covered property damage. For example, the ISO "Business Income (and Extra Expense) Coverage Form" covers the loss of net profit and operating expenses that the insured "sustain[s] due to the necessary 'suspension' of [the insured's] 'operations' during the 'period of restoration.'"[72] "Extra expense" coverage generally covers the insured for certain extra expenses incurred to minimize or avoid business interruption and to resume normal operations. For example, the ISO standard form covers, among other things, "extra expense" to "[a]void or minimize the 'suspension' of business and to continue operations at the described premises or at replacement premises or temporary locations. . . ."[73] The form defines "extra expense" as "necessary expenses" that the insured "would not have incurred if there had been no direct physical loss or damage to property caused by or resulting from a Covered Cause of Loss."[74]

A company may have coverage under these provisions for loss of business and extra expense associated with a cyber attack. For example, the Fourth Circuit, in *NMS Services Inc. v. Hartford*,[75] upheld coverage for business interruption and extra expense coverage for the costs associated with an employee hacking incident that resulted in "the erasure of vital computer files and databases necessary for the operation of the company's manufacturing, sales, and administrative systems."[76] In that case, the insured's employee "had installed two hacking programs on [the insured's] network systems while he was still employed," which "allowed [the employee] to gain full access to [the insured's] systems by overriding security codes and unencrypting secured passwords, thus enabling [the employee] to cause the damage[.]"[77] The Business Income Additional Coverage section in the policy at issue stated that the insurer would "pay for the actual loss of Business Income [the insured] sustain[s] due to the necessary suspension of your 'operations' during the

'period of restoration.' The suspension must be caused by *direct physical loss of or damage* to property at the described premises. . . ."[78] The Fourth Circuit easily determined that the business income and extra expense coverages applied because, in the court's words, there was "no question that [the insured] suffered damage to its property."[79]

A Texas appellate court likewise found coverage for business interruption in *Lambrecht & Associates, Inc. v. State Farm Lloyds*.[80] In that case, the insured sought coverage for the loss of computer data and the related loss of business income after a "virus caused the [insured's] computers to have difficulties while 'booting up,' perform a number of 'illegal functions' and eventually completely 'freeze up,' thereby rendering the computers useless."[81] The insured's computer system had to be taken offline and its employees were unable to use their computers until the server was restored.[82] The insurance policy at issue committed the insurer to "pay for accidental direct physical loss to business personal property" and "the actual loss of 'business income' [the insured] sustained due to the necessary suspension of [its] 'operations' during this 'period of restoration.'"[83] The court disagreed with the insurer's argument that "the loss of information on [the insured's] computer systems was not a 'physical' loss because the data … did not exist in physical or tangible form,"[84] and held that "the plain language of the policy dictates that the personal property losses alleged by Lambrecht were 'physical' as a matter of law."[85] The court further held that "the business income [the insured] lost as a result of the virus [wa]s covered under the policy."[86]

In addition to business interruption coverage, companies may have "contingent business interruption" coverage that covers the insured with respect to losses, including lost earnings or revenue, as a result of damage, not to the insured's own property, but to the property of an insured's supplier, customer, or some other business partner or entity.[87] This may be increasingly important coverage in the context of cloud outsourcing of maintenance and control over data to third parties. As one commentator has noted, "business interruption losses resulting from loss of access to the cloud should, in the majority of cases, be covered under so-called 'legacy' contingent business interruption forms."[88]

Newer First-Party Forms That May Contain Sublimits

It is important to note that some standard forms seek to shift data loss from the principal coverage grant by excluding electronic data from the definition of "covered property" and by instead providing coverage under "additional coverage" that may be subject to relatively low—presumptively inadequate—coverage sublimits. For example, the 2007 ISO Commercial Property Form excepts electronic data from the definition of "covered property"[89] and provides coverage under an "additional coverage" that is limited to "$2,500 for all loss or damage sustained in any one policy year, regardless of the number of occurrences of loss or damage or the number of premises, locations or computer systems."[90]

Likewise, the 2007 ISO standard form Business Income (and Extra Expense) Coverage Form excludes coverage for electronic data under the main coverage part[91] and provides coverage under an "Additional Coverage" subject to a $2,500 limit for "all loss sustained and expense incurred in any one policy year, regardless of the number of interruptions or the number of premises, locations or computer systems involved."[92]

These mechanisms underscore the importance of considering not only what cyber risks may be covered but also whether the limits are sufficient.

Potential Coverage under Other Traditional Policies

Many companies have various types of crime coverage, including fidelity insurance and financial institution bonds that may cover cyber risks and losses. Other types of conventional liability coverages, such as directors' and officers' (D&O) liability, errors and omissions (E&O), and professional liability coverages may also respond to cover cyber attacks and losses.[93] For example, in the *Eyeblaster* case discussed above, the Eighth Circuit also upheld coverage under an Information and Network Technology E&O policy.

Addressing the question of coverage under a crime policy, the Sixth Circuit recently confirmed that an insured was covered for more than $6.8 million in stipulated losses associated with a data breach that compromised customer credit card and checking account information in *Retail Ventures, Inc. v. National Union Fire Insurance Co. of Pittsburgh, Pa.*[94] In that case, the insured incurred substantial expenses for customer communications, public relations, customer claims and lawsuits, and attorney fees in connection with investigations by seven state Attorneys General and the Federal Trade Commission.[95] The Sixth Circuit confirmed that there was coverage under the computer fraud rider of the insured's blanket crime policy, which stated that the insurer would pay the insured for "Loss which the Insured shall sustain resulting directly from . . . [t]he theft of any Insured property by Computer Fraud."[96] "Computer fraud" was defined as

> the wrongful conversion of assets under the direct or indirect control of a Computer System by means of: (1) The fraudulent accessing of such Computer System; (2) The insertion of fraudulent data or instructions into such Computer System; or (3) The fraudulent alteration of data, programs, or routines in such Computer System.[97]

Specialty Cyber Policies

The *Sony* coverage suit is not the first time that insurers have refused to voluntarily pay claims resulting from a network security breach or other cyber-related liability under CGL policies. Nor will it be the last. Even where there is a good claim for coverage, insurers can be expected to continue to argue that cyber risks are not covered under CGL or other traditional policies.

Insurers are marketing newer insurance products specifically tailored to cover cyber risks, and this has been called "the new frontier of the 21st century market."[98] The new cyber policies may come under names such as "privacy and security," "network security," and names that incorporate "cyber," "media" or some form of "technology" or "digital." ISO has a standard form called "Internet Liability and Network Protection Policy"[99] on which insurers may base their coverage, although it is typical for cyber policies to vary considerably, and careful consideration should therefore be given to a company's potential risk scenarios and the specific policy language under consideration.

Companies that have purchased specialty cyber policies should be familiar with the coverage terms and applicability so that they can take full advantage of the coverage purchased. In addition, companies should review their insurance programs to determine whether there are potential gaps that can be filled through specialty cyber policies or tailored endorsements. Consideration should also be given to the overall structure of the insurance program, which should be carefully reviewed not only to eliminate potential gaps in coverage but also to minimize coverage overlaps and attendant costs and inefficiencies.

A number of the cyber risk policies offer both first-party and third-party cyber coverage as separate coverage parts. The types of losses and liabilities that cyber risk policies may cover include the following:

- losses resulting from a data breach, including third-party actions against a company and costs associated with notification requirements, public relations efforts, forensics, and crisis management
- misappropriation of intellectual property or confidential business information
- the cost to recover data that are damaged by malicious code or stolen
- business interruption resulting from operations being disabled by a cyber attack
- extortion from cyber attackers who have stolen data

The author is unaware of any cases addressing coverage under these newer policies. An overview of certain types of coverage available under these policies is provided below. Although specimens of these newer policies are available, the actual language contained in the policy issued to an insured could substantially differ from the specimen policy. It is important to note that coverage in all cases will turn on the particular language of the policy as applied to the specific facts at issue.

Third-Party Cyber Coverage for Data Breaches, Distributed Denials of Service, and Malicious Code Transmission

Third-party cyber liability policies typically cover the insured against liability arising from, for example, data breaches, transmission of malicious code, denial of third-party access to the insured's network, and misappropriation of intellectual property. For example, the new Hartford CyberChoice 2.09 specimen policy[100] provides

coverage for loss of customer data, denial of access, and other cyber risk events. The specimen policy states that the insurer will pay "damages" that the insured "shall become legally obligated to pay as a result of a Claim . . . alleging a Data Privacy Wrongful Act or a Network Security Wrongful Act."[101] "Data privacy wrongful act" is defined to include "any negligent act, error or omission by the Insured that results in: the improper dissemination of Nonpublic Personal Information"[102] or "any breach or violation by the Insured of any Data Privacy Laws."[103] "Network security wrongful act" is defined as follows:

> any negligent act, error or omission by the Insured resulting in Unauthorized Access or Unauthorized Use of the Organization's Computer System, the consequences of which include, but are not limited to:
>
> (1) the failure to prevent Unauthorized Access to, use of, or tampering with a Third Party's computer systems;
> (2) the inability of an authorized Third Party to gain access to the Insured's services;
> (3) the failure to prevent denial or disruption of Internet service to an authorized Third Party;
> (4) the failure to prevent Identity Theft or credit/debit card fraud; or
> (5) the transmission of Malicious Code.[104]

Malicious code includes "unauthorized and either corrupting or harmful software code, including but not limited to computer viruses, Trojan horses, worms, logic bombs, spyware, malware or spider ware."[105]

The AIG netAdvantage specimen policy[106] provides similar types of coverage. The specimen policy states that the insurer will "pay amounts" that the insured is "legally obligated to pay as damages and claims expenses arising from a claim first made against" the insured for "wrongful acts,"[107] as defined in the specimen policy to include "any actual or alleged breach of duty, neglect, act, error or omission that results in a failure of security; or a privacy peril."[108] "Failure of security" includes "the actual failure and inability of the security of [the insured's] computer system to mitigate loss from or prevent a computer attack,"[109] which in turn is defined as "unauthorized access, unauthorized use, receipt or transmission of a malicious code [including but not limited to "computer viruses," "Trojan horses," "worms," and "time or logic bombs"] or "denial of service attack" that

> (1) alters, copies, misappropriates, corrupts, destroys, disrupts, deletes, damages or prevents, restricts or hinders access to, a computer system;
> (2) results in the disclosure of private or confidential information stored on a computer system; or
> (3) results in identity theft.
>
> whether any of the foregoing is intentional or unintentional, malicious or accidental, fraudulent or innocent, specifically targeted at you or generally

> distributed, and regardless of whether the perpetrator is motivated for profit.[110]

"Privacy peril" includes "unauthorized disclosure by [the insured] of private information or failure by [the insured] to protect private information from misappropriation, including, without limitation, any unintentional violation of your privacy policy or misappropriation that results in identity theft. . . ."[111] "Private information" includes "information from which an individual may be uniquely and reliably identified or contacted, including without limitation, an individual's name, address, telephone number, social security number, account relationships, account numbers, account balances, account histories and passwords. . . ."[112]

There are numerous other products currently available on the market that respond to third-party cyber risks.[113]

Third-Party Cyber Coverage for Liability for Infringement of Intellectual Property Rights

The third-party policies often also include coverage for claims for infringement of copyright and other intellectual property rights. For example, the new Hartford CyberChoice 2.09 specimen policy states that the insurer will pay damages that the insured "shall become legally obligated to pay as a result of a claim "alleging a e-Media Wrongful Act."[114] "E-media wrongful act" includes "any negligent act, error or omission by the Insured that results in the following:

> (1) infringement of copyright, service mark, trademark, or misappropriation of ideas or any other intellectual property right, other than infringement of patents or trade secrets; defamation, libel, product disparagement, trade libel, false arrest, detention or imprisonment, or malicious prosecution, infringement or interference with rights of privacy or publicity; wrongful entry or eviction; invasion of the right of private occupancy; and/or plagiarism, misappropriation of ideas under implied contract invasion or other tort related to disparagement or harm to the reputation or character of any person or organization in the Insured Entity's Electronic Advertising or in the Insured Entity's Advertising; or
>
> (2) misappropriation or misdirection of Internet based messages or media of third parties on the Internet by the Insured, including meta-tags, web site domains and names, and related cyber content.[115]

The AIG netAdvantage specimen policy likewise covers "amounts" the insured is "legally obligated to pay . . . as damages resulting from any claim" against the insured for the insured's "wrongful acts,"[116] which are defined to include certain acts and omissions "which result[] in a covered peril,"[117] which in turn is defined to include the following:

> (1) infringement of copyright, title, slogan, trademark, trade name, trade dress, mark, service mark or service name including without limitation, infringement of domain name, deep-linking or framing; plagiarism, piracy or misappropriation of ideas under implied contract or other misappropriation of property rights, ideas or information; or any alleged violation of Section 43(a) of the Lanham Act or any similar state statutes; including without limitation unfair competition in connection with a claim for damages in connection with such conduct;
>
> (2) form of defamation or other tort related to disparagement or harm to character, reputation or the feelings of any person, including, but not limited to, libel, slander, product disparagement, trade libel; including without limitation, unfair competition, emotional distress or mental anguish in connection with a claim for damages in connection with such conduct; or
>
> (3) form of invasion, infringement or interference with rights of privacy or publicity, including without limitation, false light, public disclosure of private facts, intrusion and commercial appropriation of name, persona or likeness; including without limitation, emotional distress or mental anguish in connection with a claim for damages in connection with such conduct.[118]

There are numerous other products currently available on the market that cover infringement of copyright and other intellectual property rights.[119]

First-Party Cyber Coverage for Damage to Computer Systems

First-party risks may include damage to the insured's own computer hardware or data, and cyber policies often cover this risk. For example, the AIG netAdvantage specimen policy states that the insurer will pay the insured's "actual information asset loss … resulting directly from injury to information assets" that results "from a failure of security of your computer system."[120] "Information asset loss" is defined to include "software or electronic data, including without limitation, customer lists and information, financial, credit card or competitive information, and confidential or private information" "that are altered, corrupted, destroyed, disrupted, deleted or damaged. . . ."[121] CNA's NetProtect 360 specimen policy states that the insurer will pay the insured "all sums" for "reasonable and necessary expenses resulting from an Exploit [defined as Unauthorized Access, Electronic Infection or a Denial of Service Attack that results in Network Impairment, each as separately defined]" that are "required to restore the Insured Entity's Network or information residing on the Insured Entity's Network to substantially the form in which it existed immediately prior to such Exploit."[122] Many other products offer similar types of coverage.[123]

First-Party Cyber Coverage for Business Interruption and Extra Expense

Cyber policies often include coverage for business interruption and extra expense caused by malicious code (viruses, worms, Trojans, malware, spyware, and the like),

distributed denial-of-service attacks, unauthorized access to or theft of information, and other security threats to networks. For example, the AIG netAdvantage specimen policy covers the insured's "actual business interruption loss . . . which [the insured] sustains during the period of recovery (or the extended interruption period if applicable), resulting directly from a material interruption [defined as "the actual and measurable interruption or suspension of [the insured's] computer system, which is directly caused by a failure of security"]."[124] "Business interruption loss" includes "the sum of: (1) income loss; (2) extra expense; (3) dependent business interruption loss; and (4) extended business interruption loss,"[125] each as separately defined.[126]

CNA's NetProtect 360 specimen policy states that the insurer will pay the insured

> all sums . . . for reduction of business income the Insured Entity sustains during a Period of Restoration due to the interruption of Commerce Operations [defined as "income producing activities"] by a Network Impairment that has been caused by an Exploit defined as Unauthorized Access, Electronic Infection or a Denial of Service Attack that results in Network Impairment [each as separately defined] during the Policy Period; and, for Extra Expense that the Insured Entity sustains to minimize any such Network Impairment in order to resume Commerce Operations[.][127]

Many other products offer similar types of coverage.[128]

Other First-Party Coverages

Cyber risk policies may provide other potentially valuable coverages, including the following:

Notification and Credit Monitoring. Cyber risk policies frequently provide coverage for the costs associated with notification of a data breach and credit monitoring services. For example, Beazley's AFB Media Tech specimen policy provides coverage for "Privacy Notification Costs . . . resulting from the Insured Organization's legal obligation to comply with a Breach Notice Law because of an incident (or reasonably suspected incident) described in [the Information Security & Privacy Liability] Insuring Agreement. . . ."[129] "Privacy Notification Costs" is defined to include a number of "reasonable and necessary costs incurred by the Insured Organization," among them costs "to provide notification to individuals who are required to be notified by the applicable Breach Notice Law" and costs of "offering of one (1) year of credit monitoring services to those individuals whose Personally Identifiable Non-Public Information was compromised or reasonably believed to be compromised as a result of theft, loss or Unauthorized Disclosure of information giving rise to a notification requirement pursuant to a Breach Notice Law."[130] [131]

Investigation. Cyber risk policies often provide coverage for the costs associated with determining the cause of an attack. For example, Hartford's CyberChoice

2.09SM specimen policy states that the insurer "will reimburse the Insured Entity for reasonable and necessary Cyber Investigation Expenses," which include "reasonable and necessary expenses the Insured Entity incurs to conduct an investigation of its Computer System by a Third Party to determine the source or cause of the Data Privacy Wrongful Act or Network Security Wrongful Act."[132]

Crisis Management and Public Relations. The costs associated with a cyber attack often include activities intended to prevent a loss of consumer trust and goodwill, crisis management, and public relations efforts. For example, the AIG netAdvantage specimen policy Crisis Management Module Form covers "crisis management expenses"[133] as defined to include "amounts which an organization incurs for the reasonable and necessary fees and expenses incurred by a crisis management firm in the performance of crisis management services for an organization" arising from a "failure of security" or "privacy peril," each as defined.[134] CNA's NetProtect 360 specimen policy likewise covers "Public Relations Event Expenses . . . to respond to adverse or unfavorable publicity or media attention arising out of a Public Relations Event," defined as "any situation which in the reasonable opinion of an Executive did cause or is reasonably likely to cause economic injury to the Insured Entity."[135]

Extortion. Cyber policies often cover losses resulting from extortion (payments of an extortionist's demand to prevent network loss or implementation of a threat), which may be an increasingly valuable protection. For example, the AIG netAdvantage specimen policy indemnifies the insured "for those amounts" the insured pays "as extortion monies resulting from an extortion claim. . . ."[136] "Extortion claim" is defined to include "any threat or connected series of threats to commit an intentional computer attack. . . ."[137] The Hartford CyberChoice 20 specimen policy likewise covers "amounts which the Organization pays as Extortion Payments directly resulting from a Cyber Extortion Claim."[138]

Beware the Fine Print

Cyber insurance coverages may be extremely valuable, but they deserve—indeed, require—a careful review. The specific policy terms and conditions must be analyzed carefully to ensure that the coverage provided meets the company's specific loss scenarios and potential exposures. In addition, the exclusions and other terms and conditions must be carefully read and understood. Some insurers, for example, may insert exclusions based on purported shortcomings in the insured's security measures if identified in the underwriting process or known to the insured prior to policy inception.[139]

One specimen form policy excludes any claim "alleging, arising out of or resulting, directly or indirectly" from "(1) any shortcoming in security that [the insured] knew about prior to the inception of this policy," "(2) [the insured's] failure to take reasonable steps, to use, design, maintain and upgrade [the insured's] security, or "(3) the inability to use, or lack of performance of, software: (a) due to expiration, cancellation, or withdrawal of such software; (b) that has not yet been released from

its development stage; or (c) that has not passed all test runs or proven successful in applicable daily operations."[140]

However, it remains to be seen whether broad exclusions of this kind will be upheld and enforced by the courts, particularly given that the new policies are specifically marketed to cover the risk of liability for negligence in connection with the failure of network security.

Conclusion

Virtually every company is vulnerable to cyber attacks—a fact amply illustrated by the recent instances involving some of the world's most sophisticated organizations. When targeted by an attack or facing a claim, companies should carefully consider the coverage that may be available. Insurance is a valuable asset. With the assistance of experienced coverage counsel, companies facing potential exposure will be in the best possible position to present a claim most effectively and, ideally, maximize their coverage. Before an attack, companies should take the opportunity to evaluate and address their potential vulnerabilities, the sufficiency of their existing insurance coverage, and the potential role of specialized cyber risk coverage. Experienced counsel can assist in negotiating the most favorable terms available and ensuring that there are no gaps, or overlaps, in coverage.

Keywords: cyber risk, business interruption coverage, time element coverage, extra expense, property damage, intellectual property, privacy rights

Roberta D. Anderson is a partner with K&L Gates LLP, Pittsburgh.

---

[1] Roberta D. Anderson is a partner with K&L Gates LLP, Pittsburgh, a law firm that regularly represents policyholders in insurance coverage disputes. The opinions expressed in this article are those of the author and should not be construed as necessarily reflecting the views of her law firm or the firm's clients or as an endorsement by the law firm or the law firm's clients of any legal position described in the article.
[2] Kevin Robinson-Avila, "Cyber Attacks on the Rise Worldwide," *ABQJournal*, Dec. 17, 2012 (last visited Dec. 20, 2012).
[3] *See* Robert Vamosi, "Twenty-Six Banks Identified in Latest Malware Threat," *DeviceLine Blog* (Mocana) (Oct. 18, 2012) (last visited Dec. 20, 2012); Chris Strohm & Eric Engleman, "Cyber Attacks on Banks Expose U.S. Infrastructure Vulnerability," *Bloomberg.com* (Sept. 28, 2012) (last visited Dec. 18, 2012).
[4] *See* Editorial, "The Cloud Darkens," *N.Y. Times*, June 29, 2011 (last visited Dec. 19, 2012) (opining that "[c]ompanies and the government are unprepared").
[5] Editorial, *supra* note 4.
[6] Towers Watson, *2012 Towers Watson Risk and Finance Manager Survey* 1 (last visited Dec. 26, 2012).

[7] Towers Watson, *supra* note 6, at 4.
[8] SEC Division of Corporation Finance, Cybersecurity, CF Disclosure Guidance: Topic No. 2 (Oct. 13, 2011) (Dec. 27, 2012).
[9] *See* Michael P. Voelker, "*After 'Year of the Data Breach,' Carriers Increase Capacity, Competition for Cyber Risks*," *Property Casualty 360°* (Feb. 2, 2012) (last visited Dec. 19, 2012); Ephraim Schwartz, "The Biggest, Baddest Data Breaches of 2011," *Tech Security Today* (last visited Dec. 18, 2012); Zack Whittaker, "2012: Looking Back at the Major Hacks, Leaks and Data Breaches," *ZDNet* (Dec. 17, 2012) (last visited Dec. 18, 2012).
[10] Shara Tibken, "SecurID Clients Get Jitters," *Wall St. J.*, June 8, 2011 (last visited Dec. 19, 2012).
[11] Privacy Rights Clearinghouse, Chronology of Data Breaches: Security Breaches 2005–Present (last visited Jan. 2, 2013).
[12] Privacy Rights Clearinghouse, Chronology of Data Breaches: FAQ (last visited Dec. 23, 2012).
[13] Ponemon Institute, *2012 Cost of Cyber Crime Study: United States*28 (Oct. 2012) (last visited Dec. 18, 2012).
[14] *2012 Cost of Cyber Crime Study: United States*, *supra* note 13,at 1.
[15] *2012 Cost of Cyber Crime Study: United States*, *supra* note 13,at 1.
[16] Siobhan Gorman, "Iran Renews Internet Attacks on U.S. Banks," *Wall St. J.*, Oct. 17, 2012 ("These latest attacks, which investigators say are at least 10 times as potent as the types of denial-of-service attacks hackers have mounted in the past, have disrupted service at even the largest U.S. banks. The highly sophisticated computer attack is using a new cyberweapon called 'itsoknoproblembro[.]'") (last visited Dec. 20, 2012).
[17] *See* Kevin P. Kalinich, J.D., "AON Network Risk Insurance 2012 Update," *in Privacy and Security Exposures and Solutions* 4 ("The dramatic increase in use of mobile devices by company employees presents new security threats to corporate networks"), *available at* http://www.aon.com/risk-services/network-security-privacy.jsp (last visited Dec. 20, 2012).
[18] Ponemon Institute, *2013 State of the Endpoint* 1 (Dec. 2012) (last visited Dec. 18, 2012).
[19] Forty-six states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information, which are in addition to numerous federal statutes and regulations. *See* National Conference of State Legislatures, State Security Breach Notification Laws (updated *Aug. 20, 2012*) (last visited Dec. 18, 2012).
[20] Ponemon Institute LLC, *2011 Cost of Data Breach Study: United States* 2 (Mar. 2012), *available at* http://www.ponemon.org/library (last visited Dec. 18, 2012).
[21] *2011 Cost of Data Breach Study*, *supra* note 20, at 2.
[22] *2011 Cost of Data Breach Study*, *supra* note 20, at 3.
[23] *2011 Cost of Data Breach Study*, *supra* note 20, at 2.
[24] *See* Paul Tassi, "Sony Pegs PSN Attack Costs at $170 Million, $3.1B Total Loss for 2011," *Forbes - Business*, May 23, 2011 (last visited Dec. 20, 2012).
[25] Liana B. Baker & Jim Finkle, "Sony's Insurers to Help Foot Bill for Data Breach: Experts Say the Final Tally Could Exceed $2 Billion," *Reuters*, May 5, 2011

(last visited Aug. 21, 2011).
[26] *2012 Cost of Cyber Crime Study*, *supra* note 13, at 1.
[27] No. 651982/2011 (N.Y. Sup. Ct. New York City) (filed July 20, 2011).
[28] Complaint at ¶ 28, *Zurich American Insurance Co.*, No. 651982/2011.
[29] ISO Form CG 00 01 12 07 (2007), Section I, Coverage A, §1.a .
[30] ISO Form CG 00 01 12 07, Section I, Coverage A, §1.b.(2) .
[31] "Property damage" is defined in the current form as follows:

> 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 of use shall be deemed to occur at the time of the "occurrence" that caused it.
> 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 CG 00 01 12 07, Section V, §§3, 17 .
[32] ISO Form CG 00 01 12 07, Section V, §17 .
[33] ISO Form CG 00 01 12 07, Section I, Coverage A, §1.a .
[34] 469 N.W.2d 735 (Minn. Ct. App. 1991), *review denied* (Aug. 2, 1991).
[35] *Retail Systems, Inc.*, 469 N.W.2d at 737.
[36] *Retail Systems, Inc.*, 469 N.W.2d at 737.
[37] 2000 WL 726789 (D. Ariz. Apr. 18, 2000) .
[38] *Ingram Micro, Inc., 2000 WL 726789, at *2*.
[39] *Ingram Micro, Inc., 2000 WL 726789, at *3*. Although *Ingram Micro* concerned an all-risk policy, the decision clearly holds that data are tangible and can therefore suffer "physical injury."
[40] *See, e.g., Ward Gen. Ins. Servs., Inc. v. Emp'rs Fire Ins. Co., 7 Cal. Rptr. 3d 844, 851 (Cal. App. Ct. 2003)*; *Am. Online Inc. v. St. Paul Mercury Ins. Co., 207 F. Supp. 2d 459, 467 (E.D. Va. 2002), aff'd, 347 F.3d 89 (4th Cir. 2003)*; *State Auto Prop. & Cas. Ins. Co. v. Midwest Computers & More, 147 F. Supp. 2d 1113, 1116 (W.D. Okla. 2001) (Oklahoma law).*
[41] 9 *Couch on Insurance § 126:40 (3d ed. 2012)* .
[42] *See supra* note 31.
[43] *See* ISO Form CG 00 01 12 07 (2007), Section I, Coverage A, §2.l . This section defines "electronic data" as follows:

> 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, CDROMS, tapes, drives, cells, data processing devices or any other media which are used with electronically controlled equipment.

[44] ISO Form CG 04 37 12 04 (2003).
[45] *See, e.g.*, ISO Form CG 00 01 07 98 (1997), Section V, §17 ; ISO Form CG 00 01 01 96 (1994), Section V, §15 ; ISO Form CG 00 01 10 93 (1992), Section V, §15 ; ISO Form CG 00 01 11 88 (1991), Section V, §12 .
[46] Complaint at ¶¶41, 48, 55, *Zurich American Insurance Co.*, No. 651982/2011.
[47] 613 F.3d 797 (8th Cir. 2010).
[48] *Eyeblaster, Inc.*, 613 F.3d at 799.
[49] *Eyeblaster, Inc.*, 613 F.3d at 800.
[50] *Eyeblaster, Inc.*, 613 F.3d at 800.
[51] *Eyeblaster, Inc.*, 613 F.3d at 801.
[52] *Eyeblaster, Inc.*, 613 F.3d at 801.
[53] *Eyeblaster, Inc.*, 613 F.3d at 801.
[54] *Eyeblaster, Inc.*, 613 F.3d at 801–02.
[55] ISO Form CG 00 01 12 07 (2007), Section I, Coverage B, §1.a .
[56] ISO Form CG 00 01 12 07, Section I, Coverage B, §1.b .
[57] The 2007 CGL defines "personal and advertising injury" as follows:

> 14. "Personal and advertising injury" means injury, including consequential "bodily injury", arising out of one or more of the following offenses:
> a. False arrest, detention or imprisonment;
> b. Malicious prosecution;
> c. The wrongful eviction from, wrongful entry into, or invasion of the right of private occupancy of a room, dwelling or premises that a person occupies, committed by or on behalf of its owner, landlord or lessor;
> d. Oral or written publication, in any manner, of material that slanders or libels a person or organization or disparages a person's or organization's goods, products or services;
> e. Oral or written publication, in any manner, of material that violates a person's right of privacy;
> f. The use of another's advertising idea in your "advertisement"; or
> g. Infringing upon another's copyright, trade dress or slogan in your "advertisement".

ISO Form CG 00 01 12 07, Section V, §14 .

[58] ISO Form CG 00 01 12 07, Section V, §14.e .
[59] ISO Form CG 00 01 12 07, Section I, Coverage B, §1.a .
[60] 2003 WL 21960374 (Mass. Super. Ct. 2003) .
[61] *Tamm, 2003 WL 21960374, at *2*.
[62] *Tamm, 2003 WL 21960374, at *3*.
[63] *Tamm, 2003 WL 21960374, at *3*.
[64] 343 F. App'x 271 (9th Cir. 2009) .
[65] 2007 WL 1288192, at *1 (N.D. Cal. Apr. 27, 2007) .
[66] 2007 WL 2972924, at *2 (N.D. Cal. Oct. 10, 2007), *aff'd in part, rev'd in part*, 343 F. App'x 271 (9th Cir. 2009) .

[67] *Id. at *6*.
[68] *Netscape Communications Corp.*, 343 F. App'x at 271 .
[69] The ISO policies written or effective on or after December 1, 2001, for example, contain exclusions relating to Internet activities. *See* ISO Form CG 00 01 12 07 (2007), Section I, Coverage B, §2.j ., k.
[70] *See* 2 *Couch on Insurance § 22:31 (3d ed. 2012) ("provisos, exceptions, or exemptions, and words of limitation in the nature of an exception . . . are strictly construed against the insurer….")*.
[71] ISO Form CP 00 99 06 07 (2007), Section A.
[72] ISO Form CP 00 30 06 07 (2007).
[73] ISO Form CP 00 30 06 07.
[74] ISO Form CP 00 30 06 07.
[75] 62 F. App'x 511 (4th Cir. 2003) .
[76] *NMS Services Inc.*, 62 F. App'x at 512 .
[77] *NMS Services Inc.*, 62 F. App'x at 512 .
[78] *NMS Services Inc.*, 62 F. App'x at 514 (emphasis in original) .
[79] *NMS Services Inc.*, 62 F. App'x at 514 .
[80] 119 S.W.3d 16 (Tex. App. Ct. 2003).
[81] *Lambrecht & Associates, Inc.*, 119 S.W.3d at 23.
[82] *Lambrecht & Associates, Inc.*, 119 S.W.3d at 19.
[83] *Lambrecht & Associates, Inc.*, 119 S.W.3d at 19.
[84] *Lambrecht & Associates, Inc.*, 119 S.W.3d at 23.
[85] *Lambrecht & Associates, Inc.*, 119 S.W.3d at 25.
[86] *Lambrecht & Associates, Inc.*, 119 S.W.3d at 25; *see also S.E. Mental Health Ctr., Inc. v. Pac. Ins. Co., Ltd., 439 F. Supp. 2d 831 (W.D. Tenn. 2006) (Tennessee law)*.
[87] ISO CP 15 08 04 02 (2001).
[88] Lon Berk, "CBI for the Cloud," *Coverage*, Vol. 21, No. 6 (November/December 2011), at 11.
[89] ISO Form CP 00 99 06 07 (2007), Section A.2.n.
[90] ISO Form CP 00 99 06 07, Section A.4.e.(1), (2), (4).
[91] ISO Form CP 00 30 06 07 (2007), Section A.4.
[92] ISO Form CP 00 30 06 07, Section A.5.d.
[93] *See* Louis Chiafullo & Brett Kahn, "Coverage for Cyber Risks," *Coverage*, Vol. 21, No. 3 (May/June 2011), at 6–7 (discussing coverage for cyber risks under D&O, E&O, and other types of insurance coverages).
[94] 691 F.3d 821(6th Cir. 2012) (predicting Ohio law).
[95] *Retail Ventures, Inc.*, 691 F.3d at 824.
[96] *Retail Ventures, Inc.*, 691 F.3d at 826.
[97] *Retail Ventures, Inc.*, 691 F.3d at 826–27.
[98] Harry Cylinder, "Evaluating Cyber Insurance," *CPCU eJournal* (Dec. 2008), http://www.cpcusociety.org/file_depot/0-10000000/0-10000/3267/conman/CPCUeJournalDec08article.pdf (last visited Dec. 20, 2012).
[99] ISO EC 00 10 07 05 (2004).
[100] Hartford CyberChoice 2.09SM Specimen Network Security Liability Insurance Policy Form #DP 00 H003 00 0312 (2012) (visited Dec. 20, 2012).

[101] Hartford CyberChoice 2.09SM Specimen Form, Section I (A).
[102] Hartford CyberChoice 2.09SM Specimen Form, Section III (N(1)). Section III (DD) defines "Nonpublic Personal Information" as follows:

> (1) a natural person's first name and last name combination with any one or more of the following:
>
> (a) social security number;
> (b) medical or healthcare information or data;
> (c) financial account information that would permit access to that individual's financial account; or
>
> (2) a natural person's information that is designated as private by a Data Privacy Law.

[103] Hartford CyberChoice 2.09SM Specimen Form, Section III (N(2)).
[104] Hartford CyberChoice 2.09SM Specimen Form, Section III (CC).
[105] Hartford CyberChoice 2.09SM Specimen Form, Section III (AA).
[106] The AIG netAdvantage forms discussed herein are on file with the author. In April 2012, Chartis began marketing its new CyberEdgeSM product, which is described at http://www.chartisinsurance.com/us-network-security-and-privacy-insurance_295_182553.html (last visited Dec. 20, 2012).
[107] AIG netAdvantage Specimen Policy, Base Form #91239 (2006), Section 2 .
[108] AIG netAdvantage Specimen Policy, Security & Privacy Liability Module Form #90599 (2007), Section 4 . SL (i).
[109] AIG netAdvantage Specimen Policy, Base Form #91239 (2006), Section 3(m) .
[110] AIG netAdvantage Specimen Policy, Base Form #91239, Section 3(g) .
[111] AIG netAdvantage Specimen Policy, Security & Privacy Liability Module Form #90599, Section 4 . SL (f).
[112] AIG netAdvantage Specimen Policy, Security & Privacy Liability Module Form #90599, Section 4 . SL (e).
[113] *See, e.g.*, Cybersecurity By ChubbSM Specimen Policy Form #14-02-14874 (02/2009) (last visited Dec. 20, 2012); ACE DigiTech Digital Technology & Professional Liability Insurance Policy Form #PF-26996 (05/09) (last visited Dec. 20, 2012); CNA NetProtect 360SM Specimen Policy Form #G-147051-A (2007) (a copy is on file with the author); Axis PRO® TechNet Solutions™ Specimen Policy Form TNS-7000 (03-10) (last visited Dec. 20, 2012); Beazley's AFB Media Tech® Specimen Policy Form # F00226 (2011) (last visited Dec. 20, 2012).
[114] CyberChoice 2.09SM Specimen Policy Form, Section I (B).
[115] CyberChoice 2.09SM Specimen Policy Form, Section III (Q).
[116] AIG netAdvantage Specimen Policy, Internet Media Module Form #90596 (2006), Section 3 .
[117] AIG netAdvantage® Specimen Policy, Internet Media Module Form #90596, Section 5 MEDIA (h).
[118] AIG netAdvantage Specimen Policy, Internet Media Module Form #90596, Section 5 MEDIA (c).
[119] *See, e.g.*, ACE DigiTech Specimen Form, Section II. OO.2; Cybersecurity By

ChubbSM Specimen Form, Section II ("Content injury"); Axis PRO® TechNet Solutions Specimen Policy Form TNS-7000 (03-10), Sections A.2., V. KK.2; AFB Media Tech® Specimen Policy, Form # F00226 (2011), Section I.F.
[120] AIG netAdvantage Specimen Policy, Information Asset Module Form #90612 (2006), Section 3 .
[121] AIG netAdvantage Specimen Policy, Information Asset Module Form #90612, Section 5 IA (b, c).
[122] CNA NetProtect 360SM Specimen Form, Section II.B.
[123] *See, e.g.*, Cybersecurity By ChubbSM Specimen Form, Section I.H.
[124] AIG netAdvantage Specimen Policy, Business Interruption Module Form #90593 (2006), Section 3 , Section 5 BI (k).
[125] AIG netAdvantage Specimen Policy, Business Interruption Module Form #90593, Section 5 BI (b). Section 5 BI (*l*) defines "period of recovery" as follows:

> "Period of recovery" means the time period that:
> (1) begins on the date and time that a material interruption first occurs; and
> (2) ends on the date and time that the material interruption ends, or would have ended if you had exercised due diligence and dispatch.
> Provided, however, the period of recovery shall end no later than thirty (30) consecutive days after the date and time that the material interruption first occurred.

.
[126] AIG netAdvantage Specimen Policy, Business Interruption Module Form #90593, Section 5 BI (d, e, g, j).
[127] CNA NetProtect 360SM Specimen Form, Section II.C, Section X. "Period of Restoration" is defined as follows:

> Period of Restoration means the period of time that:
> A. Begins with the date and time that Commerce Operations have first been interrupted by a Network Impairment and after application of the Business Interruption Waiting Period Deductible, as specified in the Declarations; and
> B. Ends with the earlier of:
> 1. the date and time Commerce Operations have been restored to substantially the level of operation that had existed prior to the Network Impairment; or
> 2. one hundred and twenty hours from the time that Commerce Operations were first interrupted by such Network Impairment.

[128] Hartford CyberChoice 20SM Specimen Policy Form #CC 00 H003 00 0608 (2008) (a copy is on file with the author), Section I (D), Section III (D), (ff); Cybersecurity By ChubbSM Specimen Form, Section I.D, Section II.
[129] AFB Media Tech Specimen Policy, Section I.D.
[130] AFB Media Tech Specimen Policy, Section I.D. 2.(a), 4.(a).
[131] AFB Media Tech Specimen Policy, Section III.(EE); *see also* Hartford

CyberChoice 2.09SM Specimen Form, Section II.(D).
[132] Hartford CyberChoice 2.09SM Specimen Form, Section III.(I); see also AFB Media Tech Specimen Policy, Section I.D.1.
[133] AIG netAdvantage Specimen Policy, Crisis Management Module Form #90594 (2007), Section 3 .
[134] AIG netAdvantage Specimen Policy, Crisis Management Module Form #90594, Section 5 , CM(a), (b)(1).
[135] CNA NetProtect 360SM Specimen Form, Section I.B.1., Section X; *see also* Hartford CyberChoice 2.09SM Specimen Form, Section III.((G),(H)); AFB Media Tech Specimen Policy, Section I.D.3.
[136] AIG netAdvantage Specimen Policy, Cyber Extortion Module Form #90595 (2006), Section 2 .
[137] AIG netAdvantage Specimen Policy, Cyber Extortion Module Form #90595, Section 5 CE(b).
[138] Hartford CyberChoice 20SM Specimen Policy #CC 00 H003 00 0608, Section I (E); *see also* Cybersecurity By ChubbSM Specimen Form, Section I.G.; ACE DigiTech Specimen Form, Section I.F.; CNA NetProtect 360SM Specimen Form, Section II.A., Section X.
[139] *See* Ben Berkowitz, "Hacking Blitz Drives Cyberinsurance Demand," *Reuters*, June 14, 2011 (last visited Dec. 26, 2012) ("As with any kind of insurance, data breach policies carry all sorts of exclusions that put the onus on the company.").
[140] AIG netAdvantage Specimen Policy, Base Form #91239 (2006), Section 4 (t) .