K&L GATES

CYBERSECURITY:
Minimizing Risk and Managing Consequences

CLE PROGRAM

K&L Gates, Pittsburgh

Tuesday, December 9, 2014

K&L GATES

Cybersecurity: Minimizing Risk and Managing Consequences Agenda

Tuesday, December 9, 2014

2:00 P.M.
WELCOME REMARKS
Carolyn Branthoover (Administrative Partner, K&L Gates-Pittsburgh)

2:00 P.M. - 2:30 P.M.
UNDERSTANDING CYBER RISKS AND SECURITY OPTIONS
Presented by David Bateman (Partner, K&L Gates-Seattle) and David Kennedy (TrustedSEC)

- Identifying cyber risks, including new and emerging threats
- Improving Internet safety and network security

2:30 P.M. - 3:00 P.M.
MANAGING THE CONSEQUENCES OF A DATA BREACH
Presented by Nick Ranjan (Partner, K&L Gates-Pittsburgh) and Roberta Anderson (Partner, K&L Gates-Pittsburgh)

- Civil litigation issues and trends
- The first 24 hours
- Notice requirements

3:00 P.M. - 3:30 P.M.
MANAGING AND MITIGATING CYBER RISKS
Presented by Jeff Maletta (Partner, K&L Gates-Washington, D.C.) and Susan Altman (Partner, K&L Gates-Pittsburgh)

- Understanding the legal framework surrounding cyber risks
- Pro-active management at the Board level
- Vendor contracting

3:30 P.M. - 3:40 P.M.
BREAK

K&L GATES

3:40 P.M. - 4:10 P.M.

GOVERNMENT INITIATIVES AND RESPONSES TO A BREACH
Presented by Mark Rush (Partner, K&L Gates-Pittsburgh), U.S. Attorney David J. Hickton and Assistant U.S. Attorney James T. Kitchen

4:10 P.M. - 4:40 P.M.

INSURING AGAINST CYBER RISKS
Presented by Bob Parisi (Marsh, Inc.) and Roberta Anderson (Partner, K&L Gates-Pittsburgh)

4:40 P.M. - 5:10 P.M.

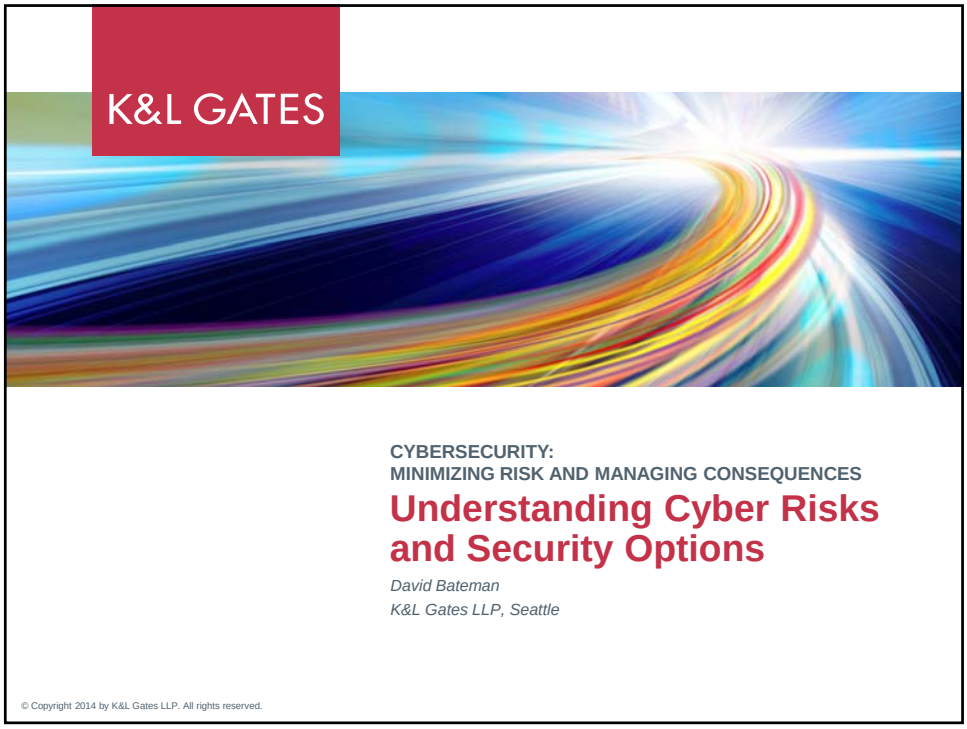
LEGISLATIVE AND REGULATORY INITIATIVES
Presented by Mike O'Neil (Partner, K&L Gates-Washington, D.C.)

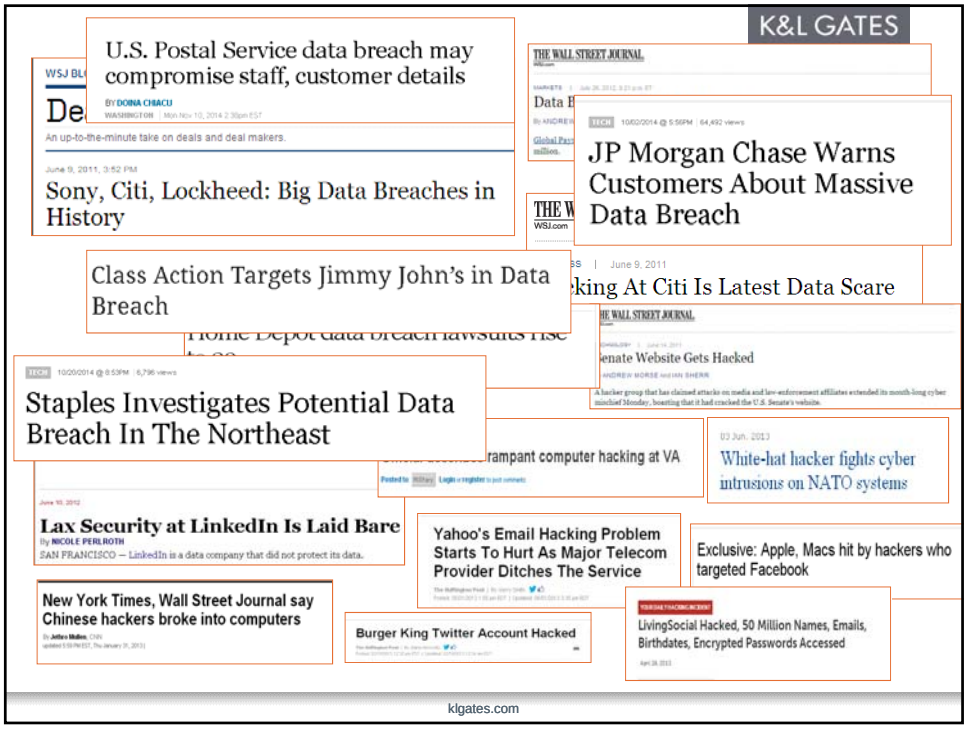
PLEASE JOIN US FOR A NETWORKING AND COCKTAIL RECEPTION FOLLOWING THE PROGRAM.

K&L GATES

Understanding Cyber Risks and Security Options

Presenters: *David Bateman, K&L Gates - Seattle and David Kennedy, TrustedSEC*


K&L GATES
CYBERSECURITY:
MINIMIZING RISK AND MANAGING CONSEQUENCES
Understanding Cyber Risks and Security Options
David Bateman
K&L Gates LLP, Seattle
© Copyright 2014 by K&L Gates LLP. All rights reserved.

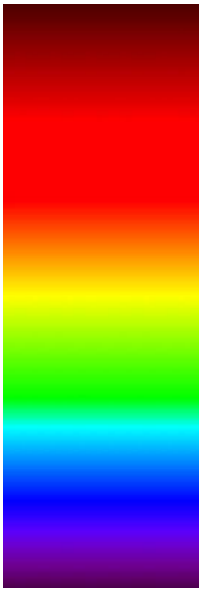

K&L GATES
U.S. Postal Service data breach may compromise staff, customer details
Sony, Citi, Lockheed: Big Data Breaches in History
JP Morgan Chase Warns Customers About Massive Data Breach
Class Action Targets Jimmy John's in Data Breach
Staples Investigates Potential Data Breach In The Northeast
Lax Security at LinkedIn Is Laid Bare
White-hat hacker fights cyber intrusions on NATO systems
Yahoo's Email Hacking Problem Starts To Hurt As Major Telecom Provider Ditches The Service
Exclusive: Apple, Macs hit by hackers who targeted Facebook
New York Times, Wall Street Journal say Chinese hackers broke into computers
Burger King Twitter Account Hacked
LivingSocial Hacked, 50 Million Names, Emails, Birthdates, Encrypted Passwords Accessed
klgates.com

K&L GATES

K&L GATES

The Spectrum of Cyber Attacks

- Advanced Persistent Threats (“APT”)
- Cybercriminals, Exploits and Malware
- Denial of Service attacks (“DDoS”)
- Domain name hijacking
- Corporate impersonation and Phishing
- Employee mobility and disgruntled employees
- Lost or stolen laptops and mobile devices
- Inadequate security and systems: third-party vendors



klgates.com

K&L GATES

The Practical Risks of Cyber Attacks

- Loss of “crown jewels,” IP and trade secrets
- Compromise of customer information, credit cards and other PII
- Loss of web presence and online business
- Interception of email and data communications
- Loss of customer funds and reimbursement of charges
- Brand tarnishment and reputational harm
- Legal and regulatory complications

klgates.com

K&L GATES

Advanced Persistent Threats

- Targeted, persistent, evasive and advanced
- Nation state sponsored

P.L.A. Unit 61398
"Comment Crew"

klgates.com

K&L GATES

Advanced Persistent Threats

- United States Cyber Command and director of the National Security Agency, Gen. Keith B. Alexander, has said the attacks have resulted in the "greatest transfer of wealth in history."

U.S. Blames China's Military Directly for Cyberattacks

By DAVID E. SANGER
Published: May 6, 2013 | 264 Comments

WASHINGTON — The Obama administration on Monday explicitly accused China's military of mounting attacks on American government computer systems and defense contractors, saying one motive could be to map "military capabilities that could be exploited during a crisis."

FACEBOOK
TWITTER
GOOGLE+
SAVE
E-MAIL

U.S. and China Agree to Hold Regular Talks on Hacking

By DAVID E. SANGER and MARK LANDLER
Published: June 1, 2013

WASHINGTON — The United States and China have agreed to hold regular, high-level talks on how to set standards of behavior for cybersecurity and commercial espionage, the first diplomatic effort to defuse the tensions over what the United States says is a daily barrage of computer break-ins and theft of corporate and government secrets.

FACEBOOK
TWITTER
GOOGLE+
SAVE
E-MAIL

Source: New York Times, June 1, 2013.

klgates.com

K&L GATES

Advanced Persistent Threats

- Penetration:
  - 67% of organisations admit that their current security activities are insufficient to stop a targeted attack.*
- Duration:
  - average = 356 days**
- Discovery: External Alerts
  - 55 percent are not even aware of intrusions*

*Source: Trend Micro, USA.
http://www.trendmicro.com/us/enterprise/challenges/advance-targeted-attacks/index.html

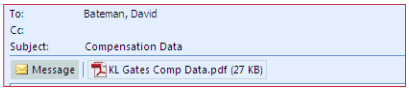
**Source: Mandiant, "APT1, Exposing One of China's Cyber Espionage Units"

klgates.com

K&L GATES

Advanced Persistent Threats: Penetration

- Spear Phishing



- Watering Hole Attack

  rely on insecurity of frequently visited websites

- Infected Thumb Drive

**Source: Mandiant, "APT1, Exposing One of China's Cyber Espionage Units"

*Source: Trend Micro, USA.
http://www.trendmicro.com/us/enterprise/challenges/advance-targeted-attacks/index.html

klgates.com

K&L GATES

Advanced Persistent Threats

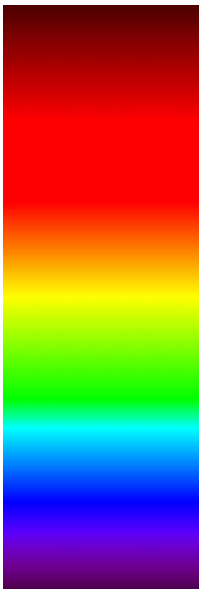
- Target Profiles
  - Industry:
    - *Government*
    - *Information Technology*
    - *Aerospace*
    - *Telecom/Satellite*
    - *Energy and Infrastructure*
    - *Engineering/Research/Defense*
    - *Chemical/Pharma*
  - Activities:
    - Announcements of China deals
    - China presence

klgates.com

K&L GATES

The Spectrum of Cyber Attacks

- Advanced Persistent Threats (“APT”)
- Cybercriminals, Exploits and Malware
- Denial of Service attacks (“DDoS”)
- Domain name hijacking
- Corporate impersonation and Phishing
- Employee mobility and disgruntled employees
- Lost or stolen laptops and mobile devices
- Inadequate security and systems: third-party vendors



klgates.com

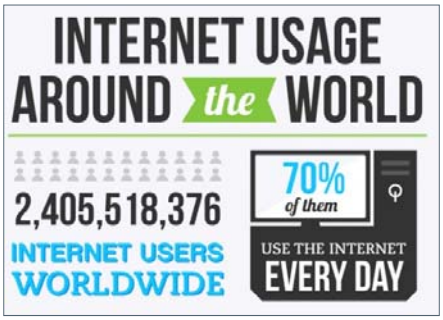
K&L GATES

Cybercriminals, Exploits and Malware

TECHNOLOGY

Russian Hackers Amass Over a Billion Internet Passwords

By NICOLE PERLROTH and DAVID GELLES AUG. 5, 2014



klgates.com

K&L GATES

Cybercriminals, Exploits and Malware

- 60,000 known software vulnerabilities
- 23 new zero-day exploits in 2014

Shellshock Bug May Be Even Bigger Than Heartbleed: What You Need to Know

Sep 26, 2014, 1:18 PM ET

klgates.com

K&L GATES

Cybercriminals, Exploits and Malware

- Ransomware

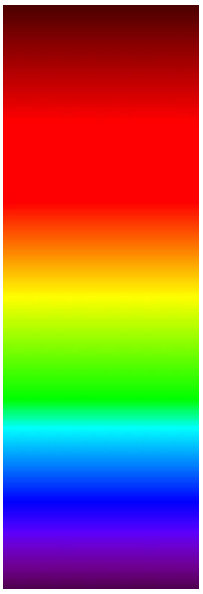
Law Enforcement Spoofing

CryptoLocker

K&L GATES

The Spectrum of Cyber Attacks

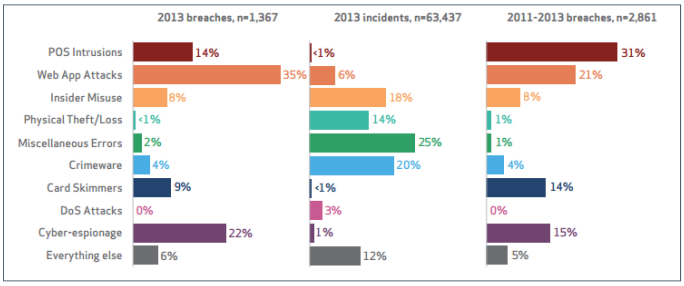
- Advanced Persistent Threats (“APT”)
- Cybercriminals, Exploits and Malware
- Denial of Service attacks (“DDoS”)
- Domain name hijacking
- Corporate impersonation and Phishing
- Employee mobility and disgruntled employees
- Lost or stolen laptops and mobile devices
- Inadequate security and systems: third-party vendors



K&L GATES

Inadequate security and systems: third-party vendors

- Vendors with client data
- Vendors with password access
- Vendors with direct system integration
  - Point-of-sale



klgates.com

K&L GATES

Inadequate security and systems: third-party vendors

TARGET

klgates.com

K&L GATES

Cloud Computing Risks

- Exporting security function and control
- Geographical uncertainty creates exposure to civil and criminal legal standards
- Risk of collateral damage

klgates.com

K&L GATES

Mobile Device Risks

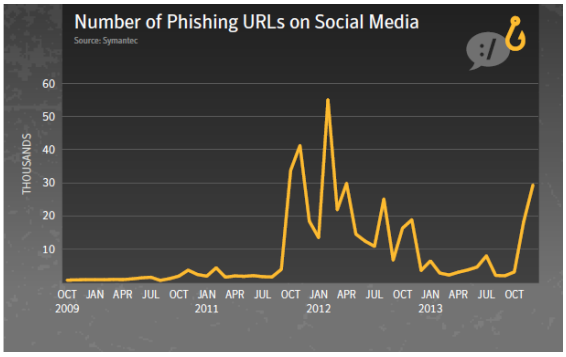
- 52% of mobile users store sensitive files online
- 24% of mobile users store work and personal info in same account
- 21% of mobile users share logins with families
- Mobile malware: apps
- Insufficient mobile platform security

klgates.com

K&L GATES

Social Media Risks

- Consumer harm and reputational damage



klgates.com

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

- Selected to the Washington Super Lawyers List (2004-2013)

K&L GATES

Managing the Consequences of a Data Breach

Presenters: *Nick Ranjan, K&L Gates - Pittsburgh and Roberta Anderson, K&L Gates - Pittsburgh*

K&L GATES

MANAGING THE CONSEQUENCES OF A DATA BREACH

Civil Litigation Issues and Trends

Nicholas Ranjan
K&L Gates LLP, Pittsburgh

K&L GATES

LEGAL FRAMEWORK

- Federal Statutory Violations
  - *e.g.* FCRA, SCA, CFAA, CAN-SPAM Act, GLBA, APA, HIPAA, HITECH Act
- Violations of State Consumer Protection or Unfair Competition Statutes
- Violations of State Privacy, Cybersecurity, and Notice Statutes
- State Common Law Claims
- Securities and Shareholder Claims
- Government Enforcement Tag-Along Actions

K&L GATES

K&L GATES

TYPES OF DAMAGE

- Injuries asserted by data breach plaintiffs
  - Identity theft and resulting financial harm
  - Increased risk of future harm
  - Mitigation
    - Expenses for credit monitoring, card replacement etc.
    - Lost time and inconvenience
  - Emotional distress
  - Violation of privacy
  - Statutory damages

K&L GATES

STANDING ISSUES

- **Injury-in-fact**
  - Most courts have been skeptical that data breach plaintiffs can establish an injury-in-fact for standing purposes
  - Nonetheless, there is some split in the courts on whether increased risk of harm is sufficient to establish an injury-in-fact
    - *Katz,* 672 F.3d 64 (1st Cir. 2012) and *Reilly,* 664 F.3d 38 (3d Cir. 2011) rejected increased risk as basis for standing
    - *Krottner*, 628 F.3d 1139 (9th Cir. 2010) and *Pisciotta,* 499 F.3d 629 (7th Cir. 2007) accepted increased risk as basis for standing
    - *Clapper,* 133 S.Ct. 1138 (2013) reiterated that "threatened injury must be certainly impending to constitute injury in fact, and … [a]llegations of possible future injury are not sufficient"
- **Causation**
  - Even if the court finds injury-in-fact, causation can be difficult to establish
- **Damages**
  - Even if the court finds Article III standing, injury may not result in actual damages, warranting a dismissal for failure to state a claim

K&L GATES

CLASS CERTIFICATION ISSUES

- "Predominance" As a Defense to Class Certification
  - **Causation** – Individualized inquiry may be required to establish that injury to each plaintiff is the result of *this* data breach
  - **Damages** – *In re Hannaford,* 293 F.R.D. 21 (D. Me. 2013) (declining to certify because individualized causation and damages issues predominated)
  - **Consent** – *In re Gmail Litigation*, No. 13-2430 (N.D. Cal. 2013) (declining to certify because individualized issues of consent predominated)
- Arbitration/Class Waiver Provisions
  - *Sanchez v. J.P. Morgan Chase Bank,* 2014 WL 4063046 (S.D. Fla. 2014) (enforcing arbitration clause with class waiver against putative class action plaintiffs)
  - *In re Zappos*.com, 893 F.Supp.2d 1058 (D. Nev. 2012) (declining to enforce arbitration clause where plaintiffs had not consented and terms were illusory)

K&L GATES

CLASS SETTLEMENT ISSUES

- Class action settlements are subject to court approval
- Under CAFA, notice must be sent to federal and state government regulators
- Companies should monitor: (i) what settlements are being approved; (ii) objector rates; (iii) claims rates; (iv) total pay-outs; and (v) reactions to the CAFA notices
- *Fraley v. Facebook,* 2012 WL 5838198 (N.D. Cal. 2012) (preliminary settlement approval denied due to concerns over lack of payment to class, cy pres distribution, and plaintiffs' attorneys fees)

K&L GATES

J. Nicholas Ranjan

Partner

Pittsburgh
T 412.355.8618
F 412.355.6501
nicholas.ranjan@klgates.com

OVERVIEW

Mr. Ranjan is a commercial litigator with “first chair” trial experience, whose practice focuses on class action defense and energy litigation. He was recently selected as one of two “up and coming” litigators in Pennsylvania by Chambers USA.

Mr. Ranjan is also the chair of the Pittsburgh office’s diversity committee and member of the K&L Gates global diversity committee, and is active in leading diversity initiatives within the firm and in the community.

Class Action Defense

Mr. Ranjan’s class action defense experience includes litigating in state and federal courts a variety of consumer, health-care, FTC tag-along, and employment-related class actions. He has handled class certification proceedings and has negotiated complex class settlements, including coupon settlements.

He has counseled clients on telecommunications class action liabilities and risks, including those associated with text messaging and junk faxes under the TCPA. He has represented private equity clients in conducting due diligence associated with class action liabilities. He has also advised clients and published articles on the use of arbitration/class waiver agreements as a means to reduce class-action liability.

In addition to his class-action experience, Mr. Ranjan has handled a number of other complex commercial disputes, ranging from oil and gas/energy, false advertising, intellectual property, catastrophic injury, trade secret, corporate raiding, transportation/3PL, and insurance coverage litigation.

He also has an active pro bono practice, representing prisoners, criminal defendants, and religious entities in free speech, religious liberties, civil rights, criminal, and habeas cases, both at the trial level and on appeal. Several of these cases have garnered local and national media attention.

PROFESSIONAL BACKGROUND

Mr. Ranjan was a judicial clerk to the Honorable Deborah L. Cook of the United States Court of Appeals for the Sixth Circuit.

J. Nicholas Ranjan (continued)

Mr. Ranjan also held the position as the “Simon Karas Fellow” with the Ohio Attorney General solicitor’s office, briefing cutting-edge appellate matters before the Supreme Court of the United States, federal courts of appeals, and the Ohio Supreme Court.

RECENT CLASS ACTION-RELATED PUBLICATIONS

- “Connecticut Supreme Court Issues Decision that Could Expand State Law Liability in Data Breach Class Actions for Businesses Subject to HIPAA,” Nov. 21, 2014
- “Lessons Learned from the Fourth Circuit’s Decision to Vacate Class Certification in Coalbed Methane Royalty Underpayment Cases,” Sept. 29, 2014
- “The Third Circuit Issues a “Double-Edged” Decision that Could Increase Individual Lawsuits under the Telephone Consumer Protection Act, but Limit TCPA Class Actions,” Sept. 23, 2013
- “Arbitration/Class Waiver Clauses in Oil and Gas Leases: The Applicability of Concepcion and Italian Colors Restaurant to the Natural Gas Industry,” Sept. 11, 2013

PROFESSIONAL/CIVIC ACTIVITIES

Mr. Ranjan has been an active mentor for Pittsburgh-area middle-school, high-school, and law-school students, and has been featured by various local news outlets, Duquesne University, and the United Way for his mentoring activities.

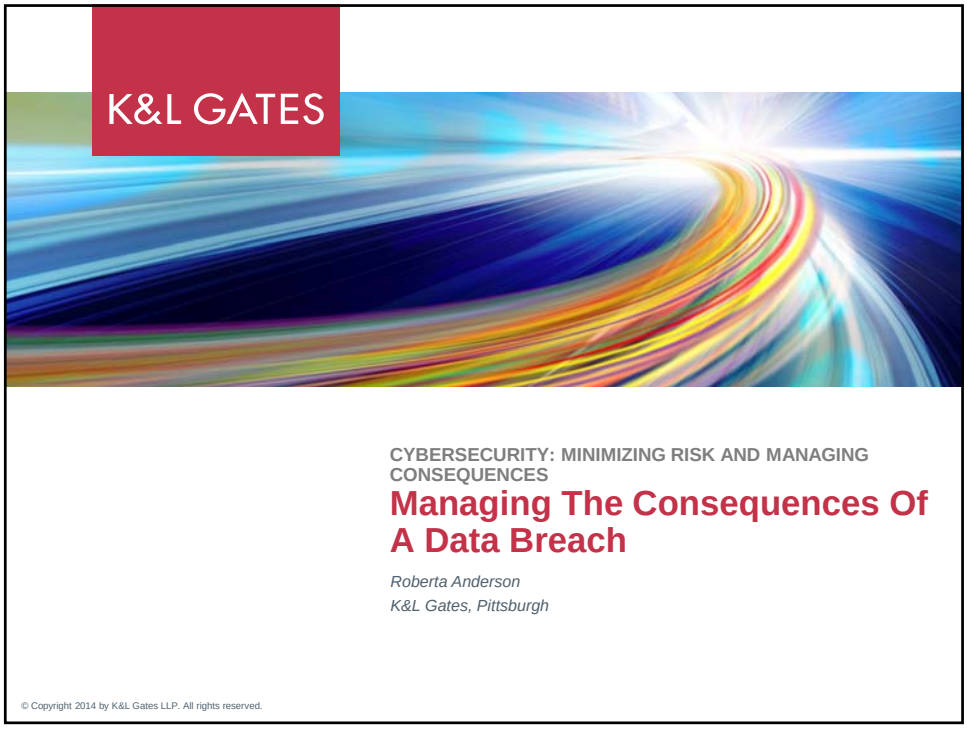
Mr. Ranjan was a recipient of the Leadership Excellence Award, awarded by the Pittsburgh Leadership Conference.

Mr. Ranjan is also an accomplished classical and jazz violinist of over 30 years.

EDUCATION

J.D., University of Michigan Law School, 2003 (*cum laude*; Note Editor, *The Michigan Law Review*)

B.A., Grove City College, 2000 (*summa cum laude*)


K&L GATES
CYBERSECURITY: MINIMIZING RISK AND MANAGING CONSEQUENCES
Managing The Consequences Of A Data Breach
Roberta Anderson
K&L Gates, Pittsburgh
© Copyright 2014 by K&L Gates LLP. All rights reserved.


MANAGING THE CONSEQUENCES OF A DATA BREACH

K&L GATES

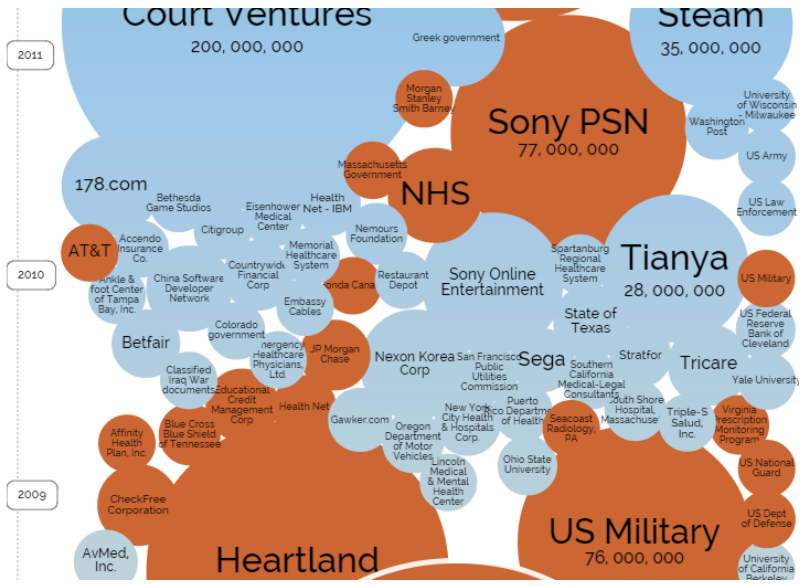
K&L GATES

MANAGING THE CONSEQUENCES OF A DATA BREACH

Agenda

- Achieving cyber-reliance in the face of increased risk and exposure
  - The last 18 months
  - The next 60 days
  - The first 24 hours
- Notice requirements

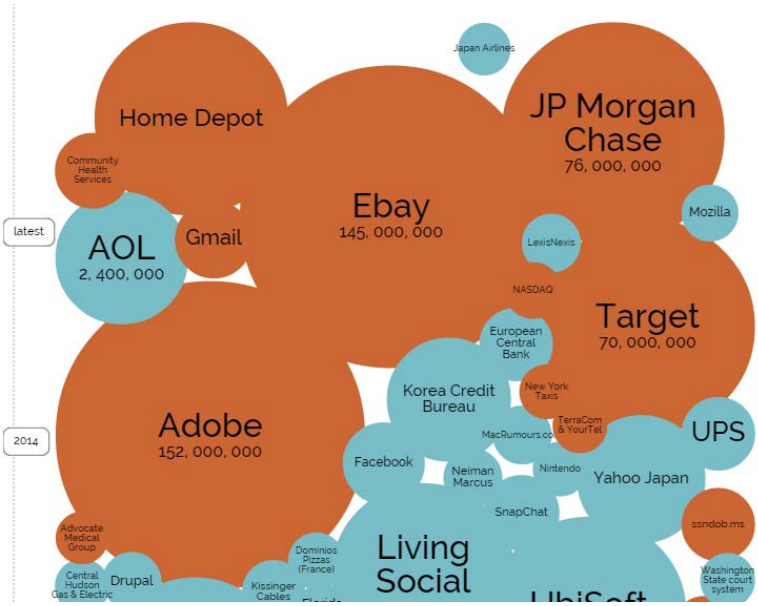
klgates.com



http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

4

klgates.com



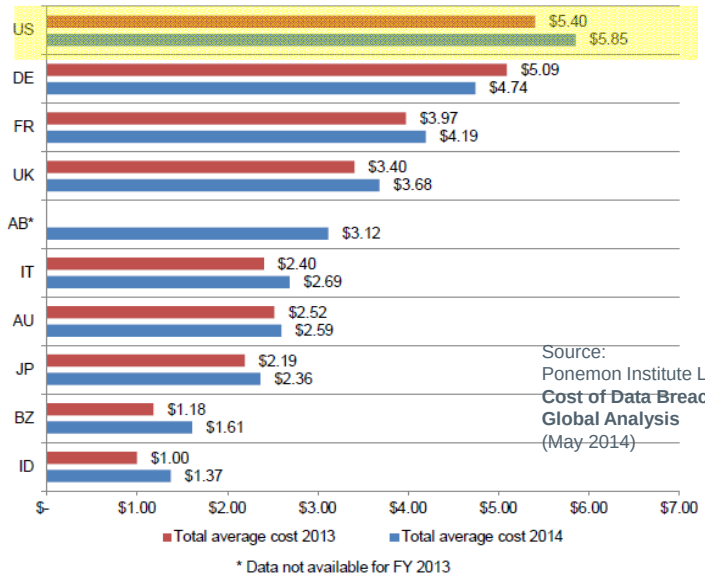
http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

5

klgates.com

K&L GATES

Figure 3. The average total organizational cost of data breach over two years
Measured in US$ ($000,000 omitted)



* Data not available for FY 2013

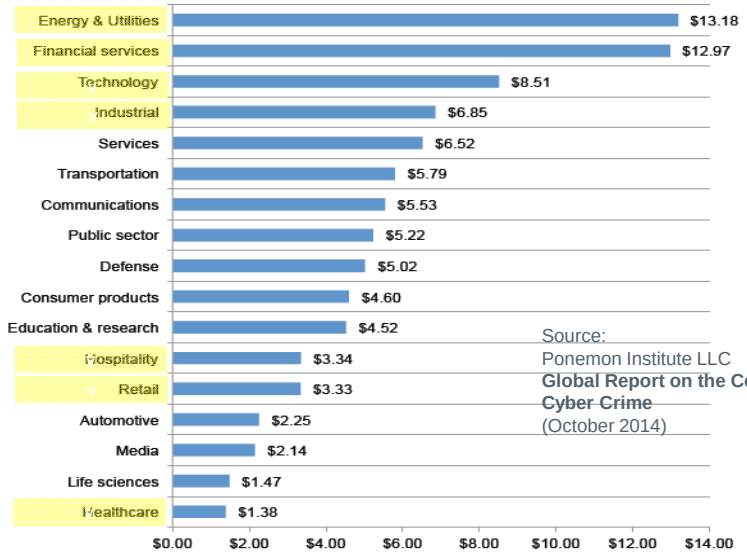
Source:
Ponemon Institute LLC
Cost of Data Breach Study: Global Analysis
(May 2014)

6

klgates.com

K&L GATES

Figure 7. Average annualized cost by industry sector
Cost expressed in US dollars, $1,000,000 omitted
Consolidated view, n = 257 separate companies

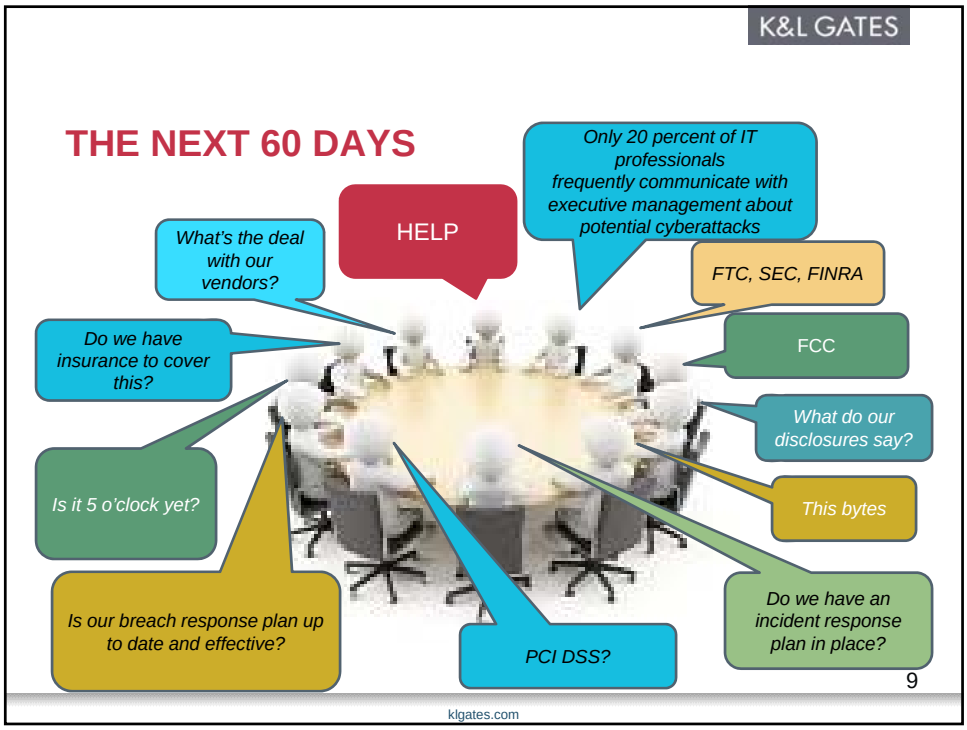


Source:
Ponemon Institute LLC
Global Report on the Cost of Cyber Crime
(October 2014)

7

klgates.com


THE NEXT 60 DAYS


K&L GATES
THE NEXT 60 DAYS
HELP
Only 20 percent of IT professionals frequently communicate with executive management about potential cyberattacks
What's the deal with our vendors?
FTC, SEC, FINRA
Do we have insurance to cover this?
FCC
What do our disclosures say?
Is it 5 o'clock yet?
This bytes
Is our breach response plan up to date and effective?
PCI DSS?
Do we have an incident response plan in place?
9
klgates.com

K&L GATES

K&L GATES

THE NEXT 60 DAYS

How to become resilient

- C-Suite attention
- Cybersecurity assessment
- Compliance review
- Breach response plan
- Employee training
- Vendors
- Information governance
- Insurance

klgates.com

K&L GATES

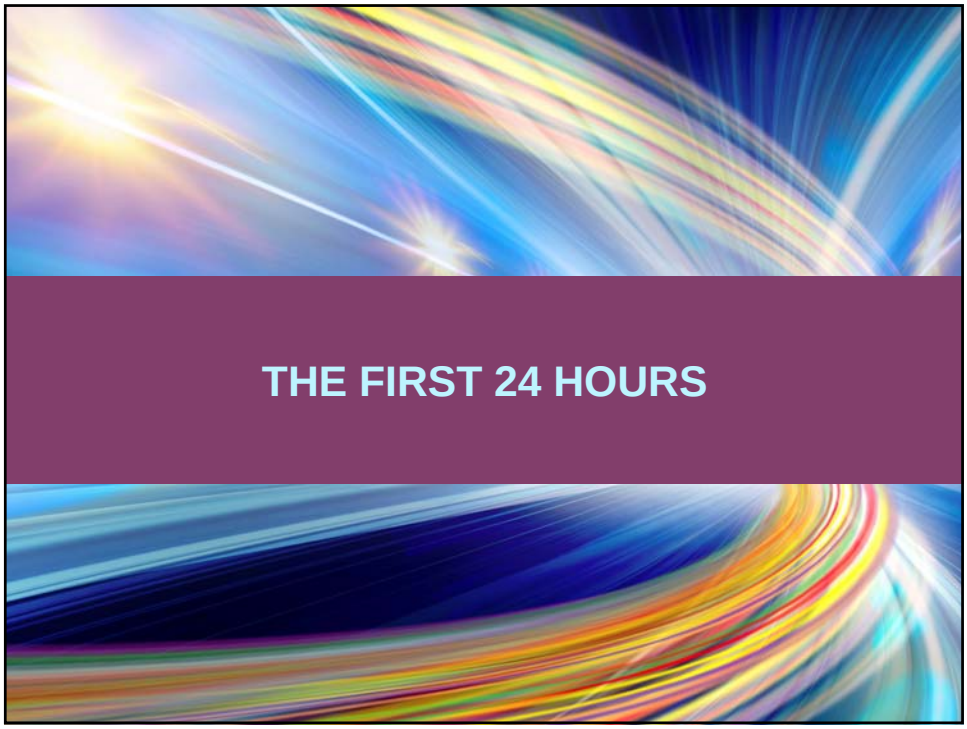
THE NEXT 60 DAYS

Ponemon INSTITUTE

- **Factors that decreased and increased the cost of a data breach.** Having a strong security posture, incident response plan and CISO appointment reduced the cost per record by $14.14, $12.77 and $6.59, respectively. Factors that increased the cost were those that were caused by lost or stolen devices (+ $16.10), third party involvement in the breach (+ $14.80), quick notification (+ $10.45) and engagement of consultants (+ $2.10).

Source:
Ponemon Institute LLC
Cost of Data Breach Study: Global Analysis
(May 2014)

klgates.com



K&L GATES

THE FIRST 24 HOURS

Don't panic. Follow the plan.

- Mobilize first-response team
- Immediately call breach coach counsel
- Forensics
  - Investigate, isolate, contain, and secure systems / data
  - Preserve evidence
  - Document everything
- PR
- Consider contacting law enforcement
- Start thinking notification

klgates.com

K&L GATES

K&L GATES

THE FIRST 24 HOURS

Don't Panic.

1. Record the date and time of discovery and time when response efforts begin
2. Alert and activate everyone on the response team, including external resources, to begin executing your preparedness plan.
3. Investigate, while preserving evidence
4. Stem additional data loss
5. Document **everything** known about the breach.

Follow the plan.

6. Interview those involved in discovering the breach and anyone else who may know about it.
7. Consider notifying law enforcement after consulting with legal counsel
8. Revisit state and federal regulations governing your industry and the type of data lost.
9. Determine all persons/entities that need to be notified, i.e. customers, employees, the media,
10. Ensure all notifications occur within any mandated timeframes.

klgates.com

K&L GATES

K&L GATES

NOTICE REQUIREMENTS

Ponemon INSTITUTE

- **Factors that decreased and increased the cost of a data breach.** Having a strong security posture, incident response plan and CISO appointment reduced the cost per record by $14.14, $12.77 and $6.59, respectively. Factors that increased the cost were those that were caused by lost or stolen devices (+ $16.10), third party involvement in the breach (+ $14.80), quick notification (+ $10.45) and engagement of consultants (+ $2.10).

Source:
Ponemon Institute LLC
Cost of Data Breach Study: Global Analysis
(May 2014)

klgates.com

K&L GATES

NOTICE REQUIREMENTS

Different types notice

- Industry-specific, e.g. HIPAA / HITECH
- 47 different state notification laws
  - e.g., Pennsylvania
- Business partners
  - e.g., New Jersey
- Others, e.g., Regulators, AGs, consumer reporting agencies, law enforcement?
- Media
- Social media
- SEC filings

klgates.com

K&L GATES

K&L GATES

NOTICE REQUIREMENTS

Industry-specific, e.g. HIPAA / HITECH

45 C.F.R. § 164.404

(a) Standard--

(1) General rule. A covered entity shall, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach.

(2) Breaches treated as discovered. For purposes of paragraph (a)(1) of this section, §§ 164.406(a), and 164.408(a), a breach shall be treated as discovered by a covered entity as of the first day on which such breach is known to the covered entity, or, by exercising reasonable diligence would have been known to the covered entity. A covered entity shall be deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent of the covered entity (determined in accordance with the federal common law of agency).

(b) Implementation specification: Timeliness of notification. Except as provided in § 164.412, a covered entity shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.

klgates.com

K&L GATES

NOTICE REQUIREMENTS

47 different state notification laws, e.g., Pennsylvania

§ 2303. General rule.

(a) General rule.--An entity that maintains, stores or manages computerized data that includes personal information shall provide notice of any breach of the security of the system following discovery of the breach of the security of the system to any resident of this Commonwealth whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person. Except as provided in section 4 [FN1] or in order to take any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system, the notice shall be made without unreasonable delay. For the purpose of this section, a resident of this Commonwealth may be determined to be an individual whose principal mailing address, as reflected in the computerized data which is maintained, stored or managed by the entity, is in this Commonwealth.

§ 2308. Civil relief. A violation of this act shall be deemed to be an unfair or deceptive act or practice in violation of the act of December 17, 1968 (P.L. 1224, No. 387), known as the Unfair Trade Practices and Consumer Protection Law. The Office of Attorney General shall have exclusive authority to bring an action under the Unfair Trade Practices and Consumer Protection Law for a violation of this act.

19

klgates.com

K&L GATES

K&L GATES

NOTICE REQUIREMENTS

Business partners, e.g., New Jersey

N.J.S.A. 56:8-163

Any business or public entity that compiles or maintains computerized records that include personal information on behalf of another business or public entity shall notify that business or public entity, who shall notify its New Jersey customers, as provided in subsection a. of this section, of any breach of security of the computerized records immediately following discovery, if the personal information was, or is reasonably believed to have been, accessed by an unauthorized person.

20

klgates.com

K&L GATES

NOTICE REQUIREMENTS

Others?

21

klgates.com

K&L GATES

THE MEDIA

K&L GATES

SOCIAL MEDIA

K&L GATES

SEC FILINGS

We note your disclosure that an unauthorized party was able to gain access to your computer network "in a prior fiscal year." So that an investor is better able to understand the materiality of this cybersecurity incident, please revise your disclosure to identify when the cyber incident occurred and describe any material costs or consequences to you as a result of the incident. Please also further describe your cyber security insurance policy, including any material limits on coverage.

- Alion Science and Technology Corp. S-1 filing (March 2014)

K&L GATES

AN INTERNATIONAL ISSUE

25

klgates.com

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 with over fifteen years of experience in complex commercial litigation and alternative dispute resolution. A member of the firm's global Insurance Coverage practice group, and a co-founder of the firm's global Cyber Law and Cybersecurity practice group, Ms. Anderson concentrates her practice in the areas of insurance coverage litigation and counseling and emerging cybersecurity and data privacy-related issues, including incident planning and response. She has represented policyholders in connection with a broad spectrum of insurance issues and disputes arising under almost every kind of business insurance, including general liability, commercial property and business interruption, data privacy and "cyber" liability, directors and officers (D&O) liability, errors and omissions (E&O), technology E&O, professional liability, employment practices liability (EPL), political risk, environmental, fidelity, fiduciary, crime, terrorism, residual value, and nuclear. Ms. Anderson provides strategic advice on ways to maximize the value of clients' current and historic insurance assets.

Ms. Anderson also counsels clients on complex underwriting and risk management issues. She has unique and substantial experience in the drafting and negotiation of D&O, technology E&O, data privacy and "cyber"-liability, and other insurance coverages. She provides strategic insurance coverage advice to clients in assessing their potential risks, analyzing new insurance products, considering the adequacy of existing insurance programs, and negotiating new placements tailored to the clients' specific risk profile. 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

A recognized national authority in insurance coverage, cybersecurity and data privacy related issues, Ms. Anderson frequently lectures on these subjects, including for the American Bar Association (ABA), the Risk and Insurance Management Society (RIMS), the Pennsylvania Bar Association, Practicing Law Institute, Strafford Continuing Legal Education, and Law Seminars International. In addition, she regularly provides interviews and comments on these subjects to

Roberta D. Anderson (continued)

leading industry publications, such as *Law360* and *Advisen*. Ms. Anderson also publishes extensively, and currently serves on a number of editorial boards for leading industry publications, including 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 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.

SPEAKING ENGAGEMENTS AND INSTRUCTION

LIVE PRESENTATIONS (CLE, CPU, CE AND CPD)

- Panelist: "The Board's Role in Management of Cybersecurity and Data Privacy Threats: Achieving Cybersecurity and Data Privacy Resilience Before the Breach," K&L Gates LLP (Seattle, WA), November 25, 2014
- Panelist: "The Exchange Data Privacy and Cyber Security Forum," Today's General Counsel and Institute (Capital Hilton, Washington, DC), November 18, 2014
- Lecturer: "Cyber Risk, Regulatory Issues, and Insurance Mitigation," ISACA Pittsburgh Information Security Awareness Day (Rivers Casino, Pittsburgh, PA), November 17, 2014
- Panelist: "Cyber Speed Debates 2.0," 2014 PLUS Conference, November 6, 2014 (Caesars Palace, Las Vegas, NV)
- Panelist: "Boardroom Risks," 22nd Annual SMU Corporate Counsel Symposium, October 31, 2014 (Park Cities Hilton, Dallas, TX)
- Panelist/Moderator: "Coverage Considerations," Advisen 2014 Cyber Risk Insights Conference , October 28, 2014 (Grand Hyatt, New York, NY)
- Lecturer: "Cyber Crimes: Trends and Protections," The Allegheny Chapter CPCU All Industry Day,, October 15, 2014 (Wyndham Grand, Pittsburgh, PA)
- Panelist: "Cyber Risk and Global Security Issues: is your business fully prepared?," October 2, 2014 (One New Change, London)
- Lecturer: "Cybersecurity Law 2014: Minimizing Data Legal Liability Risk in the Digital Age," Pennsylvania Bar Institute CLE Program, August 11, 2014 (Pittsburgh, PA)
- Panelist: "D&O & Cyber Forum," AON, May 7, 2014 (The Duquesne Club, Pittsburgh, PA)
- Speaker/Coordinator: "Cyber3.0: Cutting Edge Advancements in Insurance Coverage For Cyber Risk & Reality," RIMS Annual Conference, April 29, 2014 (Denver. CO)

Roberta D. Anderson (continued)

- Panelist: “What Your Company Needs to Know about Cybersecurity,” OCTANe Presentation, April 17, 2014 (Irvine, CA)
- Lecturer: “Cutting-Edge Advancements in Insurance Coverage for Cyber Risk and Reality,” RIMS Pittsburgh Chapter Meeting, April 8 2014 (Pittsburgh, PA)
- Panelist: “Cybersecurity Threats in the Financial Sector,” March 5, 2014 (Pershing LLC, Jersey City, NJ)
- Panelist: “Who's On First? Insurance Coverage For Mass And Class Actions,” ABA Tort Trial & Insurance Practice Section Insurance Coverage Litigation Committee Midyear Program, February 20-22, 2014 (Pheonix, AZ)
- Speaker: “Cybersecurity and Privacy: Managing Threats, Risks and Protection,” October 22, 2013 (University Club, Palo Alto, CA)
- Speaker: “Insurance Coverage For Cyber Risks And Realities,” Co-Sponsored by the Association of Corporate Counsel, Western Pennsylvania Chapter and K&L Gates, September 24 ,2013 (Pittsburgh, PA)
- Speaker: "Additional Insured Coverage & Contractual Indemnification," K&L Gates Insurance Coverage Training Series CLE, June 3, 2013 (Pittsburgh, PA)
- Speaker: “Cyber Risk And Insurance,” K&L Gates Insurance Coverage Training Series CLE, September 5, 2012 (Pittsburgh, PA)
- Panelist: “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)
- Speaker: "Insurance Coverage Training Series: Nuclear-Related Liabilities" Insurance Coverage Training Series CLE, January 7, 2009 (Pittsburgh, PA)
- Panelist: “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 Insurance Coverage Litigation Committee Midyear Program, February 28–March 1, 2008 (Marina Del Rey, CA)
- Panelist: “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 Insurance Coverage Litigation Committee Midyear Program, February 15–17, 2007 (Tucson, AZ)
- Speaker: “Challenging the Guidelines & the Carrier’s Response,” LexisNexis® Mealeys™ Litigation Management Guidelines Conference, July 20-21, 2006 (New York, NY)
- Speaker: “Broker Contingent Commissions Investigations,” RIMS Pittsburgh Chapter Meeting, April 2005 (Pittsburgh, PA)
- Speaker: “Getting the Most Out of Lloyd’s And Equitas: Basics I: Organization And Terminology,” ABA Section of Litigation Essential Intelligence for US Coverage Lawyers™ Conference, May 14-15, 2002 (Chicago, IL)

Roberta D. Anderson (continued)

LIVE WEBINARS

- Panelist: “Feeling the Heat? How to Cool Off with Cyber Risk Insurance,” AccessData Webinar, October 16, 2014
- Lecturer: “Data Privacy and Cybersecurity Due Diligence in M&A Deals,” Strafford CLE Webinar, October 9, 2014
- Panelist: “Cyber Exposures of Small and Mid-Size Businesses – A Digital Pandemic,” Advisen, October 7, 2014
- Lecturer: “Dropping the ‘Hammer’ on Security Threats with Rapid Detection and Resolution,” ALM Virtual LegalTech Webinar, September 12, 2014
- Lecturer: “FDIC and Other Banking Agency Litigation Against Auditors, Law Firms, Appraisers and Other Outside Advisors: Latest Developments in Defending Agency Claims and Maximizing E&O Insurance Coverage,” Strafford CLE Webinar, August 7, 2014
- Lecturer: “Insurance Coverage for Data Breaches and Privacy Violations: Are Your Corporate Clients Truly Protected?,” Strafford CLE Webinar, August 6, 2014
- Panelist: “Cyber Sanity: Innovative Approaches to Data Security,” Advisen, July 22, 2014
- Lecturer: “Before the Breach: Insurance and Other Ways to Proactively and Effectively Mitigate Cyber Risk,” FX Conferences, July 14. 2014
- Lecturer: “Cybersecurity Brief: Understanding Risk, Legal Framework, & Insurance Managing a Cyber Disaster: Cyber Insurance and Tools to Mitigate Losses and Liability 2014,” Practicing Law Institute CLE Webcast, July 8, 2014
- Lecturer: “Cyber-Attacks: Insurance Coverage for Cyber Risks and Realities,” K&L Gates CLE Webinar, June 25, 2014 (Pittsburgh, PA)
- Lecturer: “Cybersecurity Brief: Understanding Risk, Legal Framework, & Insurance,” Securedocs Webinar, June 12, 2014
- Lecturer: “Cultivating Ethics: Mitigating Vulnerability to Cyber and Data Security Threats in Order to Maintain Client Confidentiality.” ALM Virtual LegalTech Webinar, May 15, 2014
- Lecturer: “Insurance Coverage for Data Breaches and Privacy Violations: Are Your Corporate Clients Truly Protected?,” Strafford CLE Webinar, February 26, 2014
- Lecturer: “Insurance Coverage For Cyber Security Beaches: Insurance Strategies For Managing Cyber Risk,” Law Seminars International TeleBriefing, October 25, 2013
- Speaker: “What Your Company Needs to Know about Cybersecurity,” K&L Gates Webinar, June 6, 2013 (Pittsburgh, PA)

Roberta D. Anderson (continued)

INTERVIEWS/MEDIA QUOTES

- “The Hidden Strategic Advantage in Cyber Insurance,” Jim McFarland for SecurityWeek, December 4, 2014
- “Cybersecurity Experts Warn Pittsburgh Conference About Dangers Of Hacking,” Pittsburgh Tribune-Review, Nov. 17, 2014
- “Cyber-Insurance Becomes Popular Among Smaller, Mid-Size Businesses ,” The Washington Post, August 12, 2014
- “Financial Institutions Warned On Cyber-Insurance ,” COOConnect, October 8, 2014
- “Insurers Flocking To Data Breach Exclusions In CGL Policies,” Law360, August 27, 2014
- “Cybersecurity easing its way into M&A due diligence,” Advisen Cyber Risk Network, August 22, 2014
- “Disruptors,” Fox Business News, August 20, 2014
- “Specialized Cyber Insurance Becoming A Must For Many Cos.,” Law360, August 12, 2014
- “Cyber Security Insurance Difficult for Business to Navigate,” The Huffington Post, August 4, 2014
- “Third-party Vendor Contracts Must Reflect Data Risk,” Advisen Cyber Risk Network, May 30, 2014
- “FTC Shines Data Security Badge After Wyndham Ruling,” Advisen Cyber Risk Network, April 14, 2014
- “Cyber Insurance vs. General Liability,” The Huffington Post, April 10, 2014
- “Cyber Threat: Aviation, Unmanned Risk,” Risk & Insurance, April 7, 2014
- “No Right Way Or Right Time, But Data Breach Notification A Must,” Advisen Cyber Risk Network, April 4, 2014
- "NIST Cybersecurity Framework Remains Potential Standard of Care, Lawyers Say," Vol. 34, No. 46, Communications Daily, March 10, 2014
- ”Policy Language Interpretation Favors Insurers in Sony Case,” Advisen Cyber Risk Network, March 7, 2014
- “Sony Coverage Denial Could Be Boon For Cyber Insurers,” Law360, February 25, 2014
- “Insurers prepare for implementation of new cyber liability exclusions,” Business Insurance, January 19, 2014
- “Cyber policies a good deal, but choose carefully,” Healthcare Risk Management, Vol. 36, No. 1, January 2014
- “Insurer tried to say CGL offered no breach coverage,” Healthcare Risk Management, Vol. 36, No. 1, January 2014
- “Court says insurer liable for data breach expenses,” Healthcare Risk Management, Vol. 36, No. 1, January 2014

Roberta D. Anderson (continued)

- "Target credit card thefts a cue to review cyber coverage terms," Advisen, December 23, 2013
- "TalkingPoint: Managing Risk In The Chemicals Industry," Financer Worldwide, December 2013
- "CGL exclusions will fuel cyber purchase trend," Advisen, November 18, 2013
- "PA Ruling Favors Nuclear Insurers," Business Insurance, December 6, 2002

PUBLICATIONS

"CYBER" INSURANCE

- What to Consider When Buying Cyberinsurance, *Risk Management Magazine*, October 1, 2014
- Retailers Face a Blizzard of Breaches: Are You Covered?, *Insurance Coverage Alert*, September 11, 2014, originally published in *Law360*, September 2, 2014
- Why Buy Cyber and Privacy Liability Insurance, *Insurance Thought Leadership*, July 21, 2014
- You Have a Perfectly Good CGL, So Why Buy Cyber and Privacy Liability Insurance?, *Advisen Cyber Risk Network*, July 15, 2014
- Why Buy Cyber and Privacy Liability When You Have a Perfectly Good Commercial General Liability Program?, *Advisen Risk Network*, July 3, 2014
- Does Your Cybersecurity Policy Cover Cyberterrorism?, *Advisen Cyber Risk Network*, June 5, 2014
- Viruses, Trojans and Spyware, Oh My! The Yellow Brick Road to Coverage in the Land of Internet Oz, *Tort Trial & Insurance Practice Law Journal*, Vol. 49-2, May 2014
- Coming To A CGL Policy Near You: Data Breach Exclusions, *Law360,* April 23, 2014
- Does Your Insurance Cover a Data Breach? Don't Be So Sure, *The Security Advocate*, April 21, 2014
- Another Reason to Consider Cyber Insurance, *Insurance Thought Leadership*, April 3, 2014
- Viruses, Trojans and Spyware, Oh My! The Yellow Brick Road to Coverage in the Land of Internet Oz, *FC&S Legal, The Insurance Coverage Law Report*, Part I (December 2013/January 2014), Part II (February 2014), Part III (March 2014), and Part IV (April 2014)
- Coming Soon to a CGL Policy Near You: ISO's New Data Breach Exclusions, *Advisen Cyber Risk Network*, March 21, 2014
- How to Purchase Cyber Insurance, *Insurance Thought Leadership*, March 14, 2014
- Five Reasons Why The Sony Data Breach Coverage Decision Is Wrong, *Insurance Coverage Alert*, March 10, 2014, originally published in *Law360*, February 28, 2014

Roberta D. Anderson (continued)

- Recall Decision Points Toward CGL Coverage For Data Breach, *Advisen Cyber Risk Network*, January 24, 2014
- Before Becoming The Next Target: Recent Case Highlights The Need To Consider Insurance For Data Breaches, *Insurance Coverage Alert,* January 16, 2014, originally published in *Law360*, January 14, 2014
- How to Purchase Cyber Insurance, *FC&S Legal, The National Underwriter Company*, January 2014
- Top 10 Tips For Insuring Cyber Risks, The Risk Report, *International Risk Management Institute, Inc. (IRMI)*, Volume XXXVI, No. 4, December 2013
- Recent California Decision Upholds Data Breach Coverage, *Commercial Disputes Alert*, November 26, 2013
- How to Secure Data Breach Coverage, *FC&S Legal, The Insurance Coverage Law Information Center*, November 26, 2013
- Some Traditional Insurance Policies May Cover Data Breach, *Law360*, November 19, 2013
- When Companies Need Cyber Insurance, *Today's General Counsel*, October 25, 2013
- Cyber Insurance - Selecting the Right Policy to Identify and Mitigate Risk*, TMT Law Watch Blog*, October 23, 2013, *Legal Cloud Central Blog*, October 25, 2013
- How to Purchase "Cyber" Insurance, *Insurance Coverage Alert*, October 21, 2013
- Recent California Decision Holds That Privacy / Data Breach Liability Covered Under "Traditional" Insurance Policy, *Insurance Coverage Alert*, October 18, 2013
- How to Purchase "Cyber" Insurance, *FC&S Legal, The Insurance Coverage Law Information Center*, October 17, 2013
- ISO's Newly-Filed Data Breach Exclusions Provide Yet Another Reason To Consider "Cyber" Insurance, *Law360*, September 26, 2013
- Yet Another Reason To Consider Cyber Insurance, *Law360*, September 23, 2013
- Extend Cyber Insurance Coverage To The Cloud, *Today's General Counsel*, July 10, 2013
- Shine a Spotlight on Cyber "Cloud" Coverage, *IRMI Update*, Issue 297, July 10, 2013
- Spotlight On Cyber "Cloud" Insurance Coverage, *Legal Cloud Central Blog*, July 1, 2013
- Insurance Coverage for Cyber Attacks, *The Insurance Coverage Law Bulletin*, Part 1, Volume 12, Number 4, May 2013, and Part 2, Volume 12, Number 5, June 2013
- The Role of Insurance in the Land of Viruses, Trojans, and Spyware, *Coverage*, Volume 23, Number 1, January-February 2013
- "Cyber-Attacks": Important Insurance Coverage Considerations, *Insurance Coverage Alert*, June 30, 2011
- Insurance Coverage for "Cyber-Losses," 35 Tort & Ins. L. J. 891, *Tort & Insurance Law Journal*, Summer 2000

Roberta D. Anderson (continued)

- Companies May Be Covered For Business Interruption or Related Losses Resulting from "Hacker Attacks" and Other E-Commerce Risks, *Insurance Coverage Bulletin*, March 2000

CYBERSECURITY AND DATA PRIVACY

- Cybersecurity: Five Tips to Consider When Any Public Company Might be the Next Target, *Global Boardroom Risk Solutions Newsletter*, July 2014
- 3 Tips for Navigating Data Breaches, *Insurance Thought Leadership*, July 14, 2014
- Tips For Navigating US And International Data Breaches, *Law360*, June 20, 2014
- Cyber Challenges Under NIST's Framework, *Insurance Thought Leadership*, April 21, 2014
- FTC Has Power to Regulate Data Security Practices, Court Rules, *TMT Law Watch Blog*, April 17, 2014
- Target Security Breach Could Be a Wake-up Call, *Pittsburgh Post-Gazette*, April 12, 2014
- Cybersecurity: Five Tips on Disclosure Requirements, *Insurance Thought Leadership*, March 24, 2014
- After Data Breach, The Best First Responder Is A Law Firm, *Law360*, Interview, March 13, 2014
- NIST Unveils Cybersecurity Framework, *Cybersecurity and Insurance Coverage Alert*, February 17, 2014
- Five Tips to Consider When Any Public Company Might be The Next Target, *Cybersecurity Risk Factors Alert*, February 11, 2014
- 5 Cybersecurity Considerations For Public Companies, *Law360*, February 10, 2014
- Suffer a Data Breach? Your 1st Call Should Be to… a Lawyer, *The Security Advocate,* Interview, January 27, 2014
- NIST Unveils Preliminary Cybersecurity Framework, *Cybersecurity Alert*, November 25, 2013
- Shine a Spotlight on Cyber "Cloud" Coverage, *IRMI Update*, Issue 297, July 10, 2013
- Policy Matters: Insurance Facts of Life Every IT Leader Should Know, *Best Practices In IT Leadership*, October 2000

DIRECTORS AND OFFICERS LIABILITY INSURANCE

- *U.S. Bank v. Indian Harbor*: Insurers Face Another Restitution/Disgorgement Setback, *Insurance Coverage Alert*, September 11, 2014
- Your D&O Insurance Policy Post-Halliburton, *Insurance Coverage Alert*, July 28, 2014
- Your D&O Insurance Policy Post-Halliburton, *Law360*, July 25, 2014

Roberta D. Anderson (continued)

- Halliburton II: Supreme Court Upholds Fraud on the Market Presumption, but Gives Securities Defendants a Fighting Chance at Defeating Class Certification, *Securities and Transactional Litigation Alert*, July 7, 2014
- Basic fraud-on-the-market presumption survives Halliburton, *Advisen Risk Network*, July 1, 2014
- Untimely Notice Under a Claims-Made Policy, *The Insurance Coverage Law Bulletin*, Vol. 8, No. 5, June 2009
- A Timely Lesson From The WorldCom And Enron Settlements: Make Sure Your D&O Program Is Adequate, *Insurance Coverage Alert*, January 2005
- Insurance Coverage for Investigations and Demands of State Attorneys General, *Insurance Coverage Alert*, September 2005
- 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*, Vol. XXVI, No. 7, February 17, 2003

BUSINESS INTERRUPTION INSURANCE

- The Calm Before the Storm Is the Time to Consider Insurance Coverage, *The Insurance Coverage Law Bulletin* Part I, Volume 12, Number 12, January 2014, and Part 2, Volume 12, Number 13, February 2014
- Recent Developments in a Post-Sandy World, Recent Developments in Insurance Coverage Litigation, 49 Tort Trial & Ins. Prac. L.J. 271, Fall 2013
- Key Insurance Coverage Considerations in the Wake of Superstorm Sandy, *The Insurance Coverage Law Bulletin,* Volume 11, Number 12, January 2013
- 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
- Recent Developments in Insurance Coverage Litigation, 47 Tort Trial & Ins. Prac. L.J. 297, *Tort Trial & Insurance Practice Law Journal,* Fall 2011
- Losses from Hurricane Irene: Are You Covered?, *Insurance Coverage Alert*, August 30, 2011
- Disaster in Japan: Worldwide Insurance Coverage Considerations, *Insurance Coverage Alert*, March 16, 2011
- Potential Business Interruption Coverage: July 18, 2007 Manhattan Steam Pipe Explosion, *Insurance Coverage Alert*, August 31, 2007
- Companies May Be Covered For Business Interruption or Related Losses Resulting from "Hacker Attacks" and Other E-Commerce Risks, *Insurance Coverage Bulletin*, March 2000

Roberta D. Anderson (continued)

COMMERCIAL GENERAL LIABILITY INSURANCE

- Texas Supreme Court Holds “Contractual Liability” Exclusion Inapplicable, *Insurance Coverage Alert,* January 21, 2014
- Texas High Court Fortunately Says 'No' In Ewing, *Law360*, January 17, 2014
- Leading Coverage Lawyers: The Most Significant Insurance Coverage Decisions Of 2013, *Coverage Opinions*, Vol. 3, Issue 1, January 8, 2014
- Late Notice Decision Favors Policyholders, *The Insurance Coverage Law Bulletin*, Vol. 7, No. 1, February 2008
- Decision Favors Policyholders Asserting Construction Defect Claims, *The Insurance Coverage Law Bulletin*, Vol. 6, No. 10, November 2007
- 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
- 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*, Vol. 6, No. 7, August 2007
- NY Decision Favors Policyholders Seeking Coverage for Unresolved Asbestos-Related Liabilities, *The Insurance Coverage Law Bulletin*, Vol. 6, No. 5, June 2007
- Pennsylvania Supreme Court Rules On Assignments, *The Insurance Coverage Law Bulletin*, Vol. 6, No. 1, February 2007
- Insurance Coverage For Silica Claims, *Silica Legal News Report*, Vol. 1, No. 1, July 2005
- Insurance Coverage For Silica Claims, *The Insurance Coverage Law Bulletin*, Vol. 3, No. 7, August 2004
- Insurance Coverage For *Mandolidis*-Type Claims, *Insurance Coverage Update*, February 2003
- Insurance Coverage for Natural Resource Damages, *Insurance Coverage Alert*, January 2003
- Terrorism Risk Insurance Act of 2002, *Insurance Coverage Alert*, December 2002
- *Lititz Mutual Insurance Co. v. Steely*. Pennsylvania Supreme Court Takes a Second Look at the Absolute Pollution Exclusion, *Journal of Insurance Coverage*, Summer 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

Roberta D. Anderson (continued)

- 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

ADDITIONAL INSURED ISSUES

- Wrap Your Head Around ISO's Additional Insured Revisions, *Insurance Coverage Alert*, July 16, 2013, originally published in *Law360*, June 14, 2013
- Determining the Scope of "Additional Insured" Coverage: Recent ISO CGL Insurance Form Revisions Merit Close Attention By Contracting Parties, Insurance Coverage Alert, 9 May 2013
- ISO's 2013 "Additional Insured" Endorsement Changes Merit Close Attention, *Coverage*, Vol. 23. No. 3, May-June 2013

INTERNATIONAL ARBITRATION

- The International Comparative Legal Guide to: International Arbitration: USA, Chapter 62 (2014), Chapter 64 (2013), Chapter 58 (2012), Chapter 51 (2012)
- ICC To Unveil New Rules of Arbitration, *Arbitration World*, August 2011
- 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
- Protocol of Enforcement Affords Reassurance on Enforcement of DIFC-LCIA Arbitral Awards and DIFC Judgments Beyond DIFC Boundaries, *Arbitration World*, October 2009

THE LONDON MARKET

- Proposed Part VII Transfer of Liability on Lloyd's Policies: Considerations for Lloyd's Policyholders, *Insurance Coverage Alert*, May 22, 2009
- Proposed Equitas Transaction with Berkshire Hathaway: What Does It Mean for Lloyd's Policyholders?, *Insurance Coverage Alert*, January 2007
- Threatened Equitas Insolvency: Is The Lloyd's "Chain of Security" Really Secure? *Journal of Insurance Coverage*, Summer 2002
- Is it Still Possible to Litigate Against Lloyd's in Federal Court?, 34 Tort & Ins. L. J. 1065, *Tort & Insurance Law Journal*, Summer 1999

Roberta D. Anderson (continued)

CLASS ACTION LITIGATION

- Utilizing Recent Case Law to Develop Effective Products Liability Class Action Strategies, *Copyright 2011 Thomson Reuters/Aspatore*, July 18, 2013
- Utilizing Recent Case Law to Develop Effective Products Liability Class Action Strategies, *Litigating Products Liability Class Actions* , Chapter 1, Aspatore Books (Inside the Minds Series), November 2011

OTHER PUBLICATIONS

- Federal Insurance Office Unveils Long-Awaited Modernization Report, *Insurance Coverage Alert*, December 17, 2013
- TalkingPoint: Managing Risk In The Chemicals Industry, *Financer Worldwide*, December 2013
- New York Appellate Court Clarifies Fidelity Bond "Direct Loss" Requirement, *Insurance Coverage Alert,* August 7, 2013
- Recent Developments in Insurance Coverage, 48 Tort Trial & Ins. Prac. L.J. 285, *Tort Trial & Insurance Practice Law Journal*, Fall 2012.
- Recent Developments in Insurance Coverage Litigation, 47 Tort Trial & Ins. Prac. L.J. 297, *Tort Trial & Insurance Practice Law Journal,* Fall 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
- 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
- Upheaval in the Insurance Industry: Potential Implications for Policyholders, *Practical Law Company Cross-Border*, Vol. 1, No. 1, April-June 2005
- Marsh Settles Spitzer Charges For $850 Million, *Insurance Coverage Alert*, February 2005
- Insurance Industry Bid-Rigging/Steering Scheme Allegations Demand Policyholder Attention, *Insurance Coverage Alert*, October 2004
- Proposed Life Insurance Employee Notification Act, *Corporate Alert*, February 2003
- Terrorism Risk Insurance Act of 2002, *Insurance Coverage Alert*, December 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*, Vol. 2, No. 3, Winter 2002

Roberta D. Anderson (continued)

PROFESSIONAL/CIVIC ACTIVITIES

- United Way of Allegheny County
  - Tocqueville Committee (2012 to present)
  - Emerging Leaders Tocqueville Sub-Committee Tocqueville Committee (2013 to present)
  - Young Leaders Group (Member, 2000 to present; Committee Member, 2001; Co-Chair, 2002; Philanthropy Sub-Committee, 2006)
  - Women's Leadership Counsel (Member, 2001 to present)
  - 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 School Of Law
  - Chancellor's Circle
  - Law Fellows
  - Murray S. Love Mock Trial Competition Judge (2011 and 2012)
  - Alumni Reunion Class Representative (2008 and 2013)
- American Bar Association
  - Section of Litigation
  - Tort and Insurance Practice Section
- Allegheny County Bar Association (Civil Litigation Section)
- Pennsylvania Bar Association (Civil Litigation Section)

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

Roberta D. Anderson (continued)

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 typically contained in CGL policies. Reported in *Risk & Insurance*.
- Briefed a precedent-setting victory on behalf of the policyholder in a landmark decision concerning insurance coverage for claims alleging injuries resulting from exposure to radioactive emissions from nuclear fuel processing facilities. Reported in *Business Insurance*.
- Successfully 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.
- Successfully 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.
- Successfully 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.
- Successfully 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.

Roberta D. Anderson (continued)

- Successfully 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.
- Successfully 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.
- Successfully 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.
- Successfully 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 arising under almost every kind of business insurance policy, including under "cyber"/privacy policies in connection with the largest data breaches to date. 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.

Roberta D. Anderson (continued)

Insurance Coverage Negotiation and Placement

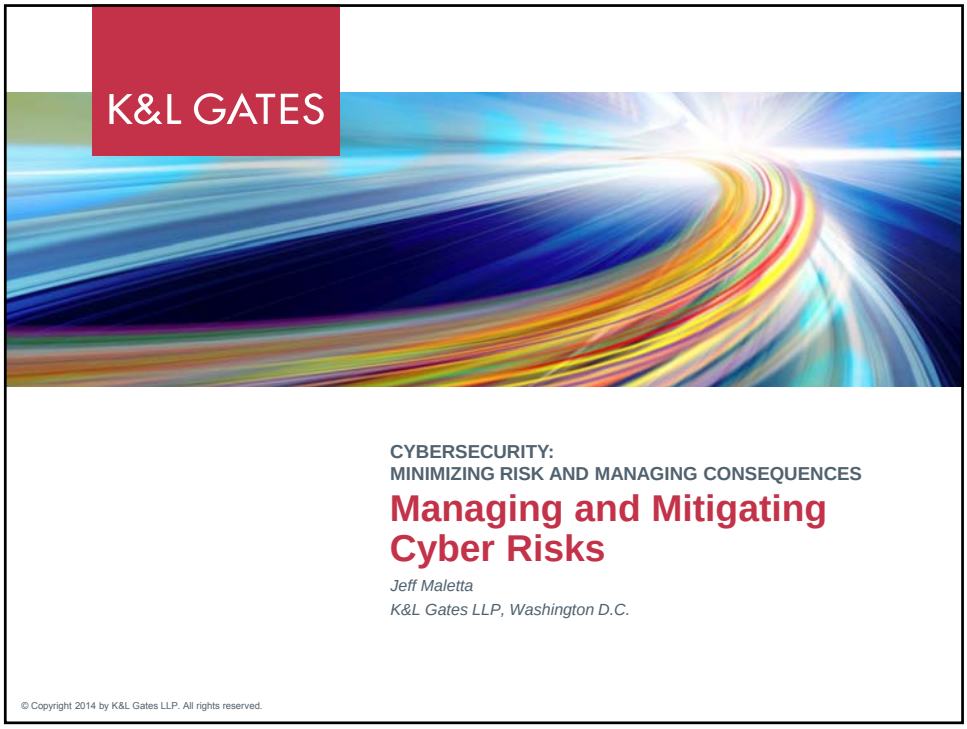
Ms. Anderson has counseled clients on complex underwriting and risk management issues, including the drafting and negotiation of D&O, E&O, data privacy and "cyber"-liability, and other insurance policy and blended program placements. Representative matters include:

- Represented the world's largest global and telecommunications company in structuring and negotiating the terms of its technology E&O, cybersecurity and data privacy and D&O insurance programs , with unprecedented market capacity
- Represented one of the world's four largest media conglomerates in structuring and negotiating the terms of its D&O insurance program
- Represented a Fortune 100 multinational financial services corporation in assessing and negotiating the terms of its cybersecurity and data privacy insurance program
- Represented one of the five largest U.S. banks in structuring and negotiating the terms of its cybersecurity and data privacy insurance program
- Represented the world's largest private operator of health care facilities in assessing and negotiating the terms of its technology E&O, cybersecurity and data privacy insurance program
- Represented a Fortune 500 retailer in assessing and negotiating the terms of its technology E&O, cybersecurity and data privacy and D&O insurance programs

K&L GATES

Managing and Mitigating Cyber Risks

Presenters: *Jeff Maletta, K&L Gates - Washington, D.C. and Susan Altman, K&L Gates - Pittsburgh*



CYBERSECURITY:
MINIMIZING RISK AND MANAGING CONSEQUENCES

Managing and Mitigating Cyber Risks

Jeff Maletta
K&L Gates LLP, Washington D.C.

K&L GATES

THE CURRENT ENVIRONMENT

- "[B]oards that choose to ignore or minimize the importance of cybersecurity liability do so at their own peril"−SEC Commissioner Luis A. Aguilar, Speech at "Cyber Risk and the Board Room" Conference, NYSE, June 10, 2014
- How should a director approach cybersecurity?

K&L GATES

K&L GATES

RESPECTIVE ROLES OF THE BOARD AND MANAGEMENT IN RISK MANAGEMENT

- Traditional view
  - Board not involved in day to day operations
  - Board has an oversight role
  - Management is responsible for risk management
- Trend toward greater board involvement
  - Case law developments
  - Best practice pronouncements
  - Financial crisis

klgates.com 2

K&L GATES

DIRECTORS DUTIES CONCERNING OVERSIGHT AND RISK MANAGEMENT

- Principally a function of state law
- Duty of care
  - Acting on informed basis
  - Acting in good faith
  - Acting in best interest in company
- Duty of loyalty
  - Placing the company interests first
  - Acting in good faith

klgates.com 3

K&L GATES

DUTY OF OVERSIGHT

- Directors have a duty to insure that adequate information systems exist to detect violations of law
- Directors have a duty to monitor systems to keep informed
- Directors face liability when they consciously fail to act to implement systems or consciously fail to monitor systems
- Tantamount to not acting in good faith – no protection of the "business judgment" rule
- No protection under exculpatory charter provisions

In re Caremark Int'l Derivative Litigation (Del. Ch. 1996);*Stone v. Ritter* (Del. 2006)

klgates.com 4

K&L GATES

CASES AGAINST DIRECTORS

Target Corporation *Collier v. Steinhafel et al.*
(D.Minn. 2014)

- "This action arises out of the Individual Defendants' responsibility for, release of false and misleading statements concerning, and the bungling of the aftermath of the ***worst data breach in retail history."*** (emphasis in original)
- "All of the Individual Defendants violated and breached their fiduciary duties of loyalty, good faith, due care, oversight, fair dealing, and candor."

klgates.com 5

K&L GATES

K&L GATES

CASES AGAINST DIRECTORS *(cont'd)*

Target Corporation *(cont'd)*

- "Each of the Individual Defendants had actual or constructive knowledge that they had caused Target to maintain improper security controls of customer data and to make false and misleading statements about the data breach once it occurred."
- "These actions could not have been a good faith exercise of prudent business judgment to protect and promote the Company's corporate interests."
- Institutional Shareholders Services recommends voting against seven incumbent Target directors

K&L GATES

CASES AGAINST DIRECTORS *(cont'd)*

Wyndham Worldwide Corporation *Palkon v. Holmes et al.* (D. N.J. 2014)

- "As a result of WWC's complete and utter lack of appropriate security measures, thieves were able to steal sensitive personal and financial data from over 619,000 of the Company's customers."
- "Among other things, the Individual Defendants failed to ensure that the Company and its subsidiaries implemented adequate information security policies and procedures (such as by employing firewalls) prior to connecting their local computer networks to other computer networks."
- "Additionally, the Company's property management system server used an operating system so out of date that WWC's vendor stopped providing security updates for the operating system more than ***three years*** prior to the intrusions." (emphasis in original)

K&L GATES

K&L GATES

CASES AGAINST DIRECTORS *(cont'd)*

Wyndham Worldwide Corporation *(cont'd)*

- "Further, the Individual Defendants allowed the Company's software to be configured inappropriately, resulting in the storage of payment card information in clear readable text."
- "The FTC Action poses the risk of tens of millions of dollars in further damages to the Company. Moreover, WWC's failure to protect its customers' personal and financial information has damaged its reputation with its customer base."

klgates.com 8

K&L GATES

CASES AGAINST DIRECTORS *(cont'd)*

The TJX Companies, Inc. *Louisiana Mun. Police Employees Union v. Alvarez* (Del. Ch. 2010)

- "Neither the Board itself, nor the Audit Committee on its behalf, took sufficient steps to cause the Company to achieve full compliance with the PCI Data Security Standards by establishing effective firewalls, rotating the WEP encryption key or avoiding the storage of Payment Card data in clear text, or to convert to WPA technology."
- Defendants were "at all relevant times, aware that the Company's computer system was at risk of attack, and that in the event of a successful attack, Payment Card data and customer personal information would be vulnerable to being accessed and stolen by outside intruders."

klgates.com 9

K&L GATES

K&L GATES

CASES AGAINST DIRECTORS *(cont'd)*

The TJX Companies, Inc. *(cont'd)*

- "From the time of the discovery of the Computer Intrusion late in fiscal 2007, through the end of fiscal 2009, the Company cumulatively expensed $171.5 million (pre-tax) with respect to the Computer Intrusion."

K&L GATES

SEC DISCLOSURE OBLIGATIONS

- Cybersecurity risks and their impacts should be disclosed
- Division of Corporation Finance Disclosure Guidance No. 2 (October 13, 2011)
- Areas where disclosure may be needed
  - Risk Factors
  - Management Discussion and Analysis
  - Description of Business
  - Legal Proceedings
  - Financial Statements
    - Expenses for compliance
    - Expenses to mitigate
    - Loss contingencies
  - Disclosure and Internal Controls

K&L GATES

K&L GATES

SEC DISCLOSURE OBLIGATIONS *(cont'd)*

- Directors May be Personally Liable for Misstatements in and Omissions from SEC Filings.
  - Sections 11 and 12(a)(2) of Securities Act of 1933
  - Sections 10(b) of the Securities Exchange Act of 1934 and Rule 10b-5
- *In re Heartland Payment Systems, Inc. Securities Litigation* (D. N.J. 2009)
- SEC May Consider Enforcement Action

klgates.com 12

K&L GATES

NO SINGLE PRIVACY AND DATA LAW OF GENERAL APPLICABILITY AND NO STANDARD COMPLIANCE PROGRAM

- Certain Industries Have Specific Requirements
- Law Often Relies on Incentives
- Standards Set Through Enforcement
- Compliance/Risk Management Best Practices

klgates.com 13

K&L GATES

K&L GATES

INDUSTRY SPECIFIC LEGAL STANDARDS

- Gramm-Leach-Bliley Act
- Health Insurance Portability Accountability Act
- Health Information Technology for Economic and Clinical Health Act
- Fair Credit Reporting Act
- Fair and Accurate Credit Transactions Act

klgates.com 14

K&L GATES

LIABILITIES AND INCENTIVES

- Civil litigation against company
- Director liability under state corporation law
- Liability under federal securities law
- Federal prosecutions
  - Compliance program a mitigating factor
  - Regulation by enforcement
- Federal Trade Commission proceedings

klgates.com 15

K&L GATES

K&L GATES

REGULATION BY ENFORCEMENT

- Standards may be set through settlements of enforcement actions
- FCPA paradigm
  - A decade of enforcement actions prior to official guidance
  - "Our actions against entities have had a tremendous impact in the last 10 years…[C]ompanies have increased their compliance spending exponentially" Andrew Ceresney, Director, SEC Division of Enforcement, Remarks at 31st International Conference on FCPA (Nov. 19, 2014)
- FTC cases provide "guidance" for cybersecurity

klgates.com 16

K&L GATES

FTC SETTLEMENTS

FTC Required "Information Security Programs"

- The **designation of an employee or employees** to coordinate and be accountable for the security program.
- The **identification of material internal and external risks** to the security, confidentiality, and integrity of covered information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, whether such information is in respondent's possession or is input into, stored on, captured with, or accessed through a computer using respondent's products or services, and assessment of the sufficiency of any safeguards in place to control these risks.

klgates.com 17

K&L GATES

K&L GATES

FTC SETTLEMENTS *(cont'd)*

- At a minimum, this risk assessment required by Subpart B should include **consideration of risks in each area of relevant operation**, including, but not limited to, (1) employee training and management, including in secure engineering and defensive programming; (2) product design and development; (3) secure software design, development, and testing; (4) review, assessment, and response to third-party security vulnerability reports, and (5) prevention, detection, and response to attacks, intrusions, or systems failures.
- The **design and implementation of reasonable safeguards** to control the risks identified through risk assessment, and **regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures,** including through reasonable and appropriate software security testing techniques.

klgates.com 18

K&L GATES

FTC SETTLEMENTS *(cont'd)*

- The development and use of reasonable steps to select and retain **service providers capable of maintaining security practices** consistent with this order, and requiring service providers by contract to implement and maintain appropriate safeguards; and
- The **evaluation and adjustment of respondent's security program in light of the results of the testing and monitoring** required by subpart B, any material changes to respondent's operations or business arrangements, or any other circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of its security program.

In the Matter of Fandango, LLC FTC Docket No. C-4481 (Aug. 13, 2014)

klgates.com 19

K&L GATES

K&L GATES

ENTERPRISE RISK MANAGEMENT ("ERM")

- Best Practices
  - Committee on Sponsoring Organizations of the Treadway Commission ("COSO") Enterprise Risk Management Framework
  - COSO Internal Controls Framework
  - National Institute of Standards Technology ("NIST") Cybersecurity Framework
  - Voluntary – So far

klgates.com 20

K&L GATES

COSO ERM FRAMEWORK COMPONENTS

- Internal environment
- Objective setting
  - strategic
  - operations
  - reporting
  - compliance
- Event identification
- Risk assessment

klgates.com 21

K&L GATES

K&L GATES

COSO ERM FRAMEWORK *(cont'd)*

- Risk response
  - avoiding
  - accepting
  - reducing
  - sharing
- Control activities
- Information and communication
- Monitoring – modification

klgates.com 22

K&L GATES

BOARD'S ROLE IN ERM – COSO FRAMEWORK

- Risk management "effected by an entities' board or directors, management and other personnel"
- Board is a critical part of internal environment and significantly influences other elements
- "Although directors primarily provide oversight, they also provide direction and approved strategy and certain transactions and policies."
- Directors should satisfy themselves that process provides "reasonable assurance"
- Reasonable assurance is not absolute assurance; even effective risk management can experience a failure

klgates.com 23

K&L GATES

K&L GATES

BOARD'S ROLE IN ERM – COSO FRAMEWORK *(cont'd)*

- Board should possess an appropriate degree of management and technical expertise
- At least a majority of board should be "outside" directors independent of management

K&L GATES

NIST FRAMEWORK

- Provides a "common language for understanding, managing and expressing cybersecurity risk both internally and externally".
- Describes activities to define and evaluate cybersecurity risks and improve outcomes.
- Does not discuss involvement responsibilities of board.
- Directors should become familiar with its vocabulary and its processes.

K&L GATES

K&L GATES

ENHANCEMENTS TO BOARD PROCESS

- Full board should be involved
- Education on risks and risk management
- Use of external resources
- Addition of directors with expertise
  - *Cf.* "financial expert," Sarbanes Oxley Act ("SOX") § 407
- "Risk management" committee(s)
- Increased audit committee resources
  - Audit committee retained experts, SOX § 301

klgates.com 26

K&L GATES

Jeffrey B. Maletta

Partner

Washington, D.C.
T 202.778.9062
F 202.778.9100
jeffrey.maletta@klgates.com

OVERVIEW

Mr. Maletta represents public and private companies, broker-dealers, investment companies and their advisors, and individuals in securities and corporate litigation, and in investigations by the Department of Justice and Securities and Exchange Commission involving the federal securities laws and related statutes. He also advises companies on compliance matters and performs compliance reviews and internal investigations.

PROFESSIONAL BACKGROUND

Prior to practicing at K&L Gates, Mr. Maletta served as law clerk to Barrington D. Parker, United States District Judge for the District of Columbia, and in the Office of General Counsel of the Securities and Exchange Commission.

PUBLICATIONS

- Co-Author, “Securities Litigation,” in *Business and Commercial Litigation in the Federal Courts*, West Group, 3d ed., 2011
- Co-author, “Litigating SEC Injunctive Actions” and author “Ethical Issues” chapters, *SEC Enforcement Manual*, American Bar Association, 2d ed. 2007
- Co-Author, “Standards for Professional Conduct” in *Sarbanes-Oxley Act: Planning & Compliance*, Aspen, 2006

PROFESSIONAL/CIVIC ACTIVITIES

- American Bar Association, Business Law and Litigation Sections, Federal Reg. of Securities Committee
- Adjunct Professor, Georgetown University Law Center, 2006-2014

ADMISSIONS

- District of Columbia
- Court of Federal Claims
- U.S. Courts of Appeal for the District of Columbia, First, Second, Third, Fourth, Sixth, Ninth and Tenth Circuits

Jeffrey B. Maletta (continued)

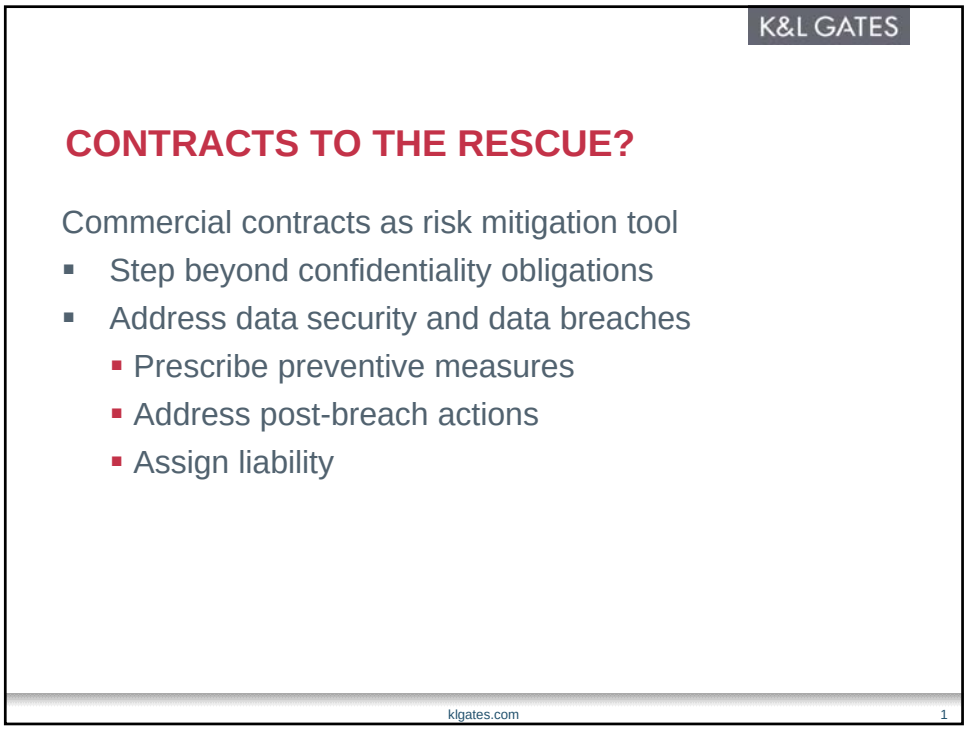
- U.S. District Courts for the District of Columbia, District of Maryland, and District of Colorado
- U.S. Supreme Court
- U.S. Tax Court

EDUCATION

J.D., Stanford University, 1979 (Member and Senior Editor, *Stanford Law Review*)

B.A., Harvard University, 1975 (*magna cum laude*)


K&L GATES
CYBERSECURITY:
MINIMIZING RISK AND MANAGING CONSEQUENCES
Vendor Contracts: Another Layer of Risk Mitigation
Susan P. Altman
K&L Gates LLP, Pittsburgh
© Copyright 2014 by K&L Gates LLP. All rights reserved.


K&L GATES
CONTRACTS TO THE RESCUE?
Commercial contracts as risk mitigation tool
Step beyond confidentiality obligations
Address data security and data breaches
Prescribe preventive measures
Address post-breach actions
Assign liability
klgates.com
1

K&L GATES

K&L GATES

PRESCRIBE PREVENTIVE MEASURES

- Require vendor to comply with customer's vendor security policies
- Require administrative, technical, and physical safeguards, and appropriate technical and organizational measures to protect customer's data
- Require subcontractor flow-down provisions
- Require consent to security audits

K&L GATES

ADDRESS POST-BREACH ACTIONS

- Immediate notice
  - Suspected or confirmed?
- Full cooperation with customer
- Prompt remedial action
- Notifications to individuals (customer's customers)
  - Who prepares
  - Who pays
- Customer termination rights

K&L GATES

DEFINE SCOPE OF VENDOR LIABILITY

- Historical approach to vendor liability for data breaches:
  - Phase 1
    - Pre-GLB: Silence
  - Phase 2
    - Vendors assume unlimited liability
  - Phase 3
    - Vendors push back
  - Phase 4
    - Revised market terms adopted

klgates.com 4

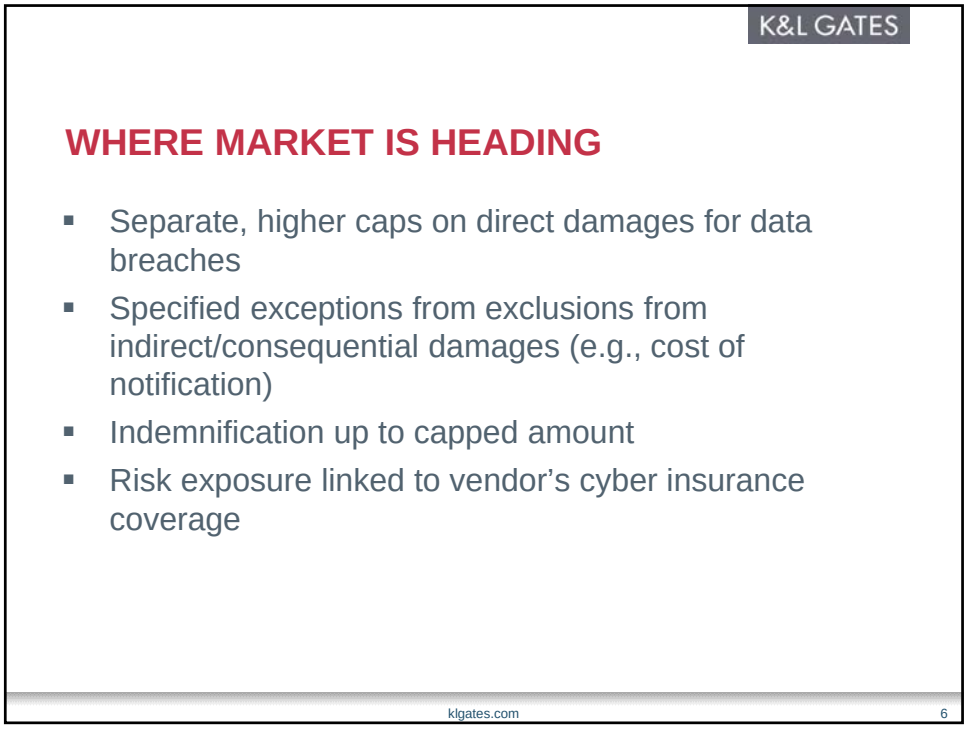
K&L GATES

VENDOR AS DUMB INSURER

- Customer "Vendor Bears All Risk" position:
  - Vendor is charging for its services
  - Vendor should bear all risk of data breach
- Vendor position:
  - Vendor's profit margin on services is less than customer's profit margin on customer's business enterprise
  - Vendor is not an insurer of customer's entire business risk
  - No insurer will take unlimited risks
  - Services could not be offered at prices less than customer's cost to provide services itself if vendor carries all business risk

∴ Customer's "Vendor Bears All Risk" position is economically inefficient

klgates.com 5


K&L GATES
WHERE MARKET IS HEADING
Separate, higher caps on direct damages for data breaches
Specified exceptions from exclusions from indirect/consequential damages (e.g., cost of notification)
Indemnification up to capped amount
Risk exposure linked to vendor's cyber insurance coverage
klgates.com
6

K&L GATES

Susan P. Altman

Partner

Pittsburgh
T 412.355.8261
F 412.355.6501
susan.altman@klgates.com

OVERVIEW

Susan Altman navigates businesses through the complexities of dealing with suppliers and customers in order to help lower costs and improve revenues. Ms. Altman helps clients properly structure contracts in ways that foster long-term, positive commercial relationships, whether through licensing, strategic alliances, outsourcing transactions or joint ventures. For example, she recently assisted a major healthcare system in negotiating its electronic medical records software license so as to incentivize the parties to achieve a long-lasting successful relationship through a fair balance of obligation and risk.

Ms. Altman brings to bear a substantial background as a transactional lawyer serving clients in a broad array of commercial needs. In addition to assisting clients with IT and business process outsourcing activities, Ms. Altman has negotiated commercial contracts supporting the implementation of complex ERP, EMR, customer information, and smart meter systems. She has also negotiated numerous licenses of intellectual property rights in the software, medical device, and biotechnology industries. She addresses privacy and data protection in commercial contracts, including many transactions in the financial services and healthcare industries.

The commercial transactions and outsourcing arena demands technically sound, practical advice, informed by awareness of market conditions and best practices. To meet this need, Ms. Altman draws from the knowledge base and assistance of the Commercial Transactions and Outsourcing practice group, located across four continents, as well as firm resources in areas such as intellectual property, privacy and data protection, tax, employment, dispute resolution, bankruptcy, antitrust, FDA, and Internet safety.

Ms. Altman is a frequent lecturer on commercial and technology issues.

PRESENTATIONS

- “Contract Lifecycle Management,” presented to Western Pennsylvania Chapter, American Association of Corporate Counsel, September 30, 2014
- “Commercial Contract Drafting--Technique and Structure,” CLE presentation, Pittsburgh, August 19, 2014
- “Commercializing Medical Devices--Using Contracts to Your Advantage,” presented to Pittsburgh Technology Council, Medical Device 2014, Pittsburgh, August 14, 2014
- “Managing the Risks of Importing: Contractual Considerations,” Seminar on Off-Shore Procurement and Importing into the U.S., client presentations in Cleveland and Pittsburgh, October 24 and 25, 2011

Susan P. Altman (continued)

- Development of University Partnerships for the Promotion of Innovation, a Project for Russia: "Critical Issues in Licensing," International Leadership Program of the U.S. Department of State, Pittsburgh, February 22, 2011
- "Strategic Contractual Alliances," presented to Western Pennsylvania Chapter, American Association of Corporate Counsel, May 18, 2010
- "Transition Services," presented at client's global headquarters, March 17, 2009
- "Online Services Agreements," CLE presentation, Pittsburgh, May 30, 2008
- "Contract Drafting: Technique and Structure," CLE presentation, Pittsburgh, January 4, 2008
- "Open Source Software," TiE Pittsburgh Open Source Summit, February 15, 2007
- "Managing the Website," University of Pittsburgh GSPIA, April 5, 2005
- "Secrets of a Successful Software License," CLE presentation, Pittsburgh, May 13, 2004
- "Anatomy of a Tech Contract," CIO/ARTS Seminar, October 2, 2003
- "Structure of Contracts for the Sale of Goods and Services," Lorman Education Services Seminar, January 15, 2003
- "Legal Aspects of Establishing a U.S. Base of Operations," Dortmund Economic Development Agency, Dortmund, Germany, July 1, 2002

ADMISSIONS

- Pennsylvania
- Supreme Court of Pennsylvania
- U.S. District Court of the Western District of Pennsylvania

EDUCATION

J.D., University of Chicago, 1983 (Editor, *University of Chicago Law Review*)

A.B., Mount Holyoke College, 1979 (*cum laude*)

ADDITIONAL INFORMATION

Fellowship

Fulbright Fellowship, University of Bonn, Germany 1979-1980

REPRESENTATIVE WORK

- Representation of a software company offering web-based software for managing, measuring, and reporting on high net worth and ultra high net worth trust portfolios to British multi-national banking and financial services company and also to German global banking and financial services company

Susan P. Altman (continued)

- Representation of retailer of nutritional supplements in development of international distribution initiative
- Representation of major U.S. health system in licensing of enterprise electronic health software
- Representation of provider of innovative colon cancer screening test in negotiation of a variety of manufacturing and laboratory agreements
- Representation of medical device manufacturers in negotiation of international distribution agreements
- Advise various public companies on contract formation and battle of the forms issues
- Representation of major university medical center in negotiation of group purchasing agreement
- Representation of a major university in the sale and related license of adaptive learning technology
- Representation of a major university medical system in the negotiation of its group purchasing organization agreement
- Representation of a drug discovery and development company in the negotiation of a license for drug development and commercialization with a global provider of neurology products
- Representation of a $3 billion utility company in its negotiations with a global systems integrator and managed application service provider of a customer information system
- Representation of a software company offering inventory optimization and forecasting applications to global consumer packaged goods manufacturers

PUBLICATIONS

- Author of Chapter *Licensing, Product Development and Commercialization* "Medical Devices Law and Regulation Answer Book 2015." Ed. Onel and Becker. New York: Practising Law Institute, 2014.
- "Don't Touch that Technology" *K&L Gates Legal Insight*, November 2, 2010, with T. Fisher, reprinted in *Cyberspace Lawyer,* December 2010
- "Are Smart Meters Ready for Us?" *California Cleantech Resource Newsletter*, July 2010
- "Are You Ready for the Smart Grid?" *K&L Gates Legal Insight,* February 2, 2010
- *Doing Business in The United States: A Guidebook for Foreign Companies Operating in the United States*, 2009

K&L GATES

Government Initiatives and Responses to a Breach

Presenters: *Mark Rush, K&L Gates - Pittsburgh; U.S. Attorney David J. Hickton and Assistant U.S. Attorney James T. Kitchen*

K&L GATES

A Guide to the Development of a Cyber Data Breach Action Plan

Mark A. Rush and Thomas C. Ryan

INTRODUCTION

Cyber data breaches are now part of the cost of doing business. Regardless of industry, size or location, no company is immune from the real and imminent threat presented by a data breach. In 2013 alone, nearly 1,400 breaches were confirmed[1] and each data breach was unique, reinforcing the point that there is no one solution to an exponentially growing problem.

The growth of data breach litigation emphasizes the real and imminent litigation exposure to any company that is victimized. Whether brought by private litigants (usually in the form a class action on behalf of consumers) or public agencies (in the form of governmental enforcement actions) companies must accept that data breaches will result in some form of litigation.

One step that a company can take to limit this exposure is to focus on how it *handles* the data breach. A well-designed breach response plan, delineating clear lines of authority and responsibility, will ensure that every possible step is taken to minimize exposure. Deployment of such a plan is critical.

Data breaches are going to occur. That fact and the how and when of such breaches is beyond a company's control. How a company handles its response to breach, however, is the only thing left to control. And the first 48 hours matter most. While every crisis is unique, this guide is intended to highlight the fundamental steps that any company should take in those critical first moments to maximize its efforts to minimize risk.

ESTABLISHING A DATA BREACH RESPONSE POLICY

A data breach occurs. Chaos may ensue. Having a plan in the event of a data breach is essential. A quick response to a cyber intrusion can minimize loss of information, reduce liability exposure, and can ultimately save time and money down the road. Any plan must have at least these core components:

- **Internal Reporting Thresholds**

  A difficult task for managing cybersecurity threats is determining when a cybersecurity threat is significant enough to warrant notification to upper-level management and, perhaps even the board of directors. Working with its information technology department, a company should develop certain criteria based on that particular company's business establishing when a threat is to be elevated, how and to whom. Importantly, it is critical for the company to determine when to involve its general counsel, as the legal department will play a crucial role in handling notice issues arising from a data breach.

- **Assessing Scope**

  The sooner a company can appropriately determine the scope, duration, depth and breadth of a data breach, the sooner the company can refine a targeted plan to mitigate

[1] Verzion 2014 Data Breach Investigation Report, *available at*, http://www.verizonenterprise.com/DBIR/2014/

risk. A successful breach response plan must task someone with finding answers to basic questions while preserving evidence: How long did the breach occur? What type of data was accessed? How many different sources of data were breached? How many consumers or other constituents may be affected? The answers to these questions, even preliminarily, will be key to shaping the company's response.

- **Designated Persons**

  A breach response plan will only be successfully executed if the roles of the critical players are defined. This plan should assign specific duties to specific "designated persons" in upper-level management. For instance, someone should be designated with responsibility to communicate with law enforcement, while another person should be assigned to communicate with the board of directors. Maintaining consistent points of contact is the only way to ensure the flow of timely information.

- **Notice and Reporting Obligations**

  As discussed in more detail below, someone must be tasked with understanding the company's reporting obligations and ensuring all requirements have been met. This is the most important step in ensuring that the company minimizes its exposure, particularly within the first 48 hours.

CONSIDERATIONS RELATED TO SPECIFIC NOTICE OBLIGATIONS

The most important responsive step in the immediate aftermath of a data breach is to ensure that *all* notice or reporting obligations are satisfied. These notice obligations come in different forms for different parties, but in accordance with a well-designed breach response plan discussed above, notices and reports should be carefully drafted, coordinated and contain a consistent message. Also, to the extent that, over time, new or different information is obtained, *each* notice should be updated accordingly to maintain consistency. Although each situation is unique, below are some of the critical notice or reporting obligations that should be considered and, if applicable, included in a breach response plan.

- **Data Preservation and Preparation for Potential Law Enforcement Contact**

  Most likely, a company that is victim to a data breach is also victim of a crime. The relevant data, hardware and software may become evidence not only for civil litigation, but also criminal prosecution, if the hackers are apprehended and charged. A federal or state law enforcement agency could, if so inclined, exercise its search and seizure power to physically remove relevant evidence. A governmental agency could alternatively issue a subpoena or exercise other administrative power to compel the preservation and production of evidence. It is imperative that a company's designated law enforcement coordinator be trained in how to appropriately interact with law enforcement and also consult with counsel in handling the matter. The shifting sands of the current federal and state regulatory regimes, as discussed below, may turn today's victim into tomorrow's law enforcement target. Regardless, the company, through a designated person identified in the breach response plan, must quickly notify in writing all relevant company personnel to ensure the proper preservation of affected property. What may not seem important at the moment may ultimately lead to the prosecution of an intruder and perhaps, more importantly, the prevention of additional data breaches. And maintaining the relevant

evidence may not only stave off civil litigation, but help persuade law enforcement to view the company as an ally in pursuing a hacker.

- **Federal and State Governmental Agency Reporting**

  A company's obligation to notify federal and state governmental agencies of a data breach is changing. These obligations are complex and evolving, practically every day, yet often require timely notifications.

  Several federal government agencies have requirements regarding data breach reporting. For example, the Securities Exchange Commission (SEC) has noted that, even though the federal securities laws do not explicitly refer to cyber risks and incidents, "a number of disclosure requirements may impose an obligation on registrants to disclose such risks and incidents."[2] The Federal Communications Commission (FCC) requires certain breaches of Customer Proprietary Network Information (CPNI) be reported to the United States Secret Service and the Federal Bureau of Investigation.[3] The Federal Trade Commission (FTC) has been heavily involved in enforcing privacy laws and bringing actions against companies for failing to maintain security of consumers' private information.[4] Although not currently requiring notice of cyber data breaches, it is likely that expanded cybersecurity rule-making and enforcement capabilities by the FTC are in the pipeline.

  The federal government, through multiple agencies, is not the only governmental agency insisting on notification. Reporting obligations to various state government agencies represent a patchwork of uncoordinated laws presenting ample opportunities for missteps. For example, some states, including Connecticut and Virginia, currently require notice to the state Attorney General regarding a breach of personal information.[5] In South Carolina, however, notice is only required if more than 1,000 consumers are affected by the data breach and that notice must be provided to the Consumer Protection Division of the South Carolina Department of Consumer Affairs.[6] Hawaii requires similar notice to its state Office of Consumer Protection.[7]

  The lesson here is that no federal and state governmental reporting requirement is the same, and the law is constantly changing. As part of a breach response plan, it is critical that someone within an organization be tasked with ensuring that these obligations are met to avoid potential consequences and penalties.

---

2 SEC CF Disclosure Guidance: Topic No. 2, *available at*, http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

3 FCC CPNI Breach Reporting Facility, *available at*, http://www.fcc.gov/encyclopedia/cpni-breach-reporting-facility

4 FTC Enforcing Privacy Promises, *available at*, http://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises

5 CONN. GEN. STAT. § 36a-701b(b)(2); VA. CODE ANN. § 18.2-186.6(B.).

6 S.C. Code Ann. § 39-1-90(K).

7 HAW. REV. STAT. § 487N-2(f).

- **Consumers, Constituents and Other Affected Third Parties**

  Forty seven states currently require consumer notification when a breach involving personally identifiable information occurs.[8] For example, California has enacted a comprehensive statute regarding disclosure of security breaches, which provides:

  > Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.[9]

  The California statute provides detailed requirements for the information to be contained in the notice to California residents and directs the agency to submit a sample of the notification to the Attorney General when notice to more than 500 California residents is required.

  Although many aspects of the states' data breach notification laws are similar, it is important to note the differences between them. For instance, in Alaska, consumer notice is not required if there is a determination that "there is not a reasonable likelihood that harm to the consumers whose personal information has been acquired has resulted or will result from the breach."[10] Under Pennsylvania's Breach of Personal Information Notification Act ("BPNI Act"), the general rule is that an entity must provide notice to Pennsylvania residents "whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person."[11] The BPNI Act goes on to specify that notice of the breach of encrypted information in unencrypted form is required "if the security breach is linked to a breach of the security of the encryption or if the security breach involves a person with access to the encryption key."[12] In New Jersey, before notifying consumers of a personal information data breach, an entity must report the breach to the Division of State Police for investigation.[13] Because each state's notification laws are different, the company, most likely the General Counsel, must give particular consideration to the requirements of each state involved in a company's data breach.

- **Shareholders**

  It is important to keep notice to shareholders in mind when handling a cyber data breach. Directors must adhere to the duty of care and perform his or her duties "(1) in good faith and, (2) in a manner the director reasonably believes to be in the best interests of the corporation."[14] Although notice to shareholders of a data breach is not specifically

---

8 The state security breach notification laws have been compiled by the National Conference of State Legislatures and are available at http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

9 CAL. CIV. CODE § 1798.29(a).

10 ALASKA STAT. § 45.48.010(c)(noting that such determination must be in writing and follow an appropriate investigation and written notification to Alaska's Attorney General).

11 73 PA. CON. STAT. § 2303(a).

12 73 PA. CON. STAT. § 2303(b).

13 N.J. STAT. ANN. § 56:8-163(c.).

14 MODEL BUSINESS CORPORATION ACT § 8.30.

required, notice may help to facilitate communication with the shareholders and to avoid derivative lawsuits.

- **Insurers**

  Insurance policies can be a critical resource in responding to cyber threats. More and more insurers are offering specialized cyber policies, which cover certain costs associated with data breaches, such as hiring forensic experts to determine the cause of the breach or notifying individuals whose personal information may have been compromised. In addition, other standard policies, such as directors' and officers' insurance or commercial general liability insurance, may provide coverage, as well and should be reviewed carefully for this purpose.

  Importantly, most policies require the insured to notify the insurer within a certain period of time of claims or events that may trigger coverage obligations. Policyholders who fail to do so may risk losing any coverage otherwise available. As a result, it is important to promptly notify one's insurance carrier(s) of a data breach. A designated person, most likely the company's risk manager or experienced outside coverage counsel, can assist the company in providing this notice in the immediate aftermath of a breach and in assisting to maximize recovery under the company's existing coverage program.

CONCLUSION

Navigating the legal implications imposed in the aftermath of a cyber data breach can be complicated and complex. No two breaches should be treated the same. The first 48 hours will be hectic and overwhelming. The only thing that help a company ensure it manages the chaos without committing a critical error is to have a plan in place that clearly defines the role and responsibility of each pivotal player. That plan, specifically tailored and implemented based on the facts surrounding any particular breach, must ensure that the company makes all proper notifications, or risk running afoul of regulatory obligations, unnecessarily created civil liability or worse, being accused of intentionally destroying evidence of crime.

K&L GATES

Mark A. Rush

Partner

Pittsburgh
T 412.355.8333
F 412.355.6501
mark.rush@klgates.com

OVERVIEW

Mr. Rush is a partner with the firm and concentrates his practice on litigation as a trial lawyer, with emphasis on internal investigations, corporate criminal defense, False Claims Act defense and complex commercial litigation. Mr. Rush has defended public and private corporations, public officials, government contractors, hospitals and healthcare systems who are subjects of federal and state grand jury investigations and investigations by various federal and state agencies. His representations also include defending and counseling corporations and individuals charged with violations of various federal and state statutes such as: Foreign Corrupt Practices Act, False Claims Act, Bank Secrecy Act, securities laws, tax statutes, mail and wire fraud, healthcare fraud, environmental violations and money laundering. Mr. Rush has coordinated and conducted internal and special committee investigations and due diligence projects within the United States and in numerous foreign countries related to anti-corruption issues, fraud, and corporate governance issues. Mr. Rush assisted in the representation of a Presidential Advisor in the Independent Counsel Investigation of President Clinton. Mr. Rush also served as an investigator for the WorldCom bankruptcy examiner investigating corporate governance issues. He also represents the Pennsylvania House and Senate Republican Caucuses.

Mr. Rush was trial counsel in the case of United States v. Cyril H. Wecht, No. 06-26 (W.D.Pa.). The U.S. Attorney's Office obtained an 84-count indictment against Dr. Wecht, a public official and internationally renowned forensic pathologist, charging, *inter alia*, honest services fraud, mail fraud, and wire fraud. Following a nine week trial the jury could not reach a verdict on any count. The defense then re-raised suppression issues. The evidence was suppressed and all remaining charges were dismissed. This case also involved testimony before Congress regarding selective political prosecutions.

PROFESSIONAL BACKGROUND

From 1991-1995, Mr. Rush served as an Assistant United States Attorney for the Western District of Pennsylvania where his responsibilities included conducting grand jury investigations and prosecutions of various types of fraud and organized crime. During that time, Mr. Rush also lectured and published for the Executive Office of United States Attorneys, Attorney General Advocacy Institute on innovative uses of the racketeering statutes.

Mr. Rush has previously served as a United States Army Judge Advocate assigned to the U.S. Army, Japan. He was also appointed as a Japan Trial Court U.S. Representative by the U.S. Ambassador to Japan.

Mark A. Rush (continued)

Mr. Rush has been inducted into *The Academy of Trial Lawyers,* Allegheny County. He is listed in *The Best Lawyers in America*® (Woodward/White, Inc.) and *Corporate Counsel Magazine* Top Lawyers for criminal defense-white collar. Mr. Rush has received an AV® rating from Martindale-Hubbell, its highest rating. Mr. Rush is also listed in *PA Super Lawyers.*

He is a contributing author to *Sarbanes-Oxley Planning & Compliance,* published by Thompson Publishing Group, November 2003; and *Forensic Experts in Criminal Trials, Expert Witness Answer Book,* Practicing Law Institute 2012.

PUBLICATIONS

- "Enhanced Protections for Federal-Employee Whistleblowers: Sign of Things to Come?", by Mark A. Rush, Michael D. Ricciuti, and Joseph Valenti, published by K&L Gates LLP, January 11, 2013.
- "Sending the Privilege Away: Attorney-Client E-Mails in the Corporate Setting," by Mark A. Rush, Amy O. Garrigues, Bryan D. Rohm, and Joseph A. Valenti, published by K&L Gates LLP, January 2013.
- "Forensic Experts in Criminal Trials," by Mark A. Rush, *Expert Witness Answer Book 2012*, Practicing Law Institute 2012.
- "When Law Enforcement is at Your Door," by Mark A. Rush, *TRACE*, Winter 2007-08.
- "Corporate Responses to Investigative Requests by the Federal Government," by Mark A. Rush, published by Kirkpatrick & Lockhart Nicholson Graham, September 2005.
- "Sarbanes-Oxley's New Crimes, Enhanced Penalties and Ways to Avoid Them," by Mark A. Rush, published by Kirkpatrick & Lockhart Nicholson Graham, February 2004.
- Contributing Author, *Sarbanes-Oxley Planning & Compliance*, published by Thompson Publishing Group, November 2003.
- "Combating Counterfeits," by Mark A. Rush and Lucas G. Paglia, *Pharmaceutical Executive*, June 2002.
- "Balancing Privacy, Public Safety, and Network Security Concerns after September 11," by Mark A. Rush and Lucas G. Paglia, *Information Systems Security*, May/June 2002.
- "End Game: The Ex Parte Seizure Process and the Battle Against Bootleggers," by Mark A. Rush, *Vanderbilt Journal of Entertainment Law & Practice*, Winter 2002.
- "The International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001," by Mark A. Rush and Heather Hackett, *K&L Alert,* October 2001.
- "Preventing, Investigating and Prosecuting Computer Attacks and E-Commerce Crimes: Public/Private Initiatives and Other Federal Resources," by Mark A. Rush and Lucas G. Paglia, *e-Business Law Bulletin*, September/October 2001 and *White-Collar Crime Reporter*, July/August 2001.
- "Protecting Trade Secrets from Dumpster Divers and Other Snoops: The Law Protects Those that Protect Themselves," by Mark A. Rush, Mark D. Feczko, and Thomas D. Manganello, *Mealey's Litigation Report: Intellectual Property*, August 7, 2000.

Mark A. Rush (continued)

- "Recording Conversations in Pennsylvania: Criminal and Civil Penalties for the Unwary," by Mark A. Rush and Mark D. Feczko, *Pennsylvania Association of Criminal Defense Lawyers Forum*, Volume 12, Number 1, 2000.
- "Protecting the Open Seas: Fighting Cyberpiracy," by Mark A. Rush, Jeffrey M. Gitchel and Wade J. Savoy, *Cyberspace Lawyer*, March 2000.
- "Protecting Your Computer Systems: The Federal Response," by Mark A. Rush and Lucas G. Paglia, *Cyberspace Lawyer*, September 1999.
- "How Corporations Can Avoid or Minimize Federal Criminal Liability For the Illegal Acts of Employees," by Mark A. Rush and Brian F. Saulnier, published by Kirkpatrick & Lockhart Nicholson Graham, March 1999.
- "Federal Resources to Protect Your Computer Systems From Economic Espionage," by Mark A. Rush and Lucas G. Paglia, published by Kirkpatrick & Lockhart Nicholson Graham, February 1999.
- "New Voluntary Disclosure Program," by Mark A. Rush and Erica Merkow, *Health Law Update,* December 1998.
- "DOJ and OIG Issue New False Claims Act Guidelines," by Mark A. Rush and Elisa A. Long, *Health Law Update*, July 1998.
- "How To Protect Your Internal Corporate Investigations From Discovery" by Michael A. Agresti and Mark A. Rush, published by Kirkpatrick & Lockhart Nicholson Graham, May 1998.
- "An Inside Look at False Claims Act Investigations," by Mark A. Rush, *Health Law Alert*, December 1997.
- "The FBI Is at Your Reception Desk - Now What?" by Mark A. Rush, *Health Law Alert*, March 1997.

PRESENTATIONS

- "DOJ's Enforcement Trends, Investigative Strategies and Corporate Internal Investigations," The Audit Committee Forum, Philadelphia, Pennsylvania, November 29, 2012
- "From the Boardroom to the Courtroom: The Evolving Legal Status of Corporate Crime," Miami Law Review Symposium, University of Miami School of Law, February 18-19, 2011.
- "Foreign Corrupt Practices Act (FCPA): New Trends in Compliance & Enforcement" presented at the Greater Dallas Chamber, Dallas, Texas, November 6, 2007.
- "Corporate Responses to Investigative Requests by the Federal Government," presented at *Government & Internal Corporate Investigations: Responding to Concerns About Alleged Wrongdoing*, Association of Corporate Counsel, October 20, 2005.

Mark A. Rush (continued)

- "Responses When Financial Services Companies Suffer Cyber Intrusion Attacks," presented at *National Law Enforcement and Industry Cyber Crime Conference: Digital Phishnet*, May 11 - 12, 2005.
- "Sarbanes-Oxley's New Crimes, Enhanced Penalties and Ways to Avoid Them," presented at *Corporate Investigations: Role of the Attorney Workshop*, February 19 & 26, 2004.
- "Anticipating E-Discovery in the Digital Business Era: Preventive Medicine," presented at *I-4 Conference*, October 15, 2002.
- "Handling Investigations - Administrative, Non-Criminal and Criminal," presented at the *Annual Legal Symposium: Issues Affecting Long-Term Care*, March 30, 1999.
- "False Claims Act Investigations: The FBI is at Your Desk--Now What?" presented at the *1998 Annual Convention of the Pennsylvania Health Care Association,* September 21, 1998.
- "False Claims Act," *21st Annual Emergency Medical Services Conference*, Lancaster, Pennsylvania, August 14, 1998.
- "Managing Internal and Government Conducted Investigations," Kirkpatrick & Lockhart's *Compliance Plans for Providers* seminar, Hershey, Pennsylvania, January 7, 1997.
- "Hospital Fraud Investigations: What To Do When The FBI Shows Up," Kirkpatrick & Lockhart seminar, Sharon, Pennsylvania, May 14, 1996.

PROFESSIONAL/CIVIC ACTIVITIES

- Allegheny County Bar Association (Civil and Federal Criminal Practice Section)
- American Bar Association (Civil and Criminal Litigation Sections)
- Chair, Western PA Chapter, National Pancreas Foundation
- Coordinator, pro bono prisoner civil rights cases, Western District of PA

ADMISSIONS

- Pennsylvania
- Admitted *Pro Hac Vice* in numerous state and federal courts throughout the U.S.
- Supreme Court of Pennsylvania
- U.S. Court of Appeals for the Third Circuit
- U.S. District Court for the Western District of Pennsylvania and the Eastern District of Michigan

EDUCATION

J.D., Duquesne University, 1987

B.A., Washington & Jefferson College, 1984 (*Dean's List*)

David J. Hickton

United States Attorney for the Western District of Pennsylvania

David J. Hickton was nominated for United States Attorney for the Western District of Pennsylvania by President Barack Obama on May 20, 2010, and was confirmed by the U.S. Senate on Aug. 5, 2010. He was sworn in as the District's 57th U.S. Attorney on Aug. 12, 2010.

Prior to becoming U.S. Attorney, Mr. Hickton co-founded Burns, White & Hickton LLC in 1987. From 1983 to 1987 he was an Associate Attorney at Dickie, McCamey & Chilcote. He practiced in the areas of transportation, litigation, commercial and white collar crime. Mr. Hickton began his legal career serving as a Law Clerk for the Honorable United States District Judge Gustave Diamond from 1981 to 1983. For more than a decade, Mr. Hickton was an Adjunct Professor of Law at Duquesne University School of Law where he taught antitrust.

Mr. Hickton is a Fellow in the American College of Trial Lawyers, and a Fellow of the Academy of Trial Lawyers of Allegheny County. Mr. Hickton has been admitted before the United States Supreme Court, the Pennsylvania Supreme Court, the United States District Court for the Western District of Pennsylvania and several of the U.S. Circuit Courts.

Previously, Mr. Hickton was involved in a wide range of community activities, and has long been an active supporter of and participant in organizations which benefit children and the arts. He is a past Executive Board Member of the Pittsburgh Public Theater, and served as its President. Mr. Hickton also was a longtime member of the Pittsburgh Cultural Trust, a non-profit organization that uses arts and culture to reinvigorate the Downtown.

His nomination as United States Attorney marks Mr. Hickton’s second Presidential appointment. From 1999 to 2001, Mr. Hickton served on the President’s Advisory Committee on the Arts for the John F. Kennedy Center for the Performing Arts at the request of then-President Bill Clinton.

Mr. Hickton is a 1978 graduate of the Pennsylvania State University and a 1981 graduate of the University of Pittsburgh School of Law.

Jimmy Kitchen

Jimmy Kitchen has been an Assistant United States Attorney for the past 10 years, serving in the Southern District of Texas, District of New Jersey, and the Western District of Pennsylvania. He currently serves as the National Security Cyber Specialist and Anti-Terrorism Advisory Council Coordinator for the US Attorney's Office in Pittsburgh, as well as serving as the Deputy Chief of the National Security and Cyber Crime Section of the Office. Since being in Pittsburgh, he has led several notable investigations, including those leading to the conviction on online jihadist Emerson Begolly, and charges against the University of Pittsburgh online bomb threatener Adam Busby, and most recently the five Chinese PLA officers who hacked into five major Pittsburgh-based corporations.

K&L GATES

Insuring Against Cyber Risks

Presenters: *Bob Parisi, Marsh, Inc. and Roberta Anderson, K&L Gates - Pittsburgh*

MARSH

SOLUTIONS...DEFINED, DESIGNED, AND DELIVERED.

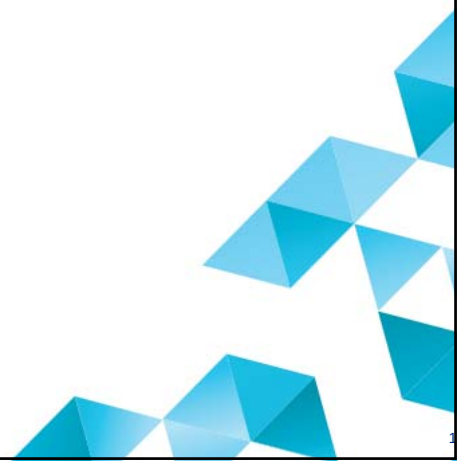
Cyber & Privacy Risk Overview

Bob Parisi, Marsh, Inc.

MARSH

SOLUTIONS...DEFINED, DESIGNED, AND DELIVERED.

The Insurance



CYBER INSURANCE DEFINED - INSURING AGREEMENT SUMMARY

- 1st Party Insurance coverage: direct loss and out of pocket expense incurred by insured
- 3rd Party insurance coverage: liability incurred from harm caused by the insured, including defense of claims

Coverage	Description
Business Income/ Extra Expense	Reimbursement for loss of income and/or extra expense resulting from an interruption or suspension of computer systems due to a failure of technology. Includes coverage for dependent business interruption and forensic expenses.
Data Asset Protection	Recovery of costs and expenses you incur to restore, recreate, or recollect your data and other intangible assets (i.e., databases, software, applications) that are corrupted or destroyed by a computer attack.
Event Management	The following costs resulting from a privacy breach: • Forensic services. • Breach notification services (including legal fees, call center, etc.). • Identity/fraud monitoring expenses. • Public relations.
Cyber Extortion	Costs of consultants and extortion monies for threats related to interrupting systems and releasing private information.
Privacy Liability	Defense and liability for failure to prevent unauthorized access, disclosure or collection of confidential information, or for failure of others to whom you have entrusted such information (e.g., pension actuary, data storage facility, credit card processor). Also includes liability for not properly notifying of a privacy breach. Coverage includes corporate information such as third-party trade secrets. **Likely Claimants:** customers, employees, trading partners.
Network Security Liability	Defense and liability for failure of system security to prevent or mitigate a computer attack including but not limited to spread of virus or a denial of service. Failure of system security includes failure of written policies and procedures addressing technology use. **Likely Claimants:** 3rd Party Loss, customers, employees.
Privacy Regulatory Defense Costs	Costs to defend an action or investigation by regulator due to a privacy breach, including indemnification for any fines or penalties assessed. **Likely Claimants:** Attorney General, FTC.
Media Liability	Defense and liability for online libel, slander, disparagement, misappropriation of name or likeness, plagiarism, copyright infringement, negligence in content to those that relied on content. **Likely Claimants:** authors, producers, publishers, competitors, license holders.

Potential Insurable Costs in a Breach or Technology Outage

Item	Insurable Under Cyber Insurance?	Coverage Part
Forensics	Yes	• Event Management • Business Income/Extra Expense
Notification	Yes	Event Management
Call Center	Yes	Event Management
Credit Monitoring	Yes	Event Management
Sales Discounts	Maybe	• Event Management • Security Liability • Privacy Liability
Public Relations	Yes	Event Management
Regulatory Defense	Yes	Privacy Regulatory Defense Costs
Prep to Testify to Congress	Maybe	Privacy Regulatory Defense Costs
Regulatory Fines and Penalties	Yes- depending on venue	Privacy Regulatory Defense Costs
PCI Investigation	Yes	Privacy Regulatory Defense Costs
PCI Fines and Penalties	Yes – depending on venue	Privacy Regulatory Defense Costs
Bank Lawsuits	Yes	• Security Liability • Privacy Liability
Consumer Lawsuits	Yes	• Security Liability • Privacy Liability
Investor Lawsuit	No	D&O coverage
Lost Income	Yes	Business Income and Extra Expense
Extra Expense	Yes	Business Income and Extra Expense
Restoration of corrupted data	Yes	Data Asset Protection

MARSH

The Marsh Approach

- **Placement of coverage is the last step in the process**
- Insurance is never a valid alternative to good risk management
- However, technology is not a “silver bullet” that will defend against all risks
- Marsh’s approach to the privacy and cyber risks combines elements of:
  - **Assessment;**
  - Remediation;
  - Prevention;
  - Education; and
  - **Risk transfer.**

The Marsh Approach

- **Privacy and Information Security Assessment. Marsh helps your company evaluate internal policies and procedures related to human, physical, and network security, privacy, and breach preparedness**
- **Risk Mapping: Marsh works to identify potential exposure —this includes a scorecard, a gap analysis of your breach response policies and procedures, and a risk map identifying and evaluating both the severity and probability of key privacy and information security risks.**
- **Benchmarking & Modeling: Going beyond simple matching you against what your peers do, Marsh will add a layer of benchmarking that details the costs and expenses associated with likely risk scenarios, including an analysis of a catastrophic privacy and information security event**
- **Coverage gap analysis: Marsh reviews your current insurance policies to determine what coverage may be already respond to claims and losses in the event of network disruption, breach of privacy, or loss of confidential information.**

Step 1: Security A

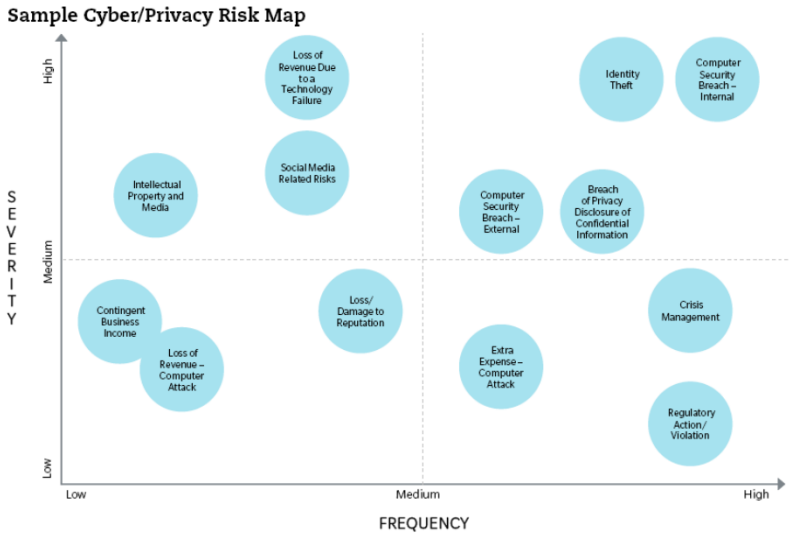
- Marsh utilizes a proprietary ISO 27002 based Privacy & Information Security Assessment ("Assessment") to assist you in evaluating internal policies and procedures related to human, physical and network security, privacy and breach preparedness.
- The Assessment is both insurance and technology "neutral" that enables the company to better understand how "cyber" risks are being managed.
- Accepted by most underwriters as the principal submission document for a cyber placement.
- The object is to better understand the risks and best position you for your renewal.

Scores		
Overall Score		71%
Domain Scores		
Access Control		99%
Computer and Network Management		85%
Security Policy and Standards		63%
Security Organization		65%
Business Continuity		67%
Physical and Environmental Security		86%
Compliance		81%
Systems Development and Maintenance		75%
Vendor Management		89%
Critical Issues		
Patch management process		71%
Managing user accounts		100%
Virus protection		100%
Access control procedures		100%
Physical security controls		86%
Information security policies		77%
Business continuity plans		57%
Information security infrastructure/ organization		63%
Security configuration documentation		46%
Security testing		86%

MARSH December 8, 2014 6

Taking what we learn from the information security assessment and policy review, we will work with you to create a risk map of the organization's principal information security and technology exposures. This map would be a graphical representation of our mutual thoughts on the relative frequency and severity of designated risks.

Step 2: Risk Mapping



7

Step 3: Benchmarking and Modeling

Marsh executes transactions for over 115,000 policies across the globe. Each placement is automatically logged into our global database, and this data set is the foundation for one of our industry's most powerful tools. Our proprietary Marsh Benchmarking Portal. Each placement is tracked and includes details such as product line, limits purchased, cost, rate on line, and insurer details, and can also include headcount, gross sales, gross revenue, number of locations, and other characteristics.

The Marsh Benchmarking Portal was created to address client queries including appropriate limits to buy, what the standard limits are, and what peers are buying. It also is an excellent predictor of any early market shifts and trends in pricing and coverage development.

The following benchmarking diagrams are a sample which can be customized to your needs.

IDEAL Cyber

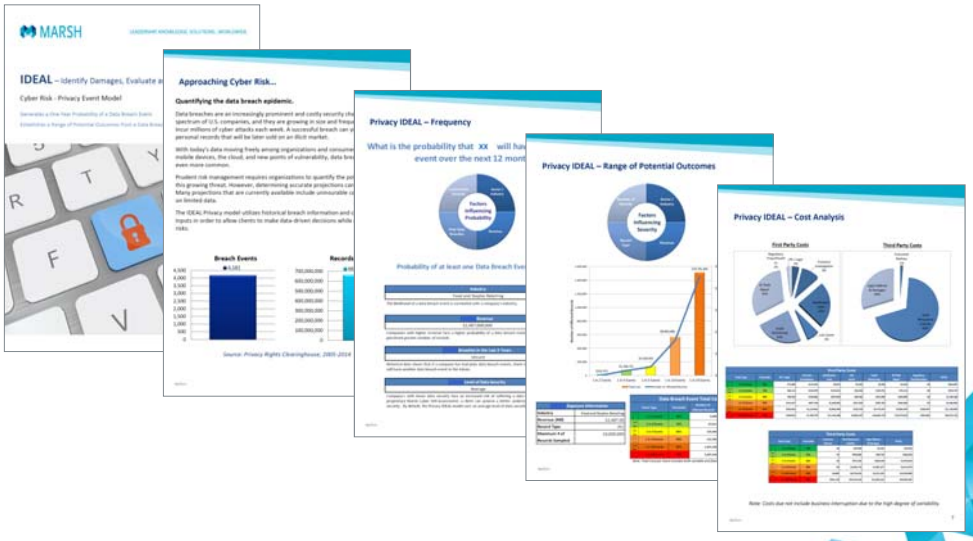
IDEAL Cyber is a dynamic decision support tool created by Marsh's cyber and actuarial experts to project a full range of outcomes to guide cyber insurance purchase decisions based on your company-specific inputs and historical data.

IDEAL Cyber was developed by Marsh Global Analytics (MGA). MGA harmonizes analytics offerings globally, aggregates data, and provides industry-leading analytics through cutting-edge technology.

IDEAL Cyber has two parts:

- **Frequency Model**: Predicts the likelihood of unauthorized disclosure.
- **Severity Model**: Estimates the likely cost per breach event.

IDEAL Cyber – Privacy Event Model:



Step 4: Insurance Gap Analysis

Note: All insurance coverage is subject to the terms, conditions, and exclusions in the applicable individual policies. Marsh cannot provide assurance that insurance can be obtained for any particular client or risk.

Once we thoroughly understand your risk profile, Marsh will conduct a comprehensive coverage gap analysis across all product lines to determine what coverage may be available to respond to claims and losses in the event of computer attack, breach of privacy, or loss of confidential information.

The example depiction on the following page is an illustration of a sample gap analysis.

Not Covered | Covered | Dependent upon specifics of claims, may not be covered

Privacy & Cyber Perils	Property	General Liability	Traditional Fidelity Bond	Computer Crime	E&O	Special Risk	Broad Privacy & Cyber Policy
Destruction, corruption or theft of your electronic information assets/data due to failure of computer or network							Information asset protection
Theft of your computer systems resources							Information asset protection
Business Interruption due to a material interruption in an element of your computer system due to failure of computer or network security (including extra expense and forensic expenses)							Network Business Interruption
Business interruption due to your service provider suffering an outage as a result of a failure of its computer or network security							Network Business Interruption (sublimitted or expanded based upon risk profile)
Indemnification of your notification costs, including credit monitoring services							Privacy Liability (sub-limited)
Defense of regulatory action due to a breach of privacy regulation							Privacy Liability (sub-limited)
Coverage for Fines and Penalties due to a breach of privacy regulation							Privacy Liability
Threats or extortion relating to release of confidential information or breach of computer security							Cyber Extortion
Liability resulting from disclosure of electronic information & electronic information assets							Network Operations Security
Liability from disclosure confidential commercial &/or personal information (i.e. breach of privacy)							Privacy Liability
Liability for economic harmed suffered by others from a failure of your computer or network security (including written policies & procedures designed to prevent such occurrences)							Network Operations Security

MARSH December 8, 2014 12

The Cyber Market

- **Market capacity**:
  - Over 50 markets selling or participating in cyber insurance
  - Over $600M deployable capacity; largest placements still in $200M range
- **Appetite & Approach:** different for each insurer
  - Varies by:
    - Size: revenue, record count, transaction volume
    - Industry: Healthcare, Retail, Finance, Higher Ed, etc.
    - Jurisdiction: USA, Canada, Europe, Asia, etc.
- **Principal Markets**:
  - For larger risks, primary leads: AIG, Beazley, Zurich, Chubb
  - For SME, key markets: capacity is plentiful
- **Market Size**:
  - Estimates vary at between $750M & $1B GWP 2013

MARSH December 8, 2014 13

The Market

- Market capacity:
  - Over 50 markets selling or participating in cyber insurance
  - over $600 million
- Appetite & Approach to underwriting is different by each insurer
  - Varies by:
    - Size: revenue, record count, transaction volume
    - Industry: Healthcare, Retail, Finance, Higher Ed, etc
    - Jurisdiction: USA, Canada, Europe, Asia, etc
- Principal Markets:
  - For larger risks, primary markets: AIG, Beazley, Zurich, Chubb
  - For SME, key markets: lots and lots

Cyber Product Innovation

- **Traditional Approach:**
  - **Fines & Penalties** drop down coverage through Bermuda as an Excess & DIC component of standard cyber capacity
  - **Business Interruption**
    - System Outage/Technology Failure trigger expands beyond a cyber attack
    - Dependent Business Interruption trigger
  - **Catastrophic Approach**
    - Broad form coverage for accounts taking catastrophic approach to risk transfer—i.e. taking a retention above $100M
- **Non-Traditional Approach:**
  - **Industrial Risks**
    - Coverage for property damage caused by technology failure of industrial components, i.e. industrial control systems
  - **P&C Excess-DIC**
    - Excess/DIC coverage over traditional coverage lines (property, casualty, etc.) that picks up covered loss/damage otherwise excluded because caused by a cyber attack

The Process

Application & Quote

- Process gets you a quote.

Or, Understanding the Risk

- Security self-assessment:
  - Security ISO 27001/2
- Risk Mapping
- Modeling & Benchmarking
- Coverage Gap Analysis

- Enables client to make an informed decision on how to approach the risk
- Pre-underwrites the applicant so no surprises

Thank You

MARSH

Robert A. Parisi, Jr.
Managing Director, FINPRO
National Practice Leader for Tech/Telecom E&O and Network Risk

Marsh
1166 Avenue of the Americas
New York, NY 10036

Office: 212.345.5924
Email: robert.parisi@marsh.com

For More Information: www.marsh.com

Marsh

MARSH

MARSH MERCER KROLL
GUY CARPENTER OLIVER WYMAN

Professional Biography

Robert A. Parisi, Jr.

Senior Vice President

Current Responsibilities

Robert Parisi is a Senior Vice President and Technology, Network Risk & Telecommunications National Practice Leader for the Financial and Professional Services ("FINPRO") unit of Marsh. His current responsibilities include advising clients on issues related to technology, privacy, and cyber related risks as well as negotiating with the carriers on terms and conditions.

Experience

Prior to joining Marsh, Robert was the Senior Vice President and Chief Underwriting Officer ("CUO") of eBusiness Risk Solutions of AIG. Robert joined the AIG group of companies in 1998 as legal counsel for its Professional Liability group and held several executive and legal positions within AIG, including CUO for Professional Liability and Technology. While at AIG, Robert oversaw the creation and drafting of underwriting guidelines and policies for all lines of Professional Liability. In addition to working with AIG, Robert has also been in private practice, principally as legal counsel to various Lloyds of London syndicates.

Education

- Law Degree from Fordham University School of Law
- BA in Economics from Fordham College

Affiliations

- Spoken at various business, technology, legal, and insurance forums throughout the world
- Written, on issues effecting professional liability, privacy, technology and telecommunications, media, intellectual property, computer security, and insurance
- Admitted to practice in New York and the U.S. District Courts for the Eastern and Southern Districts of New York
- Honored by *Business Insurance* (2002) magazine as one of the Rising Stars of Insurance
- In 2009, honored by *Risk & Insurance* magazine as a Power Broker


K&L GATES
CYBERSECURITY: MINIMIZING RISK AND MANAGING CONSEQUENCES
Insuring Against Cyber Risks
Roberta Anderson
K&L Gates, Pittsburgh
© Copyright 2014 by K&L Gates LLP. All rights reserved.


INSURING AGAINST CYBER RISKS

K&L GATES

K&L GATES

INSURING AGAINST CYBER RISKS

Agenda

- Potential coverage under “legacy” insurance policies
- Limitations of “legacy” insurance policies
- Specialized “cyber”/privacy insurance policies
- Negotiate … remember the snowflake
- Avoid the traps
- Beware the fine print

klgates.com

K&L GATES

POTENTIAL COVERAGE UNDER "LEGACY" POLICIES

- Directors' and Officers' (D&O)
- Errors and Omissions (E&O)/Professional Liability
- Employment Practices Liability (EPL)
- Fiduciary Liability
- Crime
- Property
- Commercial General Liability (CGL)

4

klgates.com

K&L GATES

POTENTIAL COVERAGE UNDER "LEGACY" POLICIES

- Coverage B provides coverage for damages because of "personal and advertising injury"
- "Personal and Advertising Injury" is defined in part as injury arising out of "[o]ral or written publication, in any manner, of material that violates a person's right of privacy"
  - What is a "Person's Right of Privacy"?
  - What is a "Publication"?

5

klgates.com

K&L GATES

LIMITATIONS OF “LEGACY” INSURANCE POLICIES

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

AMENDMENT OF PERSONAL AND ADVERTISING INJURY DEFINITION

This endorsement modifies insurance provided under the following:

COMMERCIAL GENERAL LIABILITY COVERAGE PART

With respect to **Coverage B Personal And Advertising Injury Liability**, Paragraph **14.e.** of the **Definitions** section does not apply.

14. "Personal and advertising injury" means injury, including consequential "bodily injury", arising out of one or more of the following offenses:

e. Oral or written publication, in any manner, of material that violates a person's right of privacy;

7

klgates.com

K&L GATES

LIMITATIONS OF "LEGACY" INSURANCE POLICIES

This insurance does not apply to:

Access Or Disclosure Of Confidential Or Personal Information

"Personal and advertising injury" arising out of any access to or disclosure of any person's or organization's confidential or personal information, including patents, trade secrets, processing methods, customer lists, financial information, credit card information, health information or any other type of nonpublic information.

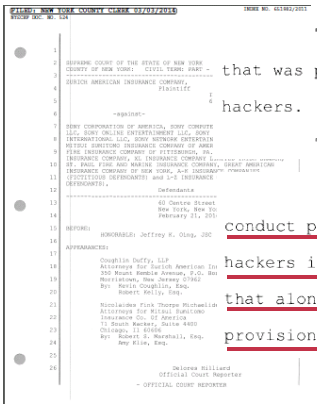
This exclusion applies even if damages are claimed for notification costs, credit monitoring expenses, forensic expenses, public relations expenses or any other loss, cost or expense incurred by you or others arising out of any access to or disclosure of any person's or organization's confidential or personal information.

8

K&L GATES

LIMITATIONS OF "LEGACY" INSURANCE POLICIES

- Zurich American Insurance Co. v. Sony Corp. of America et al.



The question now becomes, was that a publication that was perpetrated by Sony or was that done by the hackers.

There is no way I can find that Sony did that.

In this case my finding is that there was no act or conduct perpetrated by Sony, but it was done by 3rd party hackers illegally breaking into that security system. And that alone does not fall under paragraph E's coverage provision.

9

K&L GATES

THE TYPES OF RISKS COVERED

- Privacy And Network Security
  - Provides coverage for liability (defense and indemnity) arising out of data breaches, transmission of malicious code, denial of third-party access to the insured’s network, and other network security threats
- Regulatory Liability
  - Provides coverage to deal with regulators and liability arising out of administrative or regulatory investigations, proceedings, fines and penalties
- Crisis Management
  - Provides coverage for forensics experts, notification, call centers, ID theft monitoring, PR and other crisis management activities

11

klgates.com

K&L GATES

THE TYPES OF RISKS COVERED

- Network Interruption And Extra Expense (and CBI)
  - Coverage lost business income and extra expense caused by malicious code, DDoS attacks, unauthorized access to, or theft of, information, and other security threats to networks
- Information Asset Coverage
  - Coverage for damage to or theft of the insured's own systems and hardware, and may cover the cost of restoring or recreating stolen or corrupted data.
- Extortion
  - Coverage for losses resulting from extortion (payments of an extortionist's demand to prevent network loss or implementation of a threat).

12

klgates.com


14


AVOID THE TRAPS

K&L GATES

Massive Target Hack Traced Back To Phishing Email

Posted: 02/12/2014 3:56 pm EST | Updated: 02/12/2014 5:59 pm EST

Hackers gained access to Target's computer system and stole financial and personal data of 110 million shoppers by tricking an employee at an outside vendor into clicking on a malicious email, according to a report Wednesday by security blogger Brian Krebs.

An employee at Fazio Mechanical, a Sharpsburg, Pa.-based heating, ventilation and air-conditioning company with access to Target's network, fell for a "spear phishing" attack, in which hackers send malware-laced emails that appear to come from trusted sources to take over victims' computers, according to Krebs, who cited sources close to the investigation.

16

klgates.com

TRAP EXAMPLE

I. INSURING AGREEMENTS

A. DATA BREACH LIABILITY

The Company will pay on behalf of the **Insured** all sums in excess of the Deductible amount stated in the Declarations which the **Insured** shall become legally obligated to pay as **Damages** and **Claims Expenses** resulting from **Claims** first made against the **Insured** and reported to the Company in accordance with the Notice provisions in Section VI of this policy during the **Policy Period**, or **Extended Reporting Period**, if applicable, said **Claim** or **Claims** arising as a result of a **Data Breach Wrongful Act** ~~by the Insured~~, provided that:

(1) Such **Data Breach Wrongful Act** was committed on or after the **Retroactive Date** and before the end of the **Policy Period**; and

(2) prior to the **Knowledge Date** stated in the Declarations, no **Senior Executive** knew or could have been reasonably expected to know that such **Data Breach Wrongful Act** might give rise to a **Claim**.

"**Data Breach Wrongful Act**" means any actual or alleged act, failure to act, error, omission, misstatement, misleading statement, neglect, or breach of duty that causes:

a) **Personal Injury** arising out of a **Privacy Breach** or the **Insured's Media Content**;

b) **Unauthorized Access** as a result of any unauthorized act caused by an employee of an **Entity Insured**;

c) the failure to prevent **Unauthorized Access** to **Computer Systems**;

d) the inability of a third party, who is authorized to do so, to gain access to **Computer Systems**;

e) the failure to prevent transmission of **Malicious Code**; and

17

klgates.com

K&L GATES

BUSINESS INSURANCE

Unintended disclosure, paper records loss most common data breaches: Study

Judy Greenwald

September 18, 2014 - 1:30 pm ET

A study of more than 1,500 data breaches in 2013 and 2014 by a unit of Beazley P.L.C. reveals that the two most common sources of breaches are unintended disclosure and the physical loss of paper records.

18

klgates.com

TRAP EXAMPLE

I. **INSURING CLAUSES**

A. **CYBER LIABILITY**

The Company shall pay **Loss** on behalf of an **Insured** on account of any **Claim** first made against such **Insured** during the **Policy Period** or, if exercised, during the Extended Reporting Period, for **Injury**.

Injury means **Disclosure Injury**, **Reputational Injury**, **Content Injury**, **Conduit Injury** or **Impaired Access Injury**.

Disclosure Injury means injury sustained or allegedly sustained by a natural person because of the potential or actual unauthorized access to such natural person's **Record** by another **Person** when such access:

A. occurs on or after the **Retroactive Date** and before the end of the **Policy Period**; and

B. results directly from:

1. a **Cyber-attack** into a **System** owned by an **Insured Organization**; or

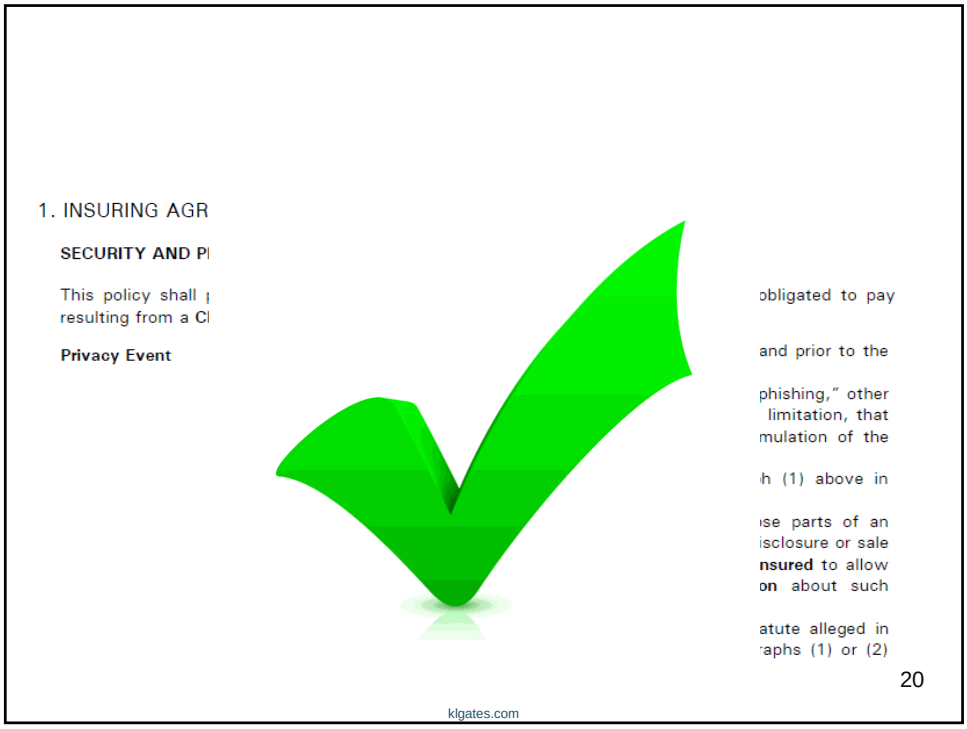
2. a natural person who has gained unauthorized access to, or has exceeded authorized access to a **System** or **System Output** owned by:

i. an **Insured Organization**; or

ii. an organization that is authorized by an **Insured** through a written agreement to process, hold or store **Records** for an **Insured**.

19

klgates.com


1. INSURING AGR
SECURITY AND P
This policy shall
resulting from a C
Privacy Event
obligated to pay
and prior to the
phishing," other
limitation, that
mulation of the
h (1) above in
ise parts of an
isclosure or sale
nsured to allow
on about such
atute alleged in
raphs (1) or (2)
20
klgates.com


BEWARE THE FINE PRINT

K&L GATES

K&L GATES

BEWARE
THE
FINE
PRINT

22

klgates.com

K&L GATES

TIPS FOR A SUCCESSFUL PLACEMENT

- Embrace a Team Approach
- Understand the Risk Profile
- Review Existing “Legacy” Coverages
- Purchase Specialty “Cyber” Coverage as Needed
- Remember the “Cyber” Misnomer
- Spotlight the “Cloud”
- Consider the Amount of Coverage
- Pay attention to the Retroactive Date and ERP
- Look at Defense and Settlement Provisions
- Engage Coverage Counsel

23

klgates.com

K&L GATES

Legislative and Regulatory Initiatives

Presenters: *Mike O'Neil, K&L Gates - Washington, D.C.*

K&L GATES

CYBERSECURITY:
MINIMIZING RISK AND MANAGING CONSEQUENCES

Regulatory and Legislative Developments

Mike O'Neil
K&L Gates LLP, Washington D.C.

K&L GATES

CURRENT FEDERAL CYBER SECURITY REQUIREMENTS

- No overarching federal cyber security laws……yet
- Sectoral approach, e.g.:
  - HIPAA & HITECH for personal health information
  - Graham Leach Bliley for personal financial information
  - FCRA & FACTA for credit reports
  - FAR for federal contractors
  - FISMA for federal agencies
  - Process requirements rather than specified administrative, physical and technical issues

K&L GATES

K&L GATES

CURRENT FEDERAL CYBER SECURITY REQUIREMENTS (CONT'D)

- Key Points:
  - Reasonable, not perfect measures
  - Appropriate to threat environment
  - Informed by experience
  - Calibrated to sensitivity of information protected
  - Continuous review and adjustment as necessary
  - All part of holistic information security program

K&L GATES

PRACTICALLY EVERY STATE HAS CYBER SECURITY LAW

Two approaches

- **Directly** require information security programs
  - Must develop and implement reasonable measures, e.g., California
  - Massachusetts' approach – require specific elements, e.g., firewalls, security patches, protection, secure malware protection, secure authentication
  - encryption required when sent over public network, via WiFi, stored on laptops/portable devices
- **Indirectly**, as part of data breach laws, e.g., Pennsylvania

K&L GATES

FEDERAL REGULATORS

- **Federal contracts** – DOD, NASA, GSA administer the FAR; DOD administers DFAR
- **Financial information –** FRB, FTC, OCC, FDIC, SEC, WCUA, OTS, and CFTC enforce GLB
- **Health information** – HHS enforces HIPAA
- **Closest to national regulator is FTC:**
  - Sec. 5 of the FTC Act provides jurisdiction over "unfair or deceptive acts or practices in or affecting commerce"
- Few specific regulations/standards issued per Sec. 5 – reliance on guidance, guides
- Pursues specific cases – typically seeking 20 yr. consent decrees, compliance audits of comprehensive information security program, sometimes fines

K&L GATES

FTC ENFORCEMENT SETTLEMENTS – A PROGRESSION

- **Microsoft (2002) –** false and misleading advertising
  - no breach, no security flaw
  - charge was overstatement of security
- **Tower Records (2004) –** false and deceptive statements
  - claimed customer data encrypted
  - no encryption, vulnerable to unauthorized access
- **Petco (2005) –** false and deceptive claims
  - claimed customer data encrypted
  - not encrypted in storage, vulnerable to known attacks
  - breach of customer data
  - first time settlement requires stored data be encrypted

K&L GATES

K&L GATES

FTC SETTLEMENTS

- **Sunbelt Lending (2005)** – unfair and deceptive acts
  - failure to follow FTC Safeguards Rule and Privacy Rule (GLB)
  - therefore, violation of Sec. 5
- **BJ's Wholesale Club** – charged as unfair practice
  - failure to encrypt transmitted/stored data
  - stored data could be reached using common default IDs/passwords
  - failed to use measure to detect intrusions
- **The Pattern in these and other subsequent FTC settlements:**
  - Require specific elements in comprehensive data security plans
  - Enforce FTC Safeguards, Privacy, Disposal Rules
  - Often no data breach
  - Impose fines

klgates.com 6

K&L GATES

RECENT REGULATORY TRENDS

FTC's broad authority over data security unfairness upheld earlier this year:

- Despite lack of published regulations
  - *FTC vs. Wyndham Worldwide Corp. et al*, case no. 2:13-cv-01887, U.S. Dist. Ct. for the District of New Jersey
- For companies that must also answer to other regulators
  - *In the Matter of LabMD*, Case No. 9357, FTC

klgates.com 7

K&L GATES

K&L GATES

LEGISLATIVE DEVELOPMENTS

113th Congress has focused on:

- NSA Reform
  - H.R. 3361 passed in House
  - S. 2685 blocked in Senate
- **Prospects for 114th Congress better because**
  - Key PATRIOT Act provisions expire in 2015
  - Cyber threat information sharing
  - H.R. 624 passed in House
  - S. 2588 reported from Senate Committee - prospects unlikely in lame duck - better prospects in 114th Congress

klgates.com 8

K&L GATES

KEY PROVISIONS IN CYBER THREAT SHARING BILLS

- Anti-trust exemption for cyber threat sharing with feds
- Liability protection for cyber threat sharing with feds
- Cyber threats shared with feds exempt from public disclosure
- Personal information minimized within government
- Private sector can employ countermeasures
- Issues yet to be resolved:
  - Purposes for which feds can use cyber threat information
  - Extent of privacy protections
  - Use of countermeasures

klgates.com 9

K&L GATES

USE OF COUNTERMEASURES

> "…an action, device, procedure, technique, or other measure applied to an information system of information that is stored on, processed by, or transiting an information system that prevents or mitigates a known or suspected cyber security threat or security vulnerability." - S.2588

- Could embrace defenses
  - Firewalls
  - Shutdowns
  - Tagging
- Other possibilities include active defense – "hack back" through tracking, infiltration, deletion, exploitation, destruction
- Problems: misattribution, retaliation, escalation, and liability

klgates.com 10

K&L GATES

RELATED DEVELOPMENT

- **US-EU Safe Harbor Agreement**
  - Intended to permit digital trade where U.S. companies cannot comply with EU Data Protection Directive
  - Allows sharing of information about Europeans with U.S. companies that certify compliance with EU data protection principles, including "reasonable precautions to protect personal information from loss, misuse and unauthorized access, disclosure, alteration and destruction."
  - Called into question in wake of Snowden
  - EU demanding data protection for EU citizens equal to U.S. citizens
  - Failure to reach agreement on data protection could imperil TTIP and significantly affect trans-Atlantic trade
  - Ongoing discussions but no resolution

klgates.com 11

Senate Cybersecurity Legislation

S.1353 - Cybersecurity Act of 2013 (Rockefeller, Thune)

- Enables NIST to support the development of a voluntary, industry-led set of standards and procedures to reduce cyber risks to CI. Requires NIST to:
  - Coordinate with the private sector, critical infrastructure owners and operators
  - Consult with the heads of agencies, state and local governments, governments of other nations, and international organizations
  - Identify an approach that may be adopted by CI operators to help manage cyber risks

- Prohibits information provided to NIST from being used by federal, state, tribal, or local agencies to regulate the activity of any entity.

- Directs OSTP to develop a federal cybersecurity research and development plan to meet cybersecurity objectives, including how to guarantee individual privacy, verify third-party software and hardware, address insider threats, determine the origin of messages transmitted over the Internet, and protect information stored using cloud computing or transmitted through wireless services.

- Directs NSF to support cybersecurity research and directs NIST to continue coordinating a national cybersecurity awareness campaign.

S.2588 -- *Cybersecurity Information Sharing Act (Feinstein)*

- House Companion Bill: H.R.624 - Cyber Intelligence Sharing and Protection Act (Rogers) (See below for differences between the two bills)

- Requires DNI, DHS, DOD, and DOJ to develop procedures for sharing cyber threat indicators with private entities; non-federal government agencies; or state, tribal, or local governments.

- Permits private entities to monitor and operate "countermeasures" to prevent or mitigate cybersecurity threats on their own systems and, with written consent, the systems of other entities. Authorizes such entities to monitor information that is stored on, processed by, or transiting such monitored systems.
  - Countermeasure is defined as "an action an action, device, procedure, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that prevents or mitigates a known or suspected cybersecurity threat or security vulnerability."

- Permits state, tribal, or local agencies to use shared indicators (with the consent of the agency sharing the indicators) to prevent, investigate, or prosecute computer crimes.

- Exempts private entities that exchange cyber threat indicators from antitrust laws.

- Requires DOJ to develop guidelines to limit receipt, retention, use, and dissemination of PII.

- Directs DHS to develop a process for the federal government to accept cyber threat indicators and countermeasures from entities in an electronic format and distribute such indicators and countermeasures to appropriate federal entities.

- Prohibits government agencies from using indicators and countermeasures provided to the federal government to regulate the lawful activities of an entity.

- Provides liability protections to entities that monitor information systems, and share and receive indicators and countermeasures.

- Prohibits requirements on entities to provide information to the federal government.

- Directs the DNI to report cybersecurity threats, including attacks, theft, and data breaches, to Congress.

S.2519 -- National Cybersecurity and Communications Integration Center Act of 2014 (Carper, Coburn)

- Authorizes DHS to oversee critical infrastructure protection, cybersecurity, and related DHS programs with respect to security and resilience. Specifies activities that may be carried out, including:
    - Federal civilian information sharing
    - Sharing of cybersecurity threat, vulnerability, impact, and incident information among federal, state, and local government entities and private sector entities
    - Providing technical assistance and recommendations to federal and non-federal entities.

- Requires the operations center to be composed of:
    - Representatives of federal agencies, including civilian and law enforcement agencies and elements of the intelligence community
    - State and local governments and other non-federal entities, including private sector owners and operators of critical information systems.

- Prohibits DHS from creating regulations or setting standards relating to the cybersecurity of private sector CI that were not in effect on the day before the enactment of this Act.

S.1611 —Federal Data Center Consolidation Act of 2013 (Bennet)

- Requires the heads of specified federal agencies to submit a comprehensive inventory of data centers owned, operated, or maintained by the agency and a multi-year strategy to achieve the consolidation and optimization of the data centers to OMB each fiscal year.

- Requires agencies to implement their data center consolidation and optimization strategies consistent with federal guidelines on cloud computing security

- Authorizes DNI to waive the applicability of any provision of this Act to any element of the intelligence community if such waiver is in the interest of national security.

- Expires October 1, 2018.

S.2521 - Federal Information Security Modernization Act of 2014 (Carper, Coburn)

- House Companion Bill: H.R.1163 -- Federal Information Security Amendments Act of 2013 (See below for differences between the two bills)

- Establishes OMB oversight of agency information security policies, and establishes authority for DHS to carry out the operational aspects for information systems.

- Requires DHS to develop and oversee implementation of operational directives to implement OMB standards and guidelines and requires DHS to ensure the operation of the federal information security incident center (FISIC).

- Requires OMB to establish procedures for agencies to follow in the event of a breach involving disclosure of PII, including requirements for notice to affected individuals, FISIC, and Congress.

- Requires agencies to notify Congress of discovered security incidents within seven days and directs agencies to submit an annual report regarding major incidents to OMB, DHS, Congress, and the Comptroller General (GAO).

- Directs FISIC to provide agencies with intelligence about cyber threats, vulnerabilities, and incidents for risk assessments.

Senate Cybersecurity Legislation

House Cybersecurity Bills

H.R.624 - Cyber Intelligence Sharing and Protection Act (Rogers)

- Senate Companion Bill: S.2588 -- *Cybersecurity Information Sharing Act (Feinstein)*

- Directs the federal government to conduct cybersecurity activities to provide "shared situational awareness."
  - Defines "shared situational awareness" as an environment where cyber threat information is shared in real time between all designated federal cyber operations centers to provide actionable information about all known cyber threats.

- Directs the President to designate an entity within DHS to receive cyber threat information and an entity within DOJ to receive information related to cybersecurity crimes.

- Directs DHS, DOJ, DNI, and DOD to establish and review policies and procedures governing the receipt, retention, use, and disclosure of non-publicly available cyber threat information shared with the federal government. Procedures must:
  - Minimize the impact on privacy and civil liberties;
  - Reasonably limit the receipt, retention, use, and disclosure of cyber threat information associated with specific persons that is unnecessary to protect against or mitigate cyber threats in a timely manner
  - Include requirements to safeguard non-publicly available cyber threat information that may be used to identify specific persons from unauthorized access or acquisition;
  - Protect the confidentiality of cyber threat information associated with specific persons;
  - Not delay or impede the flow of cyber threat information necessary to defend against or mitigate a cyber threat.

- Requires DNI to establish procedures that allow intelligence community elements to share cyber threat intelligence with private-sector entities and utilities.

- Authorizes a cybersecurity provider, with the express consent of a protected entity to:
  - Use cybersecurity systems to identify and obtain cyber threat information in order to protect the rights and property of the protected entity;
  - Share cyber threat information with any other entity designated by the protected entity, including the DHS and DOJ entities designated by the President.

- Requires anonymization or minimization of information and prohibits the use of such information to gain a competitive advantage and, if shared with the federal government, exempts such information from public disclosure and prohibits the use of the information for regulatory purposes.
  - A non-federal recipient may only use such information for a cybersecurity purpose.

- Prohibits a civil or criminal cause of action against a protected entity, a self-protected entity, or a cybersecurity provider acting in good faith and in accordance with the act.

- Prohibits shared information requirements from being construed to provide new authority to:
    - A cybersecurity provider to use a cybersecurity system to identify or obtain cyber threat information from a system or network other than a system or network owned or operated by a protected entity for which such cybersecurity provider is providing goods or services for cybersecurity purposes
    - A self-protected entity to use a cybersecurity system to identify or obtain cyber threat information from a system or network other than a system or network owned or operated by such self-protected entity.

- Allows the federal government to use shared cyber threat information for:
    - Cybersecurity purposes to ensure the integrity, confidentiality, availability, or safeguarding of a system or network
    - The investigation of cybersecurity crimes;
    - The protection of individuals from the danger of death or serious bodily harm and the prosecution of crimes involving such dangers.
    - Prohibits the federal government from affirmatively searching such information for any other purpose.

- Prohibits the federal government from using PII such as library records, firearms sales records, educational records, tax returns, and medical records for any unauthorized use.

- Prohibits this Act from being construed to provide new or alter any existing authority for an entity to sell personal information of a consumer to another entity for marketing purposes.

H.R.2952 — Critical Infrastructure Research and Development Advancement (CIRDA) Act of 2014

- Requires DHS to present a plan to Congress regarding cybersecurity technology R&D efforts for protecting CI, which would:
    - Identify CI security risks, security technology gaps
    - Prioritize CI security technology needs
    - List programmatic initiatives for deployment of CI security technology
    - Describe progress made on each CI security risk from previous report
    - Focus on CI protection operated by the private sector

- Requires DHS to designate a technology clearinghouse for sharing proven technology solutions for protecting CI.

H.R. 3107 -- Homeland Security Cybersecurity Boots-on-the-Ground Act (Clarke)

- Requires DHS to classify a cybersecurity workforce, and assess that workforce on a semi-annual basis, to include:
    - Physical locations;

  - Whether employed by independent contractors or federal employees;
  - Progress on the 2009 authorized hiring of 1,000 cybersecurity positions;
  - Vacancies;
  - What percentage of workforce has received essential training; and
  - Recruiting costs

- Requires DHS to establish and maintain a process for independent contractors to receive initial and recurring security training

- Requires GAO to study the DHS assessment and workforce strategy

H.R. 3635 -- Safe and Secure Federal Websites Act of 2014

- Prevents an agency from launching a Federal PII website prior to agency CIO certifying to Congress that website is "fully functional and secure"
  - "Federal PII website" means a website that:
    - Is operated by (or under a contract with) an agency;
    - Elicits, collects, stores, or maintains personally identifiable information of individuals and is accessible to the public; and
    - Is first made accessible to the public and collects or stores personally identifiable information of individuals, on or after October 1, 2012.

  - PII means information about an individual elicited, collected, store, or maintained by an agency, including:

    - Any information able to trace identity of an individual, such as name, SSN, date of birth, place of birth, mother's maiden name, biometric records; and
    - Any other information linked or linkable to an individual, such as medical, education, financial and employment information

- Requires OMB to establish and oversee policies and procedures in case of data breach of a federal website, including:
  - Notice to individuals within 72 hours; and
  - Timely report to Federal cybersecurity center

H.R.3696 — National Cybersecurity and Critical Infrastructure Protection Act of 2014

- Requires DHS to conduct cybersecurity activities to enable federal entities to prevent and respond to "cyber incidents"
  - "Cyber incident" is an incident (or attempt) that would: (1) jeopardize the security, integrity, confidentiality, or availability of an information system or network or any information stored on, processed on, or transiting such a system; (2) violate laws or procedures relating to system security, acceptable use policies, or acts of terrorism against such a system or network; or (3) deny access to or degrade, disrupt, or destruct such a system or network or defeat an operations or technical control of such a system or network.

- Requires DHS to coordinate with federal, state and local governments, national labs, and critical infrastructure owners and operators to, among other things, seek industry

sector-specific expertise to develop voluntary security and resiliency strategies and to ensure that the allocation of federal resources is cost effective and reduces burdens on critical infrastructure owners and operators

- Requires DHS to, among other things, manage federal efforts to secure federal civilian information systems and, upon request, to support the efforts of private CI owners and operators to protect against cyber threats

- Requires DHS to designate CI sectors, including:
  - chemical;
  - commercial facilities;
  - communications;
  - critical manufacturing;
  - dams;
  - Defense Industrial Base;
  - emergency services;
  - energy;
  - financial services;
  - food and agriculture;
  - government facilities;
  - health care and public health;
  - information technology;
  - nuclear reactors, materials, and waste;
  - transportation systems; and
  - water and wastewater systems.

- Each sector is designated a Sector Coordinating Council (SCC) and at least one Information Sharing and Analysis Center (ISAC)
  - SCC comprised of small, medium and large CI owners and operators, private entities, and representative trade associations, which serve as a self-governing, self-organized policy, planning, and strategic communications entity for coordinating with DHS regarding resilience activities and emergency response efforts
  - Government entities which regulate may not be an SCC member
  - DHS may not determine SCC membership

- Permits DHS to enter into contracts with private entities that provide electronic communication, remote computing, and cybersecurity services

- Codifies the National Cybersecurity and Communications Integration Center as a federal-civilian information sharing interface to:
  - Provide shared situational awareness to enable real-time, integrated, and operational actions across the federal government; and
  - Share cyber threat information among federal, state, and local government entities, ISACs, private entities, and critical infrastructure owners and operators that have information sharing relationships

- Requires DHS to establish Cyber Incident Response Teams in order to provide technical assistance and recommendations to federal, state, local governments, private entities, and CI owners and operators

- Redesignates the National Protection and Programs Directorate as the Cybersecurity and Infrastructure Protection Directorate
    - Creates an Under Secretary for Cybersecurity and Infrastructure Protection, Deputy Under Secretary for Cybersecurity, and Deputy Under Secretary for Infrastructure Protection

- Requires NIST to support the development of voluntary, industry-led standards and processes to reduce cyber risks to CI

H.R.1163 -- Federal Information Security Amendments Act of 2013

- Senate Companion Bill: S.2521 - Federal Information Security Modernization Act of 2014

- Reestablishes OMB's oversight authority with respect to agency information and security policies and practices.

- Extends the security requirements of federal agencies to include responsibilities for:
    - Complying with computer standards developed by NIST;
    - Ensuring complementary and uniform standards for information systems and national security systems;
    - Ensuring that information security management processes are integrated with budget processes;
    - Securing facilities for classified information;
    - Maintaining sufficient personnel with security clearances; and
    - Ensuring that information security performance indicators are included in the annual performance evaluations of all managers, senior managers, senior executive service personnel, and political appointees.

- Directs agencies to determine information security levels in accordance with information security classifications and standards under NIST.

- Directs agencies to collaborate with OMB and appropriate public and private sector security centers. Requires that security incidents be reported to the federal information security incident center, appropriate security operations centers, and appropriate Inspector Generals.

- Specifies that no additional funds are authorized for agencies to carry out their responsibilities under this Act.

Senate Cybersecurity Legislation

Differences between S.2521 (Federal Information Security Modernization Act of 2014) and H.R.1163 (Federal Information Security Amendments Act of 2013)

- S.2521 sets out authority for the Secretary of Homeland Security (DHS) to carry out the operational aspects of policies for information systems rather than OMB. Requires DHS to develop and oversee implementation of operational directives to agencies to implement the OMB Director's standards and guidelines, as well as the requirements of this Act.

- S.2521 requires DHS rather than OMB to ensure the operation of the federal information security incident center (FISIC).

- S.2521 provides for OMB's information security authorities to be delegated to the Director of National Intelligence (DNI) for certain systems operated by an element of the intelligence community.

- S.2521 requires agencies to notify Congress of discovered security incidents within seven days. It also directs agencies to submit an annual report regarding major incidents to OMB, DHS, Congress, and the Comptroller General (GAO).

- S.2521 provides for OMB's information security authorities to be delegated to the Director of National Intelligence (DNI) for certain systems operated by an element of the intelligence community.

Differences between S.2588 (CISA) and H.R.624 (CISPA)

- S.2588 exempts from antitrust laws private entities that, for cybersecurity purposes, exchange or provide: (1) cyber threat indicators; or (2) assistance relating to the prevention, investigation, or mitigation of cybersecurity threats. Makes such exemption inapplicable to price-fixing, allocating a market between competitors, monopolizing or attempting to monopolize a market, boycotting, or exchanges of price or cost information, customer lists, or information regarding future competitive planning.

- S.2588 requires an entity (government or private) sharing cyber threat indicators remove any information that the entity knows at the time of sharing to be personal information of or identifying a specific person not directly related to a cybersecurity threat.

PRIVACY LEGISLATION

Geolocation privacy:

H.R. 1312: Geolocational Privacy and Surveillance Act

- Substantively identical to House GPS Act introduced in 112th.
- Would require a consumer's prior consent to use or disclose information concerning the location of a wireless communication device (telephone, GPS receiver, mobile computer, etc.). Would also prohibit unauthorized intercept of that information.
- Exceptions are for information acquired in the "normal course of business" for activities that are "a necessary incident to the rendition of service," as well as for emergency information, theft or fraud, or warrant.
- Allows for civil and criminal penalties as well as private right of action.

S. 639: Geolocational Privacy and Surveillance Act.

- Materially similar to Senate GPS Act introduced in 112th and H.R. 1312 in 113th; but clarifies that bill does not create cause of action against electronic communication service provide, remote computing service provide, geolocation service provider, or law enforcement or investigative officer.

H.R. 983: Online Communications and Geolocation Protection Act

- Defines "Geolocation Information Service" (GIS) as one that generates or uses geolocation information for provision of mapping, locational, or directional information to the public . . . by or through the operation of any wireless communication device.
- Generally, prohibits government entity from intercepting, disclosing, or using geolocation information (but exceptions for FISA, consent, public information, emergency, warrant. Would also prohibit GIS from providing that information to a government entity unless excepted under the statute.
- Authorizes civil action for statutory damages of actual loss or greater of $100/day or $10,000. Defense for good faith reliance on warrant, court order, subpoena, legislative authorization, or statutory authorization.

Senate Cybersecurity Legislation

Do Not Track:

S. 418: Do-Not-Track Online Act of 2013

- Substantively identical to Do-Not-Track Online Act of 2011 (112th Cong.).
- Provides for FTC rulemaking in 12 months that would create a process for consumers to indicate that they do not wish for "providers of online services" to collect "personal information" (undefined) about them. Prohibits providers of online services from collecting information about a user who has expressed this.
- Exceptions for (1) necessary information collected to provide a service requested by the user, if anonymized or deleted upon provision of the service; or (2) affirmative consent based on clear and conspicuous notice.
- Provides for FTC and State enforcement, civil penalties.

Data security and breach notification:

S. 1193: Data Security and Breach Notification Act of 2013

- Requires a covered entity to take "reasonable measures" to protect and secure data containing personal information.
- Requires a covered entity that owns or licenses data to provide notice of data breach to individuals and law enforcement.
- "Covered entity" defined as any entity that acquires, maintains, stores, or utilizes personal information. Excludes GLBA/HIPAA-covered entities.
- Provides for FTC enforcement; sets a statutory cap of $500,000 each for a security and notification violation arising from same act/omission/breach.
- No private cause of action.
- Preempts state or local laws regarding data security or data breach.

H.R. 1468: SECURE IT (Title V only)

- Title V of bill contains materially similar data security and breach notification obligations to S. 1193.

H.R. 1121: Cyber Privacy Fortification Act of 2013

- Creates criminal penalties for knowing failure to notify of a security breach involving sensitive PII.
- Creates a general statutory penalty cap of $500,000 for federal and state enforcement of federal laws relating to data security, or $1 million for intentional violations.
- Requires federal agencies to create and publish for comment a "privacy impact assessment" for any proposed rulemakings that would pertain to collection/maintenance/use/disclosure of PII from 10 or more individuals. Would also require a final assessment for final rulemakings, and a periodic review of existing rules to determine if appropriate given privacy implications.

Other:

H.R. 210: To require retail establishments that use mobile device tracking technology to display notices to that effect

- Requires a retail establishment that uses mobile device tracking to post a notice that the technology is in use, and that individuals can avoid tracking by turning off their mobile device.
- Provides for FTC enforcement.

H.R. 1913: Application Privacy, Protection, and Security Act of 2013

- Requires prior consent before a mobile application collects personal data about a user.
- Safe harbor for regulations promulgated under the Act if developer adopts and follows industry code of conduct.
- Provides for FTC, State enforcement; would supersede conflicting state laws.

Committee	House	Senate
Commerce		**Cybersecurity and American Cyber Competitiveness Act of 2013 (S.21)** • Sen. Jay Rockefeller introduced the bill on 1/22/13, referred to Senate Commerce Committee. **Cybersecurity Act of 2013** (S.1353) • Sen. Jay Rockefeller introduced the bill on 7/24/13. • Ordered to be reported with an amendment in the nature of a substitute favorably on 7/30/2013. Report No. 113-270. • Placed on Senate Legislative Calendar under General Orders. Calendar No. 490. **Do-Not-Track Online Act of 2013** (S.418) • Sen. Rockefeller introduced bill, referred to Commerce Committee on 2/28/13. **Do-Not-Track Kids Act of 2013** (S.1700) • Sen. Markey introduced bill, referred to Commerce Committee on 11/14/13. **Data Security and Breach Notification Act of 2013** (S.1193) • Sen. Toomey introduced bill, referred to Commerce Committee on 6/20/13.
Energy & Commerce	**Do-Not-Track Kids Act of 2013** (H.R. 3481) • Rep. Barton introduced bill, referred to Energy & Commerce Subcommittee on Communications & Technology on 11/14/13. **SECURE IT** (H.R. 1468) • Rep. Blackburn introduced bill, referred to Energy & Commerce Committee on 6/24/13. **To require retail establishments that use mobile device tracking technology to display notices to that effect** (H.R. 210) • Rep. Serrano introduced bill, referred to Energy & Commerce Subcommittee on Commerce, Manufacturing & Trade on 1/4/13. **APPS Act of 2013** (H.R. 1913) • Rep. Hank Johnson introduced bill, referred to Energy & Commerce Subcommittee on Commerce, Manufacturing & Trade on 5/10/13.	
Judiciary	**USA FREEDOM Act** (H.R. 3361) • Rep. Sensenbrenner introduced bill on 10/29/13.	**USA FREEDOM Act** (S.1599) • Leahy introduced bill, referred to Judiciary Committee on 10/29/2013.

Committee	House	Senate
	• Reported out of Judiciary Committee on 5/15/2014. H. Rept. 113-452, Part I • Reported out of Intelligence Committee 5/15/14 H. Rept. 113-452, Part II • Passed House on 303 - 121 vote on 5/22/14. (Roll no. 230).(text: CR H4789-4793) **Geolocational Privacy and Surveillance Act** (H.R. 1312) • Rep. Chaffetz introduced bill, referred to Judiciary Committee on 3/21/13. **Online Communications and Geolocation Protection Act** (H.R. 983) • Rep. Lofgren introduced bill, referred to Judiciary Committee on 3/6/13. **SECURE IT** (H.R. 1468) • Rep. Blackburn introduced bill, referred to Judiciary Committee on 6/24/13. **Cyber Privacy Fortification Act of 2013** (H.R. 1121) • Rep. Conyers introduced bill, referred to Judiciary Subcommittee on Crime, Terrorism, Homeland Security & Investigations on 4/15/13.	**USA FREEDOM Act** (S.2685) • Leahy introduces bill, referred to Judiciary Committee on 7/29/14. • Cloture motion on the motion to proceed to the measure presented in Senate on 11/12/14. **Geolocational Privacy and Surveillance Act** (S.639) • Sen. Wyden introduced bill, referred to Judiciary Committee on 3/21/13.
Intelligence	**USA FREEDOM Act** (H.R. 3361) • Rep. Sensenbrenner introduces on 10/29/13. • Reported out of Judiciary Committee on 5/15/2014. H. Rept. 113-452, Part I • Reported out of Intelligence Committee 5/15/14 H. Rept. 113-452, Part II • Passed House on 303 - 121 vote on 5/22/14. (Roll no. 230).(text: CR H4789-4793) **Cyber Intelligence Sharing and Protection Act (H.R.624)** • Rep. Mike Rogers introduced bill on **2/13/13.** • Reported (Amended) by the Committee on Intelligence on 4/15/13. H. Rept. 113-39. • Passed/agreed to in House: On passage Passed by the Yeas and Nays: 288 - 127 (Roll no. 117). **Online Communications and Geolocation Protection Act** (H.R. 983) • Rep. Lofgren introduced bill, referred to Intelligence Committee on 3/6/13. **SECURE IT** (H.R. 1468) • Rep. Blackburn introduced bill, referred to Intelligence Committee on 6/24/13.	**Cybersecurity Information Sharing Act of 2014** (S.2588) • Sen. Dianne Feinstein introduced the bill on 7/10/2014. • Reported out of committee without written report on 7/10/2014. • Placed on Senate Legislative Calendar under General Orders. Calendar No. 462 on 7/10/2014.
Governmental Affairs	**Federal Information Security Amendments Act of 2013** (H.R.1163) • Rep. Darrell Issa introduced the bill on 3/14/13.	**Federal Data Center Consolidation Act of 2013** (S.1611) • Sen. Michael Bennet introduced the bill on 10/30/2013.

Committee	House	Senate
	• Ordered to be Reported by Voice Vote on 3/20/13 • Reported (Amended) by the committee H. Rept. 113-40. • House passes 416-0 on 4/16/13. • Received in the Senate and referred to the Committee on Homeland Security and Governmental Affairs on 4/17/14.	• Committee reported with an amendment in the nature of a substitute on 5/06/2014. Report No. 113-157. • Passed/agreed to in Senate: Passed Senate with an amendment by Unanimous Consent on 9/18/2014. (text: CR S5864-5865) **National Cybersecurity and Communications Integration Center Act of 2014** (S.2519) • Sen. Tom Carper introduced the bill on 6/24/12. • Committee reported on 7/31/14. Report No. 113-240. **Federal Information Security Modernization Act of 2014** (S.2521) • Sen. Tom Carper introduced the on 06/24/2014. • Committee reported without amendment. Report No. 113-256. on 9/15/14. • Placed on Senate Legislative Calendar under General Orders. Calendar No. 564 on 9/15/14.
Homeland Security	**National Cybersecurity and Critical Infrastructure Protection Act of 2014 (H.R.3696)** • Rep. Mike McCaul introduced the bill on 12/11/13. • Reported (Amended) by the Committee on Homeland Security on 7/23/14. H. Rept. 113-550, Part I. • Passed House by voice vote on 7/28/14.(text: CR H6909-6915) **Critical Infrastructure Research and Development Advancement Act of 2014** (H.R.2952) • Rep. Patrick Meehan introduced the bill on 08/01/13. • Reported (Amended) by the Committee on Homeland Security on 1/9/14. H. Rept. 113-324. • Passed/agreed to in House: On motion to suspend the rules and pass the bill, as amended Agreed to by voice vote.7/28/14. (text: CR H6922-6923) • Received in the Senate and Read twice and referred to the Committee on Homeland Security and Governmental Affairs on 7/29/14. **Homeland Security Cybersecurity Boots-on-the-Ground Act** (H.R.3107) • Rep. Yvette Clarke introduced the bill on 9/17/2013 • Reported (Amended) by the Committee on Homeland Security on 12/12/13. H. Rept. 113-294. • Passed/agreed to in House: On motion to suspend the rules and pass the bill, as amended Agreed to by recorded vote (2/3 required): 395 - 8 (Roll no. 457) on 7/28/14. (text: CR H6925-6926) • Received in the Senate and Read twice and referred to the Committee on Homeland Security and Governmental Affairs on 7/29/14.	

K&L GATES

Michael J. O'Neil

Partner

Washington, D.C.
T 202.661.6226
F 202.778.9100
mike.oneil@klgates.com

OVERVIEW

Mr. O'Neil's practice focuses on international trade, cyber security, information technology, privacy and federal policy. He advises foreign and domestic clients on both regulatory and legislative solutions. His counsels U.S. and foreign parties on investment in the U.S., and assists a range of U.S. clients on critical infrastructure protection, privacy, trade compliance, and Congressional investigations. His work also includes counselling clients who must deal with cyber intrusions, data theft and remediation measures.

Mr. O'Neil also serves as the North American Director of the Trilateral Commission. He heads up the Trilateral office, meets regularly with Trilateral members in North America, Europe and Pacific Asia, and helps coordinate Trilateral studies. Mr. O'Neil has had a distinguished public service career in defense and intelligence matters and has served in positions in the Central Intelligence Agency, the Department of Defense and the U.S. House of Representatives.

Immediately prior to joining the firm, Mr. O'Neil served as the general counsel of the Central Intelligence Agency. In this position he was responsible for the conduct of all legal affairs of the Agency. He also served as the chief of staff of the Agency where he coordinated the legislative and public affairs strategy and acted as the Agency's liaison to the National Security Council and Intelligence Community agencies.

In 1995, Mr. O'Neil served as the counselor to the secretary and deputy secretary of defense. In this position he advised the secretary and deputy secretary on policy, organizational and legislative matters. From 1989 to 1994, he served as the counsel to the Speaker of the U.S. House of Representatives, Thomas S. Foley (D-WA). In addition to advising the speaker on all legal and national security issues, he acted as liaison to foreign embassies and U.S. national security agencies. Before his work for the speaker, Mr. O'Neil served as the chief counsel to the House Permanent Select Committee on Intelligence from 1977 to 1989.

Mr. O'Neil is the recipient of the Distinguished Intelligence Medal, the highest honor awarded by the Central Intelligence Agency, and a member of the Council on Foreign Relations.

ALERTS AND PUBLICATIONS

- "Congressional Investigations 101: What You Need to Know," *Public Policy and Law Alert,* January 17, 2008
- "Did You Expect Less Scrutiny – Dubai Ports World, Congress Broadens Review of Foreign Investment," *Legal Times,* September 17, 2007

Michael J. O'Neil (continued)

ADMISSIONS

- District of Columbia
- Ohio

EDUCATION

LL.M., Georgetown University Law Center, Tax, 1976

M.Sc., London School of Economics and Political Science, 1973

J.D., Georgetown University Law Center, 1971

B.A., College of Holy Cross, 1968