From the IT Department to the GC's Office
The Role of Lawyers Before, During and After a Cyber Event

Presented by
Jon Leibowitz
Antonio Perez-Marques
Joseph Kniaz

November 5, 2015

Davis Polk

CLE PRESENTATION

Responsibility for Mitigation of Cyber Risks is Moving

From the IT Department to:

- The Board Room
- The C-Suite
- The Risk Management Department
- And the General Counsel's Office

Why?

- Significant Commercial / Reputational Risks
- Multiplied and Clarified Legal Risks
- Importance (and Expectations) of Non-IT-level Measures

Cybersecurity Has Become Front Page News

Sample Headlines:

"New OPM data breach numbers leave federal employees anguished, outraged," WASHINGTON POST, Jul. 9, 2015

"Insurance giant Anthem hit by massive data breach," CNN, Feb. 6, 2015

"Target Admits Massive Credit Card Breach; 40 Million Affected," WIRED, Dec. 19, 2013

.

"[R]esources devoted to cyber-based threats will equal or even eclipse the resources devoted to non-cyber based terrorist threats." – Testimony of FBI Director James. B. Comey before Senate Committee on Homeland Security and Governmental Affairs

The Commercial and Reputational Stakes Have Become Clear and Are Significant

- Loss of Business
- Loss of Executives (Ashley Madison, Target, Sony, OPM)
- Loss of Intellectual Property
- Costs of Investigation and Remediation
- Embarrassment
- Employee Morale

Former Target CEO Gregg Steinhafl

Former Sony Pictures Co-Chair Amy Pascal

The Legal Risks Have Come Into Focus

Regulatory	Broadening Universe of Interested and Increasingly Prescriptive Regulators FTC Only → FTC, SEC, FCC, CFTC, White House, NIST, Congress, Banking Agencies, State AGs, Others
Civil Litigation	Consumers Shareholders (Derivative) Shareholders (Securities) Employee Bank Actions
Disclosure Obligations	Ex Ante – SEC After a Breach – ~47 overlapping state and federal breach disclosure laws, differing by type and location of information
Privacy Law Constraints on Monitoring & Remediation	State law restrictions on surveillance of employees Tort claims Overseas restrictions are even more onerous

Paradox of Prevention

A sense of inevitability as to the eventuality of a breach…

- E.g. Comey: There are two types of companies, those that know that they've been hacked by the Chinese, and those that have been hacked but don't know it yet
- 67% of victims are notified of breach externally (e.g. FBI, Secret Service)
- Median # of days to detection: 229

… but increasingly clear expectations as to best practices.

Results in (e.g.):

- Legislative proposals for safe harbors
- *Possibility* of non-adversarial relationship with regulators
- Premium on ability to establish reasonable care
- Focus on "benchmarks" of care (e.g., NIST)
- Non-technical measures as disproportionate driver of legal risk?

Importance is Not Proportional to Degree of Difficulty

Many of the most common and effective attack methods call for an employee-level, not IT, defense:

- Phishing / Spear-Phishing
- Thumb Drives
- Lost Laptops
- Company Data -> 3rd Party Sites (Gmail, Dropbox)

Expectation is not of foolproof prevention, but of reasonable care.

Categories of Bad Actors

	Motives	Objectives	Selected Examples
Traditional / Criminal Hackers	Profit	Identity Theft Data Ransom Unauthorized Transfers MNPI	Nasdaq Global Payments Inc. Marketwired L.P. Business Wire JetBlue 7-Eleven
"Hacktivists"	Political, Social	Embarrassment Public Attention	Ashley Madison NSA?
Nation States	Geopolitical, Commercial Cyberwarfare	Espionage / Intellgience Theft of IP Benefit Domestic Business / SOEs Disruption / Retaliation	OPM (China) Westinghouse, U.S. Steel, Alcoa et al. (China) Sony (North Korea) Sands Casino (Iran)
Terrorist	Various	Disruption Physical Damage	
Insiders	Various	Various	NSA (Snowden)

Illustrative Categories of Information at Risk

Industry	Selected Information at Risk
Retail	Credit Card Information (PCI)
Financial Institutions	Customer Information Deal Information MNPI Market Infrastructure
All Employers	Employee Data (SSN, Health Information (PHI))
Utilities / Heavy Industry	Industrial Controls
Tech / Most Industries	Intellectual Property / Trade Secrets
Law Firms / Accountants	Deal Information, MNPI
Health Care / Pharma	PHI / Intellectual Property

Regulatory Action

- State and federal agencies have become increasingly aggressive cybersecurity enforcers
- Not all agencies should automatically be seen as adversarial
  - Criminal and national security agencies are more likely to view a company that has been hacked as a victim
  - DOJ, FBI DHS, the Secret Service and others might want to work with a company that has been breached to track down the hackers, rather than investigate the company itself
  - But companies should be careful of waiving attorney-client privilege when sharing information with the government, even with a “friendly” agency
- Many other agencies will pursue enforcement against companies that have been the victim of cyber attacks
  - That said, some agencies, like the FTC, will close investigations of even major breaches when companies have sound data security in place. Law enforcement should recognize that even best in class data security can’t stop every hacker

Regulatory Action

- Numerous federal agencies have published non-binding data security guidance with technical and non-technical advice
- Agency guidance provides critical insight into regulators' expectations for companies
- Implementing non-technical security measures extracted from regulatory guidance has several important benefits
  - Reduce the chances of a successful cyberattack
  - Improve company's response to an attack
  - Help to build a record of "reasonable" cybersecurity practices for a regulator or a court

Regulatory Action

EXAMPLES OF RECENT GUIDANCE

Agency guidance includes:

- FTC:
  - "Start with Security: A Guide for Business" (June 2015)
- SEC:
  - Investment Management Cybersecurity Guidance (April 2015)
  - Office of Compliance Inspections and Examinations ("OCIE") Risk Alert (2014 and 2015) and Examination Sweep Summary (2015)
- CFTC
  - CFTC Staff Advisory No. 14-21
- FINRA:
  - "Report on Cybersecurity Practices" (February 2015)
- DOJ:
  - Cybersecurity Unit's "Best Practices for Victim Response and Reporting of Cyber Incidents" (April 2015)
- NIST:
  - "Framework for Improving Critical Infrastructure Cybersecurity" (2014)

Regulatory Action

FEDERAL TRADE COMMISSION

- The FTC has historically been the country's foremost data security enforcer
- The FTC has brought over 50 enforcement actions against companies in a variety of industries, including tech, telecom and hospitality
- To bring data breach cases, the FTC has typically relied on its "UDAP" authority under Section 5 of the FTC Act, which prohibits "unfair or deceptive acts or practices"
- The FTC has advanced two legal theories to bring actions against companies hit by a data breach
  - Theory #1: The company made inaccurate or misleading statements to consumers regarding its data security, constituting a "deceptive" act or practice (*E.g.*, Snapchat, Fandango)
  - Theory #2: The company failed to implement reasonable data security measures to protect consumers' personal information, constituting an "unfair" act or practice (*E.g.*, Twitter)

Regulatory Action

FEDERAL TRADE COMMISSION (CONT.)

- Recent test of unfairness theory: *FTC v. Wyndham Worldwide Corp*.
  - The FTC sued Wyndham after hackers gained access to the personal information of Wyndham hotel customers three separate times
  - The FTC alleged that Wyndham's cybersecurity practices "unreasonably and unnecessarily exposed consumers' personal data to unauthorized access and theft"
  - Wyndham's allegedly unreasonable practices included:
    - Allowing use of easily guessed passwords to access electronic data systems
    - Failing to adequately restrict access of third-party vendors
    - Failing to follow proper incident response procedures
  - The Third Circuit rejected Wyndham's arguments on its motion to dismiss
    - Unreasonable cybersecurity practices do not fall outside plain meaning of "unfair"
    - Congress has not excluded cybersecurity from the FTC's unfairness authority

Regulatory Action

SECURITIES AND EXCHANGE COMMISSION

Cybersecurity "is an area where we have not brought a significant number of cases yet, but is high on our radar screen"

—Director of SEC's Chicago Regional Office

Potential Theories

- Ex Ante Disclosure (All Issuers) – expectation of robust and company-specific disclosure of cyber risks.
- Post-Breach Disclosure (All Issuers) – see Corp Fin Guidance; e.g. Target
- Compliance with Regulation S-P (Broker Dealers or Investment Advisers) (e.g., RT Jones)

Civil Litigation

CATEGORIES

Plaintiff Group	Example
Consumers	Target, Ashley Madison, Home Depot, Heartland Payment Systems
Issuing Banks	Target, Home Depot, Heartland Payment Systems
Employees	Sony
Shareholders (Derivative)	Home Depot, Wyndham, Target
Shareholders (Securities)	Heartland Payment Systems

Civil Litigation

CATEGORIES (CONT.)

Company	Consumer Suit	Bank Suit	Shareholder	Employees
Target	X	X	X	
Sony				X
Home Depot	X	X	X	
Ashley Madison	X			
Wyndham			X	
Heartland	X	X	X	
Neiman Marcus	X			
Adobe	X			

Civil Litigation

SONY PICTURES CLASS ACTION

- Background
  - In late November and December 2014, the systems of Sony Pictures were hacked and 38 million files were posted on file-sharing websites on the Internet
  - This included not only unreleased movies and the embarrassing emails of Sony Pictures executives, but also sensitive employee information such as Social Security numbers, salary and bank account information, and medical information
  - Employees filed seven class actions that were ultimately consolidated
  - FBI stated that the North Korean government was behind the attacks
- Claims in employee class action included:
  - Negligence
  - Violation of California state law protecting medical information (state HIPAA statute)
  - Violation of Californian unfair trade practices law (i.e., “mini FTC Act”)
  - Violation of California, Virginia and Colorado state data breach notification laws

Civil Litigation

SONY PICTURES CLASS ACTION (CONT.)

- Standing
  - Sony argued on its motion to dismiss that plaintiffs lacked standing because they failed to allege a current injury or a threatened injury that is "certainly impending."
  - Clapper v. Amnesty International USA:
    - The Supreme Court held that, for the purposes of establishing Article III standing, a plaintiff must show that it has suffered "injury in fact," and that a threatened injury must be "certainly impending" to satisfy this requirement
    - The Court rejected Sony's standing arguments, finding that plaintiffs adequately alleged injury based on public posting of PII and threats of physical injury made to individual employees
- Merits
  - The court held that plaintiffs adequately plead claims for negligence, violation of California's unfair trade practices law, and violation of California's Confidentiality of Medical Information Act
- Key Takeaway: Breadth of information stolen (including social security numbers and sensitive health information) was critical to the court's decision
  - Might have been a different result had it been a "credit cards only" case

Civil Litigation

TARGET DATA BREACH

- Background
  - In late 2013, hackers obtained the financial information of up to 40 million of Target's customers
  - The hackers placed malware on Target's point-of-sale terminals that recorded card data as credit or debit cards were swiped
  - Class action suits were brought by consumers and financial institutions
  - Shareholders brought derivative suits as well
- Financial Institutions Class Action
  - The financial institutions class consists of issuer banks that issued the credit cards accessed in the breach
  - Unlike consumer and employee class actions, standing and damages were uncontested
    - Issuer banks clearly damaged because they paid to reissue compromised credit cards and reimburse customers from fraudulent charges
  - Class survived a motion to dismiss and prevailed on a motion for class certification
  - Target reached $67 million settlement with issuers of Visa brand cards but claims of other issuers remain outstanding

Civil Litigation

TARGET DATA BREACH (CONT.)

- Shareholder Derivative Action
  - Shareholders brought derivative actions against Target's directors and officers, claiming that they had breached their fiduciary duties and wasted corporate assets by failing to take adequate steps to prevent the data breach and by failing to provide customers with adequate information in the wake of the breach
  - Target's Special Litigation Committee's investigation is ongoing

Privacy Law Constraints

- Network monitoring and information sharing for cybersecurity purposes could give rise to civil liability
  - Electronic Communications Privacy Act
  - State privacy statutes and common law torts
  - "Deceptive" consumer-facing policies
- Overcoming liability risks has been a major focus of recent cybersecurity legislation discussions
  - "With carefully crafted liability protections, private entities would finally be able to share cyber threat indicators with their private sector counterparts without fear of liability." – Rep. John Ratcliffe (R-Texas) on the Protecting Cyber Networks Act
- Recent proposed legislation might resolve this concern
  - Protecting Cyber Networks Act
  - Cybersecurity Information Sharing Act

Role of Lawyers in Mitigating Risk

STEPS *BEFORE* A BREACH

1. **Monitor and assist in implementation of regulatory guidance**
   - Many of regulators' suggestions are non-technical and easily understood by lawyers
   - Tech team should implement security measures consistent with regulators' expectations
2. **Develop and implement robust and up-to-date written policies and procedures on data security**
   - The SEC's enforcement action against RT Jones alleged that the investment adviser failed to devise any written policies and procedures to safeguard its customers' personal information
3. **Review vendor and employment agreements**
   - Company's vendors should be required to employ industry-standard cybersecurity practices and to cooperate in the event of a breach
   - Obtain consent to monitor electronic communications on the company's network to avoid liability under privacy laws

Role of Lawyers in Mitigating Risk

STEPS *BEFORE* A BREACH (CONT.)

4. **Help to develop and rehearse a written Incident Response Plan**
   - This plan should, among other things:
     - Assign responsibilities for certain functions to a specific group (legal, technical, PR, etc.)
     - Provide for escalation guidelines and emergency contact information for key personnel
     - Explain how to preserve data in a forensically sound way
   - Plan should be practiced through regularly conducted exercises
5. **Draft appropriate risk disclosures**
   - *See* 2011 Division of Corporate Finance Guidance on Cybersecurity Disclosures
6. **Identify potential state law breach disclosure obligations <u>in advance</u>**
7. **Engage the board in overseeing cyber risks**
   - SEC and FFIEC have emphasized importance of the board's involvement
   - Active board participation critical to defending against breach of fiduciary duty claims
8. **Develop point of contact in law enforcement**
   - DOJ recommends a point of contact through FBI's cyber task forces

Role of Lawyers in Mitigating Risk

STEPS *BEFORE* A BREACH (CONT.)

9. Facilitate retention of an outside vendor to assess the company's current cybersecurity measures

- A third party can help benchmark against similar institutions
- Consider retaining a consultant through outside counsel to shield the report from discovery
  - Under the *Kovel* doctrine, cybersecurity reports prepared by consultants engaged though counsel might be privileged
  - *Kovel* will not apply if the consultant does not assist in the provision of legal advice, but is actually hired to perform some other business function
  - *Kovel* has been found to apply to cybersecurity reviews
    - In *Genesco, Inc. v. Visa U.S.A., Inc.*, private plaintiffs sought the records created by a cybersecurity consultant retained by counsel after a data breach
    - The Middle District of Tennessee held that the materials were protected by attorney-client privilege

Role of Lawyers in Mitigating Risk

STEPS *DURING* AND *AFTER* A BREACH

1. **Make appropriate disclosures under state data breach laws**
   - Breach disclosure laws in the U.S. are currently a patchwork of state laws
     - 47 states and the District of Columbia have enacted data breach notification laws
     - In some instances these impose different or even contradictory obligations
   - Common Themes
     - Definition of "Personal Information"
     - Risk of Harm Analysis
     - Private Cause of Action
     - Safe Harbor
     - Delay for Law Enforcement Action
   - Congress is currently considering various federal data breach disclosure bills
     - If enacted, this legislation would replace the numerous state laws with a single disclosure standard
2. **Make ongoing disclosures under federal securities laws**
   - Includes disclosures regarding scope of the breach, financial consequences, and remediation efforts

Role of Lawyers in Mitigating Risk

STEPS *DURING* AND *AFTER* A BREACH (CONT.)

3. Consider affirmatively contacting key government agencies

- Law enforcement/national security contacts: DOJ, FBI, DHS or U.S. Secret Service
- Principal State Attorney General
- FTC
- SEC

4. Cooperate with requests from "friendly" agencies

- *Practice Point*: Consider implications for attorney client privilege
- Some materials the government requests could be privileged
- Ordinarily, disclosure of privileged materials to a third party will waive the privilege
- A majority of Circuits have rejected the "selective waiver" doctrine
  - Selective waiver would permit waiver to a government or regulatory agency without waiving the privilege as to third parties
  - Disclosure of privileged materials to a non-adversarial government agency should be done only after serious consideration of the potential legal implications

Role of Lawyers in Mitigating Risk

STEPS *DURING* AND *AFTER* A BREACH (CONT.)

5. **Participate in or lead breach response team**
   - Lawyers can coordinate multiple corporate functions involved in responding to the breach
   - Might be privilege benefits to an attorney leading the post-beach remediation and investigation efforts
6. **Represent the company in civil litigation or enforcement agency proceedings**
7. **Provide advice on public messaging**
   - Must understand facts before making disclosures to the press that could turn out to be inaccurate/premature
   - Repeated updates can exacerbate reputational harm to the company

Jon Leibowitz

PARTNER

Washington DC Office
202 962 7050 tel
202 962 7097 fax

New York Office
212 450 4991 tel
212 701 5991 fax

jon.leibowitz@davispolk.com

Mr. Leibowitz is a partner in Davis Polk's Washington DC and New York offices. His practice focuses on the complex antitrust aspects of mergers and acquisitions, as well as government and private antitrust investigations and litigation. He also provides counsel in the developing area of privacy law and with respect to advocacy involving Congress.

Mr. Leibowitz was Chairman of the Federal Trade Commission from 2009 through 2013, and was noted for his bipartisanship. He served as a Commissioner from 2004 to 2009. While at the FTC, his priorities included health care and high-tech competition.

WORK HIGHLIGHTS

- While at the FTC:
  - Presided over a major revision of the Horizontal Merger Guidelines in collaboration with the Antitrust Division of the Department of Justice
  - In the international sphere, headed multiple delegations of American government officials to international conferences on antitrust and privacy matters, including China and EU
- During his term as Chairman, the FTC:
  - Won notable Supreme Court victories involving an allegedly anticompetitive hospital merger and so-called "Pay for Delay" pharmaceutical arrangements
  - Focused attention on the impact of patent assertion entity (PAE) activities on innovation and competition and the implications for antitrust enforcement and policy
  - Played a leading role in the FTC's efforts to protect the privacy of consumers, including dozens of spam and spyware cases and high profile settlements with leading technology companies
  - Led the FTC's efforts to police single firm conduct, achieving settlements with high-tech firms

RECOGNITION

Jon Leibowitz (cont.)

PARTNER

- *National Law Journal* – "Antitrust and M&A Trailblazer," 2015
- *Washington Business Journal* – "Greater Washington Legal Champion," 2014
- *Benchmark Litigation* – Washington DC "Litigation Star"
- Member of Davis Polk's Antitrust Group, which was named "Law Firm of the Year" in Antitrust Law by *U.S. News - Best Lawyers Best Law Firms 2013* and a "Competition Group of the Year" by *Law360 2014*

OF NOTE

- Co-author of amicus briefs before the U.S. Supreme Court on issues ranging from gun control to the census

CURRENT MEMBERSHIPS

- Co-Chair, 21st Century Privacy Coalition (a group of telecom companies and broadband providers seeking uniform federal privacy policies)
- Member, Advisory Board, Reputation.com

PROFESSIONAL HISTORY

- Partner, Davis Polk, 2013-present
- Chairman, Federal Trade Commission, 2009-2013
- Commissioner, Federal Trade Commission, 2004-2009
- Vice President, Congressional Affairs, The Motion Picture Association of America, 2000-2004
- Chief Counsel and Staff Director, U.S. Senate Antitrust Subcommittee, 1997-2000
- Chief Counsel and Staff Director, Senate Subcommittee on Terrorism and Technology, 1995-1996
- Chief Counsel and Staff Director, Senate Subcommittee on Juvenile Justice, 1991-1994
- Chief Counsel, Senator Herb Kohl, 1989-2000
- Counsel, U.S. Senator Paul Simon 1986-1987
- Attorney, private practice, 1984-1986

Jon Leibowitz (cont.)

PARTNER

ADMISSIONS

- District of Columbia
- State of New York

EDUCATION

- B.A., American History, University of Wisconsin - Madison, 1980
  - Phi Beta Kappa
- J.D., New York University School of Law, 1984

Antonio J. Perez-Marques

PARTNER

New York Office
212 450 4559 tel
212 701 5559 fax
antonio.perez@davispolk.com

Mr. Perez-Marques is a partner in Davis Polk's Litigation Department, focusing on complex commercial litigation, including securities and M&A-related litigation and securities enforcement. He also has extensive experience advising Spanish, Latin American and other foreign clients concerning U.S. litigation matters, and domestic clients concerning overseas and cross-border disputes.

WORK HIGHLIGHTS

Selected Recent and Current Representations

- The Brazilian state-owned electric utility in federal securities class action litigation based on allegations of corruption arising from the Brazilian *Lavo Jato* investigation
- DBRS, Inc., a nationally recognized statistical rating organization, in connection with a recently settled enforcement action brought by the U.S. Securities and Exchange Commission (SEC) related to surveillance of RMBS ratings
- Standard & Poor's Ratings Services, in connection with investigations, examinations and enforcement actions brought by the SEC and state attorneys general
- Morgan Stanley in federal litigation, through trial preparation, related to a $9 billion structured investment vehicle (SIV) backed in part by subprime mortgage-backed securities, including the defeat of class certification and grant of partial summary judgment
- Morgan Stanley, in various state and federal litigations related to residential mortgage-backed securities
- Enel S.p.A. and Enelpower S.p.A. in U.S. litigation to enforce an alleged €433 million judgment of an Albanian court related to an agreement to develop a hydroelectric plant in Albania
- Special committee of SWS Group in shareholder class action litigation challenging its acquisition by Hilltop Holdings

Antonio J. Perez-Marques (cont.)

PARTNER

- The Solomon R. Guggenheim Foundation in litigation by descendants of Peggy Guggenheim challenging the management of the Peggy Guggenheim Collection in Venice
- Comcast Corporation in shareholder class action litigation challenging its announced acquisition of Time Warner Cable
- Guy Carpenter (a Marsh & McLennan Company) in litigation related to the no-hire provision of a non-disclosure agreement signed in contemplation of an M&A transaction
- Royalty Pharma in litigation related to hostile takeover bid for Elan Corporation plc
- A European oil and gas company in U.S. litigation related to expropriation of South American subsidiary
- Comcast Corporation in parallel state court and FCC proceedings through trial against the National Football League
- Fortune 100 corporation in criminal bribery investigations, through the acquittal at federal jury trial of two former executives, with no charges against or settlement by the company

FCPA Practice

- Fortune Global 100 corporation in pending SEC investigation
- Advised on the design and implementation of comprehensive FCPA compliance program for clients, including Siemens AG
- Led investigations, post-closing due diligence and other FCPA compliance reviews in Argentina, Brazil, Colombia, Costa Rica, the Dominican Republic, Ecuador, Germany, Guatemala, Mexico, South Africa and Switzerland
- Delivered FCPA training in English and Spanish to clients in the United States, Europe, Asia and South America

PRO BONO

- Argued and won Fourth Amendment search case before the New York Court of Appeals
- Successful and ongoing representations of political asylum seekers and veterans claiming benefits

RECOGNITION

- Member of Davis Polk's Securities Litigation Group, which was named:

Antonio J. Perez-Marques (cont.)

PARTNER

- *Chambers USA* – Securities Litigation, Band 1
- *The American Lawyer* – "Securities Litigation Department of the Year" finalist, 2014
- *Law360* – "Securities Group of the Year," 2013

PROFESSIONAL HISTORY

- Partner, 2011-present
- Associate, 2002-2011

ADMISSIONS

- State of New York
- U.S. Court of Appeals, Second Circuit
- U.S. District Court, S.D. New York

EDUCATION

- A.B., Princeton University, 1999
  - *magna cum laude*
- J.D., New York University School of Law, 2002
  - *cum laude*
  - Allen Scholar

Joseph Kniaz

ASSOCIATE

Washington DC Office
202 962 7036 tel
202 962 7119 fax
joseph.kniaz@davispolk.com

Mr. Kniaz is an associate in Davis Polk's Litigation Department.

PROFESSIONAL HISTORY

- Davis Polk since 2011

ADMISSIONS

- District of Columbia
- State of New York

EDUCATION

- B.A., History, University of Michigan, 2008
  - with highest distinction
  - with highest honors
- J.D., University of Virginia School of Law, 2011
  - Order of the Coif
  - Editorial Board, *Virginia Law Review*