Cybersecurity and Legal Issues

PULLMAN &COMLEY LLC
ATTORNEYS

Pulling Together. Succeeding Together.

Steven J. Bonafonte

AMWA Water Policy Conference

PULLMAN &COMLEY LLC
ATTORNEYS

CURRENT LEGAL LANDSCAPE

Cybersecurity vs. Privacy

PULLMAN &COMLEY LLC
ATTORNEYS

- Privacy Law is different than Cybersecurity Law. This is important to realize, even though both operate in conjunction with each other.

- Privacy law typically deals with how an entity collects and uses personally identifiable information (PII) and also the transparency behind consent to use an marketing.

- Some “Privacy” laws, however, have security components that trigger a duty to protect the information using “reasonable” means or other technologies.

Cybersecurity vs. Privacy

PULLMAN &COMLEY LLC
ATTORNEYS

- Data Breach Reporting Statutes – (States) and those Federal rules that govern certain types of protected information (e.g., HIPAA – Health Information) may have both Privacy and Security components.

- Generally, encryption is a good mechanism to provide safe harbor and avoid triggering data breach reporting.

- Establishing robust policies and procedures for the protection of sensitive information – and more importantly, following these procedures – is essential to the legal defense of any organization experiencing a data security incident.

Cybersecurity: Federal
Bush Administration Efforts

PULLMAN &COMLEY LLC
ATTORNEYS

On January 8, 2008, President Bush issued National Security Presidential Directive 54 – Homeland Security Presidential Directive 23 concerning Cybersecurity Policy.

Unfortunately, President Bush's directive was classified "Top Secret." Thus, it was not until 2010 that his successor revealed that those directives were comprised of a dozen initiatives, including:

- Consolidating external access points to federal systems;
- Cybersecurity education and awareness; and,
- Mitigating risks to the global supply chain for information technology.

Cybersecurity: Federal
Obama Administration Efforts

PULLMAN &COMLEY LLC
ATTORNEYS

Executive Order 13636, Improving Critical Infrastructure Cybersecurity and Presidential Policy Directive 21, which:

- Requires information sharing and collaboration between the public and private sectors,
- Mandates the development of a process for identifying and protecting critical infrastructure,
- Requires regulatory agencies to assess and address risks, and, perhaps most significantly to today's topic,
- Requires NIST to lead in developing cybersecurity standards and best practices for protecting critical infrastructure.

Fun NIST Facts:

PULLMAN &COMLEY LLC
ATTORNEYS

The National Institute of Standards and Technology ("NIST")

- Established by Congress in 1901 -- with a budget of $40,000 – and known as the National Bureau of Standards until 1988.
- NIST has been responsible for developing national standards for everything from anti-freeze to radio weather broadcasting.
- NIST's Boulder, CO facility houses the atomic clock which is source of our nation's official time.

NIST Cybersecurity & Privacy

PULLMAN &COMLEY LLC
ATTORNEYS

- On February 12, 2014, NIST released its first version of its Framework for Improving Critical Infrastructure Cybersecurity as ordered by the President in his Executive Order (13636)

- The President's executive order charged NIST with creating a "voluntary Cybersecurity Framework that provides a 'prioritized, flexible, repeatable, performance-based, and cost-effective approach' for assisting organizations responsible for critical infrastructure services to manage cybersecurity risk."

NIST….

PULLMAN &COMLEY LLC
ATTORNEYS

- This Framework provides a reference to Critical Infrastructure operators to follow – and also references third party standards as benchmark guidance (e.g., ISO 27000, NIST SP 800)

- Specifically acknowledges critical infrastructure sectors, e.g., Water and Dams

NIST Standards…

PULLMAN &COMLEY LLC
ATTORNEYS

- The Framework is intended to be used by entities to review and assess not only core systems (networks, ERM, and operations systems) but also Industrial Control Systems (ICS) such as SCADA.

- Regulatory Agencies will be required to review whether they can/should issue regulations that will require organizations to implement the Framework.

NIST….

PULLMAN &COMLEY LLC
ATTORNEYS

Immediate Advice:

Critical Infrastructure Entities should become very familiar with the NIST Framework and strongly consider conducting a full review of cybersecurity practices against the NIST risk assessment modules

Consider engaging third party cybersecurity consultants for security testing via legal counsel to create additional protections (Attorney/Client Communication and Attorney Work-Product) to shield against exposure in potential litigation or regulatory actions.

State Regulation

PULLMAN &COMLEY LLC
ATTORNEYS

- State regulators also have expressed an interest in adopting the Framework as part of their regulatory mandates. No federal pre-emption exists in cybersecurity regulation.

- The Connecticut utility regulator (PURA), for example, recently released a 31-page report on Cybersecurity and public utilities and issued (this year) a RFP for cybersecurity consultant services in anticipation of issuing regulations and/or audits of utility self-assessments.

State Regulation (an example)

PULLMAN &COMLEY LLC
ATTORNEYS

- PURA held an informational cybersecurity docket on 3/18/15 (last week) where they took informal testimony and comments from the PURA regulated entities in attendance

- One entity commented that the municipal utilities (not subject to PURA) had equal cybersecurity risks – if not greater – and should be subject to some statutory oversight in this space.

- PURA appears to be concentrating on certain best practices as promulgated by the Center for Internet Security as the foundation for their regulation and examination vs. the principles-based NIST framework.

Follow-ons to regulations

PULLMAN &COMLEY LLC
ATTORNEYS

- While the Executive Order and proposed state self-assessment programs tend to describe their respective frameworks as “voluntary” programs, observers believe that it will evolve to a regulatory requirement and/or will be tied to various “incentives” as described by the White House.

- Proposed Incentives include: Rate Recovery for Price-Regulated Industries; Liability Limitation and Federal Grant Funding.

Data Breach: Probably more a question of "when," and not "if."

PULLMAN &COMLEY LLC
ATTORNEYS

Ponemon–IBM 2014 Cost of Data Breach Study:

The probability of a material data breach over the next 2 years involving 10,000 records or more is nearly 19 percent.

This likelihood varies by industry.

- For public sector organizations, the probability is 23.8%.
- For energy and utility companies, the probability is 7.5 percent.

Consequences and Frequency

PULLMAN &COMLEY LLC
ATTORNEYS

- Data breaches are on the increase in frequency, size and severity.
- Breach can happen in seconds, but take months to discover.
- The average cost to a company from a data breach has increased to $5.9 million -- on average, that's more than $200 per record.
- The cost per record varies by industry – Healthcare is $326/ record.
- Data loss or exfiltration from malicious attacks costs approximately $246 per record on average.
- Companies report that they are losing more customers (abnormal churn) following a data breach.

Breach Response Plan

PULLMAN &COMLEY LLC
ATTORNEYS

- What role does your counsel have in your organization's breach response plan (or one at all)?
- What is your mechanism for continuous monitoring (Detection)?
- What is your mechanism for response?
- To what level have you drilled with your legal and communications staff regarding how you will deal with public impact?
- Do you have an awareness of your contractual obligations – and more importantly – the contractual obligations of your suppliers/ vendors should a cybersecurity incident take place?

Response…

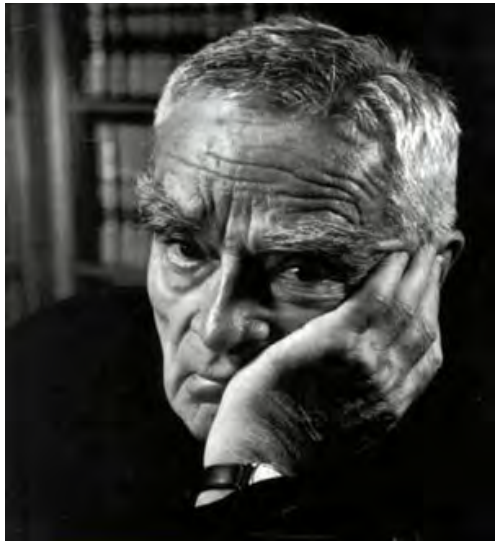
PULLMAN &COMLEY LLC
ATTORNEYS

- HIPAA, GLB (some), California State Data Breach Laws….
- Who OWNS the response when there is a Data Breach?
- Who is on your team? Who is not? Who should be?
- What is the best way to defend you after you failed to prevent a data loss? (Oops or circle the wagons)
- CAUSE(s): Human error? Lack of compliance? Lack of preventative investment in technology?
- Important to engage quickly and with team of specialists that deal with these issues – litigation is increasing and plaintiff's lawyers are becoming very creative at getting past hurdles of damages

Analyzing Cybersecurity Breaches as Torts

PULLMAN &COMLEY LLC
ATTORNEYS

Lessons learned from Judge Learned Hand and tugboats and barges that break loose in the middle of the night:



Where something goes wrong and, God forbid, there is no clearly defined standard of care governing the situation, some Judge will create one.

The "calculus of negligence."

PULLMAN &COMLEY LLC
ATTORNEYS

In re Eastern Transportation Co. (T. J. Hooper), 60 F.2d 737 (2d Cir.), cert. den., 287 U.S. 662 (1932).

United States, et al., vs. Carroll Towing Co., et al., 159 F.2d 169 (2d Cir. 1947).

Two otherwise forgettable cases – one about a tugboat that went down without a radio and the other about the sinking of an unmanned barge loaded with flour in New York harbor -- that are now famous for Judge Hand's articulation of the cost-benefit analysis for determining negligence and assigning liability, expressed algebraically as whether $B \geq PL$ or $B < PL$.

The Discretion of the Court in Evaluating Risk vs. Utility

PULLMAN &COMLEY LLC
ATTORNEYS

- The “Hand Formula” balances the burden and cost of taking adequate precautions against magnitude and gravity of the potential loss multiplied by the probability of the occurrence of such loss.
- In the absence of clearly articulated “best practices” Judge Hand’s risk vs. utility framework has been offered as a means of determining liability for companies suffering from less than optimum cybersecurity.
- It is an appealing formula, however, each of its components is subjectively determined – affording great discretion to judges and leaving room for a great deal of uncertainty and a wide range of outcomes.

Contractual and Legal Liability

PULLMAN &COMLEY LLC
ATTORNEYS

- So, what is the "Standard of Care" in order to protect against a negligence case in cybersecurity matters?

- This is a moving target – and the NIST Framework may ultimately create a floor for minimum diligence and "duty of care" of critical infrastructure operators (despite disclaiming use as such)

- For example, if a compnany had a critical cyber event which caused interruption in service such that there was resulting harm and damages to its customers, BI litigation may ensue.

Legal Liability….

PULLMAN &COMLEY LLC
ATTORNEYS

- Would certain defenses that might afford the utility with immunity from suit/liability apply in such a case?

- The law is evolving – and the plaintiff's bar is paying a great deal of attention in how to craft claims (class actions or large tort business interruption claims) against utilities that fail to take appropriate measures to avoid service interruption.

- One of the proposed potential benefits of adopting and integrating the NIST Framework into core operations may be that it provides utilities with additional protections (safe harbor) from liability to third parties resulting from a cyber event.

Legal Liability…

PULLMAN &COMLEY LLC
ATTORNEYS

- For publicly traded utilities, derivative shareholder suits are also a possibility.

- These suits may allege breach of fiduciary duty and gross mismanagement (among other things) in that officers and directors failed to exercise their requisite standard of care.

- Failing to meet cybersecurity industry standards could rise to the level of this breach of duty.

Class Actions and Fiduciary Duties

PULLMAN &COMLEY LLC
ATTORNEYS

- It remains too early to tell how effective these class actions will be at shaping law and policy in this area.
- One recent case filed against the executives with Wyndham Hotels following 3 separate attacks by Russian-based hackers alleged these theories -- *Palkon v. Holmes*, Case No. 2-14-cv-01234-SRC (D.N.J.) -- but it was dismissed recently by the court.
- However, *Kulla v. Steinhafel*, Case No. 0-14-cv-00203-SRN (D. Minn.) a shareholder derivative action filed against Target Corporation executives following that company's infamous data breach is still winding its way through the court.

(You may recognize the name [Gregg] Steinhafel as that of the 35-year "lifer" and former CEO of Target Corporation, who stepped down within months of that company's infamous data breach.)

Contact Information

Steven J. Bonafonte

Pullman & Comley, LLC
90 State House Square
Hartford, CT 06103

Tel: 860.424.4333

sbonafonte@pullcom.com

PULLMAN &COMLEY LLC

ATTORNEYS

Pulling Together. Succeeding Together.