BakerHostetler

BRAEMAR ADJUSTING

Physical Damage from Cyber Attacks on Energy Facilities

October 9, 2014

BakerHostetler

BakerHostetler Privacy & Data Protection

Jerry Ferguson, Esq.
Co-Leader Privacy & Data Protection Team
New York, New York
Tel. 212.589.4238
gferguson@bakerlaw.com

Twitter @JerryFergusonNY

Blog: www.dataprivacymonitor.com

BakerHostetler

Overview & Goals

- What are the threats?
- What are the potential consequences?
- What are the potential legal and regulatory liabilities?
- What are the best practices for risk management and liability limitation?
- How is the insurance market resonding?

BakerHostetler

Where are the threats?

- Inside threats
  - Employee negligence
    - Security failures
  - Employee ignorance
    - Lack of education and awareness
  - Malicious employees

Where are the threats? (cont.)

- Outside threats
  - Malicious Hackers
    - Malware
    - Phishing and Spear Phishing
  - Thieves (including Social Engineering Tools)
  - Vendors

BakerHostetler

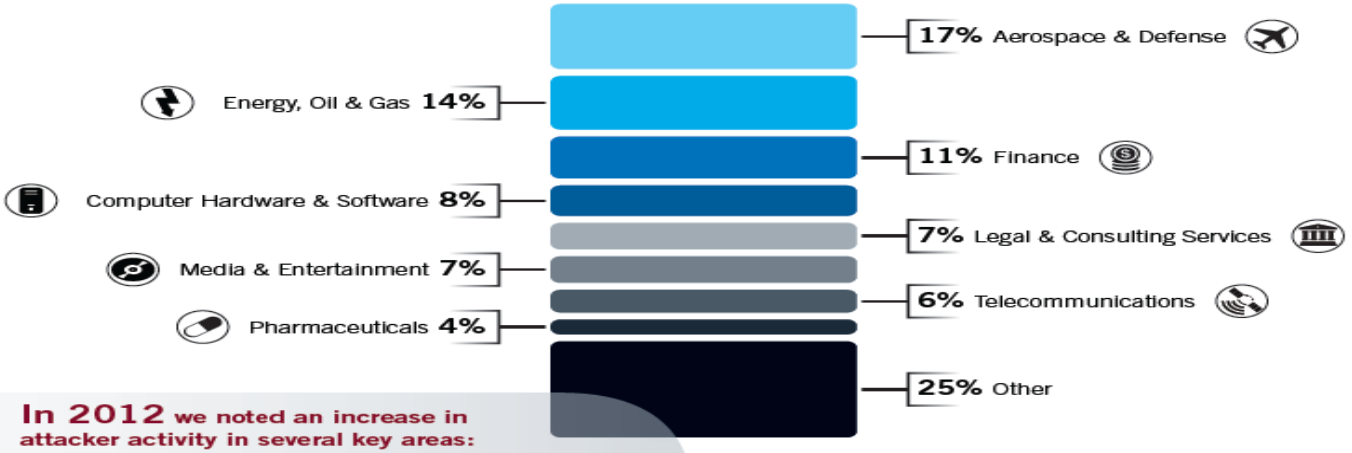
Breaches by Industry

Trustwave 2013 Global Security Report

BakerHostetler

VICTIMS BY THE NUMBERS

Industries Being Targeted by Advanced Attackers



In 2012 we noted an increase in attacker activity in several key areas:

- Media & Entertainment — up from 2% to 7%
- Pharmaceuticals — up from 1% to 4%
- Finance — up from 7% to 11 %

How Compromises Are Being Detected

37%

of victims discovered the breach internally

63%

of victims were notified by an external entity

BakerHostetler

Energy Industry Vulnerbility

- 2014 Allianz "Risk Barometer" Survey identifies cyber risk as 8th most significant global business risk – 1st time in top 10
- DHS reports that 106 of 200 incidents responded to in past 2 years by ICS –CERT were directed at energy industry
- UK estimates that UK energy industry is losing GBP400 million/year from cyber attacks

BakerHostetler

Cyber Vandalism

- Project Pandora
  - Test Performed March 2007
  - Simulated cyber attack by Idaho National Laboratory / Department of Homeland Security
  - Method: Rewrote a 27 ton generator's computer code to try to destroy it
  - **It worked** – Generator began smoking and shaking and then stopped.
- Stuxnet
  - Computer worm allegedly designed by US and Israel
  - Reported to destroy Iran's nuclear centrifuges by causing them to spin too quickly
  - Security experts report that variants are now spreading on Internet

BakerHostetler

Cyber Theft

- Economically Motivated
  - "Advanced Persistent Threat"
  - "The greatest transfer of wealth in history" – General Alexander, U.S. Cyber Command
  - Mandiant Report, February 2013
    - Identifies "secret division" of Chinese military targeting trade secrets of Western companies
    - 140 companies affected worldwide
- Politically Motivated
  - Anonymous
  - Wikileaks
  - Environmental activists

BakerHostetler

Energy Industry Threats

- 2011: China-based hackers targeted international oil and energy companies in cyberattacks dubbed "night dragon."

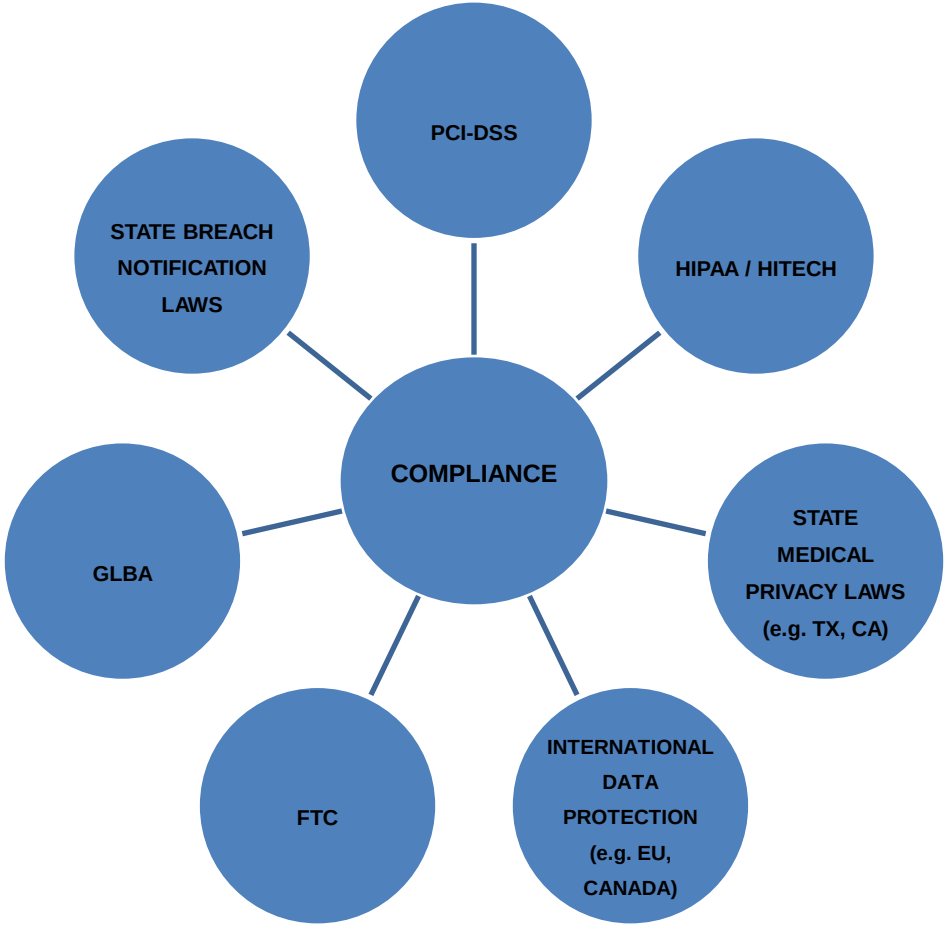
- 2012: cyber hackers tried to halt all oil production in Saudi Arabia by attacking the operations of Aramco; breach damaged 30,000 computers

- June 2014: More than 1,000 organisations have been infected by malware known as 'Energetic Bear', said to be operated by a state-backed group with ties to Russia

- August 2014: Massive cyber attack on oil and energy industry in Norway

BakerHostetler

Compliance Complexity



BakerHostetler

State Laws

- 47 states, D.C., & U.S. territories
- Laws vary between jurisdictions
- Varying levels of enforcement by state attorneys general
- Limited precedent
  - What does “access” mean
  - What is a reasonable notice time

BakerHostetler

State Law Resources

- State-by-State breach notification law comparison

http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/State_Data_Breach_Statute_Form.pdf

- Key Issues in state breach notification laws

http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/Data_Breach_Charts.pdf

BakerHostetler

HIPAA / HITECH

("Acquisition" "Access" "Use" Trigger w/ Risk of Harm)

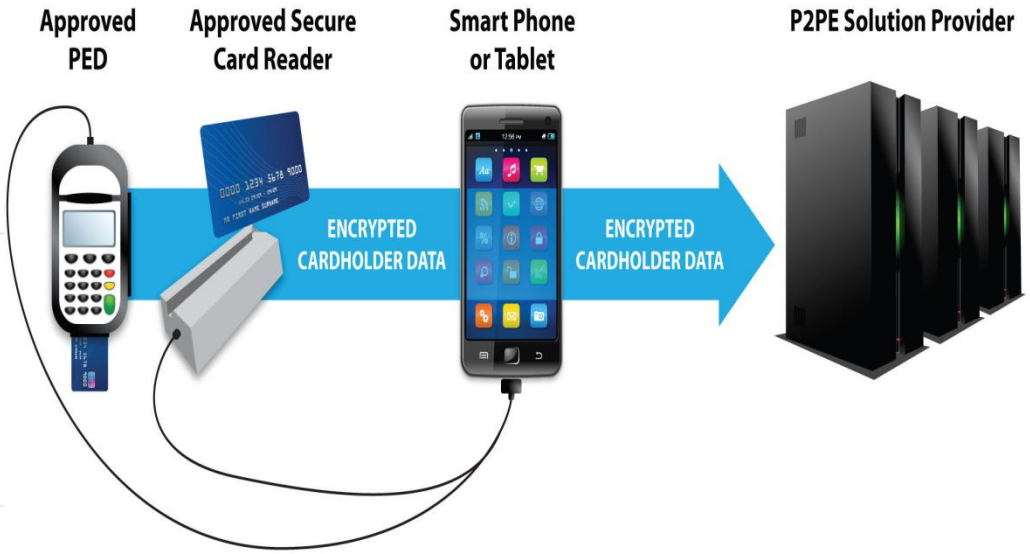
- **HIPAA Privacy Regulations (45 CFR §164): Breach by a Covered Entity**

- **Applies To:** A health plan, health care clearinghouse and health care provider who transmits any health information in electronic form in connection with a covered transaction.
- **Information Covered:** Unsecured protected health information – individually identifiable health information that is transmitted or maintained in electronic media or any other form or media.
- **Definition of Breach:** The acquisition, access, use, or disclosure of PHI in a manner not permitted by the HIPAA Privacy Rule, which compromises the security or privacy of the PHI. Until Omnibus Final Rule, "compromise" meant "poses a significant risk of financial, reputational, or other harm to a patient as documented in a risk assessment.
- **Who Must Be Notified:** The patient or their personal representative, HHS and the media if more than 500 residents of a state or jurisdiction are affected.
- **Notification Timeframe**: Without unreasonable delay and in no case later than sixty (60) calendar days after the breach is discovered.
- **Preemption**: More stringent state laws are not preempted

Gramm-Leach-Bliley and Breach Notification Regulations

- Interagency Guidelines, authorized under GLBA 501(b), impose certain breach notification requirements on financial institutions
- Investigation
  - Must promptly investigate when alerted to unauthorized access to customer information
- Notification
  - Notification to Federal regulator of unauthorized access or other criminal activity
  - Notification to customers required when determined that misuse of a customer's information has occurred or is reasonably possible
  - Notification must occur “as soon as possible”
  - If unable to determine which specific customers possibly affected, must notify relevant group(s) of customers

Payment Card Industry ("PCI")



BakerHostetler

NERC/FERC Cyber & Grid Security Standards

- The North American Electric Reliability Corporation (NERC) is an international, non-profit corporation charged with ensuring the reliability of "bulk power systems" in the United States.

- The "Critical Infrastructure Protection" or CIP standards issued by NERC and approved by the Federal Energy Regulatory Commission (FERC) deal with the physical and cyber security of bulk power operators:
    - CIP-001: Sabotage Reporting
    - CIP-002: Critical Cyber Asset Identification
    - CIP-003: Security Management Controls
    - CIP-004: Personnel & Training
    - CIP-005: Electronic Security Perimeters
    - CIP-006: Physical Security of Critical Cyber Assets
    - CIP-007: Systems Security Management
    - CIP-008: Incident Reporting and Response Planning
    - CIP-009: Recovery Plans for Critical Cyber Assets

- These standards are mandatory and enforceable by NERC

BakerHostetler

NERC/FERC Enforcement

Identities of Violators Withheld by NERC, Penalties are public:

- April 30, 2013: $40,000 fine (CIP-007)
- March 27, 2013: $120,000 fine (CIP-004, CIP-005, CIP-006, CIP-007)
- February 28, 2013: $151,000 fine (CIP-005, CIP-006, CIP-007)
- January 31, 2013: $150,000 fine (CIP-005, CIP-006, CIP-007)

BakerHostetler

SEC Guidance on Cyber-Security Disclosure Obligations

- SEC Guidelines
  - Issued October 13, 2011
  - Suggests that publicly traded companies:
    - Disclose incidents of cyber intrusions in SEC filings
    - Disclose "risk factors" of cyber intrusions
  - SEC has issued letters requesting certain high-profile cyber intrusions be disclosed
    - Amazon's Zappos.com breach
    - Google
  - October 2014 disclosure of loss of customer mailing information by JP Morgan Chase

Cyber Risk Information Sharing

- Cyber Security Executive Order
  - NIST Framework
  - NIST Roadmap
- Department of Defense Contractors Information Sharing Program
- Federal Legislation?

BakerHostetler

International

- Mandatory notification
  - Germany
  - Mexico
- “Voluntary” notification
  - UK
- Sector Specific notification
- Pending EU Regulations
- http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/International-Compendium-of-Data-Privacy-Laws.pdf

What Do Regulators Expect?

- Transparency
- Prompt and thorough investigation
- Good attitude & cooperation Appropriate and prompt notification
- Corrective action Remediation and mitigation

Regulators Expectations (cont.)

- Cyber Security Risk Assessment
- Adaptive Risk Management Plan
- Senior Management Direction of Cyber Risk Strategy
- Vendor Management

BakerHostetler

Litigation Risks

- Personal injury and property damage
- Inability to discharge contractual obligations
- Business interruption experienced by third parties

BakerHostetler

Decisions, Decisions, Decisions

- Does the event trigger notification obligations?
- Do you involve law enforcement?
- Do you hire a forensics company?
- Do you retain counsel?
- Do you involve regulatory agencies?
- Is crisis management necessary?

Best Practices

- Prepare and practice a response plan
- Respond quickly
- Bring in the right team
- Preserve evidence
- Contain & remediate
- Let the forensics drive the decision-making
- Work with Law enforcement, if necessary, but don't lose control of response

Best Practices (continued)

- Document your analysis, but preserve the attorney client privilege
- Involve the C-suite
- Plan for likely reaction of customers, employees, & key stakeholders
- Be guarded, consistent, and honest in communications
- Mitigate harm

Coverage for Cyber Attacks?

- Common Exclusions
  - Institute Cyber Attack Exclusion Clause CL380
  - Terrorism Form LMA3030 Exclusion 9
  - Electronic Data Exclusion NMA 2914
- Enforceable?
  - Fire following doctrine
  - Proximate causation issues

BakerHostetler

"Traditional" Cyber Insurance

- Coverage
  - Incident response cost
  - Business Interruption
  - Third party claims
  - Restoration of data and/or software
- Excluded
  - Physical damage from cyber events
  - War and Terrorism risks

BakerHostetler

Filling the Cyber Gap

- 2014: London Market Innovations
- Underwriting Challenges
  - Lack of Loss History
  - Potentially Catastrophic Loss
- Creative Solutions
  - Risk assessments
  - Service offerings
- Help from the US Government?

BakerHostetler

Questions?

Jerry Ferguson

Tel. 212.589.4238

gferguson@bakerlaw.com

Twitter @JerryFergusonNY