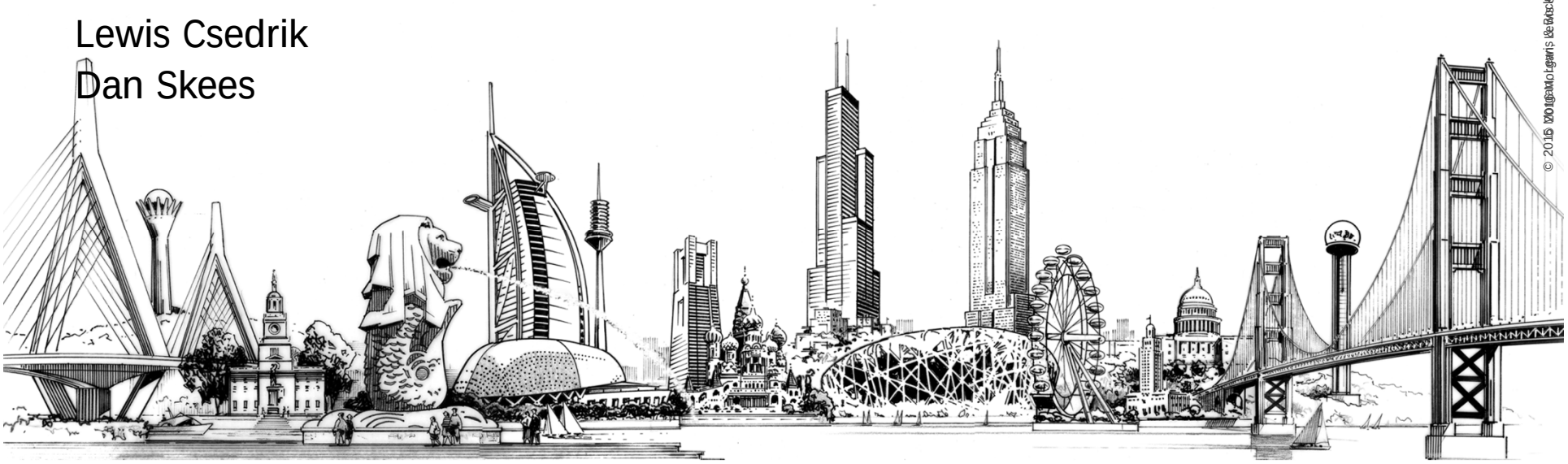
Morgan Lewis

CYBERSECURITY AND CRISIS MANAGEMENT FOR THE ENERGY INDUSTRY

October 12, 2017

Matthew Miner
Paul Bessette
Lewis Csedrik
Dan Skees



Before we begin...

- If you are experiencing technical difficulties, please contact WebEx Tech Support at +1.866.779.3239.
- The Q&A tab is located near the bottom right hand side of your screen; choose “All Panelists” before clicking “Send.”
- We will mention a code at some point during the presentation for attendees who requested CLE. Please make note of that code, and insert it in the pop-up survey that will appear in a new browser tab after you exit out of this webinar. You will receive a Certificate of Attendance from our CLE team in approximately 30 to 45 days.
- The audio will remain quiet until we begin at 1:00 pm ET.
- This event uses the Audio Broadcasting feature. You will hear sound through your computer speakers/headphones automatically. Make sure your speakers are ON and UNMUTED.
- If you would prefer to access the audio for today’s presentation by telephone, please click the “phone” icon below your name on the Participants Panel for teleconference information.

Agenda

- The Dimensions of a Crisis
- Advance Planning
- Crisis Communications
- Management and Strategic Resolution
- Lessons Learned

What Is a Crisis?

What Is A Crisis?

Three categories:

1. An emergency or catastrophic event like an unexpected indictment or data breach.
2. An evolving issue that may culminate in highly visible exposure.

    A. Often starts with a government investigation or internal whistleblower allegation.

3. A crisis that may be avoided through foresight and early internal action or litigation containment.

Despite Best Intentions, Crises Happen to Good Companies

- Common Threads of Crisis Scenarios
  - High public visibility
  - Communications challenges
  - Complex legal, regulatory, business and technical issues
  - Urgency to understand complex facts
  - Immediate demands for answers and solutions
  - Multiple agency investigations
  - Overlapping litigation

Crises Occur Often Within the Energy Sector

- **Sniper Attack on Calif. Power Station Raises Terrorism Fears** (NPR, Feb. 5, 2014)
- **U.S. Power Grid Vulnerable to Attack: Congressional Research Service** (Bloomberg BNA, July 8, 2014)
- **Cyberattacks Raise Alarm for U.S. Power Grid** (Wall Street Journal, Dec. 30, 2016)
- **Malware Reportedly Used in the December 2016 Ukrainian Power System Attack** (Electricity Information Sharing and Analysis Center, Aug. 2, 2017)

Crises Occur Often Within the Energy Sector

- Nuclear Safety
  - Crises caused by natural disasters- Fukushima Daiichi
  - Radioactive waste management – leak at Carlsbad (intersection of environmental and safety concerns)
- Environmental Issues
  - Aliso Canyon/Porter Ranch Gas leak
  - 2014 coal ash spill at Dan River OR *Deepwater Horizon* Oil Spill
- Industrial/Workplace Safety
  - Safety lapses resulting in employee injury or death
  - OSHA investigations
- Terrorism/Cybersecurity/Physical Security
  - Grid vulnerability to foreign and domestic cyberattacks – Attack on Ukrainian power grid, Aurora vulnerability
  - State-sponsored hacking - attack on Bowman Dam in Rye, NY by Iranian nationals associated with the Islamic Revolutionary Guards Corps
  - Security/access breaches - Metcalf Incident

Crises Occur Often Within the Energy Sector

- Consumer/Retail Issues
  - Accusations of price manipulation and fixing
- FCPA Cases Against Energy Companies
  - TX water management, construction, and drilling company found to have made improper payments to African gov't officials to get beneficial regulatory treatment and reduce tax liability
  - Drilling services and project management firm found to have authorized improper payments to a third-party intermediary for gifts and entertainment for Nigerian officials to resolve customs issues
  - International power company found to have used a subsidiary to pay bribes to officials at Mexico's largest power company as well as to pay kickbacks to Iraq to obtain contracts under U.N. program

Crisis Management: Key Objectives

- Minimize the element of surprise
- Mitigate risk and limit liability
- Protect the company's reputation and goodwill
- Don't let the response become the next crisis
- Integrate legal concerns and response with business needs

ADVANCE PLANNING

Crisis Management: Advance Planning

- The first hours of a crisis are chaotic – Don't panic.
- An advance written crisis management plan manages chaos.
- Draft the plan with outside counsel who can act as the legal crisis manager.
- The plan must have instructions for in-house counsel and key team members to follow immediately.

Crisis Management: Advance Planning

- Basic Elements of a Crisis Management Plan
  - Anticipate Potential Areas of Crisis
  - Pre-Plan Immediate Response Steps
    - Identify Crisis Management Team with Designated Roles and Authority
    - Identify Communications Team
      - Consider likely affected constituents

Crisis Management: Advance Planning

- Form and lead an emergency response team as a cohesive unit.
  - Define your team and key roles **in advance**.
  - Provide authority to:
    - direct resources;
    - support any outside crisis manager;
    - control company messages;
    - interface with government responders; and
    - begin evidence collection and preservation

Crisis Management: Advance Planning

- Know your IT structure and backup systems and ensure a knowledgeable resource is on the team.
- Create a single document and research database for use in all related proceedings.
- Manage document review/retention and key personnel interviews, while executive leaders, government authorities and the public are clamoring for instant answers.
- Consider developing one or more privileged crisis-management checklists.
- **PRACTICE in advance!**

Potential Key Players on a Crisis Management Team

- CEO, Relevant Business Unit Leaders
- General Counsel And Relevant In-house Counsel
- Outside Counsel – Potential Crisis Manager
- Corporate Communications
- Outside Communications Consultant
- Investor Relations
- Government Relations
- Board Chair/Board
- Compliance Director
- IT/Record Management
- Building/Facility Security

Unique Challenges for the Nuclear Industry

- There is already heightened Congressional focus on nuclear security
  - *See* July 10, 2017 Letter from Senator Markey to DOD, DOE, FBI, DHS & NRC referencing "profound risks to public safety" posed by cyber-attacks on nuclear plants
- Unique, prompt NRC event reporting requirements will pose challenges to coordinated, measured event response strategies
  - Unlike certain industries that report cyber intrusions weeks or months after such events and fact gathering (if at all), NRC has mandatory reporting requirements—some as early as 1 and 4 hours after detection
  - Reports required for events that caused or "*could have caused*" an adverse impact--the latter is unique to the nuclear industry
  - All reports are recorded and saved for one month in case there is private or public inquiry
- As a result, companies with nuclear facilities must plan for potentially very rapid dissemination of preliminary cyber event information

CRISIS COMMUNICATIONS

Crisis Fast Movers Looking for Immediate "Answers"

- Governmental Actors, including Regulators/Congress/Local Politicians
- Media
- Shareholders
- Customers
- Employees
- The Board
- Consumer Groups
- Community Organizations

Crisis Management: Communications Strategy

- Every crisis management plan must carefully consider and address communications strategy.
  - Requests for information or public comment will come in rapid-fire succession.
  - Requests will come before information is fully known or a legal strategy has been developed.
  - Some crises begin with external reporting or disclosures, putting the company in a “catch up” posture.
  - Communications must be coordinated and only include facts that are demonstrably true.
    - Increased risk of government action.
- Communications to the public may impact legal considerations and strategy.
  - Every press release is fodder for a potential deposition, trial exhibit, or basis for further litigation or investigation.

Crisis Management: Communications Strategy

Five Common Approaches to Communication Strategy in a Crisis Scenario.

1. Full disclosure and immediate acceptance of responsibility
2. Limited disclosure with limited and/or “rolling” acceptance of responsibility
3. Denial (which may be the right answer or look like a “cover up”)
4. Redefine the playing field
   - Articulate a core corporate message that does not admit or deny a particular allegation
5. Say nothing
   - Create a vacuum for others to control the message
   - A holding statement is preferable to saying nothing

Factors Bearing on Choice of Approach

1. Inevitability and timing of ultimate disclosure
2. Proliferation of information/opinion sources and speed of dissemination
3. Whistleblower protections and incentives
4. First Amendment issues in US
5. Multiplicity of potential governmental agencies
6. Exposure to individual claims
7. Effect on insurance coverage
8. Effect on “brand” and stock price

Crisis Management: Communications Strategy

- Enforcement agencies and lawyers know to target the communications and public relations components of a crisis team to gain information, admissions, and a window into legal strategy.
  - Plaintiffs' lawyers have long challenged whether attorney-client privilege should apply to communications between company counsel and outside communications consultants.
    - In house public relations personnel stand in a somewhat different position from properly engaged outside consultants.

Crisis Management: Communications Strategy

- Structure relationship with communications firm to enhance privilege protection.
- Best practices for managing communications risks
  - The crisis management plan should include internal procedures for managing the creation, retention, and content of written communications.
  - The crisis management plan should provide for retention of an outside counsel crisis manager who sets guidelines for communications with third-parties.
  - Discuss legal strategy in person or on the phone in lieu of written communications.
- Even with the best practice in place, assume all communications with, and within, consulting firms would be produced.

MANAGEMENT AND STRATEGIC RESOLUTION

Crisis Management: Coordination

- Formulate a single, unified response and litigation strategy.
  - Quickly learn the facts that are critical to make informed choices and consider impact on likely constituents.
  - Avoid taking inconsistent legal or factual positions in the multiple ongoing proceedings (*i.e.*, one set of facts).
  - Ensure that the approach to any component of the crisis-related proceedings does not impair the company's position in any other ongoing related matters.
- Rigorously control company messaging (media, court, internal) not to impair the company's litigation position or create constituent relations issues.
  - Know the facts you report.

Crisis Management: Coordination

- A crisis will generate a range of different legal/operational risks and reporting obligations that can require multiple parallel workflows.
- Must coordinate investigation and reporting/fact assertion.
  - If different legal teams, employees, or consultants are working on a matter, they may seek to gather facts separately.
  - Separate simultaneous fact investigations can yield inconsistencies in factual findings, preservation and collection of documents, and reporting to government agencies.
  - Separate investigations can also result in needless duplication of tasks.

Crisis Management: Coordination

- Fact investigation must to be coordinated as part of an overall strategic approach to all disclosures to regulators and in litigation.
  - Stakeholders should be called upon to coordinate input on:
    - Document preservation and collection
    - Witness lists
    - Topics for witness interviews
    - Timing of and need for any disclosures
    - Filings and regulatory responses
    - Conclusions to be drawn from investigation
  - Coordination is essential to ensure that all filings and disclosures are consistent on facts and across legal risks.
- **Teamwork and coordination are essential**.

Crisis Management: Investigation & Root Cause Analysis

- **Investigation** in this context must include the identification and analysis of physical and other evidence to determine events that led to the crisis.
- **Root Cause Analysis (RCA)** is the process of identifying those factors that, but for their occurrence, the crisis would have been prevented.
  - Identifying the root cause of a disaster is critical to prevent the disaster from occurring again.

Crisis Management: Preserving Information

- Must preserve key information to ensure that all relevant documents and data will later be available for regulatory disclosures and investigations.
- To protect both the process and company personnel, it is important to define what is potentially relevant and the types of data that need to be preserved.
  - Topics of information for preservation
  - Categories of personnel at issue
  - Types of devices and data for preservation

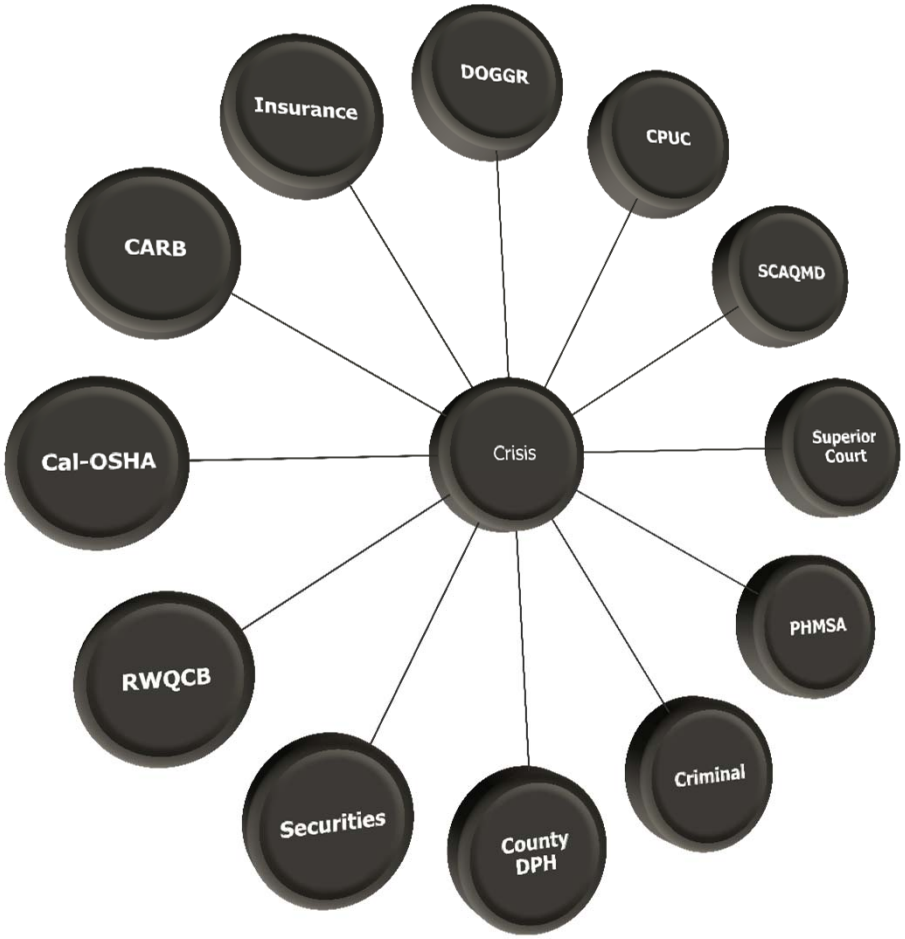
Crisis Management: Preserving Information

- Those working on crisis response need to be informed of their preservation obligations and the risks of failing to preserve that information.
  - If the government identifies documents or data that weren't preserved, it often concludes that information was intentionally destroyed or that the information was relevant.
- Remind personnel of their preservation obligations, especially as it relates to new communications and work-related data on personal devices and laptops.

Crisis Management: Multiple Parallel Matters & Resolution Strategy

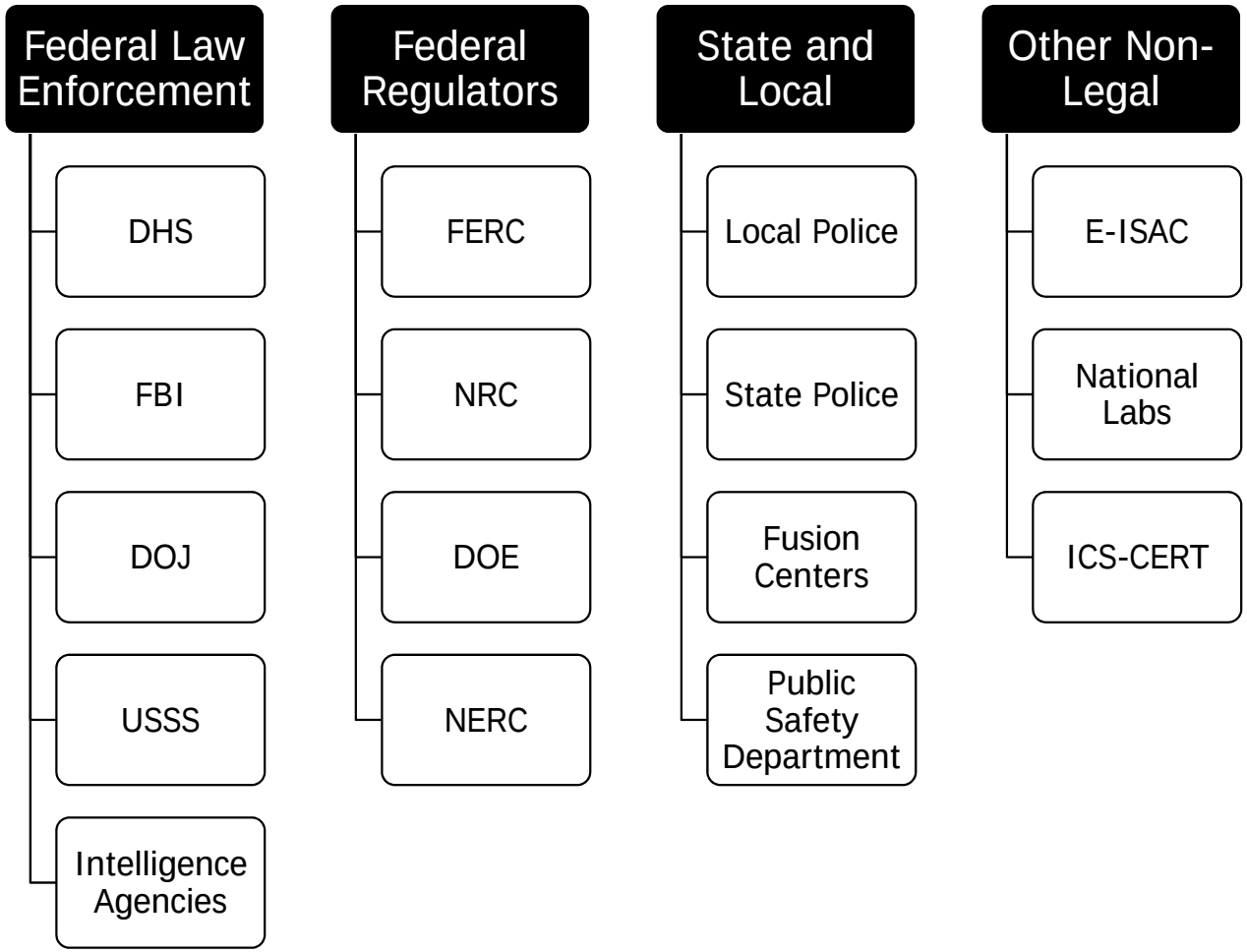
- To strategize effectively, first identify end goals.
- How does each tactical decision move you closer to your goal?
- Remember that overlapping litigations and administrative proceedings are interconnected.
  - Favorable rulings in a small, related case can influence outcomes in big cases.
  - Early unfavorable outcomes may haunt the company throughout the litigation.
  - Admissions in administrative proceedings may bind the company in court.

Overlapping Legal Proceedings & Agency Investigations



- Multiple state and federal agency investigations occurring simultaneously.
- Civil litigation, criminal litigation, insurance coverage issues & securities litigation.
- A unified legal defense and communication strategy is needed to ensure consistent messaging in all proceedings.
- The company must establish an internal system to work with outside counsel to respond.

The Range of Agencies Involved in Responding to Physical or Cyber Attacks on Grid Assets



Crisis Management: Multiple Parallel Matters & Resolution Strategy

- Only after each stage can the company eliminate, try, or settle pieces of the interrelated proceedings.
- Some components may need to be litigated to conclusion; others might be settled.
- Settlements should be negotiated methodically so as not to disadvantage other proceedings.
- This takes time. Government agencies have statutory mandates. They will not talk settlement until all the facts are in. Private plaintiffs follow the governments' lead.
- There will be a time and a place for settlements.

Crisis Management: Multiple Parallel Matters & Resolution Strategy

- Don’t agree to a settlement that doesn’t actually end a case.
- If a settlement does not have a dollar cap, plaintiffs will find a way to increase the claim.
- Lessons learned:
  - Don’t rush to avoid a trial with private plaintiffs in phase one.
  - Focus on the end goal.
  - Make sure to get a dollar cap.

LESSONS LEARNED

Lesson Learned: Media Message Control

- A Lesson in how **NOT** to handle PR in a crisis
  - *Careless* – Don't carelessly point fingers at others
  - *Uncaring* – Make sure message show empathy towards those affected by the crisis
  - Don't fail to communicate the three key messages in any crisis:
    1. That you are **accountable**
    2. That you are deeply **concerned** about the harm caused
    3. That you have a **plan** for what to do

Lesson Learned: Be Wary of Data Requests and Subpoenas

- State and Federal agency strategy:
  - Bury the company in subpoenas and data requests
  - Force errors and admissions – it works.
    - Some companies have pled guilty to criminal “Obstruction of Congress”
    - Some companies have submitted data responses that had not been reviewed by outside counsel – big mistake

Lesson Learned: No Good Deed Goes Unpunished

- The law requires certain mitigation and remediation actions
- But be wary of voluntary mitigation to try to improve the company's image
  - Voluntary reimbursements can come to be viewed as entitlements
  - Little can be done to improve the company's public perception
- For example, some have tried to argue that mitigation expenses should be credited against penalties
- The DOJ may argue "no credit" for things the company is required by law to do, and little or no credit for things the company volunteers to do

Lesson Learned: Managing the Politics of Crisis

- The politics of a post-crisis scenario are remarkably resistant to facts.
  - Conspiracy theories and hysteria proliferate on social media
  - Plaintiffs' lawyers encourage overheated media reporting
  - Politicians respond opportunistically
- This dynamic significantly complicates companies' communication and disclosure planning.

Case Study: Regulators React to a Perceived Threat

- April 16, 2013: Sniper attack on Metcalf Transmission Substation, critically damaging more than a dozen transformers, losing 52,000 gallons of oil
- Early-mid 2014: Series of press articles highlight electric system vulnerability to physical attacks
- March 7, 2014: FERC directs development of reliability standard requiring physical security protections for critical electric system facilities
- May 23, 2014: NERC, industry body responsible for reliability standard development, files proposed standard in record time
- July 17, 2014: FERC issues NOPR proposing to approve new standard
- November 20, 2014: FERC issued Order No. 802 approving new standard
- October 2, 2015: New standard becomes effective, resulting in significant compliance costs for the industry

Lesson Learned: Prepare for the Long Haul

- Control the pace – the crisis will not stay in the headlines forever.
- Something else will seize the media's and politicians' attention soon enough
- Until then, the company's world will be turned upside down. Regulators and politicians will be hostile, and the courts can't be trusted to do the right thing.
- The company must dig in and prepare a trial ready defense, limit damage where it can, and wait for opportunities to move the case forward.

Universal Lessons from Crisis & Litigation

- Lessons learned
  - Plan for a crisis in advance
  - Approaches to post-crisis communications
  - Consistent messaging from legal, business, and operations is key
  - Don't be caught by data requests & subpoenas
  - *What* happened is less important than *why* (Root Cause Analysis)
  - Be wary of voluntary mitigation efforts
  - Identify a reasonable end goal and a strategy to achieve it
  - Ensure all tactical decisions advance the strategy
  - Bad facts=bad press=bad politics=bad law
  - A settlement must actually settle the case
  - There is a new life after a crisis

Life After a Crisis

- In some cases, there can be new life for a company on the other side of a crisis
  - The rigorous internal review can lead to a more efficient and more safety conscious organization
  - New regulations passed after a crisis can bring welcome clarity to an entire industry
  - New technologies can make operations safer

Biography

Matthew S. Miner
Washington, D.C.
T +1.202.739.5987
F +1.202.739.3001

Matthew S. Miner focuses his practice on white collar enforcement and compliance matters, as well as US congressional inquiries and committee investigations. Matt has experience in investigations involving alleged corporate misconduct—including matters related to the FCPA—in jurisdictions on five continents. He regularly represents companies and individuals in grand jury investigations, matters involving the US Department of Justice, Securities and Exchange Commission, and Office of Foreign Assets Control, internal and audit committee investigations, and inquiries by non-governmental entities, such the World Bank.

Biography

Paul M. Bessette
Washington, D.C.
T +1.202.739.5796
F +1.202.739.3001

Paul M. Bessette counsels nuclear utilities, reactor designers, and other nuclear service providers in licensing, regulatory, adjudicatory, and litigation matters. He has litigated more than 10 lawsuits before the US Court of Federal Claims in connection with federal obligations to accept and remove spent nuclear fuel, and supports ongoing settlements of spent fuel claims with the government. He also advises clients on licensing of new-generation nuclear power plants, and counsels nuclear utilities in their applications to renew existing nuclear power plant operating licenses.

Biography

Lewis M. Csedrik
Washington, D.C.
T +1.202.739.5166
F +1.202.739.3001

Lewis M. Csedrik represents clients before the US Nuclear Regulatory Commission (NRC), Department of Energy (DOE), and Department of Labor in whistleblower litigation and government investigations, including investigations into alleged retaliation and regulatory violations. Lewis also performs independent investigations into various types of alleged wrongdoing. He assists clients with assessing and enhancing their work environments and provides training in the area of investigations, complete and accurate reporting, and maintaining and enhancing the Safety Conscious Work Environment and Safety Culture.

Biography

J. Daniel Skees
Washington, D.C.
T +1.202.739.5834
F +1.202.739.3001

J. Daniel Skees represents electric utilities before the Federal Energy Regulatory Commission (FERC) and other agencies on rate, regulatory, and transaction matters. He handles rate and tariff proceedings, electric utility and holding company transactions, reliability standards development and compliance, and FERC rulemaking proceedings. The mandatory electric reliability standards under Section 215 of the Federal Power Act are a major focus of Dan's practice. He advises clients regarding compliance with reliability standards, and helps them participate in the development of new standards.

Our Global Reach

Africa
Asia Pacific
Europe
Latin America
Middle East
North America

Our Locations

Almaty
Astana
Beijing*
Boston
Brussels
Century City
Chicago
Dallas
Dubai
Frankfurt
Hartford
Hong Kong*
Houston
London
Los Angeles
Miami
Moscow
New York
Orange County
Paris
Philadelphia
Pittsburgh
Princeton
San Francisco
Shanghai*
Silicon Valley
Singapore
Tokyo
Washington, DC
Wilmington

Morgan Lewis

*Our Beijing and Shanghai offices operate as representative offices of Morgan, Lewis & Bockius LLP. In Hong Kong, Morgan Lewis operates through Morgan, Lewis & Bockius, which is a separate Hong Kong general partnership registered with The Law Society of Hong Kong as a registered foreign law firm operating in Association with Luk & Partners.

THANK YOU

Morgan, Lewis & Bockius UK LLP is a limited liability partnership registered in England and Wales under number OC378797 and is a law firm authorised and regulated by the Solicitors Regulation Authority. The SRA authorisation number is 615176.

Our Beijing and Shanghai offices operate as representative offices of Morgan, Lewis & Bockius LLP. In Hong Kong, Morgan Lewis operates through Morgan, Lewis & Bockius, which is a separate Hong Kong general partnership registered with The Law Society of Hong Kong as a registered foreign law firm operating in Association with Luk & Partners.