
Morgan Lewis
TECHNOLOGY MAY-RATHON
NAVIGATING CYBERSECURITY CONTROLS IN THE ELECTRIC ENERGY INDUSTRY
J. Daniel Skees
May 9, 2017
© 2017 Morgan, Lewis & Bockius LLP

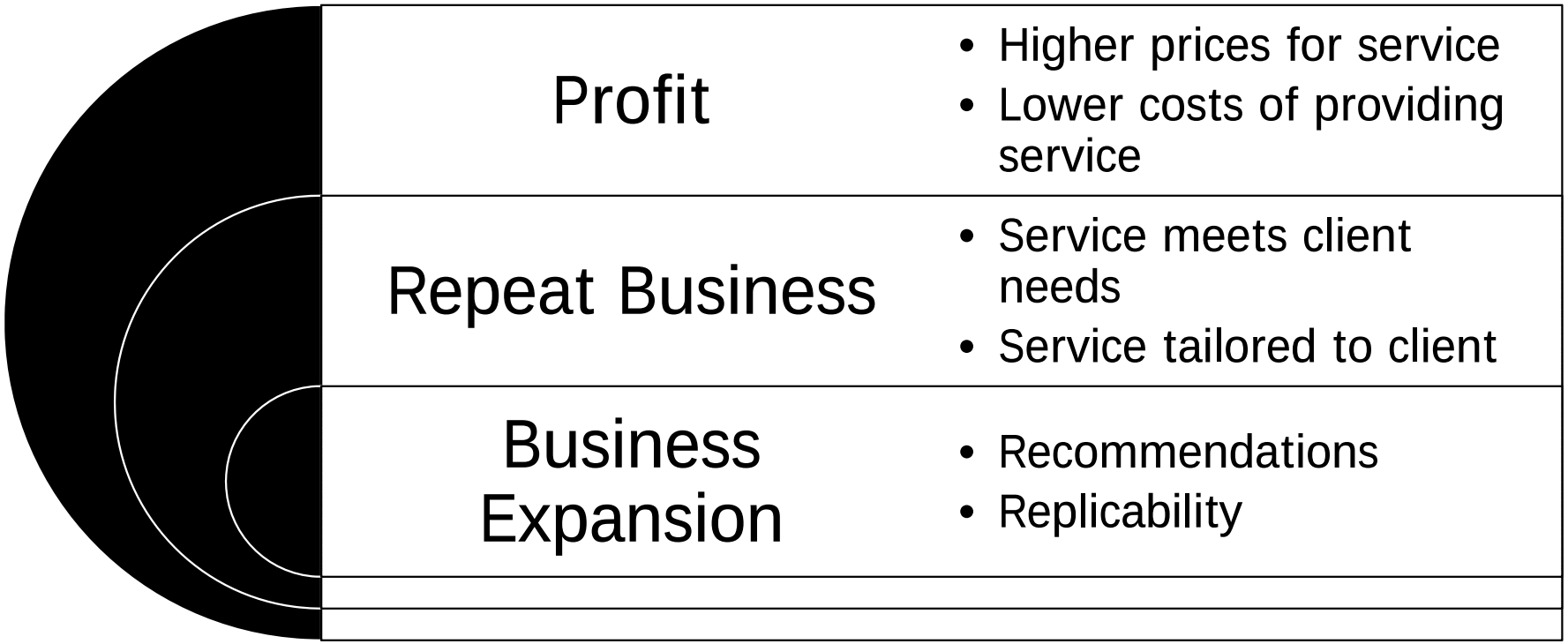
Agenda

- Perspectives of the Contracting Parties
- Cybersecurity Regulatory Reality for Electric Utilities
- Addressing the Concerns of Utility Clients
- Addressing the Concerns of Vendors
- Getting to Yes in a Regulated Environment

SECTION 01

PERSPECTIVES OF THE CONTRACTING PARTIES

Vendor Perspective



Regulated Company Perspective

Cost	Business Needs	Compliance Needs
• Low cost services	• Services that meet established business objective	• Services that avoid fines, compliance costs, and harm to regulatory reputation

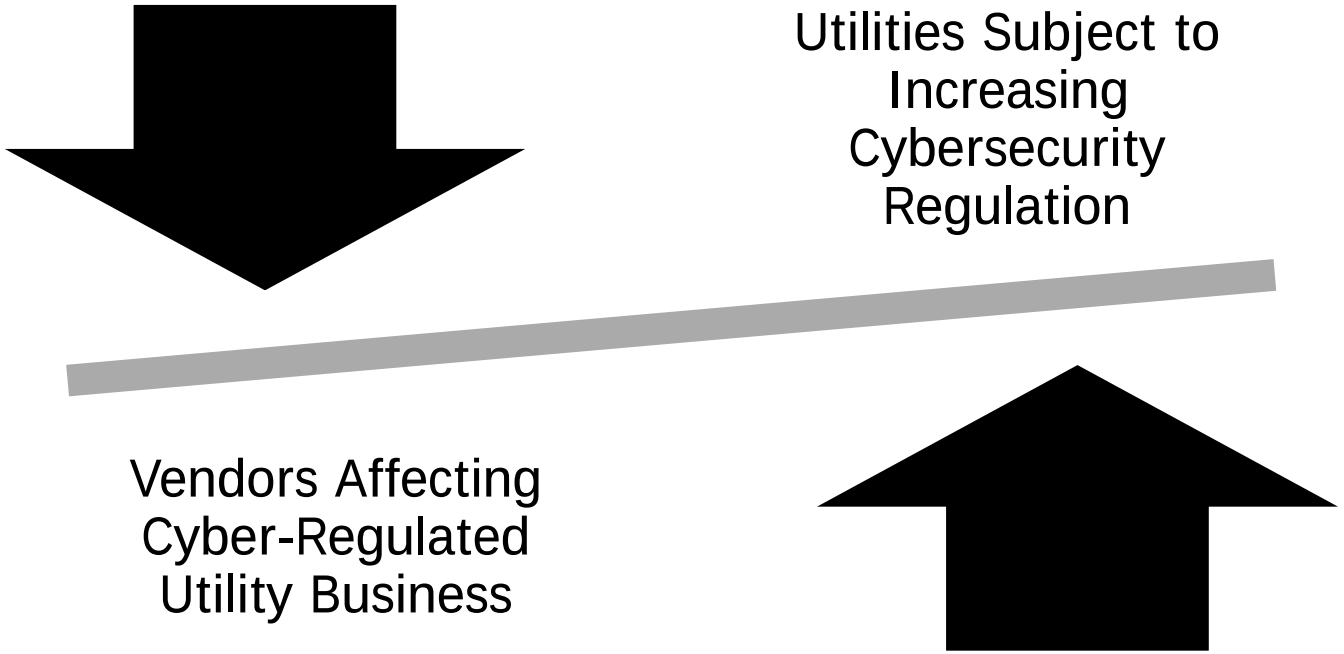
Why the Cyber Threat to Utilities Can Be Different

- Damages are not strictly direct financial harm to the utility corporation
  - August 2003 Northeast Blackout: approximately $6 billion in total economic cost
    - Shut down 70 auto and parts plants, idling 100,000 workers
    - Loss of oil refinery capacity led to localized gasoline shortages
    - Steel plants knocked offline for days
    - Chemical plants knocked offline for up to a week
    - $50 million in lost stock at grocery stores in Michigan
    - New York City suffered $1 billion in economic cost, including $250 million in frozen and perishable food
  - Sewage contamination and resulting public health problems
  - Property losses (accidents, crime)
- Overtime costs for first responders
- Lost tax revenue due to drop in economic activity
- Increased litigation, including insurance recovery issues

What Utilities (and Other Critical Infrastructure Owners) Think About

- **2015**: Hackers infected several substation control systems in Ukraine, causing localized blackouts lasting several hours
  - Considered a "proof of concept" for cyberattacks on substations
- **2010**: Stuxnet virus targets Iranian nuclear program centrifuges
- **2003**: SQL Slammer worm disables certain safety and process systems at nuclear power plant for several hours
- **2001**: Attackers access computer networks at the California ISO for more than two weeks
- **2000**: Disgruntled employee hacked sewage control equipment in Queensland, Australia, causing 800,000 liters of raw sewage to spill
- **1994**: Trojan attack on Salt River Project SCADA system allowed disgruntled customer to control 131-mile canal system for five hours
- **1982**: Trojan attack on SCADA system controlling Siberian pipeline resulted in an explosion equivalent to three kilotons of TNT

Clashing Perspectives in the Electric Utility Business



SECTION 02

CYBERSECURITY REGULATORY REALITY FOR ELECTRIC UTILITIES

The Scope of Cybersecurity Regulation for Electric Utilities (Hint: It's All Regulated)

NIST Cybersecurity Framework	NERC CIP Reliability Standards
Identify	Identifying "BES Cyber Systems" (CIP-002-5.1a)
Protect	Developing Cybersecurity Policies (CIP-003-6)
Detect	Backgrounds Checks, Personnel Access Controls, and Training (CIP-004-6)
Respond	Electronic Access Controls (CIP-005-5)
Recover	Physical Security Controls (CIP-006-6)
	Asset-Specific Cybersecurity Controls (CIP-007-6)
	Incident Response (CIP-008-5); Recovery Planning (CIP-009-6)
	Change Management and Vulnerability Testing (CIP-010-2)
	Information Protection (CIP-011-2)

Example Compliance Requirements Relevant to Vendors (Providing Services)

- Training on required topics prior to access and re-training at least every 15 months
- Background checks every seven years (criminal history at every location lived for at least six months) prior to access
- Removal of physical and remote access upon termination (completed within 24 hours)
- Revocation of user accounts within 30 days of termination
- Logging of all physical entry into protected areas (name, date, and time)
- Continuous escorted access for visitors
- Logging of visitor access (date and time of entry and exit, name, contact name)

Example Compliance Requirements Relevant to Vendors (Providing Equipment)

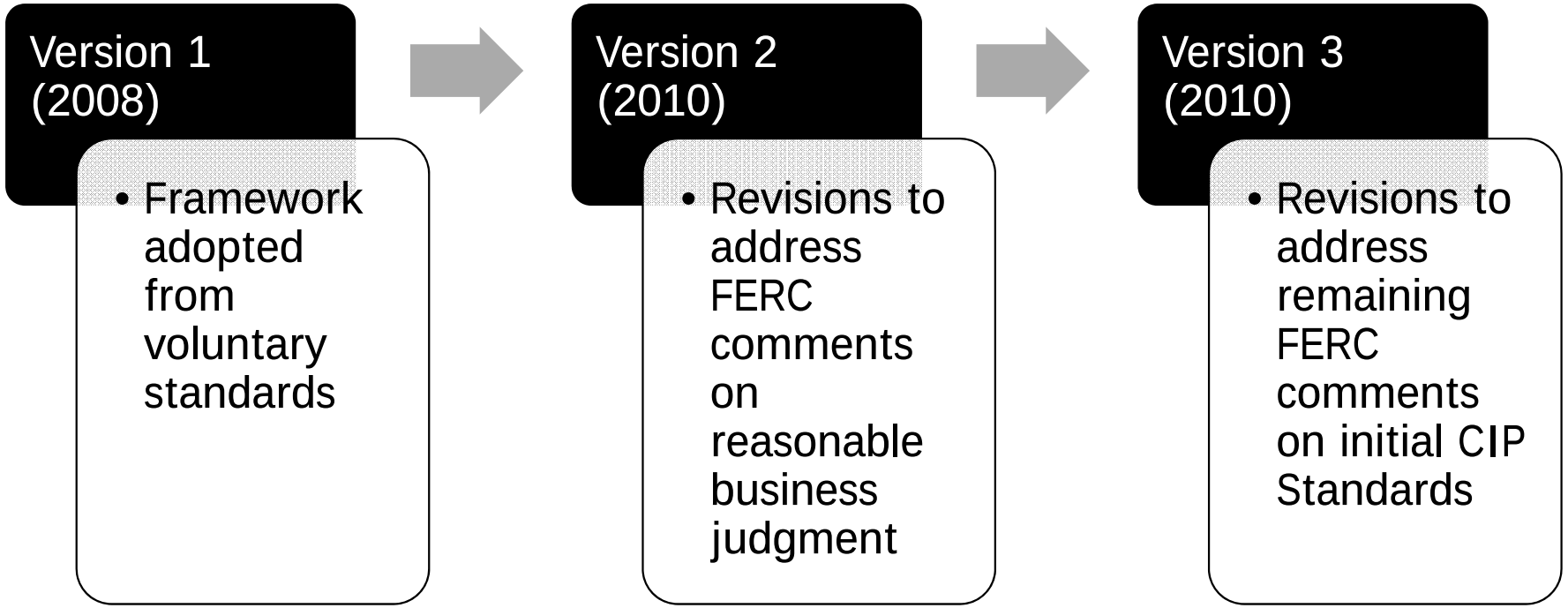
- Patching for security vulnerabilities (and patch testing)
- Logging for security events (successful login, failed login, detected malicious code)
- Alerting for security events (detected malicious code, detected logging failure)
- Password complexity and password changes
- Baseline configuration and updating for OS, firmware, software, ports, and patches

. . . And additional requirements for vendors providing core functionality for energy systems

The Fines and Other Costs Imposed on Electric Utilities

- Statutory maximum is $1 million, per day, per violation, but costs add up in other ways as well
  - Example: Vendor employee is accompanied by untrained assistant when entering protected area, but fails to provide constant monitoring for that assistant for ten minutes
  - Costs for utility:
    - Potential $1m fine (but probably far less)
    - $50-100k mitigation costs (updated training, escort control, compliance processing)
      - Typically ~8 months to resolve report, mitigate, and complete paperwork
      - Mitigation costs can go much higher (see, e.g. NP15-24)
    - Costs from damage caused by unescorted bad actor (direct and indirect)
- Essentially all noncompliance is detected (1188 reported violations in 2016; 87% self-reported)

Cybersecurity Regulation for Utilities Is Constantly Changing



More recent changes . . .

Version 4 (not effective)

- Standardization of Critical Assets subject to protections

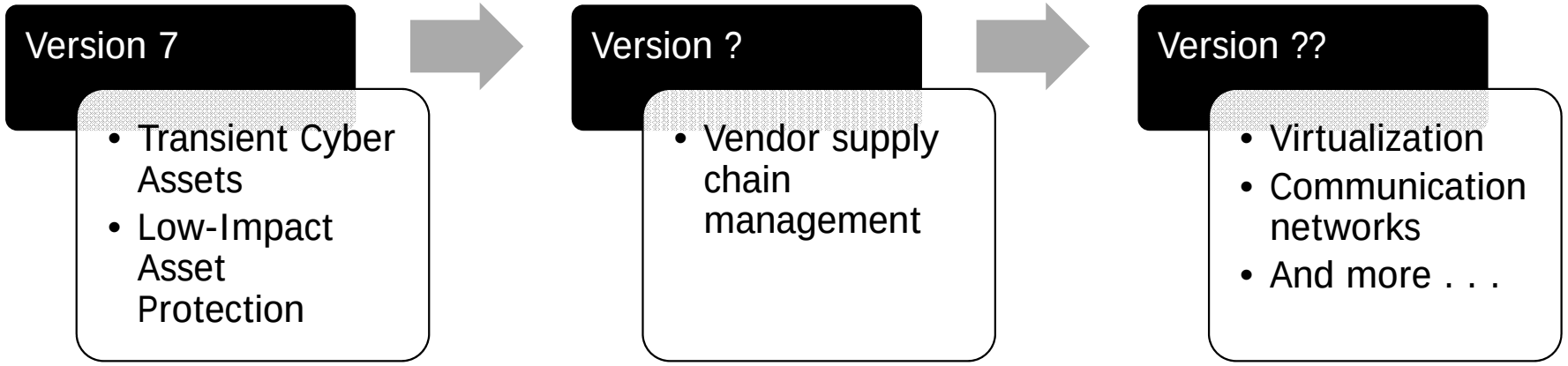
Version 5 (~2016)

- Complete re-write of standards from top-to-bottom

Version 6 (2016)

- Revisions to address FERC comments on "identify, assess, and correct" language

And future changes . . .



SECTION 03

ADDRESSING CONCERNS

Utility Concerns & Vendor Solutions

Vendor Noncompliance Will Be Expensive

- Can the vendor be compliant?
- Will the vendor cooperate in our compliance programs and take them seriously?
- Will the vendor share the cost of noncompliance?

Vendor Noncompliance Will Harm Others

- Does the vendor have strong security practices?
- Can the vendor cover the cost of damage it causes?
- Do our stakeholders trust this vendor?

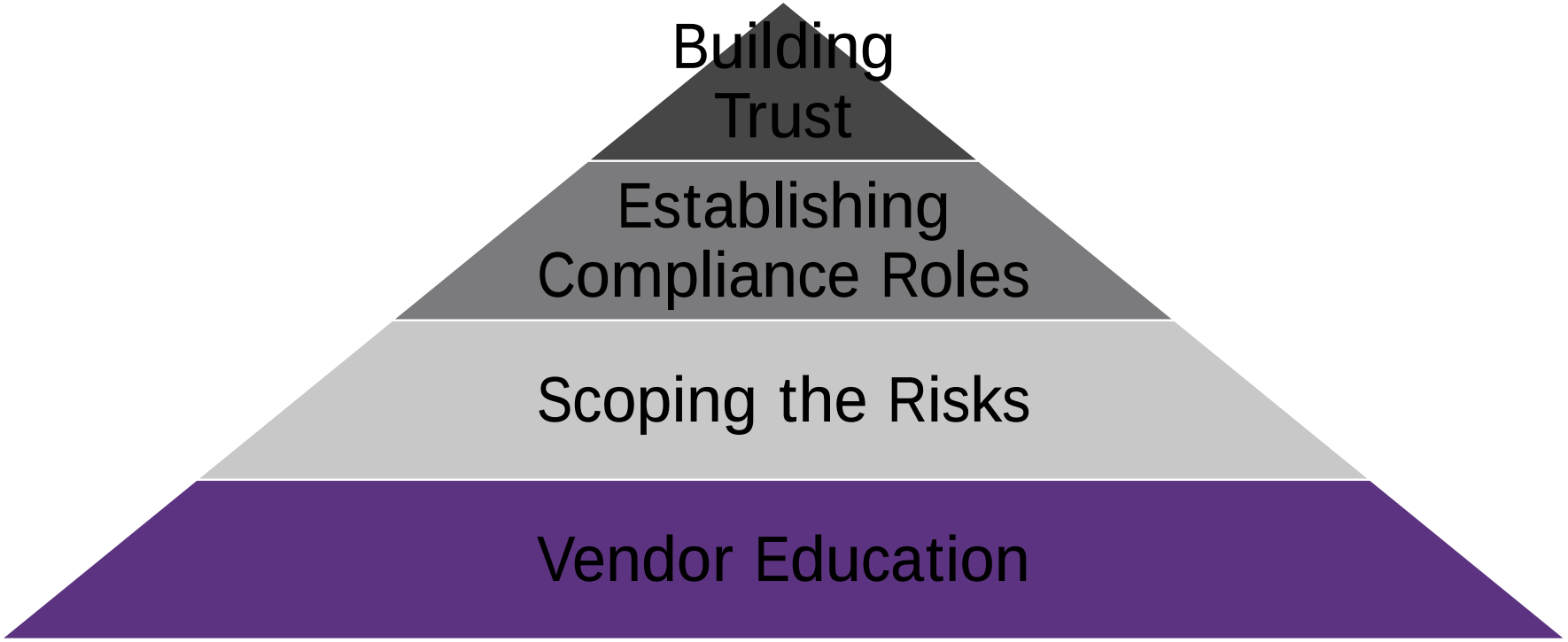
Vendor Concerns & Utility Solutions

Utility Demands Will Drive Up Costs	• Can the utility's current compliance program cover vendor personnel? • What can be outsourced to the utility?
We Cannot Comply with These Requirements	• Is this a learning curve issue? • Does the vendor have other clients subject to similar regulatory risks?
The Risk Is Too Great	• How much risk does the utility need its vendor to bear? • How likely is it that the vendor's scope of work could create significant liability for third-party harms? • Is there a statutory or regulatory bar on liability that could protect the vendor?

SECTION 03

GETTING TO YES IN A REGULATED ENVIRONMENT

Laying the Groundwork



Getting to Yes on Risk Allocation

Risk Costs	Allocating Risk
• Regulatory penalties • Enforcement costs • Mitigation costs • Damages	• Price of service • Indemnification • Insurance • Liability caps

Getting to Yes on Contract Language

- Allocation of risk
- Compliance commitments and the costs of compliance activities
  - Specific contract language
  - Incorporating company policies
  - Use of utility compliance personnel
- Coordination in regulatory compliance proceedings
- Indemnification process
- Confidentiality
- Changes in law
- Communication provisions

After Getting to Yes

- Standardizing your company's terms when there's no "market"
- Setting expectations
  - Communications
  - Process Changes
  - Points of contact
- The mutual advantages of repeat business
- Protecting yourself for when things go wrong
- Preparing for the future of cybersecurity regulation

Biography

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

Dan Skees is a partner in the energy practice. He represents electric utilities before the Federal Energy Regulatory Commission (FERC) and other agencies on rate, regulatory, and transactional 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.

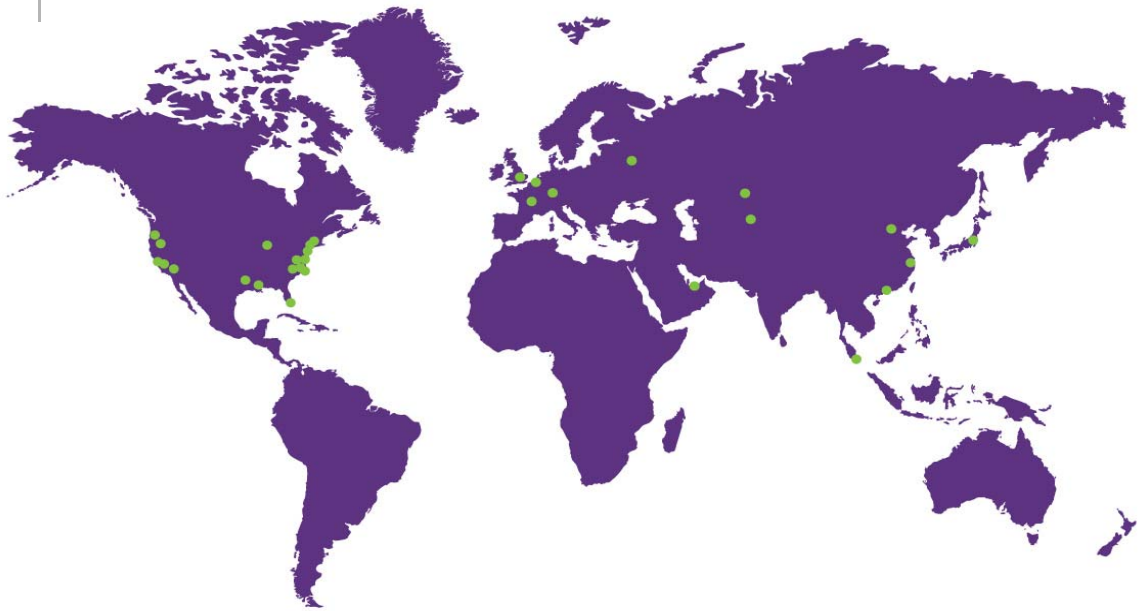
Dan's counsel includes the unique compliance concerns presented by the Critical Infrastructure Protection (CIP) reliability standards. Working with business and technical leads within companies and their outside IT consultants, he assists electric utilities in designing their CIP compliance programs and defending those efforts when necessary. The process includes proceedings on reliability compliance before FERC, the North American Electric Reliability Corporation (NERC), and regional entities charged with enforcing compliance.

Our Global Reach

Africa
Asia Pacific
Europe
Latin America
Middle East
North America

Our Locations

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



Morgan Lewis

*Our Beijing office operates as a representative office of Morgan, Lewis & Bockius LLP. In Shanghai, we operate as a branch of Morgan Lewis Consulting (Beijing) Company Limited, and an application to establish a representative office of the firm is pending before the Ministry of Justice. In Hong Kong, Morgan Lewis has filed an application to become a registered foreign law firm and is seeking approval with The Law Society of Hong Kong to associate 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 office operates as a representative office of Morgan, Lewis & Bockius LLP. In Shanghai, we operate as a branch of Morgan Lewis Consulting (Beijing) Company Limited, and an application to establish a representative office of the firm is pending before the Ministry of Justice. In Hong Kong, Morgan Lewis has filed an application to become a registered foreign law firm and is seeking approval with The Law Society of Hong Kong to associate with Luk & Partners.
This material is provided for your convenience and does not constitute legal advice or create an attorney-client relationship. Prior results do not guarantee similar outcomes. Attorney Advertising.