Technology Marathon 2022

Our Technology Marathon is an annual series of tailored webinars focused on hot topics, trends, and key developments in the technology industry that are of essential importance to our friends and clients. Now in its 12th year, our expansive curriculum kicks off in May and continues into June.

For more information:
https://www.morganlewis.com/events/technology-marathon

Morgan Lewis

Before we begin

Tech Support

If you are experiencing technical difficulties, please contact WebEx Tech Support at +1.866.779.3239.

Q&A

The Q&A tab is located near the bottom right hand side of your screen; choose "All Panelists" before clicking "Send."

CLE

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.

Audio

The audio will be silenced until we begin at 1:30 pm ET.

You will hear sound through your computer speakers/headphones automatically. Make sure your speakers are ON and UNMUTED.

To access the audio by telephone, please click the "phone" icon below your name on the Participants Panel for teleconference information.

Morgan Lewis

TECHNOLOGY MARATHON

The Current Cybersecurity Threat Landscape: Lessons Learned

The Current Cybersecurity Threat Landscape: Lessons Learned

June 29, 2022

Morgan Lewis

Presenters

Kirstin E. Gibbs

Sergio F. Oehninger

J. Daniel Skees

Arjun Prasad Ramadevanahalli

Teri J. Diaz

Morgan Lewis

Agenda

- The latest federal cybersecurity directives and controls needed to satisfy regulators
- Lessons learned from energy infrastructure industries
- Next industries on the watch list
- Cyberinsurance strategies and considerations

The latest federal cybersecurity directives and controls needed to satisfy regulators

Morgan Lewis

Recent Federal Initiatives

- TSA Pipeline Security Directives
- Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)
- SEC Cybersecurity Disclosure Rules
- Russia/Ukraine Conflict - CISA "Shields Up" Initiative
- February 2022 – NIST Guidance on Software Supply Chain Security Requirements for Federal Software Procurement
- May 2021 - Executive Order (EO 14028 - *Improving the Nation's Cybersecurity)*
- July 2021 - National Security Memorandum
  - Establishes voluntary cybersecurity goals and expectations of owners and operators of critical infrastructure.
- April 2021 - Industrial Control Systems Cybersecurity Initiative

Case Study: TSA Pipeline Security Directives

TSA is the federal entity primarily responsible for securing surface transportation modes.

Source: GAO analysis of Transportation Security Administration documents; Art Explosion (photos). | GAO-20-558

Case Study: TSA's Emergency Authority

- TSA can issue regulations or Security Directives on an emergency basis as needed "to protect transportation security." (49 U.S.C. § 114(l)(2)(A))
- No notice or comment opportunity required (49 U.S.C. § 114(l)(2)(A))
  - Contrast to other common regulatory frameworks
  - Example: NERC CIP requirements are stakeholder developed regulations subject to multiple rounds of public notice and comment and prescriptive procedural rules
- Security Directives have the force of law and are mandatory by their specified effective date.
  - Subject to review by the Transportation Security Oversight Board
  - Effective for a period not to exceed 90 days, unless ratified or disapproved by the Board or rescinded by TSA. (49 U.S.C. § 114(l)(2)(B)).

Case Study: TSA Pipeline Security Directives

- Security Directive Pipeline 2021-01 (SD1) – first issued May 2021
  (1) Assess whether current operations are consistent with TSA's guidelines;
  (2) Identify any gaps and remediation measures; and
  (3) Report the results to TSA and others.

- Security Directive Pipeline 2021-02 (SD2) – first issued July 2021
  (1) Implement specific mitigation measures to protect IT and OT systems;
  (2) Develop and implement a cybersecurity contingency and recovery plan; and
  (3) Conduct a cybersecurity architecture design review (CADR).

NIST Federal Software Procurement Guidance

- Developed pursuant to EO 14028
  - NIST required to develop guidance
  - Federal agencies required to follow guidance in software procurements
- Major components:
  - Use Secure Software Development Framework (SSDF) terminology and structure to organize communications about secure software development requirements.
    - From NIST 800-218 (SSDF Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities)
  - Require attestation to cover secure software development practices performed as part of processes and procedures throughout the software life cycle.
  - Accept first-party attestation of conformity with SSDF practices unless a risk-based approach determines that second or third-party attestation is required.
  - When requesting artifacts of conformance, request high-level artifacts.
- Not a replacement for more stringent requirements

Lessons learned from energy infrastructure industries

Morgan Lewis

Mandatory Cybersecurity Regulations

Accountability

Litmus test

Access to insights

Socialization of best practices

Cost recovery

Limits entity discretion

"One-size fits all"

Costs

Administrative burden

Disclosure risks

Case Study: TSA SD2 Implementation Challenges

Key Implementation Challenges	
Scoping (IT / OT)	Timing
Dual-Regulated Assets (e.g., NERC CIP)	Administrative Process • Extensions • Alternative Compliance • Rehearing
Developing Mitigation Strategies	Vendor procurement
Supply Chain Constraints	Cost Recovery (Regulated Utilities)

Leveraging Non-Binding NIST Guidance to Fill Gaps

- Mandatory and enforceable requirements do not always cover each issue, or may not at first
- NIST guidance, even if aimed at federal agencies, can:
  - Fill in the gaps between mandatory requirements and comprehensive protection
    - Provide content
    - Check for gap identification
  - Provide a preview of what may become enforceable
  - Serve as a useful guide when contracting
  - Prepare for federal contracting relationships
  - Provides a degree of standardization on often highly confidential topics
- Key examples include:
  - NIST Cybersecurity Framework
  - NIST SP 800-161r1 (Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations)
  - NIST Federal Software Procurement Guidance

Importance of Preparing for Mandatory Requirements

- All new mandatory schemes have a steep learning curve, often with short timeframes and significant legal risk
- Tools to prepare for implementation
  - Policy advocacy: Take a stakeholder interest in shaping what mandatory requirements may be like up front, even before formal rulemaking begins; regulator education is key
  - Voluntary compliance: Moving to NIST or similar practices in advance of mandatory compliance can make the jump to mandatory compliance more manageable
  - Interdisciplinary: achieving and demonstrating compliance requires coordinated action by IT/OT security, compliance, and legal; shortchanging one or the other creates risks

Noncompliance Can Be Costly

- Regulators are increasingly turning attention to cybersecurity risks.
  - Regulators will assess topical cybersecurity concerns, pushing audits beyond minimum CIP reliability standards
- Regulators are equipped with financial penalty authority.
  - Example: Under Section 215 of the Federal Power Act, fines for electric utilities available up to $1M (inflation-adjusted to $1,388,496).
- Regulatory compliance penalties can have ripple effects.
  - Tort claims and third-party liability.
  - Reputational risk should not be ignored.
- Utilities in the energy industry have been tasked with demonstrating strong cybersecurity culture that proactively addresses best cybersecurity practices and evolving threats, **especially for newer technology**

Next industries on the watch list

Morgan Lewis

Next Steps

- **Pipeline**
  - Ongoing work under SD2.
    - Auditing through on-site inspections; industry gets first impressions on regulator's approach to compliance and enforcement.
    - Lessons learned during initial inspections and subsequent audits.
  - Continued evolution of Security Directives under TSA's emergency authority.
  - Ultimately, notice and comment rulemaking.
- **Rail**
  - Initial cybersecurity requirements issued in Dec. 2021 for higher-risk freight railroads, passenger rail, and rail transit.
  - TSA expected to expand requirements for certain surface transportation entities.
- **Water/Wastewater**
  - EPA to periodically survey using light touch administrative methods.
  - No formalized regulations, but which entity would administer and under what authority? Legislation needed?
  - In the meantime, utilities can leverage federal loan programs and funding to enhance cybersecurity controls.

Cyberinsurance strategies and considerations

Morgan Lewis

Cyberinsurance: How Can It Help?

Key points to remember

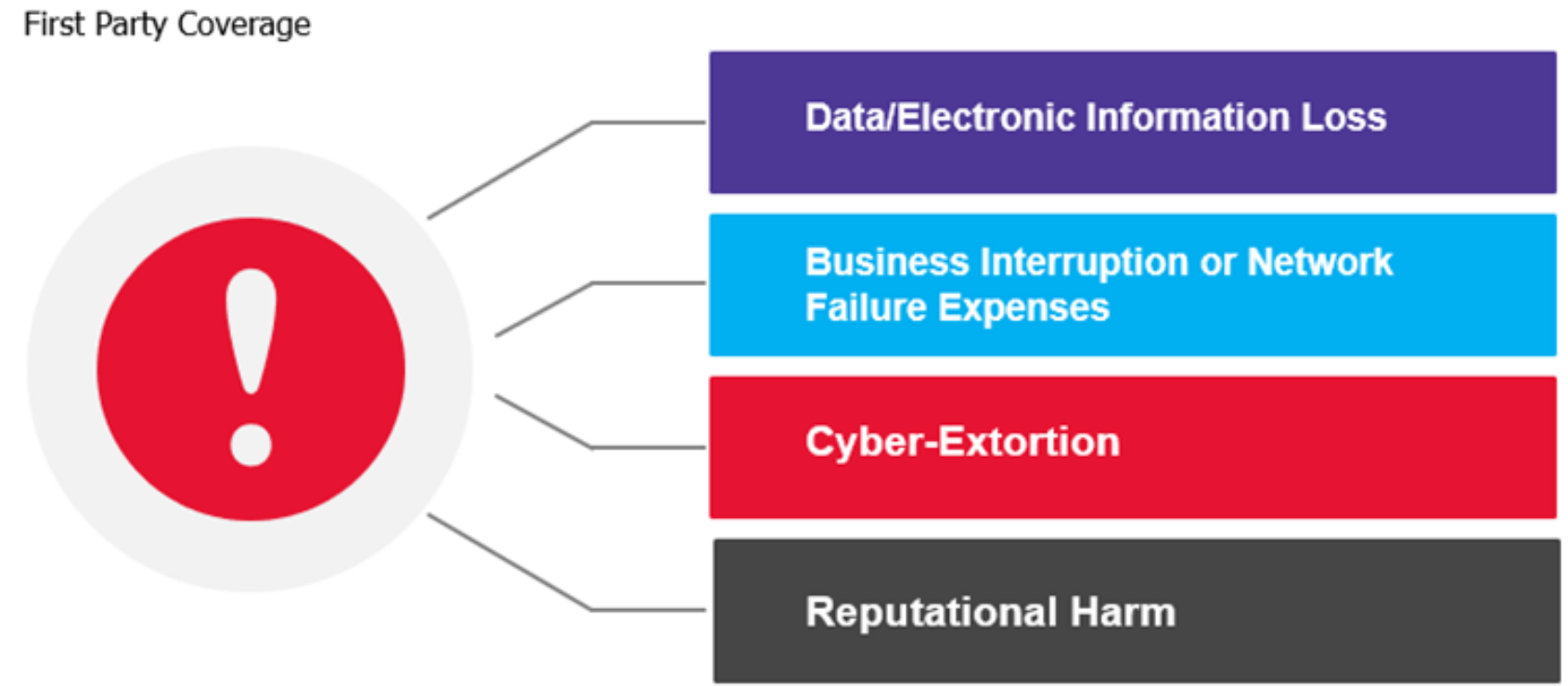
Given threats, having prevention-only strategy is insufficient

Expect that your network or computer system has been or will be compromised

Insurance is one way to minimize impact

Don’t rely exclusively on traditional insurance policies

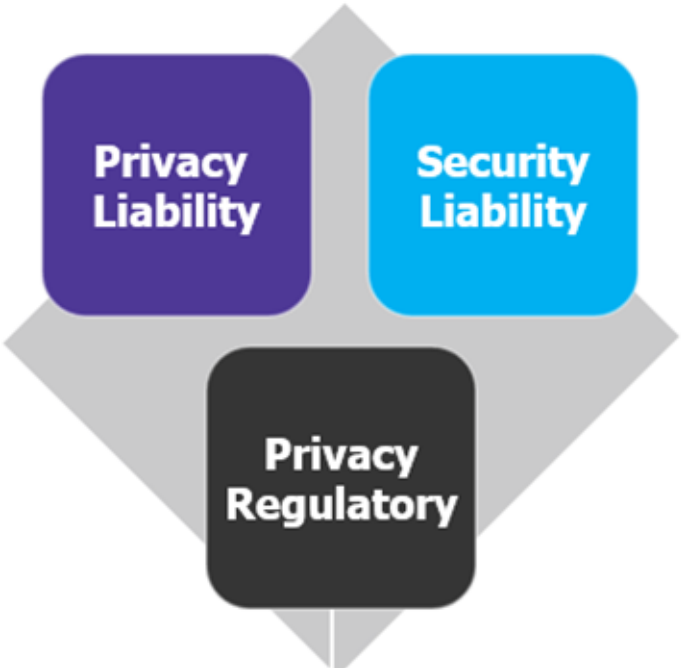
What Does Cyberinsurance Cover?
First Party Losses



First Party Losses

- Forensic studies
- Crisis response
- Public relations
- Legal advice / breach coach counsel
- Repairs
- Improving cyber security
- Lost income
- Lost or damaged digital assets
- Lost or damaged physical assets
- Fraud payments
- Ransom payments

What Does Cyberinsurance Cover?
Third Party Coverage



Third Party Liabilities and Related Costs

- Lawsuits (customers, consumers, shareholders, etc.)
- Government inquiries and investigations
- Defense costs in connection with claims, suits, and government investigations
- Other exposures:
  - Incidents involving PII
  - Contractual or other payments like those related to PCI DSS
  - Fines and Penalties (e.g., GDPR, CCPA)

Common Cyberinsurance Coverage Sections

Specialty Professional Liability Insurance

Third party coverage for compensatory damages, judgments, settlements, and defense costs for claims alleging any wrongful act regarding a specific set of professional services.

Media Content Insurance

Third-party coverage for litigation losses resulting from any act or omission related to IP infringement, plagiarism or misappropriation, invasion of privacy, defamation, wrongful entry or trespass, or negligent infliction of emotional distress.

Security and Privacy Liability Insurance

Third party coverage for compensatory damages, fines, judgments, settlements, and defense costs resulting from litigation or regulatory enforcement actions related to security and privacy incidents such as **data breaches** or **ransomware attacks**.

Security Failure/Privacy Event Management Insurance

First party coverage for losses a company incurs in responding to security and privacy incidents such as data breaches or phishing attacks that result in the theft of confidential information.

Network Interruption Coverage

First party coverage for if company systems are taken down or interrupted, such as with a denial-of-service attack. This coverage covers costs caused by interruptions, such as lost income and costs to restore the system.

Cyber Extortion Coverage

First party coverage for specific incidents of active extortion or ransomware and covers both the approved payment of ransom to a bad actor to resolve a threat situation, and the costs to investigate and respond to such a threat

Cyber Liability Coverage: Falling Through the Gaps

- Cyber risks may fall through gaps in traditional first-party and third-party policies, most of which now have potentially applicable exclusions.

Navigating the Gaps to Find Coverage

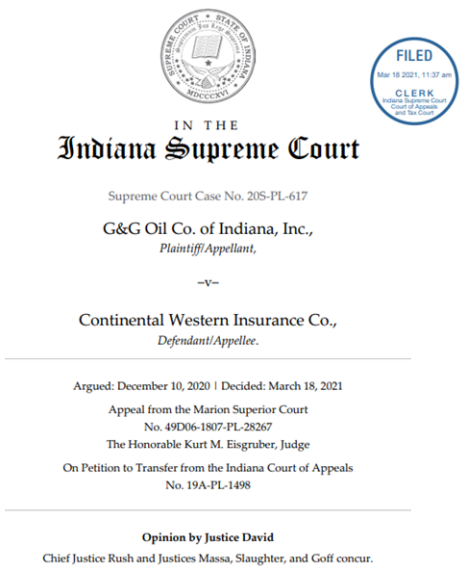
1. **Traditional First Party Property Policies** – Look for coverage for cyber-related exposures.

2. **D&O** – Check for coverage for shareholder class actions related to data breaches and failure to insure for cyber liabilities (risk management).

3. **Crime/Fidelity Policies** – Look for coverage for employee dishonesty, vandalism and theft, computer fraud, kidnap/ransom or extortion.

4. **Commercial General Liability Policies** – CGL policies provide protection for financial loss due liability for property damage or personal and advertising injury caused by your services, business operations or employees. Beware of cyber exclusions.

G&G Oil of Indiana v. Continental Western Insurance Co. (2021)



IN THE

Indiana Supreme Court

Supreme Court Case No. 20S-PL-617

G&G Oil Co. of Indiana, Inc.,
Plaintiff/Appellant,

–v–

Continental Western Insurance Co.,
Defendant/Appellee.

Argued: December 10, 2020 | Decided: March 18, 2021

Appeal from the Marion Superior Court
No. 49D06-1807-PL-28267
The Honorable Kurt M. Eisgruber, Judge

On Petition to Transfer from the Indiana Court of Appeals
No. 19A-PL-1498

Opinion by Justice David

Chief Justice Rush and Justices Massa, Slaughter, and Goff concur.

FILED
Mar 18 2021, 11:37 am
CLERK
Indiana Supreme Court
Court of Appeals
and Tax Court

Norfolk Truck Center, Inc., 430 F.Supp.3d 116, 129 (E.D. Va. 2019) (observing, *arguendo*, that "some intervening cause could sever the chain of events between loss and use of a computer, if that intervening cause was sufficiently significant to destroy the straightforward or proximate relationship between the use of a computer and the loss" and defining direct as "something that is done in a 'straightforward' or 'proximate' manner and 'without deviation' or 'without intervening agency' from its cause").

These definitions inform our understanding of the Policy term

Insurance contracts "are governed by the same rules of construction as other contracts." *Justice v. American Family Mut. Ins. Co.*, 4 N.E.3d 1171, 1175 (Ind. 2014) (quoting *Colonial Penn Ins. Co. v. Guzorek*, 690 N.E.2d 664, 667 (Ind. 1997)). Interpretation of an insurance contract is a question of law, which we address de novo. *Id.* (citation omitted).

Discussion and Decision

G&G Oil raises the same issues on transfer as it has below: Whether the

Oil would have incurred even greater loss to its business and profitability. These payments were "voluntary" only in the sense G&G Oil consciously made the payment. To us, however, the payment more closely resembled one made

payment w

find that G

Conclu

Althoug

computer,

therefore

Continenta

and remai

Indiana Supre

insurance companies and insureds." *Justice*, 4 N.E.3d at 1176 (citations omitted). One such rule is that courts construe ambiguous terms against the policy drafter and in favor of the insured. *Id.* (citing *Am. States Ind. Co.*

Analyzing G&G Oil's actions in this case, its transfer of Bitcoin was nearly the immediate result—without significant deviation—from the use of a computer. Though certainly G&G Oil's transfer was voluntary, it was

omitted). One such rule is that courts construe ambiguous terms against the policy drafter and in favor of the insured. *Id.* (citing *Am. States Ind. Co. v. Kiger*, 662 N.E.2d 945, 947 (Ind. 1996)); *see also Eli Lilly and Co. v. Home Ins. Co.*, 482 N.E.2d 467, 470 (Ind. 1985) (observing "[a]n ambiguous insurance policy should be construed to further the policy's basic purpose of indemnity").

National Ink & Stitch v. State Auto Property and Casualty Company, 435 F.Supp.3d 679 (D. Md. 2020)

NATIONAL INK AND STITCH, LLC, Plaintiff,

v.

STATE AUTO PROPERTY AND CASUALTY INSURANCE COMPANY, Defendant.

Civil Case No. SAG-18-2138

United States District Court, D. Maryland.

Signed 01/23/2020

Background: Insured brought action against insurer to recover under business-owners policy for damage to its computer system in a ransomware attack. Parties filed cross-motions for summary judgment.

Holdings: As a matter of first impression, the District Court, Stephanie A. Gallagher, United States Magistrate Judge, held that:

(1) loss of computer data and software was covered, and

(2) loss of functionality of computer system was covered.

Insured's motion granted; insurer's motion denied.

In the instant case, State Auto seems to equate "physical loss or damage" to Plaintiff's computer system to require an utter inability to function. The Policy language, and the relevant case law, impose no such prerequisite. The more persuasive cases are those suggesting that loss of use, loss of reliability, or impaired functionality demonstrate the required damage to a computer system, consistent with the "physical loss *or damage to*" language in the Policy (emphasis added). Indeed, in

operable. Here, not only did Plaintiff sustain a loss of its data and software, but Plaintiff is left with a slower system, which appears to be harboring a dormant virus, and is unable to access a significant portion of software and stored data. Because the plain language of the Policy provides coverage for such losses and damage, summary judgment will be granted in favor of Plaintiff's interpretation of the Policy terms.

Handling Cyber Claims – Best Practices

When in doubt – report

- Notice/Reporting requirements and thresholds
  - Consider reporting obligations (state by state).
  - Consider minimum requirements , narrow control groups, or bordereaux if reporting obligations are burdensome.
- Retention requirements and other limitations
  - Report even where exceeding retention is doubtful.
  - Note any temporal limits on recovery, notice, reporting, proof of loss, and for filing claim or suit.
- Proof of Loss and Suit Provisions.
  - Check the deadlines and negotiate extensions.
  - Work closely with coverage counsel and privacy counsel on Proofs of Loss.
    - Words matter – make sure you are triggering all appropriate coverages.
  - Consider any confidentiality obligations.
  - Scrutinize requirement for filing suit
    - Timing (e.g., 1 or 2 years from inception of loss)
    - Forum Selection and Choice of Law

Handling Cyber Claims - Best Practices

- Common Requests for Information from Insurers
  - Duty to cooperate with insurer's investigation and reasonable requests
  - Bottom-line Numbers: How many people/states/countries affected?
  - Correspondence with regulators.
  - Legal memos (e.g., consumer/regulator notifications).
  - Invoices (consider confidentiality, redactions, etc.).

- Non-waiver/Non-Disclosure Agreements
  - Consider role of brokers.
  - Consider third-party claims-handling vendors.
  - Consider litigation risk of exchanging written information.

Handling Cyber Claims – Best Practices

- **Review Pre-approved Vendors and Counsel**
  - Obtain advance approval of new vendors, including breach counsel.
  - Negotiate rates for specific vendors.

- **Check Other Coverages**
  - First-Party Property and Business Interruption Insurance
  - Crime Coverage
  - D&O Coverage
  - GL Coverage

- **Subrogation**
  - Evaluate priority of recovery between insurer and insured.
    - Made-whole Doctrine
    - Deductibles/Retentions
    - Equitable versus Contractual Subrogation
  - High retentions combined with subrogation clauses create potential conflicts with insurance carriers.


Questions
Morgan Lewis

Biography

Kirstin E. Gibbs
Washington, D.C.
+1.202.739.5026
kirstin.gibbs@morganlewis.com

Kirstin Gibbs, co-leader of the firm's energy industry team, as well as a leader of the climate change and sustainability working group, represents pipelines, producers, traders, marketers, utilities, and end users, on a host of issues. She handles transactional matters related to the development of new oil and gas infrastructure and regularly provides assistance with negotiation of midstream transportation and storage agreements, complex asset management agreements, and commodity transactions. Kirstin also counsels global clients interested in addressing climate change and sustainability initiatives by investing in clean energy technologies, including renewable natural gas and hydrogen, and decarbonizing their operations.

Biography

Sergio Oehninger
Washington, D.C.
+1.202.739.5521
sergio.oehninger@morganlewis.com

Sergio Oehninger represents companies in complex insurance coverage and bad-faith disputes in the United States and around the world. He counsels multinational corporations on insurance coverage and risk management issues arising in various industries, including financial services, retail, energy, technology, real estate, construction, and hospitality.

Biography

J. Daniel Skees
Washington, D.C.
+1.202.739.5834
daniel.skees@morganlewis.com

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, utility financing, electric markets and trading issues, reliability standards development and compliance, including cybersecurity requirements, administrative litigation, and transmission development. In handling appeals of FERC decisions, Dan has successfully represented clients before both the US Court of Appeals for the District of Columbia Circuit and the US Court of Appeals for the Fifth Circuit.

Biography

Arjun Prasad Ramadevanahalli
Washington, D.C.
+1.202.739.5913
arjun.ramadevanahalli@morganlewis.com

Arjun Prasad Ramadevanahalli represents electric power, natural gas, and oil industry participants in regulatory and transactional matters. He assists clients on issues regarding wholesale markets, utility transactions, rate matters, and enforcement proceedings before the Federal Energy Regulatory Commission (FERC), and on cybersecurity matters in the energy industry. Arjun regularly advises utilities and other industry participants on North American Electric Reliability Corporation (NERC) reliability standards enforcement and compliance matters, including cybersecurity compliance and controls under the Critical Infrastructure Protection (CIP) suite of standards. Arjun counsels pipeline owners and operators on cybersecurity compliance before the Transportation Security Administration (TSA).

Biography

Teri J. Diaz
Washington, D.C.
+1.202.739.5632
teri.diaz@morganlewis.com

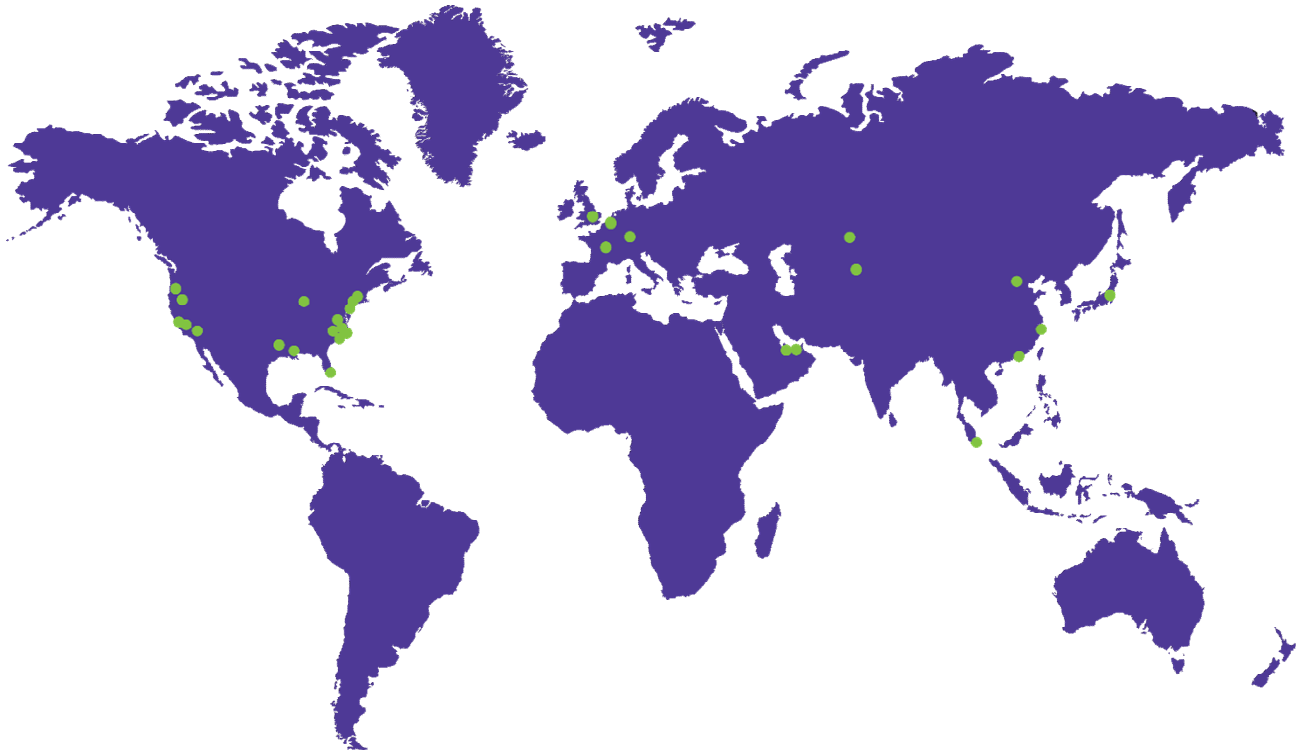
Teri J. Diaz focuses her practice on representing corporate policyholders in the preservation and recovery of insurance assets. Teri has advised companies in complex insurance recovery matters including disputes involving toxic torts, property damage, business interruption loss, and other liabilities. She represents clients in federal and state courts across the United States and in mediation and arbitration proceedings. Her clients include companies in a wide range of industries, including manufacturing, technology, retail, energy, and healthcare.

Our Global Reach

Africa
Asia Pacific
Europe
Latin America
Middle East
North America

Our Locations

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



Morgan Lewis

THANK YOU