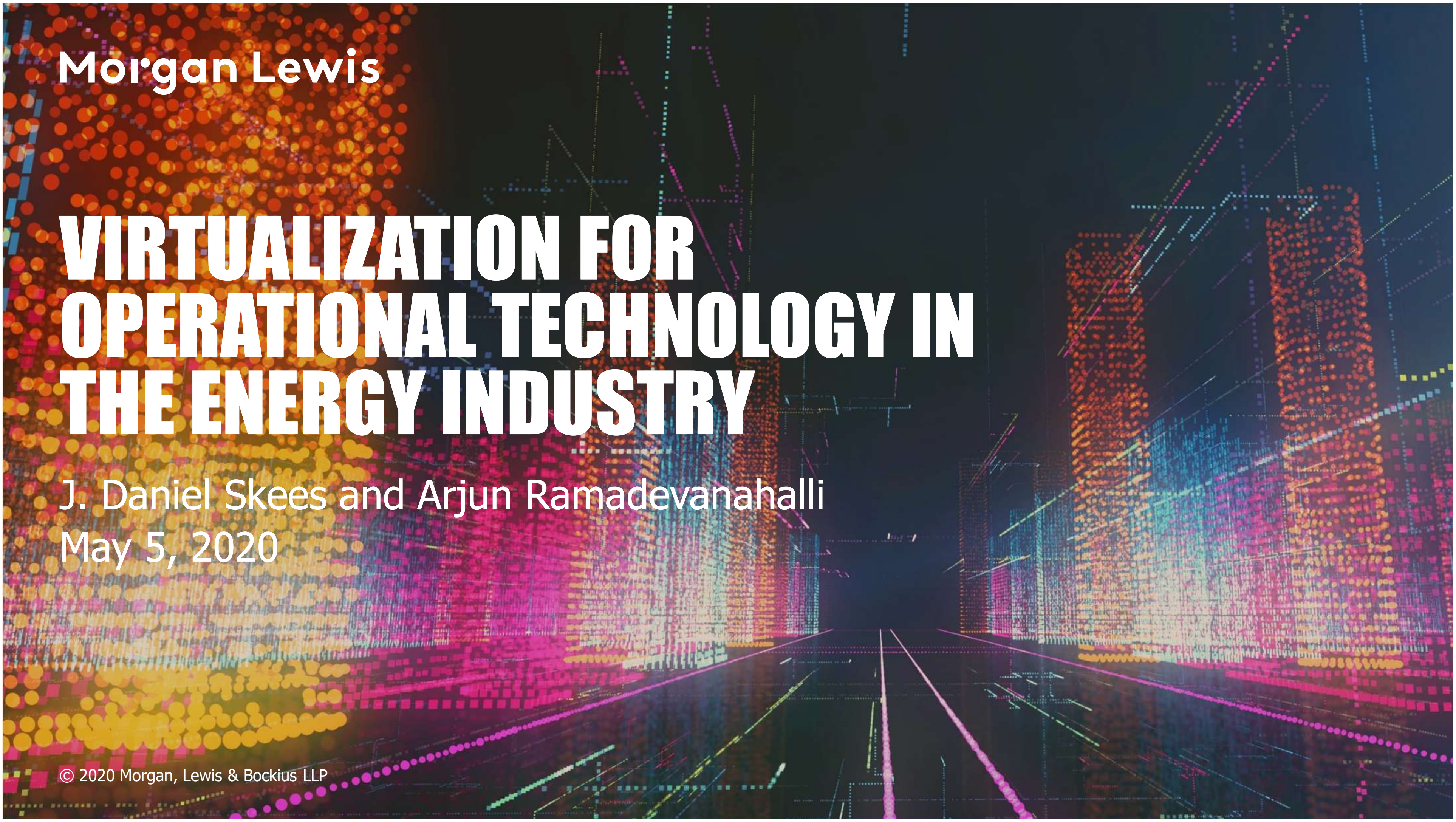


Morgan Lewis

VIRTUALIZATION FOR OPERATIONAL TECHNOLOGY IN THE ENERGY INDUSTRY

J. Daniel Skees and Arjun Ramadevanahalli

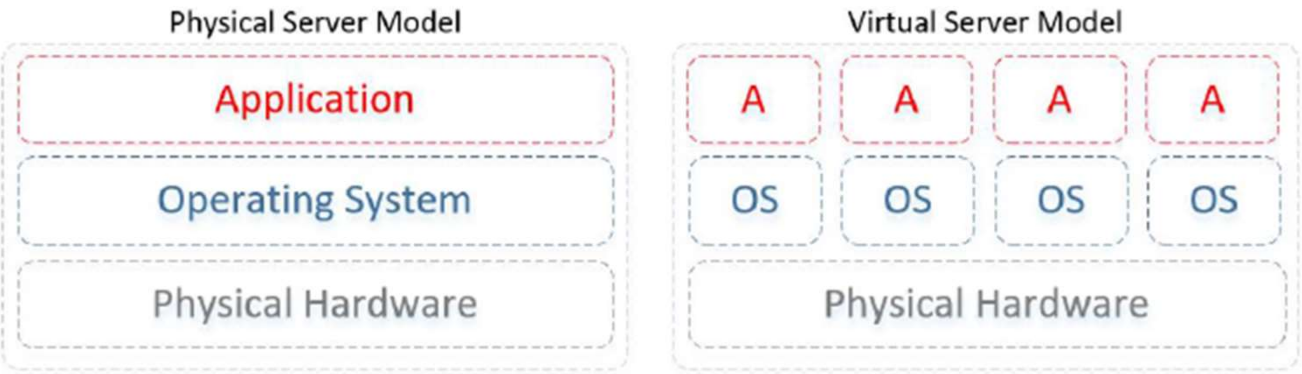
May 5, 2020

SECTION 01

VIRTUALIZATION AND THE CLOUD

Virtualization

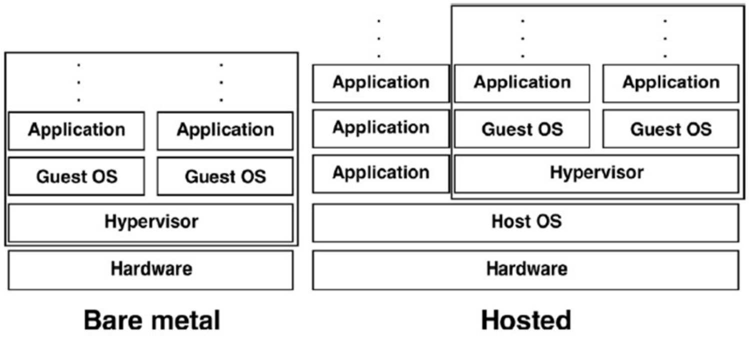
- Virtualization is the process of simulating an application, system, device, server, storage, or network through the creation and use of a virtual representation.
- Allows for use of multiple virtual systems, operating systems, and applications to run independently off a host machine.



Source: NIST SP 800-125
Image: NERC, Virtualization and Future Technologies: Case for Change White Paper (Apr. 2019)

Virtualization

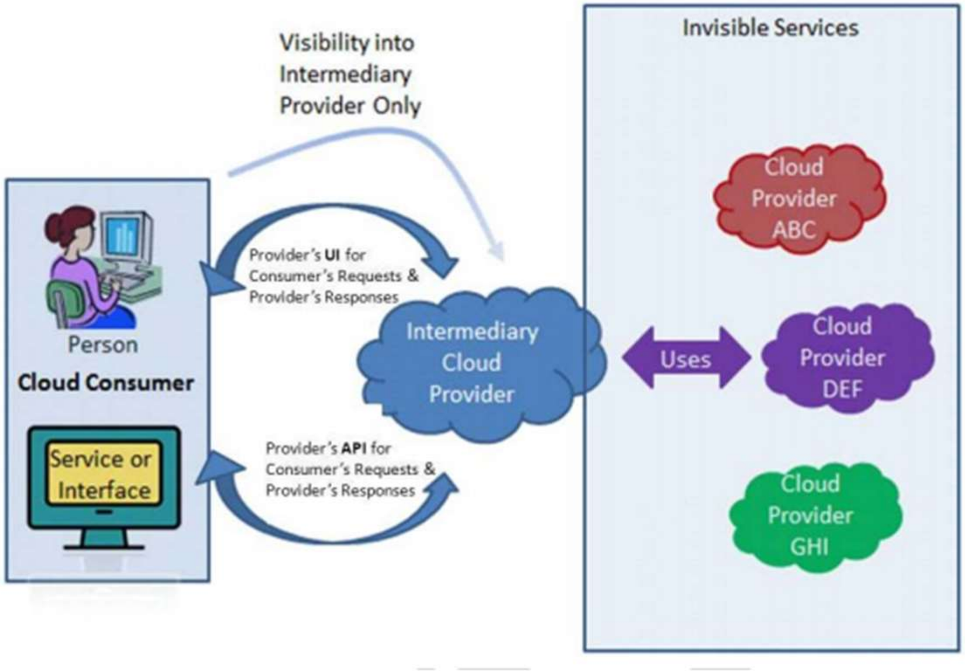
- In "*full virtualization*," one or more OSs and the applications they contain are run on top of virtual hardware.
- Each instance of an OS and its applications runs in a separate VM called a *guest operating system*.
- The guest OSs on a host are managed by the *hypervisor*, which controls the flow of instructions between the guest OSs and the physical hardware, such as CPU, disk storage, memory, and network interface cards.



Source: NIST SP 800-125

The Cloud

- Cloud computing is a model for enabling on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.


Visibility into Intermediary Provider Only
Invisible Services
Person
Cloud Consumer
Service or Interface
Provider's UI for Consumer's Requests & Provider's Responses
Provider's API for Consumer's Requests & Provider's Responses
Intermediary Cloud Provider
Uses
Cloud Provider ABC
Cloud Provider DEF
Cloud Provider GHI

Source: NIST SP800-145
Image: NIST SP500-29 (Draft)

SECTION 02

USE CASES AND SECURITY RISKS

Use Cases in the Energy Industry

- Virtualization and Cloud Use Cases
  - Virtualized control system infrastructure or entire control centers
  - Cloud-based SCADA and ICS
  - Dynamic VMs for discrete tasks operating independent of hardware
  - Less need for on-premises physical assets, saving space and money
  - Enhanced incident recovery
  - Enhanced computing power
  - Secure, on-demand storage

Benefits of Virtualization and the Cloud

- Benefits of these technologies are game-changing
  - Cost-savings
  - Efficiency
  - Operational flexibility
  - Redundancy
- Operational benefits are wide-ranging
  - Enhanced computing power
  - Microsegmentation provides tailored logical controls for virtualized tasks
  - Application of policy-based security controls
  - Zero trust models
  - Vendors provide dedicated support, protection, and redundancy for sensitive cloud data

Security Risks

- Implementing security for these advanced systems is multi-faceted
  - Virtual environments introduce layer(s) of complexity
  - Monitoring and logging for virtual system communications
  - "Hyperjacking"
- Preventing unintended outcomes
  - Maintaining an accurate "asset" inventory
  - Processes for controlling changes in the cloud
- Data concerns
  - Cloud - Securing data in transit and at rest
  - Virtualization - Ensuring proper sanitization for virtual storage

Recent Headlines

WSJ	“U.S. Moves to Address ‘Extraordinary Threat’ From Some Foreign Electric Gear”
ZDNet	“DHS Says Ransomware Hit US Gas Pipeline Operator”
E&E NEWS	“Report Reveals Play-By-Play of First U.S. Grid Cyberattack”
The New York Times	“Russian Hackers Appear to Shift Focus to U.S. Power Grid”

SECTION 03

LEGAL CONSIDERATIONS

Existing Regulatory Regime

- FPA Section 215 requires all “users, owners, and operators of the bulk-power system” to comply with the applicable Reliability Standards.
  - As the designated Electric Reliability Organization, NERC is charged with overseeing development and enforcement of the Reliability Standards.
- Critical Infrastructure Protection (CIP) Standards set forth cybersecurity requirements for utilities.
  - Risk-based approach to protecting critical assets that support the reliable operation of the bulk electric system.
  - Requires implementation of complex technical controls, encryption and protection of critical information, access management program, training regime, background checks, supply chain risk management plan, etc.

Noncompliance Can Be Costly

- Under Section 215 of the Federal Power Act, fines available up to $1M per day, per violation
  - Inflation-adjusted to $1,269,500 in 2019 under the Federal Civil Penalties Inflation Adjustment Act Improvements Act of 2015 (and FERC Order No. 853)
- Traditionally, only blackout-related violations received significant monetary penalties, but regulators are increasingly turning attention to cybersecurity risks.
  - FERC has been conducting audits of CIP compliance since 2016.
  - Regulators will assess topical cybersecurity concerns, pushing audits beyond minimum CIP reliability standards
- Utilities are tasked with demonstrating strong cybersecurity culture that proactively addresses best cybersecurity practices and evolving threats, **especially for newer technology.**
  - Risk to reputation if not done carefully

Catching Up to New Technology

- Virtualization and cloud environments not contemplated by CIP Standards, creating a regulatory "gap".
- Implementation under CIP Standards is based on identifying physical assets.
  - Standards generally apply to a class of "programmable electronic devices" (i.e., BES Cyber Assets) and their associated devices.
  - VMs and some types of remote cloud storage are not technically "devices".
- Compliance obligations are heavily dependent on regulatory terminology.
  - Certain protections apply based on interconnected devices.

    Example: Electronic Security Perimeter is a logical protection but requires connection to a BES Cyber System.

Compliance Risks

- Compliance concerns arise when new technologies do not use traditional technical architecture.
  - Vendors are innovating.
  - Industry-standard products now virtualize reliability tasks and can require CIP system information to be stored off-premises.
- Lack of clarity for how to implement these technologies in a CIP environment
  - How do you classify a hypervisor?
  - Is a VM just software sitting on a physical device or is it an “asset” subject to logical protections?
  - How do you prove that you protected a dynamic VM that exists for only a short time?

Outsourcing

- Many utilities are incorporating cloud products and services into operations (IT and OT).
- Challenges arise when trying to prove vendors are compliant.
  - CIP-004-6 R4 requires utilities to demonstrate that individual access rights to sensitive information repositories are tightly controlled and based on legitimate business need (even off-premises).
- Looming supply chain requirements will put more pressure on vendors to help utilities comply.
  - CIP-013-1 R1 requires that utility procurements of critical systems address vendor coordination (e.g., disclosure of known vendor vulnerabilities, incident response).

Data Security and Data Privacy

- Cloud services offer many benefits for processing and storing information but can also present compliance and legal risks.
- Data Security
  - CIP-011-2 information protection requirements for storing and handling BES Cyber System Information
  - Risk of disclosure of sensitive Critical Energy/Electric Infrastructure Information
- Data Privacy
  - Potential exposure under state and federal privacy laws if sensitive customer data is not handled properly or becomes compromised

Ongoing Regulatory Initiatives

- NERC Standards Drafting Team is working on changes to better accommodate virtualization and cloud technologies into CIP framework.
- Project 2016-02: revisions to support use of virtualized technologies
  - Proposed modifications to CIP-004-6, CIP-005-5, CIP-006-6, CIP-007-6, and CIP-010-2 to address virtualization
- Project 2019-02: revisions to facilitate use of third-party data storage and analysis systems
  - Intention is to clarify minimum protections expected when using cloud services
  - Proposed modifications to CIP-004-6 and CIP-011-2

FERC Proceedings

- **Docket No. RM20-8**: Notice of Inquiry on "Virtualization and Cloud Computing Services"
- Proceeding will address:
  - Potential benefits and risks associated with the use of virtualization and cloud computing services
  - Examine barriers in the CIP Standards that impede the voluntary adoption of virtualization or cloud computing services
- Four specific requests for comment:

1. Scope of potential use of virtualization and cloud computing services (such as which BES reliability operating services can they provide)
2. Potential benefits and risks associated with virtualization and cloud computing services
3. Potential impediments to adopting virtualization and cloud computing services (including needed changes to CIP standards)
4. Potential use of new and emerging technologies in the current CIP standards framework (including whether existing compliance requirements limit the ability to leverage new tech)

Deadline for comments extended to July 1

FERC Proceedings

- **Docket No. RD20-2**: Order Directing Informational Filings on NERC Virtualization/Cloud Projects
- Order directs information on the ongoing NERC virtualization/cloud projects:
  - Current status of the project; interim target dates and the anticipated filing date for new or modified Reliability Standards
  - Quarterly status updates until such time new or modified Reliability Standards are filed with the Commission
- According to NERC, Project 2016-02 addressing virtualization modifications should result in revised standards filed with FERC in December 2021.
- According to NERC, Project 2019-02 on information controls (such as cloud computing and similar vendor storage) should result in a FERC filing in September 2020.
- These are pre-COVID-19 estimates
  - Potential delays are unclear

Staying Engaged

- Utilities should stay engaged in these regulatory proceedings to ensure eventual compliance burden is tailored appropriately to the risks.
- Regulatory developments could lead to significant changes in required controls and require utilities to absorb additional costs.
- Risk of over-expansive regulations or rules that encourage “scope creep”
- Complexity of technology leaves challenges to address:
  - How to inventory and track large numbers of assets;
  - Managing virtual baselines;
  - Patching with minimal disruption to operations; and
  - Many more . . .

Managing Compliance Risks in the Interim

- Utilities should be well prepared to engage regulators.
  - Provide regulators with a clear story of how your organization is deploying virtualized environments while maintaining sound cybersecurity posture.
- Ensure that third-party providers, such as cloud vendors, are adequately trained on how they can support your compliance obligations.
  - Request documentation proving limited physical and electronic access to BCSI (including provisioning for job need and access revocations) and adequate encryption.
  - Have them demonstrate compliance with third-party audits.
- Demonstrate that your own systems are sound based on industry standard “seals of approval”
  - Independent security evaluations
  - ISO 27001
  - SOC 2
  - FedRAMP

Preparing for New Restrictions

- On May 1, President Trump signed an executive order declaring a national emergency with respect to the power grid.
  - Recognizes that the bulk-power system is a valuable target for malicious actors
- Order restricts importation and use of bulk-power system equipment supplied by companies controlled by foreign adversaries.
- Effective immediately, even though the foreign adversaries and the target equipment have not yet been publicly identified.
- During contracting and procurement, utilities should be mindful of the country of origin of bulk-power system equipment.
  - Secure backups
  - Maintain documentation supporting origin of imported components

SECTION 04

CONCLUSION AND TAKEAWAYS

Presentation Takeaways

1. Virtualization and cloud technologies are revolutionizing the ways in which utilities supply and distribute power and gas.

2. The significant cost and operational benefits of these technologies must be weighed against the security risks.

3. Regulations are still catching up to the technology.

4. Utilities have an opportunity to make the case for appropriately tailored regulations.

COVID-19

- Current conditions have prompted many utilities to leverage virtualization and cloud computing to support remote operations.
- Increase in remote functions presents security risks.
- COVID-19 has provided a “stress test” for the use of these technologies on a scale not seen before.

Morgan Lewis Coronavirus/COVID-19 Resources

We have formed a multidisciplinary **Coronavirus/COVID-19 Task Force** to help guide clients through the broad scope of legal issues brought on by this public health challenge.

To help keep you on top of developments as they unfold, we also have launched a resource page on our website at

www.morganlewis.com/topics/coronavirus-covid-19

If you would like to receive a daily digest of all new updates to the page, please please visit the resource page to subscribe using the purple "Stay Up to Date" button.

Presenters

J. Daniel Skees
Partner
Washington, DC
daniel.skees@morganlewis.com

Arjun P. Ramadevanahalli
Associate
Washington, DC
arjun.ramadevanahalli@morganlewis.com

Morgan Lewis and Global Technology

Be sure to follow us at our website and on social media:

Web:	**www.morganlewis.com/sectors/technology**
Twitter:	**@MLGlobalTech**
LinkedIn Group:	**ML Global Tech**

Check back to our Technology May-rathon page frequently for updates and events covering the following timely topics:

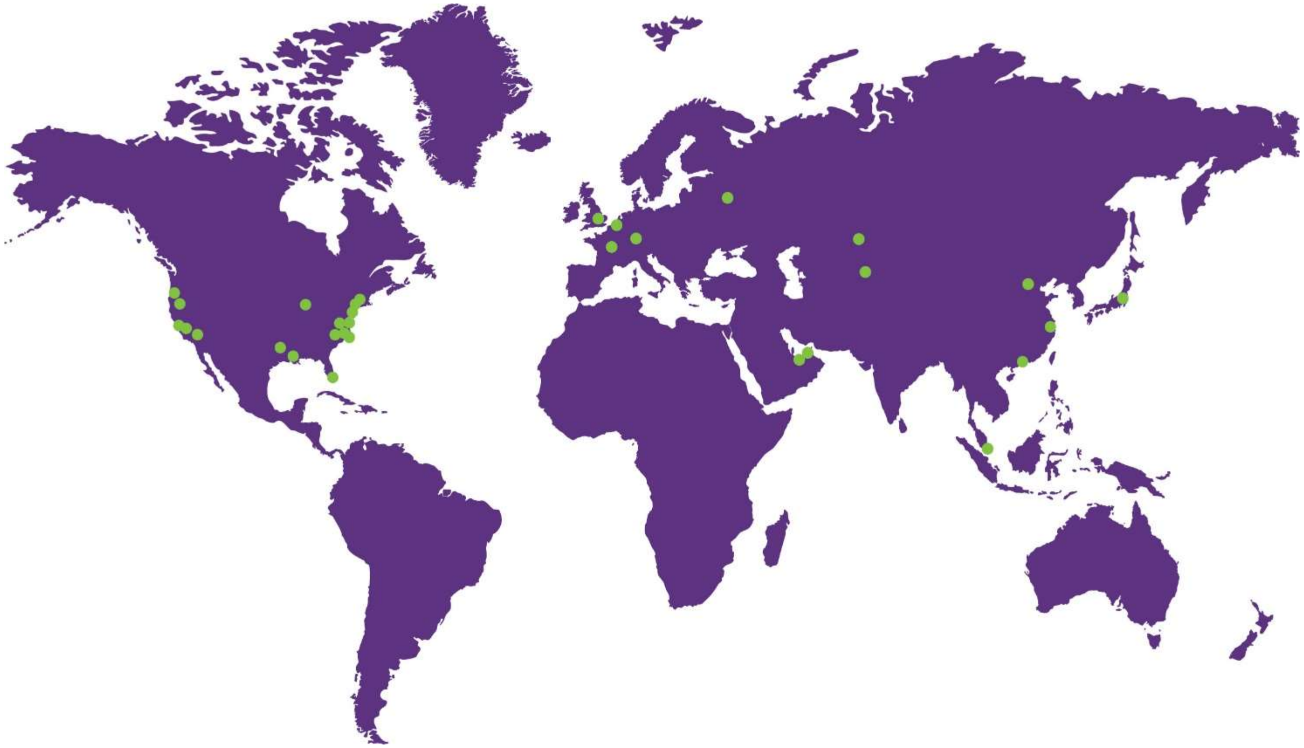
21st Century Workplace	**Cybersecurity, Privacy and Big Data**	**Medtech, Digital Health and Science**
Artificial Intelligence and Automation	**Fintech**	**Mobile Tech**
COVID-19	**Global Commerce**	**Regulating Tech**

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
Moscow
New York
Nur-Sultan
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. Morgan Lewis Stamford LLC is a Singapore law corporation affiliated with Morgan, Lewis & Bockius LLP.

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. Morgan Lewis Stamford LLC is a Singapore law corporation affiliated with Morgan, Lewis & Bockius LLP.

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.