

# Before we begin: Morgan Lewis and Global Technology

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

## Web

[www.morganlewis.com/sectors/technology](http://www.morganlewis.com/sectors/technology)

## Twitter

[@MLGlobalTech](https://twitter.com/MLGlobalTech)

## LinkedIn Group

[ML Global Tech](#)

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

<b>21st Century Workplace</b>	<b>Diversity, Environment, Social Justice</b>	<b>Medtech, Digital Health and Science</b>
<b>Artificial Intelligence and Automation</b>	<b>Fintech</b>	<b>Mobile Tech</b>
<b>Cybersecurity, Privacy and Big Data</b>	<b>Global Commerce</b>	<b>Regulating Tech</b>

Morgan Lewis

**Morgan Lewis**

# **TECHNOLOGY MAY-RATHON**

**Cyberinsurance: Is Your Company Covered?**

May 20, 2021

**Mark Krotoski**

**Jeff Raskin**

© 2021 Morgan, Lewis & Bockius LLP

# Presenters



**Mark L. Krotoski**



**Jeffrey S. Raskin**

**Morgan Lewis**



# Overview

The background of the slide is a dark, almost black, space filled with a complex network of glowing lines and points. The lines are thin and radiate from a central point, creating a sense of depth and perspective. The points are small, bright spheres in various colors, including blue, purple, red, and green. The overall effect is that of a digital or data landscape, with the lines and points representing connections and data points in a network.

Morgan Lewis



# Overview

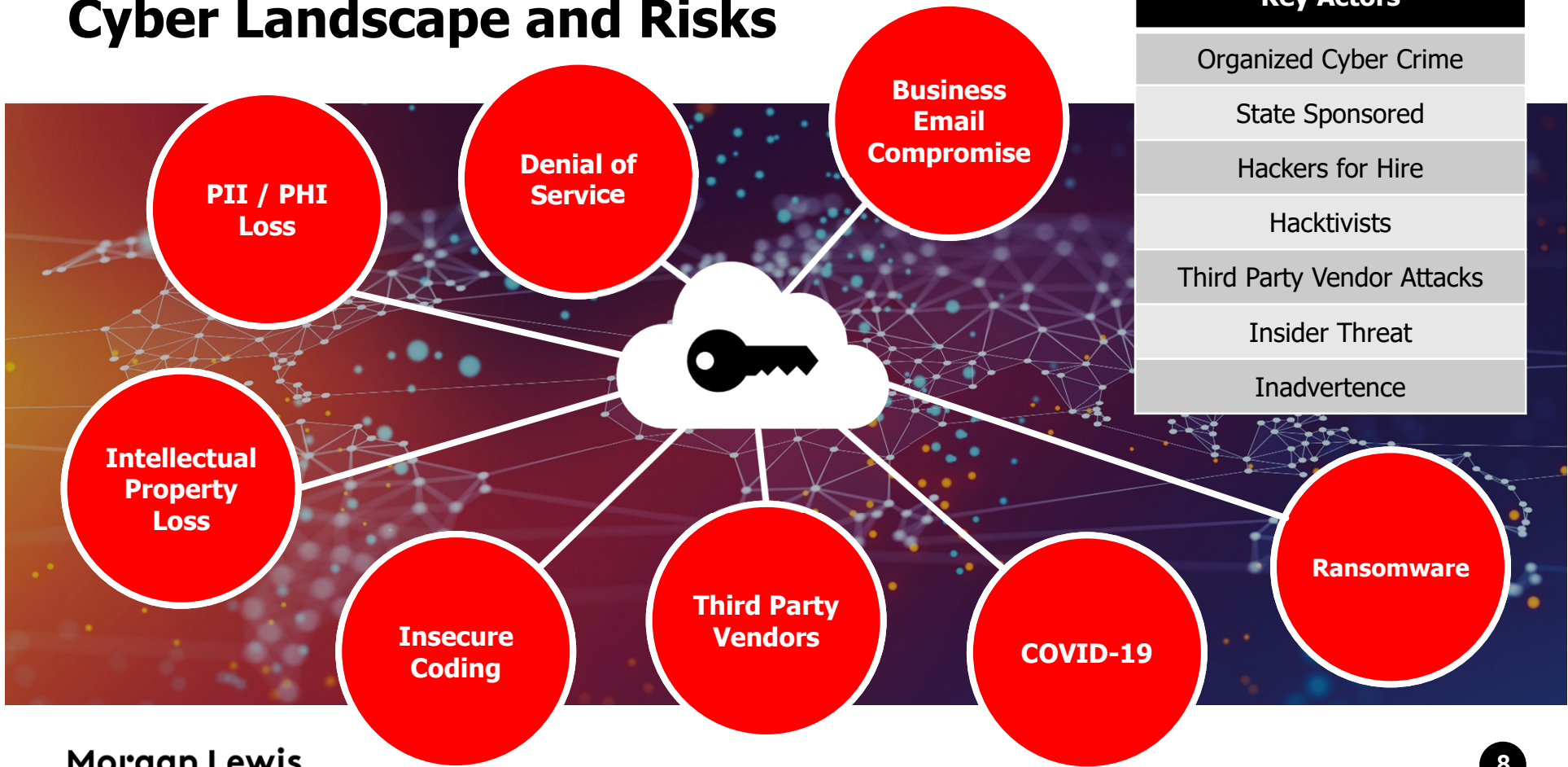
- Cyber Landscape and Risks
- Challenges in the Business Context
- Challenges in the Context of Insurance Practice
- Anatomy of an Insurance Claim



# Cyber Landscape and Risks

Morgan Lewis

# Cyber Landscape and Risks



Key Actors
Organized Cyber Crime
State Sponsored
Hackers for Hire
Hacktivists
Third Party Vendor Attacks
Insider Threat
Inadvertence



# Business Email Compromise



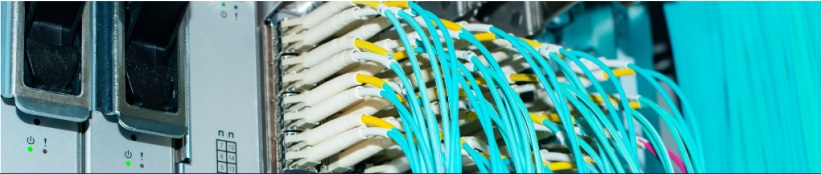
- “In **2020**, the IC3 received **19,369** Business Email Compromise (BEC)/Email Account Compromise (EAC) complaints with adjusted losses of over **\$1.8 billion**. BEC/EAC is a sophisticated scam targeting both businesses and individuals performing transfers of funds.”
  - Increased BEC losses every year since 2013.
  - US and Global Impact: Reported in all 50 states and in 177 countries.
- Past decade trend from on-site email systems to cloud-based email services.
  - Phishing emails designed to steal email account credentials and identify financial transactions in email accounts.

# New Threats

LILY HAY NEWMAN SECURITY 03.19.2020 02:12 PM

## Coronavirus Sets the Stage for Hacking Mayhem

As more people work from home and anxiety mounts, expect cyberattacks of all sorts to take advantage.



<https://www.wired.com/story/coronavirus-cyberattacks-ransomware-phishing>

ComputerWeekly.com IT Management Industry Sectors Technology Topics Search Computer Weekly

## Coronavirus now possibly largest-ever cyber security threat

The cumulative volume of coronavirus-related email lures and other threats is the largest collection of attack types exploiting a single theme for years, possibly ever

By Alex Scroxton, Security Editor Published: 18 Mar 2020 15:47

The total volume of phishing emails and other security threats relating to the Covid-19 coronavirus now represents the largest coalescing of [cyber attack](#) types around a single theme that has been seen in a long time, and possibly ever, according to Sherrod DeGrippe, senior director of threat research and detection at Proofpoint.

How to get the most out of the Internet of Things CIO Trends #7

Tailoring your IT operating model to the digital age Free Download ComputerWeekly.com

<https://www.computerweekly.com/news/252480238/Coronavirus-now-possibly-largest-ever-cyber-security-threat>

Morgan Lewis


# Various New Vulnerabilities

- Unsecure connections and networks
- Access controls
  - Authentication
  - Weak password security
- Unencrypted devices and data
- Loss of data
- Lost devices
- External access to internal resources
- Lack of physical security controls







# Example: Discovery of Phishing Email


**PREMERA** |   
BLUE CROSS

Shop for Plans ▾ Health Plan Basics ▾ Find a Doctor ▾ Pharmacy ▾ Member Services ▾ Healthsource Blog ▾

## About the Premera cyberattack



Tuesday, March 17, 2015  
About the *Experian Cyberattack* 

[Go here](#)  for information on the cyberattack involving Excellus Blue Cross Blue Shield.

On January 29, 2015, Premera Blue Cross (Premera) discovered that cyberattackers had executed a sophisticated attack to gain unauthorized access to our Information Technology (IT) systems. Our investigation further revealed that the initial attack occurred on May 5, 2014. As part of our own investigation, we notified the FBI and are coordinating with the Bureau's investigation into this attack.

- Phishing email used to install malware and compromise system
- Discovered **269 days later (nearly 9 months)**
  - May 5, 2014 initial attack
  - Jan. 29, 2015 discovery
  - March 17, 2015 public disclosure
- Affected Protected Health Information of more than 10.4 million current, former and affiliated members and employees

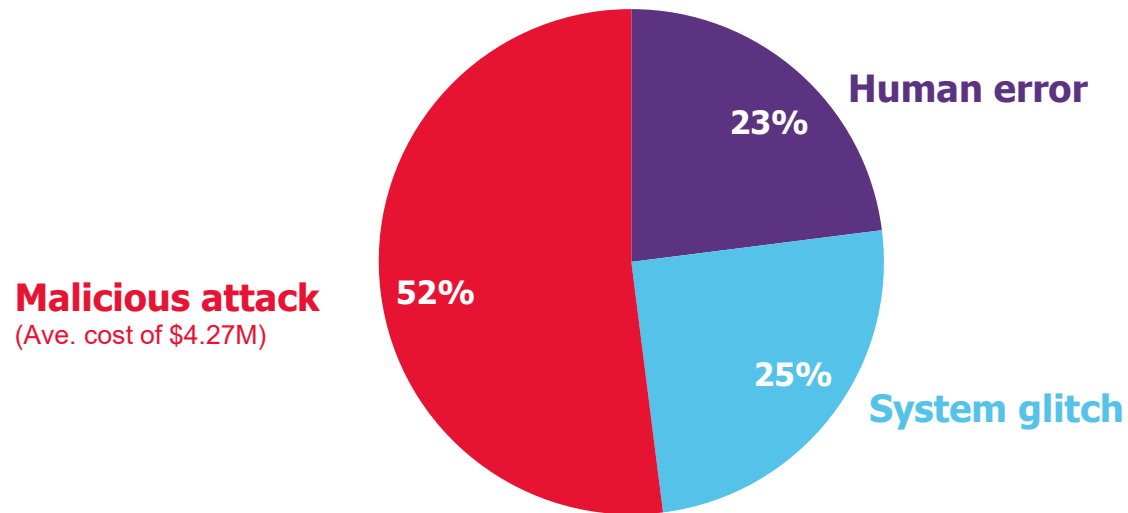
# 2020 Cost of Data Breach Report: Key Findings

- **\$3.86 million** average total cost
- Lost business costs accounted for nearly 40% of the average total cost of a data breach of \$1.52 million
  - Including increased customer turnover, lost revenue due to system downtime, and the increasing cost of acquiring new business due to diminished reputation.
- **280 days** average time to detect and contain a data breach
  - 315 days average time to detect and contain a data breach caused by a malicious attack



# Data Breach Root Cause Breakdown

Malicious attacks cause a majority of data breaches



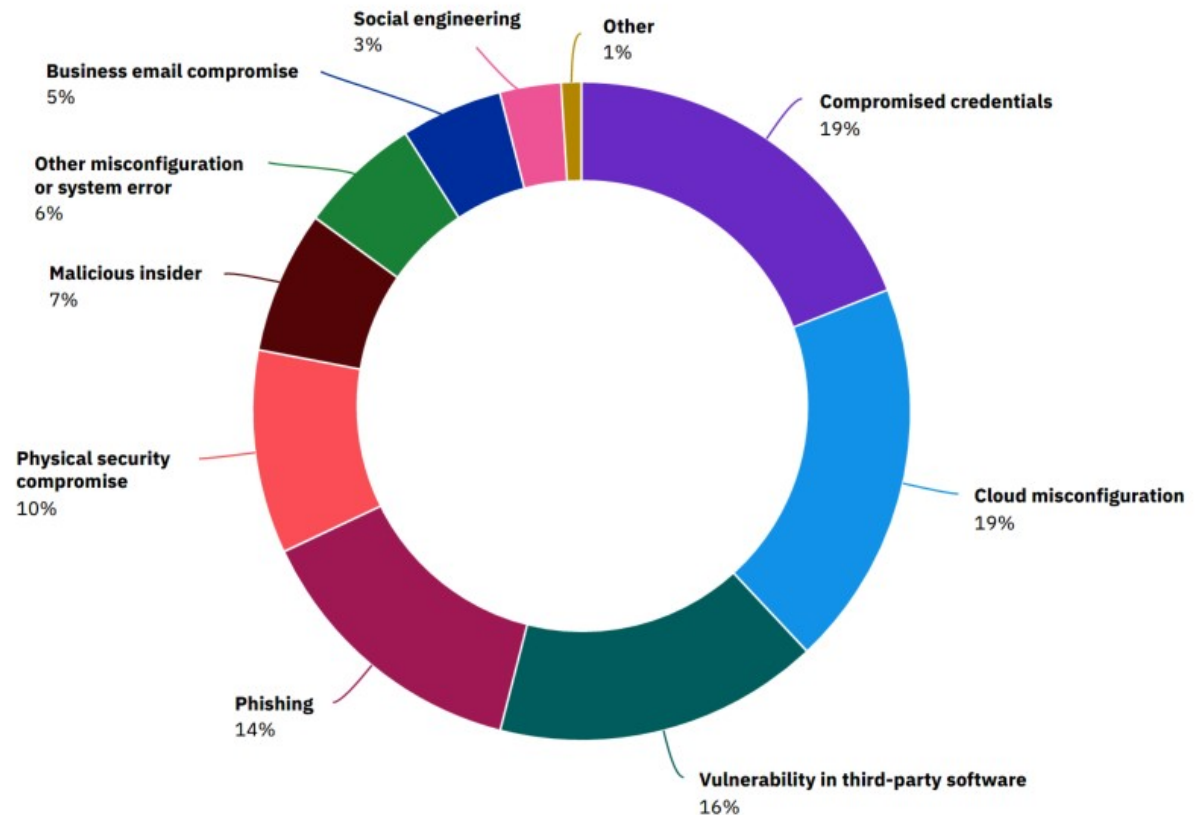
IBM Security | Cost of a Data Breach Report 2020

**Morgan Lewis**



# Breakdown of Malicious Attacks

- A majority of malicious breaches were caused by compromised credentials, cloud misconfiguration, or a third-party software vulnerability.





# Challenges in the Business Context and Context of Insurance Practice

Morgan Lewis

# The Problem in the Business Context

- Increased digitalization of the world during the pandemic resulted in:
  - Record numbers of ransomware attacks
  - Record numbers of ransomware payouts
  - Increased value of individual ransomware payouts
    - \$10 million demanded of Garmin; payout was reportedly in the seven-figures
  - Average “downtime” cost of a ransomware attack in 2020 was \$283,000, roughly double the 2019 number

“Thirty years of history have shown us that cyber risk is difficult to understand, problematic to hedge, only likely to grow, and characterized by a continually changing threat environment. Tomorrow’s cyberattacks may not look much like today’s . . .”

**Tom Johansmeyer**

*“Cybersecurity Insurance Has a Big Problem,”*

Harvard Business Review

January 11, 2021

# The Problem in the Business Context

- State-backed hackers: Approximately 18,000 companies impacted by the Solar Winds malicious software update, including multiple US government agencies
- Increasingly sophisticated ransomware variants seek not to not only freeze data, but also to *exfiltrate data*
  - Creates potential legal liability for the victim company, including mandating notification to affected individuals and regulators
- Old habits die hard
  - Approximately 65% of people reuse passwords across multiple accounts
  - 18% of Windows PCs still use Windows 7
  - Munich Re: “[R]emote work still leaves organizations unprepared to monitor or identify threats and vulnerabilities – with unauthorized remote access, weak passwords, unsecured networks, and the misuse of personal devices.”



# The Problem in the Business Context

- Cybersecurity Ventures: Global economic cybercrime costs will grow by 15% per year over the next five years, reaching \$10.5 trillion annually by 2025
- Anti-Phishing Working Group: The average loss for cyber spoofing/business email compromise was \$80,183 in 2020 Q2, up from \$54,000 from Q1.
- Results
  - Cyberinsurance market has hardened. Premiums are up 35% over last year.
  - Ransomware is the biggest driver of rate increases. The recent Colonial Pipeline attack exposed systemic vulnerabilities and likely will lead to increased demand for coverage and further rate hikes.
  - Losses are reaching excess layers of coverage, therefore reducing excess capacity.
  - Coverage restrictions, sub-limits, co-insurance, and exclusions for some or all parts of ransomware coverage are popping up.

## The Problem in the Context Of Insurance Practice

*G&G Oil Co. of Indiana, Inc. v. Continental Western Insurance Co.*,  
Indiana Supreme Court, March 20, 2021 (165 N.E.3d 82 (2021))

- G&G Oil suffered a ransomware attack on November 17, 2017
  - Company hard drives were encrypted, and one screen prompted: “To decrypt contact [email user]. Enter password.” G&G Oil believed it would have to contact the person or entity responsible for the attack to regain access.
  - After consulting the FBI and other experts, G&G Oil ultimately paid the requested ransom with four bitcoins valued at nearly \$35,000. G&G Oil thereafter regained access to its computer systems.

# The Problem in the Context Of Insurance Practice

- G&G Oil sought coverage under a commercial crime policy
  - Computer Fraud
    - “We will pay for loss or damage to ‘money’, ‘securities’ and ‘other property’ *resulting directly* from the use of any computer to *fraudulently cause a transfer* of that property from inside the ‘premises’ or ‘banking premises’:
      - a) To a person (other than a “messenger”) outside those ‘premises’; or
      - b) To a place outside those ‘premises’.”
- Continental denied the claim because it believed the Bitcoin was voluntarily transferred by G&G Oil to the computer hacker, and therefore the hacker did not “transfer funds directly” from G&G Oil.

# The Problem in the Context Of Insurance Practice

- After discussing the case and consulting dictionary definitions, the court concluded that the term “fraudulently cause a transfer” can be reasonably understood as simply “to obtain by trick.”
  - Neither party was entitled to summary judgment on this issue:
    - In its proof of loss statement to the insurer, G&G Oil stated: “It is our belief that the hijacker hacked into our system via a targeted spear-phishing email with a link that led to a payload downloading to our system and propagating through our entire network . . .”
    - The court: “We do not think every ransomware attack is necessarily fraudulent. For example, if no safeguards were put in place, it is possible a hacker could enter a company’s servers unhindered and hold them hostage. There would be no trick there. G&G Oil’s *belief* of a spear-phishing campaign does not entitle it to summary judgment.” (emphasis original)
    - The court: “Nor is summary judgment appropriate for Continental . . . [T]here is a question as to whether G&G Oil’s computer systems were obtained by trick. Though little is known about the hack’s initiating event, enough is known to raise a reasonable inference the system could have been obtained by trick.”



## The Problem in the Context Of Insurance Practice

- The court then examined whether G&G Oil's loss "resulted directly from the use of a computer."
  - Prior decisions: "The word 'direct' means, among other things, immediate; proximate; without circuitry."
  - The court: In order to obtain coverage under this provision, G&G Oil must demonstrate that its loss "resulted either 'immediately or proximately without significant deviation from the use of a computer.' We think that G&G Oil has satisfied that definition."
  - The court: G&G Oil's 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 made only after consulting with the FBI and other computer tech services.
  - The court: Without access to its computer files, G&G Oil reasonably 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 under duress. Under those circumstances, the 'voluntary' payment was not so remote that it broke the causal chain."

# Anatomy of an Insurance Claim

The background is a dark, abstract digital landscape. It features a grid of glowing lines that recede into the distance, creating a sense of depth. The lines are primarily blue and purple, with some red and orange accents. At the end of each line is a small, bright dot, resembling a star or a data point. The overall effect is that of a futuristic, data-driven environment.

Morgan Lewis

# Anatomy of a Claim

## First Step

- Notify the insurer (or insurers) of an incident or a claim that may be covered under the policy or policies “as soon as is practicable.”
- The policy will identify the information that the insurer wants to receive with the initial notice. Sometimes, this might simply be stated as “full details.”
- The insured usually does *not* need to specify the coverage in the policy that it believes is applicable.
- A sworn “proof of loss” likely will be required within a specified period for claims involving the theft of money, such as “social engineering fraud” (business email compromise), funds transfer fraud, telecommunications fraud, etc. Recovery for these claims usually requires notification of law enforcement and an attempt to reverse the loss or recover from a financial institution or telecommunications provider.
- Identify and retain previously “approved” providers, or providers that could readily obtain insurer approval, to assist with legal, forensic, and public relations issues.

# Ransomware Scenario

- Network Access
  - Phishing
  - Remote Desktop Protocol
  - Attachments
  - Surveillance, command and control
  - Disable anti-virus or other defenses
- Encrypt or Lock Computer Files
  - Usually search and encrypt file types
  - Normally does not search content
- Demand Payment
  - Usually in bitcoin
  - Urgency
  - Threats to release or destroy data





# Payment?

## RANSOMWARE

What It Is and What To Do About It



### WHAT IS RANSOMWARE?

Ransomware is a type of malicious software cyber actors use to deny access to systems or data. The malicious cyber actor holds systems or data hostage until the ransom is paid. After the initial infection, the ransomware attempts to spread to shared storage drives and other accessible systems. If the demands are not met, the system or encrypted data remains unavailable, or data may be deleted.

### HOW DO I PROTECT MY NETWORKS?

A commitment to cyber hygiene and best practices is critical to protecting your networks. Here are some questions you may want to ask of your organization to help prevent ransomware attacks:

1. **Backups:** Do we backup all critical information? Are the backups stored offline? Have we tested our ability to revert to backups during an incident?
2. **Risk Analysis:** Have we conducted a cybersecurity risk analysis of the organization?
3. **Staff Training:** Have we trained staff on cybersecurity best practices?
4. **Vulnerability Patching:** Have we implemented appropriate patching of known system vulnerabilities?
5. **Application Whitelisting:** Do we allow only approved programs to run on our networks?
6. **Incident Response:** Do we have an incident response plan and have we exercised it?
7. **Business Continuity:** Are we able to sustain business operations without access to certain systems? For how long? Have we tested this?
8. **Penetration Testing:** Have we attempted to hack into our own systems to test the security of our systems and our ability to defend against attacks?

### HOW DO I RESPOND TO RANSOMWARE?

**Implement your security incident response and business continuity plan.** It may take time for your organization's IT professionals to isolate and remove the ransomware threat to your systems and restore data and normal operations. In the meantime, you should take steps to maintain your organization's essential functions according to your business continuity plan. Organizations should maintain and regularly test backup plans, disaster recovery plans, and business continuity procedures.

**Contact law enforcement immediately.** We encourage you to contact a local FBI<sup>1</sup> or USSS<sup>2</sup> field office immediately to report a ransomware event and request assistance.

**There are serious risks to consider before paying the ransom.** We do not encourage paying a ransom. We understand that when businesses are faced with an inability to function, executives will evaluate all options to protect their shareholders, employees, and customers. As you contemplate this choice, consider the following risks:

- Paying a ransom does not guarantee an organization will regain access to their data; in fact, some individuals or organizations were never provided with decryption keys after having paid a ransom.
- Some victims who paid the demand have reported being targeted again by cyber actors.
- After paying the originally demanded ransom, some victims have been asked to pay more to get the promised decryption key.
- Paying could inadvertently encourage this criminal business model.

"We do not encourage paying a ransom.

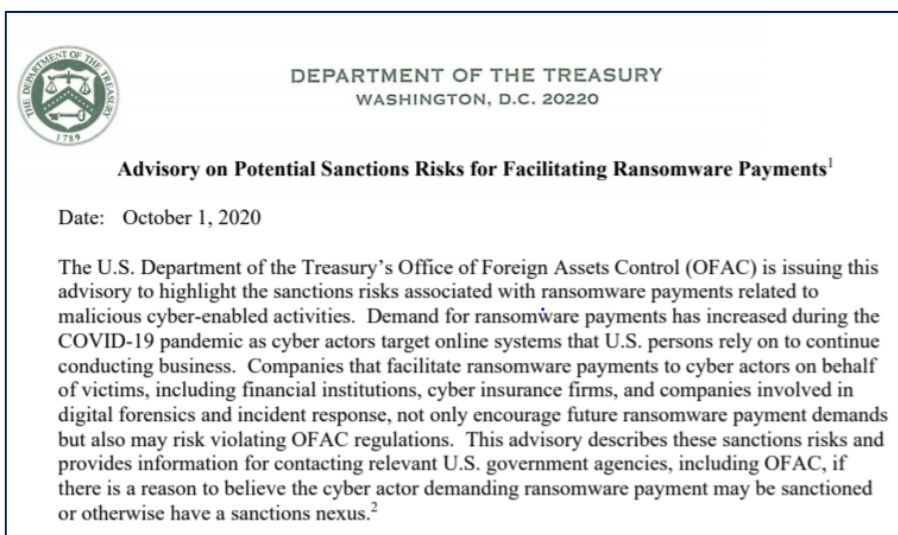
As you contemplate this choice, consider the following risks:

- Paying a ransom does not guarantee an organization will regain access to their data; in fact, some individuals or organizations were never provided with decryption keys after having paid a ransom.
- Some victims who paid the demand have reported being targeted again by cyber actors.
- After paying the originally demanded ransom, some victims have been asked to pay more to get the promised decryption key.
- Paying could inadvertently encourage this criminal business model."

# US Department of the Treasury's Office of Foreign Assets Control (OFAC) Advisory



- U.S. persons are generally prohibited from engaging in transactions, directly or indirectly, with individuals or entities ("persons") on OFAC's **Specially Designated Nationals and Blocked Persons List (SDN List)**, other blocked persons, and those covered by comprehensive country or region embargoes (e.g., Cuba, the Crimea region of Ukraine, Iran, North Korea, and Syria)."
- "OFAC may impose civil penalties for sanctions violations based on **strict liability**, meaning that a person subject to U.S. jurisdiction may be held civilly liable even if it did not know or have reason to know it was engaging in a transaction with a person that is prohibited under sanctions laws and regulations administered by OFAC."



# Potentially Available Coverages

## Ransomware/Network Extortion

- Definition of Network Extortion
  - Credible threat or series of threats to:
    - Attack or continue an attack on an insured's network
    - Disclose private, proprietary, or confidential information obtained via unauthorized access to the insured's network
    - Commit cyberterrorism
    - Refuse to return or unencrypt the insured's digital assets
- Coverage provided
  - Necessary costs and expenses recommended by an "approved" provider for:
    - Services to avoid, defend, or preclude a network extortion
    - Money or securities sought or demanded as a result of a network extortion
  - Insurer consent required to incur expenses or pay money to the extortionists

# Cyber Coverage

**Cyber  
Extortion:  
Two possible  
coverages:**

The policy will cover an extortion payment, made with insurer consent, in response to a threat to (a) alter or destroy data; (b) perpetrate unauthorized access to systems; (c) prevent access to systems and or/data; (d) steal or misuse personally identifiable information; (e) introduce malware into the system; (f) interrupt or suspend the system.

Or the policy will cover reasonable and necessary expenses, incurred with insurer consent, to prevent or respond to an extortion threat.

# Incident Response Coverage

- Covers services or expenses due to a network security and privacy wrongful act
  - Network security and privacy wrongful act includes any actual, alleged, or reasonably suspected:
    - Unauthorized access to, disclosure, accidental release of, or failure to protect private information
    - Breach of security of a network resulting in:
      - Unauthorized access to, use of or tampering with a third-party network
      - Failure to provide an authorized third-party access to the insured's services
      - Failure to prevent the transmission of a computer virus, ransomware, or malicious code to a third-party



# Incident Response Coverage

- Covers services or expenses due to a network security and privacy wrongful act
  - Benefits payable
    - **Breach consultation costs:** The costs necessary to determine whether the insured must comply with breach notification laws, notify affected persons, and report to regulatory authorities
    - **Data Forensics:** Necessary costs and expenses incurred by an approved provider for services to determine the cause and extent of a network security and privacy wrongful act
    - **Breach response costs:** (1) costs of notifying affected persons provided that private information was at least reasonably believed to have been disclosed to an unauthorized person, (2) establishment of a call center for a reasonable period of time to provide information to persons whose private information was disclosed or was reasonably believed to have been disclosed to an unauthorized person, (3) up to two years of triple bureau credit monitoring, credit freezing, credit thawing, identity theft resolution, identity restoration, and the purchase of identity theft insurance for affected persons.
    - **Public relations costs:** The costs and expenses incurred by an approved provider for public relations and crisis communications to protect, restore, or mitigate harm to the insured.

# State Data Breach Notification Laws

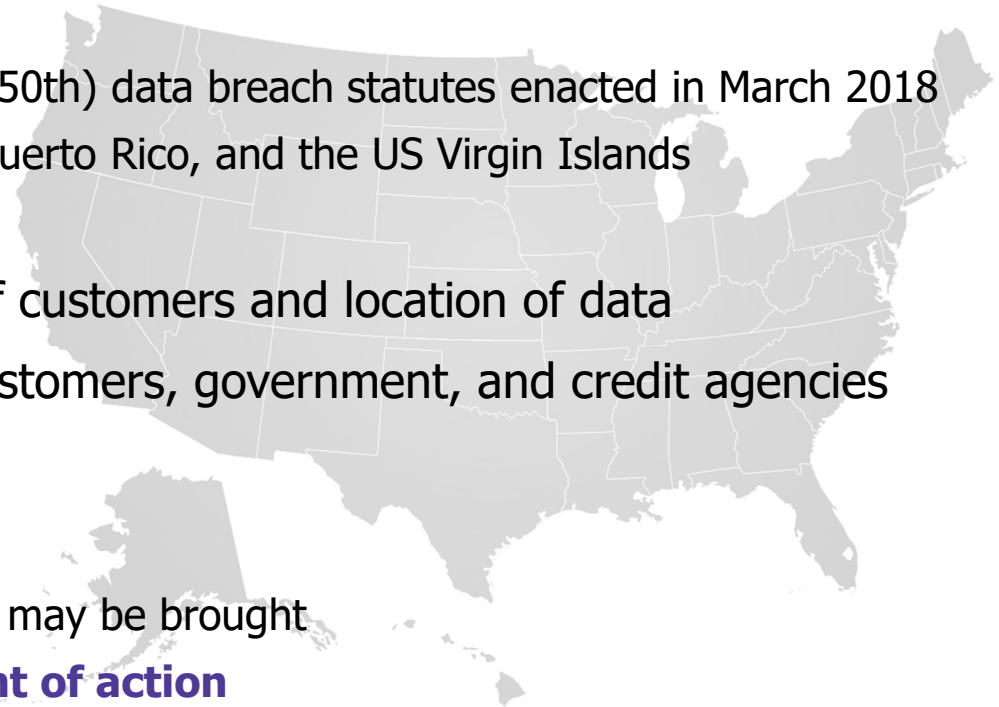
- **54 US Jurisdictions**

- South Dakota (49th) and Alabama (50th) data breach statutes enacted in March 2018
- Also: District of Columbia, Guam, Puerto Rico, and the US Virgin Islands

- State law depends on residency of customers and location of data
- Notification may be required to customers, government, and credit agencies

- Enforcement and Actions

- Separate **AG enforcement action** may be brought
- Some States provide a **private right of action**



# Examples of Disparate Data Elements in Current Data Breach Statutes

DATA ELEMENT	JURISDICTION
Birth certificate	South Dakota and Wyoming
Marriage certificate	Wyoming
Challenge questions	South Dakota
Date of birth	North Dakota, Texas, and Washington
Digital signature	North Carolina and North Dakota
DNA profile	Delaware and Wisconsin
Information or data collected through the use or operation of an automated license plate recognition system	California
Password	Georgia, Maine, North Carolina, and South Dakota
Financial account password	Alaska
Maiden name of the individual's mother	North Dakota and Texas

<https://www.law360.com/articles/1210779/next-steps-for-cos-in-light-of-new-calif-privacy-laws>

Morgan Lewis

# Data Restoration Coverage

- Covers digital asset restoration costs due to a network security and privacy wrongful act
  - The necessary costs recommended by an approved provider to replace, restore, or recollect digital assets (from written records or from partial or fully matching electronic records) due to their corruption, deletion, or destruction resulting from a network security and privacy wrongful act
  - If the assets cannot be replaced, restored, or recollected, the insurer will pay the costs incurred to reach this determination.

# Business Interruption Coverage

- Payable when there has been:
  - An actual and measurable interruption, suspension or failure of the insured's network resulting from a network attack, including the purposeful interruption of the network by the insured reasonably necessary to mitigate the effects of a network attack
    - Network attack: (1) unauthorized access to or use of a network, (2) intentional attack of a network, including denial of service, (3) introduction of malicious code which could destroy, contaminate, corrupt or degrade the quality or performance of a network or the software or electronic data stored on the network.
  - An unintentional or unplanned outage of a network resulting from a cause other than a network attack



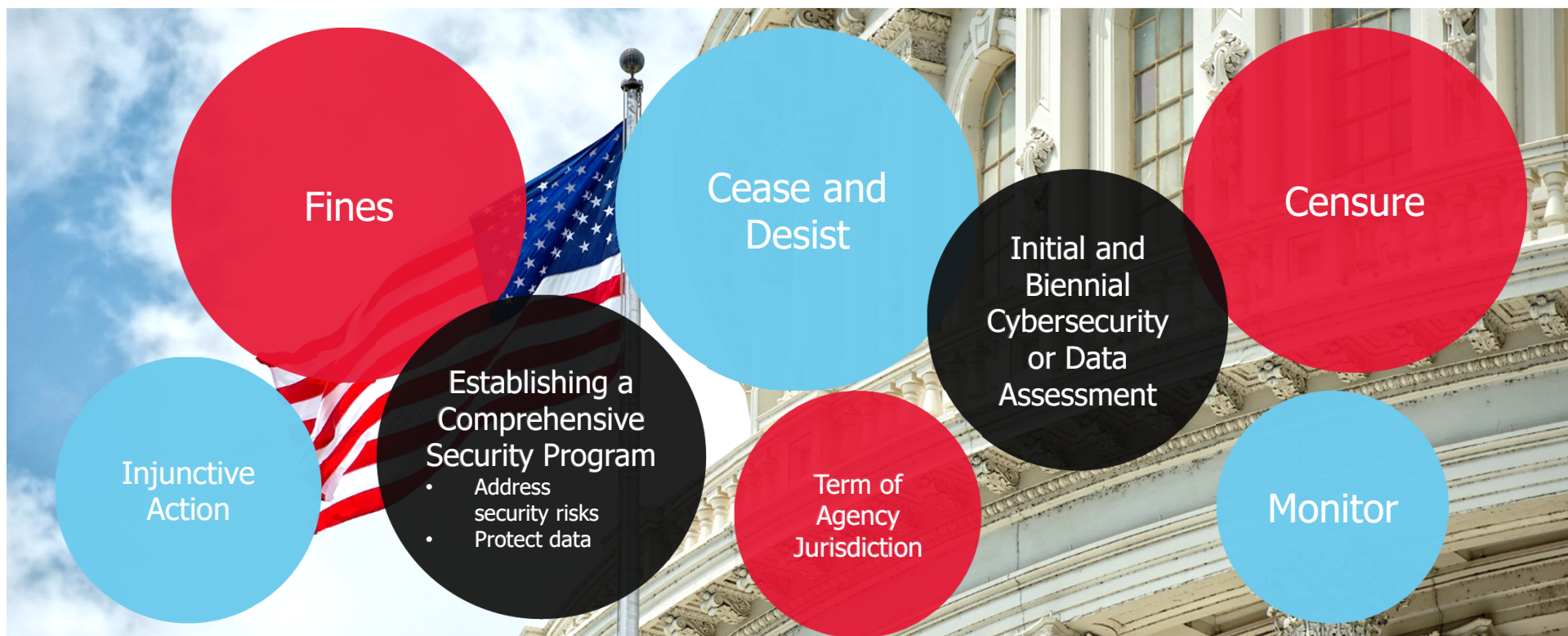
# Business Interruption Coverage

- Benefits payable
  - Net profit or loss before interest and tax the insured would have earned or incurred or which the insured would have avoided but for an interruption in service.
  - Extra operating expenses
- Benefits payable during the “period of restoration” – the time when the insured does, or reasonably could, resume business operations substantially to the level that existed before the interruption or a specific time stated in the policy (often 120 days), whichever is less.

# Cyber Crime Coverages

- Social engineering fraud: Unauthorized and fraudulent instruction by a person falsely purporting to be a vendor, client, employee or executive officer of the insured with the intention of misleading the insured into transferring money or securities to a fraudulent account.
- Funds transfer fraud: Unauthorized and fraudulent instruction by a third-party directing a financial institution to transfer, pay or deliver money or securities from an insured's account without the insured's authorization or consent.
- Telecommunications fraud: Unauthorized access to or use of the insured's telecommunication system by a third-party that results in unauthorized charges to the insured.
- Computer Fraud (crime policies): Covers loss of money, securities or other property "resulting directly" from the use of a computer from inside the insured's premises, or a banking premises, to a person (other than a messenger) or place outside of the insured's premises.

# Government Agency Enforcement Actions



# CCPA Attorney General Enforcement



- **Attorney General Civil Enforcement Action**
  - Not more than \$7,500 for each intentional violation of the CCPA
  - \$2,500 for unintentional violations that the company fails to cure within 30 days of notice
  - Injunctive relief
  - New Consumer Privacy Fund
    - 20 percent of the collected UCL penalties allocated to a new fund to “fully offset any costs incurred by the state courts and the Attorney General”
    - 80 percent of the penalties allocated “to the jurisdiction on whose behalf the action leading to the civil penalty was brought”

# CCPA Private Right of Action

- Limited Consumer Private Right of Action
  - Individual consumer or classwide basis
  - Only to data breaches, but proposed legislation looks to expand the private right of action to violations of the privacy requirements.
    - 1) Nonencrypted or nonredacted **personal information**\*
    - 2) “subject to an unauthorized access and exfiltration, theft, or disclosure
    - 3) as a result of the business’s violation of the duty to implement and maintain **reasonable security** procedures and practices appropriate to the nature of the information to protect the personal information”

# Statutory Damages Range

- Court imposes the **greater of statutory or actual damages**
- **Statutory Damage Range**
  - Statutory damages are “not less than” \$100 and “not greater than” \$750 “per consumer per incident”
- **Statutory Damages Factors**
  - Nature and seriousness of the misconduct
  - Number of violations
  - Persistence of the misconduct
  - Length of time over which the misconduct occurred
  - Willfulness of the defendant’s misconduct
  - Defendant’s assets, liabilities, and net worth
  - Other “relevant circumstances presented by any of the parties”

[Cal. Civil Code § 1798.150(a)(2)]

# Regulatory Proceeding/CCPA Coverage

- Definition of “regulatory proceeding”
  - Request for information, civil investigative demand or civil proceeding commenced by the service of a complaint or similar proceeding
    - By the Federal Trade Commission, Federal Communications Commission, or any federal, state, local or foreign governmental entity in the entity’s regulatory or official capacity in connection with a proceeding arising out of a security failure or data breach.
  - Proceeding alleging a violation of the CCPA, the EU’s General Data Protection Regulation or similar federal, state, local, or foreign regulation arising from a privacy liability.



## Key Points

- Do you have the coverage you need based on your risk assessment and circumstances?
- Insurers are likely to embed the underwriting process with new controls. It likely will be longer, more detailed and involve third-party vendors/consultants assessing the vulnerabilities of prospective insureds.
- Insurers will want to work increasingly closely with insureds to make sure that “best practices” are in place to protect against potential attacks and other types of data breaches.
- Coverage options and amounts vary significantly. Subtle wording differences can mean the difference between a claim being paid and a claim being denied.
- Cyberpolicies and crime policies should be assessed in tandem to make sure potential coverage gaps do not arise.

# Questions

An abstract digital landscape with a dark background. The foreground is a grid of glowing lines in various colors (blue, purple, red, green) that recede into the distance. Numerous vertical lines of varying heights rise from the grid, each topped with a small, glowing point of light in the same color as the line. The overall effect is a sense of depth and digital connectivity.

Morgan Lewis

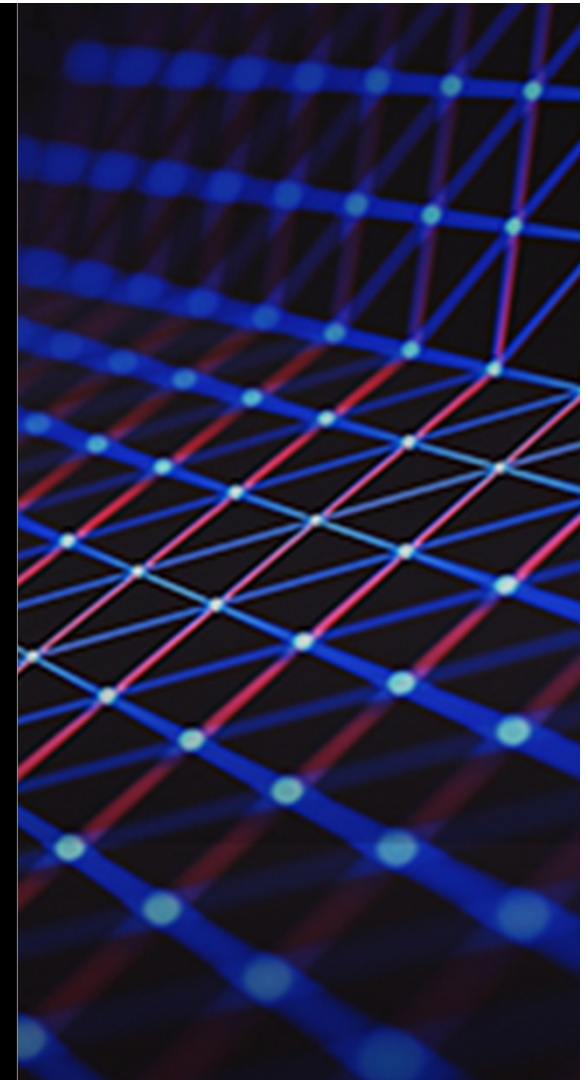
# Coronavirus COVID-19 Resources

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.

**Morgan Lewis**

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](http://www.morganlewis.com/topics/coronavirus-covid-19)

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



# Mark L. Krotoski



## **Mark L. Krotoski**

Silicon Valley

Washington DC

+1.650.843.7212

+1.202.739.5024

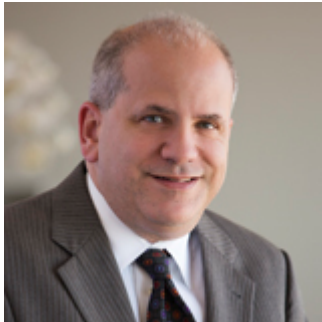
[mark.krotoski@morganlewis.com](mailto:mark.krotoski@morganlewis.com)

## **Litigation Partner, Privacy and Cybersecurity and Antitrust practices**

- Co-Head of Privacy and Cybersecurity Practice Group
- More than 20 years' experience handling cybersecurity cases and issues
- Assists clients on litigation, mitigating and addressing cyber risks, developing cybersecurity protection plans, responding to a data breach or misappropriation of trade secrets, conducting confidential cybersecurity investigations, responding to regulatory investigations, and coordinating with law enforcement on cybercrime issues.
- Variety of complex and novel cyber investigations and cases
  - At DOJ, prosecuted and investigated nearly every type of international and domestic computer intrusion, cybercrime, economic espionage, and criminal intellectual property cases.
  - Served as the national coordinator for the Computer Hacking and Intellectual Property (CHIP) Program in the DOJ's Criminal Division, and as a cybercrime prosecutor in Silicon Valley, among other DOJ leadership positions.



## Jeffrey S. Raskin



### **San Francisco**

San Francisco

+1.415.442.1219

[jeffrey.raskin@morganlewis.com](mailto:jeffrey.raskin@morganlewis.com)

Jeffrey S. Raskin advises clients in litigation, mediation, and arbitration around insurance coverage matters, and intellectual property, commercial, real estate, and environmental disputes. Head of Morgan Lewis's Insurance Recovery Practice in the San Francisco office, Jeffrey counsels clients seeking recovery for catastrophic losses in securities, environmental, asbestos, silica, toxic tort, product liability, intellectual property, and employment practices cases. Jeffrey has handled first-party claims for loss covered by policies for physical damage and business interruption, title, and fidelity and crime.



## 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

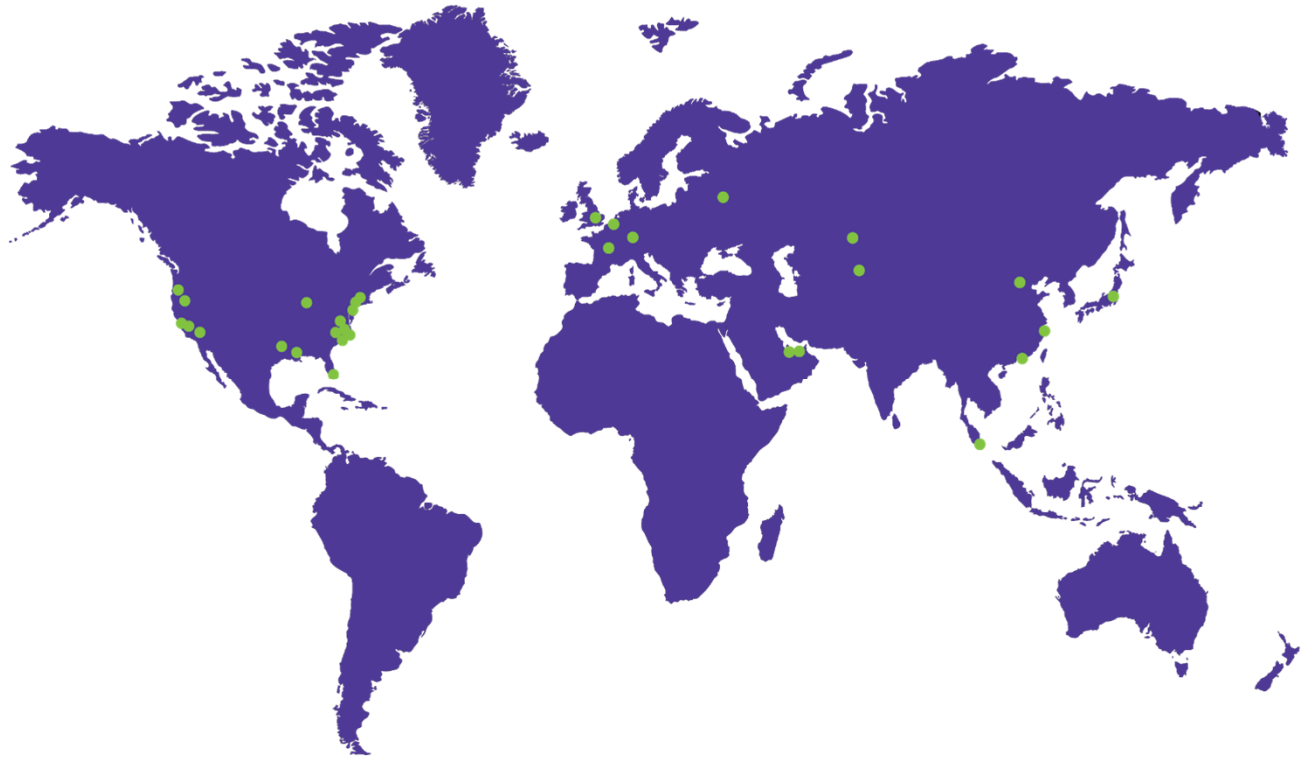
Silicon Valley

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 & Bockius is a separate Hong Kong general partnership registered with The Law Society of Hong Kong. Morgan Lewis Stamford LLC is a Singapore law corporation affiliated with Morgan, Lewis & Bockius LLP.

# THANK YOU

© 2021 Morgan, Lewis & Bockius LLP  
© 2021 Morgan Lewis Stamford LLC  
© 2021 Morgan, Lewis & Bockius UK LLP

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 & Bockius is a separate Hong Kong general partnership registered with The Law Society of Hong Kong. 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.

**Morgan Lewis**