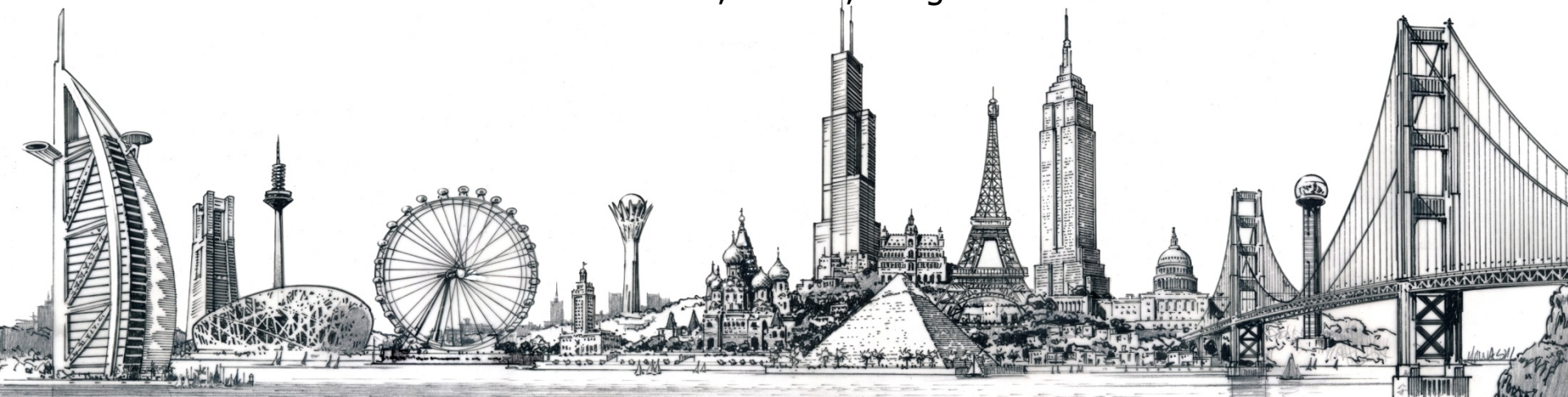
Morgan Lewis Privacy Panacea

WHAT TO DO *BEFORE* YOU EXPERIENCE A SECURITY BREACH: INCIDENT RESPONSE PLANS AND OTHER PREVENTIVE MEASURES

SF ISACA Education Event
May 19, 2015

Sharon A. Anolik, President, Privacy Panacea

Reece Hirsch, Partner, Morgan Lewis



Data Security as a Front-Burner Issue

- Each year it becomes more and more clear that data security is a critical legal compliance issue
- A recent survey report from Experian Data Breach Resolution and the Ponemon Institute lists data breach "among the top three occurrences that affect a company's reputation"
- However, in a recent FTI Consulting survey, 27% of directors said their company did not have a written security breach response plan; 31% weren't sure
- Breach response planning is an area where many companies have not yet appropriately addressed their risk

A Question of Trust

- Failure to appropriately address privacy and security compliance is a bottom-line issue for companies because
  - Privacy is personal
  - Privacy goes right to the heart of a consumer's relationship with a company
  - No company can have perfect security and breaches are inevitable
  - Privacy and security regulatory enforcement and litigation are on the rise

The Worst Case Scenario

- Most security breaches are garden-variety incidents that do not pose significant risks if properly handled
- A major security breach that results in actual damages can lead to:
  - Class action lawsuits
  - Drop in stock price for public companies
  - Regulatory action by state Attorneys General or other regulators
  - DAMAGE TO BRAND AND CUSTOMER RELATIONSHIPS

The Retail Sector Responds

- Of the 100 largest U.S. retailers, 91 have cited risk factors related to security breaches in their regulatory filings
- May 2014: Retail Industry Leaders Association announced that Target, J.C. Penney and other prominent retailers have launched an organization to prevent cyberattacks
  - Retail Cyber Intelligence Sharing Center permits retailers to share cyber threat information among themselves and with Dept. of Homeland Security, Secret Service and FBI

The First Line of Defense Against Breaches: Data Security Compliance Programs

- Privacy has long been a subject of state and federal legislation, but data security laws are a relatively recent development
- It is becoming increasingly clear that development of a formal, written data security compliance programs is a best practice
- Under a patchwork of state and federal laws, they are also often required

"Proactive" Data Security Laws

- The HIPAA Security Rule
  - Now applicable to business associates pursuant to the HITECH Act
- Gramm-Leach-Bliley "safeguards" regulations
- State insurance privacy law "safeguards" measures
- General state security mandates in Massachusetts, Nevada, California, Connecticut, Rhode Island, Oregon and Maryland

"Reactive" Security Breach Notification Laws

- Part of trend that started in 2005 after ChoicePoint incident
- 47 states (plus D.C., Puerto Rico and Virgin Islands) have security breach notification laws (most recently KY)
- Many of the laws incentivize use of encryption by providing that notification is not required for a breach involving encrypted data
- Increased legislative activity to broaden state security breach notification laws (FL, MN, CA)
  - Example: New FL law requires notification within 30 days
  - May reflect lack of confidence in passage of federal legislation

HIPAA Breach Notification Rule

- HITECH Act created new breach notification rules for the healthcare industry, requiring covered entities (CEs) to notify affected individuals, the Secretary of HHS and, in some instances, the media following discovery of a breach of unsecured PHI

- Business associates (BAs) are also required to notify CEs of a breach of unsecured PHI occurring at or by the BA

HIPAA Low Probability of Compromise Standard

- The HIPAA Final Rule (effective Sept. 23, 2013) defines a "breach" as:
  - Generally, the unauthorized acquisition, access, use or disclosure of PHI that compromises the privacy or security of that information
  - There is an express presumption that an impermissible use or disclosure is considered to be a breach UNLESS
    - The CE or BA is able to demonstrate that there is a "low probability" that the PHI has been compromised

Breach Risk Assessment Factors

- The Final Rule identifies 4 factors to consider when performing a risk assessment to determine whether there is a low probability of compromise
- Evaluate the nature and extent of the PHI involved
  - Type of PHI, types of identifiers, likelihood of re-identification
- Consider the individual who impermissibly used the PHI or to whom the impermissible disclosure was made
  - Was disclosure made to a CE? To a fraudster?

Breach Risk Assessment Factors (cont.)

- Investigate whether the PHI was actually acquired or viewed or if only the *opportunity* existed for information to be acquired or viewed
  - Forensic analysis of stolen laptop
- Consider the extent to which the risk to PHI has been mitigated
  - Did the recipient certify that the PHI was not further used or disclosed, and was destroyed?

Learning from HIPAA

- Even businesses that are not regulated by HIPAA can take lessons from HIPAA's approach to breach response
  - More detailed than any state law
  - In many ways reflects best practices, such as:
    - Documenting risk assessment of incidents
    - Mandating information to be provided by vendors to customers regarding breach
    - Mandating contractual safeguards imposed on vendors
    - Requiring written breach response policies and procedures

Cybersecurity

- On Feb. 12, 2014, the Obama administration released the final version of a much-anticipated voluntary cybersecurity framework
  - Developed by the National Institute of Standards and Technology (NIST) in collaboration with stakeholders
  - At the direction of Pres. Obama's executive order one year prior
  - Focuses on protection of "critical infrastructure"

Critical Infrastructure Defined

- "Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets could have a debilitating impact on cybersecurity, national economic security, national public health or safety, or any combination of those matters"
- Transportation, financial services, energy and utilities, government and the public Internet qualify
- Applicability to other industries, such as healthcare, is still uncertain

Enabling and Incentivizing Adoption

- The DHS Critical Infrastructure Cyber Community Voluntary (C3) program will assist stakeholders in understanding the framework and support development of sector-specific guidance

- At present there are no incentives for compliance, but there has been discussion about tying the framework to benefits such as liability protections, grants, cyberinsurance and government contracts

The Framework

- The framework borrows from existing industry security standards and encourages organizations in the critical infrastructure sector to
  - Map out a "current profile" of cyberattack readiness
  - Pinpoint a "target profile" that reflects readiness based on an analysis of the likelihood and impact of a cybersecurity event
  - Identify "gaps" between the profiles
  - Implement an action plan to address those gaps

Beyond Critical Infrastructure

- Any company experiencing a cybersecurity event will want to be able to demonstrate that its security practices are consistent with the framework – regardless of industry sector
- Dovetails with other legal trends supporting the adoption of formal security compliance programs
- The framework should prompt increased focus on cybersecurity in US corporations at the senior executive level
- October 2011: SEC Division of Corporate Finance released cybersecurity risk and incident disclosure guidance

Privacy By Design

- March 2012: FTC releases a set of recommendations for businesses and Congress about collection and use of consumer personal information
- "Privacy by design" is central to the FTC's recommendations
  - The philosophy of embedding privacy from the outset into the design specifications of information technologies, accountable business processes, physical spaces and network infrastructures
- Avoiding "embarrassment by design"
- Tough to correct architectural deficiencies after rollout

PbD: Baking In Privacy Protections

- PbD represents a proactive, holistic approach to protecting the privacy of individuals
- Contrasts with the reactive approach associated with traditional privacy frameworks, which focus on:
  - Minimum standards for information practices
  - Remedies for privacy breaches after breaches have occurred and harm has been done
- Ontario Information and Privacy Commissioner Ann Cavoukian has been a major proponent of this concept since the 1990s

FTC's PbD Enforcement

- February 2013: FTC settles charges with mobile device manufacturer HTC America that it failed to take reasonable steps to secure the software it developed for smartphones and tablet computers
- FTC cites "permission re-delegation" issues
  - User consents to App A's use of geolocation data, but App A then shares with App B without user permission
- Settlement included comprehensive security program, conducting independent audits and reporting to the FTC for 20 years, and developing required security patches

Incorporating PbD

- Several FTC enforcement actions focus on use of default settings in collecting or sharing personal information
- Companies that design and market products capable of collecting, storing, accessing or transmitting personal information should carefully review data flows
  - Are they consistent with
    - Product descriptions?
    - Legal requirements?
    - User expectations?
    - Posted privacy policies?

Best Preventive Medicine for Breaches: A Security Compliance Program

- The best way to avoid breaches is through rigorous data security, demonstrated and documented through a formal, written security compliance program
- Companies should develop security programs in light of all applicable legal standards, including
  - State security and security breach notification laws
  - HIPAA Security and Breach Notification Rules
  - FTC guidance
  - Cybersecurity Framework
  - Privacy (and security) by design

Recommended Steps

- As part of overall oversight of risk management, a CEO should report regularly to the board on the company's security risk profile and related internal information governance systems
- Companies should develop a security strategy under the direct supervision of a C-level officer
- In addition to protecting personal information, companies should consider how their trade secret and IP could be better protected in light of domestic and foreign cyber threats

Security Breach Response

- The drumbeat of major security breaches continues
- Cybercriminals are increasingly sophisticated, targeting large databases of customer information
  - Often seeing export of data to URLs in China, Russia
  - Corporate trade secrets and IP are increasingly a target
- Review of major recent security breaches

Security Breach Incident Response Plan

- A key component of a security compliance program is a security breach response plan
- Often developed as a stand-alone module distinct from security policies and procedures
  - More than just a technical, systems document, requires input from legal, compliance and others
  - Includes employee-facing components

My company just experienced a massive security breach – and we have no breach response plan!

Incident Response Plans

- An effective incident response plan should:
  - Establish an incident response team with representatives from key areas of the organization
  - Identify necessary external resources in advance (forensic IT consultant, mailing vendor, call center operator, credit monitoring service)
  - Provide for training of rank-and-file personnel to recognize and report security breaches
  - Outline media relations strategy and point person

The Incident Response Team Leader

- There should be an incident team leader
  - Often an attorney or Chief Privacy Officer
  - Manages overall response
  - Acts as liaison between management and incident response team members
  - Coordinates responsibilities of team members
  - Develops project budgets
  - Ensures that systemic issues brought to light by a breach are addressed going forward

The Incident Response Team

- Because of the far-reaching impact of a significant breach, the Incident Response Team should include representatives from
  - Management
  - IT & Security
  - Legal
  - Compliance/Privacy
  - Public relations

The Incident Response Team (cont.)

- Customer care
- Investor relations (for public companies)
- Human resources
- External legal counsel (as appropriate)
- Data breach resolution provider (as appropriate)

Meet During Peacetime

- No incident response team should be forced to learn their roles on the fly during a breach
  - Meet in peacetime
  - Understand the steps outlined in the breach response plan and each team member's role and responsibility
  - Run scenarios in advance
    - What does your company's worst-case scenario look like?
    - Is your company protected from potential breach liabilities through indemnification? Cyberinsurance?
    - How likely is it that breach damages might exceed contractual limitations of liability? Insurance liability limits?

Training

- Incident response plan should include a module that is shorter and directed to employees
  - Can form the basis for regular training (once a year is advisable)
  - Employees should be able to identify the significance of a breach when it occurs and report it promptly to supervisors
- Discovery of a breach by an employee may be imputed to the organization
  - Clock begins ticking for notification of affected individuals
  - HIPAA recognizes this type of constructive knowledge

Spotting the Signs

- The employee-facing portion of an incident response plan should help employees spot the many possible signs of a security breach, such as:
  - Suspicious entries in system or network logs
  - Unsuccessful logon attempts
  - Unusually poor system performance
  - "Doorknob rattling," such as social engineering attempts
  - System alarms or other indications from intrusion detection systems

Consequences of Failure to Train

- An employee knows that a laptop went missing and may have been stolen, but doesn't think it's significant
  - Reports the incident a month later to supervisor
  - Laptop contained 100,000 employee Social Security numbers and is being used to commit identity theft
  - By the time that the matter has come to the attention of the Incident Response Team and management, it is no longer possible to notify individuals within a reasonable or legally mandated time frame
  - Nevertheless, notification letters must be sent

Training and Role-Based Access

- Security breach response training may go hand-in-hand with more general security training
- Role-based access to personal information and sensitive information can limit potential breaches
  - HIPAA's "minimum necessary" standard
- The best training recognizes how personal information is actually used and disclosed within an organization
  - Consider department-specific training
- Employees need to know who to contact in the event of a breach

The First 24 Hours

- The incident response plan should enable a focused approach to the first 24 hours following discovery of a breach, including:
  - Performing forensics before evidence can be destroyed, using internal security resources or an external forensics firm
  - First, and foremost, prevent further data loss
  - Move systematically but promptly through your investigation

Investigation and Risk Assessment

- The incident response plan should provide a roadmap for not only conducting, but properly documenting, the investigation
  - Document not only what you did, but why you did it
  - Particularly if you determine that no breach occurred (and no notification will be provided to individuals or a customer), document the factors you weighed in reaching that conclusion
  - Document the lessons learned from a breach and follow-up measures to correct any systemic deficiencies

The Investigation Report

- Because a possible breach may be scrutinized long after the fact, make sure the investigation report includes all relevant documentation, including:
  - Forensics reports
  - Correspondence
  - Breach notification letters
  - Relevant contract provisions, such as those specifying timing for breach notification

Line Up External Resources

- Prior to a breach, the Incident Response Team should vet and engage appropriate external resources, to be employed as needed, including:
  - Computer forensics firm
  - Data breach resolution vendor (which may include call center, notification mailing services and credit monitoring services)
- Offering credit monitoring services is increasingly becoming a best practice
  - Previously reserved for incidents involving actual fraud or identity theft

Legal Compliance Modules

- If your company is subject to multiple security breach notification standards, it is advisable to create separate modules in the incident response plan
  - A HIPAA business associate should have a module tracking BA breach notification responsibilities, including template risk assessment
  - HIPAA module will be slightly different for covered entities
  - If your company operates in one or a limited number of states, consider a module tracking elements of applicable state breach notification laws

Common Security Breach Response Mistakes

- Understand whether you are legally obligated to notify affected individuals
  - Don't overreact
  - Can't "unring the bell" once a notification letter has been sent
- Remember that the triggers for notification under state laws differ.
  - Is there a "reasonable belief" that the information has been acquired by an unauthorized person (California)?
  - Is there a "likelihood of harm" (Delaware)?

Common Security Breach Response Mistakes

- In a notification letter, address the risks posed by the particular breach
  - If the breach involves medical information, address the risk of medical identity theft and how to mitigate
  - If the breach involves Social Security numbers or financial account information, address risks of financial fraud and identity theft

Common Security Breach Response Mistakes

- In the heat of a crisis, organizations often forget that they adopted a security incident response plan

- If regulators or plaintiffs in a class action charge that you acted unreasonably, being able to demonstrate that you followed a reasonable security incident response plan is a good way to show otherwise

Failing to Appropriately Coordinate with Law Enforcement

- Consider whether it's appropriate to notify law enforcement
  - Choose the right agency:
    - Local high tech crimes task force
    - FBI
    - Secret Service
    - Department of Homeland Security
  - Don't use a half-hearted law enforcement investigation as an excuse to delay notification!

Secret Service Guidance

- June 2014: U.S. Secret Service's Criminal Investigative Division publishes "Incident Response and Planning Strategies When Notifying Law Enforcement"
  - Emphasizes importance of incident response team
- Identifies 3 basic components of a data breach:
  - How did they get in?
  - How did they move through your network and what they take or alter?
  - How did they exit your system?

Recommended Practices

- California Office of Privacy Protection (now AG's office) issued recommended practices document regarding CA's breach notification law
- http://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/recom_breach_prac.pdf
- A practical guide to current breach notification best practices
- Sample notice letters are included
- Updated to reflect new risks associated with medical identity theft

Vendor Agreements

- Incident response plan should address security breach notification in agreements with vendors/agents
- Provisions are legally required in HIPAA business associate agreements but the concept should be implemented in all agreements in which personal information is shared with a vendor
- Consider indemnification for security breach liabilities
- Consider interaction with limitation of liability provisions in vendor agreements
- Consider requiring vendors to obtain cyberinsurance

Breaches Are Inevitable

- When a severe breach occurs, companies are judged by the reasonableness of their efforts to prevent and mitigate incidents

- A comprehensive, well-implemented incident response plan is critical to demonstrate that your organization takes privacy and security matters seriously

Security Breach Prevention and Preparation

- Because the liability associated with a major and mishandled security breach can be enormous, a multi-pronged approach to prevention and mitigation should include:
  - A comprehensive data security compliance program
  - An effective and fully implemented written breach response plan, addressing:
    - Internal processes, such as development of an Incident Response Team and
    - Employee-directed materials and training

Security Breach Prevention and Detection

- In today's environment of sophisticated hackers and cybercriminals and ever-larger databases of personal information, breaches are an inevitability
- But organizations that have effectively prepared for these events will
  - Be able to eliminate many types of incidents that plague less well-prepared companies
  - And be poised to poised to respond effectively to those breaches that do occur and avoid damage to the company's reputation, brand and customers

Questions?

Speaker Contact Information:

Sharon A. Anolik

President, Privacy Panacea

datastrategy@yahoo.com

Reece Hirsch

Partner, Morgan Lewis

rhirsch@morganlewis.com

415-442-1422

ASIA

Almaty
Astana
Beijing
Singapore
Tokyo

EUROPE

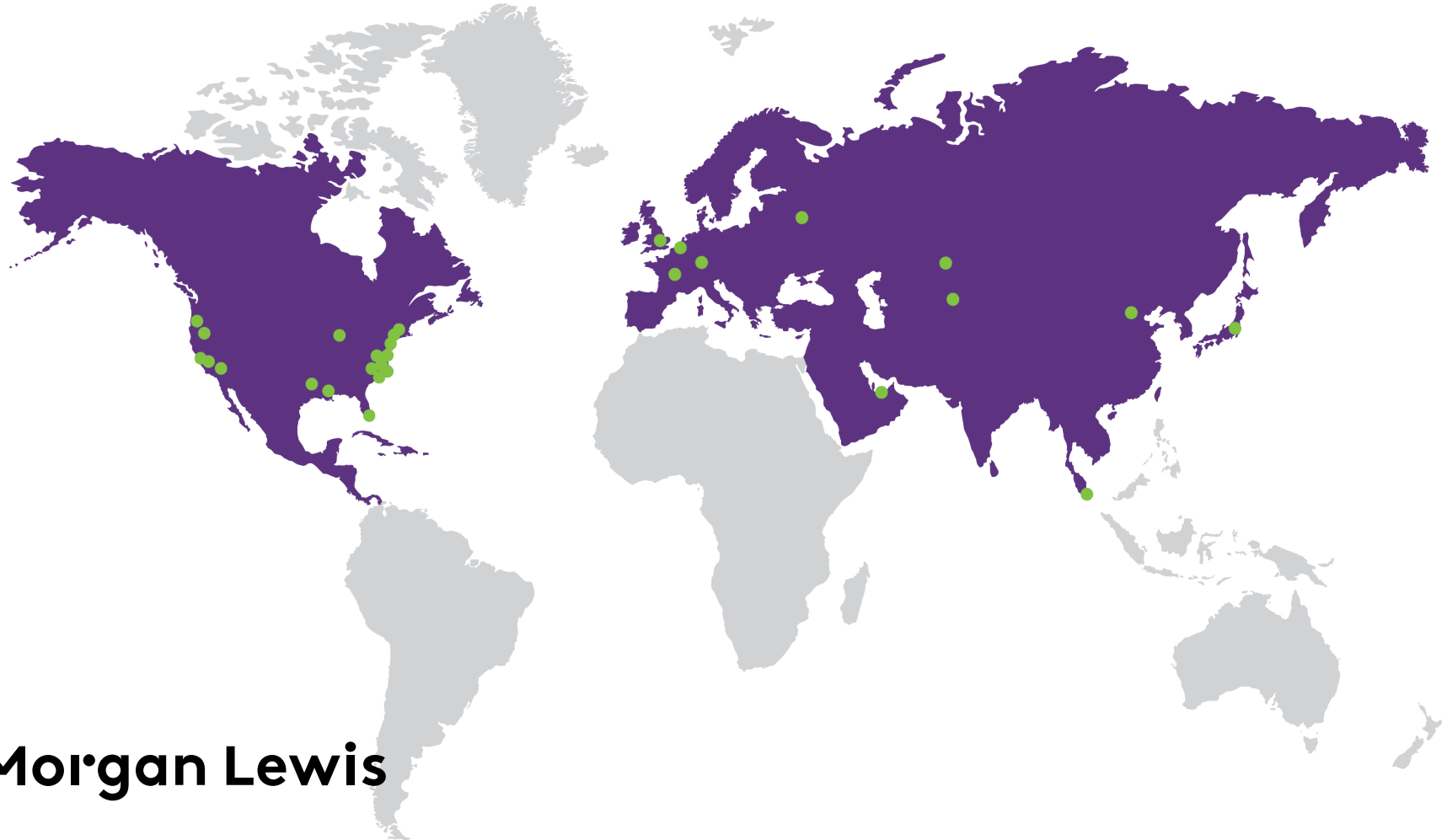
Brussels
Frankfurt
London
Moscow
Paris

MIDDLE EAST

Dubai

NORTH AMERICA

Boston
Chicago
Dallas
Harrisburg
Hartford
Houston
Los Angeles
Miami
New York
Orange County
Philadelphia
Pittsburgh
Princeton
San Francisco
Santa Monica
Silicon Valley
Washington, DC
Wilmington



Morgan Lewis

THANK YOU