

Deloitte.

Morgan Lewis



Third-Party Cyber Risk Management
Webinar

May 23, 2017

Today's speakers



Nikole Davenport

Senior Manager | Deloitte & Touche LLP

Nikole is a senior manager in Deloitte's Cyber Risk Services practice, specializing in cyber strategy and privacy matters. She concentrates on cyber incident assessments, plans and response, as well as privacy impact evaluations and compliance. Nikole, who was previously a partner at a law firm, has more than 15 years of experience leading teams on complex projects and providing analysis and strategy recommendations to clients. She has been appointed Special Outside Counsel to the Attorney General in a number of states, and has a broad history of working with both public and private entities.



Mark Krotoski

Partner | Morgan, Lewis & Bockius LLP

Mark is a litigation partner in Morgan Lewis's Privacy and Cybersecurity practice, with 20 years' experience handling cybersecurity cases and issues. He advises clients on mitigating and addressing third party cyber risks, developing Cybersecurity Protection Plans, and responding to a data breach or misappropriation of trade secrets. Previously he served as National Coordinator for the Computer Hacking and Intellectual Property (CHIP) Program in the Department of Justice (DOJ) in Washington, D.C., and CHIP prosecutor in Silicon Valley, among other DOJ leadership positions.



Adam Thomas

Principal | Deloitte & Touche LLP

Adam is a principal in Deloitte's Cyber Risk Services practice for the Financial Services industry and has more than 15 years of experience in the field. Over last seven years, Adam has led the development of Deloitte's third-party assessment offering and has been responsible for the execution of thousands of third-party security assessments on behalf of Deloitte's banking clients. Adam has helped a number of Deloitte's global financial services clients transform their third party risk management, IT risk and information security programs as they were brought under the supervision of regulators or required assistance responding to supervisory matters pertaining to their respective programs.

Overview

Third-party cyber risk

Emerging regulatory focus

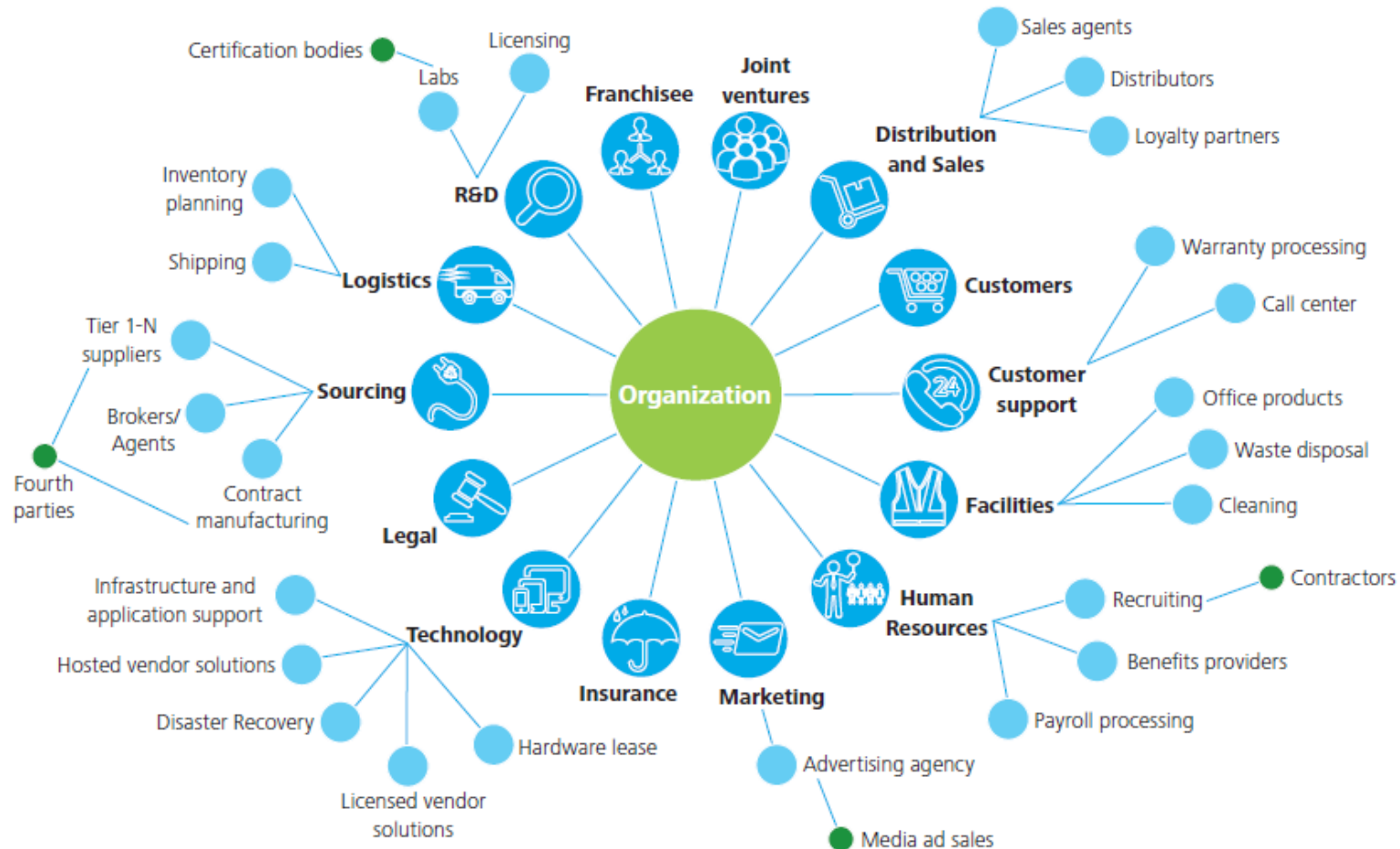
Incident response involving a third-party

Solution considerations for managing third-party cyber risk

Third-party cyber risk

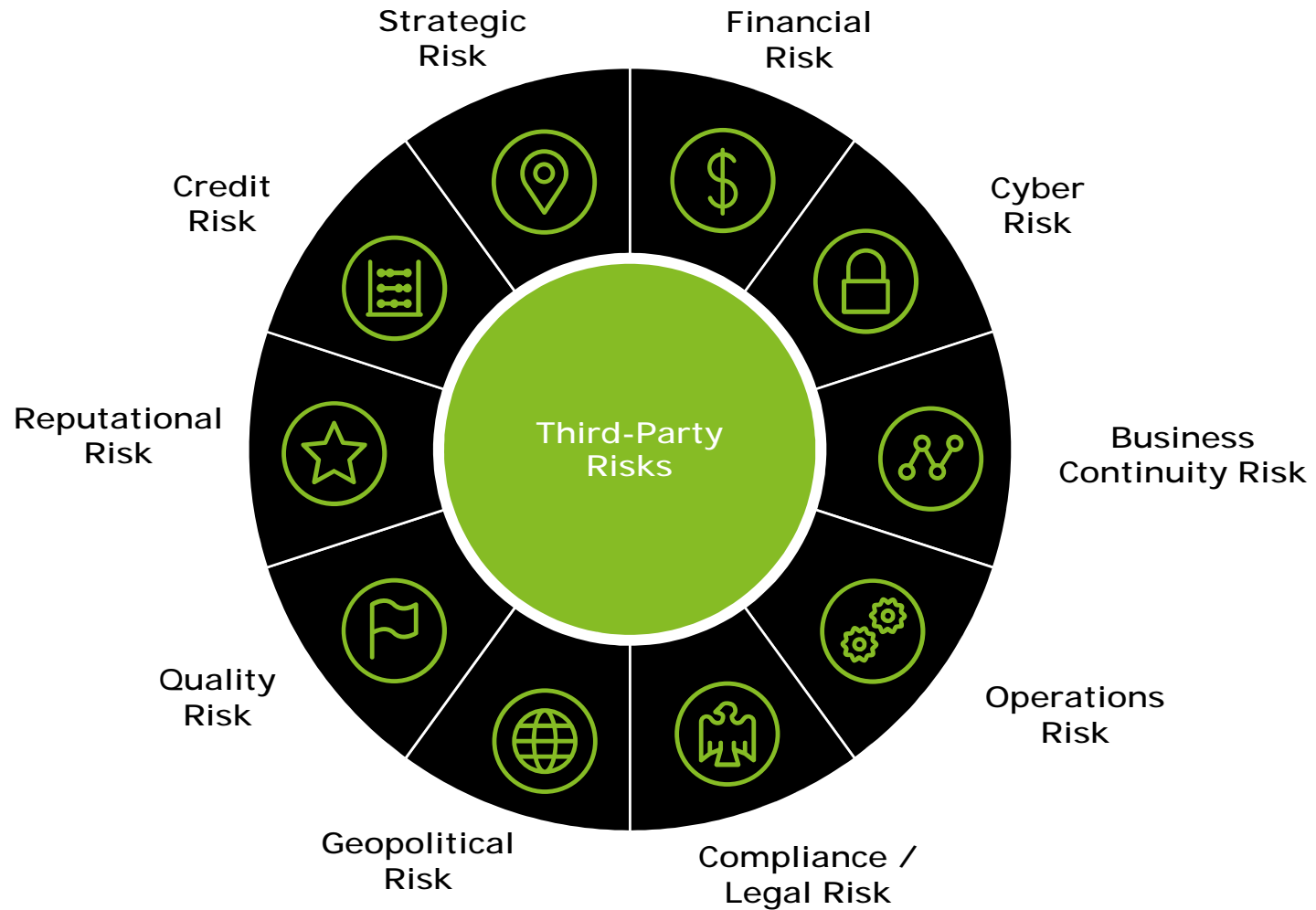
The extended enterprise of third-parties

An organization does not operate in isolation because its success is dependent upon a complex network of third-party relationships.



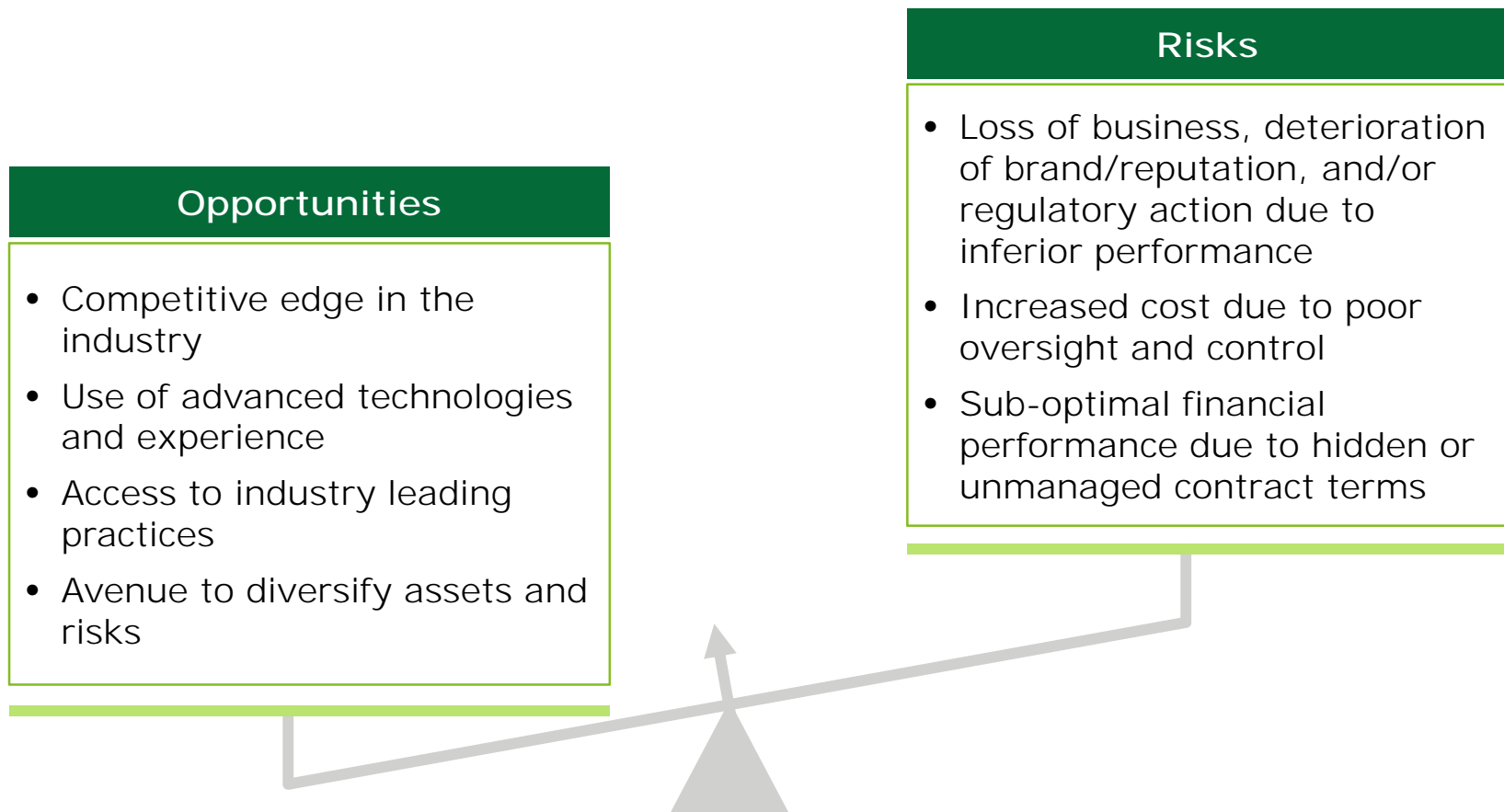
Third-party risk landscape

As organizations engage and outsource work to third parties, there is a large portfolio of third-party risks that must be managed.



Third-party risks and opportunities

Reliance on third parties can drive performance but also pose significant risks.



While third parties bring multiple benefits to business, there is a corresponding **increase in cyber risk exposure as third parties access critical systems, sensitive information, and engage sub-contractors**

Recent Third Party Cyber Risk Attacks

Newsroom

- Press Releases
- Public Statements
- Speeches
- Testimony
- Spotlight Topics
- Media Kit
- Events
- Webcasts
- What's New
- Special Studies
- RSS Feeds
- Social Media

PRESS RELEASE

SEC Charges 32 Defendants in Scheme to Trade on Hacked News Releases

Hackers, Traders Allegedly Reaped More Than \$100 Million of Illegal Profits

FOR IMMEDIATE RELEASE
2015-163

Washington D.C., Aug. 11, 2015 — The Securities and Exchange Commission today announced fraud charges against 32 defendants for taking part in a scheme to profit from stolen nonpublic information about corporate earnings announcements. Those charged include two Ukrainian men who allegedly hacked into newswire services to obtain the information and 30 other defendants in and outside the U.S. who allegedly traded on it, generating more than \$100 million in illegal profits.

The SEC's complaint unsealed today was filed under seal on August 10 in U.S. District Court in

Newsroom

- Press Releases
- Public Statements
- Speeches
- Testimony
- Spotlight Topics
- Media Kit
- Press Contacts
- Events
- Webcasts
- What's New
- Special Studies
- RSS Feeds
- Social Media

Press Release

SEC Obtains \$30 Million From Traders Who Profited on Hacked News Releases

Litigation Continues Against 32 Other Defendants in Alleged \$100 Million Scheme

FOR IMMEDIATE RELEASE
2015-191

Washington D.C., Sept. 14, 2015 — The Securities and Exchange Commission today announced that Ukrainian-based Jaspem Capital Partners Limited and CEO Andriy Supranonok have agreed to pay \$30 million to settle allegations they profited from trading on non-public corporate information hacked from newswire services.


The SEC announced charges in August against 34 defendants who allegedly took part in a scheme in which two of the defendants surreptitiously hacked into newswire services and transmitted the stolen data to a web of international traders, including Jaspem and Supranonok. By getting an early look at the information before its public release, the traders allegedly generated more than \$100 million of illegal profits over a five-year period. The case was filed in U.S. District Court for the District of New Jersey, which entered an asset freeze and other emergency relief against Jaspem and Supranonok, among others.

"Barely a month after we froze tens of millions of dollars in illegal profits from the defendants' trading on illegal inside information obtained from hacked news releases, we obtained a settlement with foreign traders that deprives them of their wrongful gains," said Andrew J. Ceresney, Director of the SEC's Enforcement Division. "Today's settlement demonstrates that even those beyond our borders who trade on stolen nonpublic information and use complex instruments in an attempt to avoid detection will ultimately be caught."

DealB%k WITH FOUNDER ANDREW ROSS SORKIN

Nine Charged in Insider Trading Case Tied to Hackers

By MATTHEW GOLDSTEIN and ALEXANDRA STEVENSON AUG. 11, 2015



NEWARK ASSOCIATED PRESS

After stealing corporate news from the underbelly of Wall Street, nine defendants were made public. How-to videos by

THE UNITED STATES ATTORNEY'S OFFICE
SOUTHERN DISTRICT of NEW YORK

HOME ABOUT U.S. ATTORNEY DIVISIONS NEWS PROGRAMS

U.S. Attorneys » Southern District of New York » News » Press Releases

Department of Justice
U.S. Attorney's Office
Southern District of New York

FOR IMMEDIATE RELEASE Tuesday, December 27, 2016

Manhattan U.S. Attorney Announces Arrest Of Macau Resident And Unsealing Of Charges Against Three Individuals For Insider Trading Based On Information Hacked From Prominent U.S. Law Firms

Iat Hong Arrested On December 25 In Hong Kong On U.S. Insider Trading And Hacking Charges; In Addition To Successful Cyber Intrusions Into Two Law Firms, Defendants Charged With Attempting To Hack Into Total Of Seven Law Firms

Preet Bharara, the United States Attorney for the Southern District of New York, and William F. Sweeney Jr., the Assistant Director-in-Charge of the New York Field Office of the Federal Bureau of Investigation ("FBI"), announced the arrest of IAT HONG and the unsealing today of a 13-count superseding indictment charging HONG, BO ZHENG, and CHIN HUNG (the "Defendants"). The Defendants are charged with devising and carrying out a scheme to enrich themselves by obtaining and trading on material, nonpublic

Industry perspectives on third-party cyber risk

Many organizations are struggling to effectively manage their third party cyber risks across the extended enterprise.



Over 60% of survey executives find it necessary to take action to enhance their third party monitoring¹

¹Source: Deloitte. "Third party governance and risk management – Global survey 2016"

Polling Question

How would you rate your organization's controls in being able to minimize third party risk?

- a. Excellent
- b. Satisfactory
- c. Need improvement
- d. Need significant improvement


Emerging regulatory focus

Regulatory landscape



SEC focus on third-party platforms

Vendor Management: Some of the **largest data breaches** over the last few years may have resulted from the hacking of **third-party vendor** platforms. As a result, examiners may focus on firm practices and controls related to vendor management, such as due diligence with regard to vendor selection, monitoring and oversight of vendors, and contract terms. Examiners may assess how vendor relationships are considered as part of the firm's ongoing risk assessment process as well as how the firm determines the appropriate level of due diligence to conduct on a vendor.

| | |
|--|--|
|  | <i>By the Office of Compliance Inspections and Examinations ("OCIE")¹</i> |
| Alert: | Volume IV, Issue 8 |
| <i>Cybersecurity Initiative</i> | September 15, 2015 |
| | OCIE's 2015 Cybersecurity Examination Initiative |

SEC focus on third-party platforms



The screenshot shows a webpage layout for a SEC Press Release. On the left is a vertical navigation menu with items: Newsroom, Press Releases (highlighted), Public Statements, Speeches, Testimony, Spotlight Topics, Media Kit, Press Contacts, Events, Webcasts, and What's New. The main content area features the title "SEC Charges Investment Adviser With Failing to Adopt Proper Cybersecurity Policies and Procedures Prior To Breach" and the text "FOR IMMEDIATE RELEASE 2015-202". Below this is the release text starting with "Washington D.C., Sept. 22, 2015— The Securities and Exchange Commission today announced that a St. Louis-based investment adviser has agreed to settle charges that it failed to establish the required cybersecurity policies and procedures in advance of a breach that compromised the personally identifiable information (PII) of approximately 100,000 individuals, including thousands of the firm's clients." A second paragraph follows, stating "The federal securities laws require registered investment advisers to adopt written policies and procedures reasonably designed to protect customer records and information. An SEC investigation found that R.T. Jones Capital Equities Management violated this 'safeguards rule' during a nearly four-year period when it failed to adopt any written policies and procedures to ensure the security and confidentiality of PII and protect it from anticipated threats or unauthorized access." On the right side, there are social media icons (print, Facebook, Twitter, Email, and a plus sign) and a "Related Materials" section containing two links: "SEC order" and "Investor Alert - Identity Theft, Data Breaches, and Your Investment Accounts".

Third-party service provider (TPSP) security policy

Written Policies and Procedures

- § Based upon the overall risk assessment

Policies and Procedures Addressing:

- § The identification and risk assessment of TPSPs
- § Minimum cybersecurity practices
- § Due diligence processes used to evaluate the adequacy of cybersecurity practices of TPSPs
- § Periodic assessment of TPSPs based on risk they present and the continued adequacies of their cybersecurity policies

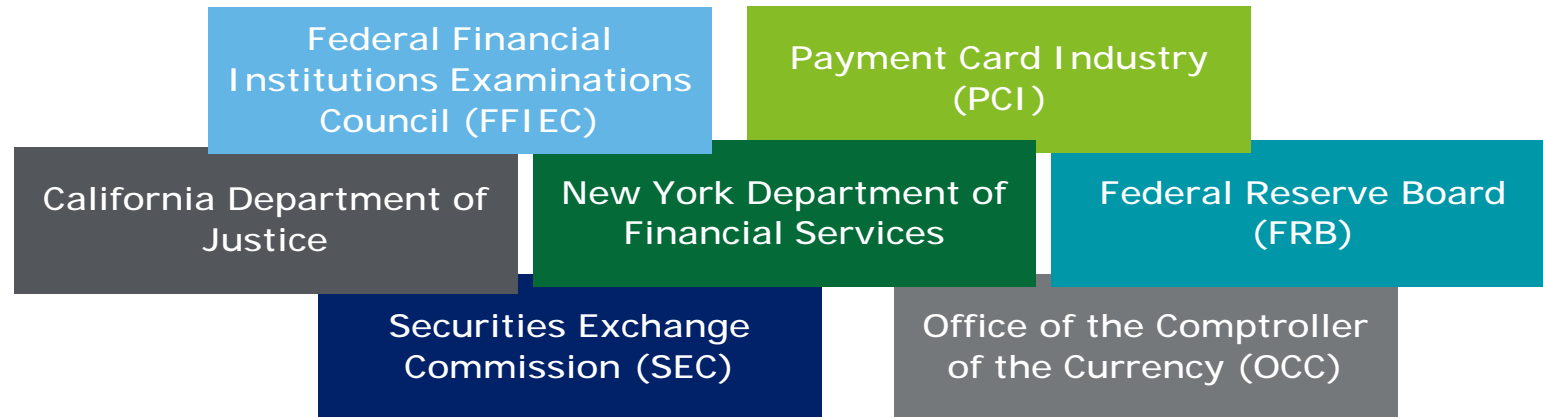
Outline Contractual Protections:

- § Policies regarding access controls, including its use of Multi-Factor Authentication
- § Use of encryption (both in transit and at rest)
- § Incident response and notice policies in the event of a Cybersecurity Event directly impacting the Covered Entity's Information Systems or its Nonpublic Information
- § Representations and warranties addressing cybersecurity policies and procedures relating to security controls

Third-party cyber risk regulatory landscape

Regulators have issued heightened standards and guidance for third-party cyber risk management.

Third-Party Risk Management Regulators



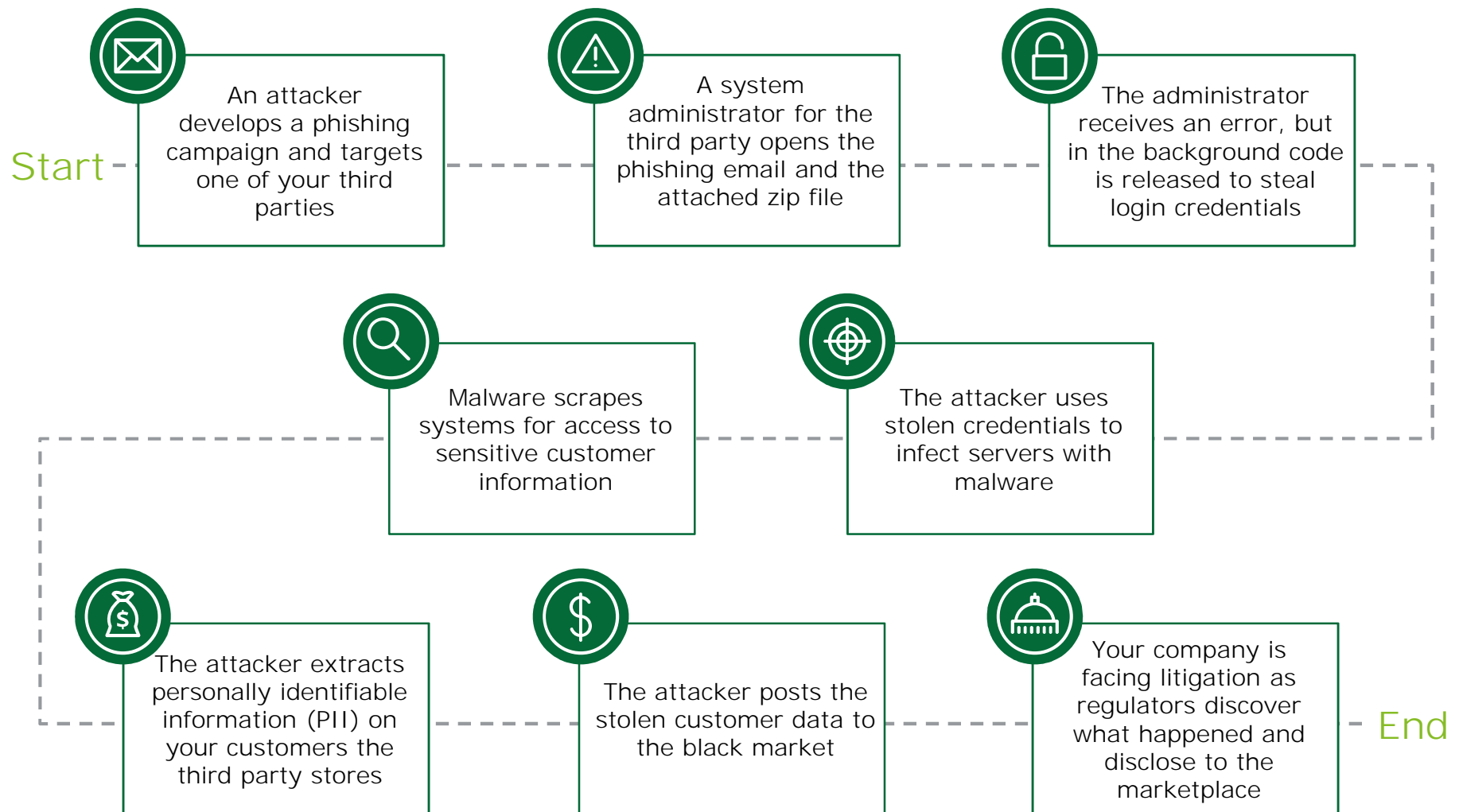
Increasing Areas of Regulatory Focus

- § **Identifying, assessing, and mitigating** third-party risks
- § Periodic **assessment of third parties based on the risk** they present to the business
- § Responsibility to **control business continuity risk** associated with third parties
- § Consideration of the potential **impact of disruptions** on a third party's ability to restore services to multiple clients
- § **Supplier selection and auditing of third-party services**
- § Clearly **documented agreements** with third parties

Incident response involving a third-party

Illustrative third-party cyber risk attack

A malicious actor targeting an organization's third parties can cause serious damage including, but not limited to operational, financial, legal and reputational costs.



Overseeing internal investigations



Initial call

§ How was the cyber compromise / incident discovered?

- Notification obligation?



Determine Scope and Nature of Breach

§ Did a “data breach” occur?



Attorney Client Privilege

§ Is the privilege effectively in place?



Assess Legal Consequences

§ What regulatory agencies? Was information accessed, acquired or exfiltrated?

§ Which customers?

§ What legal standards apply?



Coordination Issues / Coverage Obligations

Role of attorney-client privilege

§ For the purpose of seeking or providing legal advice

- Aids in the **careful evaluation** of threats/intrusions and **responsive action** for investigation, legal obligations, and litigation
- Early in the process
- Risks if not properly used/protected

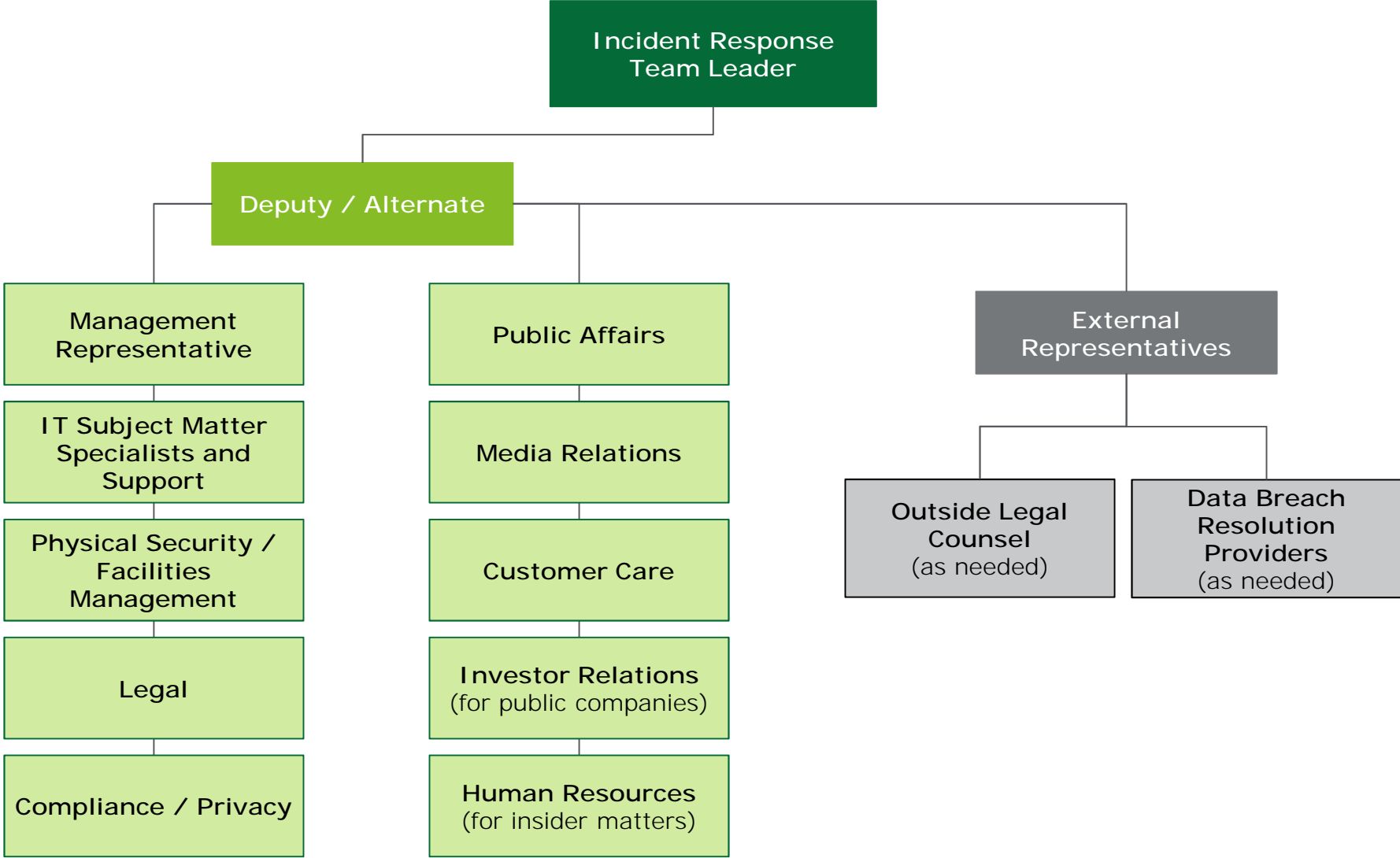
§ Company counsel working with outside counsel

§ Role of counsel with vendors

- At the direction of counsel

**Confidential Document
Attorney-Client Privilege**

Incident response team



State data breach notification laws

§ 52 Jurisdictions

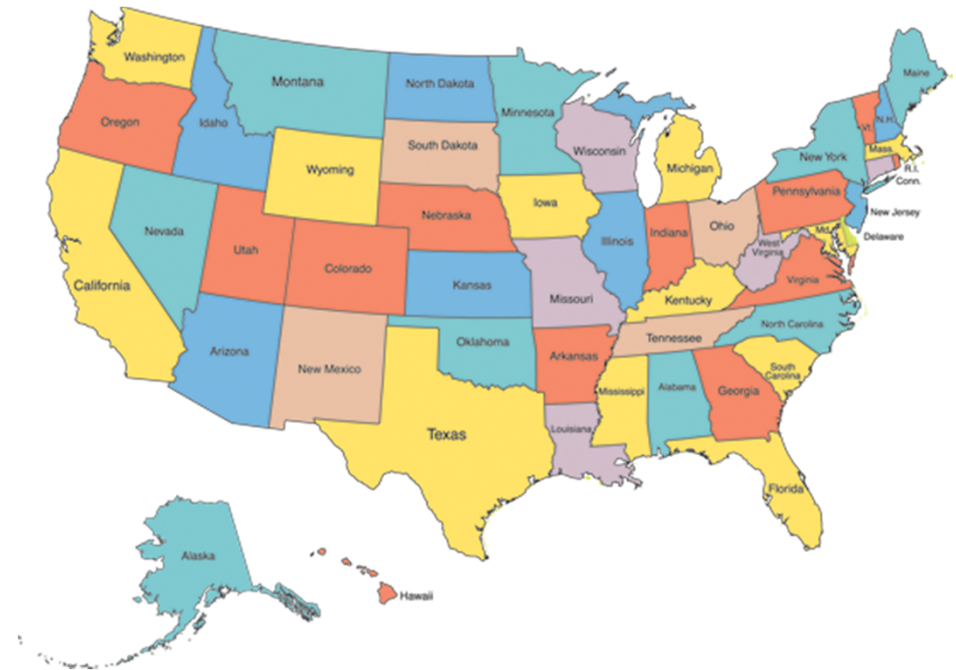
- Also: District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands
- 2 States with no security breach law
 - **Alabama and South Dakota**

§ Notification may be required to customers, government, and credit agencies

§ State law depends on residency of customers and location of data

§ Separate **Attorney General (AG) enforcement action** may be brought

§ Many States provide a **private right of action**



Polling Question

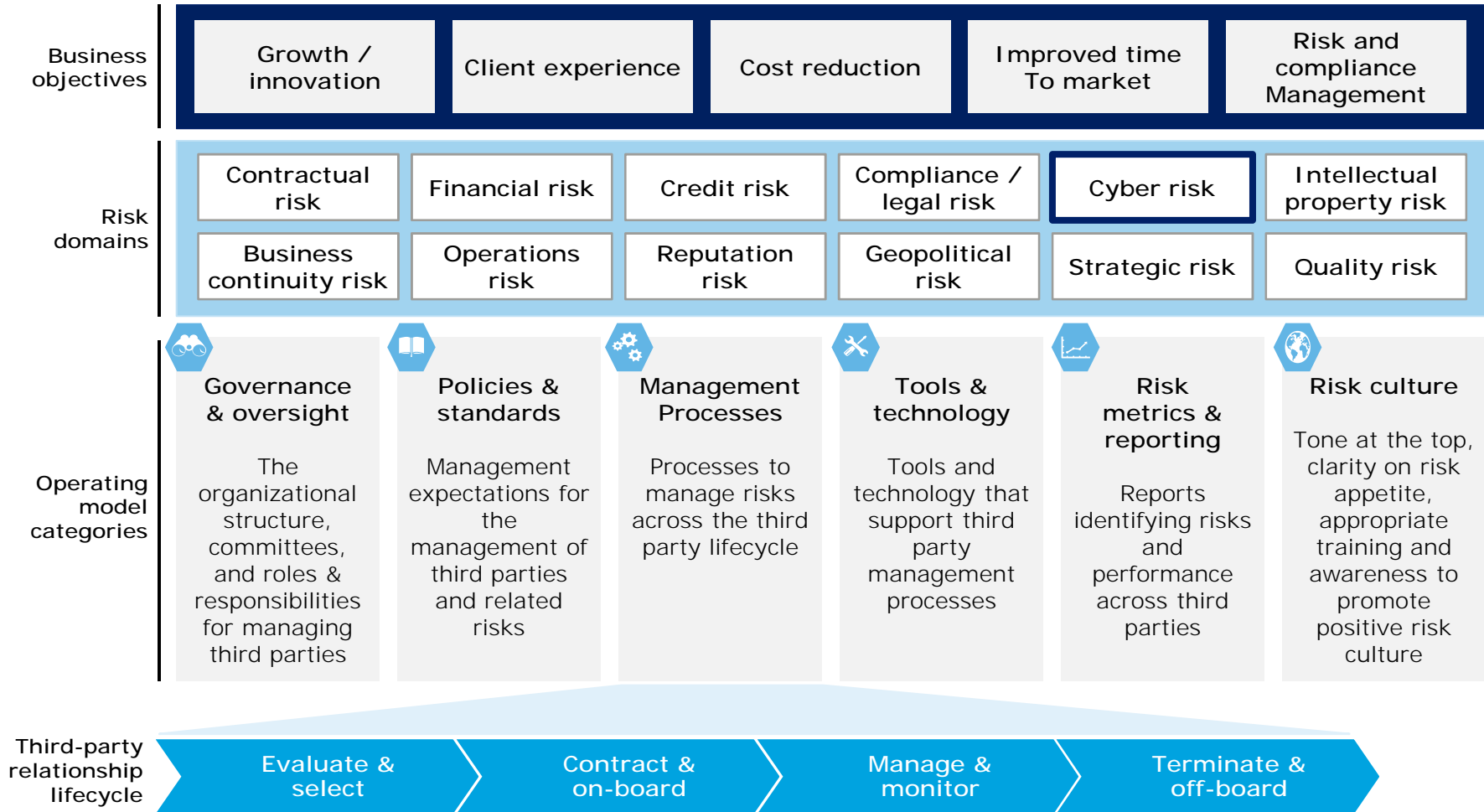
Does your data breach / incident response plan incorporate responding to third party risks?

- a. Yes
- b. No

Solution considerations for managing third-party cyber risk

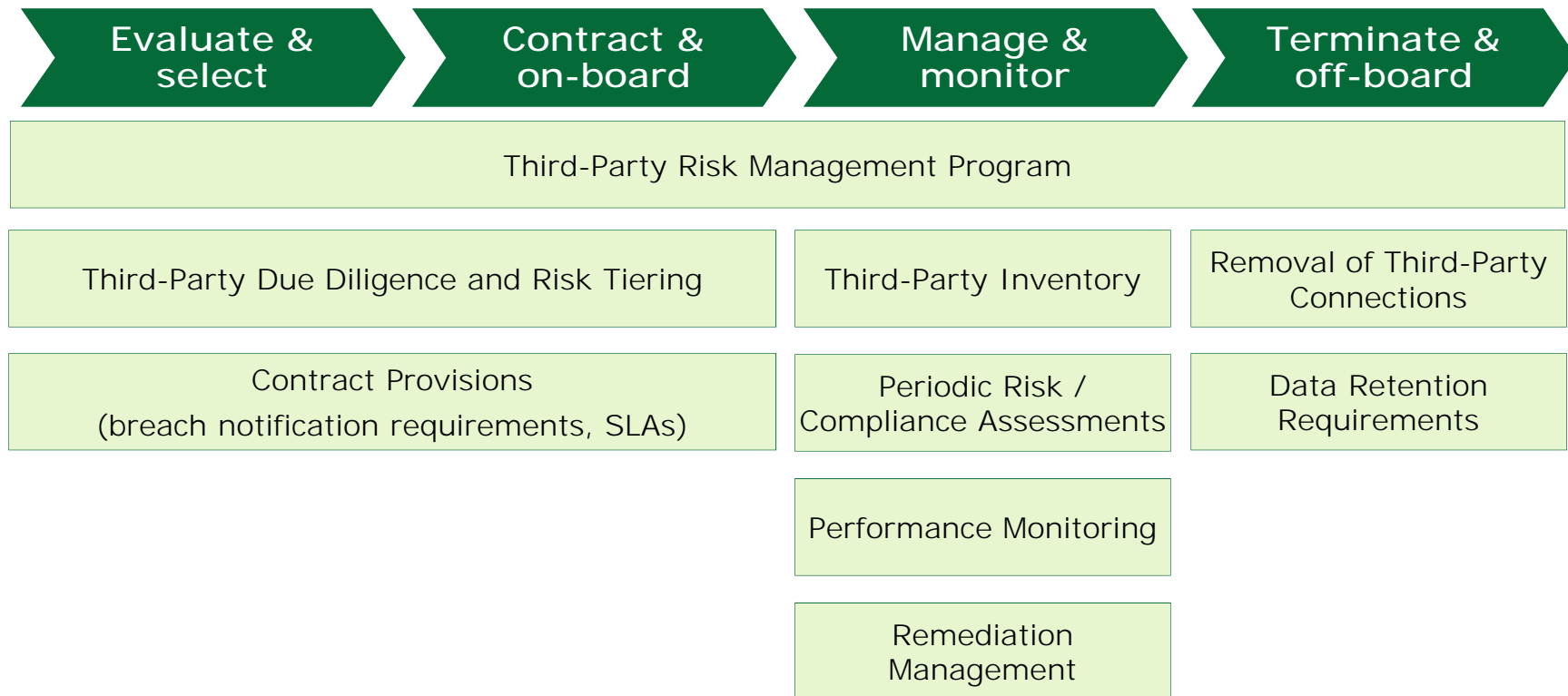
Managing Third Party Cyber Risk

Developing a holistic approach to managing third-party relationships, while considering business objectives and risk domains is pivotal to a effective program.



Third-party cyber risk management solutions

Organizations should establish robust third-party risk management practices / solutions to effectively manage third-party risk.



Contact Information

Mark Krotoski

Partner

Morgan, Lewis & Bockius LLP

mark.krotoski@morganlewis.com

+1.650.843.7212

Adam Thomas

Principal

Deloitte & Touche LLP

adathomas@deloitte.com

+1.602.234.5172

Nikole Davenport

Senior Manager

Deloitte & Touche LLP

ndavenport@deloitte.com

+1.404.631.2860

Question and answer



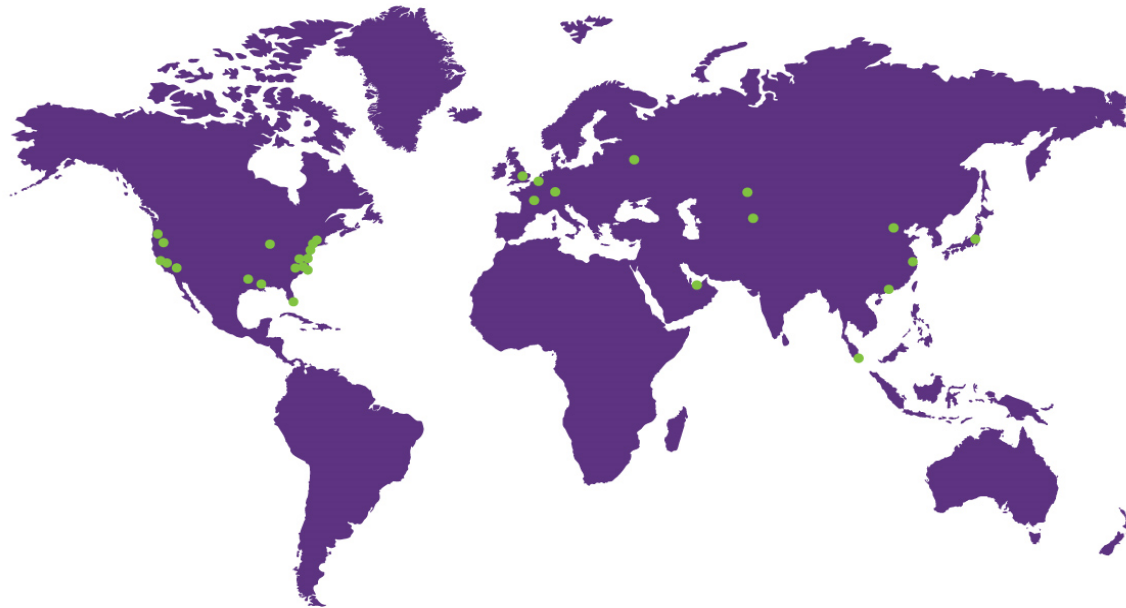
Morgan Lewis' Global Reach

Our Global Reach

Africa
Asia Pacific
Europe
Latin America
Middle East
North America

Our Locations

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



Morgan Lewis

*Our Beijing office operates as a representative office of Morgan, Lewis & Bockius LLP. In Shanghai, we operate as a branch of Morgan Lewis Consulting (Beijing) Company Limited, and an application to establish a representative office of the firm is pending before the Ministry of Justice. In Hong Kong, Morgan Lewis has filed an application to become a registered foreign law firm and is seeking approval with The Law Society of Hong Kong to associate with Luk & Partners.

This presentation contains general information only and Morgan Lewis and Deloitte are not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Morgan Lewis and Deloitte shall not be responsible for any loss sustained by any person who relies on this presentation.

Deloitte.

Morgan Lewis

© 2017 Morgan, Lewis & Bockius LLP

© 2017 Morgan Lewis Stamford LLC

© 2017 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 office operates as a representative office of Morgan, Lewis & Bockius LLP. In Shanghai, we operate as a branch of Morgan Lewis Consulting (Beijing) Company Limited, and an application to establish a representative office of the firm is pending before the Ministry of Justice. In Hong Kong, Morgan Lewis has filed an application to become a registered foreign law firm and is seeking approval with The Law Society of Hong Kong to associate with Luk & Partners.