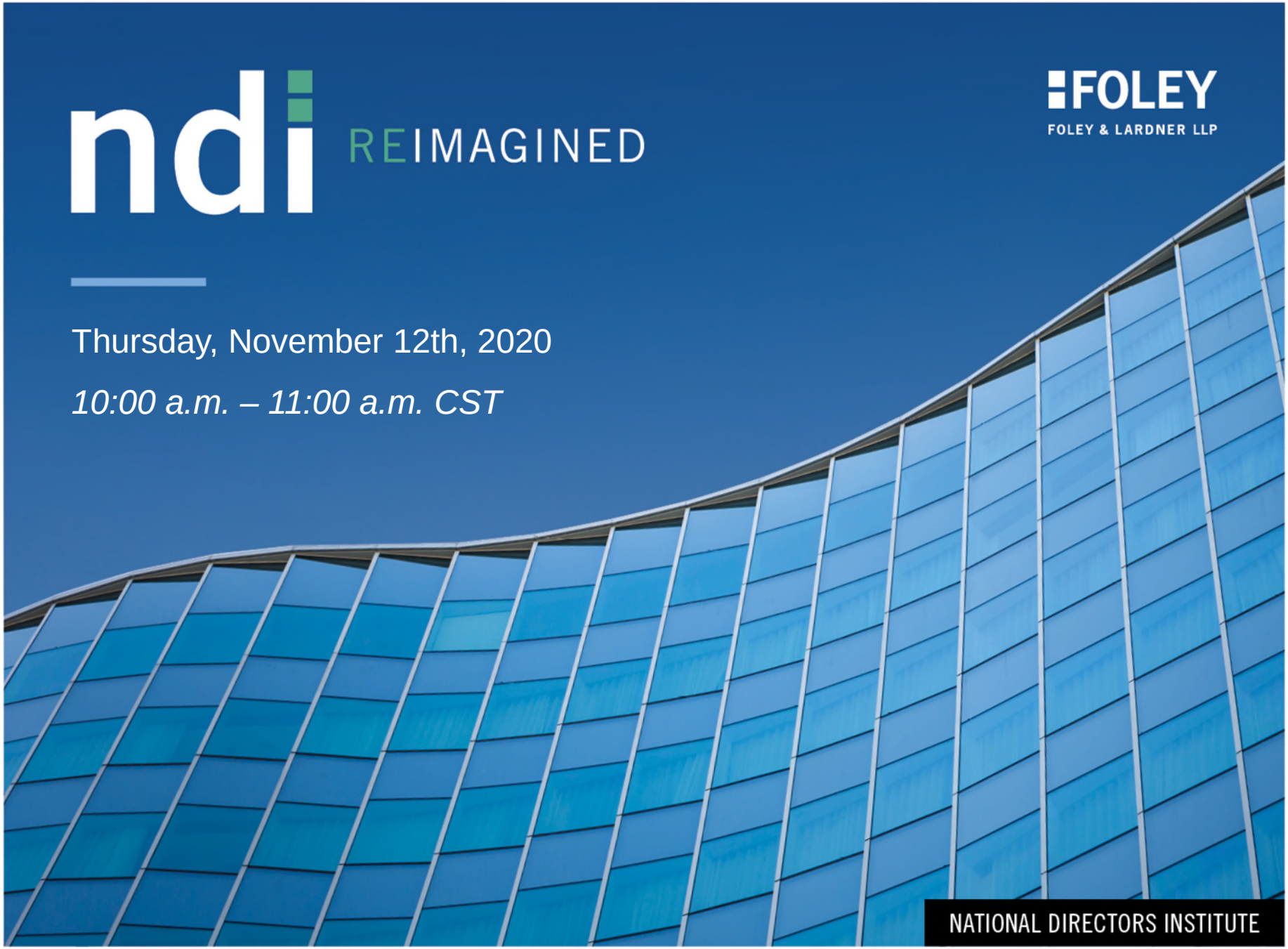

ndi REIMAGINED
FOLEY
FOLEY & LARDNER LLP
Thursday, November 12th, 2020
10:00 a.m. – 11:00 a.m. CST
NATIONAL DIRECTORS INSTITUTE

Webinar Housekeeping

- Questions can be entered via the Q&A widget open on the left-hand side of your screen. We will address questions at the end of the program, time permitting
- The recorded version of this presentation will be available on Foley.com in the next few days and you can find a copy of the slides in the Resource List widget on the left-hand side of your screen.
- Foley will apply for CLE credit after the program. To be eligible for CLE, you will need to answer a polling question during the program.
- If you did not supply your CLE information upon registration, please e-mail it to NDIinfo@foley.com. Certificates of attendance will be distributed via email to eligible participants approximately 8 weeks after the web conference.
- NOTE: Those seeking Kansas, New York & New Jersey CLE credit are required to complete the Attorney Affirmation Form in addition to answering the polling question. Please email the form in the Resource List to NDIinfo@foley.com immediately following the program.

BREAKOUT SESSION

The Board's Role in Evaluating Third Party Cybersecurity Risks

PANELISTS

Jennifer Urban

Partner

Foley & Lardner LLP

jurban@foley.com

414.297.5864

Mike Overly

Partner

Foley & Lardner LLP

moverly@foley.com

213.972.4533

Angela Johnson

Chief Information Security Officer and Vice President of Supply Chain

Children's Hospital of Wisconsin

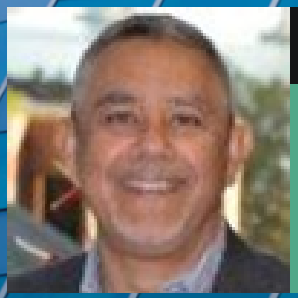
ajohnson2@chw.org

Che Bhatia

Vice President, Cyber Resilience

Aon's Cyber Solutions (formerly Stroz Friedberg)

che.bhatia1@strozfriedberg.com



Yusuf Cassim

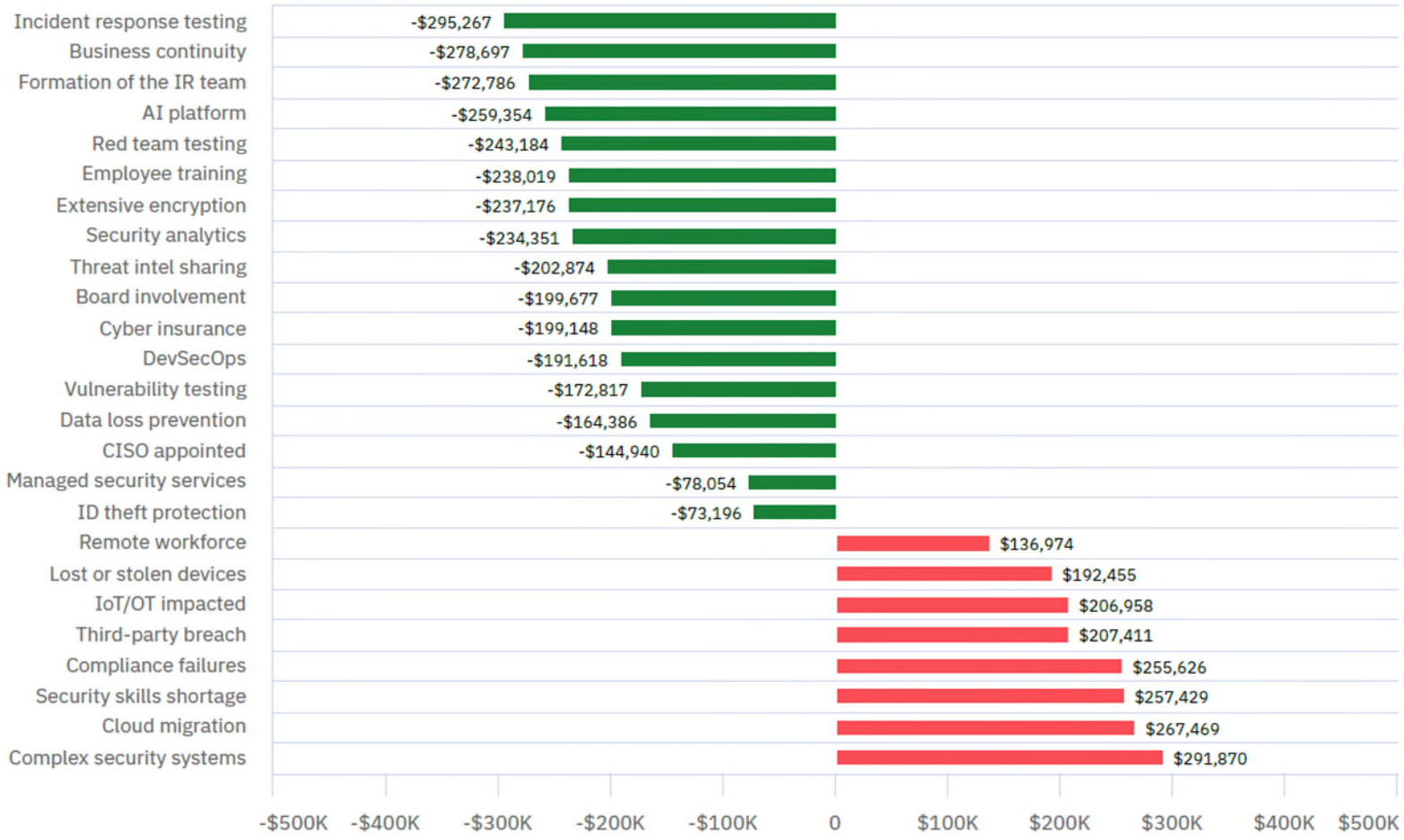
Vice President, Associate General Counsel,

Charles Schwab & Co., Inc.

yusuf.cassim@schwab.com

Cost Factors in a Data Breach

Change in US$ From Average Total Cost of $3.86 Million



SOURCE: *Cost of a Data Breach Report 2020*, Produced Jointly Between Ponemon Institute and IBM Security, July 2020

Five Cybersecurity Principles Every Board Director Needs to Know

- Understand and Approach Cybersecurity as an Enterprise-wide Risk Management Issue. Not Just an IT Issue.
- Understand the Legal Implications of Cyber Risks as They Relate to the Company's Specific Circumstances.
- Have Adequate Access to Cybersecurity Expertise and Give Cyber Risk Management Regular and Adequate Time on Board Meeting Agendas.
- Set the Expectation That Management Will Establish an Enterprise-wise Risk Management Framework. With Adequate Staffing and Budget.
- Management Discussions Should Include Identification and Quantification of Financial Exposure to Cyber Risks and Which Risks to Accept, Mitigate, or Transfer (e.g., Through Insurance), as well as Specific Plans Associated with Each Approach.

ndi REIMAGINED

SOURCE: *NACD Director's Handbook on Cyber-Risk Oversight*, National Association of Corporate Directors, 2020

Top 10 Questions the Board Should Ask to Assess Third-Party Risk

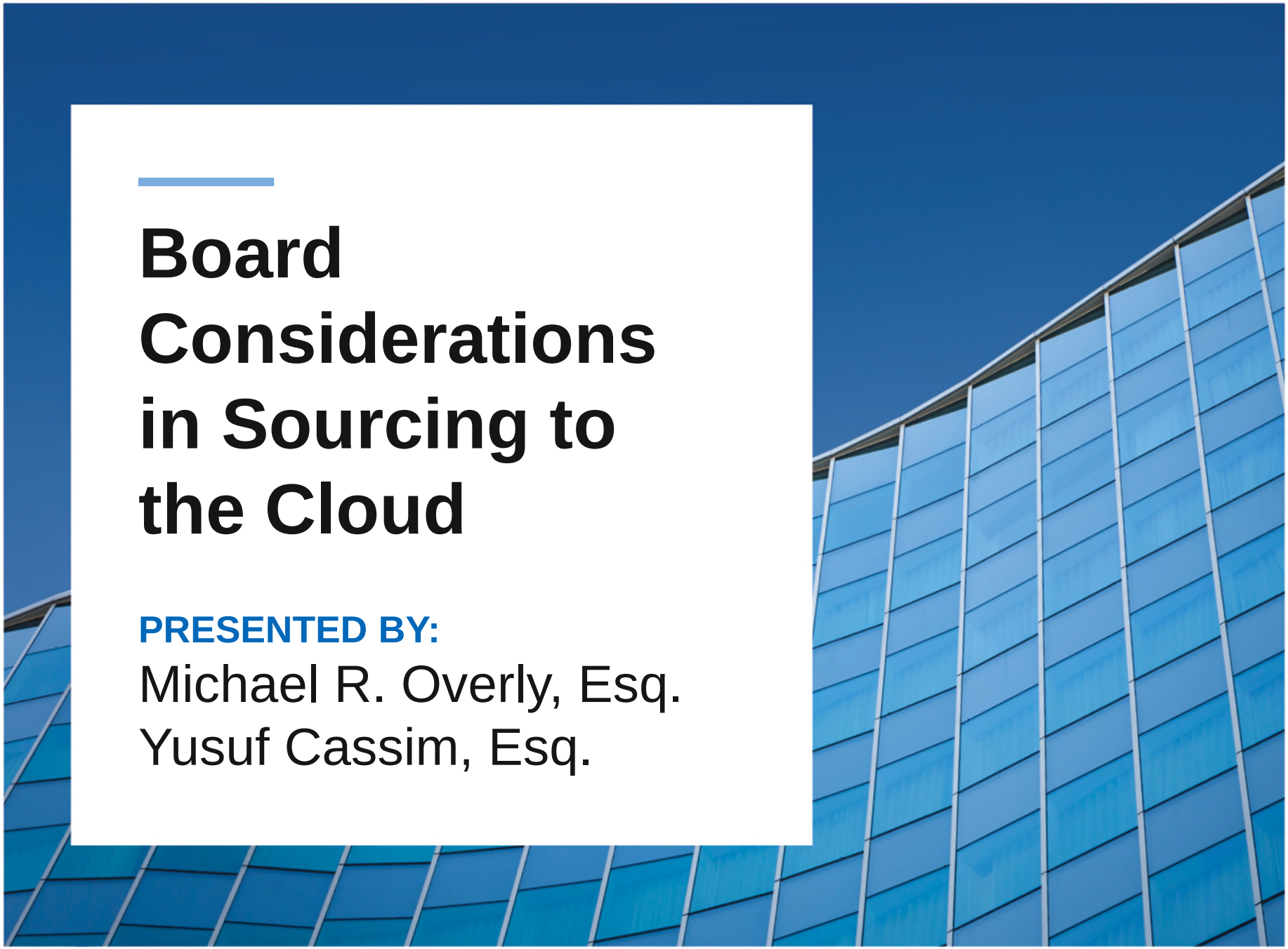
PRESENTED BY:
Jennifer L. Urban
Angela Johnson

Top Ten Questions the Board Should Ask to Assess Third-Party Risk

1. **Who Are Our Organization's Critical Vendors/Third-Party Partners?**
   - Who are we most dependent upon to stay up and running?
   - Who has access to large amounts of data or system-wide access to our infrastructure?
2. **What Is Our Organization's Internal Process for Approving and Terminating Third-Parties?**
   - Do we have a Third Party Management (TPM) Program?
   - How do we conduct screening for vendor selection/due diligence?
   - Who approves? IT, legal, business owner or a committee?
   - Beyond Onboarding: How do we conduct ongoing due diligence?
3. **Does Our Organization Have a Contingency Plan or Transition Services Available for Critical Vendors/Third-Parties?**
4. **How Does Our Organization Manage Cloud v. On-Premise Vendors?**

Top Ten Questions the Board Should Ask to Assess Third-Party Risk

5. **For Critical Vendors/Third-Parties: Do We Have Insight Into Their Incident Response Process? Do We Have A Contact For Incident Response Coordination?**
6. **What Third-Parties Are Critical to Our Organization's Business Continuity/Disaster Recovery Plan?**
7. **Does Our Insurance Cover Vendor/Third Party Breaches?**
8. **Are There Functions/Operations Our Organization Should Consider Outsourcing Instead of Keeping Risk In-House?**
   - Lift and Shift: Are we taking on unnecessary internal risk? Are there processes we are doing in-house that we could outsource to shift that risk to third-parties?
9. **How Does Fourth Party Risk Get Assessed?**
   - Are there prohibitions on subcontracting/assignment or other pass through requirements?
10. **How Does our TPM Program Correlate With Our Internal Enterprise-wide Risk Management Program?**



Board Considerations in Sourcing to the Cloud

PRESENTED BY:
Michael R. Overly, Esq.
Yusuf Cassim, Esq.

Common Misconceptions

- Commodity pricing and services are always less than locally installed solutions
- Easier to budget
  - Confusing pricing metrics and hidden costs
- There is safety in numbers
- Cloud providers are the experts

Case Study – Cloud Desktop

Common Failure Points

- Failure to align expectations
- Vendor – Customer
- Within Customer's own organization
- "Contract float" – not only is data in the cloud, but also key contract terms
- No transition-out plan, no fall-back
- Loss of institutional knowledge

Common Failure Points

- Liability and performance
- The dawn of the as-is technology agreement
- Data held hostage
- Regulatory issues

Risk Assessment in Practice

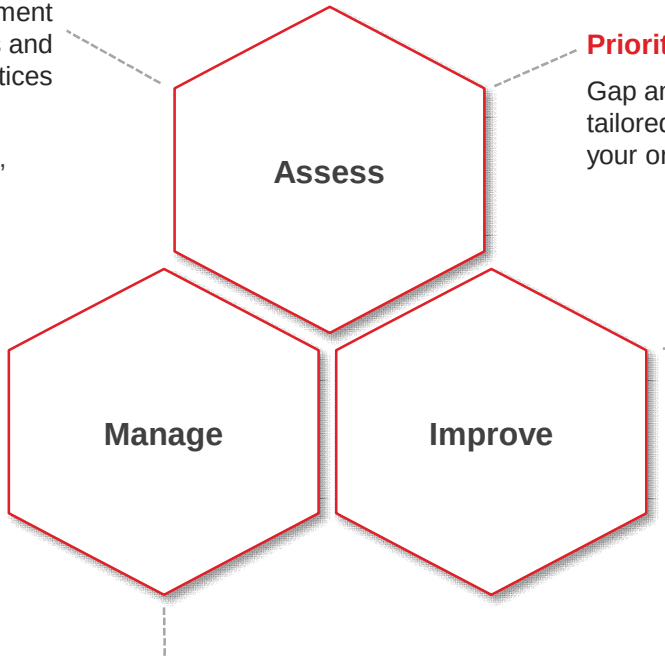
PRESENTED BY:
Chetan Bhatia

Best Practices with Mitigating Risk with Third Parties

Maturity Review

Review your third-party risk management program and, identify gaps against needs and leading best practices

Potential services: Program Review and Gap Analysis, Identify Prioritized Initiatives, Develop High-Level Roadmap



Prioritized Roadmap

Gap analysis and roadmap for improvement tailored and prioritized based on the needs of your organization

Continuous Monitoring

Continuously monitor third-party progress to address identified risks and that adequate security controls and processes are in-place to protect your organization.

Program Development

Assist in developing or enhancing your third-party risk management program to deliver well-documented policies, procedures are a rigorous set of cradle to grave practices to execute your third party risk management program

Potential services: Policy Development,
Risk Framework Adoption,
Implement / Modify Risk Register

Risk Assessments

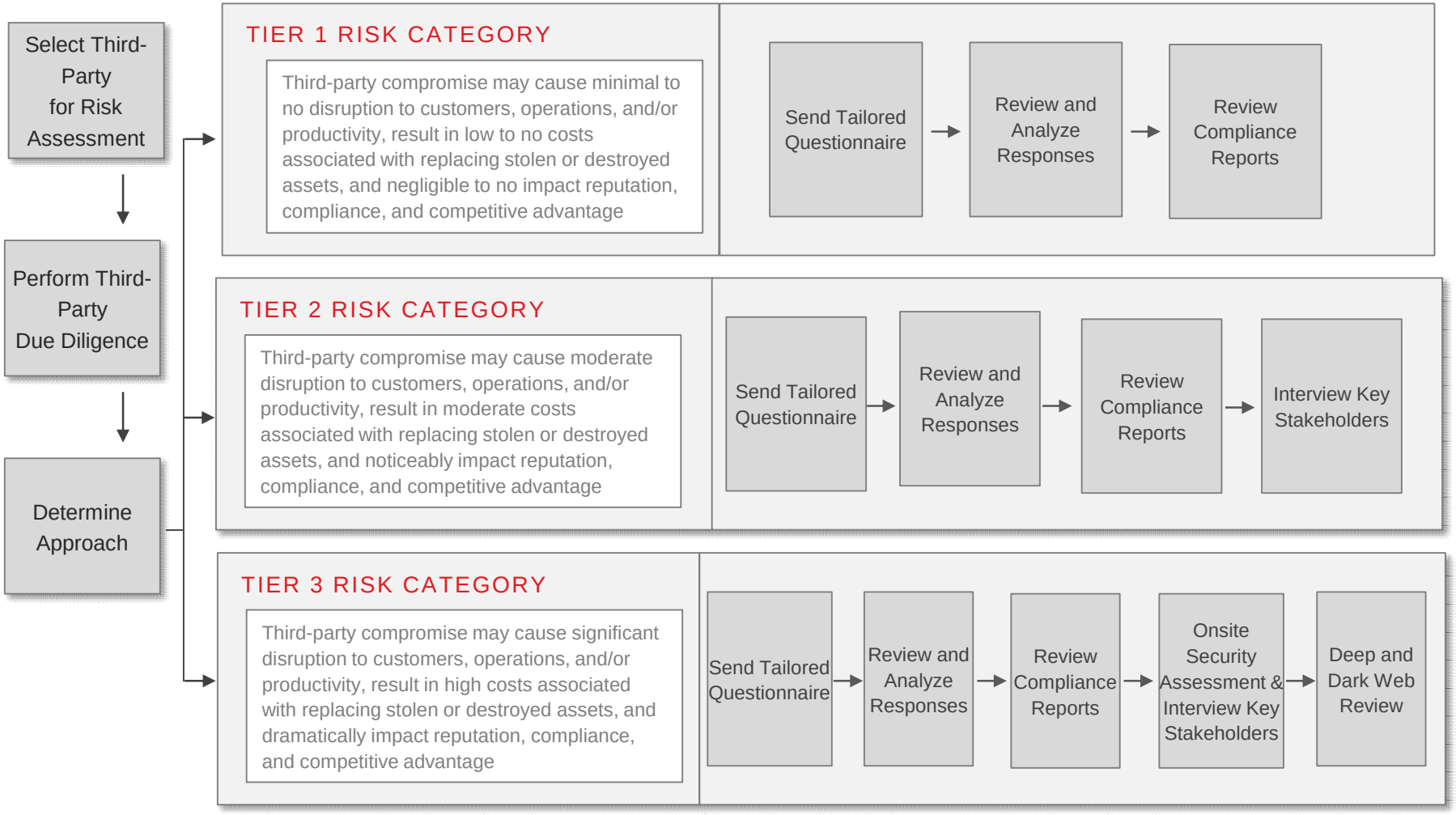
Perform a tailored assessment (on-site or remote) based on the risk a third-party poses to your organization

Third Party Categorization/Discovery

Identify, define, categorize your third-party relationships to ensure time and resources are spent on areas that pose the greatest risk

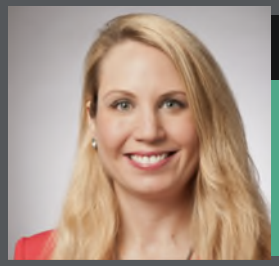
ndi REIMAGINED

Effective and Efficient Risk Assessments



ndi REIMAGINED

Thank You



Jennifer Urban

Partner

Foley & Lardner LLP

jurban@foley.com

414.297.5864

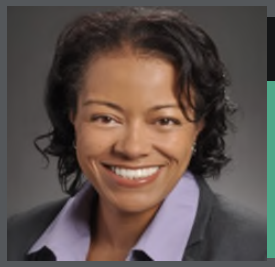
Mike Overly

Partner

Foley & Lardner LLP

moverly@foley.com

213.972.4533



Angela Johnson

Chief Information Security Officer and Vice President of Supply Chain

Children's Hospital of Wisconsin

ajohnson2@chw.org

Che Bhatia

Vice President, Cyber Resilience

Aon's Cyber Solutions (formerly Stroz Friedberg)

che.bhatia1@strozfriedberg.com

Yusuf Cassim

Vice President, Associate General Counsel,

Charles Schwab & Co., Inc.

yusuf.cassim@schwab.com

ATTORNEY ADVERTISEMENT. The contents of this document, current at the date of publication, are for reference purposes only and do not constitute legal advice. Where previous cases are included, prior results do not guarantee a similar outcome. Images of people may not be Foley personnel. | © 2020 Foley & Lardner LLP

FOLEY

FOLEY & LARDNER LLP