

Cybersecurity

Jonathan Gimblett, Covington & Burling LLP

Kyiv Arbitration Days, 13 September 2019

COVINGTON

BEIJING BRUSSELS DUBAI FRANKFURT JOHANNESBURG LONDON LOS ANGELES

NEW YORK PALO ALTO SAN FRANCISCO SEOUL SHANGHAI WASHINGTON

www.cov.com

The General Threat

- Criminal attacks on commercial data networks
 - Equifax, 2017 (145.5 million individuals affected)
 - Aadhar, 2018 (1.1 billion)
 - Forbes article, Aug. 2019: “Data Breaches Expose 4.1 billion Records in First Six Months of 2019.”
- Rampant identity theft
 - Dark web
- State-sponsored hacking and information operations
 - Democratic National Committee
 - Bundestag

The Threat in International Arbitration

- Expectation of privacy/confidentiality
 - Commercially sensitive information
 - Personal data
- Trustworthiness of evidence
- Network integrity

Growing Focus on the Problem

- Draft Cybersecurity Protocol for International Arbitration
 - ICCA
 - New York City Bar Association
 - International Institute for Conflict Prevention & Resolution
- Consultation Draft, April 2018
- Consultation period ended 31 December 2018
- Expected release of “Final” Version, Late 2019.

Draft Protocol – Key Features

- Cybersecurity defined:
 - “[T]he means employed to protect digitally stored information from intrusion by threat actors not authorized to have access that information.”
- Flexible, non-prescriptive approach.
- Reasonableness test to determine appropriate measures:
 - Nature of information at issue
 - Potential security threats / consequences of breach
 - Applicable rules / legal obligations
 - Other relevant circumstances

Issue: Where Does Responsibility Lie?

- Tension over “ownership” for cybersecurity procedures
- Party autonomy
 - Institutional rules commonly provide for agreement between the parties on the conduct of proceedings
 - *E.g.*, LCIA Article 14.2, SCC Article 23(1), ICSID Rule 20(1), etc.
- Authority of Tribunal
 - Institutional rules also generally provide for tribunal authority to set the conduct of proceedings
 - *E.g.*, UNCITRAL (2010) Article 17(1), LCIA Article 14.4-5, ICSID Rule 19.
- Institutional initiatives
 - *E.g.*, SCC Platform, ICC Cyber Security Guide for Business.

Issue: What Does Reasonable Mean in Practice?

- Different norms and perspectives of parties.
- Varying IT sophistication of arbitrators.
- Third party costs of data breaches.
- Can an arbitration ever be 100% secure from data breach?

Issue: Commercial v. Investor-State Arbitration

- Draft Protocol:

Although the Protocol is drafted with international commercial arbitrations in mind, Arbitral Participants may find it a useful starting point for ... investor-state arbitrations.

- Differing incentives, capabilities of parties in investor-state arbitrations.
- Secrecy considerations.
- Sanctions for misconduct.

Issue: Eventual Form of Guidance

- Protocol
- Code of Conduct
- Guidelines
- Rules