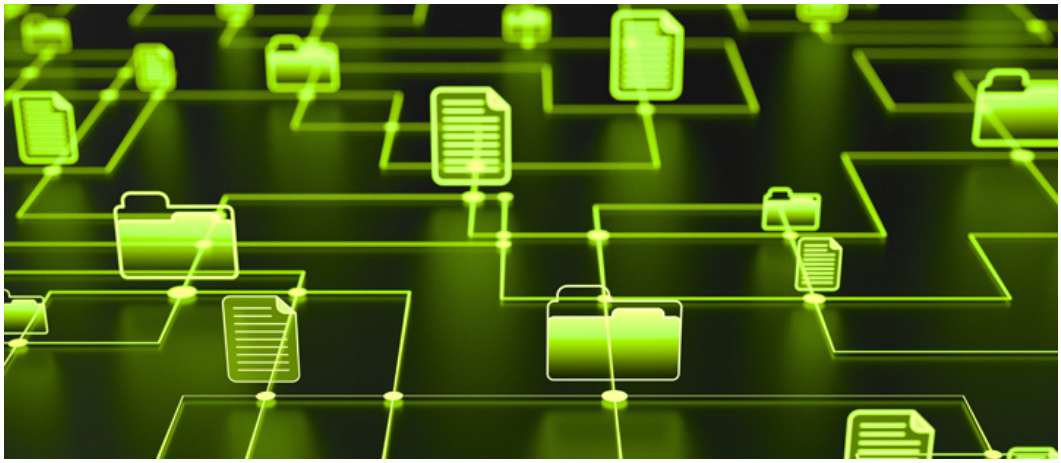
Legal BlackBook™

CyberInsecurity

JULY 2018

A NEW PROTOCOL TO COUNTER CYBERATTACKS IN INTERNATIONAL ARBITRATION



The drafters are seeking comments from in-house counsel.

BY OLIVIER P. ANDRÉ, HAGIT M. ELUL AND PAVLOS PETROVAS

In today's environment of ever-escalating data breaches in all sectors of society, international arbitration is not immune to cyberattacks. And a failure to implement reasonable cybersecurity protocols may have dramatic consequences for the players involved. In fact, given the sensitivity of the information involved in complex international disputes, international arbitrations may well become a prime target for cybercriminals unless defensive measures are quickly adopted.

What makes international arbitration so vulnerable? Digital discovery is inevitable and routinely involves highly sensitive information, such as trade secrets and business plans. The information collected is typically organized in easily searchable and retrievable data sets, such as pleadings, witness statements, expert reports, transcripts of hearings, arbitral deliberation materials, and draft and final awards. Moreover, each fixed or portable device, cloud-based storage platform and courtroom technology used is a digital portal potentially allowing for unauthorized access to arbitration-related materials. The fact that the information is held by a variety of digitally interdependent players (in-house and outside counsel, government officers and agencies, arbitral institutions and tribunals, etc.) only increases the likelihood that a data breach affecting one participant will affect all.

The risks are not merely hypothetical. One widely reported hacking incident took place during a contentious and politically sensitive arbitration between the Philippines and China over territorial claims in the South China Sea. In the course of that arbitration in 2015, a strain of malware originating in China targeted the Philippines' Department of Justice, the law firm representing the Philippines and the website of the Permanent Court of Arbitration in The Hague, allowing the hackers to steal data from infected machines.

The use of illegally obtained evidence by a party in the arbitration may violate the fundamental principles of integrity, fairness and due process that are inherent in any adjudicatory

proceeding. The disclosure of nonpublic information may result in economic and reputational damage to corporations, states, counsel, arbitrators and institutions whose actions were negligent or whose information was compromised. Data breaches may also lead to liability and regulatory sanctions under applicable privacy regimes. Perhaps most important, because confidentiality is at the heart of international arbitration, any cybersecurity shortcomings will inevitably erode the credibility and legitimacy of international arbitration as a form of dispute resolution.

Over these heightened concerns, the International Council for Commercial Arbitration (ICCA), the International Institute for Conflict Prevention & Resolution (CPR) and the New York City Bar Association jointly established a Working Group to raise awareness and offer protective measures for practitioners to fend off cybersecurity risks in international arbitration. Two of the authors of this article are members of this group, and on April 16 our group released for consultation a Draft Cybersecurity Protocol for International Arbitration (Draft Protocol). This document provides a framework for parties and arbitrators to determine and implement reasonable cybersecurity measures on a case-by-case basis.

The protocol warns that the credibility of international arbitration depends on ensuring a reasonable degree of protection of digital information exchanged during the proceedings, because, unlike other dispute resolution mechanisms, arbitration offers the unique advantage of maintaining the confidentiality of not only the information exchanged in the process, but also the existence of the arbitration itself (see, e.g., Rule 20 of the CPR Rules for Administered Arbitration of International Disputes on Confidentiality). Because of the high-value, high-stakes nature of the disputes, parties opting for this form of dispute resolution have an expectation that the arbitral process will have reasonable cybersecurity safeguards in place to protect nonpublic information from unauthorized access. Therefore, the protocol explains, "reasonable cybersecurity measures are essential to ensure that international arbitration maintains this advantage" (Draft Protocol, pp. 3-4).

The protocol goes on to identify substantive and procedural measures designed to prevent and mitigate the occurrence of a cyberattack. Specifically, the protocol invites parties and arbitrators to consider adopting measures:

- Limiting the disclosure of confidential information and personal data by applying the narrow discovery standard that is typical in international arbitration (Art. 6 and Commentary).
- Protecting the transmission of arbitration-related material by (i) identifying secure methods of document transmission for all participants (e.g., email, third-party platform, virtual data room, USB drive or other portable devices); (ii) encrypting, redacting, pseudonymizing or anonymizing sensitive information; and (iii) restricting access to confidential material through need-to-know or "attorneys-eyes-only" designations (id.).
- Managing data storage platforms by agreeing on the service provider, restricting access to specific users and limiting the nature, amount and duration of the data stored (id.).
- Mitigating data breaches by (i) identifying the source, nature and scope of the breach; (ii) retrieving lost information, correcting security systems'[Office1] weaknesses and preventing further breaches; (iii)[Office2] timely notifying all affected parties in accordance with applicable laws and regulations; and (iv) enlisting expert vendors and law enforcement, where appropriate (Art. 18 and Commentary).
- Detailing post-arbitration [Office3] document retention and destruction policies (Art. 6 and Commentary).

Cybersecurity is viewed as the shared responsibility of all participants in the arbitration, as any individual actor can be the weak link.

The Working Group purposefully avoided recommending specific cybersecurity measures. Recognizing that no one size fits all, the protocol does not require parties and arbitrators to follow a "specific and immutable" set of rules. Instead, it recommends a risk-based and individualized approach to determine which cybersecurity measures best fit the circumstances of each case. To help with such a determination, the protocol suggests conducting a risk analysis based on case-specific factors, which include the nature of the information at issue; the potential security threats and consequences of a data breach; and practical considerations, such as existing capabilities and costs (Arts. 7 and 12 and Commentary to Art. 7). Information that may require special care includes intellectual property, trade secrets, and commercially and politically sensitive information (Art. 8 and Commentary).

The parties may adopt the protocol by agreement, with specific language proposed by the Draft Protocol (see Schedule A), or the tribunal may decide on its own to follow it (Art. 1).

Procedurally, the protocol recommends that the tribunal discuss cybersecurity procedures and draw up a procedural order as early as possible—no later than the initial case management conference setting the procedural ground rules (Art. 14). This is in line with arbitration rules adopted by CPR, which expressly invite parties and tribunals to address cybersecurity issues at the very beginning of the proceedings (see, e.g., 2018 CPR Non-Administered Arbitration Rules, Rule 9.3[f]).

The protocol concludes that cybersecurity is the shared responsibility of all participants in the arbitration, as any individual actor can be the weak link. To help individuals improve their cybersecurity practices, Schedule C highlights general measures that actors may use to protect information.

The Working Group has set a consultative period until December 31. During this time it will hold public workshops worldwide to solicit comments. Interested parties may also submit comments at cybersecurity@arbitration-icca.org.

Following the consultative period, the Working Group will revise the protocol and release a final version in 2019. In the coming years, we anticipate further revisions as cybersecurity and

cyberthreats evolve, regulatory frameworks adjust and a consensus on best practices emerges.

From our perspective, in-house lawyers are the front line of cybersecurity, and the most important drivers of change in managing cyber risks. In most instances, they will be in a unique position to inform the participants in the arbitration about the fundamentals of effective cybersecurity precautions required by their case or the law. They will know what sensitive information that their corporations or governmental entities hold; what the most secure method of storage and transmission of sensitive information is; how to detect and remediate security vulnerabilities; and how to respond to data breaches.

The Working Group particularly invites in-house lawyers to provide comments on the protocol and engage in constructive dialogue with the broader arbitration community in order to develop a reasonable data security framework for international arbitration.

Olivier P. André *is Vice President, International and Dispute Resolution Services, at the International Institute for Conflict Prevention & Resolution (CPR) in New York and Member of the ICCA-CPR-NYCBA Working Group on Cybersecurity in International Arbitration. He is responsible for CPR's international activities, as well as international arbitration and mediation matters brought before CPR. He can be reached at oandre@cpradr.org.*

Hagit M. Elul *is a partner in Hughes Hubbard's New York office who focuses on business dispute resolution, including high-stakes cross-border litigation and international arbitration involving energy, pharmaceuticals, intellectual property, construction and professional services. She is also a Member of the Working Group and can be reached at hagit.elul@hugheshubbard.com.*

Pavlos Petrovas *is a litigation associate in Hughes Hubbard's New York office, where his practice focuses on international and U.S. litigation across a variety of industries, including energy, financial services and construction. He can be reached at pavlos.petrovas@hugheshubbard.com.*