ISSN : 1875-4120
Issue : Vol. 16, Issue 3
Published : May 2019

This paper is part of the TDM Special Issue on **"Cybersecurity in International Arbitration"** prepared by:

Stephanie Cohen
Independent Arbitrator
View profile

Mark C. Morril
MorrilADR
View profile

Transnational Dispute Management
www.transnational-dispute-management.com

TDM Special Issue "Cybersecurity in International Arbitration" - Introduction by S. Cohen and M.C. Morril

About TDM

TDM (Transnational Dispute Management): Focusing on recent developments in the area of Investment arbitration and Dispute Management, regulation, treaties, judicial and arbitral cases, voluntary guidelines, tax and contracting.

Visit www.transnational-dispute-management.com for full Terms & Conditions and subscription rates.

Open to all to read and to contribute

TDM has become the hub of a global professional and academic network. Therefore we invite all those with an interest in Investment arbitration and Dispute Management to contribute. We are looking mainly for short comments on recent developments of broad interest. We would like where possible for such comments to be backed-up by provision of in-depth notes and articles (which we will be published in our 'knowledge bank') and primary legal and regulatory materials.

If you would like to participate in this global network please contact us at info@transnational-dispute-management.com: we are ready to publish relevant and quality contributions with name, photo, and brief biographical description - but we will also accept anonymous ones where there is a good reason. We do not expect contributors to produce long academic articles (though we publish a select number of academic studies either as an advance version or an TDM-focused republication), but rather concise comments from the author's professional 'workshop'.

TDM is linked to **OGEMID**, the principal internet information & discussion forum in the area of oil, gas, energy, mining, infrastructure and investment disputes founded by Professor Thomas Wälde.

TDM Special Issue "Cybersecurity in International Arbitration" - Introduction

Stephanie Cohen[1], Mark C. Morril[2]

A 2016 program that we organized about cybersecurity in international arbitration had the provocative title "Red Flag Alert." Back then, which was around the time of the "Panama Papers" breach of now-defunct law firm Mossack Fonseca, any discussion about cybersecurity in arbitration largely centered on raising general awareness regarding the risks of cyber intrusion into the arbitral process and seeking to persuade the international arbitration community that user expectations about privacy and confidentiality mandate that all arbitral participants take steps to proactively address those risks.

The initial message was that international arbitration is not uniquely susceptible to cyber intrusion, nor is it immune. Much of what makes international arbitration attractive to its participants makes it enticing to cybercriminals. International commercial arbitrations routinely involve sensitive commercial and personal information that is not publicly available and has the potential to move markets, impact competition or damage reputations if disclosed. Now a highly digitized process, international arbitration typically involves multiple participants in different jurisdictions, including parties, counsel, arbitral institutions, arbitrators, experts and supporting vendors. Participants are digitally interdependent as the process typically involves the aggregation and transmission of large data sets and collaborative elements such as arbitrator deliberations, and anyone can be the "weak link" in protecting the security of the shared information. Proactive attention to cybersecurity is required to ensure that international arbitration will maintain its advantage over cross-border litigation as a more confidential and sophisticated forum to resolve complex commercial disputes.

The initial message has been well-received. According to a recent Bryan Cave Leighton Paisner survey, arbitration participants widely recognize that effective cybersecurity requires that all participants in the process be actively engaged with a cybersecurity strategy and share responsibility. Counsel, arbitrators and institutions are more aware of the risks of digital intrusion, including that the "human factor" poses the biggest security risk of all. Users proactively address these risks in their own businesses and have begun insisting that arbitral institutions, counsel and arbitrators step up efforts to protect the digital information users submit to the arbitral process.

Three years in, the conversation is no longer limited to "whether" and "why" arbitral participants should pay heed to cybersecurity, but rather has evolved to consider a series of (sometime contentious) questions about "who," "what" and "how." Who will (and who should) ultimately take the lead as among the various arbitral participants and non-governmental organizations in driving change? What cybersecurity practices should be implemented in participants' regular business operations and is it desirable or foolhardy to define certain practices as part of a minimum standard of security? How should cybersecurity measures for

[1] Stephanie Cohen is an independent arbitrator in New York City. For more information, visit www.cohenarbitration.com.

[2] Mark C. Morril is an independent arbitrator and mediator in New York City. For more information, visit www.morriladr.com.

individual arbitrations be established, and who is in the best position (the parties and their counsel, the arbitral tribunal or arbitral institutions) to determine what measures should apply?

An important milestone in the conversation occurred in 2018 when a Working Group on Cybersecurity in International Arbitration established by the International Council for Commercial Arbitration, the New York City Bar Association and the International Institute for Conflict Prevention and Resolution released a Consultation Draft Cybersecurity Protocol[3] (the "Cybersecurity Protocol") at the ICCA Congress in Sydney. The Draft Cybersecurity Protocol was well-received as an initiative to facilitate collaboration between parties and arbitrators in individual arbitration matters about what cybersecurity measures, if any, should reasonably be taken in light of the individualized risk profile of each case, and the Working Group received substantial feedback during the consultation period. The forthcoming final revision of the Cybersecurity Protocol promises to be a useful tool for the arbitration community to determine what cybersecurity measures are reasonable in individual arbitration matters going forward.

Also in 2018, the International Bar Association published Cybersecurity Guidelines[4] focused on providing best practices for law firms to protect themselves from breaches. Unlike the Cybersecurity Protocol, the IBA Cybersecurity Guidelines do not focus on issues unique to the arbitration process, but they do offer general, practical recommendations about technical and organizational measures that law firms can take to improve their security posture, and they reference additional resources such as bar association materials from across the globe.

This TDM Special Issue on Cybersecurity in International Arbitration continues to take the conversation forward. The first two articles in the Issue consider the unique roles—and consequent cybersecurity obligations—of important participants in the arbitral process: arbitrators and arbitral institutions. Our own article, *A Call to Cyberarms: the International Arbitrator's Duty to Avoid Digital Intrusion*, first published in the Fordham International Law Journal, considers the role of the arbitrator as the presiding actor in the arbitration process. We posit that existing and well-established obligations of arbitrators to maintain confidentiality, be competent and preserve the integrity and legitimacy of the arbitral process impose a front-line duty on arbitrators to take reasonable steps to avoid unauthorized digital intrusion. We advocate a risk-based approach to determine what is reasonable and contend that arbitrators must attend to their "baseline" security as their day-to-day digital architecture and security practices pre-exist individual arbitrations. At the same time, we recognize the digital interdependence of all participants in the process and argue that cybersecurity is a shared responsibility.

Claire Morel de Westgaver sees institutions as being best placed to raise the level of cybersecurity in international arbitration as a whole. Her article, *A Systemic Approach to Cybersecurity in International Arbitration – Imperative and Implementation,* analyzes the limitations of a risk-based approach to cybersecurity and urges a "systemic approach" that would create cybersecurity obligations of general application, imposed on all stakeholders in the arbitration community. Morel de Westgaver considers cybersecurity a matter of "administration" rather than "procedure," and thus proposes that institutions amend their rules based on accepted information security principles to address baseline risks applicable to virtually every international arbitration.

[3] https://www.arbitration-icca.org/media/10/43322709923070/draft_cybersecurity_protocol_final_10_april.pdf

[4] https://www.ibanet.org/Document/Default.aspx?DocumentUid=2F9FA5D6-6E9D-413C-AF80-681BAFD300B0

Institutional rules typically provide a general framework for particular aspects of the arbitration process, such as document disclosure, but leave it to the tribunal to determine how to apply that framework in individual matters. It thus seems unlikely that institutional rules about cybersecurity, or even the adoption of secure sharing platforms, however welcome both might be, would negate the need for ongoing shared responsibility for cybersecurity by other participants in the arbitral process. In this respect, we note that the procedural, risk-based approach recommended by the Draft Cybersecurity Protocol to address cybersecurity issues in individual matters is not necessarily incompatible with institutional cybersecurity initiatives, including new rules. **Javier Fernández-Samaniego** and **Gonzalo Hierro Viéitez** recognize the significance of the Draft Protocol in raising greater awareness about cybersecurity risks in international arbitration and commend its individualized, risk-based approach to cybersecurity. In *The Draft ICCA-CPR-New York City Bar Association Protocol for Cybersecurity in Arbitration: A Leading Light, at Least,* Fernández-Samaniego and Hierro Viéitez analyze the Draft Protocol. They opine that cybersecurity issues will evolve with changing technology, new cyber threats, changing laws and regulatory schemes, and argue that the Draft Protocol will achieve wide use in the arbitration community and avoid premature obsolescence by refraining from specifying cybersecurity measures that should be adopted in every arbitration. They also consider whether the Cybersecurity Protocol will evolve into a "soft law" code of conduct over time.

A second group of articles provides an international comparative viewpoint and underscores the significance of the proliferation of data protection laws around the globe to the emergence—at least in developed nations—of a security imperative. **Pablo Debuchy** and **Alex Kamath**, in their article entitled *Current Cybersecurity Practices in Latin American International Arbitration,* consider the data protection and cybersecurity requirements of arbitral rules and legislation in Argentina, Brazil, Chile and Mexico. They then provide suggestions as to how the guidance provided in the Draft Cybersecurity Protocol can best be adopted in Latin American arbitration practice. **Sergey Alekhin**, **Alexis Foucard** and **Greg Lourie**'s article, *Cybersecurity, International Arbitration and the Ethical Rules and Obligations Governing the Conduct of Lawyers,* provides an overview of the ethical rules and obligations applicable to lawyers in France, Germany, Switzerland, Russia, the United States and the United Kingdom. The authors endeavor to distill from these sources an international minimum standard for cybersecurity in international arbitration. **Nishanth Vasanth** and **Arpan Banerjee**'s article, *(Cyber)securing the Indian Arbitral Transition – Paperbooks, E-Courts and Practicing Therein,* explores the possibility of cybersecurity reform in the evolving Indian arbitration regime. They consider that, notwithstanding some considerable headwinds and impediments including sluggish digitization of the judiciary and a conservative litigation culture, it would be opportune to develop cybersecurity measures in the arbitration regime while the entire Indian legal system is digitizing.

A third group of articles explores practical issues that have arisen in respect to cybersecurity. **Edna Sussman**'s article, *Cyber Intrusion as the Guerilla Tactic: an Appraisal of Historical Challenges in an age of Technology and Big Data,* considers some of the challenges arbitrators will face as they increasingly are presented with issues related to breaches of cybersecurity. How should tribunals treat proffered evidence that was illegally obtained? What sanctions should a tribunal impose if parties or their representatives are involved in improperly obtaining evidence? What is the impact of inadmissible evidence on decision-making and to what extent does an arbitrator have a duty to report a cybercrime? Lastly, **Peter A. Halprin**, **Grant Brown** and **Wendy Chiapaikeo** consider what insurance coverage may be available to law firms in the event of a cyber incident.

The articles in this Special Issue illustrate the range of issues and current points of debate that surround consideration of cybersecurity in the arbitration context. It may well be that some questions the authors pose will not result in definitive conclusions. Institutions, parties, counsel and tribunals will all likely have substantial cybersecurity roles going forward. We can foresee cybersecurity measures being addressed in institutional rules, agreements between parties, and in case management conferences and procedural orders. The use of secure document management platforms may emerge as the norm. All of this would be consistent with the fundamental conclusion of the ICCA-NY City Bar-CPR Working Group that cybersecurity is optimally a shared responsibility among all arbitral participants. Similarly, it seems likely that cybersecurity practices will continue to vary among different jurisdictions, even as some common standards, urged by the proliferation of data protection laws, evolve. All participants will grapple with practical issues such as the treatment of illegally obtained evidence, the allocation of costs, the insurance consequences of cyber incidents and considerations of relative resources and proportionality.

We are grateful to the contributors for their thoughtful analysis of these issues. We hope the readers will find the articles and issues as interesting as we have. In all events, we look forward to continuing this important conversation and welcome your views.