Cybersecurity in Arbitral Proceedings: How to Kick-Start the Conversation about Protecting your Clients' Data

Kluwer Arbitration Blog
November 25, 2018

Vanessa Naish (Herbert Smith Freehills LLP) and Maguelonne de Brugiere (Herbert Smith Freehills)

Please refer to this post as: Vanessa Naish and Maguelonne de Brugiere, 'Cybersecurity in Arbitral Proceedings: How to Kick-Start the Conversation about Protecting your Clients' Data', Kluwer Arbitration Blog, November 25 2018, http://arbitrationblog.kluwerarbitration.com/2018/11/25/cybersecurity-in-arbitral-proceedings-how-to-kick-start-the-conversation-about-protecting-your-clients-data/

The advent of the EU General Data Protection Regulation (**GDPR**), which came into force on 25 May 2018 within the EU and the European Economic Area, has sparked a renewed debate within the arbitration community about importance of adequate consideration being given to the collection, preservation and protection of data in arbitral proceedings. The GDPR has also highlighted that all parties involved in the arbitral proceedings, be they arbitrators, counsel, institutions, experts, or even witnesses, are potentially taking on the roles of controller[fn] 'Controller' is defined in the GDPR as "*the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law*".[/fn] or processor[fn] 'Processor' is defined in the GDPR as "*natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller*".[/fn] of data, and risk incurring significant penalties if they fail to comply with the regulatory requirement to ensure that appropriate security measures are

in place to protect personal data. However, the risks of failing to implement adequate cybersecurity practices, in particular in arbitration, are not new.[fn] We have seen the impact of cyberhacks in arbitration already, with documents obtained through hacking increasingly being relied on in proceedings as was the case in *Libananco v Republic of Turkey* (ICSID ARB/06/8), *Opic Karimum Corporation v Venezuela and Kılıç v. Turkmenistan* (ICSID Case No. ARB/10/14), *Caratube International Oil Company and Mr Devincci Saleh Hourani v Kazakhstan* (ICSID Case No. ARB/13/13). High profile hackings also include the hacking of the website of the Permanent Court of Arbitration in the Hague in 2015 to obtain information regarding a maritime boundary dispute between China and the Philippines. And those are just a few of the cyberattacks and hacking attempts that have been uncovered or heard of in the public domain. Undoubtedly, attacks of this nature will only continue to rise.[/fn] Given the types of companies which might choose to resolve their disputes by way of arbitration, the frequent involvement of state entities, and the potential impact on the financial markets that arbitration awards can have, arbitration proceedings are prime targets for hackers.

We have seen promising developments in the field of cybersecurity in arbitration in the past year, with the publication of the draft International Council for Commercial Arbitration (**ICCA**) Cybersecurity Protocol for International Arbitration in April, and the International Bar Association's (**IBA**) Cybersecurity Guidelines in October. The former aims to provide a framework which parties would need to agree to apply to their proceedings. It is still in draft consultation form and does not yet set out proposals in terms of the technological or organisational measures to be put in place to ensure the cyber integrity of proceedings. By contrast, the latter contains some very practical guidance on technological measures to avoid compromising the safety of data. However these guidelines are primarily aimed at law firms and single practitioners and are not tailored to arbitration proceedings. Neither provides a complete framework for cybersecurity in arbitration, nor can they. In reality, addressing cybersecurity in arbitration comprehensively will require a collective effort on the part of arbitrators, practitioners and institutions to change our working practices and to ensure that the correct measures are implemented on a case by case basis in each proceeding.

The parties and their legal advisors

In practice, cybersecurity in any specific arbitration will need to start with the parties and their legal advisors. Given the importance of confidentiality in the client-lawyer relationship, larger law firms will have stringent cyber security protections and internal rules and codes for lawyers regarding the protection of client data. Legal advisors are often best placed to assess the nature of the information that will be shared during the arbitral process and the impact of a cybersecurity breach on their client's business. They are also important actors in shaping the arbitral procedure and the main parties contributing to the flow of data.

Cybersecurity must therefore start with an initial risk assessment to be carried out in conjunction with the client. Legal advisors might consider whether highly commercially sensitive data is pertinent to the dispute and whether a particular approach should be taken to the collation of data from the client or the storage and review of that data within the law firm. They may also wish to discuss with the client whether release of that data, any particular pieces of information, the fact of the arbitration or its outcome could have a significant impact on their business.[fn] E.g. for a listed company, the outcome of an arbitration may affect share price and the hack of arbitral award before it has been sent to the parties could have important ramifications.[/fn]

Depending on the risk assessment carried out for the specific arbitration, a number of further steps may be necessary at the outset of the arbitration. Parties should consider secure ways of sending initial submissions to institutions and Tribunal members. Similarly, when considering who to appoint as an arbitrator or analysing the appointment made by the other side or arbitral institution cyber security should be a factor. Where they deem necessary, parties may wish to send a cyber practice checklist to nominated arbitrators to identify any potential security concerns which may justify a decision to refuse to appoint or challenge an arbitrator's appointment.

Once the arbitral tribunal has been constituted, cybersecurity should be one of the issues raised and discussed at the first procedural conference. The ICCA Protocol may be used to prompt that discussion or to form a basis for an arbitral protocol or agreement covering the proceedings. The cybersecurity measures that are appropriate will be based on the types of data (commercial and personal), the level of risk of a cyber-attack and the implications of breach for the parties involved. Cost will also be a factor. As part of this analysis, all stakeholders involved at this stage of the process will want to reach agreement about how, and with whom, data is to be shared and stored. Options might include the use of end-to-end encryption for email, password protection on documents sent by email, the use of secure file transfer to share documents or hosting all documents on a secure data storage platform which requires two stage authentication and does not permit downloads.

The Tribunal

It is also important that arbitrators acknowledge the critical role which they play in determining and implementing cybersecurity measures. In light of extensive digitalisation of arbitration proceedings and the increasing risks and costs associated with cyberattacks, an arbitrator's duty to preserve and protect the integrity and legitimacy of the arbitral process arguably now extends to ensuring that adequate cybersecurity measures are adopted in each proceedings.

Arbitrators should ensure they are taking appropriate cybersecurity and confidentiality precautions. On a practical, non-technical level, this might entail very basic steps, such as the use of privacy screens when viewing confidential documents on screen in public settings, ensuring that his or her operating system automatically applies updates, that their antivirus/malware software is up to date, that they use a secure email provider, that they have a unique login to their computer and that hard drive encryption is activated on their computer or any other electronic device they plan to use during the arbitration. Individuals acting as

arbitrators may also want to consider whether their cyber breach insurance is sufficient.

It also follows that Tribunals should give adequate consideration to the measures that need to be taken to preserve the confidentiality of the proceedings and to safeguard the arbitral process. Indeed, given the scope of their powers and the ongoing decisions which they make regarding the volume and flow of information, Tribunals are well placed to invite parties to make submissions on the cybersecurity measures they believe to be necessary to the proceedings in question, and to adjudicate on the appropriate levels of protection necessary, bearing in mind the consequences of breach and the costs of implementing the measures, as well as to determine the penalties for breach. Any cybersecurity protocol or agreement should cover the reporting of security concerns and actions that should be taken in the event of known breach.

Arbitral Institutions

Arbitral Institutions similarly have an important role to play in safeguarding arbitral proceedings from cyber-breaches. Arbitral Institutions are often the first to receive a transfer of data from the parties in an arbitration. Depending on the rules in question, they may also be copied in on much of the same data as is sent to the arbitrators.

However, the extent to which arbitral institutions should be involved in the security of the wider arbitration is less clear. Institutions may be questioning whether it is an unnecessary cyber risk for them to receive the large quantities of confidential data that they currently receive. Rule revisions may be being considered to highlight the importance of cyber security, along with specific institutional cybersecurity protocols. But how much further should arbitral institutions go? Should institutions be offering training to arbitrators on this issue? Should they require potential arbitrators to confirm that they have appropriate levels of

security in place? Should other institutions follow the HKIAC's example in offering or facilitating the use secure storage platforms for arbitrations?[fn] Article 3.1(e) of the new HKIAC Rules. [/fn] The market will be watching all the arbitral institutions with interest to see whether any consensus on these issues emerges, or whether each institution will reach their own conclusion on where to draw the line.

Conclusion

As the global integration of electronic communications continues to grow with the daily use of new communication technologies, we all have a part to play in ensuring that the arbitral process is not left behind. A failure to adapt our processes to new cyber threats jeopardises the attractiveness of arbitration as an international method of dispute resolution. Simple steps, such as those recommended above, can be taken at the outset of any arbitration proceedings to ensure that appropriate measures are put in place to preserve and protect the confidentiality of data in our proceedings. These steps are not necessarily complex ones. What they require, however, is a mindset shift, and an acceptance on the part of all practitioners that cybersecurity is not an optional point for discussion at the outset of proceedings, but a necessary one.