Kluwer Arbitration Blog

Cybersecurity in International Arbitration: Don’t be the Weakest Link

Claire Morel de Westgaver (Bryan Cave Leighton Paisner LLP) · Friday, February 15th, 2019 · Bryan Cave Leighton Paisner LLP

In recent years there has been a dramatic increase in cyber-attacks on corporates, governments and international organisations. Arbitration proceedings are not immune from the threat of attack as previous incidents demonstrate.

The publication last year of a draft Cybersecurity Protocol for International Arbitration by the International Council for Commercial Arbitration, the International Institute for Conflict Prevention and Resolution (**CPR**) and the New York City Bar was an important step in raising awareness of cybersecurity risks and initiating a discussion within the arbitration community. The discussion has focussed on the sorts of measures that may be appropriate to protect documents and data against unauthorised access. However, there appears to remain a critical issue upon which consensus has not yet been found: the manner in which cybersecurity measures should be designed, implemented and enforced.

As a firm, **BCLP** wanted to contribute to the discussion and formulation of cybersecurity strategies by using our Annual Arbitration Survey to find out what arbitrators, corporate counsel, external lawyers, users of arbitration and those working at arbitral institutions thought about these and other related issues.

The full **BCLP Arbitration Survey 2019** can be downloaded here and some of the key findings are summarised below.

Cybersecurity is an important (and real) issue

The results of this year’s survey confirm that the importance of cybersecurity is widely recognised. 90% of respondents said that it was an important issue in international arbitration, with 11% of respondents indicating that they had had experience of arbitral proceedings being subject to a cybersecurity breach. That more than 1 respondent out of 10 was involved in an arbitration where someone was able to obtain unauthorised access to electronic documents or other information in itself demonstrates the pressing need for cybersecurity measures to be put in place.

What measures

The two factors regarded by the largest number of respondents as being relevant to a cybersecurity strategy were the level of sensitivity/commercial value of the documents to be used in an arbitration (94%) and the consequences for the parties if someone were to gain unauthorised access to the documents/information (78%). Other factors included the costs of implementing the proposed measures (70%) and the extent to which the proposed security measures may hinder the ability of a party to present its case (61%).

In nearly all cases the percentage of respondents who regarded a particular measure as desirable was significantly higher than the percentage of respondents who had seen the same measure in practice. 83% of respondents thought it desirable for electronic documents to be transferred by means of a secure shared portal, as opposed to 53% who had seen the measure adopted in practice. 50% of respondents thought participants in an arbitration should have in place appropriate firewalls and antispyware and/or antivirus software, as opposed to 12% who had seen the measure implemented in practice.

Who and when

The majority of respondents agreed that active engagement by all participants to an arbitration would be necessary in order for a cybersecurity strategy to be effective. 96% of respondents thought that the parties would need to actively engage with the process and 94% thought that the arbitrators would need to actively engage with the process. There was, however, a recognition that obtaining agreement from all participants to observe cyber security measures would not be straightforward. Only 56% of respondents thought that obtaining the agreement of the parties or the arbitrators to observe security measures would be very or relatively easy.

There was a large measure of consensus about the desirability of considering cybersecurity measures at an early stage of the proceedings but opinion was divided over who should take the lead on initiating discussions on cybersecurity issues. 48% thought the parties should take the lead, 31% thought the supervising arbitral institution (if any) should take the lead, and 21% thought it should be the tribunal. Among respondents who act as arbitrators, nearly half (48%) thought that the parties should take the lead in initiating discussion. This suggests that a significant proportion of arbitrators are reluctant to actively engage in the assessment of cybersecurity risks and the development of appropriate measures. Whilst arbitrators may have legitimate reasons for such a position, as reflected in the numbers referred to above, there may well be circumstances where parties may not be able to take a view or agree on appropriate cybersecurity measures.

How to implement

One question that has been the subject of discussion is whether cybersecurity measures is a procedural matter, best handled by the tribunal after hearing submissions from the parties, or an administrative matter, best handled by the supervising arbitral institution, assuming there is one. Just over half of respondents (52%) thought it was a procedural matter for the tribunal, 41% thought it was an administrative matter for the institution and 7% were undecided.

This is an interesting finding as there are pros and cons with both approaches and the procedural or administrative nature of measures is likely to dictate whether such measures should be implemented in procedural orders, arbitration rules or arbitrators' terms of appointment.

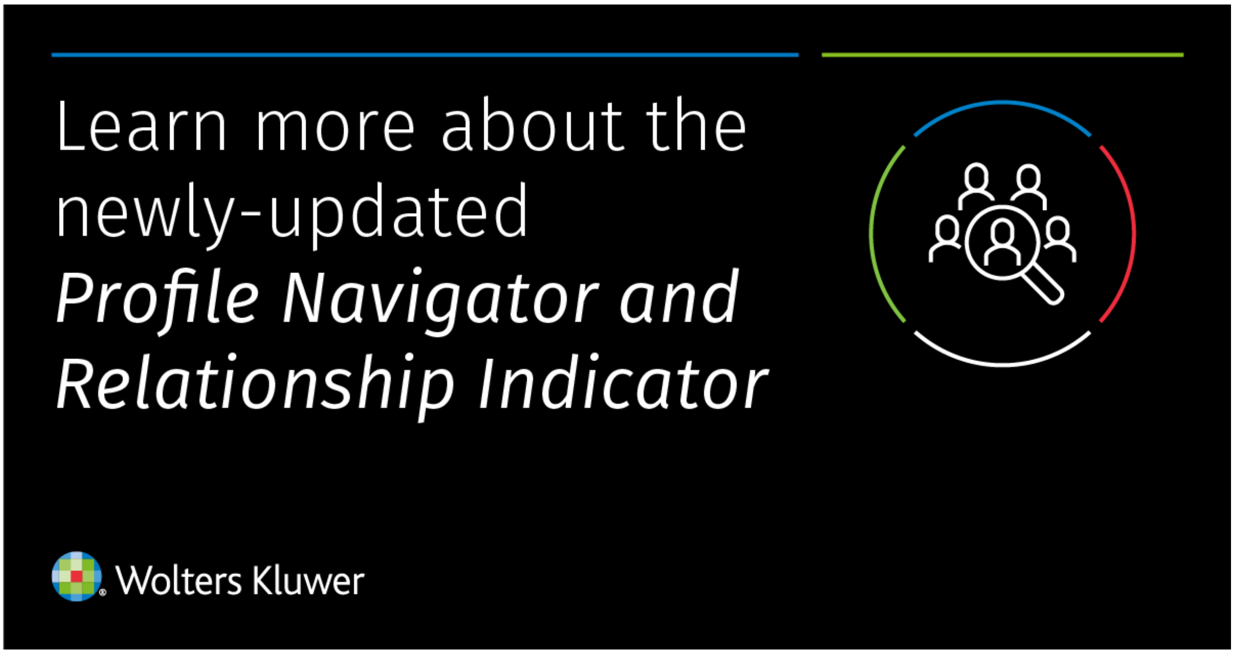
Giving arbitrators the power to impose cybersecurity measures may not sit well with the background and training of all arbitrators, and the nature of their main function. Further, depending on their level of interest and the information technology environment in which they operate, individual arbitrators may take very different approaches to cybersecurity. Whilst the nature and potential consequences of cybersecurity risks may vary from one case to another, there are certain cybersecurity risks that will arise in virtually every international arbitration. In that context, the adoption of mandatory measures addressing baseline risks would raise the level of cybersecurity in international arbitration on a more systemic basis. In addition, given that to be effective any measures adopted will have to be adhered to by the arbitral tribunal, arbitrators may find themselves in a situation where their personal preferences or practices may conflict with the objectives sought to be achieved by a robust cybersecurity strategy.

52% of respondents felt that a tribunal should have the power to impose measures in cases where the parties were unable to agree them. 71% of respondents thought that a tribunal should have the power to impose sanctions on a party that breaches data security measures that have been agreed or ordered by the tribunal. What remains unclear is how, in a system where cybersecurity measures are ordered by a tribunal (rather than stemming from arbitration rules for example), a breach of a measure on the part of the tribunal itself should be handled. It is difficult to contemplate that a tribunal would be competent to sanction itself.

It was clear that respondents felt that arbitral institutions could have an important role to play in dealing with issues of cybersecurity. 68% of respondents said that they would be more likely to use the arbitration rules of an institution that was able to provide advice or assistance on appropriate data security measures. 70% of respondents felt that support from within an institution's secretariat would be useful to improve cybersecurity.

47% of respondents indicated that, where appropriate, their clients would be willing to pay a higher fee/incur an additional cost with an arbitration institution that provided advice and assistance on appropriate security measures and/or provided a secure platform (or similar) on which all communications and data sharing storage in the arbitration could take place. This particular finding may provide comfort to institutions. It suggests that users recognise that there is a cost aspect to cybersecurity and that the pressing need for structural solutions to be put in place may in some circumstances justify the associated increase in cost. As suggested in a previous blog post published on 6 October 2017, Cybersecurity in International Arbitration – A Necessity and an Opportunity for Arbitral Institutions, arbitral institutions are particularly well positioned to implement systemic solutions to cybersecurity risks; something that a risks-based approach by which risks are assessed and dealt with by parties and tribunals on a case-by-case basis is less likely to achieve.

To make sure you do not miss out on regular updates from the Kluwer Arbitration Blog, please *subscribe here. To submit a proposal for a blog post, please consult our Editorial Guidelines.*


Learn more about the newly-updated *Profile Navigator and Relationship Indicator*
Wolters Kluwer

This entry was posted on Friday, February 15th, 2019 at 8:37 am and is filed under Cybersecurity, Cybersecurity Protocol, Surveys
You can follow any responses to this entry through the Comments (RSS) feed. You can leave a response, or trackback from your own site.