The Role of Arbitral Institutions in Cybersecurity and Data Protection in International Arbitration

Kluwer Arbitration Blog
November 24, 2020

Diana Sulamazra Abdul Rahman (Asian International Arbitration Centre)

Please refer to this post as: Diana Sulamazra Abdul Rahman, 'The Role of Arbitral Institutions in Cybersecurity and Data Protection in International Arbitration', Kluwer Arbitration Blog, November 24 2020, http://arbitrationblog.kluwerarbitration.com/2020/11/24/the-role-of-arbitral-institutions-in-cybersecurity-and-data-protection-in-international-arbitration/

Cybersecurity and data protection have been dominating conversations in the international arbitration community in recent years. From an analysis of how the stakeholders may be best equipped to address cybersecurity risks, to considerations on maintaining confidentiality in international commercial arbitration, as well as calls to address the impact of the General Data Protection Regulation ("GDPR") on virtual arbitration proceedings, much scrutiny has been afforded to these issues. Discussions on this topic have been further enhanced following the release of the IBA Cybersecurity Guidelines (the "IBA Guidelines"), the ICC-NYC Bar-CPR Protocol on Cybersecurity in International Arbitration, the latest being the 2020 Edition (the "Cybersecurity Protocol"), as well as the public consultation draft of the ICCA-IBA Roadmap to Data Protection in International Arbitration. The author opines that cybersecurity and data protection go hand in hand as both involve the receipt, usage, processing, transmission, and preservation of data in any given setting. The ongoing COVID-19 pandemic has further heightened the importance of these issues since more proceedings with high value and business-sensitive information are being conducted wholly online, are frequently held in different jurisdictions, and often involve unencrypted digital exchanges.

A previous article has highlighted how arbitral institutions are uniquely positioned to address cybersecurity risks both consistently and sustainably. This post now aims to further examine the measures that arbitral institutions may take to alleviate cybersecurity risks and to ensure that data protection principles are adhered to in institutional proceedings.

Institutional Rules and Case Management

Effectively, most arbitrations are currently managed, if not completely, through electronic and digital means, *e.g.* where correspondences and procedural papers are transmitted via email or digital file transfers. It is foreseeable that in time, more and more of these 'paperless' proceedings will take place. Undoubtedly, institutions should be up to date to the technological needs of the parties and their institutional rules and procedural guidelines should factor in cybersecurity concerns. One such example can be found in the Hong Kong International Arbitration Centre ("HKIAC") 2018 Administered Arbitration Rules, where Article 3.1(e) specifically mandates the uploading of files "*to any secured online repository that the parties have agreed to use*" as a recognised means of communication. Another example is found in the London Court of International Arbitration ("LCIA") 2020 Arbitration Rules that incorporate new provisions on data protection, cybersecurity and regulatory issues. Specifically, Article 30A provides that *"at an early stage of the arbitration the Arbitral Tribunal shall…consider whether it is appropriate to adopt:*

(i) any specific information security measures to protect the physical and electronic information shared in the arbitration; and

(ii) any means to address the processing of personal data produced or exchanged in the arbitration in light of applicable data protection or equivalent legislation."

In circumstances where such considerations have yet to be incorporated in the institutional rules or guidelines, possible steps to take would be for the administering institution to either alert the tribunal, upon confirmation of its appointment, of the existence of the Cybersecurity Protocol, or to include the protocol as part of the institution's code of conduct of arbitrators.

The Cybersecurity Protocol neither lists any specific measures to be taken, nor does it establish any liability standards for any purpose (*Principle 14*). Instead, the Cybersecurity Protocol authorises the tribunal to determine the appropriate cybersecurity measures (*Principles 11 and 12*). Although the commentary to Principle 11 acknowledges such authority, determination of applicable information security measures should fall back to parties' agreement.

In terms of case management, the arbitration community can look forward to the soon to be released Protocol for Online Case Management in International Arbitration by the Working Group on LegalTech Adoption in International Arbitration (the "LegalTech Working Group"). Having just released its Consultation Draft in July 2020, the focus of the LegalTech Working Group is the development of a consistent approach to the adoption and use of online case management tools that encompasses confidentiality, data protection, and sustainable values thereof.

Internal Management Systems

Arbitral institutions hold large volumes of valuable, highly commercial, and sensitive information pertaining to matters they administer, access to which may have far reaching impacts. This makes arbitral institutions a highly attractive target for cybercriminals. Previous incidents such as the intercepted correspondence in *Libananco v Republic of Turkey (ICSID ARB/06/8)*, and the attack on the Permanent Court of Arbitration (PCA) website during the China–Philippines maritime boundary dispute, have further emphasised the need for arbitral institutions to have effective cybersecurity technology and mechanisms in place to safeguard the confidentiality of proceedings.

What steps then should arbitral institutions take? As a reference, the IBA Guidelines, although aimed at lawyers and legal firms, contains several recommendations which are worth considering by all stakeholders in the arbitral process. They include the following three areas:

1. *Technology*: implementing endpoint protections, ensuring the use of secure networks, encrypting data and devices, strictly managing access control, implementing audit logs as well as implementing data retention, and loss recovery capabilities.
2. *Organisational processes*: implementing strong username and password

management with multi-factor authentication, implementing protection protocols, conducting periodic system testing, implementing a cybersecurity policy, implementing vendor and third-party provider risk management, and considering cyber liability insurance.

3. *Staff Training*: educating employees about the importance of cybersecurity and common threats as well as providing staff with essential cybersecurity tips and advice.

In the *Data protection, privacy, confidentiality and cybersecurity* session at the 22nd Annual IBA Arbitration Day in 2019, Catherine Amirfar further posited some concrete prevention techniques and tips, which included limiting the collection and use of sensitive data, understanding the organisational assets and electronic architecture, as well as establishing a cyber threat mitigation plan in the early stages. Although limiting the collection of sensitive data may be impracticable for arbitral institutions, implementing cybersecurity and data protection measures by design within the institutional structure may limit any risk of breaches exponentially.

Virtual Proceedings

Since the outbreak of the COVID-19 pandemic, virtual hearings have become the norm in present times. It is likely that the trend will stay due to its efficiency and convenience. Many arbitral institutions have also introduced their own guidelines to manage and support the conduct of virtual hearings. A quick comparison across some of the protocols and guidelines issued indicates that the minimum standards of cybersecurity and data protection measures in virtual proceedings include, amongst others, usage of access-controlled video conferencing platform/software with an authentication process, usage of encrypted communications, clear identification of data storage facilities, and the applicable laws as well as robust administrative controls in order to maintain the security and integrity of data. The utility of checklists is also encouraged to ensure that the proceedings are conducted in compliance with local as well as regional data protection laws, such as the GDPR.

Conclusion

The benefits for arbitral institutions to push for greater emphasis and devoting resources towards cybersecurity and data protection cannot be understated. With the threats of cybersecurity constantly growing coupled with the profound impact of strict data protection laws, addressing these concerns through innovative means provides institutions with the advantage to promote institutional arbitrations particularly to security-conscious high-value commercial arbitration users. Most importantly, it considerably minimises the chances of untoward incidents such as the PCA website hack ever happening again. As the maxim goes, *abundans cautela non nocet* (abundant caution does no harm).