Online Dispute Resolution Platforms: Cybersecurity Champions in the COVID-19 Era? Time for Arbitral Institutions to Embrace ODRs

Kluwer Arbitration Blog
September 25, 2020

Wendy Gonzales (CyberArb) and Naimeh Masumy

Please refer to this post as: Wendy Gonzales and Naimeh Masumy, 'Online Dispute Resolution Platforms: Cybersecurity Champions in the COVID-19 Era? Time for Arbitral Institutions to Embrace ODRs', Kluwer Arbitration Blog, September 25 2020,
http://arbitrationblog.kluwerarbitration.com/2020/09/25/online-dispute-resolution-platforms-cybersecurity-champions-in-the-covid-19-era-time-for-arbitral-institutions-to-embrace-odrs/

The COVID-19 pandemic has led to an increase in the interest in alternative dispute resolution, especially arbitrations conducted online. The greater utilization of online platforms and digitization has coincided with the growing frequency and sophistication of cyber-attacks. Reportedly, by 2021 a business will fall victim to cyber-attacks every 11 seconds. Therefore, it is critical for these platforms to provide secure digital environments where the exchange of communications, storage of evidence and files, and virtual hearings can be conducted remotely and securely. The necessity of providing easily accessible platforms apt to handle complex disputes has brought to light the importance of online dispute resolution (ODR) platforms. Some of these platforms have taken the initiative to encompass robust security measures through which they implement standards consistent with the existing protocol on cybersecurity (2020 Protocol). Such measures may shift the arbitration landscape, in which these platforms may play an important role in

institutional and *ad hoc* arbitration globally.

This note highlights some of the good practices of security measures, which mirror standards enshrined in the 2020 Protocol. In doing so, we make references to notable ODRs that embody these features. We then underscore the role of arbitral institutions in giving greater recognition to cybersecurity needs as they embark on the digitization of their services.

A. Online dispute resolution platforms: a viable alternative to ensure cybersecurity?

There has been a surge in the number of ODRs in the recent years. There platforms leverage sophisticated software that allows them to handle several simultaneous uploads and downloads of files in real time, and the technological advances of ODRs render these platforms suitable to addressing the emerging needs of security in the face of many cyber threats. Platforms have taken practical measures to apply and embody some of the distinctive features proposed by various cybersecurity instruments, including 2020 Protocol and international standards (ISO).

The following will outline some of the features that increase the security of online platforms by inhibiting potential hackers from deciphering and accessing sensitive information, and ultimately damaging the confidentiality, integrity, or availability (i.e., "CIA triad") of different arbitration phases.

Multi-factor authentication

Two-step verification is a salient feature of many ODRs that limits the potential for data exposure. This feature provides an additional layer of security so that only authorized individuals are accessing sensitive information. Principle 7 (b) of the 2020 Protocol recognizes "access controls" as one of the important considerations in an arbitration. This principle states that in considering the specific information security measures to be applied in arbitration, consideration should be given to issues such as "asset management" "access controls" "encryption", and "information security incident management". This is of substantive importance, as most ODRs run on browsers that leave some form of digital footprint, thereby rendering them prone to hackers who can access vulnerable browser details. Thus,

it is important to control access on a “need to know” basis, which has an advantage over self-made passwords. For instance, eArbitration, an ODR platform, has established two-factor authentication in which each participant obtains a unique ID associated with their user profile called a “token”, which has to be validated by a second factor/device upon login – e.g., on a phone or via e-mail. This allows them to access only the information they are privy to and is important given that some platforms like Zoom, which are currently being employed by some virtual hearings, had episodes of susceptibilities, with unauthorized users accessing meetings for the purpose of disrupting their security. Due to by a New York Attorney General’s recent investigation, Zoom has committed, among other things, to implement various security measures including penetration-testing, which aims to identify and solve vulnerabilities in cyber security. In doing so Zoom also included features like default passwords, pre-entry waiting rooms and enhanced encryption to keep malicious users at bay.

Encryption of data

Encryption is a cybersecurity measure that protects information by using extremely complex and unique codes that mix up data and prevents unauthorized users from deciphering sensitive information. “Encryption” is also a standard enshrined in principle 7 (c) of the 2020 Protocol. It helps to prevent the discovery of confidential information, including trade secrets, financial information, and personal identifiable information. In the absence of this feature, such sensitive data may be prone to attack, and, as a result, will amount to the breach of confidentiality, which is an important pillar of arbitration. Encryption requires routine audits during which the platform is tested to face potential security vulnerabilities. For instance, both eArbitration and Immediation ODRs conduct routine verifications to determine and ensure the encryption of sensitive data.

Collecting and storing of information

“Asset management” is another important standard in the process of collecting and storing all sorts of information during the case management of arbitral proceedings, which is encapsulated in principle 7 (a) of the 2020 Protocol. Under this standard, information disseminated should be identified, classified, and controlled. In this regard, retention and destruction is an important component of this principle, in which data is initially stored securely, and after the conclusion of arbitral proceedings, is destroyed in compliance of applicable privacy rules.

Another integral part of asset management is providing a platform that allows the secure exchange of information. For instance, Immediation and eArbitration embedded an integrated "live" chat box similar to the platform Slack uses, in which all parties who are privy to the arbitration proceeding, including the arbitrators, counsels and secretary can use to communicate with respect to the case. Such a feature captures the standards of "communications security" stipulated in principle 7(d) of the 2020 Protocol.

Managing breach incidents

Despite robust security measures, sometimes the breach of information might be inevitable, and has been especially notable during the COVID-19 era, where many online businesses have observed spike in fishing attacks, malspams, and, ransomware attacks. In these occasions, these platforms ought to act promptly to mitigate a data breach and recover lost or stolen information. This standard has also been captured in principle 7 (h) of the 2020 Protocol as "Information Security Incident Management". This can be achieved through routine platform audits to perform a studied plan of actions in order to respond to an incident. Both Immediation and eArbitration have devised periodic audits in order to detect new security vulnerabilities or potential threats.

B. Heralding institutional involvement in cybersecurity

Many arbitral institutions have pivoted towards digitizing their services in light of the demands emerging from the COVID-19 era to resolve their disputes expeditiously and efficiently, both of which are duties many arbitral institutions strive to uphold. However, these institutions have not adequately addressed essential security measures needed for virtual hearing. For instance, the ICC, SIAC, and LCIA have introduced comprehensive rules regarding how virtual hearings ought to be conducted. According to these rules, parties are entitled to incorporate measures they deem necessary to safeguard the proceedings. For instance, under 22.3 of the ICC Rules, a party can invoke confidentiality in order to protect sensitive and confidential information. Similarly, the HKIAC under Article 3.1 (e) recognizes and the AAA-ICDR Article 37.2 primarily grant parties the discretion to select the necessary measures or a secured online repository to protect sensitive and confidential information. However, the above institutions'

rules are silent regarding issues including case management, exchange of communications, and virtual hearings. No hard guidance has been provided regarding what cybersecurity measures entail.

The lack of hard guidance may bear significant consequences. A breach of the security of sensitive data may amount to the violation of confidentiality. This may undermine the integrity and viability of international arbitration, and the whole proceedings by inflicting reputational damage to arbitral institutions, arbitrators, and counsels, as well as to the system of international arbitration overall. It is now becoming increasingly important for arbitral institutions to embrace ODRs or other platforms that incorporate necessary security measures.

Concluding remarks:

In this new era of COVID-19, as more arbitration proceedings move into digitized platforms, the need to identify instances of security breaches is becoming clear. In particular, for the users of international arbitration whose primary concerns are protecting their trade secrets and confidential information while having their disputes resolved in an expeditious and cost-effective manner. Thus, most stakeholders in arbitration, in particular, arbitral institutions have the onus to acknowledge the threat and explore the nature of cybersecurity because a cyber-threat may undermine the integrity of arbitration. In doing so, stakeholders shall take proactive steps in adopting tailored automatized safeguard tools that encompasses essential security measures. Effectively, instituting an ODR platform that would embody the necessary features, such as multi-tiered authentication, encryption, secured collection and storage, as well as managing breach incidents in order to minimize the risk of a security breach during online proceedings.

Without a doubt, COVID-19 crisis will serve as a catalyst for improvement, as it will underline the aptitude of ODRs in navigating the obstacles presented by this new circumstances and will perhaps garner more significance to address cybersecurity concerns.