Cybersecurity In International Arbitration – A Necessity And An Opportunity For Arbitral Institutions

Kluwer Arbitration Blog
October 6, 2017

Claire Morel de Westgaver (Bryan Cave Leighton Paisner LLP)

Please refer to this post as: Claire Morel de Westgaver, 'Cybersecurity In International Arbitration – A Necessity And An Opportunity For Arbitral Institutions', Kluwer Arbitration Blog, October 6 2017, http://arbitrationblog.kluwerarbitration.com/2017/10/06/cyber-security/

Cybersecurity bears particular significance to the realm of international arbitration. In addition to the ambient cybersecurity risks faced by each participant in international arbitral proceedings, the need to share information between the parties, the tribunal and the institution for the resolution of a dispute increases the likelihood that data will be lost or breached. Arbitral institutions may be uniquely positioned to address cybersecurity risks in a consistent and sustainable way. Doing so provides an opportunity for arbitral institutions to advocate for institutional arbitration (as opposed to ad hoc arbitration) and to differentiate themselves from the competition by attracting cybersecurity conscious users through innovation.

Why is international arbitration a target for hackers?

First, as a neutral forum for the resolution of commercial and investment disputes, international arbitration often involves parties that are themselves prominent targets of cybersecurity attacks, e.g. multi-national groups, governments or state entities, public figures and NGOs. Second, although the level and scope of confidentiality is variable, arbitration offers the possibility to resolve disputes

behind closed doors. Disputes submitted to international arbitration generally require evidence of facts which are not in the public domain and which may have the potential to influence politics and financial markets. Third, international arbitration involves actors from different jurisdictions that operate from a variety of settings. Parties are typically represented by large and often cross-border teams. In-house lawyers, counsel and arbitrators tend to travel extensively and work from multiple places including hotels, airport lounges or private home offices. These factors enhance the risk of being hacked by electronic means as well as social engineering and theft of physical data.

Analysis of the structure of international arbitration provides insight as to how cybersecurity risks may arise and which of its stakeholders may be best equipped to adequately address these risks.

Law firms

Law firms (including barristers' chambers) are depositories of their clients' data and documents. Communications that a law firm has with its clients are generally covered by privilege and/or a duty of confidentiality. With arbitrators often being associated with a law firm, such firms may also be privy to communications between members of a tribunal. The content of deliberations, including draft awards, is particularly prone to cyberattacks because they may contain confidential facts and also information which may give rise to insider trading.

Law firms are a prominent target for hackers. A 200 law firm study released by LogicForce (a cybersecurity consulting firm) found that all of them had been subjected to hacking attempts. In the context of arbitral proceedings in particular, in *Libananco v Republic of Turkey (ICSID ARB/06/8)*, Turkey admitted to have intercepted Libananco's correspondence with its counsel and third parties, albeit as part of a separate criminal investigation. In spite of their exposure and their resources, law firms are nonetheless not (yet) adequately prepared to cope with these risks. The LogicForce survey revealed that 40% of firms were actually unaware of the hacking attempts until the study was conducted and corresponding investigations made. Further, 95% of firms were not fully compliant with their own data governance and cybersecurity policies and only 23% had an adequate cyber-attack insurance policy in place.

While law firms have control over their communications with clients as well as

witnesses and experts, their channels of discourse are relatively limited compared to arbitral institutions. Law firms do not have any control over participants other than by agreeing protocols with the opposition (not always possible or appropriate) or seeking directions from the tribunal.

Arbitrators

Unlike judges, arbitrators are private practitioners. Arbitrators may operate in contexts with varying degrees of cybersecurity (e.g., law firms and universities); or they may be independent from any firm or organisation. In the former case, arbitrators are typically subject to data security processes and policies over which they may not have any control and which may not be adapted to their role of arbitrator. In the latter case, arbitrators have a higher level of freedom and flexibility but they may not have any sophisticated IT support.

Under most rules and legal systems, arbitrators and tribunals have the power to make necessary orders for the protection of confidential information and documents. Arguably arbitrators' wide procedural powers include the ability to make orders for the storage, use and transfer of data generated and produced in a given arbitration. In this regard, recommendations and protocols as to how cybersecurity risks may be tackled by parties and tribunals are a positive development and should be welcomed by the international arbitration community. However, if adopted by a tribunal, such measures would be limited in scope and enforceability. Further, whilst some arbitrators may have a strong grasp of cybersecurity issues, one needs to recognise that as a group arbitrators are not IT experts. As such, relying on them to improve cybersecurity may not be sustainable or in any event sufficient.

Arbitral institutions

As the depository of sensitive data, institutions are highly exposed to cybersecurity risks, including in terms of reputation management and compliance with the rapidly evolving regulations. In July 2015, the website of the Permanent Court of Arbitration in The Hague was hacked during a hearing of a sensitive maritime border dispute between China and the Philippines. The website was implanted with a malicious code that posed a data breach risk to anyone who visited a specific page devoted to the dispute. Despite this modern threat and the risks involved, many arbitration institutions continue to rely upon relatively insecure storage and

communication systems. Notably institutional rules tend to be silent on cybersecurity and allow communications and transfer of data between the parties and the tribunal by any electronic means. In addition, many arbitral institutions use unencrypted email and commercially available cloud data repositories.

Yet, the permanent nature of arbitral institutions allows them to regulate by way of revisiting their arbitration rules and policies. Institutions could introduce mandatory filing and communication systems under which data would be transmitted exclusively through an internet-based secured platform, moving away from sharing external drives, hard copies and emails with sensitive attachments. Such platform could include separate areas only accessible to tribunal members for the storage and sharing of draft awards for example, and could be equipped with multi-factor authentication, as well as functions preventing users from editing, printing, downloading or emailing certain classes of documents. Such tools are already available on the market and often used by parties and tribunals, albeit on an ad hoc basis.

Institutions may take the view that gaining more control over the flow of data generated and produced as part of arbitral proceedings may result in further risks and liabilities. Yet, given their role in the arbitration process and the liabilities to which they are already exposed, devoting resources to cybersecurity may be seen by institutions as a long term investment, not only in terms of hedging existing risks but also business development. Arbitration users will become increasingly cybersecurity conscious and advanced security may help arbitration institutions to stand out from the increasingly fierce competition.

The author is grateful to David Zetoony (Bryan Cave partner) for his advice and to Yeon-Ho Son (Bryan Cave trainee-solicitor) for his assistance.