NEWS

Practical steps to address cybersecurity

19 February 2020

*Akin Gump partner **Justin Williams** and counsel **Jenny Arlington** consider recent initiatives to address cybersecurity in international arbitration and what arbitrators, counsel and users can do to manage the risks.*

International arbitration is especially vulnerable to cybersecurity and data privacy risks. In particular, it typically involves the processing and cross-border transfer of large quantities of sensitive data. Arbitrators, counsel and users alike are exposed to the legal, commercial and reputational consequences of breaches of information security, but this also potentially threatens the reliability of the arbitral process itself. It is vital that effective steps are taken to manage these risks. An important contribution to this discussion has been made by the recent release of the 2020 Protocol on Cybersecurity in International Arbitration. This article outlines some steps that have been, and might be, taken to manage information security risks, and considers the substance of the 2020 Protocol.

The current cyber threat

There is no doubt that most large companies see information security as an increasing and serious business risk. World business leaders were reported in November 2019 as ranking cyberattacks as the second-most significant threat to their businesses, after the threat of a fiscal crisis. In summer 2019, around 60% of medium and large UK businesses reported having experienced cybersecurity breaches or attacks in the previous 12 months, with almost one-third

First published on the *Global Arbitration Review* website, 20 February 2020.

saying they experienced these at least once a week in 2019, as opposed to 22% saying so in 2017. In autumn 2019, 76% of small and medium-sized businesses in the US reported a cyberattack within the previous 12 months.

The impacts of cyber threats can be wide ranging, including loss of business and profit, reduced share prices, civil liability, fines (particularly onerous in Europe if there is an accompanying breach of data protection laws), data loss, diversion of staff time, reputational damage and legal costs. The average cost of a single data breach, for example,. has been reported as US$3.9 million.

The legal sector is not immune. There have been a number of high-profile and damaging cyberattacks on law firms in recent years. *American Lawyer* reports that since 2014 more than 100 US law firms of various sizes have disclosed data breaches to regulators across 14 US states. The latest figures in the UK indicate that just under 8% of all reported personal data breaches in 2019 occurred in the legal sector. And law firms are regularly targeted by fraudsters: for example, the UK's National Cyber Security Centre has reported that hackers stole more than £11 million (approximately US$14.2 million) of client money from UK law firms during 2017 alone.

And cyber activity has affected international arbitration specifically. For example, in 2015 the Permanent Court of Arbitration's website was hacked during a maritime border dispute between China and the Philippines. In *Libananco Holdings v Turkey* (ICSID Case No ARB/06/9), an ICSID tribunal considered whether the fair conduct of the arbitration had been prejudiced by Turkey's interception of privileged materials in the course of a separate money-laundering investigation.

Responses to the cyber threat

Most large businesses appear to be taking significant steps to improve their cybersecurity. Global business spending on cybersecurity is reportedly estimated to have reached US$124 billion in 2019. In the UK, for example, over the last two years a new cybersecurity business was registered every week.

Investment in cybersecurity is a response not only to risk but also to legal requirements. In the European Union, wide-ranging legal obligations arise under the General Data Protection Regulation (GDPR). Other laws that have had an impact on cybersecurity globally include national data protection laws (such as in Brazil and Canada), state legislation (such as the California Consumer Privacy Act) and industry specific regulations (such as the Health Insurance Portability and Accountability Act of 1996 in the US).

In the arbitration community, the International Council for Commercial Arbitration (ICCA) and International Bar Association (IBA) established a joint task force on data protection in international arbitration proceedings in February 2019. The IBA Cybersecurity Guidelines published in October 2018 also provide some guidance. Yet arguably the most important contribution so far has been the release of the 2020 Cybersecurity Protocol, published in late 2019 by ICCA, the New York City Bar Association and the International Institute for Conflict Prevention and Resolution (CPR).

The 2020 Cybersecurity Protocol

The protocol consists of 14 principles and provides a "recommended framework" intended to assist users of international arbitration in deciding what information security measures to

implement in an arbitration. It is not compulsory, and does not supersede applicable laws, arbitration rules and other professional or ethical obligations. In addition to the principles, the protocol also includes commentary which provides detailed background and further explanation for each principle.

The protocol does not provide rigid rules, but rather identifies factors that might be taken into account in identifying what "reasonable" information security measures might be in the circumstances of any given arbitration.

The cybersecurity risk profile of the arbitration is one of these factors and schedule B to the protocol provides a list of issues that can be considered to determine that risk. These issues include:

- the nature of the information which might be relevant in an arbitration (such as confidential commercial information, personal data or intellectual property);
- special types of data (such as information belonging to a government, sensitive personal information or information subject to professional privilege such as doctor-patient or legal privilege);
- the identity of the parties and their cyber-vulnerability track record;
- the industry/subject matter of the dispute;
- the size and value of the dispute; and
- the consequences of a cyber breach, such as risks to the integrity and confidentiality of the arbitral process, risks of financial loss and to the privacy of any affected individuals.

Further factors which would help assess what information security measures should be put in place include the burden, costs and relative resources of the parties; proportionality; existing information security practices; various categories of measures such as communications security, measures relevant to the physical environment, operations security and incident management. It is also recommended that consideration be given to the risks present in the various stages of an arbitration. Examples of specific information security measures and processes that might be adopted are set out in schedule C to the protocol. Finally, a series of suggested procedural steps to address cybersecurity are discussed.

What steps should be taken?

Arbitrators, counsel and users of international arbitration should familiarise themselves with applicable information security laws and regulations and consider applying the Cybersecurity Protocol without delay. Some of the most damaging cyberattacks achieved significant damage not so much as a result of sophistication, but rather due to a delay in the implementation of existing information security measures. The "WannaCry" ransomware attack, for example, took place in May 2017 and within one day infected more than 230,000 computers in over 150 countries, mainly exploiting organisations that had not applied the protective software patches that had been released almost two months earlier.

First published on the *Global Arbitration Review* website, 20 February 2020.

Consideration should be given to including cybersecurity in the agenda of the initial procedural hearing in each arbitration.

There may also be merit in institutional rules being amended expressly to note that the parties and the tribunal are to consider what steps may be appropriate to safeguard information security. The 2019 CPR Rules for Administered Arbitration of International Disputes include such a provision, but so far none of the major institutional rules do so. The upcoming amendment to the LCIA's 2014 Arbitration Rules presents an opportunity for this important modernisation.

First published on the *Global Arbitration Review* website, 20 February 2020.