Skadden

International Arbitration Community Turns Its Focus to Cybersecurity

Contributing Partners

Julie Bédard / São Paulo

Lea Haber Kuck / New York

Timothy G. Nelson / New York

International arbitration has long offered participants the benefit of maintaining confidentiality in high-stakes cases. Like virtually all modern activity, however, it has become potentially vulnerable to cyberattacks. The threat extends not only to the information of the disputing parties and their counsel, but also to the internal deliberations and draft decisions of the arbitrators themselves, which can be highly sensitive. Combined with reports of breaches in other contexts, this underscores the importance of maintaining the security of the information exchanged in the course of an arbitration, and communications among arbitrators and with arbitral institutions. As a result, the international arbitration community has been increasingly focused on the security of the information exchanged during the arbitral process.

The need for cybersecurity measures in international arbitration is heightened by the contentious backdrop, the high-value and high-stakes nature of disputes, and the involvement of multiple actors who are digitally interdependent. One widely reported cyberattack occurred in July 2015 during the arbitration between the Philippines and China over disputed waters in the South China Sea. The attack, which some commentators claimed originated from China, targeted the Permanent Court of Arbitration in The Hague, which was administering the arbitration; the Philippine Department of Justice; and the law firm representing the Philippines.

In late 2017, representatives of the International Council for Commercial Arbitration, the International Institute for Conflict Prevention and Resolution, and the New York City Bar Association came together to create the Working Group on Cybersecurity in Arbitration, which was charged with evaluating these issues and making recommendations.[1] The working group released the Draft Cybersecurity Protocol for International Arbitration in April 2018. A final document is expected to be released later in 2019 and will take into account input the working group has received both at public workshops it has held throughout the world and in written form from a variety of bar associations and other interested organizations.

As explained by the working group when issuing the draft for consultation, the draft protocol "suggests a procedural framework for developing specific cybersecurity measures within the context of individual cases, recognizing that what constitutes reasonable cybersecurity will vary from case-to-case based on a multitude of factors." It recommends that cybersecurity be addressed in the international arbitration process as early as practicable, ordinarily no later than the first case management conference and before the parties begin their exchange of information. In some cases, however, such as where the arbitration demand itself contains sensitive information, it may be necessary for parties and arbitral institutions to address this issue at the very outset of the proceeding.

[1] Lea Haber Kuck is a member of the working group, and associate Eva Y. Chan is its secretary. The draft protocol is available here.

This article is from Skadden's *2019 Insights*.

Four Times Square
New York, NY 10036
212.735.3000

Rather than advocate a one-size-fits-all approach to cybersecurity, the draft protocol provides a framework for parties and arbitrators to determine appropriate measures in the context of each case. As discussed in the draft protocol, factors that may influence the determination of what measures are reasonable include:

- the nature of the information expected to be exchanged in the arbitration, including any confidential commercial information and personal data;
- the potential cybersecurity threat based on the identity of the parties, and the nature and size of their dispute;
- the resources of the parties, including the existing digital infrastructure of the arbitral participants and any potential technical impediments to implementing cybersecurity measures; and
- the severity of the potential consequences of a cyberattack, which may vary depending on the value of the information to third parties; the nature, type and amount of personal data being processed and whether it is legally regulated; potential embarrassment or damage caused by public disclosure of the information; and whether and how the information could be misused by a third party (*e.g.*, politically, for extortion purposes, for insider trading purposes or to obtain a competitive advantage).

The draft protocol also recognizes that cybersecurity measures will necessarily need to evolve with changing technology and regulation.

Additionally, because cybersecurity is a shared responsibility of all participants in the arbitration process who are digitally interdependent, the protocol recognizes that the "security of information ultimately depends on the responsible conduct and vigilance of individuals." As it notes, "any individual actor can be the cause of a cybersecurity breach; [m]any security breaches result from individual conduct rather than a breach of systems or infrastructure." Accordingly, the draft includes a schedule of "General Cybersecurity Practices" highlighting steps participants, including parties, counsel, arbitrators and experts, should consider taking to make sure that information in their possession remains secure. These steps may include creating access controls through strong passwords with multifactor authentication; guarding digital perimeters using measures such as firewalls, anti-virus and anti-spyware software, operating system updates and other software patches; making routine back-ups; and being mindful of public internet use.

Arbitral institutions likely will further address this issue in their own infrastructure, internal procedures, arbitral rules and the training of arbitrators they appoint. Arbitrators will need to make sure that they are conversant in basic cybersecurity practices in order to meet the expectations of parties that have long been focused on protecting their confidential business information.

Best practices will continue to evolve as developments in technology and the regulatory landscape become increasingly complicated.

Click here for a full list of international litigation and arbitration-related articles authored by Skadden attorneys in the last year.