Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Arbitration Cybersecurity Protocol Outlines Best Practices

By **Caroline Simson**

Law360 (November 21, 2019, 7:12 PM EST) -- A new cybersecurity protocol for international arbitration unveiled Thursday aims at providing guidance to arbitrators, institutions and arbitration users on topics including baseline security measures, while making clear that it's the responsibility of all involved in an arbitration to address this increasingly important issue.

The Protocol on Cybersecurity in International Arbitration, presented by a working group at an event conducted during New York Arbitration Week, is not intended to provide a uniform approach to cybersecurity for parties to simply drop into their arbitration agreement. Rather, it's meant to provide a combination of high-level guidance in a series of 14 principles that cover topics such as determining reasonable cybersecurity methods, and more detailed guidance to address things like assessing the cybersecurity risk in a particular case.

"Throughout [the consultation period] there was a desire from some people for specific guidance, but we also recognize there's no one-size-fits all," said Skadden Arps Slate Meagher & Flom LLP partner Lea Haber Kuck, a member of the working group, during the presentation at the New York International Arbitration Center.

Considerations as to which cybersecurity measures will be appropriate for a particular arbitration will depend on the circumstances of that case, so there was no way that the working group could simply tell lawyers and institutions what to do — a request that the group spent many hours deciding how to address during the consultation process.

"We tried to build in flexibility [so that the] document can be used as guidance, rather than something that's prescriptive," said Micaela R.H. McMurrough, a partner at Covington & Burling LLP and a member of the working group.

The protocol is the culmination of two years of work by the group, which consists of representatives of the International Council for Commercial Arbitration, the New York City Bar Association and the International Institute for Conflict Prevention & Resolution.

Working group members noted Thursday that this version of the protocol ended up being quite different from the consultation draft released in April 2018, and that they expect the document to keep evolving as the technology continues to change and new cyberthreats emerge.

The document is intended to provide a framework to determine reasonable information security measures for individual arbitration matters, and also to increase awareness about information security in international arbitrations. It's meant to go beyond the "initial message" that cybersecurity is something that lawyers, parties and institutions need to be aware of, working group member Stephanie Cohen, an independent arbitrator based in New York, said Thursday.

The protocol is laid out to include a series of principles addressing its scope and applicability, and helping users to determine reasonable measures for their particular arbitration. It also discusses the appropriate process to establish cybersecurity measures, making clear that such considerations should be discussed as early as practicable in the arbitration.

The document also includes schedules to establish baseline security measures — such as identifying sensitive data and taking steps to protect it and avoiding unnecessary copies of documents — and to assess the "risk profile" of an arbitration, a calculation that takes into account the nature of the information being processed, the risks related to the arbitration's subject matter and the possible consequences of a breach.

It includes sample information security measures and sample arbitration agreement language as well.

--Editing by Orlando Lorenzo.