New York Law Journal

NEW YORK LAW JOURNAL SPECIAL REPORT

An ALM Publication

Alternative Dispute Resolution

WWW.NYLJ.COM

VOLUME 260—NO. 25

MONDAY, AUGUST 6, 2018

Fending Off Cyberattacks In International Arbitration

BY HAGIT M. ELUL AND PAVLOS PETROVAS

SHUTTERSTOCK

In an increasingly digital landscape, data security threats have become ubiquitous. Cyberattacks are becoming weapons of global economic warfare, with governments and corporations steadily reporting higher numbers of data breaches, and cybercriminals increasingly targeting law firms, large and small, in an attempt to access clients' secrets and other sensitive non-public information.

In the context of ever-escalating data breaches, international arbitration is not immune to cyberattacks. One widely reported cyberattack targeted the Permanent Court of Arbitration in The Hague (PCA) in July 2015, while the court was administering a hearing between the Philippines and China over disputed territorial waters in the South China Sea. During that arbitration, a malicious software originating in China targeted the PCA's website, the Philippines Department of Justice, the law firm representing the Philippines in the arbitration, and anyone visiting a specific page of the PCA devoted to the dispute, allowing the hackers to access classified information.

A similar cyberintrusion occurred in 2008 in the case of *Libananco Holdings Co. v. Rep. of Turkey (ICSID Case No ARB/06/9)*, where, in the course of a separate court-ordered money laundering investigation, the Turkish government intercepted privileged communications and materials that had been exchanged between Libananco and its counsel in connection with the arbitration.

Prime Target

It is therefore of no surprise that international arbitration may become a prime target for cybercriminals. This is for various reasons. *First*, as a neutral forum for the resolution of complex international disputes, international arbitration often involves parties that are themselves prominent targets of cyberattacks such as multinational corporations, governments,

HAGIT M. ELUL *is a partner at Hughes Hubbard & Reed and a member of the ICCA-CPR-NYCBA Working Group on Cybersecurity in International Arbitration.* PAVLOS PETROVAS *is an associate at Hughes Hubbard.*

state entities, and public figures. *Second*, in these types of disputes, digital discovery is the norm and inevitably involves the exchange of highly sensitive information such as trade secrets, business plans, and case strategy, which have the potential of influencing politics and moving financial markets.

Third, the risk of exposure to cyberattacks is relatively high because of the way international arbitration is conducted. The information collected is typically organized in easily searchable data sets, such as pleadings, witness statements, expert reports, transcripts of hearings, and arbitral deliberation materials, including draft and final awards. Each fixed or portable device (computers, laptops, smartphones, tablets), cloud-based storage (file-sharing platforms, virtual data rooms), and courtroom technology (real-time translations, live e-transcripts, telepresence technologies) is a digital portal allowing for unauthorized access to arbitration-related materials.

The fact that the information is hosted and exchanged by a variety of digitally interdependent players such as in-house and outside counsel, government officers and agencies, arbitral institutions and tribunals, experts and witnesses, and other custodians of large electronic information repositories only increases the likelihood that a data breach of one participant will impact all participants. The data custodians involved in the process also tend to sit in different jurisdictions and communicate through various means, including unencrypted email. Therefore, large amounts of information travel around the world in an unsecured way. Even larger amounts of information may be compromised if U.S.-style discovery takes place.

Consequences

A failure to implement cybersecurity measures may have dramatic consequences for all stakeholders in an arbitration. The disclosure of non-public information may result in economic and reputational damage to corporations, counsel, arbitrators, and institutions whose actions were negligent or whose information was compromised. Data breaches may also lead to regulatory sanctions as well as civil and criminal liability. The use of illegally obtained evidence by a party in the arbitration—a largely unsettled issue in international arbitration—may violate the fundamental principles of integrity, fairness, and due process that are inherent to any adjudicatory proceeding. Perhaps most importantly, because confidentiality is at the heart of international arbitration, any cybersecurity shortcomings will inevitably erode the credibility and legitimacy of international arbitration as a form of dispute resolution.

> Cyberattacks are becoming **weapons of global economic warfare** with cybercriminals increasingly targeting law firms in an attempt to access **clients' secrets** and other sensitive non-public information. **International arbitration is not immune**.

The Working Group

Over heightened concerns that international arbitration might be vulnerable to cyberattacks, the International Council for Commercial Arbitration (ICCA), the International Institute for Conflict Prevention & Resolution (CPR), and the New York City Bar Association launched a Working Group aiming to raise awareness and establish cybersecurity protocols for use in international arbitration proceedings. On April 16, 2018, the Working Group released for consultation a Draft Cybersecurity Protocol for International Arbitration (available at: http://www.arbitration-icca.org/media/10/43322709923070/draft_cybersecurity_protocol_final_10_april.pdf) providing a framework for practitioners to determine and implement reasonable cybersecurity measures on a case-by-case basis.

The protocol opens with a warning that the credibility of international arbitration depends on ensuring a reasonable degree of protection of digital information exchanged during the proceedings, because, unlike other dispute resolution mechanisms, arbitration offers the unique advantage of maintaining the confidentiality not only of the information exchanged during the process but of the existence of the arbitration itself. Because of the high-value, high-stakes nature of the disputes, parties opting for this form of dispute resolution have a legitimate expectation that their dispute will remain out of the public eye and that the process will have reasonable cybersecurity safeguards in place to protect non-public information from unauthorized access. Therefore, the protocol explains, "[r]easonable cybersecurity measures are essential to ensure that international arbitration maintains this advantage" (Draft Protocol at 3-4).

The protocol goes on to identify substantive and procedural measures designed to prevent and mitigate the

occurrence of a cyberattack. Specifically, the protocol invites practitioners to consider adopting measures:

- Limiting the disclosure of confidential information by applying the narrow discovery standard that is typical in international arbitration. For example, the International Bar Association Rules on the Taking of Evidence in International Commercial Arbitration (IBA Rules), which are frequently used in international disputes and govern the exchange of documents, limit discovery to "narrow and specific" categories of documents "that are reasonably believed to exist." (IBA Rules, Art. 3.3(a)(ii)).
- Protecting the transmission of arbitration-related material by (i) identifying secure transmission methods for all participants (*g.*, email, third-party platform, USB drive, or other portable devices), (ii) encrypting, redacting, pseudonymizing, or anonymizing sensitive information; and (iii) restricting access to confidential material through need-to-know or attorneys-eyes-only designations
- Mitigating data breaches by (i) identifying the source, nature, and scope of the breach; (ii) retrieving lost information and correcting security systems weaknesses; (iii) timely notifying all affected parties in accordance with applicable laws and regulations; and (iv) enlisting expert vendors and law enforcement, where appropriate.
- Adopting detailed post-arbitration document retention and destruction policies.

The protocol also invites practitioners to improve their individual day-to-day cybersecurity practices by highlighting general measures that actors may use to protect information. Examples of good general cybersecurity practices include: (i) using complex passwords with multifactor authentication; (ii) using firewalls, antivirus and antispyware software, and up-to-date software security patches; (iii) applying industry-standard encryption technology for storage and end-to-end transmission; (iv) making routine data back-ups; (v) opting for personal cellular hotspots or virtual private networks (VPN) over public Wi-Fi; and (vi) staying abreast of evolving cybersecurity risks and best practices.

The Working Group purposely avoided recommending specific cybersecurity measures. Recognizing that no one size fits all, the protocol does not require parties and arbitrators to follow a "specific and immutable" set of rules. Instead, it recommends an individualized approach to determine the cybersecurity measures that best fit the circumstances of each case. To help with such determination, the protocol suggests conducting a risk analysis based on case-specific factors, which include the nature of the information at issue, the potential security threats and consequences of a data breach, and practical considerations such as cost, burden, and the parties' existing cybersecurity capabilities.

Examples of sensitive information requiring special care includes intellectual property, trade secrets, medical information, payment information, classified or politically sensitive information, and information that is subject to confidentiality agreements or regulatory restrictions. There may be a need for stricter cybersecurity measures where international travel is frequently required or a key witness has been the target of cyberattacks in the past, handles large amounts of high-value confidential information, or is a high-ranking public official or executive . Such risk analysis offers the required flexibility for arbitrators to balance competing considerations and tailor cybersecurity measures to accommodate the parties' resources, sophistication, and legal obligations.

Procedurally, the protocol recommends that the tribunal discuss cybersecurity procedures and draw up a procedural order at the outset of the proceedings, as early as possible, and no later than the initial case management conference setting the procedural ground rules.

In concluding, the protocol notes that, because any individual actor can be the "weak link," cybersecurity is the shared responsibility of all participants in the arbitration.

The Working Group has set a consultative period until Dec. 31, 2018, during which time it will hold public workshops worldwide to solicit comments. The Working Group invites interested parties to submit comments on the protocol at cybersecurity@arbitration-icca.organd engage in constructive dialogue with the broader arbitration community in order to develop a reasonable data security framework for international arbitration.

Following the consultative period, the Working Group will revise the protocol in light of comments received and release a final version in 2019. In coming years, the Working Group anticipates revising the protocol, as cybersecurity and cyberthreats evolve, regulatory frameworks adjust, and a consensus on best practices emerges.