REPRINT

CD corporate disputes

MANAGING CYBER AND DATA RISK IN ARBITRATION

REPRINTED FROM:
CORPORATE DISPUTES MAGAZINE
APR-JUN 2019 ISSUE

www.corporatedisputesmagazine.com

Visit the website to request
a free copy of the full e-magazine

SHOOK
HARDY & BACON

Published by Financier Worldwide Ltd
corporatedisputes@financierworldwide.com

www.corporatedisputesmagazine.com

MINI-ROUNDTABLE

MANAGING CYBER AND DATA RISK IN ARBITRATION

PANEL EXPERTS

Giovanni Angles
Of Counsel
Shook, Hardy & Bacon LLP
T: +1 (305) 755 8997
E: gangles@shb.com

Giovanni Angles is of counsel in the Miami office of Shook, Hardy & Bacon LLP. His practice focuses on international arbitration and complex business litigation. Mr Angles represents individuals, corporations and sovereign governments in international commercial and investment treaty arbitrations under major arbitration rules.

Lea Haber Kuck
Partner
Skadden, Arps, Slate, Meagher & Flom LLP
T: +1 (212) 735 2978
E: lea.kuck@skadden.com

Lea Haber Kuck is a partner at Skadden, Arps, Slate, Meagher & Flom LLP. Her practice is focused on the resolution of complex commercial disputes arising out of international business transactions. She is a member of the Working Group on Cybersecurity in International Arbitration, formed by the International Council for Commercial Arbitration, the New York City Bar Association and the International Institute for Conflict Prevention and Resolution.

CD: Could you provide an overview of the types of cyber and data risks that you are seeing in connection with arbitration?

Kuck: International arbitration today often involves contentious, high-value, high-stakes disputes with multiple actors who are digitally interdependent. The participants in an arbitration who come into possession of sensitive information include not only the parties, their counsel and the arbitrators, but may also include arbitral institutions, witnesses, experts, court reporters and other vendors. As a result, various points of vulnerability exist. The risks extend 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.

Angles: In some respects, the cyber and data risks we are seeing are not too different from those in the world of dispute resolution, and the legal industry more generally. The exposure and exploitation of confidential or attorney-client privileged communications, including financial data and risk management assessments, is an ever-present concern across many practice areas. Yet, arbitration bears some risks and challenges unique to the field. Private commercial arbitration attracts the same corporate and institutional entities that are already being targeted by cyber criminals. Further, the advantage of confidentiality in arbitral proceedings is a double-edged sword in the context of cyber security. This reliance on confidential information in arbitral proceedings makes the data much more valuable to would-be thieves.

CD: What factors have driven the rise in these threats over recent years? How would you describe the current level of exposure facing parties engaged in arbitration?

Angles: There are two main factors which have driven the rise in cyber and data threats in recent years. The first factor is the further digitalisation of arbitral practice, together with other technological advances and efficiencies. There are working lawyers and arbitrators today who started their careers in an analogue world dominated by dictation machines, typewriters and the hand delivery of paper submissions. Data thieves from that era had their work cut out for them. The threat of cyber attacks arising from the modern reliance on technological efficiencies is exacerbated by the second factor: there is no express prohibition in public international law barring the use of illegally obtained evidence in arbitration proceedings. Nearly all of the major arbitral institutional rules give arbitrators the plenary power to determine the admissibility of evidence, so parties are encouraged to make use of illegally

obtained data, especially if it was procured or disseminated by a third party.

Kuck: Disruptive cyber attacks have increased in recent years. Law firms have been a prime target of cyber attacks, but we have also seen high-profile breaches involving arbitral institutions. The increased number of attacks, combined with the growing number of high profile multinational disputes and the increased amount of information being exchanged electronically in arbitration, have resulted in greater exposure. The level of exposure in any particular case will depend on a number of factors. The risk may increase, depending on the identity and nationality of the parties, and whether they are states or private parties, the nature and size of the dispute, and the nature of the information expected to be exchanged, including whether the information involves confidential commercial material or personal data and whether the information may be of value to, or could be used by, third parties politically, for extortion purposes, for insider trading purposes or to obtain a competitive advantage.

CD: What potential financial and reputational damage might result from an arbitration-related breach?

Kuck: International arbitration has long offered participants the benefit of maintaining confidentiality in high-stakes cases, so the system itself is at risk of reputational damage if users' confidentiality expectations are not met. In addition to damage to the parties or entities whose commercial information or personal data is compromised, the damage to attorneys, arbitrators and arbitral institutions is likely to be both reputational and economic. It should be noted that the General Data Protection Regulation (GDPR), which will apply in many international cases, not only provides for substantial administrative fines, but also grants individuals the right to assert civil claims seeking compensation caused by a breach of the GDPR's requirements.

> **"Cyber security is a shared responsibility of all participants in the arbitration process, and security of information ultimately depends on the responsible conduct and vigilance of individuals."**
>
> *Lea Haber Kuck,*
> *Skadden, Arps, Slate, Meagher & Flom LLP*

Angles: The potential aggregate damages arising from arbitration-related breaches are arguably

higher than breaches in commercial litigation. Because of the confidential nature of domestic and international commercial arbitration disputes, parties expect closed proceedings, attended only by the arbitrators, the parties and their counsel. The subject matter often involves sensitive data, including trade secrets, intellectual property or positions that could damage a party's public image. The types of losses include the damages at issue in the original arbitration proceeding, increased legal and forensic investigation fees and regulatory fines arising from the breach. Parties in arbitration proceedings often rely on its culture of confidentiality to prosecute their cases very differently than if they were in state or federal court. It follows that data breaches involving arbitration proceedings could lead to reputational damages that otherwise would not have occurred in the context of public litigation filings.

CD: With some arbitrations transcending national borders and thus subject to differing laws and varying levels of security, how should parties go about safely transferring and storing information throughout the process?

Angles: International arbitration practitioners and arbitrators commonly work away from their home office across multiple jurisdictions and often in high-risk public locations such as airports and hotels. Would-be thieves can electronically eavesdrop on lawyers in unsecured data transmissions as easily they can snatch their laptop or tablet. Although these discussions sometimes devolve into the classic efficiency versus security debate, there are several basic and relatively cost-effective precautions that parties could take to protect their data, such as installing a fully updated antivirus software suite, using privacy screens to reduce viewing angles on electronic devices when viewing confidential documents in public, keeping hard drives and flash drives encrypted, insisting on end-to-end encryption platforms for sensitive communications and minimising the collection and use of sensitive data to only that which is necessary.

Kuck: Cyber security is a shared responsibility of all participants in the arbitration process, and security of information ultimately depends on the responsible conduct and vigilance of individuals. As the recently released draft Cybersecurity Protocol for International Arbitration notes, "many security breaches result from individual conduct rather than a breach of systems or infrastructure". There are a number steps that individual participants in the arbitration process should consider taking to make sure that information in their possession remains secure, and many of these steps are neither technologically difficult nor expensive. Precautions against cyber security attacks may include creating access controls through strong passwords with multi-factor 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.

CD: What steps are arbitral institutions and other bodies taking to promote greater cyber security for international arbitration? What kinds of practices, duties and protocols are being encouraged?

Kuck: In late 2017, representatives of the International Council for Commercial Arbitration (ICCA), the International Institute for Conflict Prevention and Resolution (CPR) and the New York City Bar Association came together to create the Working Group on Cybersecurity in Arbitration to evaluate the issue of cyber security in international arbitration. The working group released the draft Cybersecurity Protocol for International Arbitration in April 2018 which suggests "a procedural framework for developing specific cybersecurity measures within the context of individual cases, recognising that what constitutes reasonable cybersecurity will vary from case-to-case based on a multitude of factors". There has been a high level of interest in the project within the international arbitration community, and the working group has received input both at public workshops throughout the world, and in written form from a variety of bar associations and other interested organisations. A final document is expected to be released later this year.

Angles: The International Centre for Dispute Resolution (ICDR) has implemented its Secure Case Administration initiative, composed of robust policies and procedures governing the storage of information, data encryption, data recovery and compliance issues. Other institutions have published practice guides aimed at law firms and arbitration practitioners. The International Chamber of Commerce (ICC) has published a Cyber Security Guide for Business and the International Bar Association's Cybersecurity Guidelines provides law firms and solo arbitration practitioners with best practices on how to keep sensitive data secure. These threats are not hypothetical. In 2015, the website of the Permanent Court of Arbitration (PCA) was hacked and malicious code was installed on the computers of lawyers, arbitrators, parties and government officials who visited the PCA webpage of a particular maritime boundary dispute between China and the Philippines. To help combat these threats, law firms are undertaking third-party information security audits and obtaining certifications, like ISO 27001, that they can hold out to clients and opposing parties as evidence of meeting a certain standard in cyber security.

CD: If a party suspects or confirms that sensitive data has been compromised during an arbitration process, how should it respond?

Angles: Generally, the best practice for parties handling sensitive data is to create and maintain a cyber incident response plan, which sets forth the procedures the party can use to identify, respond to, and mitigate the effects of a suspected breach. The party should undertake an initial assessment to confirm the nature and scope of the incident. The assessment results will dictate the measures needed to minimise continuing damage and the efforts to record and collect information relating to the attack or series of attacks. Finally, the party should determine whether the incident gives rise to legal obligations to notify the individuals whose information may have been compromised and other parties to the arbitration, including the tribunal and arbitral institution. Notification is particularly important in arbitration if the nature of the attack and the compromised data could threaten the integrity of the proceedings, such that it creates grounds for vacatur or non-enforcement of a subsequent award.

Kuck: There will be a need to assess the nature of the breach, whether there has been any unauthorised access to information, and whether an urgent need exists to take corrective action to prevent further breaches. Arbitral participants should be aware that applicable laws may dictate the required procedures for addressing these issues. The GDPR, for example, includes strict mandatory 72-hour breach notification requirements. Parties, law firms and arbitral institutions should already have a plan in place to deal with security breaches. In addition, as part of the planning for each arbitration at the preliminary conference, measures may be adopted proactively, taking into account the circumstances of the particular case, to cover what constitutes a breach, who must be notified of the breach, the timing of the notification and the specific steps to be taken to mitigate any information breach.

> **"Generally, the best practice for parties handling sensitive data is to create and maintain a cyber incident response plan to identify, respond to, and mitigate the effects of a suspected breach."**
>
> *Giovanni Angles, Shook, Hardy & Bacon LLP*

CD: Looking ahead, how do you expect cyber and data risks arising from arbitration to evolve? In your opinion, what technological and procedural developments are needed to address this issue?

Kuck: Technology and cyber security threats will continue to evolve and the regulatory regime relating to data privacy will continue to expand. Accordingly, all participants in an arbitration will need to be vigilant about keeping up to date on best practices to protect against security breaches. Sophisticated parties already demand this of their attorneys and we expect there will be an increased focus on whether particular arbitrators and arbitral institutions are willing and able to meet this challenge. Arbitral institutions will need to focus on these issues, as they are beginning to do, with respect to both the cases that they administer and the capabilities of the arbitrators they appoint. In this regard, a high demand exists for training programmes developed specifically for arbitrators. Arbitral institutions and professional organisations can play a leading role in developing such training and providing ongoing guidance on current best practices.

Angles: The increased attention to cyber security in arbitration could lead to a decline in ad hoc arbitration proceedings, which rely on the individual cyber security practices of the parties and the arbitrators. In this same vein, arbitral institutions are well-positioned to provide value-added services relating to cyber security integrity, in order to capture a greater share of arbitral proceedings. For example, an arbitration centre offering an in-house encrypted secure storage platform for document submissions would allow parties and arbitrators to forgo less secure providers. The role of secretariats and case managers within these institutions could be expanded to facilitate and implement the institution's cyber security protocols. This framework would also benefit the arbitrators, who can focus their attention on the fair adjudication of the dispute, rather than subject matter that may fall outside their area of expertise. At the outset of arbitration, the parties, in conjunction with the arbitrator, should agree on a cyber security protocol that establishes the technical, administrative and physical safeguards that will be required as part of any proceeding. CD