Cybersecurity in International Arbitration

Jocelyn Lim Yean Tse
Advocate and Solicitor (High Court of Malaya)
Barrister-at-Law (non-practising) (Lincoln's Inn)
Arbitrator, Adjudicator and Mediator
jocelyn.limyeantse@skrine.com

Abstract

Cybersecurity is no longer a remote topic in international arbitration, as information technology ("IT") continues to be widely used in international arbitration proceedings. Incidents of cyberattacks are no longer foreign to the arbitration community. Although some of these cyberattack incidents are rare, they have occurred, and the consequences are damaging.

This article examines the use of illegally obtained evidence, including evidence obtained through hacking as a result of cyberattacks in arbitration proceedings, the importance of cybersecurity measures and the steps taken by the arbitration community to tackle cybersecurity risks in arbitration proceedings. However, there are practical challenges in implementing the recommended cybersecurity measures.

Keywords: Cybersecurity, international arbitration, cyberattack.

1. Introduction

Cybersecurity is no longer a technical topic but one that dominates conversation. It affects our daily and work lives. As we continue to live in this digital society, the legal industry, known for its traditions and resistance to change, inevitably have had to adapt to the use of technology. Technology now plays a vital role in legal work. Paperless courtrooms, virtual hearings, digital libraries, cloud computing systems, cloud sharing platforms, and cloud data storage are some of the basic changes seen in the legal industry. The legal community is thus not spared from cyber threats.

In fact, law firms and arbitration institutions, who hold a wealth of private and confidential information, are often targets of cyberattacks. These attacks may lead to data breaches. Data breaches of documents related to legal proceedings and the resultant leak of those documents can lead to profoundly damaging effects to all parties involved, including counsel, arbitrators, and even arbitral institutions. To adapt to the digital world, the legal community has introduced guidelines and protocols as an effort to introduce cybersecurity measures for arbitration proceedings. Arbitral institutions are seen to revise their institutional rules with cybersecurity threats in mind.

However, implementing the recommended cybersecurity measures poses significant challenges.

2. Incidents of Attacks

The legal community had seen more than its fair share of cyber threats. Some of these attacks, although rare, have happened. The attacks not only resulted in loss of sensitive data and financial harm, but also resulted in reputational damage, and in some extreme cases, have led to criminal investigations and legal actions.

2.1. Panama Papers

The Panama Papers was an unprecedented leak of 11.5 million files or an equivalent of 2.76 terabytes of confidential information from the database of the offshore law firm, Mossack Fonseca.[1] The leak was claimed[2] to be due to a hack of the law firm's server. The information obtained from an anonymous source by the German newspaper Süddeutsche Zeitung was shared with the International Consortium of Investigative Journalists, who then shared them with a large network of international partners, including the Guardian and the BBC[3].

The Panama Papers exposed a myriad of information relating to offshore accounts of some of the world's most powerful people with alleged indications of money laundering and tax evasion.

One leaked memorandum from a partner of Mossack Fonseca stated: "Ninety-five per cent of our work coincidentally consists in selling vehicles to avoid taxes."[4]

In the wake of the leak, investigations were launched by dozens of tax authorities around the world. Just early this year, it was reported that the trial of 27 people charged in connection with the Panama Papers money laundering scandal started in April 2024 in a Panamanian criminal court.[5]

The firm itself, notwithstanding being one of the largest offshore firms in the world at that time, was not able to survive the leak and closed in 2018.

[1] Luke Harding, 'What are the Panama Papers? A guide to history's biggest data leak' *The Guardian* (5 April 2016) <https://www.theguardian.com/news/2016/apr/03/what-you-need-to-know-about-the-panama-papers> accessed 19 May 2024.
[2] '"Panama Papers" law firm says "hacked by servers abroad"' *Astro Awani* (6 April 2016) <https://www.astroawani.com/berita-dunia/panama-papers-law-firm-says-hacked-servers-abroad-101341> accessed 19 May 2024.
[3] Luke (n 1).
[4] Juliette Garside, Holly Watt and David Pegg, 'The Panama Papers: how the world's rich and famous hide their money offshore' *The Guardian* (3 April 2016) <https://www.theguardian.com/news/2016/apr/03/the-panama-papers-how-the-worlds-rich-and-famous-hide-their-money-offshore> accessed 19 May 2024.
[5] Mariko Oi, 'Panama Papers money-laundering trial begins' *The BBC* (9 April 2024) <https://www.bbc.com/news/articles/cnek443n8zvo> accessed 19 May 2024.

2.2. Law firm in Singapore

Not far from our homeland, Singapore, news reports indicated that Singaporean firm Shook Lin & Bok was hit by a ransomware attack in April 2024.[6] The firm reportedly paid a ransom of USD 1.4 million in Bitcoin to the Akira ransomware group, the alleged cyber intruder. It was also reported that the Singapore firm had in its statement stated that "There is thus far no evidence that the firm's core document management systems which contain client data were affected."[7] Questions have been raised as to whether that is true, as the ransom was subsequently known by the public. In any event, there certainly were operational disruptions and financial loss.

2.3. Permanent Court of Arbitration Website Attack During the China–Philippines Maritime Boundary Dispute[8]

Arbitral institutions are not spared from cyberattacks as well. The website of the Permanent Court of Arbitration ("PCA") went offline during a hearing of the territorial dispute in the South China Sea between the Philippines and China. According to reports[9], hackers embedded the PCA's web page on the case with a code that infected visitors to the page, leaving anyone interested in the landmark legal case, and possibly their organisation, at risk of data theft. Eventually, the PCA website, which contained information about other cases, had to be taken offline for security reasons.

While the timing of the attack raised questions of whether it was orchestrated by certain parties, it nonetheless shows that arbitral institutions are also targets of cyberattacks.

3. Use of Leaked Documents

3.1 Arbitral Rules

Arbitration rules give wide discretion to arbitrators to decide on the admissibility of evidence, including evidence obtained illegally through hacking.

Article 19(2) of the UNCITRAL Model Law on International Commercial Arbitration provides that "the power conferred upon the arbitral tribunal includes the power to determine the admissibility, relevance, materiality and weight of any evidence."

---

[6] Ang Hwee Min, 'Law firm Shook Lin & Bok hit by ransomware attack' *The CNA* (Singapore, 2 May 2024) <https://www.channelnewsasia.com/singapore/shook-lin-and-bok-akira-ransomware-paid-ransom-bitcoin-4308441> accessed 19 May 2024.

[7] Nimitt Dixit, 'SG: Shook Lin Hit By Cyberattack, Says No Evidence Of Client Data Theft' *Asian Legal Business* (7 May 2024) <https://www.legalbusinessonline.com/other-news/sg-shook-lin-hit-cyberattack-says-no-evidence-client-data-theft> accessed 19 May 2024.

[8] Luke Eric Peterson, 'Permanent Court of Arbitration Website Goes Offline, with Cyber-Security Firm Contending that Security Flaw Was Exploited in Concert with China-Philippines Arbitration' *IA Reporter* (23 July 2015)<https://www.iareporter.com/articles/permanent-court-of-arbitration-goes-offline-with-cyber-security-firm-contending-that-security-flaw-was-exploited-in-lead-up-to-china-philippines-arbitration/> accessed 19 May 2024.

[9] David Tweed, 'China's Cyber Spies Take to High Seas as Hack Attacks Spike' *Bloomberg* (16 October 2015) <https://www.bloomberg.com/news/articles/2015-10-15/chinese-cyber-spies-fish-for-enemies-in-south-china-sea-dispute> accessed 19 May 2024.

Article 9(1) of the International Bar Association Rules on the Taking of Evidence in International Arbitration ("IBA Rules") provides that "the Arbitral Tribunal shall determine the admissibility, relevance, materiality and weight of evidence."

Article 25.2 of the Dubai International Arbitration Centre Rules 2022 provides that "the Tribunal shall have the power to determine the admissibility, relevance, materiality and weight of any such evidence."

Rule 36(1) of the International Centre for Settlement of Investment Disputes ("ICSID") Arbitration Rules 2022 provides that "the Tribunal shall determine the admissibility and probative value of the evidence adduced."

Rule 19.2 of the Singapore International Arbitration Centre Rules 2016[10] states that "the Tribunal shall determine the relevance, materiality and admissibility of all evidence. The Tribunal is not required to apply the rules of evidence of any applicable law in making such determination."

Article 27 of the Asian International Arbitration Centre (Malaysia) Arbitration Rules 2023 states that "the arbitral tribunal shall determine the admissibility, relevance, materiality and weight of the evidence offered." Further, *Section 21(3)(a) of the Arbitration Act 2005* also provides that the power conferred upon the arbitral tribunal shall include the power to "determine the admissibility, relevance, materiality and weight of any evidence."

By contrast, the International Chambers of Commerce Arbitration Rules 2021 is silent on the arbitral tribunal's power on admissibility of evidence.[11]

3.1. Article 9(3) of the IBA Rules Specifically Addresses Illegally Obtained Evidence

The IBA Rules, one of the most widely used soft law instruments in international arbitrations[12] regardless of the administering institutions, *ad hoc*, other rules or procedures governing international arbitrations[13], specifically address illegally obtained evidence in its *Article 9(3)*.

It is a new provision added in the 2020 version of the IBA Rules[14], stating that "the arbitral tribunal may, at the request of a Party or on its own motion, exclude evidence obtained illegally." The use of the word "may", instead of "shall", was to give arbitral tribunals the discretion in deciding whether to exclude illegally obtained evidence.

[10] Similar provision is available at Article 32.2 of the SIAC Rules (7th edn) (consultation draft).
[11] Gullermo Garcia-Perrote, 'Admissibility of 'Hacked Evidence' in International Arbitration' (*Kluwer Arbitration Blog,* 7 July 2021) <https://arbitrationblog.kluwerarbitration.com/2021/07/07/admissibility-of-hacked-evidence-in-international-arbitration/> accessed 14 July 2024.
[12] Queen Mary University of London, '2015 International Arbitration Survey: Improvements & Innovations in International Arbitration' (2015) 35.
[13] International Bar Association Rules on the Taking of Evidence in International Arbitration, Foreword.
[14] Commentary on the revised text of the 2020 IBA Rules on the Taking of Evidence in International Arbitration (January 2021) <https://www.ibanet.org/MediaHandler?id=4F797338-693E-47C7-A92A-1509790ECC9D> accessed 13 July 2024.

The choice of word was made after contemplating whether to capture the specific circumstances in which illegally obtained evidence should be excluded, but the IBA 2020 Review Task Force ("IBA Task Force") concluded that there was no clear consensus on the issue. National laws vary on whether illegally obtained evidence should be excluded from criminal and civil proceedings. Similarly, arbitral tribunals have reached different conclusions depending on, among other things, whether the party offering the evidence was involved in the illegality, considerations of proportionality, whether the evidence is material and outcome determinative, whether the evidence has entered the public domain through public "*leaks"*, and the clarity and severity of the illegality. The IBA Task Force has sought to accommodate this diversity by providing that the arbitral tribunal may exclude evidence under *Article 9(3)* whereas it shall exclude evidence where the grounds of *Article 9(2)* are present[15].

Article 9(3) of the IBA Rules is to be contrasted with *Article 9(2)*, which states "the arbitral tribunal shall, at the request of a Party or on its own motion, exclude from evidence or production any Document, statement, oral testimony or inspection" on grounds of "commercially and technical confidentiality"[16], "special political or institutional sensitivity (including evidence that has been classified as secret by a government or a public international institution)"[17] and "considerations of … fairness or equality of the Parties."[18]

Illegally obtained evidence could therefore fall within those grounds under *Article 9(2) of the IBA Rules*. Under such circumstances, the arbitral tribunal is compelled to exclude the illegally obtained evidence. Nonetheless, the arbitral tribunal retains discretion to determine whether any of the specified criteria has been met. In addition, the introductory language of *Article 9(2)*, as revised by the IBA Task Force, makes clear that the arbitral tribunal has discretion to exclude the evidence in whole or in part, depending on whether the grounds listed in *Article 9(2)* apply to the whole document or only to some of its parts.[19]

3.2. Decisions of Arbitral Tribunal on Illegally Obtained Evidence

Even before the introduction of *Article 9(3) of the IBA Rules*, documents obtained through hacking or other illegal means have been requested to be admitted as part of the evidence in arbitral proceedings. In some instances, arbitral tribunals have excluded such documents from the proceedings, regardless of their relevance or materiality to the dispute.

In *ConocoPhillips v Venezuela*[20], the respondent requested[21] the arbitral tribunal for a hearing to specifically address their findings that the respondent "breached its obligation to negotiate in good faith for compensation for its taking of the ConocoPhillips assets in the three

[15] ibid 30.
[16] IBA Rules (n 13) art 9.2(e).
[17] ibid art 9.2(f).
[18] Ibid art 9.2(g).
[19] Commentary on the 2020 IBA Rules (n 14) 26.
[20] *Conocophillips Petrozuata B.V. Conocophillips Hamaca B.V. Conocophillips Gulf Of Paria B.V. and Conocophillips Company v Bolivarian Republic Of Venezuela* (ICSID Case No. Arb/07/30).
[21] Respondent's Request dated 8.9.2013 <https://www.italaw.com/sites/default/files/case-documents/italaw1583.pdf> accessed 20 July 2024.

projects"[22]. In the respondent's request, the respondent produced new evidence disclosed by WikiLeaks, which would demonstrate that the respondent had engaged in good faith negotiations with ConocoPhillips. Although the majority of the arbitral tribunal did not find that they have the power to reconsider their findings[23], Professor Abi-Saab dissented, holding that arbitrators should not "close its blinkers"[24] on such "glaring evidence"[25], despite the evidence being unlawfully obtained from a third-party source. To do so, in the words of Professor Abi-Saab, would make "mockery not only of ICSID arbitration but of the very idea of adjudication". [26]

In *Caratube v Kazakhstan*[27], the claimant requested for leave to produce certain documents out of the 60,000 documents that were publicly available on the website of "KazakhLeaks"[28]. The documents were leaked to the website following the hacking of the respondent's government system. The tribunal allowed the production of non-privileged leaked documents but excluded privileged leaked documents, namely privileged attorney-client communications.[29]

In *Yukos Universal Limited v Russian*[30], US Statement Department cables emerged via "WikiLeaks" were relied upon by parties and considered by the arbitral tribunal when making their decision[31], with no issue of admissibility being ventilated.

In *Libananco v Turkey (ICSID ARB/06/8)*[32], the respondent obtained 1,000 privileged, private and confidential emails by intercepting emails and instant messages sent by, to and between the claimant and its counsel in connection with the arbitration over the years.[33] The interception was made pursuant to a Turkish court order issued in a separate money laundering investigation[34]. The arbitral tribunal decided to exclude all privileged documents and information obtained through the interception from the arbitration[35] to uphold the principles of procedural fairness as well as respect for confidentiality and legal privilege.[36]

---

[22] Decision on Jurisdiction and the Merits dated 3.9.2013, para 404(d) <https://www.italaw.com/sites/default/files/case-documents/italaw1569.pdf> accessed 20 July 2024.
[23] Decision on Respondent's Request For Reconsideration dated 10.3.2017, para 24 <https://www.italaw.com/sites/default/files/case-documents/italaw3119.pdf> accessed 20 July 2024.
[24] Decision of Respondent's Request For Reconsideration Dissenting Opinion of Georges Abi-Saab, para 66 <https://www.italaw.com/sites/default/files/case-documents/italaw3121.pdf> accessed 20 July 2024.
[25] ibid.
[26] ibid.
[27] *Caratube International Oil Company LLP v Republic of Kazakhstan and Mr. Devincci Salah Hourani v Republic of Kazakhstan* (ICSID Case No. ARB/13/13).
[28] Award dated 27.9.2017, para 150 <https://icsidfiles.worldbank.org/icsid/ICSIDBLOBS/OnlineAwards/C2923/DC11204_En.pdf> accessed 20 July 2024.
[29] ibid para 156.
[30] *Yukos Universal Limited (Isle of Man) v The Russian Federation* (PCA Case No. AA227).
[31] Final Award dated 18 July 2014, paras 1189, 1199, 1201, 1202-1208, 1213 and 1223 <https://pcacases.com/web/sendAttach/420> accessed 20 July 2024.
[32] *Libananco Holdings Co. Limited v Republic Of Turkey* (ICSID Case No. Arb/06/8).
[33] Decision on Preliminary Issues dated 23.6.2008, para 19 <https://www.italaw.com/sites/default/files/case-documents/ita0465.pdf> accessed 20 July 2024.
[34] ibid para 19.
[35] ibid para 82.
[36] ibid para 78.

In *Methanex Corporation v United States*[37], the claimant obtained documents by deliberately trespassing onto private property and rummaging through dumpsters inside the office building for documentation.[38] The arbitral tribunal did not allow these unlawfully obtained documents to be used in the arbitration. The arbitral tribunal found that the introduction of these documents into the arbitration proceedings would be "in violation of a general duty of good faith imposed by the UNCITRAL Rules".[39] With regard to the claimant's multiple acts of trespass over five and a half months, the arbitral tribunal found that such conduct "offended basic principles of justice and fairness required of all parties in every international arbitration".[40]

In *EDF (Services) Ltd v Romania*[41], the claimant requested the arbitral tribunal to admit an audio tape and a transcript of a recording of a conversation alleged to have occurred on 19 October 2001, which captured an offer of corrupt payment. As the audio recording was recorded at the home of the respondent's officer without her consent and in breach of her right to privacy,[42] the arbitral tribunal did not allow the illegally obtained evidence to be admitted, as it "would be contrary to the principles of good faith and fair dealing required in international arbitration"[43].

The arbitral tribunal shared the position in *Methanex Corporation v United States*[44], holding that the arbitral tribunal is "the judge of the admissibility of any evidence adduced" as provided under *Rule 34(1) of the ICSID Arbitration Rules*[45], the arbitral tribunal emphasized that:

> "Good faith and procedural fairness being among such principles, the Tribunal should refuse to admit evidence into the proceedings if, depending on the circumstances under which it was obtained and tendered to the other Party and the Tribunal, there are good reasons to believe that those principles of good faith and procedural fairness have not been respected."[46]

From the cases above, it appears that illegally obtained evidence and privileged information, regardless of relevance, tend to be excluded if admitting such evidence would contradict the principles of good faith and procedural fairness. However, these are not fixed rules and the arbitral tribunal retains wide discretion in deciding whether to admit or exclude such evidence.

---

[37] *Methanex Corporation v United States of America*, North American Free Trade Agreement ("NAFTA") Chapter 11 Arbitration.
[38] Final Award of the Tribunal on Jurisdiction and Merits dated 3 August 2005, pt II – chp I - para 55 <https://www.italaw.com/sites/default/files/case-documents/ita0529.pdf> accessed 20 July 2024.
[39] ibid pt II – chp I - para 58.
[40] ibid pt II – chp I - para 59.
[41] *EDF (Services) Limited v Romania* (ICSID Case No ARB/05/13) dated 8 October 2009 <https://www.italaw.com/sites/default/files/case-documents/ita0267.pdf> accessed 20 July 2024.
[42] Procedural Order No. 3, para 1 and 38 <https://www.italaw.com/sites/default/files/case-documents/ita0264.pdf> accessed 20 July 2024.
[43] ibid para 38.
[44] ibid para 37 - 38.
[45] ICSID Arbitration Rules 2006 (as amended and effective April 10, 2006).
[46] ibid para 47.

In Malaysia, it is trite law that evidence even when obtained illegally, is admissible, as the issue is relevance. This is established in the Federal Court case of *Benjamin William Hawkes v PP*[47], where the Court held that:

> "Hence it is only procedural and not evidential. It is trite law that even in cases of evidence obtained illegally, its admissibility is unaffected as the issue is relevancy. This was explained by Lord Goddard in the Privy Council case of Karuma v The Queen [1955] AC 197:
>
> 'the test to be applied in considering whether evidence is admissible is whether it is relevant to the matter in issue. If it is, it is admissible and the court is not concerned with how the evidence is obtained.'"

In other words, evidence is admitted when it is relevant to proving or disproving an alleged fact. Once admitted, it is entered into record and can be considered by the arbitrator in deciding the matter. Admissible evidence therefore means that "the evidence introduced is of such a character that the court or judge is bound to receive it; that is, allow it to be introduced at trial."[48] This is to be distinguished from the weight of evidence. Only after the evidence is admitted will an arbitrator put the appropriate weight to it. Arbitrators are required to carefully consider whether to admit or exclude evidence tendered before them. If an arbitrator's decision to exclude evidence prevents a party from effectively presenting their case or undermines their right to a fair hearing, it could result in the arbitral award being set aside on the grounds of a breach of the principle of natural justice. Therefore, arbitrators must ensure that their decisions on admissibility of evidence do not compromise the fairness of the arbitration process.

4. Importance of Cybersecurity in International Arbitration

In the BCLP Arbitration Survey Report 2018[49], 90% of the respondents stated that cybersecurity is an important issue in international arbitration. The remaining respondents either considered it not important (6%) or were unsure (4%). Interestingly, two-thirds of those who did not consider it important sat both as arbitrators and practising counsel.

Despite the recognition of cybersecurity as an important issue in international arbitration, according to the 2021 International Arbitration Survey by the Queen Mary University of London[50], only around a quarter of respondents had "frequently" (18%) or "always" (9%) seen cybersecurity measures being implemented in their international arbitrations. The majority (57%) encountered such measures in less than half of their cases, while 16% respondents had "never" seen such measures in place.

[47] [2020] 5 MLJ 417.
[48] Henry Campbell Black, Joseph R. Nolan and Jacqueline M. Nolan-Haley, *Black's Law Dictionary* (6th edn, St. Paul, Minn. West Publishing Co 1990) 47.
[49] Bryan Cave Leighton Paisner, 'International Arbitration Survey: Cybersecurity in Arbitration Proceedings' (Bryan Cave Leighton Paisner) 6 <https://www.bclplaw.com/a/web/160089/3WJsPc/bryan-cave-leighton-paisner-arbitration-survey-report-2018p.pdf> accessed 23 June 2024.
[50] Queen Mary University of London, '2021 International Arbitration Survey: Adapting Arbitration to a Changing World' (Queen Mary University of London) <https://www.qmul.ac.uk/arbitration/research/2021-international-arbitration-survey/> accessed 23 June 2024.

Implementing cybersecurity measures is crucial, as the consequences of security breaches can be highly damaging.

4.1. Reputational Damage

When a high-profile cyberattack happens, it often attracts media attention.[51] The media coverage can have a negative impact on the reputation of the parties, arbitrators, administering institutions and in some cases, third parties as well.[52] The exposure of sensitive data, confidential information and privileged communication as a result of cyberattack can result in an erosion of public trust and a loss of existing and potential clients' trust[53], who might be concerned with the cybersecurity measures are not up to par. The unavailability of data, networks, platforms, or websites due to disruption caused by a cyberattack incident[54] would bring about huge inconvenience to others and pose great risk to reputation.

4.2. Financial Loss

A study[55] on the impact of data breaches on share prices shows that the stocks of breached companies, on average, underperformed by -3.2% in the six months after a breach disclosure. It also shows that stock prices bottomed out 41 business days following a breach, sinking -1.4% on average. Stock prices recovered to their pre-breach disclosure levels 53 days after a breach.

Apart from the impact on share prices, financial losses may arise from ransom payments, operational disruptions such as down time, loss of productivity, expenses incurred for data recovery and investigations, loss of revenue due to loss of clients' trust, and increased insurance premiums.[56]

4.3. Legal and Regulatory Implications

A breach of data used in an arbitration may lead to a breach of confidentiality by arbitration stakeholders. Such a breach of confidentiality may then lead to actions based on either contract law or the tort of breach of confidential information, giving rise to injunctive relief to protect from potential or further breaches.[57] The disclosure of commercially sensitive,

[51] David Carnal, '5 Ways Cyberattacks Can Damage a Company's Reputation' (*Anapaya*, 19 May 2023) <https://www.anapaya.net/blog/5-ways-cyberattacks-can-damage-a-companys-reputation> accessed 23 June 2024.

[52] International Council for Commercial Arbitration, 'The ICCA Reports No. 6: ICCA-NYC Bar-CPR Protocol on Cybersecurity in International Arbitration' (2022) International Council for Commercial Arbitration 9 <https://static.cpradr.org/docs/Cybersecurity%20ICCA-NYC%20Bar-CPR-protocol-international-arbitration-2022.pdf> accessed 20 July 2024.

[53] David (n 49).

[54] ICCA-NYC Bar-CPR Protocol (n 50).

[55] Paul Bischoff, 'How data breaches affect stock market share prices' (*Comparitech*, 5 June 2024) <https://www.comparitech.com/blog/information-security/data-breach-share-price-analysis/> accessed 24 July 2024.

[56] Thangaraj Petchiappan, 'The Financial Impact of Cyber Breaches on Businesses: Direct & Hidden Expenses' (*iLink Digital*, 2 October 2023) <https://www.ilink-digital.com/insights/blog/financial-impact-cyber-breaches-business-costs/> accessed 24 July 2024.

[57] Asian International Arbitration Centre (AIAC), 'Confidentiality in Arbitration: Fundamental Virtue or Mere Illusion?' (AIAC, 10 October 2023) <https://www.aiac.world/news/189/CONFIDENTIALITY-IN-ARBITRATION:-Fundamental-Virtue-or-Mere-Illusion > accessed 24 July 2024.

confidential, or personal information may violate laws or contractual commitments in business agreements. It may also trigger regulatory investigations or sanctions, or negligence claims.[58] Failure to adequately protect personal data used in arbitration may lead to liability under national data protection laws, such as the European Union's General Data Protection Regulation[59], Malaysia's Personal Data Protection Act 2010[60] and the Cyber Security Act 2024[61].

Apart from the parties involved, the arbitral tribunal and the administering arbitral institution, third parties outside the arbitration process may also be implicated[62] following cybersecurity or data breach. A data breach that reveals incriminating information could lead to further investigations as well.

4.4. Authenticity and Integrity of Data in the Arbitration Process

The use of digital files has become standard practice in international arbitration. However, digital files are easily altered, often without leaving detectable traces. This, coupled with the difficulty to differentiate a digital copy from a digital original, poses a cyber threat to the authenticity and veracity of data. Returning to a physical blue ink original may not resolve this issue, because such original may not exist.[63] Therefore, cybersecurity measures against such threats are important to preserve the integrity and authenticity of data to protect it from being tampered.[64] Without such protection, loss of integrity of data, or questions about the reliability and accuracy of data may arise due to a cybersecurity incident.[65] In the long run, the legitimacy of international arbitration may be undermined.[66] This may eventually lead to reputational loss to the arbitration process.

5. Steps Taken by the Arbitration Community to Tackle Cybersecurity Risks in Arbitration Proceedings

Some arbitral institutions have incorporated cybersecurity guidelines into their arbitration rules. For example, *Article 3.1(e) of the Hong Kong International Arbitration Centre Administered Arbitration Rules 2018* requires parties to upload files "to any secured online repository that the parties have agreed to use".

---

[58] Stephen Cohen and Mark Morril, 'A Call To Cyberarms: The International Arbitrator's Duty to Avoid Digital Intrusion' [2017] 40(3) Fordham International Law Journal 981, 989.

[59] Daniel Ling Tien Chong, 'Cybersecurity in International Arbitration: An Untapped Opportunity for Arbitral Institutions' [2002] 34 SAcLJ 432.

[60] At the time of writing this article, the Personal Data Protection (Amendment) Bill 2024 was passed by the House of Representatives (Dewan Rakyat), without any amendments.

[61] At the time of writing this article, the Cyber Security Act 2024 has been gazetted but has not come into force.

[62] Asmaa Saad Hussien and Hani Mohamed Mounes, 'Cybersecurity in international commercial arbitration (Legal vision)' (2024) 11(2) International Journal of Advanced and Applied Sciences 219, 225.

[63] Erik GW Schafer, 'Managing Data Privacy and Cybersecurity Issues' (*Global Arbitration Review*, 12 October 2023)<https://globalarbitrationreview.com/guide/the-guide-evidence-in-international-arbitration/2nd-edition/article/managing-data-privacy-and-cybersecurity-issues> accessed 24 July 2024.

[64] ibid.

[65] ICCA-NYC Bar-CPR Protocol (n 50).

[66] Dragana Nikolić and Sabine Leimüller, 'Cybersecurity in international arbitration: on the road towards green flags' (*schönherr*, 1 February 2024) <https://www.schoenherr.eu/content/cybersecurity-in-international-arbitration-on-the-road-towards-green-flags> accessed 24 July 2024.

Article 30A of the London Court of International Arbitration Arbitration Rules 2020 incorporated a new provision[67] providing that:

> "at an early stage of the arbitration, the Arbitral Tribunal shall…consider whether it is appropriate to adopt:
> any specific information security measures to protect the physical and electronic information shared in the arbitration; and
> any means to address the processing of personal data produced or exchanged in the arbitration in light of applicable data protection or equivalent legislation."

Rule 29(4) of the ICSID Arbitration Rules, in its 2022 revision, included a provision[68] requiring the tribunal to invite parties' views on "the treatment of confidential or protected information" before the first session.

A growing number of institutions, such as the Stockholm Chamber of Commerce, the International Centre for Dispute Resolution (being the international division of the American Arbitration Association), the Thai Arbitration Institute, and the ICC, have launched bespoke case management platforms to securely centralise file sharing in the effort to eliminate risks associated with email use.[69]

One of the most prominent steps taken to tackle cybersecurity risks in international arbitration is the publication of the Cybersecurity Protocol in International Arbitration ("Cybersecurity Protocol"). This protocol is a joint effort by the International Council for International Arbitration, the New York Bar Association and the International Institution for Conflict Prevention and Resolution. It was released in 2019 (2020 Edition) and updated in 2022. It aims to provide a framework for determining reasonable information security measures for individual arbitration matters and increasing awareness about information security in international arbitrations.[70]

Besides, the International Bar Association Cybersecurity Guidelines was published with the objective to provide a set of recommended best practices to help law firms protect themselves from breaches of data security, as stated in its introduction.

There is also the Protocol for Online Case Management in International Arbitration, which was developed to facilitate efficient and secure document sharing through the use of online case management tools. It sets out, among others, a list of properties and functionality of technical IT standards expected to be necessary for most arbitrations[71] as well as additional functionality depending on the needs of the arbitration.[72]

---

[67] LCIA Arbitration Rules 2020, art 30.5.
[68] ICSID Arbitration Rules 2022, r 29(4)(k).
[69] John Choon and others, 'Data protection and cybersecurity in international arbitration remain in the spotlight' (Freshfields Bruckhaus Deringer) <https://www.freshfields.com/en-gb/our-thinking/campaigns/international-arbitration-in-2023/data-protection-and-cybersecurity-in-international-arbitration-remain-in-the-spotlight/> accessed 25 July 2024.
[70] Cybersecurity Protocol, Foreword.
[71] Protocol for Online Case Management in International Arbitration, item 63.
[72] ibid item 64.

While there is no shortage of protocols and guidelines available for adoption by the parties in arbitration proceedings, there are practical challenges in implementing the recommended measures.

6. The Challenges in Implementing Cybersecurity Measures

There is a myriad of considerations to be taken into account when implementing relevant cybersecurity measures. The level of sensitivity or commercial value of the documents or information likely to be introduced into the arbitration is one of the main factors to consider;[73] the costs in implementing these cybersecurity measures and the financial resources of the parties to do so are also factors to consider. Therefore, any measures implemented not only have to be cost-efficient but also free from technological disparities to ensure a level playing field and prevent any party from gaining an unfair advantage.

Arbitrators and counsels involved in arbitration proceedings are often not IT experts.[74] They may lack the necessary knowledge and expertise in cybersecurity, and leaving the arbitral tribunal the power to make the necessary cybersecurity orders might require the tribunal to operate outside their professional qualifications and expertise.[75] The varying levels of awareness, resources and technical knowledge of data security issues among arbitrators may not in all cases equip them to deal with cybersecurity issues.[76]

Although guidelines and protocols set out measures or best practices, they are general in nature, and little guidance is provided as to which measures are appropriate in specific circumstances.[77] This may lead to tribunals setting their own cybersecurity measures based on their own concept of what is reasonable, without full knowledge or understanding of what may be in line with the norm or acceptable standards.[78]

According to BCLP's survey[79], 52% of respondents felt that a tribunal should in all cases have the power to impose cybersecurity measures, and 71% thought that a tribunal should have the power to impose sanctions for breach of measures either agreed upon by the parties or ordered by the tribunal.[80] However, requiring arbitral tribunals to decide on appropriate cybersecurity measures may place arbitrators in an uncomfortable position, as they need to decide the appropriate cybersecurity measures themselves.[81] At the very least, arbitrators will be making decisions which could potentially impact their own convenience, time and costs.[82]

[73] BCLP (n 47) 7.
[74] Claire Morel de Westgaver, 'Cybersecurity in International Arbitration – A Necessity and an Opportunity for Arbitral Institutions' (*Kluwer Arbitration Blog*, 6 October 2017) <https://arbitrationblog.kluwerarbitration.com/2017/10/06/cyber-security/> accessed 27 July 2024.
[75] Daniel (n 57).
[76] BCLP (n 47).
[77] Daniel (n 57).
[78] ibid.
[79] BCLP (n 47) 5.
[80] BCLP (n 47).
[81] Daniel (n 57).
[82] ibid.

7. Conclusion

In conclusion, the arbitration community is not immune to cyberattacks. The need for robust cybersecurity in international arbitration is heightened by the contentious nature of arbitration, the often high-value and high-stakes disputes, along with the cross-border elements involved.[83]

While institutional rules and protocols offer a degree of guidance, the practical implementation of those cybersecurity measures remains challenging. The practical implementation is further complicated by the lack of a one-size-fits-all solution. However, ongoing efforts to adapt and strengthen cybersecurity measures are essential to mitigate risks and ensure the arbitration community is better equipped to face future threats. There is still much work to be done, and the collective effort of the arbitration community is essential for continued progress.

[83] ICCA-NYC Bar-CPR Protocol (n 50) 8.

Bibliography

Astro Awani, '"Panama Papers" law firm says "hacked by servers abroad"' *Astro Awani* (6 April 2016) <https://www.astroawani.com/berita-dunia/panama-papers-law-firm-says-hacked-servers-abroad-101341> accessed 19 May 2024

Ang HM, 'Law firm Shook Lin & Bok hit by ransomware attack' *The CNA* (Singapore, 2 May 2024) <https://www.channelnewsasia.com/singapore/shook-lin-and-bok-akira-ransomware-paid-ransom-bitcoin-4308441> accessed 19 May 2024

Arbitration Act 2005

Asian International Arbitration Centre (AIAC), 'Confidentiality in Arbitration: Fundamental Virtue or Mere Illusion?' (AIAC, 10 October 2023) <https://www.aiac.world/news/189/CONFIDENTIALITY-IN-ARBITRATION:-Fundamental-Virtue-or-Mere-Illusion > accessed 24 July 2024

Asian International Arbitration Centre (Malaysia) Arbitration Rules 2023

Award dated 27.9.2017 <https://icsidfiles.worldbank.org/icsid/ICSIDBLOBS/OnlineAwards/C2923/DC11204_En.pdf> accessed 20 July 2024

Benjamin William Hawkes v PP [2020] 5 MLJ 417

Bischoff P, 'How data breaches affect stock market share prices' (*Comparitech*, 5 June 2024) <https://www.comparitech.com/blog/information-security/data-breach-share-price-analysis/> accessed 24 July 2024

Black HC, Nolan JR and Nolan-Haley JM, *Black's Law Dictionary* (6th edn, St. Paul, Minn. West Publishing Co 1990)

Bryan Cave Leighton Paisner, 'International Arbitration Survey: Cybersecurity in Arbitration Proceedings' (Bryan Cave Leighton Paisner) <https://www.bclplaw.com/a/web/160089/3WJsPc/bryan-cave-leighton-paisner-arbitration-survey-report-2018p.pdf> accessed 23 June 2024

Caratube International Oil Company LLP v Republic of Kazakhstan and Mr. Devincci Salah Hourani v Republic of Kazakhstan (ICSID Case No. ARB/13/13)

Carnal D, '5 Ways Cyberattacks Can Damage a Company's Reputation' (*Anapaya*, 19 May 2023)<https://www.anapaya.net/blog/5-ways-cyberattacks-can-damage-a-companys-reputation> accessed 23 June 2024

Choon J and others, 'Data protection and cybersecurity in international arbitration remain in the spotlight' (Freshfields Bruckhaus Deringer) <https://www.freshfields.com/en-gb/our-thinking/campaigns/international-arbitration-in-2023/data-protection-and-cybersecurity-in-international-arbitration-remain-in-the-spotlight/> accessed 25 July 2024

Cohen S and Morril M, 'A Call To Cyberarms: The International Arbitrator's Duty to Avoid Digital Intrusion' [2017] 40(3) Fordham International Law Journal 981

Commentary on the revised text of the 2020 IBA Rules on the Taking of Evidence in International Arbitration (January 2021)

<https://www.ibanet.org/MediaHandler?id=4F797338-693E-47C7-A92A-1509790ECC9D> accessed 13 July 2024

Conocophillips Petrozuata B.V. Conocophillips Hamaca B.V. Conocophillips Gulf Of Paria B.V. and Conocophillips Company v Bolivarian Republic Of Venezuela (ICSID Case No. Arb/07/30)

Cyber Security Act 2024

Decision of Respondent's Request For Reconsideration Dissenting Opinion of Georges Abi-Saab,<https://www.italaw.com/sites/default/files/case-documents/italaw3121.pdf> accessed 20 July 2024

Decision on Jurisdiction and the Merits dated 3.9.2013, <https://www.italaw.com/sites/default/files/case-documents/italaw1569.pdf> accessed 20 July 2024

Decision on Preliminary Issues dated 23.6.2008 <https://www.italaw.com/sites/default/files/case-documents/ita0465.pdf> accessed 20 July 2024

Decision on Respondent's Request For Reconsideration dated 10.3.2017 <https://www.italaw.com/sites/default/files/case-documents/italaw3119.pdf> accessed 20 July 2024

Dixit N, 'SG: Shook Lin Hit By Cyberattack, Says No Evidence Of Client Data Theft' *Asian Legal Business* (7 May 2024) <https://www.legalbusinessonline.com/other-news/sg-shook-lin-hit-cyberattack-says-no-evidence-client-data-theft> accessed 19 May 2024

Dubai International Arbitration Centre Rules 2022

EDF (Services) Limited v Romania (ICSID Case No ARB/05/13) dated 8 October 2009 <https://www.italaw.com/sites/default/files/case-documents/ita0267.pdf> accessed 20 July 2024

Final Award dated 18 July 2014 <https://pcacases.com/web/sendAttach/420> accessed 20 July 2024

Final Award of the Tribunal on Jurisdiction and Merits dated 3 August 2005 <https://www.italaw.com/sites/default/files/case-documents/ita0529.pdf> accessed 20 July 2024

Garcia-Perrote G, 'Admissibility of "Hacked Evidence" in International Arbitration' *(Kluwer Arbitration Blog*, 7 July 2021) <https://arbitrationblog.kluwerarbitration.com/2021/07/07/admissibility-of-hacked-evidence-in-international-arbitration/> accessed 14 July 2024

Garside J, Watt H and Pegg D, 'The Panama Papers: how the world's rich and famous hide their money offshore' *The Guardian* (3 April 2016) <https://www.theguardian.com/news/2016/apr/03/the-panama-papers-how-the-worlds-rich-and-famous-hide-their-money-offshore> accessed 19 May 2024

Harding L, 'What are the Panama Papers? A guide to history's biggest data leak" *The Guardian* (5 April 2016) <https://www.theguardian.com/news/2016/apr/03/what-you-need-to-know-about-the-panama-papers> accessed 19 May 2024

Hong Kong International Arbitration Centre Administered Arbitration Rules 2018

Hussien AS and Mounes HM, 'Cybersecurity in international commercial arbitration (Legal vision)' (2024) 11(2) International Journal of Advanced and Applied Sciences 219

International Council for Commercial Arbitration, 'The ICCA Reports No. 6: ICCA-NYC Bar-CPR Protocol on Cybersecurity In International Arbitration' (2022) International Council for Commercial Arbitration <https://static.cpradr.org/docs/Cybersecurity%20ICCA-NYC%20Bar-CPR-protocol-international-arbitration-2022.pdf> accessed 20 July 2024

International Bar Association Cybersecurity Guidelines

International Bar Association Rules on the Taking of Evidence in International Arbitration

International Centre for Dispute Resolution being the international division of the American Arbitration Association

International Centre for Settlement of Investment Disputes Arbitration Rules 2022

International Chambers of Commerce Arbitration Rules 2021

Libananco Holdings Co. Limited v Republic of Turkey (ICSID Case No. Arb/06/8)

Ling DTC, 'Cybersecurity in International Arbitration: An Untapped Opportunity for Arbitral Institutions' [2002] 34 SAcLJ 432

London Court of International Arbitration Arbitration Rules 2020

Methanex Corporation v United States of America, North American Free Trade Agreement ("NAFTA")

Nikolić D and Leimüller S, 'Cybersecurity in international arbitration: on the road towards green flags' (*schönherr*, 1 February 2024) <https://www.schoenherr.eu/content/cybersecurity-in-international-arbitration-on-the-road-towards-green-flags> accessed 24 July 2024

Oi M, 'Panama Papers money-laundering trial begins' *The BBC* (9 April 2024) <https://www.bbc.com/news/articles/cnek443n8zvo> accessed 19 May 2024

Personal Data Protection (Amendment) Bill 2024

Petchiappan T, 'The Financial Impact of Cyber Breaches on Businesses: Direct & Hidden Expenses' (*iLink Digital*, 2 October 2023) <https://www.ilink-digital.com/insights/blog/financial-impact-cyber-breaches-business-costs/> accessed 24 July 2024

Peterson LE, 'Permanent Court Of Arbitration Website Goes Offline, with Cyber-Security Firm Contending that Security Flaw Was Exploited in Concert with China-Philippines Arbitration' *IA Reporter* (23 July 2015) <https://www.iareporter.com/articles/permanent-court-of-arbitration-goes-offline-with-cyber-security-firm-contending-that-security-flaw-was-exploited-in-lead-up-to-china-philippines-arbitration/> accessed 19 May 2024

Procedural Order No. 3 <https://www.italaw.com/sites/default/files/case-documents/ita0264.pdf> accessed 20 July 2024

Protocol for Online Case Management in International Arbitration

Protocol for Online Case Management in International Arbitration (3.7.2020) <https://www.lw.com/admin/upload/SiteAttachments/Platforms%20Protocol%20-%

20WG%20on%20LegalTech%20in%20Arbitration%20-%20November%202020.pdf> accessed 27 July 2024

Queen Mary University of London, '2015 International Arbitration Survey: Improvements & Innovations in International Arbitration' (2015)

—— '2021 International Arbitration Survey: Adapting Arbitration to a Changing World' (Queen Mary University of London) <https://www.qmul.ac.uk/arbitration/research/2021-international-arbitration-survey/> accessed 23 June 2024

Respondent's Request dated 8.9.2013 <https://www.italaw.com/sites/default/files/case-documents/italaw1583.pdf> accessed 20 July 2024

Schafer EGW, 'Managing Data Privacy and Cybersecurity Issues' (*Global Arbitration Review*, 12 October 2023)<https://globalarbitrationreview.com/guide/the-guide-evidence-in-international-arbitration/2nd-edition/article/managing-data-privacy-and-cybersecurity-issues> accessed 24 July 2024

Singapore International Arbitration Centre Rules 2016

Tweed D, 'China's Cyber Spies Take to High Seas as Hack Attacks Spike' *Bloomberg* (16 October 2015) <https://www.bloomberg.com/news/articles/2015-10-15/chinese-cyber-spies-fish-for-enemies-in-south-china-sea-dispute> accessed 19 May 2024

UNCITRAL Model Law on International Commercial Arbitration

Westgaver CM, 'Cybersecurity in International Arbitration – A Necessity and an Opportunity for Arbitral Institutions' (*Kluwer Arbitration Blog*, 6 October 2017) <https://arbitrationblog.kluwerarbitration.com/2017/10/06/cyber-security/> accessed 27 July 2024

Yukos Universal Limited (Isle of Man) v The Russian Federation (PCA Case No. AA227)