Published on e-First 4 July 2022

CYBERSECURITY IN INTERNATIONAL ARBITRATION

An Untapped Opportunity for Arbitral Institutions

On the day of release of the Award of the South China Sea Arbitration, the Permanent Court of Arbitration's website was breached and implanted with a malicious code that stole the personal data of individuals who had visited the specific webpage devoted to the politically contentious China–Philippines maritime boundary dispute. The impact was far-reaching. Apart from direct losses suffered by the victims of the hacking, the reputation of the institution was left tainted, and the political outcry particularly from the Philippines against the allegedly Chinese-backed hacking resulted in distrust and resentment. In today's technological era, the need for the capacity to deal with modern cybersecurity risks cannot be understated. Many arbitrations deal with sensitive information ranging from personal data to trade secrets and politically sensitive government information. However, the cybersecurity measures employed by tribunals, institutions and the parties to safeguard such information remains few and far between. The recently published ICCA–NYC Bar–CPR Protocol on Cybersecurity in International Arbitration displays momentous effort from the arbitration community to reverse this trend. However, more must be done.

Daniel **LING** Tien Chong[1]
LLB (National University of Singapore).

I. Introduction

1 Technology has shrunk distances, making international arbitration not only more efficient, but also in many instances, commercially viable.[2] Without air travel and electronic communication, it would be nearly impossible for parties and arbitrators from different parts of the world to exchange pleadings, hold hearings, and cross-

1 The author is grateful to Prof Gary Bell, Faculty of Law, National University of Singapore, for his valuable insights and guidance.

2 Jason Popp, "3 Digital Communication Trends that are Shrinking Distances" *The Business Journals* (7 April 2016) <https://www.bizjournals.com/bizjournals/how-to/technology/2016/04/3-digital-communication-trends-that-are-shrinking.html> (accessed 9 February 2020).

examine witnesses.[3] This reliance on technology in international arbitration is only set to increase. In a recent survey conducted by White & Case LLP and Queen Mary University of London ("WCQM Report"), an overwhelming majority of respondents favoured the increased use of hearing room technologies, cloud-based storage, videoconferencing, artificial intelligence and virtual hearing rooms.[4] Respondents believed that an increased use of technology would lead to greater efficiency in the conduct of arbitral proceedings.[5]

2 However, the increased and increasing use of technology does not come without risks.[6] In a 2014 report released by the Center for Strategic and International Studies, it was estimated that cybercrime already costs the global economy more than US$400bn every year.[7] By 2021, experts estimate that cybercrimes will cost the world US$6trn annually.[8] Breaches have become so prevalent that a common saying in cybersecurity today is that "there are two kinds of companies: those that have been breached and know it, and those that have been breached but don't know it".[9]

3 Lawyers have not been spared. Cybersecurity firm Mandiant estimates that at least 80 of the 100 biggest law firms by revenue in the

3 John AM Judge, "The Impact of Technology on International Arbitration and the Nature of Substantive Claims Asserted in International Arbitration" in *Contemporary Issues in International Arbitration and Mediation: The Fordham Papers (2013)* (Brill, 2014) ch 20, at p 407.

4 Paul Friedland & Stavros Brekoulakis, *2018 International Arbitration Survey: The Evolution of International Arbitration* (White & Case LLP & Queen Mary University of London, 2018) at p 3.

5 Paul Friedland & Stavros Brekoulakis, *2018 International Arbitration Survey: The Evolution of International Arbitration* (White & Case LLP & Queen Mary University of London, 2018) at p 3.

6 See European Union Agency for Cybersecurity website: <https://www.enisa.europa.eu> (accessed 9 February 2020).

7 Dan Zureich & William Graebe, "Cybersecurity: The Continuing Evolution of Insurance and Ethics" (2015) 82 *Defense Counsel Journal* 192; see also specific cases highlighted in Christopher Kuner *et al*, "The Rise of Cybersecurity and Its Impact on Data Protection" (2017) 7 *International Data Privacy Law* 73.

8 Julien Chaisse & Cristen Bauer, "Cybersecurity and the Protection of Digital Assets -- Assessing the Role of International Investment Law and Arbitration" (2019) 21(3) *Vanderbilt Journal of Entertainment & Technology Law* 549; Steve Morgan, "Global Cybersecurity Spending Predicted to Exceed $1 Trillion From 2017–2021" *Cybercrime Magazine* (10 June 2019) <https://cybersecurityventures.com/cybersecurity-market-report/> (accessed 9 February 2020).

9 David G Ries, "Cybersecurity for Attorneys: Addressing the Legal and Ethical Duties" *Law Practice Today* (14 November 2019) <https://www.lawpracticetoday.org/article/cybersecurity-attorneys-legal-ethical/> (accessed 9 February 2020).

US have been hacked between 2011 and 2015.[10] In 2017, the American Bar Association ("ABA") reported that 22% of law firms got hacked or experienced data breaches.[11] Information security company TruShield placed the legal industry as the second most targeted sector for cyberattacks.[12] Law firms have become coveted targets for cybercriminals.

4 Notably, many cyber breaches have already made front page news.[13] A US$40bn acquisition deal was almost derailed in 2012 when Chinese-based hackers targeted several Canadian-based law firms.[14] Not long after, the Panama Papers found itself in the headlines of media outlets around the world when 2.6TB of files from the database of the world's fourth biggest offshore law firm, Mossack Fonseca, was leaked online.[15] In 2017, Cravath, Swaine & Moore LLP and Weil, Gotshal & Manges LLP, two large US-based law firms, were involved in a major cybersecurity breach linked to a US$4m insider trading scheme.[16] By stealing quarterly earnings information prior to their public release, hackers were able trade on that information.[17] Undoubtedly, cyber criminals have recognised the

10 Julie Sobowale, "Law Firms Must Manage Cybersecurity Risks" *ABA Journal* (1 March 2017) <http://www.abajournal.com/magazine/article/managing_cybersecurity_risk> (accessed 9 February 2020); Sharon Nelson, John Simek & Michael Maschke, "Technology and Cybersecurity Policies Help Lawyers Manage Technology (Instead of It Managing Them)" (2017) 34 *The Computer & Internet Lawyer* 7 at 22.

11 Kirsten Wilson, "A Guide to Law Firm Cybersecurity Risks & Ethical Compliance" *Security Boulevard* (20 May 2019) <https://securityboulevard.com/2019/05/a-guide-to-law-firm-cybersecurity-risks-ethical-compliance/> (accessed 9 February 2020).

12 Julie Sobowale, "Law Firms Must Manage Cybersecurity Risks" ABA Journal (1 March 2017) <http://www.abajournal.com/magazine/article/managing_cybersecurity_risk> (accessed 9 February 2020); Sharon Nelson, John Simek & Michael Maschke, "Technology and Cybersecurity Policies Help Lawyers Manage Technology (Instead of It Managing Them)" (2017) 34 *The Computer & Internet Lawyer* 7 at 22.

13 Paul Gupta, "What Is 'Reasonable' Under the ABA's New Cybersecurity Obligations for Law Firms?" *Legal Executive Institute* (12 July 2017) <https://web.archive.org/web/20201022071017/https://www.legalexecutiveinstitute.com/aba-new-cybersecurity-obligations/> (accessed 7 June 2022).

14 Michael A Riley & Sophia Pearson, "China-Based Hackers Target Law Firms to Get Secret Deal Data" *Bloomberg Business* (31 January 2012) <https://www.bloomberg.com/news/articles/2012-01-31/china-based-hackers-target-law-firms> (accessed 9 February 2020).

15 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 9 February 2020).

16 "Inside Arbitration: Cybersecurity Matters: Arbitration Away from Prying Eyes" *Herbert Smith Freehills* (15 July 2019) <https://www.herbertsmithfreehills.com/latest-thinking/inside-arbitration-cybersecurity-matters-arbitration-away-from-prying-eyes> (accessed 9 February 2020).

17 Robin Sidel & Nicole Hong, "Hackers Breach Law Firms, Including Cravath and Weil Gotshal" *Wall Street Journal* (30 March 2016) <https://www.wsj.com/articles/

(cont'd on the next page)

value of the confidential financial and transactional information held by lawyers.[18]

5 In light of these events, the ABA has since warned law firms that the correct thinking should not be "whether firms will be the victim of a cyber-attack, but a question of when and to what extent".[19] A recent ethics opinion issued by the New York State Bar Association also noted that:[20]

> Cyber-security issues have continued to be a major concern for lawyers, as cyber-criminals have begun to target lawyers to access client information, including trade secrets, business plans and personal data. Lawyers can no longer assume that their document systems are of no interest to cyber-crooks.

6 Amongst the arbitral community, awareness for the dangers of cybersecurity appears, at first blush, to be satisfactory. In 2019, law firm Bryan Cave Leighton Paisner LLP reported that a staggering 90% of respondents from the arbitral community thought that cybersecurity was an important issue in international arbitration, with 11% of respondents indicating that they had had experience of arbitral proceedings being subject to a cybersecurity breach[21] ("BCLP Survey").

7 However, such knowledge for the dangers of cyberattacks has failed to translate into action.[22] Time and time again, international

---

hackers-breach-cravath-swaine-other-big-law-firms-1459293504> (accessed 9 February 2020).

18 Julie Sobowale, "Law Firms Must Manage Cybersecurity Risks" *ABA Journal* (1 March 2017) <http://www.abajournal.com/magazine/article/managing_cybersecurity_risk> (accessed 9 February 2020); Sharon Nelson, John Simek & Michael Maschke, "Technology and Cybersecurity Policies Help Lawyers Manage Technology (Instead of It Managing Them)" (2017) 34 *The Computer & Internet Lawyer* 7 at 22.

19 Elizabeth Beattie, "Cyber Security: Safe and Sound" *Asian Legal Business* (30 April 2019) <https://www.legalbusinessonline.com/features/cyber-security-safe-and-sound/77747> (accessed 9 February 2020); "Cyber Security: The Reputational, Enforcement and Litigation Risks" *Eversheds Sutherland* (21 November 2019) <https://www.evershedssutherland.com/global/en/what/articles/index.page?ArticleID=en/Litigation_Support/lawyer-article-cybersecurity> (accessed 9 February 2020).

20 George Burn *et al*, *International Arbitration Survey: Cybersecurity in International Arbitration – Don't be the Weakest Link* (Bryan Cave Leighton Paisner LLP, 6 February 2019) <https://www.bclplaw.com/a/web/160089/3WJsPc/bryan-cave-leighton-paisner-arbitration-survey-report-2018p.pdf> (accessed 9 February 2020).

21 Claire Morel de Westgaver, "Cybersecurity in International Arbitration: Don't Be the Weakest Link" *Kluwer Arbitration Blog* (15 February 2019) <http://arbitrationblog.kluwerarbitration.com/2019/02/15/cybersecurity-in-international-arbitration-dont-be-the-weakest-link/> (accessed 9 February 2020).

22 "Cybersecurity Protocol Will Raise Awareness of Data Protection in Arbitration, Says Expert" *Pinsent Masons* (26 November 2019) <https://www.pinsentmasons.com/out-law/news/cybersecurity-protocol-will-raise-awareness-of-data-protection-in-arbitration> (accessed 9 February 2020).

arbitration has seen a paucity of cybersecurity measures.[23] Surveys have shown that only 41% of lawyers and law firms who recently adopted cloud computing made changes to internal technology or security policies.[24] Many lawyers also continue to use popular consumer cloud services like Google Apps, iCloud, and Evernote, at much higher rates than secure cloud computing services dedicated for lawyers.[25] As one commentator notes, the results are "shocking" and "the current state of cloud security among law firms is a train wreck waiting to happen".[26] At the same time, arbitral institutions, national arbitration laws, and soft law instruments are either silent on the matter, or offer little practical guidance to parties and arbitrators.[27] As with many enterprises today, the international arbitration community has adopted modern information and communications technologies without fully realising the new types of risks that come with them.[28]

8 Amidst this backdrop, the joint ICCA–NYC Bar–CPR taskforce published the Protocol on Cybersecurity in International Arbitration ("2020 Protocol"), an unprecedented attempt by the arbitral community to reverse the trend of neglect for cybersecurity concerns.[29] In a time when cybersecurity concerns can no longer be ignored, the 2020 Protocol is much needed.

9 This article seeks to advocate the importance of cybersecurity, arguing that it is integral to the continued success of the arbitral process and is fundamental to the legitimacy of international arbitration. It then seeks to analyse the 2020 Protocol, the latest and perhaps most significant milestone in this field to date. Finally, this article will offer

---

23 Claire Morel de Westgaver, "Cybersecurity in International Arbitration: Don't Be the Weakest Link" *Kluwer Arbitration Blog* (15 February 2019) <http://arbitrationblog.kluwerarbitration.com/2019/02/15/cybersecurity-in-international-arbitration-dont-be-the-weakest-link/> (accessed 9 February 2020).

24 Dennis Kennedy, "2019 Cloud Computing" *ABA* (2 October 2019) <https://www.americanbar.org/groups/law_practice/publications/techreport/abatechreport2019/cloudcomputing2019/> (accessed 9 February 2020).

25 Dennis Kennedy, "2019 Cloud Computing" *ABA* (2 October 2019) <https://www.americanbar.org/groups/law_practice/publications/techreport/abatechreport2019/cloudcomputing2019/> (accessed 9 February 2020).

26 Dennis Kennedy, "2019 Cloud Computing" *ABA* (2 October 2019) <https://www.americanbar.org/groups/law_practice/publications/techreport/abatechreport2019/cloudcomputing2019/> (accessed 9 February 2020).

27 Hanna Roos & Jennifer Archie, "Call for Cybersecurity Guidelines in International Arbitration" *Lexology* (24 November 2017) <https://www.lexology.com/library/detail.aspx?g=4caf2e48-f598-46c4-8353-2a150f0295fc> (accessed 9 February 2020).

28 *ICC Cyber Security Guide for Business* (International Chamber of Commerce, 2015).

29 *ICCA–NYC Bar–CPR Protocol on Cybersecurity in International Arbitration (2020 Edition) New York Arbitration Week Special Printing* (International Council for Commercial Arbitration, 2019).

suggestions for the way forward by highlighting the indispensable role of arbitral institutions.

10 In doing so, this article will rely on a variety of sources, including quantitative and qualitative work. This includes existing literature and scholarship, market surveys conducted by various sources, as well as the author's own preliminary surveys and interviews with industry experts.[30]

A. Definitions

11 At the outset, this article notes Charlotte Tschider's definition of cybersecurity:[31]

> [T]he activity of process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorised use or modification or exploitation.

12 Jeff Kosseff similarly defines cybersecurity law as:[32]

> Cybersecurity law promotes the confidentiality, integrity, and availability of public and private information, systems, and networks, through the use of forward-looking regulations and incentives, with the goal of protecting individual rights and privacy, economic interests, and national security.

---

30 At this stage, the surveys conducted were based on a small but diverse sample size of active arbitrators, practitioners, academics, users, and arbitral institution personnel. The participants were carefully chosen to represent a diverse range of views from the different stakeholders in international arbitration. A total of 40 arbitrators, practitioners, academics, and institutions were surveyed. 75% acted as arbitrators, 45% acted as counsel, 32.5% were as academics, 10% worked in institutions (some respondents acted in multiple capacities).

Among those who had kindly taken the time included (in no particular order): Prof Bernard Hanotiau (Hanotiau & van den Berg), Prof Franco Ferrari (New York University), Prof Daniel Seng (National University of Singapore, Centre for Technology, Robotics, Artificial Intelligence and the Law), Prof Benjamin Hughes (The Arbitration Chambers), Nicholas Lingard (Freshfields Bruckhaus Deringer), Dr Matthew Secomb (White & Case LLP), Romesh Weeramantry (Clifford Chance LLP), Kevin Nash (Singapore International Arbitration Centre), Jonathan Lim (WilmerHale), Daryl Chew (Three Crowns LLP), Denys Hickey (39 Essex Chambers), David Kreider (independent arbitrator), Dorothy Udeme Ufot (Dorothy Ufot & Co), Dr Hop Dang (Hop Dang Chambers), Sapna Jhangiani QC (Clyde & Co), Andrew Garnett Paton (De Berti Jacchia Franchini Forlani), Urs Weber-Stecher (Wenger & Vieli), Lawrence Teh (Dentons Rodyk), Claus von Wobeser (Von Wobeser), Dr Christopher To (The Gilt Chambers), and many others. The author expresses his utmost gratitude to all who have taken the time to complete the surveys.

31 Charlotte A Tschider, *International Cybersecurity and Privacy Law in Practice* (Wolters Kluwer, 2018) at p 185.

32 Jeff Kosseff, "Defining Cybersecurity Law" 103 *Iowa Law Review* 985 at 1010.

13 Common from both definitions is the need to protect not just the confidentiality (access to information), but also the integrity (information not altered in transit), and availability (accessible to the relevant stakeholders who require it) of the information.[33] This article will address all three aspects.

14 It is also noted that cybersecurity seeks to protect both confidentiality and privacy. Just as confidentiality is meaningless if information is passed into the public domain, privacy equally depends absolutely on security.[34] No obligation to provide privacy, whether entered into voluntarily or compelled by law, will be meaningful if the data to be protected is accessed or stolen by unauthorised third parties.[35]

15 In this regard, "privacy" refers to the fact that only parties to the arbitration agreement may attend arbitral hearings and participate in the arbitral proceedings, and "confidentiality" refers to the obligation of the parties, arbitrators or institutions not to disclose information concerning the arbitration.[36] However, while they are both different and separate concepts, it may be artificial to discuss privacy and confidentiality separately in the context of cybersecurity.[37] This is because cybersecurity can be used to facilitate the protection of both confidentiality and privacy. A cybersecurity breach and consequent leak of pleadings, notes taken by the tribunal or counsel, and other documents relating to the arbitration may lead to a breach of confidentiality. Some authorities also

---

33 Jeff Kosseff, "International Cybersecurity Law" in *Cybersecurity Law* (John Wiley & Sons, Ltd, 1st Ed, 2017) ch 10, at p 343. The EU's General Data Protection Regulation similarly protects confidentiality, integrity and availability of information; see "Security" *Information Commissioner's Office* (4 October 2019) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/> (accessed 9 February 2020); see also Art 5(1)(f) of the EU's General Data Protection Regulation.

34 See *Calcraft v Guest* [1890] 1 QB 759; *Lord Ashburton v Pape* [1913] 2 Ch 469; *Goddard v Nationwide Building Society* [1986] 3 WLR 734 and *Wee Shuo Woon v HT S.R.L.* [2017] 2 SLR 94 at [30]; see also for discussion in the arbitration context Vivek Krishnani, "Confidentiality of Already Disclosed Documents: Admissibility of Improperly Obtained 'Privileged' Evidence" *Kluwer Arbitration Blog* (24 May 2019) <http://arbitrationblog.kluwerarbitration.com/2019/05/24/confidentiality-of-already-disclosed-documents-admissibility-of-improperly-obtained-privileged-evidence/> (accessed 9 February 2020).

35 Christopher Kuner *et al*, "The Rise of Cybersecurity and Its Impact on Data Protection" (2017) 7 *International Data Privacy Law* 73.

36 Gary Born, *International Commercial Arbitration* (Kluwer International, 2nd Ed, 2009) at pp 2250–2251.

37 Flor Villaggi, "International Commercial Arbitral Awards: Moving from Secrecy to Transparency?" *Academia* <https://www.academia.edu/3567667/International_Commercial_Arbitral_Awards_Moving_from_secrecy_to_transparency> (accessed 9 February 2020).

argue that the rationale for the privacy of hearings extends naturally to the confidentiality of hearing transcripts and other aspects of the arbitral process.[38] This article therefore seeks to jointly consider both concepts.[39]

II. The importance of cybersecurity in international arbitration

16 Robust cybersecurity in the arbitral process, or the lack thereof, has the potential to affect the legitimacy of international arbitration. A lack of assurance with regards to the integrity of information security in an arbitration can erode confidence in the arbitral process.[40] Since confidence in the system is indispensable to any private dispute resolution mechanism, such erosion has the ability to undermine the system of international arbitration as a whole.[41] As one commentator notes, "the credibility and integrity of any dispute resolution process depends on maintaining a reasonable degree of protection over the data exchanged during the process".[42]

17 Cybersecurity threats may create significant operational and legal problems that can compromise the arbitral process, including loss or unauthorised disclosure of sensitive data, breaches of attorney–client confidentiality, adverse media coverage and reputational damage, costs associated with breach notification or data recovery, and legal liability.[43]

38 See *Hassneh Insurance Co of Israel v Stuart J Mew* [1993] 2 Lloyd's Rep 243 at 27.

39 In so far as privacy relates to data protection, the comments of Dr Alexander Shchavelev, that "cybersecurity and data protection issues present in international arbitration are interwoven and should be discussed together" are well noted. See also "Cybersecurity Protocol Will Raise Awareness of Data Protection in Arbitration, Says Expert" *Pinsent Masons* (26 November 2019) <https://www.pinsentmasons.com/out-law/news/cybersecurity-protocol-will-raise-awareness-of-data-protection-in-arbitration> (accessed 9 February 2020).

40 Sarah Coble, "Cybersecurity Protocol for International Arbitration Published" *Infosecurity* (21 November 2019) <https://www.infosecurity-magazine.com:443/news/cybersecurity-protocol-arbitration/> (accessed 9 February 2020).

41 Jan Heiner Nedden & Aaron de Jong, "Arbitration in a Post-Truth World: Perception v Reality" (2018) 12(2) *Dispute Resolution International* 165; see also Kevin Elbert, "Confidence in Confidentiality: An Open Defence to the Closed Nature of Arbitration" (Fountain Court Chambers & Singapore Academy of Law, 2017) <https://www.sal.org.sg/sites/default/files/PDF%20Files/LDC%20PAC/CBP%202017%20-%20Kevin%20Elbert.pdf> (accessed 9 February 2020).

42 Sarah Coble, "Cybersecurity Protocol for International Arbitration Published" *Infosecurity* (21 November 2019) <https://www.infosecurity-magazine.com:443/news/cybersecurity-protocol-arbitration/> (accessed 9 February 2020).

43 "Debevoise Updates Two Key Resources for International Arbitration" *Debevoise & Plimpton* <https://www.debevoise.com/news/2018/01/debevoise-updates-two-key-resources> (accessed 9 February 2020).

As Mauricio Duarte notes, some of the main impacts of cybersecurity breaches include:[44]

(a) economic loss to parties, arbitrators, and arbitral institutions;

(b) reputational damage to arbitral institutions, arbitrators and counsel, as well as to the system of international arbitration overall; and

(c) potential liability under applicable laws and other regulatory frameworks.

A. Economic loss

18 Many arbitrations often involve information which are highly sensitive and have the potential to cause economic loss.[45] The production of evidence in international arbitration may involve the disclosure of a client's personal health information, trade secrets, financial information, intellectual property, or corporate strategies.[46]

19 Where large sums of money are involved, especially in high stakes cases, the impact of a cyber breach may be devastating.[47] The information may have the potential to cause commercial damage, influence share prices, frustrate corporate strategies and could have significant repercussions in the financial markets, particularly for a listed company.[48] In a recent 2018 research, it was found that the share prices of listed companies suffered following a reported hack, dropping an average of -2.89% after 14 days of trading.[49]

---

44 Mauricio Duarte, "Essential Tips on Cybersecurity for Arbitrators: Identify, Protect, Detect, Respond and Recover" *Medium* (6 February 2019) <https://medium.com/@mauricioduarte_20367/essential-tips-on-cybersecurity-for-arbitrators-identify-protect-detect-respond-and-recover-f889f50d71d3> (accessed 9 February 2020).

45 Karolina Kozłowska & Marta Kozłowska, "Cybersecurity for International Arbitration" *newtech.law* (20 March 2019) <https://newtech.law/en/cybersecurity-for-international-arbitration/> (accessed 9 February 2020).

46 Jim Pastore, "Practical Approaches to Cybersecurity in Arbitration" (2017) 40 *Fordham International Law Journal* 1023.

47 Sarah Coble, "Cybersecurity Protocol for International Arbitration Published" *Infosecurity* (21 November 2019) <https://www.infosecurity-magazine.com:443/news/cybersecurity-protocol-arbitration/> (accessed 9 February 2020).

48 "Inside Arbitration: Cybersecurity Matters: Arbitration Away from Prying Eyes" *Herbert Smith Freehills* (15 July 2019) <https://www.herbertsmithfreehills.com/latest-thinking/inside-arbitration-cybersecurity-matters-arbitration-away-from-prying-eyes> (accessed 9 February 2020).

49 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 9 February 2020). Over the same period, the shares were found to have underperformed the market by -4.6%. In the long run, underperformance of the company's share price in the market reached -3.7% (one year), -11.35% (two years), and -15.58% (three years).

20 Moreover, international arbitration may involve prominent parties such as multinational organisations, governments or state entities, and public figures.[50] Many of these actors are considered high value targets by cyber criminals.[51] Very often, these arbitrations require disclosure of materials which are not in the public domain, and such information may have the potential to influence politics and financial markets.[52] In some instances, cybersecurity may be an issue of national security, and a data leak could potentially undermine the democratic process.[53] In such cases, it may well be that even the existence of the arbitration itself is highly confidential.[54]

21 Furthermore, users of international arbitration generally expect arbitrations to be confidential.[55] Confidentiality has been cited as a key reason for choosing arbitration over other methods of dispute resolution.[56] When compared to litigation in national courts, confidentiality is often indicated as one of the major advantages of arbitration.[57] According to the WCQM Report, 62% listed confidentiality as a "very important"

50 Claire Morel de Westgaver, "Cybersecurity in International Arbitration – A Necessity and an Opportunity for Arbitral Institutions" *Kluwer Arbitration Blog* (6 October 2017) <http://arbitrationblog.kluwerarbitration.com/2017/10/06/cyber-security/> (accessed 9 February 2020).

51 Claire Morel de Westgaver, "Cybersecurity in International Arbitration – A Necessity and an Opportunity for Arbitral Institutions" *Kluwer Arbitration Blog* (6 October 2017) <http://arbitrationblog.kluwerarbitration.com/2017/10/06/cyber-security/> (accessed 9 February 2020).

52 Jeff Kosseff, "Defining Cybersecurity Law" 103 *Iowa Law Review* 985 at 1010.

53 Jeff Kosseff, "Defining Cybersecurity Law" 103 *Iowa Law Review* 985 at 1010.

54 Jim Pastore, "Practical Approaches to Cybersecurity in Arbitration" (2017) 40 *Fordham International Law Journal* 1023.

55 George Burn *et al*, *International Arbitration Survey: Cybersecurity in International Arbitration – Don't be the Weakest Link* (Bryan Cave Leighton Paisner LLP, 6 February 2019) <https://www.bclplaw.com/a/web/160089/3WJsPc/bryan-cave-leighton-paisner-arbitration-survey-report-2018p.pdf> (accessed 9 February 2020).

56 George Burn *et al*, *International Arbitration Survey: Cybersecurity in International Arbitration – Don't be the Weakest Link* (Bryan Cave Leighton Paisner LLP, 6 February 2019) <https://www.bclplaw.com/a/web/160089/3WJsPc/bryan-cave-leighton-paisner-arbitration-survey-report-2018p.pdf> (accessed 9 February 2020).

57 See "Inside Arbitration: Cybersecurity Matters: Arbitration Away from Prying Eyes" *Herbert Smith Freehills* (15 July 2019) <https://www.herbertsmithfreehills.com/latest-thinking/inside-arbitration-cybersecurity-matters-arbitration-away-from-prying-eyes> (accessed 9 February 2020), in which the author argues that "one of the many reasons that companies choose to resolve disputes through arbitration over court litigation is the ability to keep their disputes and the outcome of their disputes private".

attribute of arbitration.[58] In the words of the former Secretary-General of the ICC:[59]

> It became apparent to me very soon after taking up my responsibilities at the ICC that the users of international commercial arbitration, i.e. the companies, governments and individuals who are parties in such cases, place the highest value upon confidentiality as a fundamental characteristic of international commercial arbitration. When enquiring as to the features of international commercial arbitration which attracted parties to it as opposed to litigation, confidentiality of the proceedings and the fact that these proceedings and the resulting award would not enter into the public domain was almost invariable mentioned.

22 Indeed, many national laws recognise the confidential nature of arbitrations. According to Sir Patrick Neill QC, "it would be difficult to conceive of any greater threat to the success of English arbitration than the removal of the general principle of confidentiality and privacy".[60] Some national laws, including those of Morocco, Philippines, Peru, Scotland, Hong Kong and Norway have an express obligation of confidentiality in international arbitration, while many other countries such as England, France and Singapore have similar implicit obligations.[61]

23 Authorities from some of these jurisdictions argue that the duty of confidentiality is derived from party autonomy.[62] Others argue that the lack of confidentiality "would result in a host of very real evils – 'trial by

---

58 Paul Friedland & Stavros Brekoulakis, *2018 International Arbitration Survey: The Evolution of International Arbitration* (White & Case LLP & Queen Mary University of London, 2018) at p 3.

59 Alan Redfern & Martin Hunter, *Law and Practice of International Commercial Arbitration* (Sweet & Maxwell, 4th Ed, 2004) at p 32; Flor Villaggi, "International Commercial Arbitral Awards: Moving from Secrecy to Transparency?" *Academia* <https://www.academia.edu/3567667/International_Commercial_Arbitral_Awards_Moving_from_secrecy_to_transparency> (accessed 9 February 2020).

60 See Flor Villaggi, "International Commercial Arbitral Awards: Moving from Secrecy to Transparency?" *Academia* <https://www.academia.edu/3567667/International_Commercial_Arbitral_Awards_Moving_from_secrecy_to_transparency> (accessed 9 February 2020), citing *Department of Economics Policy & Development of the City of Moscow v Bankers Trust Co* [2003] 1 WLR 2885.

61 Flor Villaggi, "International Commercial Arbitral Awards: Moving from Secrecy to Transparency?" *Academia* <https://www.academia.edu/3567667/International_Commercial_Arbitral_Awards_Moving_from_secrecy_to_transparency> (accessed 9 February 2020).

62 Benjamin H Tahyar, "Confidentiality in ICSID Arbitration after *AMCO Asia Corp. v. Indonesia*: Watchword or White Elephant" (1986) 10 *Fordham International Law Journal* 93; see also Mayank Samuel, "Confidentiality in International Commercial Arbitration: Bedrock or Window-Dressing?" *Kluwer Arbitration Blog* <http://arbitrationblog.kluwerarbitration.com/2017/02/21/confidentiality-international-commercial-arbitration-bedrock-window-dressing/?print=print> (accessed 9 February 2020).

press release', distractions from the mutually-agreed, centralised dispute resolution mechanism, aggravation of the parties' dispute and the loss of important efficiency benefits".[63] Recently, Singapore's International Arbitration Act was also amended in 2020 to expressly grant the arbitral tribunal powers to make orders or give directions to any party to protect confidentiality.[64] Such orders and directions are enforceable in the Singapore High Court.

B. Reputational loss

24 Cybersecurity breaches may also result in reputational loss for the law firms, arbitrators, counsel, and institutions involved in the arbitration.[65] Once data breaches are made public, either by the media or by other means, reputational loss for the firm is almost inevitable.[66] Even if a firm quickly remedies the situation, the damage may already be done since the coverage and company reviews can continue to haunt the firm's reputation and continue to surface when clients (and prospective clients) research the firm.[67] This is especially detrimental in the legal industry since lawyers and law firms are built on reputation.[68] Client loyalty may be eroded or lost.[69]

63 Gary Born, *International Commercial Arbitration* (Kluwer International, 2nd Ed, 2009) at p 2283.

64 International Arbitration Act 1994 (2020 Rev Ed) s 12(1)(j).

65 Karolina Kozłowska & Marta Kozłowska, "Cybersecurity for International Arbitration" *newtech.law* (20 March 2019) <https://newtech.law/en/cybersecurity-for-international-arbitration/> (accessed 9 February 2020).

66 George Burn *et al*, *International Arbitration Survey: Cybersecurity in International Arbitration – Don't be the Weakest Link* (Bryan Cave Leighton Paisner LLP, 6 February 2019) <https://www.bclplaw.com/a/web/160089/3WJsPc/bryan-cave-leighton-paisner-arbitration-survey-report-2018p.pdf> (accessed 9 February 2020).

67 Elizabeth Beattie, "Cyber Security: Safe and Sound" *Asian Legal Business* (30 April 2019) <https://www.legalbusinessonline.com/features/cyber-security-safe-and-sound/77747> (accessed 9 February 2020); "Cyber Security: The Reputational, Enforcement and Litigation Risks" *Eversheds Sutherland* (21 November 2019) <https://www.evershedssutherland.com/global/en/what/articles/index.page?ArticleID=en/Litigation_Support/lawyer-article-cybersecurity> (accessed 9 February 2020).

68 Julie Sobowale, "Law Firms Must Manage Cybersecurity Risks" *ABA Journal* (1 March 2017) <http://www.abajournal.com/magazine/article/managing_cybersecurity_risk> (accessed 9 February 2020); Sharon Nelson, John Simek & Michael Maschke, "Technology and Cybersecurity Policies Help Lawyers Manage Technology (Instead of It Managing Them)" (2017) 34 *The Computer & Internet Lawyer* 7 at 22.

69 "Cyber Security: The Reputational, Enforcement and Litigation Risks" *Eversheds Sutherland* (21 November 2019) <https://www.eversheds-sutherland.com/global/en/what/articles/index.page?ArticleID=en/Litigation_Support/lawyer-article-cybersecurity> (accessed 9 February 2020).

25 Over time, multiple breaches in different cases may also have the potential to undermine confidence in the arbitral process as a whole.[70] In one international investment arbitration case, the Government of Turkey admitted to intercepting the opposing party's correspondence with its counsel and third parties, albeit as part of a separate criminal investigation.[71] In another case before the Permanent Court of Arbitration ("PCA"), the PCA's website was hacked on the day of release of the award.[72] The website was implanted with a malicious code that posed a data breach risk to anyone who visited a specific page devoted to the dispute.[73] Until today, the reputation of the PCA continues to suffer as the hacking remains very much in the minds of users and practitioners of international arbitration. While these highly publicised events remain isolated events, the increased targeting of lawyers by cyber criminals may soon erode confidence in the system of international arbitration if left unchecked.[74]

C. Legal liability

26 Cyber breaches may also lead to liability under national laws or other regulatory frameworks. For example, the failure to adequately protect personal data used in an arbitration may result in liability under various national laws such as the European Union's General Data Protection Regulation[75] ("GDPR"), the Singaporean Personal Data

70 Hanna Roos & Jennifer Archie, "Call for Cybersecurity Guidelines in International Arbitration" *Lexology* (24 November 2017) <https://www.lexology.com/library/detail.aspx?g=4caf2e48-f598-46c4-8353-2a150f0295fc> (accessed 9 February 2020).

71 *Libananco v Republic of Turkey*, ICSID Case No ARB/06/8, Award (2 September 2011); Claire Morel de Westgaver, "Cybersecurity in International Arbitration – A Necessity and an Opportunity for Arbitral Institutions" *Kluwer Arbitration Blog* (6 October 2017) <http://arbitrationblog.kluwerarbitration.com/2017/10/06/cyber-security/> (accessed 9 February 2020).

72 "Inside Arbitration: Cybersecurity Matters: Arbitration Away from Prying Eyes" *Herbert Smith Freehills* (15 July 2019) <https://www.herbertsmithfreehills.com/latest-thinking/inside-arbitration-cybersecurity-matters-arbitration-away-from-prying-eyes> (accessed 9 February 2020).

73 Claire Morel de Westgaver, "Cybersecurity in International Arbitration – A Necessity and an Opportunity for Arbitral Institutions" *Kluwer Arbitration Blog* (6 October 2017) <http://arbitrationblog.kluwerarbitration.com/2017/10/06/cyber-security/> (accessed 9 February 2020).

74 Mark Grady & Francesco Parisi, "The Law and Economics of Cybersecurity: An Introduction" in *The Law and Economics of Cybersecurity* (Mark F Grady & Francesco Parisi eds) (Cambridge University Press, 2006).

75 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) ("GDPR"). See also *WM Morrisons Supermarkets Plc v Various Claimants* [2018] EWCA Civ 2339, where the court held

(cont'd on the next page)

Protection Act,[76] various legislation in the US,[77] and many other national laws.[78] Privacy violations may also arise.[79]

27 A breach of data may also lead to contractual liability. Lawyers often have contractual duties to protect client information and other types of confidential information.[80] According to the ABA's 2016 Legal Technology Survey Report, 30.7% of all law firms and 62.8% of firms of 500 lawyers or more reported that current or potential clients provided them with security requirements.[81] Some of these requirements have already found their way into retainers and other agreements signed between the lawyers and their clients.

28 Various ethical rules also require lawyers to give due regard for issues of cybersecurity. Under most rules, lawyers have an ethical obligation to preserve the confidentiality of client information.[82] In the US, the obligation to safeguard clients' personal information and funds is both a legal and ethical one.[83] Attorneys have ethical and common law duties to take competent and reasonable measures to safeguard client information.[84] Under the ABA's Model Rules of Professional Conduct

---

the supermarket liable for a cyberbreach caused by its own rogue employee. See Ross McKean, "UK: How Real Is the Threat of Data Protection Group Litigation in the UK?" *Privacy Matters* (6 November 2018) <https://blogs.dlapiper.com/privacymatters/uk-how-real-is-the-threat-of-data-protection-group-litigation-in-the-uk/> (accessed 9 February 2020).

76 "Personal Data Protection Act Overview" *Personal Data Protection Commission Singapore* <https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act#:~:text=Scope%20of%20the%20PDPA,an%20employee%20with%20an%20organisation.> (accessed 25 May 2022).

77 Such as the Health Insurance Portability and Accountability Act. See "Summary of the HIPAA Privacy Rule" *HHS.gov* (7 May 2008) <https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html> (accessed 9 February 2020).

78 See n 33 for a review of the national laws of different jurisdictions around the world.

79 Jeff Kosseff, "Defining Cybersecurity Law" 103 *Iowa Law Review* 985 at 1007.

80 David G Ries, "Cybersecurity for Attorneys: Addressing the Legal and Ethical Duties" *Law Practice Today* (14 November 2019) <https://www.lawpracticetoday.org/article/cybersecurity-attorneys-legal-ethical/> (accessed 9 February 2020)

81 Julie Sobowale, "Law Firms Must Manage Cybersecurity Risks" *ABA Journal* (1 March 2017) <http://www.abajournal.com/magazine/article/managing_cybersecurity_risk> (accessed 9 February 2020); Sharon Nelson, John Simek & Michael Maschke, "Technology and Cybersecurity Policies Help Lawyers Manage Technology (Instead of It Managing Them)" (2017) 34 *The Computer & Internet Lawyer* 7 at 22.

82 Nicole Black, "Lawyers and Cybersecurity in 2019: How Does Your Firm Compare?" *Above the Law* (18 April 2019) <https://abovethelaw.com/2019/04/lawyers-and-cybersecurity-in-2019-how-does-your-firm-compare/> (accessed 9 February 2020).

83 Dan Zureich & William Graebe, "Cybersecurity: The Continuing Evolution of Insurance and Ethics" (2015) 82 *Defense Counsel Journal* 192 at 193.

84 David G Ries, "Cybersecurity for Attorneys: Addressing the Legal and Ethical Duties" *Law Practice Today* (14 November 2019) <https://www.lawpracticetoday.org/article/cybersecurity-attorneys-legal-ethical/> (accessed 9 February 2020).

("ABA Model Rules"), lawyers have an obligation to "provide competent representation".[85] Comment 8 to this Rule states that:[86]

> Maintaining Competence
>
> [8] To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, *including the benefits and risks associated with relevant technology*, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject. [emphasis added]

29 As part of one's continuing education, a lawyer must be aware of "the benefits and risks associated with relevant technology" in order to maintain competence.[87] Similarly, the Florida Bar's Rules of Professional Conduct rule 4-1.1 states, "[c]ompetent representation also involves safeguarding confidential information relating to the representation, including, but not limited to, electronic transmissions and communications".[88] The ABA House of Delegates has also passed, without opposition, a cybersecurity resolution:[89]

> RESOLVED, That the American Bar Association encourages private and public sector organizations to develop, implement, and maintain an appropriate cybersecurity program that complies with applicable ethical and legal obligations, and is tailored to the nature and scope of the organization, and the data and systems to be protected.

30 In 2017, ABA also published a Cybersecurity Handbook for attorneys to rely upon.[90] While the recommendations are not strictly binding, they may be indicative of the cybersecurity standards required of lawyers and law firms.[91] A breach of cybersecurity in international arbitration may consequently result in a violation of legal or ethical rules in the lawyer's home jurisdiction, likely arising from a failure to adequately protect client information.[92]

---

85 American Bar Association Model Rules of Professional Conduct Rule 1.1.

86 American Bar Association Model Rules of Professional Conduct Rule 1.1, Comment 8.

87 Dan Zureich & William Graebe, "Cybersecurity: The Continuing Evolution of Insurance and Ethics" (2015) 82 *Defense Counsel Journal* 192 at 193.

88 Jim Pastore, "Practical Approaches to Cybersecurity in Arbitration" (2017) 40 *Fordham International Law Journal* 1023.

89 Sharon Nelson, John Simek & Michael Maschke, "Technology and Cybersecurity Policies Help Lawyers Manage Technology (Instead of It Managing Them)" (2017) 34 *The Computer & Internet Lawyer* 7 at 24.

90 *The ABA Cybersecurity Handbook: A Resource for Attorneys, Law Firms and Business Professionals* (ABA Publishing, 2nd Ed, 2017).

91 Vincent I Polley, "Cybersecurity for Lawyers and Law Firms" (2014) 53 *American Bar Association* 4.

92 Julie Sobowale, "Law Firms Must Manage Cybersecurity Risks" *ABA Journal* (1 March 2017) <http://www.abajournal.com/magazine/article/managing_cybersecurity_

(cont'd on the next page)

III. The 2020 Protocol

31 The 2020 Protocol is the culmination of a remarkable effort by the joint ICCA–NYC Bar–CPR taskforce to deal with issues of cybersecurity in international arbitration.[93] The Protocol serves the twin goals of providing a framework for determining reasonable cybersecurity measures for individual arbitration matters and increasing awareness for cybersecurity in international arbitration.[94] In this way, it provides a valuable soft law on this matter.[95]

A. Raising awareness

32 The 2020 Protocol serves as an important step in raising awareness for cybersecurity risks and initiating a discussion within the arbitration community.[96] Its release helps to move cybersecurity into the centre of attention, at a time when awareness for the issue is severely lacking.[97]

33 Principle 2 of the 2020 Protocol recommends certain baseline information security practices which parties, arbitrators and institutions should adopt in the course of their general business activities.[98] Notably, this Principle does not appear to guide the parties and tribunal in each specific case, but rather serves as a guide for the arbitration community, indicating the recommended information security practices for the

risk> (accessed 9 February 2020); Sharon Nelson, John Simek & Michael Maschke, "Technology and Cybersecurity Policies Help Lawyers Manage Technology (Instead of It Managing Them)" (2017) 34 *The Computer & Internet Lawyer* 7 at 22.

93 *ICCA–NYC Bar–CPR Protocol on Cybersecurity in International Arbitration (2020 Edition) New York Arbitration Week Special Printing* (International Council for Commercial Arbitration, 2019).

94 Sarah Coble, "Cybersecurity Protocol for International Arbitration Published" *Infosecurity* (21 November 2019) <https://www.infosecurity-magazine.com:443/news/cybersecurity-protocol-arbitration/> (accessed 9 February 2020).

95 George Burn *et al*, *International Arbitration Survey: Cybersecurity in International Arbitration – Don't be the Weakest Link* (Bryan Cave Leighton Paisner LLP, 6 February 2019) <https://www.bclplaw.com/a/web/160089/3WJsPc/bryan-cave-leighton-paisner-arbitration-survey-report-2018p.pdf> (accessed 9 February 2020).

96 Claire Morel de Westgaver, "Cybersecurity in International Arbitration: Don't Be the Weakest Link" *Kluwer Arbitration Blog* (15 February 2019) <http://arbitrationblog.kluwerarbitration.com/2019/02/15/cybersecurity-in-international-arbitration-dont-be-the-weakest-link/> (accessed 9 February 2020).

97 Dennis Kennedy, "2019 Cloud Computing" *ABA* (2 October 2019) <https://www.americanbar.org/groups/law_practice/publications/techreport/abatechreport2019/cloudcomputing2019/> (accessed 9 February 2020).

98 *ICCA–NYC Bar–CPR Protocol on Cybersecurity in International Arbitration (2020 Edition) New York Arbitration Week Special Printing* (International Council for Commercial Arbitration, 2019) at p 10.

community to adopt in their day-to-day activities. The baseline security measures are in turn set out in Schedule A of the Protocol.

34 While the Protocol regrettably falls short of imposing standards applicable to all stakeholders involved in arbitrations, it is useful in raising awareness for the need for a comprehensive cybersecurity strategy. It succeeds in providing a pathway for the arbitration community to maintain a culture of awareness and effective security.[99]

B. Framework for arbitrations

35 The 2020 Protocol also provides a framework to determine reasonable information security measures for individual arbitration matters. This framework includes procedural and practical guidance to assess security risks and identify the available measures that can be implemented.[100] This facilitates the parties' negotiation and helps them to come to an agreement on the appropriate cyber measures to adopt. It also guides tribunals when issuing orders on cybersecurity, in cases where the parties are unable to agree.[101]

36 Principle 5 of the 2020 Protocol states that "the information security measures adopted for the arbitration shall be those that are *reasonable* in the circumstances of the case"[102] [emphasis added]. Principle 6 further states that:[103]

> In determining which specific information security measures are reasonable for a particular arbitration, the parties and the tribunal should consider:
>
> > (a) the risk profile of the arbitration, taking into account the factors set forth in Schedule B;

99 Sarah Coble, "Cybersecurity Protocol for International Arbitration Published" *Infosecurity* (21 November 2019) <https://www.infosecurity-magazine.com:443/news/cybersecurity-protocol-arbitration/> (accessed 9 February 2020).

100 *ICCA–NYC Bar–CPR Protocol on Cybersecurity in International Arbitration (2020 Edition) New York Arbitration Week Special Printing* (International Council for Commercial Arbitration, 2019) at v.

101 "Inside Arbitration: Cybersecurity Matters: Arbitration Away from Prying Eyes" *Herbert Smith Freehills* (15 July 2019) <https://www.herbertsmithfreehills.com/latest-thinking/inside-arbitration-cybersecurity-matters-arbitration-away-from-prying-eyes> (accessed 9 February 2020).

102 *ICCA–NYC Bar–CPR Protocol on Cybersecurity in International Arbitration (2020 Edition) New York Arbitration Week Special Printing* (International Council for Commercial Arbitration, 2019) at p 16.

103 *ICCA–NYC Bar–CPR Protocol on Cybersecurity in International Arbitration (2020 Edition) New York Arbitration Week Special Printing* (International Council for Commercial Arbitration, 2019) at p 17.

> (b) the existing information security practices, infrastructure, and capabilities of the parties, arbitrators, and any administering institution, and the extent to which those practices address the categories of information security measures referenced in Principle 7;
>
> (c) the burden, costs, and the relative resources of the parties, arbitrators, and any administering institution;
>
> (d) proportionality relative to the size, value, and risk profile of the dispute; and
>
> (e) the efficiency of the arbitral process.

37 This reflects the working group's view that "there is no one-size-fits-all approach to information security in arbitration matters and that the risk-based approach adopted by the Protocol, bounded by reasonableness, provides necessary flexibility to accommodate changes in technology, best practices and prevailing cyber risks, as well as the individual circumstances of each case, including considerations such as cost, proportionality, risk tolerance and technical capabilities".[104] The draft protocol merely provides a framework for parties and arbitrators to determine appropriate measures in the context of each case.[105]

38 This is in line with the approach taken by the Organisation for Economic Cooperation and Development ("OECD") in its 1980 Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, where the Security and Safeguards Principle was named as one of the eight foundational principles of data protection:[106]

> Personal data should be protected by *reasonable security safeguards* against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data. [emphasis added]

104 *Protocol Consultation Process* (ICCA–NYC Bar–CPR Working Group on Cybersecurity in International Arbitration, November 2019) <https://www.arbitration-icca.org/media/14/44059883674056/protocol_consultation_process.pdf> (accessed 9 February 2020).

105 Julie Bédard & Timothy G Nelson, "International Arbitration Community Turns Its Focus to Cybersecurity" *Skadden, Arps, Slate, Meagher & Flom LLP* (17 January 2019) <https://www.skadden.com/insights/publications/2019/01/2019-insights/international-arbitration-community> (accessed 9 February 2020).

106 Christopher Kuner *et al*, "The Rise of Cybersecurity and Its Impact on Data Protection" (2017) 7 *International Data Privacy Law* 73; "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" *OECD* <https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm> (accessed 9 February 2020). This principle was retained in the 2013 revision of the OECD Guidelines. See *The OECD Privacy Framework* (OECD, 2013) <https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf> (accessed 9 February 2020).

39 Similarly, Article 32 of the GDPR also adopts a risk-based analysis.[107] It requires one to have a level of security that is "appropriate" to the risks. This reflects the GDPR's risk-based approach, and that there is no one single solution which can be applied across-the-board to all situations.[108] What is "appropriate" will depend on the circumstances, nature of the processing, and the risks it presents. Most national cybersecurity laws also utilise a standard of "reasonable" measures.[109]

40 In similar vein, Rule 1.6(c) of the ABA Model Rules of Professional Conduct states that:[110]

> A lawyer shall make *reasonable efforts* to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client. [emphasis added]

41 The Comment to Rule 1.6 further explains that the factors to be considered in determining "the reasonableness of the lawyer's efforts include the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients".[111]

42 Much resemblance can be seen between the ABA Model Rules and the 2020 Protocol. Both entail a risk-based analysis, taking into account substantially the same factors.[112] While there is an active duty to prevent the unauthorised disclosure of information, this duty is one of "reasonable efforts".[113] This is because cybersecurity is a relative (and

---

107 GDPR Art 32.

108 "Security" *Information Commissioner's Office* <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/> (accessed 9 February 2020).

109 For "reasonable" measures standards in national cybersecurity laws in the Asia-Pacific Region, see n 33 at para 10.02.

110 American Bar Association Model Rules of Professional Conduct Rule 1.6(c).

111 American Bar Association Model Rules of Professional Conduct Rule 1.6(c), Comment [18]; see also American Bar Association Model Rules of Professional Conduct Rule 1.6(c), Comment [20]. Note that these factors are non-exhaustive.

112 David G Ries "Cybersecurity for Attorneys: Addressing the Legal and Ethical Duties" *Law Practice Today* (14 November 2019) <https://www.lawpracticetoday.org/article/cybersecurity-attorneys-legal-ethical/> (accessed 9 February 2020).

113 Dan Zureich & William Graebe, "Cybersecurity: The Continuing Evolution of Insurance and Ethics" (2015) 82 *Defense Counsel Journal* 192 at 193; see also Paul Gupta, "What Is 'Reasonable' Under the ABA's Newcom Cybersecurity Obligations for Law Firms?" *Legal Executive Institute* (12 July 2017) <https://web.archive.org/web/20201022071017/https://www.legalexecutiveinstitute.com/aba-new-cybersecurity-obligations//> (accessed 2 June 2022).

not absolute) concept.[114] It is neither possible nor prudent to mandate an across-the-board standard for every arbitration to follow. The measures adopted in an arbitration must be relative to the dispute at hand.[115]

43 Once information is digitised and stored virtually, it is impossible to completely eradicate all risk of compromise. Cybersecurity therefore only seeks to mitigate the risk of a cyber breach.[116] It is a matter of risk management. The appropriate robustness of security measures employed will depend on factors such as the risk profile of the arbitration, size and value of the dispute.[117] For example, an arbitration involving highly sensitive government information, or perhaps an arbitration requiring the disclosure of Coca-Cola's secret formula may require communications through a specialised secured server. Even so, this may not be sufficiently secure, and the tribunal may be invited to visit the company's facility in Atlanta where the physical copy of the recipe is stored behind a massive vault. On the other hand, implementing robust cybersecurity measures in a small arbitration may result in the arbitration's time and costs quickly becoming disproportionate to the quantum at stake.[118]

C. The challenges

44 While the 2020 Protocol brings about much needed progress in the area of cybersecurity in international arbitration, it is far from perfect.

45 Firstly, tribunals often lack knowledge and expertise in cybersecurity.[119] Requiring arbitrators to fashion cybersecurity measures

114 Xingan Li, "Cybersecurity as a Relative Concept" (2006) 18 *Information and Security: An International Journal* 11; see also Eugene McLaughlin & John Muncie, *The SAGE Dictionary of Criminology* (SAGE Publications Ltd, 4th Ed, 2019).

115 Kristen Wilson, "A Guide to Law Firm Cybersecurity Risks & Ethical Compliance" *Security Boulevard* (20 May 2019) <https://securityboulevard.com/2019/05/a-guide-to-law-firm-cybersecurity-risks-ethical-compliance/> (accessed 9 February 2020).

116 *Cybersecurity Guidelines* (International Bar Association, October 2018).

117 David G Ries, "Cybersecurity for Attorneys: Addressing the Legal and Ethical Duties" *Law Practice Today* (14 November 2019) <https://www.lawpracticetoday.org/article/cybersecurity-attorneys-legal-ethical/> (accessed 9 February 2020).

118 Alec Stone Sweet & Florian Grisel, "The Evolution of International Arbitration: Judicialization, Governance, Legitimacy" (Oxford University Press 2017) at p 27; see also for discussion on the need for time and costs to be proportionate to the value of the claim: José Ricardo Feris, "The 2017 ICC Rules of Arbitration and the New ICC Expedited Procedure Provisions: A View from Inside the Institution" *ICC Digital Library* (2017) <https://library.iccwbo.org/content/dr/ARTICLES/ART_0658.htm?l1=Articles&l2=2017&AUTH=29d9a5c3-7d2f-4376-816b-3bd735d09cc1&Timeframe=fb&l1=Articles&l2=2017&AUTH=29d9a5c3-7d2f-4376-816b-3bd735d09cc1&Timeframe=fb> (accessed 9 February 2020).

119 Claire Morel de Westgaver, "Cybersecurity in International Arbitration – A Necessity and an Opportunity for Arbitral Institutions" *Kluwer Arbitration Blog* (6 October

(cont'd on the next page)

in each individual case typically requires the tribunals to operate outside of their professional qualifications and expertise. Arbitrators, trained in international law, often do not have the technical skills to determine what the appropriate cybersecurity measures are in each individual case. According to the BCLP Survey, there are "significant variations in the level of awareness, resources and technical knowledge of data security issues and risk abatement steps among arbitrators".[120]

46 In preliminary surveys of the arbitration community conducted by this author, it was immediately apparent that a clear majority of respondents thought that arbitrators were not the best placed to deal with issues of cybersecurity.[121] Commonly cited reasons included the lack of necessary experience, expertise or technical means to properly deal with the issue, among others. Some arbitrators also complained that they have limited resources and that cybersecurity is an area which requires specialised technical knowledge, which arbitrators often do not possess. Others argued that such matters should be dealt with by the arbitral institutions to allow the tribunal to focus on the substantive dispute before them.

47 Secondly, the 2020 Protocol's framework will lead to inconsistency of treatment. Arbitrators who sit on individual cases will not know how issues of cybersecurity are dealt with in other cases due to the lack of precedent in international arbitration. While the 2020 Protocol offers a list of measures which the tribunal may consider implementing, little guidance is offered as to which measure is appropriate in the face of specific circumstances.[122] The only guidance given is that the robustness of the necessary cybersecurity measures will depend on the factors listed in Principle 6.[123] In practice, however, tribunals will not know which measure in Schedule C will be appropriate for which circumstances. Little or no guidance is offered to inform tribunals when and in what circumstances would the restriction of use of public WiFi networks,

2017) <http://arbitrationblog.kluwerarbitration.com/2017/10/06/cyber-security/> (accessed 9 February 2020).

120 George Burn *et al*, *International Arbitration Survey: Cybersecurity in International Arbitration – Don't be the Weakest Link* (Bryan Cave Leighton Paisner LLP, 6 February 2019) <https://www.bclplaw.com/a/web/160089/3WJsPc/bryan-cave-leighton-paisner-arbitration-survey-report-2018p.pdf> (accessed 9 February 2020).

121 75% of respondents thought that arbitrators were not the best placed to deal with issues of cybersecurity. See n 30 for the composition of the respondents of the survey.

122 *ICCA–NYC Bar–CPR Protocol on Cybersecurity in International Arbitration (2020 Edition) New York Arbitration Week Special Printing* (International Council for Commercial Arbitration, 2019) Schedule C.

123 *ICCA–NYC Bar–CPR Protocol on Cybersecurity in International Arbitration (2020 Edition) New York Arbitration Week Special Printing* (International Council for Commercial Arbitration, 2019) Principle 6.

mandatory use of secured VPNs, or the use of encrypted communications might be necessary.[124] This will lead to tribunals fashioning cybersecurity measures at their own discretion, based on their own conception of what is "reasonable" in the circumstances, without knowledge or understanding of what may be in line with the "norm", or "acceptable standards".

48 While some inconsistency is inevitable, a large disparity in treatment by different tribunals may negatively affect the reliability, effectiveness and predictability of the arbitration regime and, in the long run, its credibility.[125] Creating a system where justice is determined according to the length of the chancellor's foot is neither useful nor helpful towards international arbitration's overall legitimacy.[126] On the other hand, predictability and certainty facilitates the agreement of the parties.[127] If parties know beforehand the measures which the tribunal is likely to implement, the chances of arriving at an agreement on the appropriate measures to adopt will be increased. This leads to greater efficiency and a reduction of costs.[128]

49 Thirdly, requiring tribunals to decide upon the appropriate cybersecurity measures to adopt in the arbitration will place the arbitrators in an uncomfortable situation where they have to decide on the appropriate cybersecurity measures applicable to themselves. They will be required to make a decision which has a potentially large impact on their own convenience, time and costs. Since the cybersecurity measures adopted will have to be adhered to by the arbitral tribunal, arbitrators may find themselves in a situation where their personal preferences or practices may conflict with the objectives sought to be achieved by a robust cybersecurity strategy.[129] For example, an arbitrator

124 *ICCA–NYC Bar–CPR Protocol on Cybersecurity in International Arbitration (2020 Edition) New York Arbitration Week Special Printing* (International Council for Commercial Arbitration, 2019) Schedule C.

125 Michele Potestà & Gabrielle Kaufmann-Kohler, "Can the Mauritius Convention Serve as a Model for the Reform of Investor-State Arbitration in Connection with the Introduction of a Permanent Investment Tribunal or an Appeal Mechanism? – Analysis and Roadmap" (2016) CIDS at para 27.

126 See *Report of Working Group III (Investor-State Dispute Settlement Reform) on the work of its thirty-sixth session (Vienna, 29 October–2 November 2018)* (A/CN.9/964, 6 November 2018) at para 30; see also "Equity" *Oxford Reference* <https://www.oxfordreference.com/view/10.1093/oi/authority.20110803095755848> (accessed 9 February 2020).

127 Beda Wortmann B, "Choice of Law by Arbitrators: The Applicable Conflict of Laws System" (1998) 14 *Arbitration International* 97.

128 *Report of Working Group III (Investor-State Dispute Settlement Reform) on the work of its thirty-fifth session (New York, 23–27 April 2018)* (A/CN.9/935, 14 May 2018) at para 24.

129 Claire Morel de Westgaver, "Cybersecurity in International Arbitration: Don't Be the Weakest Link" *Kluwer Arbitration Blog* (15 February 2019) <http://arbitrationblog.

(cont'd on the next page)

who has been using Gmail for many years, and does not wish to incur the additional costs of purchasing secured email services, or the increased inconvenience of using such services may be more inclined to decide that the use of secured email services is not necessary. At minimum, there may be an appearance of the arbitrator taking into account his or her own interests in making the decision.[130] This affects the legitimacy of the procedure and the integrity of the arbitral process.[131]

IV. The way forward

50 In proposing solutions to the challenges faced, this article will focus primarily on arbitral institutions. This is because institutions are the best placed to institute reforms in international arbitration.[132] According to the WCQM Report, "a clear majority of respondents (80%) indicated that 'arbitral institutions' are best placed to make an impact on the future evolution of international arbitration".[133] Through the amendment of rules, updating of practice guidelines, and revision of practices, institutions are able to quickly effect change and introduce new and innovative procedures to improve the arbitral process.[134] The permanent nature of arbitral institutions also allows them to create lasting reforms to the

kluwerarbitration.com/2019/02/15/cybersecurity-in-international-arbitration-dont-be-the-weakest-link/> (accessed 9 February 2020).

130 Simon Greenberg, Christopher Kee & J Romesh Weeramantry, *International Commercial Arbitration: An Asian Perspective* (Cambridge University Press 2011) at para 6.108; *OPIC Karimum Corp v Bolivarian Republic of Venezuela*, ICSID Case No ARB/10/14, Award (5 May 2011) at para 68; *Report of Working Group III (Investor-State Dispute Settlement Reform) on the work of its thirty-fifth session (New York, 23–27 April 2018)* (A/CN.9/935, 14 May 2018) at para 61.

131 Anthea Roberts & Zeineb Bouraoui, "UNCITRAL and ISDS Reforms: Concerns about Arbitral Appointments, Incentives and Legitimacy" *EJIL: Talk!* (6 June 2018) <https://www.ejiltalk.org/uncitral-and-isds-reforms-concerns-about-arbitral-appointments-incentives-and-legitimacy/> (accessed 9 February 2020); Nathalie Bernasconi-Osterwalder, Lise Johnson & Fiona Marshall, *Arbitrator Independence and Impartiality: Examining the Dual Role of Arbitrator and Counsel* (IV Annual Forum for Developing Country Investment Negotiators Background Papers, New Delhi, 27–29 October 2010).

132 Claire Morel de Westgaver, "Cybersecurity in International Arbitration – A Necessity and an Opportunity for Arbitral Institutions" *Kluwer Arbitration Blog* (6 October 2017) <http://arbitrationblog.kluwerarbitration.com/2017/10/06/cyber-security/> (accessed 9 February 2020).

133 Paul Friedland & Stavros Brekoulakis, *2018 International Arbitration Survey: The Evolution of International Arbitration* (White & Case LLP & Queen Mary University of London, 2018) at p 3.

134 Michelle Grando, "Challenges to the Legitimacy of International Arbitration: A Report from the 29th Annual ITA Workshop" *Kluwer Arbitration Blog* (19 September 2017) <http://arbitrationblog.kluwerarbitration.com/2017/09/19/challenges-legitimacy-international-arbitration-report-29th-annual-ita-workshop/> (accessed 9 February 2020).

overall system of international arbitration, something which individual arbitrators find difficult to achieve.[135] As Michelle Grando writes:[136]

> Arbitral institutions have revised their rules and practices to increase the efficiency and fairness of the arbitral process. These include the LCIA in 2014, the ICC in 2015 and 2017, the ICDR in 2014, and SIAC in 2016. ICSID is currently in the process of amending its Arbitration Rules for the fifth time. Professional associations such as the International Bar Association have revised and adopted guidelines addressing relevant subjects such as conflicts of interest and counsel conduct. All this activity shows the vibrancy of international arbitration. As long as the arbitral community does not become deaf to relevant criticisms, international arbitration will not become irrelevant. It will continue to be a legitimate – and the most effective – way of resolving international disputes.

51 From the perspective of the arbitral institutions, it is in their best interests to innovate. Doing so provides an opportunity for the institutions to advocate for institutional arbitration (as opposed to *ad hoc* arbitration) and to differentiate themselves by attracting cyber-conscious users.[137] This is likely to be highly marketable. The BCLP Survey reported that 90% of respondents thought that cybersecurity is an important issue in international arbitration.[138] A further 70% of respondents felt that support from within an institution's secretariat would be useful to improve cybersecurity.[139] 68% of respondents said that they would be more likely to use the arbitration rules of an institution that was able to provide advice and assistance on appropriate data security measures.[140] As arbitration users become increasingly conscious of cybersecurity

135 Claire Morel de Westgaver, "Cybersecurity in International Arbitration – A Necessity and an Opportunity for Arbitral Institutions" *Kluwer Arbitration Blog* (6 October 2017) <http://arbitrationblog.kluwerarbitration.com/2017/10/06/cyber-security/> (accessed 9 February 2020).

136 Michelle Grando, "Challenges to the Legitimacy of International Arbitration: A Report from the 29th Annual ITA Workshop" *Kluwer Arbitration Blog* (19 September 2017) <http://arbitrationblog.kluwerarbitration.com/2017/09/19/challenges-legitimacy-international-arbitration-report-29th-annual-ita-workshop/> (accessed 9 February 2020).

137 Claire Morel de Westgaver, "Cybersecurity in International Arbitration – A Necessity and an Opportunity for Arbitral Institutions" *Kluwer Arbitration Blog* (6 October 2017) <http://arbitrationblog.kluwerarbitration.com/2017/10/06/cyber-security/> (accessed 9 February 2020).

138 George Burn *et al*, *International Arbitration Survey: Cybersecurity in International Arbitration – Don't be the Weakest Link* (Bryan Cave Leighton Paisner LLP, 6 February 2019) <https://www.bclplaw.com/a/web/160089/3WJsPc/bryan-cave-leighton-paisner-arbitration-survey-report-2018p.pdf> (accessed 9 February 2020).

139 George Burn *et al*, *International Arbitration Survey: Cybersecurity in International Arbitration – Don't be the Weakest Link* (Bryan Cave Leighton Paisner LLP, 6 February 2019) <https://www.bclplaw.com/a/web/160089/3WJsPc/bryan-cave-leighton-paisner-arbitration-survey-report-2018p.pdf> (accessed 9 February 2020).

140 George Burn *et al*, *International Arbitration Survey: Cybersecurity in International Arbitration – Don't be the Weakest Link* (Bryan Cave Leighton Paisner LLP,

(cont'd on the next page)

concerns, institutions which are able to show that they are at the forefront of cybersecurity will likely stand out from the increasingly fierce competition.[141]

52 When asked about increased costs, 47% of respondents indicated that, where appropriate, their clients would be willing to pay a higher fee or incur an additional cost to arbitrate under an arbitral institution which provided advice and assistance on appropriate security measures and/or provided a secure platform (or similar) on which all communications and data sharing storage in the arbitration could take place.[142] This suggests that users recognise that there is a cost aspect to cybersecurity and that the pressing need for structural solutions to be put in place may justify the associated increase in cost.[143]

53 It should also be appreciated that parties are generally less sensitive to institutional fees since they typically constitute a small proportion of the overall legal fees – counsel fees generally take the lion's share.[144] In a study conducted by the ICC, the "arbitration costs", which include the arbitrators' fees and the administrative charges of the arbitral institution, and the "party costs", which include legal costs and other expenses incurred by a party for the arbitration, the latter category was found to account for more than 80% of the total costs of the arbitration.[145] Some practitioners have also noted that there may also be a reduction in legal fees if cybersecurity matters are quickly and efficiently dealt with by the arbitral institution.[146] Clear institutional rules or guidelines on cybersecurity may result in lawyers spending less time fighting over cybersecurity issues.

---

6 February 2019) <https://www.bclplaw.com/a/web/160089/3WJsPc/bryan-cave-leighton-paisner-arbitration-survey-report-2018p.pdf> (accessed 9 February 2020).

141 Claire Morel de Westgaver, "Cybersecurity in International Arbitration – A Necessity and an Opportunity for Arbitral Institutions" *Kluwer Arbitration Blog* (6 October 2017) <http://arbitrationblog.kluwerarbitration.com/2017/10/06/cyber-security/> (accessed 9 February 2020).

142 George Burn *et al*, *International Arbitration Survey: Cybersecurity in International Arbitration – Don't be the Weakest Link* (Bryan Cave Leighton Paisner LLP, 6 February 2019) <https://www.bclplaw.com/a/web/160089/3WJsPc/bryan-cave-leighton-paisner-arbitration-survey-report-2018p.pdf> (accessed 9 February 2020).

143 George Burn *et al*, *International Arbitration Survey: Cybersecurity in International Arbitration – Don't be the Weakest Link* (Bryan Cave Leighton Paisner LLP, 6 February 2019) <https://www.bclplaw.com/a/web/160089/3WJsPc/bryan-cave-leighton-paisner-arbitration-survey-report-2018p.pdf> (accessed 9 February 2020).

144 Micha Bühler, "Costs" *Global Arbitration Review* (29 November 2018) <https://web.archive.org/web/20200923222518/https://globalarbitrationreview.com/chapter/1177437/costs> (accessed 7 June 2022).

145 *Decisions on Costs in International Arbitration* (International Chamber of Commerce, 2015).

146 Live interviews with various reputable members of the arbitration community.

54 Notably, the 2020 Protocol envisioned that "as general awareness of the importance of cybersecurity to the arbitral process increases, arbitral institutions and others will introduce new initiatives aimed at improving information security in arbitration, some of which may supplement the Protocol".[147] Commentators have also predicted that "arbitral institutions likely will further address this issue in their own infrastructure, internal procedures, arbitral rules and the training of arbitrators they appoint".[148] Indeed, the author knows of at least one leading institution which has been actively working with cybersecurity experts, in view of developing new capacity to safeguard cybersecurity in international arbitration.[149] It is therefore safe to say that much more can – and should – be done by institutions.

A. Allow issues of cybersecurity to be dealt with by arbitral institutions

55 Perhaps the simplest solution to the above-mentioned challenges would be to allow the institutions to deal with matters of cybersecurity as a matter of administration, instead of having arbitrators deal with the issue as a matter of procedure in the first procedural order. At this juncture, this article notes that existing scholarship is presently divided on whether cybersecurity is a matter of procedure or administration.[150] It is unclear whether cybersecurity is a procedural matter falling within the scope of the tribunal's responsibilities, or an administrative matter to be dealt with by the arbitral institution. Public opinion is also divided: in the BCLP Survey, slightly more than half of the respondents, just 52%, thought that it was a procedural matter, while 42% thought that it was an administrative matter for the institution.[151]

147 *Protocol Consultation Process* (ICCA–NYC Bar–CPR Working Group on Cybersecurity in International Arbitration, November 2019) <https://www.arbitration-icca.org/media/14/44059883674056/protocol_consultation_process.pdf> (accessed 9 February 2020).

148 Julie Bédard, Lea Haber Kuck & Timothy G Nelson, "Skadden's 2019 Insights: International Arbitration Community Turns Its Focus to Cybersecurity" *JDSUPRA* (25 January 2019) <https://www.jdsupra.com/legalnews/skadden-s-2019-insights-international-88611/> (accessed 9 February 2020).

149 The institution is, at the time of writing, currently working with leading cybersecurity consultants.

150 Carol Mulcahy, "Cybersecurity in International Arbitration: Don't Be the Weakest Link" *Thomson Reuters Practical Law Arbitration Blog* (7 February 2019) <http://arbitrationblog.practicallaw.com/cybersecurity-in-international-arbitration-dont-be-the-weakest-link/> (accessed 9 February 2020).

151 George Burn *et al*, *International Arbitration Survey: Cybersecurity in International Arbitration – Don't be the Weakest Link* (Bryan Cave Leighton Paisner LLP, 6 February 2019) <https://www.bclplaw.com/a/web/160089/3WJsPc/bryan-cave-

(cont'd on the next page)

56 It is argued that the better view should be that cybersecurity is a matter of administration. The institutions are better placed to deal with such issues as they are more capable of quickly developing capacity in this field. They are able to hire specialised information technology experts and cybersecurity lawyers, unlike arbitrators who may have to appoint *amicus curiae* on an *ad hoc* basis. It would also be unreasonable to expect tribunals to re-train, learn and become cybersecurity experts overnight, especially since this is an area which requires a tremendous amount of technical expertise.[152] Giving arbitrators the power to impose cybersecurity measures may not sit well with the background and training of all arbitrators, and the nature of their main function.[153] This article notes that from the author's preliminary survey, 75% of respondents thought that arbitrators were not the best placed to deal with issues of cybersecurity.[154] Among the main reasons cited was that arbitral institutions were better placed to deal with such issues.[155]

57 Furthermore, such a system would eliminate the conflicting situation whereby an arbitrator has to decide on measures applicable to himself or herself.[156] Institutions can more easily address the issue of communications between parties and tribunal, between tribunal members, and between institution and tribunal.[157]

58 Moreover, institutions are able to approach cybersecurity matters in a more systemic manner.[158] They are able to better implement a risk-

leighton-paisner-arbitration-survey-report-2018p.pdf> (accessed 9 February 2020); a small number of respondents chose "I don't know".

152 In the course of the survey conducted by this author, many arbitrators provided feedback stating that they felt incapable of gaining the requisite expertise required to decide on issues of cybersecurity.

153 Claire Morel de Westgaver, "Cybersecurity in International Arbitration: Don't Be the Weakest Link" *Kluwer Arbitration Blog* (15 February 2019) <http://arbitrationblog.kluwerarbitration.com/2019/02/15/cybersecurity-in-international-arbitration-dont-be-the-weakest-link/> (accessed 9 February 2020).

154 See n 30 for the composition of the respondents of the survey.

155 One arbitrator also argued that allowing the institution to deal with such matters would allow the tribunals to focus on the substantive matters of the case before them.

156 Claire Morel de Westgaver, "Cybersecurity in International Arbitration: Don't Be the Weakest Link" *Kluwer Arbitration Blog* (15 February 2019) <http://arbitrationblog.kluwerarbitration.com/2019/02/15/cybersecurity-in-international-arbitration-dont-be-the-weakest-link/> (accessed 9 February 2020).

157 George Burn *et al*, *International Arbitration Survey: Cybersecurity in International Arbitration – Don't be the Weakest Link* (Bryan Cave Leighton Paisner LLP, 6 February 2019) <https://www.bclplaw.com/a/web/160089/3WJsPc/bryan-cave-leighton-paisner-arbitration-survey-report-2018p.pdf> (accessed 9 February 2020).

158 George Burn *et al*, *International Arbitration Survey: Cybersecurity in International Arbitration – Don't be the Weakest Link* (Bryan Cave Leighton Paisner LLP, 6 February 2019) <https://www.bclplaw.com/a/web/160089/3WJsPc/bryan-cave-leighton-paisner-arbitration-survey-report-2018p.pdf> (accessed 9 February 2020).

based approach because they can look across a larger number of different cases and apply cyber measures in each individual case in a consistent manner.[159] On the other hand, arbitrators sit on individual cases, and are often unable to view the entire system of international arbitration from a vantage point. Depending on their level of interest and the information technology environment in which they operate, individual arbitrators may take very different approaches to cybersecurity.[160] Consistency is unlikely to be achieved through a risk-based approach whereby risks are assessed and measures are decided by parties and tribunals on a case-by-case basis.[161]

59 In the interests of clarity, institutions may wish to consider amending their rules to presume that the parties agree for issues of cybersecurity to be dealt with by the institution. Arbitral institutions may also wish to amend their model arbitration clauses to encourage parties to allow the matter to be dealt with by the institution as a matter of administration.

B. Greater involvement of the institution in cybersecurity decisions by the tribunal

60 In the alternative, if cybersecurity is deemed to be a procedural matter for the tribunal to decide, the institution should be more involved in the decision-making process.

(1) Provision of cybersecurity consultants

61 70% of respondents in the BCLP Survey agreed that arbitral institutions should have a staff member within the secretariat experienced in data security measures and able to assist the parties and tribunal in deciding on appropriate security measures.[162] Therefore, arbitral institutions should provide, as part of the secretariat, cybersecurity

159 Mauricio Duarte, "Essential Tips on Cybersecurity for Arbitrators: Identify, Protect, Detect, Respond and Recover" *Medium* (6 February 2019) <https://medium.com/@mauricioduarte_20367/essential-tips-on-cybersecurity-for-arbitrators-identify-protect-detect-respond-and-recover-f889f50d71d3> (accessed 9 February 2020).

160 Claire Morel de Westgaver, "Cybersecurity in International Arbitration: Don't Be the Weakest Link" *Kluwer Arbitration Blog* (15 February 2019) <http://arbitrationblog.kluwerarbitration.com/2019/02/15/cybersecurity-in-international-arbitration-dont-be-the-weakest-link/> (accessed 9 February 2020).

161 Claire Morel de Westgaver, "Cybersecurity in International Arbitration: Don't Be the Weakest Link" *Kluwer Arbitration Blog* (15 February 2019) <http://arbitrationblog.kluwerarbitration.com/2019/02/15/cybersecurity-in-international-arbitration-dont-be-the-weakest-link/> (accessed 9 February 2020).

162 George Burn *et al*, *International Arbitration Survey: Cybersecurity in International Arbitration – Don't be the Weakest Link* (Bryan Cave Leighton Paisner LLP, *(cont'd on the next page)*

consultants who are able to recommend the appropriate cybersecurity measures for tribunals to adopt.

62 Perhaps it can be said that such a system is neither groundbreaking nor revolutionary. Arbitral institutions already scrutinise awards and provide recommendations to the tribunal.[163] Alternatively, these consultants may be appointed as expert witnesses, to provide advice to the tribunal on the appropriate cybersecurity measures to adopt. It may also be useful to allow the consultant to act independently of the tribunal as a resource available to the parties in discussions on the topic.[164]

(2) Issuing of practice directions or guidance notes

63 Institutions may also consider issuing practice directions or guidance notes providing greater clarity on what cybersecurity measures may ordinarily be reasonable. Such directions or guidelines will encourage consistent "best practices".[165] Based on the institution's experience in administering different cases, the secretariat may provide clear examples or scenarios on what they deem to be appropriate in the circumstances. This will provide tribunals with better guidance when fashioning cybersecurity measures, allowing there to be greater consistency between cases.[166] This will enable tribunals to better tackle cybersecurity concerns in a more predictable manner, rather than having to fashion measures out of thin air or a laundry list of possible measures (as provided in

6 February 2019) <https://www.bclplaw.com/a/web/160089/3WJsPc/bryan-cave-leighton-paisner-arbitration-survey-report-2018p.pdf> (accessed 9 February 2020).

163 Prakash Pillai & Umer Chaudhry, "The Singapore Approach to Scrutiny of Arbitral Awards" *Kluwer Arbitration Blog* (24 December 2014) <http://arbitrationblog.kluwerarbitration.com/2014/12/24/the-singapore-approach-to-scrutiny-of-arbitral-awards/> (accessed 9 February 2020).

164 See George Burn *et al*, *International Arbitration Survey: Cybersecurity in International Arbitration – Don't be the Weakest Link* (Bryan Cave Leighton Paisner LLP, 6 February 2019) <https://www.bclplaw.com/a/web/160089/3WJsPc/bryan-cave-leighton-paisner-arbitration-survey-report-2018p.pdf> (accessed 9 February 2020). 68% of respondents said that they would be more likely to use the arbitration rules of an institution that was able to provide advice or assistance on appropriate data security measures.

165 George Burn *et al*, *International Arbitration Survey: Cybersecurity in International Arbitration – Don't be the Weakest Link* (Bryan Cave Leighton Paisner LLP, 6 February 2019) <https://www.bclplaw.com/a/web/160089/3WJsPc/bryan-cave-leighton-paisner-arbitration-survey-report-2018p.pdf> (accessed 9 February 2020).

166 George Burn *et al*, *International Arbitration Survey: Cybersecurity in International Arbitration – Don't be the Weakest Link* (Bryan Cave Leighton Paisner LLP, 6 February 2019) <https://www.bclplaw.com/a/web/160089/3WJsPc/bryan-cave-leighton-paisner-arbitration-survey-report-2018p.pdf> (accessed 9 February 2020).

the 2020 Protocol), with little guidance as to which measure would be appropriate in which situation.[167]

64 For example, the practice directions may state that in ordinary circumstances, it would be reasonable to require parties to use a secured file sharing service to exchange all pleadings and documents; no documents should be sent via email attachments. However, in a case where personal data, trade secrets, classified government information, or other sensitive information are involved, it may be necessary to require that such files are to be transferred through a specialised secured file transfer service with end-to-end encryption.

65 Another useful example may be that: in ordinary circumstances, it would be reasonable to require all documents relating to the arbitration be destroyed 90 days after the final award is rendered, unless these are necessary for the purposes of pending setting aside proceedings, enforcement and recognition proceedings, or are necessary for compliance with any other legal requirements or obligations.[168] Such a guideline is likely to be useful since the most commonly reported form of data breach for law firms is the improper disposal (or the lack of proper disposal) of documents.[169] Data which is no longer needed should be destroyed and not left lying around or in tucked away in a remote corner of a server or data drive.[170]

66 Similar guidelines may also be issued to ensure that information is only shared to witnesses and other third parties to the arbitration on a need-to-know basis.[171] Witnesses who do not require access to all the evidence submitted to the tribunal should only be granted limited access

167 *ICCA–NYC Bar–CPR Protocol on Cybersecurity in International Arbitration (2020 Edition) New York Arbitration Week Special Printing* (International Council for Commercial Arbitration, 2019) Schedule C.

168 The institutions, which are likely to have a wealth of experience, is likely to be better placed than myself to determine the appropriate length of time. This article therefore defers to the arbitral institution's discretion as to the appropriate number of days.

169 Eric Hawley, "Cybersecurity and Disaster Recovery Issues for Law Firms" (2016) 33 *The Computer & Internet Lawyer* 12.

170 Sharon Nelson, John Simek & Michael Maschke, "Technology and Cybersecurity Policies Help Lawyers Manage Technology (Instead of It Managing Them)" (2017) 34 *The Computer & Internet Lawyer* 7 at 22; Rick Weber, "ABA Urges Lawyers to Adopt Encryption, other Cybersecurity Practices in Latest 'Handbook'" *Inside Cybersecurity* (24 October 2017) <https://insidecybersecurity.com/share/7329> (accessed 7 June 2022); *The ABA Cybersecurity Handbook: A Resource for Attorneys, Law Firms and Business Professionals* (ABA Publishing, 2nd Ed, 2017). The ABA Handbook recommends for data retention and destruction plans to be developed.

171 *Cybersecurity Guidelines* (International Bar Association, October 2018).

to the documents relating to the arbitration. This is because fewer access points will make it more difficult for attackers to obtain the data.[172]

(c) Power to issue interim measures

67 Finally, institutions should also consider amending its rules to allow the secretariat or registrar to issue interim measures prior to the constitution of the tribunal. Under the framework set out in the 2020 Protocol, "[i]nformation security should be raised as early as practicable in the arbitration, which ordinarily will not be later than the first case management conference".[173] However, there may be a lapse of time between the initial statement of claim, the constitution of the arbitral tribunal and the first procedural conference.[174] In the interim phase, there is a danger that communications, pleadings and other documents exchanged may be hacked. In some arbitrations, the existence of the arbitration itself may also be highly confidential.[175]

68 In this author's preliminary surveys, 77.5% of respondents thought that institutions should be allowed to issue preliminary or temporary cybersecurity measures or orders prior to the constitution of the tribunal (which would subsequently be subject to review by the arbitral tribunal).[176] However, this article notes that some members of the arbitration community have raised concerns that institutions may not be properly equipped to make such orders. To this, this article argues that where capacity must be obtained, it would be easier for the institution, rather than the arbitrators, to develop capacity.[177]

---

172 Steven Chabinsky, "Limiting Access Is the First Step to Securing Networks" *Security* (1 February 2016) <https://www.securitymagazine.com/articles/86886-limiting-access-is-the-first-step-to-securing-networks> (accessed 9 February 2020).

173 *ICCA–NYC Bar–CPR Protocol on Cybersecurity in International Arbitration (2020 Edition) New York Arbitration Week Special Printing* (International Council for Commercial Arbitration, 2019) Principle 10; see also "Cybersecurity Protocol Will Raise Awareness of Data Protection in Arbitration, Says Expert" *Pinsent Masons* (26 November 2019) <https://www.pinsentmasons.com/out-law/news/cybersecurity-protocol-will-raise-awareness-of-data-protection-in-arbitration> (accessed 9 February 2020).

174 Commentators have noted that other than in cases that are expedited, the establishment of the tribunal typically takes at least two months from the submission of the notice of request for arbitration. See "Establishment and Organisation of an Arbitral Tribunal" in Nigel Blackaby *et al*, *Redfern and Hunter on International Arbitration* (Oxford University Press, 6th Ed, 2015) at p 230.

175 Jim Pastore, "Practical Approaches to Cybersecurity in Arbitration" (2017) 40 *Fordham International Law Journal* 1023.

176 See n 30 for the composition of the respondents of the survey.

177 One reputable arbitrator and counsel also noted that such orders may face enforcement problems under the New York Convention since these are not issued by an arbitrator, but rather the institution. Indeed, this is a legitimate flaw of such

(cont'd on the next page)

69 A few reputable arbitrators also opined that institutions should apply such measures with appropriate restraint and inform the arbitral tribunal as early as possible after its constitution. This author cannot help but agree. With guidelines and directions in place to guide the tribunals as well as cybersecurity consultants to advise the tribunal and parties, the role of the institution here would simply be to safeguard cybersecurity interests in the interim phase. The tribunal, once constituted, has the final say on the matter, and the institution only serves to preserve the integrity of the arbitral process.[178]

70 Therefore, the power to order interim measures should only be exercised in appropriate circumstances where a failure to do so may result in a real risk of injury or harm to the parties. Orders should be issued judiciously. One possible example which may require intervention is where the parties had agreed to arbitration itself being confidential, and there is a risk of serious irreparable harm caused to one party if the existence of the arbitration is made known to the public.

C. Amendment of institutional rules to mandate minimum cybersecurity standards applicable to all arbitrations

71 Whilst the nature and potential consequences of cybersecurity risks may vary from one case to another, there are certain cybersecurity risks that will arise in virtually every international arbitration.[179] Certain basic cybersecurity standards may be so fundamental that they would severely affect the legitimacy of international arbitration if a breach

a system. However, we must not overlook the fact that non-compliance with the institution's orders may result in sanctions imposed by the tribunal when allocating costs or calculating damages. Non-compliance may also result in the tribunal being less receptive towards the party's position. In practice, preliminary orders are generally complied with by the parties, since failing to do so could be detrimental to one's case at a later stage of the arbitration.

178 A similar analogy can be drawn from the Singapore International Arbitration Centre's ("SIAC") approach on joinder and consolidation, although in a slightly different context. Under the *Arbitration Rules of the Singapore International Arbitration Centre* (6th Ed, 1 August 2016) ("SIAC Rules") Rule 7.4, consolidation is part of the institution's administrative powers, and the institution makes the preliminary decision. The tribunal, however, gets the final say on matter by deciding on jurisdiction. See also John Choong, Mark Mangan & Nicholas Lingard, *A Guide to the SIAC Arbitration Rules* (Oxford University Press, 2nd Ed, 2018). Another analogy can be drawn from the Emergency Arbitration Procedure adopted by the SIAC, International Chamber of Commerce and the London Court of International Arbitration.

179 Claire Morel de Westgaver, "Cybersecurity in International Arbitration: Don't Be the Weakest Link" *Kluwer Arbitration Blog* (15 February 2019) <http://arbitrationblog.kluwerarbitration.com/2019/02/15/cybersecurity-in-international-arbitration-dont-be-the-weakest-link/> (accessed 9 February 2020).

occurred due to such complete ignorance for the risks involved. Notably, the implementation of such minimum standards was discussed during the consultation process of the 2020 Protocol.[180]

72 It may therefore be prudent for institutions to mandate a minimum standard for all arbitrations.[181] The adoption of mandatory measures addressing baseline risks may also raise the overall level of cybersecurity in international arbitration.[182]

73 In the preliminary surveys conducted, 87.5% of respondents thought that there should be a minimum level of cybersecurity measures applicable to all arbitrations.[183] Among the commonly cited reasons were the need to protect confidentiality, adapt to modern risks, and to protect information handled in the arbitration.

(1) Use of secured email accounts

74 One possible baseline measure is to require all counsel and arbitrators to utilise secured email accounts in the course of the arbitration. In this regard, free webmail services such as Gmail or Yahoo should not be used.[184] The use of such accounts raises serious questions of data security and integrity.[185]

75 As fundamental as it may seem, many arbitrators continue to utilise such email accounts. As one commentator notes, "arbitrators continue to use conventional web-based email services such as Gmail or Yahoo even in sensitive multimillion arbitrations, counsel continue to communicate by means of unencrypted email and even the parties

180 *Protocol Consultation Process* (ICCA–NYC Bar–CPR Working Group on Cybersecurity in International Arbitration, November 2019) <https://www.arbitration-icca.org/media/14/44059883674056/protocol_consultation_process.pdf> (accessed 9 February 2020).

181 To ensure arbitrator compliance with these standards, it may be necessary to require arbitrators to agree to these standards in their engagement letters.

182 Claire Morel de Westgaver, "Cybersecurity in International Arbitration: Don't Be the Weakest Link" *Kluwer Arbitration Blog* (15 February 2019) <http://arbitrationblog.kluwerarbitration.com/2019/02/15/cybersecurity-in-international-arbitration-dont-be-the-weakest-link/> (accessed 9 February 2020).

183 See n 30 for the composition of the respondents of the survey.

184 Jim Pastore, "Practical Approaches to Cybersecurity in Arbitration" (2017) 40 *Fordham International Law Journal* 1023.

185 *Cybersecurity Guidelines* (International Bar Association, October 2018) at p 7; Kate O'Flaherty, "New Warning Reveals Gmail's Major Privacy Problem" *Forbes* (27 June 2019) <https://www.forbes.com/sites/kateoflahertyuk/2019/06/27/new-warning-reveals-gmails-major-privacy-problem/> (accessed 9 February 2020).

seem not to care much about this".[186] The author knows of one case where counsel led by a reputable global law firm challenged (unsuccessfully) an arbitrator's use of his Gmail account for correspondence relating to the arbitration.

76 In practice, it is often independent arbitrators who utilise webmail accounts since lawyers typically have email services provided by their respective law firms or chambers. It would therefore be problematic to require arbitrators to decide this matter since the inconvenience caused by ruling out free webmail accounts would primarily be borne by the arbitrators themselves. Therefore, a mandatory rule imposed by the institution may be required to ensure that all counsel and arbitrators to the arbitral proceedings only utilise secured email accounts for correspondence.

77 In the course of these preliminary surveys, one reputable arbitrator also commented that "the courts in Italy use certificate secure mail for communications and so should the arbitral institutions". Perhaps the institutions may wish to consider providing such services for arbitrators who do not have secured email accounts. For Singapore, which already provides a host of services through Maxwell Chambers Suites including "Virtual Tenancy" options for international law firms and institutions, providing secured email services may not be a tall order.[187]

(2) Use of secured file sharing services

78 Institutions may also wish to amend their rules to mandate the use of secured file sharing services for documents exchanged in an arbitration. The use of free cloud computing services such as Dropbox, Google Drive, and Baidu should not be utilised because they fall short of basic information security standards.[188] Any cloud computing services used in an arbitration should meet certain baseline cybersecurity guidelines.[189]

79 Notably, awareness for this need is not lacking. According to the results of the BCLP Survey, 83% of respondents thought that it is

186 "Cybersecurity Protocol Will Raise Awareness of Data Protection in Arbitration, Says Expert" *Pinsent Masons* (26 November 2019) <https://www.pinsentmasons.com/out-law/news/cybersecurity-protocol-will-raise-awareness-of-data-protection-in-arbitration> (accessed 9 February 2020).

187 "Maxwell Chambers Suites" *Maxwell Chambers* <https://www.maxwellchambers.com/maxwell-chambers-suites/> (accessed 9 February 2020).

188 Stephanie Kimbro & Tom Mighell, "Popular Cloud Computing Services for Lawyers: Practice Management Online" (2011) 37 *Law Practice Magazine* 5.

189 *Cybersecurity Guidelines* (International Bar Association, October 2018) at p 9.

desirable for electronic documents to be transferred by means of a secure shared portal.[190] Unfortunately, only 53% had seen the measure adopted in practice.

80 In determining whether a cloud computing service is adequately secure, regard may also be given to the type of encryption used by the service provider.[191] By many accounts, the use of encryption is a "no-brainer".[192] Strong encryption has not been broken, even by the National Security Agency or Central Intelligence Agency. Services which utilise encryption at rest, and end-to-end encryption for data transfer may be more desirable.[193] This means that the data has to be encrypted both in transit and at rest. Most importantly, the user should be the one who holds the decryption key. In the case of iCloud, Dropbox, OneDrive, Box, and Google Drive, the terms of service make it clear that these providers have master decryption keys.[194]

81 To facilitate this process, arbitral institutions may also wish to consider providing secured file sharing services themselves and mandate the use of their services. The BCLP Survey reported that 62% of respondents thought that compulsory use of a secure platform hosted by the institution would be useful.[195] 52% of respondents also said that arbitration institutions should make compulsory the use of a secure platform hosted by the institution on which all communications and data sharing or storage would take place.[196] It would not be difficult for

190 George Burn *et al*, *International Arbitration Survey: Cybersecurity in International Arbitration – Don't be the Weakest Link* (Bryan Cave Leighton Paisner LLP, 6 February 2019) <https://www.bclplaw.com/a/web/160089/3WJsPc/bryan-cave-leighton-paisner-arbitration-survey-report-2018p.pdf> (accessed 9 February 2020).

191 Vincent I Polley, "Cybersecurity for Lawyers and Law Firms" (2014) 53 *American Bar Association* 4.

192 Sharon Nelson, John Simek & Michael Maschke, "Technology and Cybersecurity Policies Help Lawyers Manage Technology (Instead of It Managing Them)" (2017) 34 *The Computer & Internet Lawyer* 7.

193 Jim Pastore, "Practical Approaches to Cybersecurity in Arbitration" (2017) 40 *Fordham International Law Journal* 1023; such encryption is also recommended by *The ABA Cybersecurity Handbook: A Resource for Attorneys, Law Firms and Business Professionals* (ABA Publishing, 2nd Ed, 2017)

194 For the utility and need for encryption of data, see Rick Weber, "ABA Urges Lawyers to Adopt Encryption, other Cybersecurity Practices in Latest 'Handbook'" *Inside Cybersecurity* (24 October 2017) <https://insidecybersecurity.com/share/7329> (accessed 7 June 2022).

195 George Burn *et al*, *International Arbitration Survey: Cybersecurity in International Arbitration – Don't be the Weakest Link* (Bryan Cave Leighton Paisner LLP, 6 February 2019) <https://www.bclplaw.com/a/web/160089/3WJsPc/bryan-cave-leighton-paisner-arbitration-survey-report-2018p.pdf> (accessed 9 February 2020).

196 George Burn *et al*, *International Arbitration Survey: Cybersecurity in International Arbitration – Don't be the Weakest Link* (Bryan Cave Leighton Paisner LLP,

(cont'd on the next page)

arbitral institutions to provide such services.[197] The legal industry has already been actively working with cybersecurity firms over secured cloud computing services.[198]

82 Some commentators have also recommended for institutions to introduce mandatory filing and communication systems under which data would be transmitted exclusively through a secured platform. Such tools are already available on the market and are often used by parties and tribunals, albeit on an *ad hoc* basis.[199]

V. Conclusion

83 In today's digital age, the world's most valuable resource is no longer oil, but data.[200] Just as steel fences and armed guards are commonly placed around precious oil rigs and other extraction facilities, the same must be done for data, the new oil.[201] Reasonable safeguards must be employed to protect valuable assets.

84 As this article has shown, the level of cybersecurity measures appropriate to each case varies and there is no one-size-fits-all solution. Nuanced solutions are required. In this area, the arbitral institutions are once again given an opportunity to prove their worth to the international community. As it currently stands, few – if any – arbitral institutions have made any serious effort to implement cybersecurity measures. None have taken the first basic step of expressly stating in their institutional rules that

6 February 2019) <https://www.bclplaw.com/a/web/160089/3WJsPc/bryan-cave-leighton-paisner-arbitration-survey-report-2018p.pdf> (accessed 9 February 2020).

197 The author knows of at least one leading arbitral institution which has already been actively engaging with various vendors over the possible implementation of secure cloud computing services for arbitration users.

198 Paul Gupta, "What Is 'Reasonable' Under the ABA's New Cybersecurity Obligations for Law Firms?" *Legal Executive Institute* (12 July 2017) <https://web.archive.org/web/20201022071017/https://www.legalexecutiveinstitute.com/aba-new-cybersecurity-obligations//> (accessed 2 June 2022).

199 Claire Morel de Westgaver, "Cybersecurity in International Arbitration – A Necessity and an Opportunity for Arbitral Institutions" *Kluwer Arbitration Blog* (6 October 2017) <http://arbitrationblog.kluwerarbitration.com/2017/10/06/cyber-security/> (accessed 9 February 2020).

200 "The World's Most Valuable Resource is No Longer Oil, but Data" *The Economist* (19 November 2019) <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data> (accessed 9 February 2020).

201 Kiran Bhageshpur, "Data is the New Oil -- And That's a Good Thing" *Forbes* (15 November 2019) <https://www.forbes.com/sites/forbestechcouncil/2019/11/15/data-is-the-new-oil-and-thats-a-good-thing/> (accessed 9 February 2020).

reasonable cybersecurity measures shall be adopted in the arbitration.[202] The playing field is equal, and the starter pistol has just been fired by the 2020 Protocol.

---

202 Hanna Roos & Jennifer Archie, "Call for Cybersecurity Guidelines in International Arbitration" *Lexology* (24 November 2017) <https://www.lexology.com/library/detail.aspx?g=4caf2e48-f598-46c4-8353-2a150f0295fc> (accessed 9 February 2020).