ISSN : 1875-4120
Issue : Vol. 16, Issue 3
Published : May 2019

This paper is part of the TDM Special Issue on **"Cybersecurity in International Arbitration"** prepared by:

Stephanie Cohen
Independent Arbitrator
View profile

Mark C. Morril
MorrilADR
View profile

Previously published as "A Call to Cyberarms: The International Arbitrator's Duty to Avoid Digital Intrusion", in 40 FORDHAM INTERNATIONAL LAW JOURNAL (981) (2017).

Transnational Dispute Management
www.transnational-dispute-management.com

A Call to Cyberarms: The International Arbitrator's Duty to Avoid Digital Intrusion by Taking Reasonable Cybersecurity Measures
by S. Cohen and M.C. Morril

About TDM

TDM (Transnational Dispute Management): Focusing on recent developments in the area of Investment arbitration and Dispute Management, regulation, treaties, judicial and arbitral cases, voluntary guidelines, tax and contracting.

Visit www.transnational-dispute-management.com
for full Terms & Conditions and subscription rates.

Open to all to read and to contribute

TDM has become the hub of a global professional and academic network. Therefore we invite all those with an interest in Investment arbitration and Dispute Management to contribute. We are looking mainly for short comments on recent developments of broad interest. We would like where possible for such comments to be backed-up by provision of in-depth notes and articles (which we will be published in our 'knowledge bank') and primary legal and regulatory materials.

If you would like to participate in this global network please contact us at info@transnational-dispute-management.com: we are ready to publish relevant and quality contributions with name, photo, and brief biographical description - but we will also accept anonymous ones where there is a good reason. We do not expect contributors to produce long academic articles (though we publish a select number of academic studies either as an advance version or an TDM-focused republication), but rather concise comments from the author's professional 'workshop'.

TDM is linked to **OGEMID**, the principal internet information & discussion forum in the area of oil, gas, energy, mining, infrastructure and investment disputes founded by Professor Thomas Wälde.

A CALL TO CYBERARMS: THE INTERNATIONAL ARBITRATOR'S DUTY TO AVOID DIGITAL INTRUSION BY TAKING REASONABLE CYBERSECURITY MEASURES*

*Stephanie Cohen*** & *Mark Morril****

* **PREVIOUSLY PUBLISHED AS** *A Call to Cyberarms: The International Arbitrator's Duty to Avoid Digital Intrusion*, in 40 FORDHAM INTERNATIONAL LAW JOURNAL (981) (2017). The authors welcome comments addressed to cohen@cohenarbitration.com and mark.morril@morriladr.com.

** Stephanie Cohen is a Canadian arbitrator of international and domestic commercial disputes based in New York City (www.cohenarbitration.com). Prior to establishing her practice as an arbitrator, she was Counsel in the international arbitration group at White & Case LLP.

*** Mark Morril is an independent arbitrator and mediator based in New York City who focuses on complex commercial disputes (www.morriladr.com). Previously, he served as General Counsel of the publisher Simon & Schuster, then the world's largest English language publisher, as Deputy General Counsel of the global media company Viacom and as a law firm partner.

I. INTRODUCTION

International commercial arbitration rests on certain fundamental attributes that cut across the different rule sets and cultural and legal systems in which it operates. There is common ground that any international commercial arbitration regime must encompass integrity and fairness, uphold the legitimate expectations of commercial parties, and respect essential elements of due process such as equal treatment of the parties, a fair opportunity for each party to present its case and neutral adjudicatory proceedings, untainted by illegal conduct.[1]

The system and its integrity depend substantially on the role of the arbitrator. As Professor Rogers has stated: "[T]he authoritative nature of adjudicatory outcomes, as well as their existence within a larger system, imposes on adjudicators an obligation to preserve the integrity and legitimacy of the adjudicatory system in which they operate."[2] Cyberbreaches of the arbitral process, including intrusion

1. *See e.g.,* UNCITRAL MODEL LAW ON INT'L COM. ARB., art. 18 (1985) [hereinafter UNCITRAL Model Law], ("The parties shall be treated with equality and each party shall be given a full opportunity of presenting his case."); Convention on the Recognition and Enforcement of Foreign Arbitral Awards, art. V(1)(b) (1958) (party inability to present case is grounds to refuse recognition and enforcement of an award); ENGLISH ARBITRATION ACT 1, § 33 (1996) (general duty of tribunal); LONDON CT. OF INT'L ARB., LCIA ARBITRATION RULES (2014) [hereinafter LCIA RULES] art. 14.4 (conduct of proceedings); William Park, *Arbitrators and Accuracy*, 1 J. OF INT'L DISP. SETTLEMENT 43, note 89 (2010) (arbitrators rejecting complicity with money laundering, fake arbitrations, and other illicit schemes.); LEADING ARBITRATORS' GUIDE TO INTERNATIONAL ARBITRATION 485 (Lawrence W. Newman & Richard D. Hill eds., 3d ed., 2014); Klaus Peter Berger & J. Ole Jensen, *Due Process Paranoia and the Procedural Judgment Rule: a Safe Harbour for Procedural Management Decisions by International Arbitrators*, 32 (3) ARB. INT'L 415 (2016).

2. CATHERINE ROGERS, ETHICS IN INTERNATIONAL ARBITRATION 283 (2014).

into arbitration-related data and transmissions, pose a direct and serious threat to the integrity and legitimacy of the process.[3] This article posits that the arbitrator, as the presiding actor, has an important, front-line duty to avoid intrusion into the process.

The focus here on cyberintrusion into the arbitral process does not imply that international arbitration is uniquely vulnerable to data breaches, but only that international arbitration proceedings are not immune to increasingly pervasive cyberattacks against corporations, law firms, government agencies and officials and other custodians of large electronic data sets of sensitive information.[4]Similarly, our focus on the role and responsibilities of the arbitrator should not obscure that cybersecurity is a shared responsibility and that other actors have independent obligations.[5] Arbitrators are not uniquely vulnerable to data breaches and are not guarantors of cybersecurity.[6] In the highly interdependent landscape of international commercial arbitration, data associated with any arbitration matter will only be as secure as the weakest link. Since data security ultimately depends on

3. Though we focus primarily on the threat of data breaches, the analysis here is generally applicable to other forms of unauthorized digital intrusion in proceedings, such as surreptitious surveillance of a hearing or of arbitration counsel in their offices, or the inadvertent recording and disclosure of an otherwise private conversation between members of the tribunal.

4. *See infra* Part II.

5. Most notably, counsel have ethical duties to protect client confidentiality and to keep abreast of the risks and benefits of technology related to their practice. Further, all actors in the process may have contractual or regulatory obligations to protect sensitive personal or commercial information. *See* infra Sections III.A and III.C.

6. High profile examples of arbitration-related cyberattacks or data breaches have involved arbitral institutions, counsel, and parties as targets. *See* Zachary Zagger, *Hackers Target Anti-Doping, Appeals Bodies Amid Olympics*, LAW360.COM, (Aug. 12, 2016), https://www.law360.com/articles/827962/hackers-target-anti-doping-appeals-bodies-amid-olympics (reporting that hackers attempted to infiltrate the website of the Court of Arbitration for Sport during the Rio Olympic Games); Alison Ross, *Tribunal Rules on Admissibility of Hacked Kazakh Emails*, GLOBAL ARBITRATION REV., (Sept. 22, 2015), http://globalarbitrationreview.com/article/1034787/tribunal-rules-on-admissibility-of-hacked-kazakh-emails (reporting that privileged e-mails between a government and its arbitration counsel were disclosed by hackers of the government's internal network); Alison Ross, *Cybersecurity and Confidentiality Shocks for PCA*, GLOBAL ARBITRATION REV., (July 23, 2015), http://globalarbitrationreview.com/article/1034637/cybersecurity-and-confidentiality-shocks-for-the-pca (reporting that the Permanent Court of Arbitration website was hacked during a hearing of China-Philippines arbitration and counsel in a Russia-related arbitration received "Trojan downloaders" that, if opened, would have enabled hackers to listen in on conversations).

the responsible conduct and vigilance of individuals, any individual actor can be that weak link, whatever their practice setting, whatever the infrastructure they rely upon, and whatever role they play in an arbitration.[7]

We explore in Part II the threat that cybersecurity breaches pose to international commercial arbitrations, using some examples of high-profile breaches that already have occurred.[8] We analyze in Part III the obligations that underpin the arbitrator's duty to avoid intrusion. That duty, in our view, need not be created anew. Rather, it rests securely on well-established duties of arbitrators to safeguard both the confidentiality and the legitimacy and integrity of proceedings, as well as to be competent to handle each individual matter.[9] In an era of significant cyberthreats to the international commercial arbitration process, the duty to avoid intrusion is an inherent duty that follows as a matter of necessity from these earlier identified duties.

We then discuss, in Part IV, the nature and scope of the arbitrator's duty to avoid intrusion, which is bounded and fulfilled by taking reasonable measures to prevent unauthorized digital access to

---

7. The impact of individual conduct on cybersecurity has been highlighted in recent high profile security breaches. *See*, *e.g.*, Gregory Krieg & Tal Kopan, *Is This the Email That Hacked John Podesta's Account?*, CNN (Oct. 28, 2016), http://www.cnn.com/2016/10/28/politics/phishing-email-hack-john-podesta-hillary-clinton-wikileaks/index.html; Eric Lipton, et al., *The Perfect Weapon: How Russian Cyberpower Invaded the United States*, N.Y. TIMES (Dec. 13, 2016), https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html; Tom Vanden Brook & Michael Winter, *Hackers Penetrated Pentagon E-mail*, USA TODAY (Aug. 7, 2015), http://www.usatoday.com/story/news/nation/2015/08/06/russia-reportedly-hacks-pentagon-email-system/31228625; Tom Fox-Brewster, *Sony Needed to Have Basic Digital Protection. It Failed*, THE GUARDIAN (Dec. 20, 2014), https://www.theguardian.com/commentisfree/2014/dec/21/sony-hacking-north-korea-cyber-security.

8. Although the focus of this article is on international commercial arbitration, many of the considerations discussed here will apply as well in investor-state and public international arbitration. Notably, some of the high profile data security breaches discussed in this article occurred in those contexts. *See supra* note 6. At the same time, however, there may be important differences between the scope of the arbitrator's duty to avoid intrusion in the two regimes owing to the public interest in investor-state arbitration and initiatives to increase transparency in the settlement of investor-state disputes. *See*, *e.g.*, UN Convention on Transparency in Treaty-Based Investor-State Arbitration (2015).

9. *See* William Park, *The Four Musketeers of Arbitral Duty: Neither One-For-All No All-For-One*, 8 ICC DOSSIERS 24 (2011).

arbitration-related information. There is no bright line list of measures that will fulfill the duty. Rather, assessment of the cybersecurity necessary in international commercial arbitration is an ongoing, risk-based process that requires all participating individuals to understand data security threats in context. As threats evolve, participants must know their own digital architecture and security vulnerabilities (including those that arise from their personal day-to-day work habits) in order to implement protective measures responsive to the threats that apply to their data landscape and individual matters.

The specific protective measures required to satisfy the duty will depend on an analysis of the security risks and on the measures that are practically available, as both will undoubtedly evolve from time to time. They will also depend upon considerations of convenience, cost and efficiency, as the arbitrator may need to balance the duty to avoid intrusion against other duties, including the duty to conduct proceedings in an expeditious and cost-effective manner[10] and, in the absence of overriding considerations, consistent with the parties' choices.[11]

Finally, in Part V, we address some practical considerations for arbitrators as they determine what measures to implement to avoid intrusion and, in Part VI, suggest for future dialogue some ways in which all participants in the international commercial arbitration system may collaborate to address the ongoing threats. The

---

10. *See* INT'L CHAMBER OF COMMERCE [ICC], RULES OF ARBITRATION (2017) [hereinafter ICC RULES], art. 22(1) (tribunal shall make every effort to conduct the arbitration in an expeditious and cost-effective manner); INT'L CTR. FOR DISP. RES., INTERNATIONAL CENTRE FOR DISPUTE RESOLUTION INTERNATIONAL ARBITRATION RULES (2014) [hereinafter ICDR RULES], art. 20(2) ("The tribunal shall conduct the proceedings with a view to expediting the resolution of the dispute"); LCIA RULES, *supra* note 1, at art. 14.4(ii) (tribunal's general duty to adopt suitable procedures, avoiding unnecessary delay or expense, so as to provide a fair and efficient means for the final resolution of the parties' dispute).

11. *See*, *e.g.*, UNCITRAL Model Law, *supra* note 1, at art. 34(2)(a)(iv) (award may be set aside if "the arbitral procedure was not in accordance with the parties' agreement, unless such agreement was in conflict with a provision of this Law from which the parties cannot derogate"); LCIA RULES, *supra* note 1, at art. 14.2 ("The parties may agree on joint proposals for the conduct of their arbitration for consideration by the Arbitral Tribunal. They are encouraged to do so in consultation with the Arbitral Tribunal and consistent with the Arbitral Tribunal's general duties . . ."); ICDR RULES, *supra* note 10, at 1 (rules apply "subject to modifications that the parties may adopt in writing" except that "where any rule[] is in conflict with any provision of the law applicable to the arbitration from which the parties cannot derogate, that provision shall prevail").

fundamentals of effective cybersecurity management are accessible and not unduly burdensome. The arbitrator who keeps abreast of risks and benefits of technology in the arbitration process, is conscious of his or her digital assets and infrastructure, and who implements reasonable protective measures, will readily meet the obligation to avoid intrusion.

II. DATA SECURITY THREATS IN INTERNATIONAL ARBITRATION

Cyberintrusion, or hacking as it is more commonly known, is often in the news in respect to geo-politics[12] and major corporate and government records data breaches.[13] Law firms, too, are increasingly

12. See, e.g., U.S. Federal Bureau of Investigation and U.S. Department of Homeland Security, Joint Analysis Report, *GRIZZLY STEPPE-Russian Malicious Cyber Activity*, JAR-16-20296A (2016), https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf (providing technical details regarding the tools and infrastructure used by the Russian civilian and military intelligence services to compromise and exploit networks and endpoints associated with the US election); David E. Sanger & Mark Mazzetti, *U.S. Had Cyberattack Plan if Nuclear Dispute Led to Conflict*, N.Y. TIMES (Feb. 16, 2016), https://www.nytimes.com/2016/02/17/world/middleeast/us-had-cyberattack-planned-if-iran-nuclear-negotiations-failed.html.

13. See, e.g., Vindu Goel and Nicole Perlroth, *Yahoo Says 1 Billion Accounts Were Hacked*, N.Y. TIMES (Dec. 14, 2016), https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html (stating that following a September 2016 disclosure that sensitive personal information associated with 500 million users was stolen in late 2014 in an apparently state-sponsored attack, Yahoo disclosed that a separate 2013 attack compromised more than one billion users.); Kevin McCoy, *Cyber Hack Got Access to Over 700,000 IRS Accounts*, USA TODAY (Feb. 26, 2016), http://www.usatoday.com/story/money/2016/02/26/cyber-hack-gained-access-more-than-700000-irs-accounts/80992822/; James Billington, *Hackers Carry Out $55M Cyber Heist From Boeing Aerospace Parts Manufacturer*, INT'L BUS. TIMES (Jan. 27, 2016), http://www.ibtimes.co.uk/hackers-carry-out-55m-cyber-heist-boeing-aerospace-parts-manufacturer-1540455; Ahiza Garcia, *Target Settles for $39 Million Over Data Breaches,* CNN (Dec. 2, 2015), http://money.cnn.com/2015/12/02/news/companies/target-data-breach-settlement/ (noting that the 2013 hack of Target database compromised roughly forty million customers); Julie Hirschfield Davis, *Hacking of Government Computers Exposed 21.5 Million People,* N.Y. TIMES (July 9, 2015), https://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html; Anna Wilde Mathews, *Anthem: Hacked Database Included 78.8 Million People*, WALL ST. J. (Feb. 24, 2015), http://www.wsj.com/articles/anthem-hacked-database-included-78-8-million-people-1424807364. *See generally* Verizon, 2016 Data Breach Investigations Report [hereinafter Verizon Report], http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/ (last visited Jan. 22, 2017) (analyzing a dataset provided by security service providers, law enforcement, and government agencies of more than 100,000 security incidents in 2015,

reported as having fallen victim to cyberattacks.[14] As awareness increases that corporations and players in the legal sector are attractive targets for cybercriminals, the multiple players involved in international private commercial arbitrations should realize that they too are vulnerable to cybercriminals.[15] International commercial arbitrations routinely involve sensitive commercial and personal information, including information that is not publicly available and that has a potential to move markets or impact competition. Conveniently for hackers, this information is culled together in large data sets, ranging from pleadings and documents produced in disclosure, documentary evidence, witness statements, expert reports, memorials, transcripts, attorney work product, tribunal deliberation materials, and case management data. As the multiple players involved often live in different countries, the information is frequently exchanged and stored in electronic form, making it vulnerable to malevolent outside actors.

Data custodians, who hold sensitive data to varying degrees, include arbitral institutions, counsel, the parties and members of the

---

revealing 3,141 confirmed data breaches in eighty-two countries); PricewaterhouseCoopers, Key Findings from the Global State of Information Security Survey (2017), http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/assets/gsiss-report-cybersecurity-privacy-possibilities.pdf [hereinafter PWC Report]; Sarah Kuranda, *New Federal Budget Proposal Raises Government Security Spending* (Feb. 9, 2016), http://www.crn.com/news/security/300079648/new-federal-budget-proposal-raises-government-security-spending-ups-opportunity-for-vars.htm (referencing hacks of United States Office of Personnel Management records and email accounts of the Director of the CIA and the Secretary of Homeland Security).

14. *See, e.g.,* Nate Raymond, *U.S. Accuses Chinese Citizens of Hacking Law Firms*, INSIDER TRADING (Dec. 28, 2016), http://www.reuters.com/article/us-cyber-insidertrading-idUSKBN14G1D5; Michael Schmidt and Steven Lee Myers, *Panama Law Firm's Leaked Files Detail Offshore Accounts Tied to World Leaders*, N.Y. TIMES (Apr. 3, 2016), https://www.nytimes.com/2016/04/04/us/politics/leaked-documents-offshore-accounts-putin.html (reporting that 11.5 million documents leaked from Panama law firm exposed the offshore accounts of 140 politicians and public officials). *See also* New York State Bar Ass'n Ethics Opinion 1019 (Aug. 2014) ("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.").

15. For an overview of the major cyber risks in the practice of international arbitration and the tradecraft of the principal threat actors (hacktivists, state actors, and criminals), see James Pastore, *Practical Approaches to Cybersecurity in Arbitration*, 40 FORDHAM INT'L L.J. 1023 (2017). *See also* Verizon Report, *supra* note 13.

arbitral tribunal (along with their respective support staff), as well as experts and vendors, including court reporters, translation services, couriers, and information technology ("IT") professionals, among others. Hackers may attack individual actors directly[16] or the digital infrastructure of their organizations.[17] Moreover, each smartphone, tablet, laptop, thumb drive, other digital device, and cloud service used for the transmission or hosting of arbitration-related data offers a potential portal for unauthorized outsiders to gain access.

The participants in international commercial arbitrations are, to a large degree, digitally interdependent, in that the process typically involves the transmission and hosting of data and collaborative elements such as communications relating to the arbitration. Consequently, any break in the custody of sensitive data has the potential to affect all participants. Indeed, since participants will frequently play host not only to their own sensitive data, but also to the sensitive data of others, intrusion into data held by one participant may injure another more than the one whose data security was compromised.

---

16. A prevalent method of attack that capitalizes on human error is ransomware, a form of malware frequently distributed through spear phishing e-mails sent to targeted individuals. The FBI explains:

> [V]ictims—upon seeing an e-mail addressed to them—will open it and may click on an attachment that appears legitimate, like an invoice or an electronic fax, but which actually contains the malicious ransomware code. Or the e-mail might contain a legitimate-looking URL, but when a victim clicks on it, they are directed to a website that infects their computer with malicious software. Once the infection is present, the malware begins encrypting files and folders on local drives, any attached drives, backup drives, and potentially other computers on the same network that the victim computer is attached to. Users and organizations are generally not aware they have been infected until they can no longer access their data or until they begin to see computer messages advising them of the attack and demands for a ransom payment in exchange for a decryption key.

FBI, *Cyber Crime*, https://www.fbi.gov/investigate/cyber (last visited Jan. 16, 2017).

17. In a July 2015 "watering hole" attack, for example, hackers implanted a malicious Adobe Flash file on the Permanent Court of Arbitration's website that allowed them to infect the computer systems of website visitors who had not patched a known Adobe Flash security flaw. Luke Eric Peterson, *Permanent Court of Arbitration Website Goes Offline, with Cyber-Security Firm Contending that Security Flaw was Exploited in Concert with China-Philippines Arbitration,* IA REP. (July 23, 2015), http://www.iareporter.com/articles/permanent-court-of-arbitration-goes-offline-with-cyber-security-firm-contending-that-security-flaw-was-exploited-in-lead-up-to-china-philippines-arbitration.

Unauthorized access of sensitive data may result in the disclosure, or even acceptance into evidence of, illegally obtained, confidential, or privileged matter in ways that undermine fundamental elements of the adjudicatory process and its baseline due process elements.[18] Disclosure of commercially sensitive information, trade secrets, or personal information may violate laws or contractual commitments in business-to-business or customer agreements, cause serious reputational and economic harm to individuals or businesses,[19] trigger regulatory sanctions[20] or negligence claims,[21] and impact the integrity of public securities markets.[22] Further, since the parties, counsel and arbitrators frequently reside in different countries and may be subject to differing data security law, privacy regimes and ethical standards, the legal effect of a data breach may be uncertain and complex.[23] Last, and not least, data security breaches, particularly those resulting from a failure to implement reasonable security protocols, threaten to undermine public confidence in the very

18. *See* Alison Ross, *Tribunal Rules on Admissibility of Hacked Kazakh Emails*, GAR (Sept. 22, 2015) (reporting on unpublished order in Caratube International Oil Co. LLP and Devincci Salah Hourani v. Republic of Kazakhstan, ICSID Case No. ARB/13/13, admitting into evidence certain documents obtained from the public disclosure of documents hacked from Kazakhstan's government computer network, yet excluding other documents on the basis of privilege).

19. *See, e.g.,* Michael Cieply and Brooks Barnes, *Sony Hacking Fallout Includes Unraveling of Relationships in Hollywood*, N.Y. TIMES (Dec. 18, 2014), https://www.nytimes.com/2014/12/19/business/media/sony-attack-is-unraveling-relationships-in-hollywood.html.

20. *See, e.g., FINRA Fines Lincoln Financial Sub $650,000 for Cybersecurity Shortcomings*, NAT'L L. REV. (Nov. 24, 2016), http://www.natlawreview.com/article/finra-fines-lincoln-financial-sub-650000-cybersecurity-shortcomings.

21. *See, e.g.,* Robert Burnson, *Yahoo's Massive Data Breach Draws Negligence Suits by Users*, BLOOMBERG TECH. (Sept. 23, 2016), https://www.bloomberg.com/news/articles/2016-09-23/yahoo-s-massive-data-breach-draws-negligence-lawsuit-by-user; *See also Shore et al. v. Johnson & Bell, Ltd.*, No. 1:16-cv-04363 (Verified Complaint) (N.D. Ill. Apr. 15, 2016) (class action alleging a Chicago law firm was negligent and engaged in malpractice by using security practices that left client information vulnerable to hacking, including, for example, a ten year-old time-entry system that had not been updated with security patches).

22. Nate Raymond, *U.S. Accuses Chinese Citizens of Hacking Law Firms*, INSIDER TRADING (Dec. 28, 2016), http://www.reuters.com/article/us-cyber-insidertrading-idUSKBN14G1D5 (reporting criminal charges for trading on confidential corporate information obtained by hacking into networks and servers of law firms working on mergers).

23. *See Cybersecurity and Arbitration: Protecting Your Documents and Ensuring Confidentiality*, NYSBA INSIDE (2016).

institution of international private commercial arbitration. We explore the latter consequence further below.

III. SOURCES OF THE ARBITRATOR'S DUTY TO AVOID INTRUSION

The arbitration rules, ethical codes, practice guidelines, and national laws that govern international commercial arbitration do not, by and large, establish an express duty for arbitrators or any other participant in the arbitral process to implement cybersecurity measures.[24] Why, then, does the arbitrator bear responsibility to avoid cybersecurity breaches? In our view, the arbitrator's duty to avoid intrusion rests on well-established arbitral duties: (i) the duty to protect the confidentiality and privacy of the proceedings, which will vary in different arbitrations, but exists to some degree in all proceedings; (ii) a fundamental duty to preserve and protect the integrity and legitimacy of the arbitral process; and (iii) a duty to be competent. In addition to these general duties, some arbitrators may have express or implied cybersecurity obligations by virtue of attorney codes of conduct, national data protection laws or regulations, or agreement with the parties.

A. Duty of Confidentiality

It is by now well-established that although parties generally have a right to keep international commercial arbitrations private (i.e., to exclude third parties from hearings),[25] it cannot be assumed that they

24. *See* Section III.C for a discussion of the ethical obligations of lawyers under the ABA Model Rules of Professional Conduct, which regulate attorney conduct.

25. *See* Simon Crookenden, *Who Should Decide Arbitration Confidentiality Issues?* 25 ARB. INT'L 603, 603 (2009) ("The privacy of arbitration proceedings is generally recognised internationally."); *see also, e.g.,* ICC RULES, *supra* note 10, at art. 26(3): (" . . . Save with the approval of the arbitral tribunal and the parties, persons not involved in the proceedings shall not be admitted."); ICDR RULES, *supra* note 10, at art. 23(6) ("Hearings are private unless the parties agree otherwise or the law provides to the contrary."); LCIA RULES, *supra* note 1, at art. 19.4: ("All hearings shall be held in private, unless the parties agree otherwise in writing."); SINGAPORE INT'L ARB. CTR., ARBITRATION RULES OF THE SINGAPORE INTERNATIONAL ARBITRATION CENTRE (2016) [hereinafter SIAC RULES], art. 24.4 ("Unless otherwise agreed by the parties, all meetings and hearings shall be in private, and any

have a general duty or right to keep arbitration-related information confidential (i.e., to refrain from disclosing, and to keep others from disclosing, such information to third parties).[26] Arbitrators are on slightly different footing. Although applicable law,[27] governing arbitration rules,[28] and party agreement may vary in the extent to which they obligate an arbitrator to keep *all* aspects of an arbitration proceeding confidential, it is uncontroversial that the arbitrator has a

---

recordings, transcripts, or documents used in relation to the arbitral proceedings shall remain confidential.").

26. UNCITRAL Notes on Organizing Arbitral Proceedings, ¶ 50 (2016) [hereinafter UNCITRAL Notes] ("there is no uniform approach in domestic laws or arbitration rules regarding the extent to which participants in an arbitration are under a duty to observe the confidentiality of information relating to the arbitral proceedings"); L. Yves Fortier, *The Occasionally Unwarranted Assumption of Confidentiality*, 15 ARB. INT'L 131 (1999); Leon Trakman, *Confidentiality in International Commercial Arbitration*, 18 ARB. INT'L 1 (2002).

27. More often than not, whether an arbitrator has a duty of confidentiality is not addressed by national legislation. *See* BORN, INTERNATIONAL COMMERCIAL ARBITRATION 2003 (Wolters Kluwer, 2d ed. 2014); *see also* Joshua Karton, *A Conflict of Interests: Seeking a Way Forward on Publication of International Arbitral Awards,* 28 ARB. INT'L 447, 450 (2012).

28. Although they differ in scope, most institutional international arbitration rules, with the notable exception of the ICC Rules, impose an express obligation of confidentiality on arbitrators. *See, e.g.,* ICDR RULES, *supra* note 10, at art. 37(1) ("Confidential information disclosed during the arbitration by the parties or by witnesses shall not be divulged by an arbitrator . . . . [T]he members of the arbitral tribunal . . . shall keep confidential all matters relating to the arbitration or the award."); LCIA RULES, *supra* note 1, at art. 30.2 ("The deliberations of the Arbitral Tribunal shall remain confidential to its members . . . ."); SIAC RULES, *supra* note 25, at art. 39.1 ("Unless otherwise agreed by the parties, a party and any arbitrator, including any Emergency Arbitrator . . . shall at all times treat all matters relating to the proceedings and the Award as confidential. The discussions and deliberations of the Tribunal shall be confidential."), art. 39. 3 (". . . matters relating to the proceedings" includes the existence of the proceedings, and the pleadings, evidence and other materials in the arbitral proceedings and all other documents produced by another party in the proceedings or the Award arising from the proceedings, but excludes any matter that is otherwise in the public domain"); JAMS FOUNDATION, JAMS INTERNATIONAL ARBITRATION RULES (2016), art. 17.1 (**"**Unless otherwise required by law, or unless the parties expressly agree, the Tribunal, the Administrator and JAMS International will maintain the confidentiality of the arbitration."), art. 17.2 ("Unless otherwise required by law, an award will remain confidential, unless all of the parties consent to its publication."); INT'L INST. FOR CONFLICT PREVENTION & RES., CPR 2014 RULES FOR ADMINISTERED ARBITRATION OF INTERNATIONAL DISPUTES (2014) [hereinafter CPR RULES], art. 20 ("Unless the parties agree otherwise, the parties, the arbitrators and CPR shall treat the proceedings, any related disclosure and the decisions of the Tribunal, as confidential . . . ."). *But see* ICC RULES, *supra* note 10, at app. I, art. 6 ("The work of the [ICC] Court is of a confidential nature which must be respected by everyone who participates in that work in whatever capacity.").

fundamental duty to keep at least *certain aspects* of a proceeding confidential. Gary Born takes a broad view of the confidentiality obligation, stemming from the arbitrator's adjudicatory role:

> Even where confidentiality obligations are not imposed upon the parties by either their agreement or applicable national law, the arbitrators are subject to separate confidentiality obligations by virtue of their adjudicative function. One element of the arbitrator's role is the duty to maintain the confidentiality of the parties' written and oral submissions, evidence and other materials submitted in the arbitration. It is generally inconsistent with the arbitrator's mandate to disclose materials from the arbitration to third parties.[29]

The *AAA/ABA Code of Ethics for Arbitrators in Commercial Disputes* is consistent with this view. Canon VI provides that "[a]n arbitrator should be faithful to the relationship of trust and confidentiality inherent in that office."[30] In particular, the arbitrator has a duty to "keep confidential all matters relating to the arbitration proceedings and decision" and "[i]n a proceeding in which there is more than one arbitrator, . . . [not to] inform anyone about the substance of the deliberations of the arbitrators."[31] Less comprehensively, the *IBA Rules of Ethics for Arbitrators* specify that the "deliberations of the arbitral tribunal and the contents of the award itself, remain confidential in perpetuity unless the parties release the

29. BORN, *supra* note 27, at 2004.

30. Similarly, the Chartered Institute of Arbitrators Code of Professional and Ethical Conduct for Members (Oct. 2009) provides: "A member shall abide by the relationship of trust which exists between those involved in the dispute and (unless otherwise agreed by all the parties, or permitted or required by applicable law), both during and after completion of the dispute resolution process, shall not disclose or use any confidential information acquired in the course of or for the purposes of the process." CHARTERED INST. OF ARBITRATORS, THE CHARTERED INSTITUTE OF ARBITRATORS CODE OF PROFESSIONAL AND ETHICAL CONDUCT FOR MEMBERS (Oct. 2009) [hereinafter CIARB ETHICS CODE], Rule 8.

31. AAA/ABA CODE OF ETHICS FOR ARBITRATORS IN COMMERCIAL DISPUTES, Canon VI (B), (C). *See also* Canon I (I) ("An arbitrator who withdraws prior to the completion of the arbitration, whether upon the arbitrator's initiative or upon the request of one or more of the parties, should take reasonable steps to protect the interests of the parties in the arbitration, including return of evidentiary materials and protection of confidentiality.").

arbitrators from this obligation."[32] At the same time, however, they encapsulate a general duty of confidentiality by stating that arbitrators should be "discreet."[33]

In contrast to arbitrators, who are thus bound by a duty of confidentiality,[34] the parties themselves may not have a *duty* to keep arbitration proceedings or certain aspects of them confidential. Nonetheless, there is a common *expectation* among users of international commercial arbitration[35] that the overall process will be

32. INT'L BAR ASSOC., IBA RULES OF ETHICS FOR ARBITRATORS, article 9. The IBA Rules of Ethics are not binding, but are deemed to reflect internationally acceptable guidelines developed by practicing lawyers from all continents. *Id*. at Introductory Note.

33. *Id.*

34. We note that while many arbitrators are lawyers and will have professional ethical obligations to preserve client confidentiality, by their terms, such obligations apply only when a lawyer is acting in a representative capacity for a client and not when serving as an arbitrator, who does not represent any party but has equal duties to all. BORN, *supra* note 27 at 1970; CPR-Georgetown Commission on Ethics and Standards in ADR, Proposed New Model Rule of Professional Conduct Rule 4.5: The Lawyer as Third-Party Neutral (2002), Rule 4.5.2, comments [1], [3]. Nonetheless, to the extent that lawyers' duties of confidentiality have been updated to take account of cyberthreats, analysis of those duties may inform how the international arbitrator should view the nature and scope of his or her duty to avoid intrusion. *See, e.g.*, U.K. Information Commission Office, Monetary Penalty Notice under the Data Protection Act 1998, Supervisory Powers of the Information Commissioner (Mar. 10, 2017), https://ico.org.uk/media/action-weve-taken/mpns/2013678/mpn-data-breach-barrister-20170316.pdf (fining UK family law barrister for failing to take "appropriate technical measures against the unauthorised or unlawful processing of personal data" in relation to confidential client files where the barrister failed to encrypt such files on her home computer and her husband inadvertently made the files accessible on an online directory while attempting to update software, noting that the Bar Council and barrister's chambers had issued guidance to barristers that a computer used by family members or others may require encryption of files to prevent unauthorized access to confidential material by shared users).

35. Notably, expectations of privacy and confidentiality may differ in investor-state arbitration. As explained in the UNCITRAL Notes on Organizing Arbitral Proceedings:

> [t]he specific characteristics of investor-State arbitration arising under an investment treaty have prompted the development of transparency regimes for such arbitrations. The investment treaty under which the investor-State arbitration arises may include specific provisions on publication of documents, open hearings, and confidential or protected information. In addition, the applicable arbitration rules referred to in those investment treaties may contain specific provisions on transparency. Further, parties to a treaty-based arbitration may agree to apply certain transparency provisions.

UNCITRAL Notes, *supra* note 26, at ¶ 55.

confidential.[36] More specifically, parties and institutions expect that the arbitrator will maintain the confidentiality of the arbitration.[37] Moreover, in the adversarial and adjudicatory context, each actor in arbitration has legitimate expectations of privacy as to the data that defines or supports its role in the process. Irrespective of the extent to which the proceeding as a whole is entirely confidential or in some respects public, counsel and clients expect that they alone will have access to their communications and case strategy, for example, while arbitrators expect that no one else will have access to their deliberations or draft adjudicative documents and other work product. Those who intrude on these boundaries by hacking or other unauthorized access may break the law[38]; at a minimum, they will threaten legitimate expectations as to privacy in any adjudicatory process and the integrity of the process as a whole. In sum, since

36. Paul D. Friedland, Arbitration Clauses for International Contracts 21 (Juris, 2d ed. 2007) ("Notwithstanding the usual absence of prohibitions on party disclosure, there is an expectation and tradition of confidentiality in arbitration, which a party violates at its own peril vis-à-vis the arbitrators."); Queen Mary Univ. of London Sch. of Int'l Arb., 2010 International Arbitration Survey: Choices in International Arbitration, at 29, http://www.arbitration.qmul.ac.uk/docs/123290.pdf, 29 (Fifty percent of corporations indicated that they "consider that arbitration is confidential even where there is no specific clause to that effect in the arbitration rules … .or agreement"); Int'l Inst. for Conflict Prevention & Res., General Commentary for CPR Rules for Administered Arbitration of International Disputes, *available at* https://www.cpradr.org/resource-center/rules/international-other/arbitration/international-administered-arbitration-rules ("Parties that choose arbitration over litigation of an international dispute do so primarily to avoid the unfamiliarity and uncertainty of litigation in a foreign court; also out of a need or desire for a proceeding that is confidential and relatively speedy."); ICC International Court of Arbitration, Note to Parties and Arbitral Tribunals on the Conduct of the Arbitration under the ICC Rules of Arbitration, ¶ 27 (July 13, 2016) ("The [ICC] Court endeavors to make the arbitration process more transparent in ways that do not compromise expectations of confidentiality that may be important to parties.")

37. UNCITRAL Notes, *supra* note 26, at ¶ 53 ("Whereas the obligation of confidentiality imposed on the parties and their counsel may vary with the circumstances of the case as well as the applicable arbitration law and arbitration rules, arbitrators are generally expected to keep the arbitral proceedings, including any information related to or obtained during those proceedings, confidential.") (emphasis added); LCIA Notes for Arbitrators, ¶ 6 (June 29, 2015) ("Parties to arbitrations are entitled to expect of the process a just, well-reasoned and enforceable award. To that end, they are entitled to expect arbitrators: . . . to maintain the confidentiality of the arbitration. . . .") (emphasis added).

38. In the United States, for example, certain federal laws criminalize hacking and most states have computer crime laws that address unauthorized access. *See* Computer Fraud and Abuse Act, 18 U.S.C. § 1030; National Conference of State Legislatures, Computer Crime Statutes (Dec. 5, 2016), http://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx.

cyberintrusion undermines or negates the legitimate expectations of confidentiality that exist in international commercial arbitration as well as the legitimate expectations of privacy that exist to some degree in all adjudicatory proceedings, it follows that the arbitrator's special duty to protect confidentiality extends to an obligation to avoid intrusion by non-participants who are determined to defeat those expectations.[39]

B. Duty to Preserve and Protect the Integrity and Legitimacy of the Arbitral Process

The arbitrator's duty to avoid intrusion also rests on a duty to protect the integrity and legitimacy of the arbitral process. Unauthorized intrusion by hackers or other malevolent actors threatens more than confidentiality: it is a direct threat to the fair, neutral, and orderly process that underlies all arbitrations and to public trust in the arbitral process. If we accept that hacking threatens the integrity of the process, it follows that the arbitrator's obligation to protect the integrity of the process encompasses some form of duty to avoid such intrusion.

Our premise that the arbitrator has a duty to avoid intrusion does not require resolution of the ongoing debate as to whether a commercial arbitrator is a mere independent service provider to the parties or if the arbitrator has a broader, adjudicative role with responsibilities also to society and the rule of law.[40] Recognizing the deference to party autonomy that characterizes international commercial arbitration, it is well-established that arbitrators also have important and independent responsibilities to maintain their own reputations and probity, to support the interests of society and to

39. *See* UNCITRAL Notes, *supra* note 26, at ¶ 58(b).

40. *See* ROGERS, *supra* note 2; Lon L. Fuller, *The Forms and Limits of Adjudication*, 92 HARV. L. REV. 353, 392 (1978) (common features of the power to adjudicate delegated by the state to judges and by consent of the parties to arbitrators); Panel Discussion, *Arbitrator Ethics Through the Lens of Arbitrator Role: Are Arbitrators Adjudicators or Service Providers?*, 10 WORLD ARB. & MED. REV. 3, 309 (2016); Margaret Moses, *The Role of the Arbitrator: Adjudicator or Service Provider?*, 10 WORLD ARB. & MED. REV. 3, 367 (2016)

uphold the legitimacy and integrity of the arbitral process.[41] Even the most articulate and well-respected proponents of the arbitrator as service provider model recognize that there are limits to party autonomy and to arbitrators' fidelity to the parties' instructions.[42]

There is little doubt that the use in an arbitration of data illegally obtained by or on behalf of a party would irreparably taint proceedings.[43] Different issues arise when external actors compromise the data security of arbitration-related information. Here, the participants are victims of the intrusion and the matter presumably may proceed, with such corrective or ongoing protective steps as the tribunal may deem appropriate.[44] Nonetheless, such an incident, particularly if it follows from a failure to adequately secure data, inevitably will erode the confidence and trust of participants, and potentially the public, in the international private commercial

41. *See e.g.,* Julie Bédard, Timothy Nelson and Amanda Kalantirsky, *Arbitrating in Good Faith and Protecting the Integrity of the Arbitral Process*, 3 PARIS J. INT'L ARB. 737, 749 (2010); ABA/AAA CODE OF ETHICS FOR ARBITRATORS IN COM. DISPUTES, Canon 1 ("An arbitrator should uphold the integrity and fairness of the arbitration process . . . . An arbitrator has a responsibility not only to the parties but also to the process of arbitration itself, and must observe high standards of conduct so that the integrity and fairness of the process will be preserved."); ICC RULES, *supra* note 10, at art. 5 ("[T]he emergency arbitrator shall act fairly and impartially and ensure that each party has a reasonable opportunity to present its case"); JAMS FOUNDATION, JAMS ARBITRATOR ETHICS GUIDELINES, 1 ("[A]n arbitrator should uphold the dignity and the integrity of the office of the arbitration process"); CIARB ETHICS CODE, *supra* note 30, at Part 2, Rule 2 ("A member shall maintain the integrity and fairness of the dispute resolution process.").

42. *See* Luca G. Radicati di Brozolo, *Party Autonomy and the Rules Governing the Merits of the Dispute in Commercial Arbitration*, *in* LIMITS TO PARTY AUTONOMY IN INTERNATIONAL COMMERCIAL ARBITRATION, 339 (Juris, 2016); *see also* Teresa Cheng, *panelist*, *The Theory and Reality of the Arbitrator: What is an International Arbitrator?* 7 WORLD ARB. & MED. REV. 4, 639 (2013) (commenting at the 25th Annual Workshop of the Institute for Transnational Arbitration that although arbitrators are independent service providers, there is also a duty to oneself as well as a duty to the arbitral process); ROGERS, *supra* note 2; ILA REPORT, *infra* note 47, at 17; Park, *Arbitrators and Accuracy, supra* note 1, at n.59 (stating faithfulness to the agreement would not justify violation of international public policy).

43. ILA REPORT, *infra* note 47, at 18; Bernard Hanotiau, *Misdeeds, Wrongful Conduct and Illegality in Arbitral Proceedings*, *in* INTERNATIONAL COMMERCIAL ARBITRATION: IMPORTANT CONTEMPORARY QUESTIONS, 285 (Kluwer Law International, 2003); REDFERN AND HUNTER ON INTERNATIONAL ARBITRATION ¶ 5.76 (5th ed., 2009).

44. *See Caratube*, *supra* note 18 (considering the admissibility of illegally obtained evidence, accepting some and excluding some).

arbitration process.[45] The arbitrator, along with the parties, counsel, and other actors in the process, is in a position to take reasonable protective measures to avoid that risk.

While much attention has been focused on the implied *powers* of arbitrators to fill in gaps in institutional rules or the parties' agreement where necessary to protect due process and the legitimacy of the process, less attention has been paid to the scope of the arbitrator's *duties*.[46] The ILA Arbitration Committee's *Final Report on The Inherent Powers of Arbitrator in International Commercial Arbitration* noted that the implied powers necessary to protect the core functions of arbitration amount to affirmative arbitral duties:

> It is in such situations that a third and final category of non-enumerated powers becomes relevant, encompassing that authority which can be said to be truly inherent, namely those powers necessary to safeguard a tribunal's jurisdiction and the integrity of its proceedings. Stated differently, these powers are

45. *See* Jan Paulsson, *Metaphors, Maxims and Other Mischief, The Freshfields Arbitration Lecture 2013*, 30 ARB. INT'L 4, 630 (2014) ("[P]ublic confidence is perforce at stake in the arbitral context as well [as in the judicial process], because arbitration cannot thrive without the support of the general legal system."); Charles Brower, *Keynote Address: The Ethics of Arbitration: Perspectives from a Practicing International Arbitrator*, 5 BERKELEY J. OF INT'L L. PUBLICIST, 1 (2010) ("[A]rbitrators and arbitral institutions also have an interest in maintaining legitimacy, both for the mutual acceptance of their awards by the parties before them and for broad public acceptance of the entire law-based system of which they are a part.").

46. Two widely cited cases involving the appearance of new counsel after an ICSID tribunal was constituted focused on the arbitrator's role in preserving the integrity of the arbitration proceedings. Although the tribunals reached differing results on applications to disqualify counsel and had differing views on the nature and extent of an arbitrator's inherent powers, both stated that the arbitrators had some inherent power, and presumably some obligation, to protect the essential integrity of the proceeding. *See Hrvatska Elektroprivreda d.d. v. Republic of Slovenia*, ICSID Case No. ARB/05/24, 15, (2008) (Tribunal's Ruling Regarding the Participation of David Mildon QC in further Stages of the Proceeding); *Rompetrol Group NV v. Romania*, ICSID Case No. ARB/06/03, 5-6 (2008) (Decision of the Tribunal on the Participation of a Counsel); *see also* Bédard, et al., *supra* note 41 at n.69. Similarly, in *Caratube*, although the tribunal found that the claimants failed to prove the respondent had engaged in any threatening or intimidating action that could cause an irreparable harm to the claimants' rights in the arbitration, including a right to the "integrity and the legitimacy of the arbitration," the tribunal implicitly recognized its authority to take measures to preserve the integrity of the arbitration insofar as it stressed the "[p]arties' general duty, arising from the principle of good faith, not to take any action that may aggravate the present dispute, affect the integrity of the arbitration and the equality of the Parties . . . ." *Caratube supra* note 18, at ¶¶ 111, 154.

> those required to decide a legal dispute fairly and in a manner consistent with at least the minimal requisites of due process and public policy. They trace their roots most clearly to the original notion of inherent powers as protecting jurisdiction and curtailing procedural abuses, and their exercise may justify overriding party preferences. . . . Such powers are so core to the function of arbitration that they might be more properly termed arbitral duties, the fulfillment of which is a necessary function of serving as a competent arbitrator.[47]

We conclude, then, that the arbitrator's duty to uphold the legitimacy and integrity of the arbitral process, and to ensure confidence and trust in arbitration, further supports the premise that the arbitrator has a duty to avoid intrusion.

C. Duty of Competence

It is commonly accepted that an arbitrator has a duty of competence.[48] Various arbitrator ethics codes expressly require arbitrators to be "competent." Canon 1 of the *ABA/AAA Code of Ethics for Arbitrators in Commercial Disputes*, which requires an arbitrator to uphold the integrity and fairness of the arbitration process, provides that an arbitrator should accept appointment in a particular matter only if fully satisfied that he or she is "competent to serve." The *IBA Rules of Ethics for International Arbitrators* provide a more general requirement that "international arbitrators should be . . . competent" in addition to a specific requirement that the arbitrator be competent to determine the issues in dispute in a particular matter.[49]

---

47. INTERNATIONAL LAW ASSOCIATION, REPORT FOR THE BIENNIAL CONFERENCE IN WASHINGTON, D.C., April 2014 (final report 2016) [hereinafter ILA REPORT], at 17, http://www.ila-hq.org/download.cfm/docid/04ED7050-5C2A-4A56-92FCF1857A094C8B (last visited Jan. 22, 2017).

48. *See* Henry Gabriel and Anjanette H. Raymond, *Ethics for Commercial Arbitrators: Basic Principles and Emerging Standards*, 5 WYO. L. REV 453 (2005); ILA REPORT, *supra* note 47 (stating the duty to protect integrity of the proceeding is core to necessary function of serving as a competent arbitrator).

49. *See* Introductory Note and Rule 2.2; *see also* CIARB ETHICS CODE, *supra* note 30, at Part 2, Rule 4 "Competence" ("A member shall accept an appointment or act only if appropriately qualified or experienced.").

While the arbitrator ethics codes do not define competence, important context and definition of the meaning of the term may be drawn from the evolution of lawyer ethics codes in recent years. Recognizing the need to provide some definition of competence and to update ethical codes to reflect the rise of globalization and technology, governing bar associations and disciplinary authorities have amended lawyer ethical codes to provide explicit linkage between general competence requirements and the need to keep abreast of technology.[50] For example, the American Bar Association ("ABA") *Model Rules of Professional Conduc*t, first introduced by the ABA in 1983, and adopted over time in various forms by most states in the United States,[51] provide the following lawyer competence requirement:

> Rule 1.1 Competence
>
> > A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

Notably, ABA Model Rule 1.1 is limited by its terms to the lawyer serving in a representational function. However, the Preamble to the Model Rules notes that a lawyer may serve in other roles, including "as a third party neutral, a non-representational role helping the parties to resolve a dispute or other matter," and goes on to state that,

---

50. Lawyer ethics rules obviously do not bind non-lawyer arbitrators. Indeed, some of the rules are limited to the context of client representation and thus do not expressly apply even to lawyers who, when serving as arbitrators, are not representing clients. For example, ABA Model Rule 1.1, standing alone in the form quoted in the accompanying text, does not apply directly to arbitrators, even if they are lawyers practicing in a jurisdiction where this version of the Model Rules applies. In France, the Règlement Intérieur National, the French code of ethics for lawyers, contains a general competency requirement in respect to client work in Article 1.3 ("L'avocat . . . fait preuve, à l'égard de ses clients, de competence . . . ."), http://codedeonto.avocatparis.org/acces-article; *see also* UK SOLICITORS REGULATORY AUTHORITY, SRA CODE OF CONDUCT 2011 (Version 18, 2016) [hereinafter UK SRA CODE OF CONDUCT] at 0-1.5 ("[t]he service you provide to clients is competent . . . . "), http://www.sra.org.uk/solicitors/handbook/code/content.page.

51. A notable exception is California, which maintains its own Rules of Professional Conduct. California Rule 3-110 (A) provides a general competence requirement ("A member shall not intentionally, recklessly, or repeatedly fail to perform legal services with competence.").

"[i]n all professional functions a lawyer should be competent, prompt and diligent."[52]

New York State did not adopt the Model Rules until 2009 and did not adopt the Preamble quoted above. However, Model Rule 1.1 as adopted in New York added a more general competency requirement, in addition to the client-oriented rule: "A lawyer shall not handle a legal matter that the lawyer knows or should know that the lawyer is not competent to handle . . . ."[53] Thus, at least as to lawyers working as arbitrators in jurisdictions that have adopted the ABA Preamble or who have adopted a rule similar to Rule 1.1(b) as in effect in New York State, there is a direct ethical obligation of competence.[54]From 2009 to 2013, the ABA Commission on Ethics 20/20 recommended proposed amendments to the Model Rules to account for, among other things, rapid changes in technology

52. AM. BAR. ASSOC., PREAMBLE: A LAWYER'S RESPONSIBILITIES, ¶ 4. By referring to "professional functions," the Preamble is broad enough to avoid the debate over whether participants are engaged in the practice of law. *See* Birbrower, Montalbano, Condon & Frank, P.C. v. Superior Court, 17 Cal.4th 119 (Cal. 1998), *cert den.,* 525 U.S. 920 (1998); Schiff Hardin LLP, *Arbitration and the Unauthorized Practice of Law*, 13 ARIAS QUARTERLY U.S. 1, 16-19 (2006), http://www.schiffhardin.com/Templates/Media/files/archive/binary/spector-arbitration.pdf.

53. NY Judiciary Law (Appendix: Code of Prof. Resp. §1200, Rule 1.1 (b)); The New York State Bar Association Committee on Standards of Professional Conduct ("COSAC") 2007 Report recommending the adoption of the Model Rules noted that the new rules were beneficial in describing competent representation as requiring the "legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation," in contrast to the previous Lawyer's Code of Professional Responsibility that "did not define or describe competent representation." New York State Bar Association Proposed Rules of Professional Conduct 11 (2007), *available at* http://www.nysba.org/workarea/DownloadAsset.aspx?id=26635; New York City Bar Association Professional Responsibility Committee Report on COSAC Proposals Rules 1.1-1.4, 3.1, 3.2, 3.5-3.9, and 8.1-8.4 (2006) *available at* http://www.nycbar.org/pdf/report/Prof_Resp_COSAC_506.pdf (proposed Rule 1.1 "helpfully fleshes out the definition of 'competent representation'"). Notably also, in adopting Model Rule 1.1 (b), New York State intended to preserve the concept in prior Disciplinary Rule 6-101 (competent representation) and its accompanying Ethical Consideration 6-2 that a lawyer should attain and maintain competence by keeping abreast of current legal literature and developments. *Id.*

54. Also useful by analogy is *The Code of Conduct for Lawyers in the EU*, issued by the Council of Bars and Law Societies of the European Union, which bridges the gap from the regulation of lawyers working in a representational capacity in the judicial system to those working in arbitration by providing that "[t]he rules governing a lawyer's relations with the courts apply also to his relations with arbitrators." CCBE, CODE OF CONDUCT FOR LAWYERS IN THE EUROPEAN UNION (2002) at art. 4.5, *available at* http://www.idhae.org/pdf/code2002_en.pdf.

affecting the practice of law. In 2012, the ABA House of Delegates adopted a revised Comment 8 to Model Rule 1.1, to provide in respect to competency, that "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 technology." In amending Comment 8, the ABA took the position that the revised language did not impose any new obligations on lawyers, but, rather, simply reminded lawyers that in the current environment, an awareness of technology, including the benefits and risks associated with it, is part of the lawyer's general ethical duty to remain competent.[55] The same may be said in respect to an arbitrator's competence obligation.

In its 2014 report recommending that New York adopt the revised comment 8 to Model Rule 1.1, the New York State Bar Association Committee on Standards of Professional Conduct noted that:

> . . . to keep abreast of changes in law practice, a lawyer needs to understand the risks and benefits of technology relevant to the lawyer's particular practice. For example, if a lawyer's clients are communicating with the lawyer by web-based document-sharing technology or by social media, the lawyer should have some understanding of how to ensure that confidential communications remain confidential. The proposed amendment impresses upon lawyers the key role that technology plays in law practice and creates the expectation that lawyers will keep abreast of the benefits and risks associated with the technology relevant to their own legal practice.[56]

---

55. *See* Karin Jenson, Coleman Watson, & James Sherer, *Ethics, Technology, and Attorney Competence*, *available at* http://www.law.georgetown.edu/cle/materials/ediscovery/2014/frimorndocs/ethicsinediscoverybakerhostetler.pdf (last visited Jan. 14, 2017); *see also* The State Bar Of California Standing Committee on Professional Responsibility and Conduct, Formal Opinion Interim No. 11-0004 (2014) ("An attorney's obligations under the ethical duty of competence evolve as new technologies develop and become integrated with the practice of law."); INT'L BAR ASSOC., IBA INTERNATIONAL PRINCIPLES ON CONDUCT FOR THE LEGAL PROFESSION (2011), https://www.ibanet.org/Article/NewDetail.aspx?ArticleUid=BC99FD2C-D253-4BFE-A3B9-C13F196D9E60 ("Competence . . . includes competent and effective client, file and practice-management strategies.").

56. Report of The New York State Bar Association Committee On Standards Of Attorney Conduct ("COSAC") Proposed Amendments to the New York Rules of Professional

Whether or not adopted in the form encompassing the more general obligation provided in the New York version of the rules, the Model Rules, and particularly Comment 8 to Model Rule 1.1 as it now reads, are relevant to inform and define the meaning of competence as applied to arbitrators, as well as in their direct regulation of lawyer conduct.[57]

Achieving digital literacy, including an understanding of the measures reasonably necessary to avoid cyberintrusion in an arbitration, is also closely related to the attention institutions, users, and counsel have paid in recent years to the role of the arbitrator in case management.[58] In the highly digitized and interdependent world

---

Conduct and Related Comments 10 (2014), http://www.nysba.org/WorkArea/DownloadAsset.aspx?id=54063.

57. *See, e.g.,* In re: Amendments to Rules Regulating the Florida Bar 4-1.1 and 6-10.3, No. SC16-574 (Sept. 29, 2016), at http://www.floridasupremecourt.org/decisions/2016/sc16-574.pdf (amending the comment to rule on competence to address technology); Law Society of Upper Canada, Technology Practice Management Guideline, Guideline 5.5 ("Competent Use of Information Technologies. Lawyers should have a reasonable understanding of the technologies used in their practice or should have access to someone who has such understanding") & 5.10 ("Security Measures. Lawyers should be familiar with the security risks inherent in any of the information technologies used in their practices including unauthorized copying of electronic data, computer viruses which may destroy electronic information and hardware, hackers gaining access to lawyers' electronic files, power failures and electronic storms resulting in damage to hardware or electronic information, theft of vast amounts of electronic information stored in stolen hardware. Lawyers should adopt adequate measures to protect against security threats and, if necessary, to replace hardware and reconstruct electronic information."), *available at* https://www.lsuc.on.ca/For-Lawyers/Manage-Your-Practice/Technology/Technology-Practice-Management-Guideline/ (last visited Jan. 22, 2017); Canadian Bar Association*, Legal Ethics in a Digital World* (Sept. 2, 2015), https://www.cba.org/getattachment/Sections/Ethics-and-Professional-Responsibility-Committee/Resources/Resources/2015/Legal-Ethics-in-a-Digital-World/guidelines-eng.pdf; Philipe Doyle Gray, *The Pillars of Digital Security*, BAR NEWS: J. OF THE NEW SOUTH WALES BAR ASSOCIATION (Summer 2014), http://www.philippedoylegray.com/content/view/56/45/ (although the Law Society of New South Wales has not adopted professional conduct rules addressing technology, it has published guidelines for lawyers about the use of technology such as cloud computing and social media); E-Law Committee of the Law Society of South Africa, LSSA Guidelines on the Use of Internet-Based Technologies in Legal Practice (2015), http://www.lssa.org.za/legal-practitioners/resources-for-attorneys; *see also* UK SRA CODE OF CONDUCT, *supra* note 50, at O-4.5 ("You have effective systems and controls in place to enable you to identify risks to client confidentiality . . . ."); O-7.5 ("You comply with . . . data protection legislation."); IB-7.5 ("Identifying and monitoring . . . IT failures and abuses.").

58. *See, e.g.,* ICC RULES, *supra* note 10, at app. IV (case management techniques); LCIA RULES, *supra* note 1, at art. 14 (conduct of the proceedings); ICDR RULES, *supra* note 10, at art. 20.2 (conduct of the proceedings) ("In establishing procedures for the case, the

of international arbitration, management of technology and baseline data security competence manifestly have become critical components of an arbitrator's competence to organize and conduct arbitration proceedings.[59]

D. Global Data Protection Laws and Regulations

In any given arbitration matter, data held by an arbitrator may be subject to specific cybersecurity obligations arising from international or national data protection laws and regulations that govern how certain information can be collected, stored, and transferred.[60] While there is no universal international approach to data protection, nearly 110 countries[61] have enacted laws aimed at protecting personal information by regulating categories of data or industry sectors, such as the financial and health care industries.[62] As the key players in

---

tribunal and the parties may consider how technology, including electronic communications, could be used to increase the efficiency and economy of the proceedings."); College of Commercial Arbitrators, Protocols for Expeditious, Cost-Effective Commercial Arbitration (2010) 69 (arbitrators should take control of the arbitration and actively manage it from start to finish); ICC Commission Report, Controlling Time and Costs in Arbitration (2d. ed. 2012); Christopher Newmark, *Controlling Time and Costs in Arbitration*, *in* LEADING ARBITRATORS' GUIDE TO INTERNATIONAL ARBITRATION *supra* note 1.

59. The UNCITRAL Notes on Organizing Arbitral Proceedings (2016) urge that arbitrators consider issues relating to the means of communication to be used during the proceedings at the outset, noting that the parties and the tribunal "may need to consider issues of compatibility, storage, access, data security as well as related costs when selecting electronic means of communication." UNCITRAL Notes, *supra* note 26, at ¶¶ 56, 58.

60. *See* UNCTAD, Data Protection Regulations and International Data Flows: Implications for Trade and Development, UNCTAD/WEB/DTL/STICT/2016/1/iPub, http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf (last visited Jan. 9, 2017) (overview of international and national laws and regulations) ("UNCTAD on Data Protection"); *see also* European Union Data Protection Directive (95/46/EC) (implemented in each of the twenty-eight EU Member States through national data protection law).

61. *See* UNCTAD on Data Protection at 42 (108 countries have either comprehensive data protection laws or partial data protection laws).

62. In the United States, for example, there is no omnibus privacy or data protection legislation, but a patchwork of federal privacy laws that generally regulate security breach notification statutes by sector and state. *See, e.g.*, Health Insurance Portability and Accountability Act, 42 U.S.C. § 1301 *passim* [hereinafter HIPPA] (health information); Federal Trade Commission Act, 15 U.S.C. §§ 41-58 (consumer protection); Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801-6827 (financial information); National Conference of State Legislators, Security Breach Notification Laws (Jan. 4, 2016), http://www.ncsl.org/research/telecommunications-and-information-technology/security-

international arbitrations frequently reside in different countries, resulting in continuous cross-border exchanges of information, it follows that the same data may be subject to multiple, and potentially inconsistent, laws. For example, the legal concept of "personal information" or "personally identifiable information" subject to reasonable protection from unauthorized access is defined more broadly under EU law than it is under US law.[63]

While it is beyond the scope of this article to address the complex conflict-of-law issues that may arise in these situations,[64] the global proliferation of data protection laws indicates that: (i) participants in international arbitrations who share the sensitive information of others may have legal obligations to ensure that arbitrators, acting in the capacity of service providers, safeguard that information by complying with certain security standards[65]; and (ii) increasingly, both participants and non-participants in an arbitration may have legally enforceable interests (or rights)[66] in the way that arbitrators secure and handle e-mail correspondence, witness statements,[67] and other electronically-exchanged documents that routinely disclose personally identifiable information. Moreover,

---

breach-notification-laws.aspx (forty-seven states have enacted legislation entitling individuals to notice of breaches of information of personally identifiable information).

63. *See* Practical Law, Expert Q&A on Data Security in Arbitration (Dec. 1, 2016) (stemming from the concept in EU countries that privacy is a fundamental human right, a person's name and place of employment can be considered protected information).

64. Although not the focus of this article, we note that the potential for the application of disparate data protection laws strongly favors early discussions between opposing counsel about how arbitration-related data will be handled as well as discussion of data security with the tribunal by at least the first case management conference.

65. For example, an individual or organization that must comply with health information privacy rules under HIPPA is required to have any "business associate" it engages to help carry out its functions agree to comply with those rules as well. HIPPA, *supra* note 62. *See also* EU Directive 2016/1148 (July 6, 2016).

66. *See, e.g.*, Charter of Fundamental Rights of the European Union (2012/C 326/02), art. 7 ("Everyone has the right to respect for his or her private and family life, home and communications") & 8(1) ("Everyone has the right to the protection of personal data concerning him or her.").

67. *See* INT'L BAR ASSOC., IBA RULES ON THE TAKING OF EVIDENCE IN INTERNATIONAL ARBITRATION (2010), art. 4(5) (specifying personal information to be included in fact witness statements).

when security incidents occur, a web of breach notification obligations may be triggered.[68]

Although it is not evident that the obligations or legal interests that may arise under the current global data protection regime create a bright-line duty, independent of any specific case, for arbitrators to avoid cyberintrusion, their prevalence at least supports the notion that to maintain user confidence in international arbitration process, arbitrators must not only be prepared and competent to handle sensitive information securely, but also appear to the public to be so prepared. Global data protection laws thus behoove arbitrators to be proactive (and not merely reactive, on a case-by-case basis) in dealing with cybersecurity.

IV. NATURE AND SCOPE OF THE ARBITRATOR'S DUTY TO AVOID INTRUSION

This article posits that the arbitrator's duty in relation to cybersecurity is one of avoiding intrusion, which we define as the duty to take reasonable measures to prevent unauthorized digital access to arbitration-related information. In the following sections, we first explore the nature and scope of the duty and then discuss some practical measures that will assist the arbitrator in fulfilling the duty.

A. An Umbrella Obligation

As we have shown above, the arbitrator's duty in relation to cybersecurity is not a new, independent obligation, but rather a natural extension in the digital age of an arbitrator's existing duties to keep arbitration-related information confidential, to preserve and protect the integrity and legitimacy of the arbitral process, and to be competent. By grouping the implied cybersecurity responsibilities arising under each of these duties under the new umbrella of the "duty to avoid intrusion," we recognize the unique challenges that cyberthreats pose to the practice of international arbitration in the digital age.

This is a matter of substance, not just terminology. Recognition of the threat and each actor's acceptance of responsibility to take part

68. Practical Law, *supra* note 63.

in addressing it are key building blocks to effective cybersecurity in the international commercial arbitration regime. In this article, which focuses on the arbitrator's role, we emphasize that the fulfillment of existing arbitrator duties in the digital age encompasses a duty to be proactive and vigilant in guarding against cyberintrusion.

B. An Interdependent Landscape with Independent Duties

Since the data arbitrators are entrusted to keep confidential generally originates in the arbitration from the parties and their counsel, it may be tempting for arbitrators to view cybersecurity as an issue for the parties, and particularly counsel, to address on a case-by-case basis. Parties and their counsel indisputably do have legal and ethical responsibilities to safeguard the data that they import into an arbitration.[69] In many instances, they will be uniquely positioned to secure that data and to advise the arbitrator regarding specific security precautions necessary in the case or required by law. Any view that purports to isolate any one particular participant in the arbitration process as having sole responsibility for cybersecurity, however, or to relieve the arbitrator from any responsibility for cybersecurity outside of the bounds of individual cases, ignores the interdependent digital landscape discussed above and is shortsighted. Since any break in the custody of sensitive data may affect all participants in the arbitral process, cybersecurity is an inherently shared responsibility.

While interdependent with other actors, the arbitrator's cybersecurity duty also stands alone. The arbitrator who takes the view that others are primarily responsible abjures the arbitrator's special role as adjudicator as well as the arbitrator's underlying duties to safeguard the integrity and legitimacy of the process and the confidentiality of arbitration-related information. The obligations of other players in the arbitral process (including the parties, counsel, arbitral institutions and third party service providers among others) may be governed by differing standards and other legal regimes, only some of which overlap with those governing arbitrators.

---

69. *See supra* Section III.D (discussing national data protection laws and regulations); Section III.C (discussing cybersecurity obligations arising from attorney ethical codes).

Moreover, the arbitrator's day-to-day data security architecture and practices pre-exist individual matters and persist after the matter is concluded. Thus, the strength of the arbitrator's routine cybersecurity practices will impact the overall security of arbitration-related data from the first moment the arbitrator becomes involved with a case, before counsel or the parties have an opportunity to address security protocols that may be appropriate for the specific data involved in the matter, and will continue after the matter ends as the arbitrator maintains at least some data for conflicts or other record-keeping purposes.

C. Personal Accountability

As arbitrators are appointed for their personal qualifications and reputational standing,[70] it is broadly accepted in international arbitration that the arbitrator's mandate is personal and cannot be delegated.[71] While this notion is raised most often in discussions about impermissible delegation of decision-making responsibilities to arbitral secretaries, the personal nature of the arbitrator's mandate has implications for cybersecurity as well. In particular, it is important for arbitrators to recognize that even if the security of their digital infrastructure is established and monitored by IT personnel, or they work in a large law firm setting where they have little to no influence over firm-wide security policies, they cannot assume that their responsibilities in relation to cybersecurity have been met.

First, effective security depends on individual choices and conduct. [72] Hackers' most valuable currency is human carelessness.[73]

---

70. BORN, *supra* note 27, at 2013. ("Arbitrators are almost always selected because of their personal standing and reputation . . .").

71. *See* Eric Schwartz, The Rights and Duties of ICC Arbitrators, in ICC International Court of Arbitration Bulletin, Special Supplement, The Status of the Arbitrator (1995) at 86; *see also* BORN, *supra* note 27, at 1999. ("An arbitrator's obligations include the duty not to delegate his or her responsibilities or tasks to third parties. … Most fundamentally, an arbitrator cannot delegate the duty of deciding a case, attending hearings or deliberations, or evaluating the parties' submissions and evidence to others: these are the essence of the arbitrator's adjudicative function and they are personal, non-delegable duties.").

72. To highlight the fundamental role played by individuals in protecting confidential information, whether reliance is placed on notepads, mobile telephones, or the cloud, Philipe Doyle Gray shares this anecdote:

Even if an arbitrator operates in an environment with the digital architecture of Fort Knox, important security actions will always remain in the arbitrator's personal control. Law firm or IT policy may dictate to an arbitrator, for example, that strong, complex passwords be used on all laptops and other devices and that passwords be changed regularly. However, an arbitrator risks completely undermining that security protocol by conveniently storing a reminder of the password du jour on a post-it note stuck to the cover of a laptop,[74] and then working away on the laptop in an airport lounge or other public environment, or, worse, forgetting the laptop in the security line or the airplane seat pocket after a long international

---

> I regularly walk from the Supreme Court of New South Wales down King Street to stop at the intersection with Elizabeth Street. So too do other lawyers. When it's raining we huddle under the awning of the Sydney University Law School, but in fine weather we gather around the traffic lights waiting for the signal that it's safe for pedestrians to cross. Usually, I see paper files or lever-arch folders neatly stating the names of the clients concerned, and sometimes the nature of their confidential affairs. Often, I can't help but overhear a colleague talking about his matter. A few times, sensitive material was inadvertently broadcast to passers-by that happened to include me. Once, I even overheard a colleague—speaking on his mobile phone—discuss settlement negotiations during a mediation that had adjourned over lunch: he openly discussed not only the parties' respective offers, but his own client's bottom line. The real security problems lie not in CLOUD COMPUTING, but in ourselves.

Gray, *supra* note 57. *See also Harleysville Ins. Co. v. Holding Funeral Home*, Case No. 1:15cv00057 (W.D. Va., Feb. 9, 2017), http://bit.ly/2mSkyuu (court held that insurer's attorney-client privilege was waived where entire claims file was loaded onto a cloud service and made accessible to anyone via hyperlink without password protection, stating this was the "cyber world equivalent of leaving its claims file on a bench in the public square").

73. In December 2015, The Wall Street Journal reported that "[w]eeks after J.P. Morgan Chase & Co. was hit with a massive data breach that exposed information from 76 million households, the country's biggest bank by assets sent a fake phishing email as a test to its more than 250,000 employees. Roughly 20% of them clicked on it, according to people familiar with the email." Robin Sidel, *Banks Battle Staffers' Vulnerability to Hacks*, WALL ST. J., (Dec. 21, 2015), https://www.wsj.com/articles/the-weakest-link-in-banks-fight-against-hackers-1450607401. *See* Int'l Chamber of Commerce [ICC], *Cyber Security Guide for Business*, at 8, ICC Doc. 450/1081-5 (2015) ("35% of security incidents are a result of human error rather than deliberate attacks. More than half of the remaining security incidents were the result of a deliberate attack that could have been avoided if people had handled information in a more secure manner.").

74. According to Verizon's 2016 Data Breach Investigations Report, "63% of confirmed data breaches involved weak, default or stolen passwords." Verizon Report, *supra* note 13, at 20. *See also* Fox-Brewster, *supra* note 7 (Sony hack revealed chief executive's password was "guessable to any semi-skilled hacker" and that passwords to internal accounts were stored in a file marked "passwords").

flight.[75] Similarly, although IT policy may dictate that no USB drive can be used in a networked computer before it is manually scanned for viruses by the IT department, an arbitrator sitting in a hearing in Vienna may decide before the flight home to take the USB drive handed out at a recent arbitration conference and use it to transfer notes from deliberations stored on her laptop to a public computer in the hotel business center for printing.

Second, there is danger in complacency. Arbitrators understandably want to spend time on the practice of arbitration, not on routine practice management. However, an arbitrator who dismisses cybersecurity as an "IT issue" and who assumes that "others are taking care of it" fails to appreciate how a failure to heed cybersecurity may undermine his or her ability to keep arbitration-related information confidential as well as user trust and confidence in the integrity of the international arbitration regime. Notwithstanding the steady flow of news reports about cyberbreaches, it appears that "many [attorneys and law firms] are not using security measures that are viewed as basic by security professionals and are used more frequently in other businesses and professions."[76] Arbitrators who rely on IT personnel to support their practice should thus bear in mind that their existing data security framework and digital architecture may well require an upgrade or adaptation to the unique aspects of international arbitration. Indeed, just as an arbitrator should not entrust (but may be aided by) the conflicts department in his or her law firm to determine whether he or she is bound to make any disclosures in an arbitration,[77] an arbitrator may be assisted by, but

75. Laptops and other devices are reportedly lost over 100 times more frequently than they are stolen. Verizon Report, *supra* note 13, at 44.

76. David G. Ries, *Security*, ABA TECHREPORT 2016, 1-2, https://www.americanbar.org/groups/law_practice/publications/techreport/2016.html (reporting on 2016 survey of attorneys and law firms about security incidents and safeguards). *See also* Matthew Goldstein, *Citigroup Report Chides Law Firms for Silence on Hackings*, N.Y. TIMES (Mar. 26, 2015), https://nyti.ms/1NkjfKo (In March 2015, Citigroup's internal cyberintelligence team advised bank employees to be "mindful that digital security at many law firms, despite improvements, generally remains below the standards for other industries.").

77. *See, e.g.,* Ometto v. ASA Bioenergy Holding A.G. et al., 12 Civ. 1328(JSR), 2013 WL 174259 (S.D.N.Y. Jan. 7, 2013).

should not entrust, an IT department to fulfill the duty to avoid intrusion.[78]

D. Continuous and Evolving

The duty to avoid intrusion is a continuous obligation, which is not limited in time. In part, this follows from the nature of the arbitrator's duty of confidentiality. Since arbitrators may maintain digital information from their cases beyond the lifetime of an individual matter, ranging from case administration data (including as part of conflicts or billing systems), correspondence, procedural decisions, awards, and parties' evidentiary submissions, parties and other participants have a reasonable expectation that arbitrators will continue to safeguard the confidentiality of such information once a case ends.[79] Furthermore, as we have discussed above, because arbitrators accept appointments in new matters with a digital architecture and certain security practices already in place, parties and other participants have a reasonable expectation that arbitrators will heed cybersecurity from the time of appointment (and necessarily before).

The ongoing nature of the arbitrator's duty to avoid intrusion also flows from the underlying duty to be competent. Because cyberthreats are constantly evolving alongside advancing technology, an arbitrator cannot take effective steps to avoid intrusion unless he or she keeps abreast of the changing nature and scope of cyberrisks. Otherwise, the arbitrator will not be in any position to analyze risks and weigh appropriate responses, including, for example, with respect

78. The importance of "executive-level" attention to effective cyberrisk management is frequently emphasized by cybersecurity experts. *See, e.g.,* ICC, *Cyber Security Guide for Business*, *supra* note 73, at 4 (2015); Tucker Bailey et al., *Why Senior Leaders Are the Front Line Against Cyberattacks*, MCKINSEY & CO. (June 2014), https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/why-senior-leaders-are-the-front-line-against-cyberattacks.

79. Int'l Law Ass'n, *Draft Report of the Committee on International Commercial Arbitration for the 2010 Hague Conference, Confidentiality in International Arbitration*, at 18 (2010), http://www.ila-hq.org/en/committees/index.cfm/cid/19 (although there is uncertainty regarding the duration of duties of confidentiality in arbitration, the "fact that the duty of confidentiality usually covers the award seems to point to an expectation that the regime of confidentiality should outlive the arbitral proceedings and that the obligations will not cease after the end of the arbitration.").

to whether new or additional security measures may be warranted, what work-arounds might be acceptable when complying with an established security protocol proves to be impossible or impractical, or whether a new product or service is adequately secure.

E. Bounded by Reasonableness

Cybersecurity professionals routinely advise that in today's environment of ever-escalating data breaches, there is no longer any question of *if* one's digital infrastructure and data will be hacked, but only *when*.[80] As a practical reality, it follows that the arbitrator cannot guarantee that arbitration-related information will remain safe from hackers,[81] but can only take steps to mitigate the risks of cyberintrusion. In *LabMD, Inc. v. Federal Trade Commission,* the U.S. Federal Trade Commission ("FTC") explained why "reasonableness," assessed "in light of the sensitivity and volume of consumer information [a company] holds, the size and complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities," is an appropriate touchstone for determining whether a company has implemented appropriate data security measures:

> [The FTC] has made clear that it does not require perfect security; reasonable and appropriate security is a continuous process of assessing and addressing risks; there is no one-size-

80. U.S. Attorney Preet Bharara recently made such a pronouncement in announcing criminal indictments of hackers who traded on confidential law firm information, saying, "This case of cyber meets securities fraud should serve as a wake-up call for law firms around the world: you are and will be targets of cyber hacking, because you have information valuable to would-be criminals." Nate Raymond, *U.S. Accuses Chinese Citizens of Hacking Law Firms, Insider Trading*, REUTERS, (Dec. 28, 2016), http://www.reuters.com/article/us-cyber-insidertrading-idUSKBN14G1D5. *See also*, *e.g.*, Verizon Report, *supra* note 13, at 3 ("No locale, industry or organization is bulletproof when it comes to the compromise of data."); ICC, *Cyber Security Guide for Business*, *supra* note 73, at 10 ("Even the best protected enterprise will at some point experience an information security breach. We live in an environment where this is a question of when, not if.").

81. ICC, *Cyber Security Guide for Business*, *supra* note 73, at 4 (2015) ("[A]ll business managers including executives and directors must recognize that cyber risk management is an on-going process where no absolute security is, or will be, available.").

> fits-all data security program; and the mere fact that a breach occurred does not mean that a company has violated the law.[82]

Notably, reasonableness, not perfection, also bounds the lawyer's confidentiality duty under the ABA Model Rules to protect information relating to the representation of a client from unauthorized access.[83]

A risk-based approach, bounded by reasonableness, is similarly appropriate as we examine the scope and boundaries of the arbitrator's duty to avoid the ever-evolving threats of cyberintrusion in international commercial arbitration. It follows from the conclusion there is no one-size-fits-all data security program for consumer-facing corporations that there is no one-size fits-all data security program for international commercial arbitrators; any such program would risk obsolescence and fail to account for significant contextual differences. Furthermore, as Pastore argues, a de-contextualized approach to data security may be counterproductive "in that it over-designates [sensitive] information (desensitizing practitioners to the truly critical information) and results in overly cumbersome processes for information that, in reality, needs little to no additional protections."[84]

In addition, a standard of reasonableness under the circumstances is familiar in the law, particularly in areas where the facts and circumstances vary widely and evolve over time. The reasonableness approach enables consideration of the trade-offs that will sometimes exist between increased security measures and other interests.[85] To the extent the arbitrator's duty to avoid intrusion is in tension with other important values such as conducting the proceedings expeditiously and cost-effectively and in accordance with

---

82. *LabMD, Inc*., F.T.C. No. 9357, 2016 WL 4128215 (F.T.C. July 28, 2016). California's Attorney General notes in her Breach Report 2016 that "reasonable security" is the general standard for information security adopted not only in California but also the major United States federal data security laws and regulations. *See infra*, note 111.

83. Model Rule 1.6(c) provides "[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." MODEL RULES OF PROF'L CONDUCT, r. 1.6(c) (AM. BAR ASS'N, 1983). (emphasis added)

84. Pastore, *supra* note 15.

85. *See generally* Pastore, *supra* note 15.

the parties' preferences,[86] arbitrators should be entitled to weigh all of the relevant circumstances to determine the correct balance.[87] Arbitrators, institutions, users, and counsel should be able to understand and embrace such a standard for cybersecurity.

Accordingly, it is appropriate to limit the arbitrator's duty to an obligation to take such measures to protect digital security as he or she deems reasonable in light of the relevant facts and circumstances, including developments in technology and evolving security risks, the arbitrator's individual practice setting and digital architecture, the sensitivity of the data to be protected, and any party preferences or other case-specific factors present in the matters over which the arbitrator presides.

V. IMPLEMENTING THE DUTY TO AVOID INTRUSION

In the absence of a detailed roadmap for data security, the challenge for international arbitrators is to determine what specific measures they should implement to avoid intrusion, in their own infrastructure and in arbitrations over which they preside, given that what constitutes "reasonable" measures will vary based on a risk assessment of the arbitrator's individual digital architecture and data assets, the prevalent data security threats, available protective measures and, in relation to individual matters, case-specific factors.[88] Although it is by no means comprehensive, in this Part, we aim to highlight certain practical measures and general principles that are likely to be relevant for all international arbitrators, regardless of

86. *See supra* note 10.

87. The UNCITRAL Notes on Organizing Arbitral Proceedings (2016) note that data security is but one factor to be considered when deciding whether to use electronic means of communication for proceedings.. Other factors to be considered may include compatibility, storage, access and related costs. *See* UNCITRAL Notes, *supra* note 26.

88. Security framework standards are generally directed at organizations rather than business professionals. *See generally* NAT'L INST. OF STANDARDS AND TECH., SPECIAL PUBLICATION 800-53 REVISION 4, SECURITY AND PRIVACY CONTROLS FOR FEDERAL INFORMATION SYSTEMS AND ORGANIZATIONS (2013); FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY (2014), *available at* www.nist.gov; INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, ISO/IEC 27002:2013 *Information Technology, Security Techniques, Code of Practice for Information Security Controls*, *available at* www.iso.org (last visited Jan. 22, 2017); Center for Internet Security, *Critical Security Controls for Effective Cyber Defense*, Version 6 (Oct. 15, 2015), www.cisecurity.org/.

practice setting and individual risk profile.[89] In doing so, we further aim to show that the fundamentals of effective cyberrisk management need not be overwhelming or unduly burdensome. In addition, since cyberintrusion in the arbitral process can potentially arise from both intentional, targeted attacks on arbitral participants[90] and from the inadvertent[91] disclosure or compromise of arbitration-related information (e.g., by way of a weak password, lost mobile device, or other human error),[92] we discuss below potential responses to external threats and safeguards to prevent or mitigate damage if data security is_compromised.

89. A recent working paper from the Washington Legal Foundation suggests eight data security best practices based on an analysis of FTC enforcement actions:

- Limit the collection, retention, and use of sensitive data;
- Restrict access to sensitive data;
- Implement robust authentication procedures;
- Store and transmit sensitive information securely;
- Implement procedures to identify and address vulnerabilities;
- Develop and test new products and services with privacy and security in mind;
- Require service providers to implement appropriate security measures;
- Properly secure documents, media, and devices.

Kurt Wimmer, Ashden Fein, Catlin M. Meade & Andrew Vaden, *Data Security Best Practices Derived From Ftc § 5 Enforcement Actions*, at 6 (Washington Legal Foundation Paper No. 199, 2017).

90. *See supra* notes 13-14.

91. Even a single misdirected e-mail—within an arbitration proceeding—can have serious consequences for the perceived integrity and legitimacy of proceedings. In Horndom Ltd. v. White Sail Shipping, Optima Shipping and Integral Petroleum (SCC Arbitration V094/2011), the respondents challenged their own appointee to the tribunal after he accidentally copied one of the parties' lawyers on an e-mail complaining that counsel were getting "above their station" and that he was "rather sick of these parties." While the arbitrator admitted that disagreement over the hearing date resulted in his "frustration with procedural matters" and "intemperate expression," according to the respondents, the inadvertent disclosure of this otherwise private exchange among tribunal members revealed the arbitrator's "personal animosity" toward counsel and raised justifiable doubts about his impartiality. *See also* Alison Ross, *Accidental cc Triggers Double Arbitrator Challenge in Stockholm*, GLOB. ARB. REV. (Oct. 17, 2016), http://globalarbitrationreview.com/article/1069329/accidental-cc-triggers-double-arbitrator-challenge-in-stockholm.

92. An episode of the popular CBS TV show *The Good Wife* was based on the disclosure of confidential information resulting from an open feed when a video camera was mistakenly left on after a teleconferenced deposition. THE GOOD WIFE, (CBS, 2014), http://www.cbs.com/shows/the_good_wife/episodes/213197/.

A. Keeping Abreast of Developments in Relevant Technology and Understanding Associated Benefits and Risks

There are readily accessible resources for arbitrators to educate themselves as to the evolving nature and scope of major data security threats, with a view to understanding the significance and effectiveness of specific security protocols, such as standards for passwords. These resources have been developed by bar associations, law firms, and others.[93] For example, the ABA has taken the lead internationally in developing guidance for legal practitioners in responding to the challenges of the digital world and regularly posts short, digestible articles online on topics such as ransomware and encryption, in addition to offering educational webinars and seminars.[94] Such resources frequently highlight ethical opinions from state bar associations on the responsible use of technology in the legal profession. One particularly noteworthy resource, available only to ABA members, are e-mail alerts from the FBI about evolving cyberrisks and threats targeting law firms.

Other bar associations worldwide, such as the Law Society of Upper Canada, also have developed helpful online resources.[95] For the most part, such resources are available for free online (i.e., to members and non-members alike) and can assist arbitrators in finding quick, practical answers to technical questions written for legal professionals (such as what are the risks of public wifi and what alternatives are available for mobile wifi access). Meanwhile, to keep a handle on evolving data protection obligations internationally, now that most major law firms have a dedicated data privacy or cybersecurity practice group, arbitrators may also find it helpful to sign up for e-mail alerts from several law firms based in different jurisdictions.

---

93. *See, e.g., supra* note 88 and accompanying text.

94. *Law Technology Resource Center*, AMERICAN BAR ASSOCIATION https://www.americanbar.org/groups/departments_offices/legal_technology_resources.html (last visited Jan. 20, 2017).

95. *See Technology Practice Tips*, LAW SOCIETY OF UPPER CANADA http://www.lsuc.on.ca/technology-practice-tips-podcasts-list/ (podcasts on "everything you ever wanted to know about technology, but were afraid to ask" including "[p]ractical and important information about passwords, encryption, social media, smartphone security, websites and much more . . . in an accessible, conversational manner.").

B. Implementing Baseline Security

Cybersecurity experts agree that good cyber "hygiene"—basic everyday habits relating to technological use—is essential to a strong, baseline defense.[96] Significantly, these are habits that every arbitrator, regardless of practice setting, can readily implement, with minimal cost and without the need for IT support. Basic cyber hygiene best practices include:

- creating access controls, including strong, complex passwords[97] and two-factor authentication when available[98];
- guarding digital "perimeters" with firewalls, antivirus and antispyware software, operating system updates and other software patches[99];
- adopting secure protocols such as encryption for the storage and transmission of sensitive data[100];
- being mindful of public internet use in hotel lobbies, airports, coffee shops, and elsewhere and considering making use of personal cellular hotspots and virtual private networks[101]; and
- being mindful of what one downloads.[102]

---

96. *See, e.g.*, FED. TRADE COMM'N, START WITH SECURITY: A GUIDE FOR BUSINESS, LESSONS LEARNED FROM FTC CASES (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf; Wimmer et. al., *supra* note 89.

97. On some devices, including many phones and tablets, biometric authentication technologies such as fingerprint scanners now are available to perform the authentication and access control function. *See* PWC Report, *supra* note 13, at 9-12.

98. Many services and sites that store sensitive information, including cloud storage and e-mail providers, offer two-factor authentication whereby access requires a password plus something else that you have; typically, a security code that is either sent by text message or e-mail to a separate device or generated via an app that works offline such as Google Authenticator, or a biometric like a fingerprint. *See Two-Factor Authentication for AppleID*, APPLE, https://support.apple.com/en-us/HT204915 (last visited Jan. 22, 2017); *Google Two-Step Verification*, GOOGLE, https://www.google.com/landing/2step/ (last visited Jan. 22, 2017); Seth Rosenblatt & Jason Cipriani, *Two-Factor Authentication (What You Need to Know)*, CNET, (June 15, 2015), https://www.cnet.com/news/two-factor-authentication-what-you-need-to-know-faq/.

99. *See Protections, How to Protect Your Computer*, FBI, https://www.fbi.gov/investigate/cyber (last visited Jan. 20, 2017).

100. *See e.g.,* Alex Castle, *How to Encrypt Almost Anything*, PC WORLD, (Jan, 18, 2013), http://www.pcworld.com/article/2025462/how-to-encrypt-almost-anything.html.

101. Pastore, *supra* note 15.

102. *See supra* note 99.

C. Taking a Thoughtful Approach to Assets and Architecture

As Pastore explains, determining what cybersecurity should be implemented turns on knowledge of one's "assets" and "architecture."[103] That is, what sensitive information do you have (e.g., customer lists of a client, sensitive trade secrets developed through substantial R&D expenditures, or potentially market-moving information about future business plans), and where do you store it (e.g., with a third-party cloud provider, on portable (and easily lost) external media like thumb drives, or on networks accessible by other practitioners in the firm without regard to whether the need access to such data).[104] This exercise will be relevant in respect to the arbitrator's own practice-related data, such as conflicts and billing records, closed case records, as well as the data received in matters where the arbitrator is presiding. If the arbitrator works in an organizational setting, it will also be relevant in respect to the arbitrator's use of personal devices, which are often not subject to established security protocols.[105]

Once the arbitrator knows and classifies the sensitivity of the different data he or she holds and knows where it is located, the arbitrator will be in a position to assess what protocols may be appropriate for storage and transfer of the information.[106] In addition, the arbitrator will be in a position to consider what steps can be taken to reduce the risk that sensitive data will be compromised in a cyberattack or following human error. For example:

- Though the arbitrator may own both a tablet and laptop, do arbitration-related documents need to be accessible on both devices, or is it sufficient that they are loaded on one? (Here,

---

103. In this article, we frequently refer synonymously to one's digital "infrastructure."

104. Pastore, *supra* note 15.

105. According to the ABA TechReport 2016, most lawyers (74%) use a personal rather than firm-issued phone for their legal work and a majority (51%) use a tablet for legal work, the vast majority of which (81%) are personal devices. Nonetheless, "only 43% of lawyers reported having a mobile technology policy for their firm, meaning the majority of law firms don't even have a policy for how mobile devices should be used and how client data should be stored and transmitted on them." Aaron Street, *Mobile Technology*, ABA TECHREPORT (2016), https://www.americanbar.org/groups/law_practice/publications/techreport/2016/mobile.html.

106. Pastore discusses this analysis in greater detail. *See* Pastore *supra* note 15.

an important consideration is whether the data really needs to be loaded onto a portable device and subjected to the enhanced risks of travel.)

- Can the arbitrator enable notifications for e-mail[107] or cloud services[108] when unauthorized data access may have occurred and remotely revoke that access or wipe data?
- When working at home, does the arbitrator use a separate device in lieu of a shared family computer? If not, are there other steps the arbitrator can take to segregate business data (e.g., by using separate computer logins)?

By the same token, at the conclusion of a case, the arbitrator should seek to avoid holding onto case-related data longer than is necessary.[109] With a view to developing an individualized document retention policy, the arbitrator should give thought to what information will be kept, why, for how long, where case information resides now (across which devices and in what applications/programs), and where the materials will be stored. At a minimum, the arbitrator will want to retain basic case administration data for the purposes of future conflicts checks. Otherwise, the arbitrator may wish to consider questions such as:

- During the life of a case, can the arbitrator use file-naming conventions to facilitate identifying and segregating types of documents, such as pleadings and exhibits, that the arbitrator is unlikely to have any interest in retaining after a case ends?
- Does applicable law preclude the arbitrator from retaining certain data or mandate that it be stored or disposed of in any particular fashion?

---

107. Such measures are generally not available for free consumer e-mail services. Thus it is generally preferable to use paid professional versions of these services, which have more robust security protocols.

108. Numerous lawyer ethics opinions have considered whether the use of cloud services is compatible with an attorney's obligation to maintain confidentiality. The decisions generally have concluded that lawyers may use the services, provided that they take reasonable steps to select a reliable vendor, implement available security and address the potential risks. *See* Cloud Ethics Opinions Around the U.S., AMERICAN BAR ASSOCIATION, https://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/cloud-ethics-chart.html.

109. Pastore, *supra* note 15.

- To the extent that it is desirable and appropriate to retain arbitrator work product, such as procedural orders and awards, for personal future reference, would it be workable to retain anonymized Word documents in lieu of final PDF copies?
- If the arbitrator practices in an organizational setting that has a document retention policy, are documents kept longer than necessary to comply with rules applicable to the attorney-client relationship, which do not apply to service as an arbitrator?

D. Planning for a Data Breach

Separate from considering data breach protocols for individual cases, there are a number of useful reasons for the arbitrator to consider more generally how he or she would respond to a data breach if and when one arises. First, by thinking through what steps should be taken in the event of various scenarios, the arbitrator may be able to identify and remediate security vulnerabilities that he or she had not considered. Second, the arbitrator will be in a better position to react quickly to control or limit the damage that flows from a security incident, and possibly avoid triggering duties to notify data owners, regulators, insurers, law enforcement, or others that a security incident occurred.[110] This exercise is particularly important for international arbitrators for whom international travel is a fact of life, as travel creates special risks of inadvertent data loss and vulnerability to unlawful intrusion.

---

110. *See, e.g.,* U.S. Department of Health & Human Services, *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA)*, https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/#_edn1 (last accessed Jan. 21, 2017) (explaining that there is often a safe harbor for data breach notification if sensitive information has been encrypted or otherwise de-sensitized); Kamala D. Harris, Attorney General California, Department of Justice, Breach Report 2016, *available at* https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf (last accessed Jan. 21, 2017) (explaining major differences between state notification statutes); *See* Cal. Civil Code § 1798.82 (demonstrating that in 2016, California amended its data breach notification law effective January 1, 2017 to trigger notification obligations not only if unencrypted data is compromised, but also if encrypted data is breached along with any encryption key that could render the data readable or useable).

The prospect of a lost laptop, for example, may prompt an arbitrator to consider:

- Is the laptop protected by a strong password?
- Is full disk encryption enabled?[111]
- Can the arbitrator make use of location tracking and/or remote data wiping to minimize potential disclosure of sensitive information?[112]
- Can the arbitrator provide the police with the serial number for the laptop?
- Can the arbitrator avoid lost productivity by restoring information on the laptop from a back-up?
- Is there sensitive data on the laptop that could trigger breach notification duties? If so, could that data be handled differently (e.g., securely destroyed or encrypted)?

E. Case Management Considerations

In our view, the arbitrator must be attuned to data security issues in the organizing phase of the arbitration. Taking into account such factors as the size and complexity of the case, the likelihood that confidential or sensitive data will be stored or transmitted, the parties' resources, sophistication, and preferences, as well as potential legal obligations arising under applicable law or rules in relation to data privacy or confidentiality, the arbitrator should consider whether to raise the topic of data security at the initial case management or procedural conference.[113] Thereafter, the continuing scope of the arbitrator's duty will depend on factors such as the extent to which the parties or their counsel assume responsibility for data security and the arbitrator's own assessment of the ongoing risks and the measures he

111. *See Turn On Full Disk Encryption (Windows 10)*, MICROSOFT, https://support.microsoft.com/en-us/instantanswers/e7d75dd2-29c2-16ac-f03d-20cfdf54202f/turn-on-device-encryption; *see also Use FileVault to Encrypt the Start-Up Disk on Your MAC*, APPLE, https://support.apple.com/en-us/HT204837.

112. These measures are available for Apple devices including laptops, for example, but only if the "find my iPhone" feature has been activated first.

113. *See* UNCITRAL Notes, *supra* note 26. Consistent with the 2016 UNCITRAL Notes on Organizing Arbitral Proceedings, we do not intend to suggest a binding requirement for the tribunal or parties to act in any particular manner.

or she can reasonably implement in addition to or in lieu of measures other actors are undertaking.

The arbitrator may also seek the cooperation of the parties and counsel in avoiding the unnecessary transmission of sensitive data to the tribunal. For example, at the outset of an arbitration, the arbitrator may consider telling counsel that, apart from reliance documents submitted with the parties' memorials, the arbitrator is not to be copied on, or provided with, any pre-hearing disclosure that the parties may otherwise exchange. Likewise, if the arbitrator can anticipate that sensitive personal information (such as tax returns) or commercial information (such as pricing information or trade secrets) will be exchanged, consideration may be given to having irrelevant information redacted (e.g., to show only the last four digits of a social security number). Alternatively, it may be possible to aggregate or anonymize data before it is provided to the arbitrator without diminishing either party's ability to fairly present its case.

VI. LOOKING TO THE FUTURE

We conclude this article with the well-worn maxim that "it takes a village." We hope that the challenge we present to arbitrators will stimulate discussion in the international commercial arbitration community and prompt other participants to focus on their own responsibilities and how their individual security architecture and practices may undermine or support the security measures taken by others. As awareness of cybersecurity risks in arbitration increases, we hope to see dialogue around questions such as the following:

- Should arbitral institutions amend their rules to flag data security for consideration in the initial organizing phase of an arbitration, as their rules now do with respect to other important topics,[114] and/or should they expressly establish

114. *See e.g.,* ICC RULES, *supra* note 10, at art. 22, (effective case management) and Appendix IV (case management techniques); ICDR RULES, *supra* note 10, at art. 20(2) (noting that the tribunal and the parties may consider how technology, including electronic communications, could be used to increase the efficiency and economy of the proceedings) and art. 20(7) (establishing the parties' duty to avoid unnecessary delay and expense and the tribunal's power to "allocate costs, draw adverse inferences, and take such additional steps as are necessary to protect the efficiency and integrity of the arbitration"); LCIA RULES, *supra* note 1, at art. 14 (avoiding unnecessary delay and expense) and art. 30 (confidentiality).

duties for the parties, counsel, institution and arbitrators to implement reasonable measures to avoid intrusion?

- Should counsel be charged with developing a data security plan in individual arbitration matters[115] and/or providing a secure platform for the transmission and storage of data in each matter?
- How should tribunals resolve party conflicts about appropriate security measures, breach notification obligations, and related costs?
- Should arbitrators routinely disclose their data security practices to parties and counsel (e.g., in relation to cloud computing or post-award document retention) and should those practices be subject to the parties' comments and consent?
- Should arbitral institutions or other participants develop shared secured platforms for data storage and transmission that would be available to parties as a non-exclusive choice?
- What kinds of training and education programs should be developed for parties, counsel, arbitrators, and other participants to provide baseline knowledge, as well as updated information on evolving data security threats and updates on available protective measures?
- Should institutions that maintain rosters of arbitrators require their arbitrators to complete mandatory cybersecurity training?
- Should arbitrator ethical codes be updated to define competence to include an obligation to keep abreast of new developments in arbitration and its practice, and to consider the benefits and risks associated with technology?
- Should professional organizations like the International Bar Association or the Chartered Institute of Arbitrators develop cybersecurity checklists or guidance notes for arbitrators, counsel, or other participants?

---

115. *See* David J. Kessler, et al., *Protective Orders in the Age of Hacking*, NYLJ, (Mar. 16, 2015), reprint at 1 ("In the age of cyber attacks, hacking, and digital corporate espionage… [p]rotective orders should be upgraded to require reasonable levels of security to protect an opponents' data and more stringent notification requirements if unauthorized access does occur . . .").

There will no right answer to these and other relevant questions, but we are confident that dialogue will be constructive. What will constitute a reasonable data security program and what reasonable measures individual participants in the process should take will continue to evolve. Our hope is that increased awareness will ensure that a process will emerge in every arbitration to identify data security risks and develop a response, having regard to the nature and scope of the risks, the desires and resources of the parties, and other relevant factors.