Kluwer Arbitration Blog

Arbitration Tech Toolbox: Training Arbitration Practitioners to Resist Cyber Attacks

Shatrunjay Bose and Hongwei Dang (CyberArb) · Sunday, October 2nd, 2022

> *"Dear Arbitrator,*
>
> *This is your hacker.*
>
> *You do not know me, but I already know you quite well. I am silently waiting for my opportunity to simply click and collapse your notebook.*
>
> *I have nothing against you; it is simply that you are a keeper of gold: DATA. And not any type of data; it is actually information from a company that you know as "Claimant". In fact, I have been trying for many months to build a supply-chain attack on Claimant… and guess what? I found that you are the weak spot into the company. Yes, you are the weak link in the chain as an external professional service provider.*
>
> *I discovered on social media that your favourite city is Rotterdam, and after a few clicks and noting your dog's birthday, I have your password! Unfortunately, you use almost the same password for your work devices too, so I already have access to your work notebook. You've also skipped the latest update of your operating system in your super interconnected phone – perfect, do not rush!*
>
> *Last but not least, I am still deciding if I should claim a ransomware to you directly or to the company instead. I will see how you work on your group paper, or the document titled "Award". Oh, and after checking your browser history, I see that you do not read or study anything about cybersecurity topics, suggesting that you are indeed my perfect target.*
>
> *Again, it's not personal – I just have to do my thing.*
>
> *Best of luck with your concurring opinion, I hope you can finish it before your nephew's wedding.*
>
> *Apologies, but YOU HAVE JUST BEEN HACKED!"*

Not all mail that you are surprised to see in your inbox results in a fairytale romance. To the contrary, the odds of that happening are likely to be quite low. Moving everything online, we have become perfect targets for hackers, increasing the risk of receiving a similar note. Such an email could indicate that you are actually hacked, or the email itself could be the beginning of the scam. As an arbitration community, we must get more resilient to cyber-threats.

Since the beginning of its activities in late 2020, CyberArb has aimed to provide practical tools and educational pieces, including its newly launched newsletter, to bridge the gap between theory and practice. To this end, CyberArb has partnered with ArbitrateUniversity.com to offer a new online training module on cybersecurity essentials in international arbitration, dedicated to all arbitration practitioners. The module begins with a brief introduction by **Karina Albers** (independent arbitrator, Chair of the London Branch of CIArb and member of CyberArb's Executive Board), who explains that cyber-attacks are a growing threat worldwide. The Covid-19 pandemic has compelled us to move to a hybrid work environment, one that relies heavily on the Internet and that results in an escalation of cyber-attacks. The international arbitration community has pioneered virtual hearings, which, on the one hand, have put parties at ease but, on the other hand, have made arbitral institutions and law firms especially vulnerable to cyber-attacks.

Soft Law Instruments to Promote Cybersecurity in International Arbitrations

The module includes input from **Shobana Iyer** (independent arbitrator, founder of Swan Chambers and member of CyberArb's Advisory Board), who shares her insights on the soft law of cybersecurity and international arbitration. The increase in the use of data, and advancements in technology such as videoconferencing and e-filing, have made cybersecurity a more pressing issue. The involvement of parties located in various jurisdictions using different technologies has created pressure on digital infrastructure, making it more vulnerable to cyber-attacks. Iyer highlights that any cybersecurity breach could result in reputational damage for the parties and arbitrators. This may also lead to issues in the enforcement of an award as such breaches would taint the data and confidentiality involved in the arbitral proceedings.

These risks have spurred the formulation of various soft laws in the form of guidelines and protocols in international arbitration. Such guidelines include the ICCA-NYC Bar-CPR *Protocol on Cybersecurity in International Arbitration* (the latest version of which was recently presented during the 2022 ICCA Conference in Edinburgh), which aims to increase cybersecurity awareness in international arbitrations and provide a framework for incorporating cybersecurity measures in arbitral proceedings; the AAA-ICDR *Best Practices Guide for Maintaining Cybersecurity and Privacy* (2020), which offers useful guidance to parties, their representatives and arbitrators concerning cybersecurity measures they should consider adopting; the CIArb *Framework Guideline on the Use of Technology in International Arbitration* (2021), which covers a series of principles on technology use and introduces best practice to ensure cybersecurity in arbitration; and the ICC Arbitration and ADR Commission Report on *Leveraging Technology for Fair, Effective and Efficient International Arbitration Proceedings* (2022), which contains a variety of resources to promote the safe use of technology in arbitration, including sample procedural language relating to technology tools, checklists for virtual hearings etc.

Implications for Admissibility of Evidence

Cemre Kad?o?lu (Ph.D Candidate at University of Leicester and member of CyberArb's Executive Board) discusses the consequences of cyber-attacks on arbitration. She analyses several important international arbitration cases to discuss the admissibility of evidence obtained through cyber-attacks. Kad?o?lu further touches upon the cost element of such breaches and the allocation of costs. Issues such as the role of arbitrators in cybersecurity challenges and the use of cybersecurity breaches as a guerilla tactic are addressed while relying upon existing international protocols and guidelines. These issues are not merely academic: in 2021, the defendant in a multibillion-dollar Brazilian ICC arbitration challenged the award on the grounds that the claimant had orchestrated a hacking of its servers and had thus gained access to confidential information during the arbitral proceeding.

Practical Tips to Enhance Cybersecurity Throughout Arbitrations

Uniquely, this module also includes the expertise of **Tony Gee** (an ethical hacker and Security Consultant at Pen Test Partners) who provides practical tips on how to be cyber secure at all stages of an arbitration. In particular, Gee recommends that arbitrators remain cautious and protect themselves from cyber-attack by, *inter alia*, using complex passwords with special characters and numbers; applying different passwords for different platforms; storing said passwords on a Password Manager; implementing multi-factor authentication; and keeping the systems and software of digital devices including computers and mobile-phones up to date. Gee also gives several tips on what to do if one experiences a real hack. For example, he advises that arbitrators should consider obtaining liability insurance for cybersecurity in advance, and should act rapidly to seek help from a service provider, such as an incident response company, if they experience a hack.

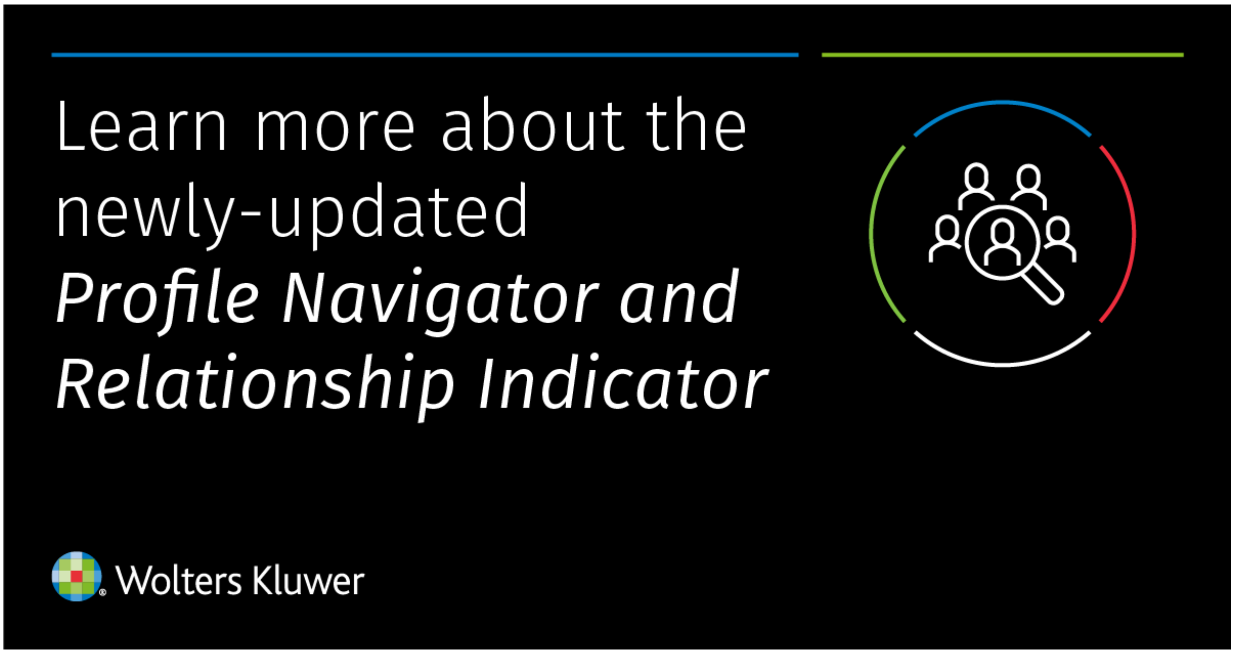
Any individual or institution involved in arbitral proceedings may become a target of cyber-attacks. Becoming aware of the threats and learning how to respond once faced with them is crucial not only to avoid cybersecurity-related problems but also to create a more robust arbitration community. The training course is a good first step to help practitioners get more knowledgeable about cybersecurity, build defenses against attack, and possibly avoid heartbreak along the way.

Readers wishing to learn more about CyberArb e-learning programs can contact CyberArb here.

Further posts on our Arbitration Tech Toolbox series can be found here.

The content of this post is intended for educational and general information. It is not intended for any promotional purposes. Kluwer Arbitration Blog, the Editorial Board, and this post's authors make no representation or warranty of any kind, express or implied, regarding the accuracy or completeness of any information in this post.

To make sure you do not miss out on regular updates from the Kluwer Arbitration Blog, please subscribe here. To submit a proposal for a blog post, please consult our Editorial Guidelines.



This entry was posted on Sunday, October 2nd, 2022 at 8:24 am and is filed under Arbitration Tech Toolbox, Cybersecurity, Soft Law Instruments, Technology
You can follow any responses to this entry through the Comments (RSS) feed. You can leave a response, or trackback from your own site.