Formula 1 Lessons for Cybersecurity in International Arbitration: The “CyberArb Roadmap”

Kluwer Arbitration Blog
March 27, 2021

Wendy Gonzales (CyberArb) and Mihaela Apostol (ArbTech)

Please refer to this post as: Wendy Gonzales and Mihaela Apostol, ‘Formula 1 Lessons for Cybersecurity in International Arbitration: The “CyberArb Roadmap”’, Kluwer Arbitration Blog, March 27 2021, http://arbitrationblog.kluwerarbitration.com/2021/03/27/formula-1-lessons-for-cybersecurity-in-international-arbitration-the-cyberarb-roadmap-2/

Both in Formula 1 and in international arbitration, small yet innocent mistakes can trigger significant risks. Lack of proper cybersecurity measures can lead to irreversible results with negative impact on all stakeholders involved.

In Formula 1 racing, the risk of danger is at every corner and one simple wrong move can change the outcome of the race. Although the driver is seen as the main actor, the success of the race and its safety is actually ensured by the seamless coordination of hundreds of team members which is made possible by (i) permanent monitoring; (ii) excellent team-work; (iii) routine pit stops; and (iv) fast intervention.

In this piece, we will first briefly address why cybersecurity matters, and secondly, we will analyze how the key lessons from Formula 1 can be transposed into the “CyberArb Roadmap” for arbitration proceedings. The overall goal is to provide readers with practical guidance in order to mitigate the risk of cyber threats.

Why cybersecurity matters?

The importance of information security has been acknowledged and promoted with more frequency by prominent organizations such as AAA-ICDR, especially during the last months as the world has swiftly moved into virtual operation and the number of attacks has exponentially increased. Starting with the ICCA-NYC Bar-CPR Cybersecurity Protocol for International Arbitration, followed by the Queen Mary 2020 International Arbitration Survey which addresses cybersecurity and data protection in their questionnaire, as well as the launch of the 2020 LCIA Rules which have a special section on Data Protection (Article 30A), all these recent initiatives show the increased interest of the arbitration community in cybersecurity and use of technology.

Being exposed to cybercrime can lead to economic losses, reputational damages and regulatory sanctions. A recent report from McAfee estimates that the global economic loss as a consequence cybercrime in 2020 was around $1 trillion, a simple calculation shows us that this represents over 1.1% of the world GDP, over $2.7 billion daily and almost $32 000 per second. Moreover, the annual cost is anticipated to reach $5.2 trillion by 2023. Unfortunately, no industry is untouched by the growing cost of cyber-attacks. The SRA (UK Solicitors Regulation Authority) reported that in the first half of 2020, nearly £2.5 millions of money held by firms had been stolen by cybercriminals (over three times the amount reported in the first half of 2019). When it comes to arbitration, readers are probably already familiar with the PCA incident from 2015.

In order to mitigate the risk of exposure to cybercrime in international arbitration, we have prepared below a “CyberArb Roadmap”, which points out the most critical measures to be integrated during the main stages of the arbitral proceedings.

Overview of CyberArb Roadmap – Formula 1 lessons

The following measures are developed around four key lessons from Formula 1 mentioned earlier. The aim is to provide a minimum, but not exhaustive, set of rules to be implemented and adapted based on the arbitration rules, the applicable law, the resources of the stakeholders involved and the state-of-the-art technology.

Permanent monitoring

Never be off guard. Every internet connection is a premise for a cyber-threat. From simple acts that we do out of automatism such as clicking on emails that have the name of the arbitrator (but a slight change of the address or domain), to accessing non-verified links to download exhibits attached to a submission, your account may then be compromised by a phishing attack. In case of doubt, make a phone call or reach the sender by other means for a second verification.

Excellent teamwork

Everyone can be a weak link. Usually when we think about the actors involved in arbitrations, we include the arbitrators, the parties, their representatives and the institution. But the web is very wide and complex: witnesses, experts, translators, librarians, video hosting providers, transcription providers, couriers, accounting team, IT team, printing team, document management team, and the list continues and could even include the neighbor who lends a laptop to a factual witness for a virtual hearing because it has a better camera. Essentially, anyone who uses their device for the arbitration cases through the internet can trigger an exposure that can impact all others involved. A cyber safe arbitration is thus highly dependent on excellent teamwork in which everyone takes precautions, and adequate guidance or training to all involved is required.

Routine pit stops

Do not wait for the risk to materialize before taking measures. Formula 1 drivers do not wait for the damage to materialize before going to a pit stop to fix it. Instead, they do routine pit stops and change tires before they are worn. Similarly, stakeholders involved in an arbitration should consider taking precautionary measures before a risk becomes imminent. It requires doing permanent checks and updating the measures already in place. Merely taking measures at the beginning of the arbitral proceedings will not suffice to eliminate the cyber-risk faced in an arbitration; routine checks up shall also be made throughout the entire process and even at the concluding phase.

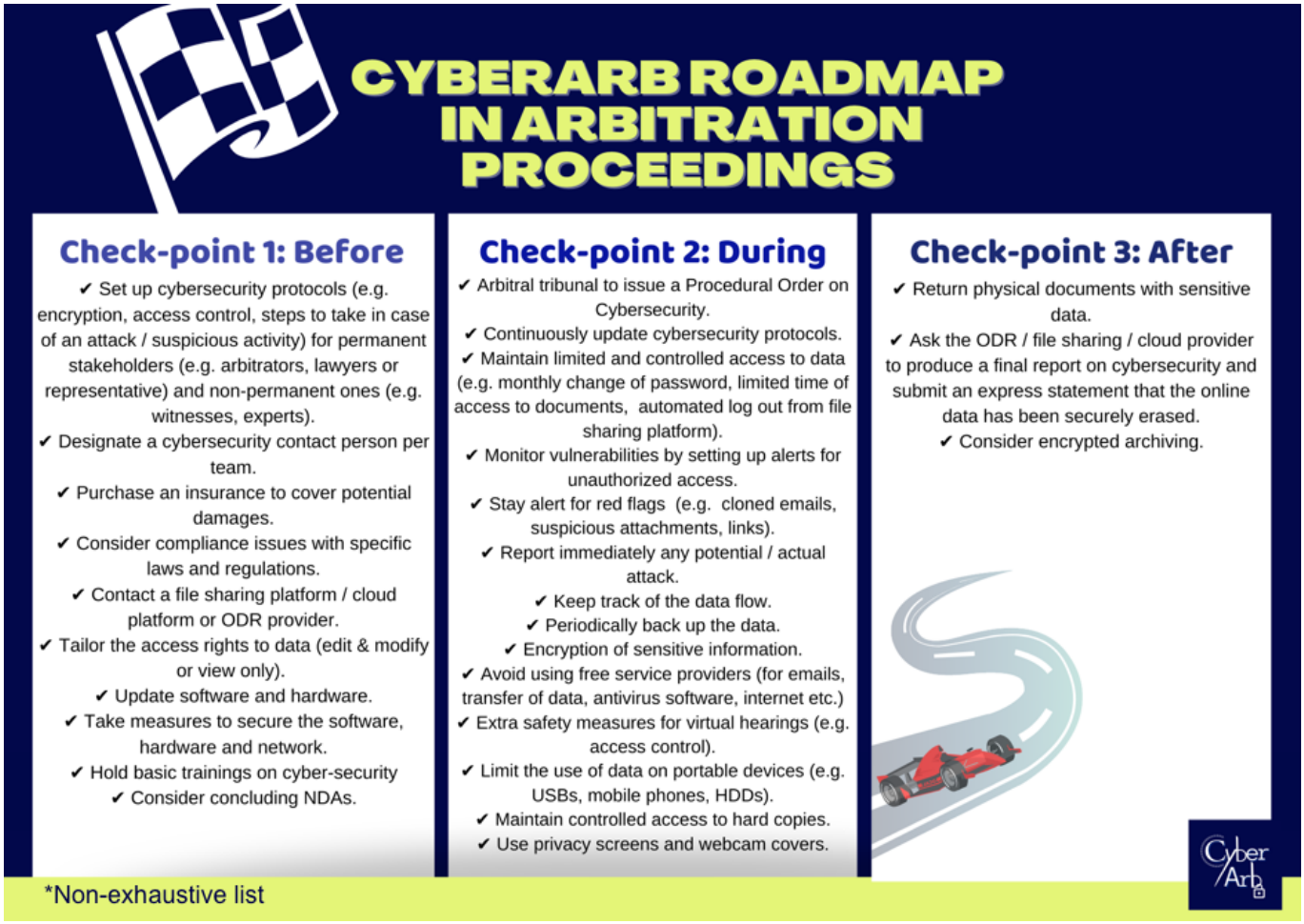
Fast intervention

Time is of the essence. Currently, the Formula 1 record of the shortest pit stop is of 1.82 seconds, and in general, a team intervention is around 2.4 seconds (during

which around 16 people would change all the tires and replace any damaged parts of the car). This incredibly swift intervention shows how vital time is for the outcome of the race. The same goes for exposure to cyber-attacks. Once an exposure happens, the longer it takes to tackle it, the more costly it will be to fix the damage. This requires teams involved to prepare in advance, protocols for interventions and to have a pre-established list of measures to mitigate potential damages.

All these key lessons should be kept in mind at all the stages of the arbitral proceedings.

When and how to apply them?



The first “check-point” which occurs before starting the proceedings lies mainly on the shoulders of law firms and arbitral institutions to establish internal protocols (guidelines/policies) to be observed during the proceedings, and to take the necessary administrative and logistical measures to safeguard cybersecurity. The

second “check-point” rests on the arbitral tribunal’s role to issue a Procedural Order on Cybersecurity aimed at preserving the major cornerstone of arbitration: confidentiality. Such Procedural Order template will soon be made by the CyberArb Team. Also, during the proceedings, all stakeholders should keep an eye out for potential red flags and continue to update the policies in place. The last “check-point” is meant to make sure that data are safely kept once the proceedings are concluded.

Concluding remarks

Cybersecurity requires a joint effort from all stakeholders in international arbitration due to its complex nature and multi-gates risk. Since there cannot be a one-size-fits-all solution, the CyberArb Roadmap comprises a general non-exhaustive list of suggestions that could help to mitigate the impact of cybercrime through monitoring, teamwork, routine checks and quick intervention. However, stakeholders are encouraged to develop tailor-made solutions in collaboration with cybersecurity experts in line with the mandatory regulatory requirements specific to the relevant jurisdiction.