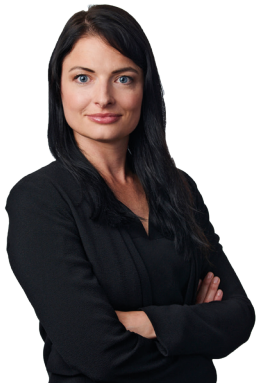

Welcome to the new interview of "Digital Coffee Break in Arbitration" by Svenja Wachtel. I am an attorney and arbitrator in the field of international arbitration and the founder of Digital Coffee Break in Arbitration, an initiative creating a debate around digital transformation in international arbitration. In this series, I discuss the latest trends in the field, covering topics such as the use of technology, digital transformation, and digitalization. Digital Coffee Break in Arbitration invites you to grab a drink, sit back and enjoy first-hand insights from General Counsel, arbitrators, legal scholars and other practitioners from all over the world of international arbitration.

Today, I will talk to Wendy Gonzales. She is the founder of CyberArb.com, a non-profit and global initiative to mind the gap between cyber security and arbitration/ADR. She is certified by University of Oxford's Saïd Business School Programme on Cyber Security for Business Leaders as well as on the pathway certificate by the Chartered Institute of Arbitrators (CIArb). She is an active member of Women4Cyber as well as Steering Committee Member at Silicon Valley Arbitration & Mediation Center (SVAMC)-YP. She is currently leading legal counsel (focus on ADR and Cyber) at a Tech-Multinational. Wendy is based in the Netherlands, while having Peruvian and Spanish roots.

In this episode, we will discuss cyber security in international arbitration and the obstacles and responsibilities the use of technology entails.

Thanks so much for joining me, Wendy! Technology and the use of technology is at the core of this interview series, so it is about time to address cyber security in international arbitration. You are a specialist when it comes to cyber security. What do we usually mean, when we talk about cyber security?

Cyber security is like a house, we have doors and locks to protect what matters to us. Not only on the front door but on every floor of the house. Nobody leaves their door open when leaving for holidays. Same for arbitration practitioners, it is a paramount to safeguard the so-called "CIA triad" – confidentiality, integrity and availability of all the data trusted by their clients in this digitized era. Data has to be understood as "reference data" (touching lines with personal data) and "business data" (such as trade secrets).

You are the founder of CyberArb which links cyber security and international arbitration. What is the idea behind CyberArb and what does it imply?

CyberArb implies opening the eyes to a topic avoided for too long. CyberArb started as a pandemic initiative when arbitration - as many other industries – was forced to accelerate its digitalization (i.e. virtual hearings). CyberArb is an initiative with a multi-disciplinary and international legal & tech team. Indeed, as volunteers, we are legal practitioners as well as engineers with expertise in cyber security. Our team is committed to (i) raising awareness and providing practical guidance in mitigating cyber risks, (ii) developing practical tools such as roadmaps, annotated procedural order templates, e-learning, workshops, blog articles, podcasts, and others, and (iii) promoting a proactive debate to develop best practices and foster an alternative dispute resolution system aligned to the digital era.

How did you become interested in cyber security yourself?

Working as a lawyer in the global technology industry for a few years, cyber security is a recurrent topic. However, it is not a popular topic in many industries (including ADR). The cyber threat landscape is increasing every second with the current digital dependency of individuals and companies. So the cyber harm propagation can be extremely damaging while cyber trust is crucial for business innovation worldwide. I found that my mission was to mind the gap and connect legal & cyber, which is one of the challenges of our times.

How tech-savvy are you and how much knowledge is required to provide for sufficient protection?

I don't know how to play video games and I do not like shopping online. I prefer to get surprised when I go to a physical shop. So I am sure there are more tech-savvy people than me. However, I am extremely passionate about the topic as cyber security and law are literally everywhere. Nobody has to be an expert, just to keep good cyber hygiene, same as locking the doors of your house. The truth is that 100% digital security or sufficient protection does not exist. At this stage of digital transformation or 4th Industrial Revolution, it is not a matter of "if" but "when" a hack will happen. Where you can be a target or simply on the way to the target. Once accepting this fact we can move forward to prepare and get ready. As, for example, when there is an earthquake or fire. We train for it. For this reason, I invite everyone to visit the CyberArb Academy for tailor-made cyber security e-learning for arbitration practitioners in collaboration with ArbitrateUniversity.com, as well as the other projects promoted by CyberArb with different partners such as Women4Cyber-SP.

"CYBER SECURITY IS LIKE A HOUSE, WE HAVE DOORS AND LOCKS TO PROTECT WHAT MATTERS TO US."

What is a typical scenario of a cyber attack?

The attack taxonomy or types of attack will depend on the target and result (i.e. companies and ransomware accordingly). In any case, cyber threats might be mostly related to systems or humans. For instance, a cyber attack could happen if an employee does not update the operating system of the laptop when working from home or a malware/virus produces a supply chain attack to a whole group of companies. In general, the weakest link is still humans so cyber criminals could get a "copy of the house's key" by obtaining access with social engineering and phishing to employees or arbitration practitioners, for example.

A few years ago, some major law firms were targeted in cyber attacks. Are cyber attacks a real threat for international arbitration too?

Yes, of course. The increase ransomware attacks (a kidnapping of company data) is unstoppable due to its high profitability for cyber criminals. We cannot eliminate international arbitration from the direct or indirect targets of cyber attacks. International arbitration proceedings are at risk of cyber attacks. Potential attackers may have different interests. They might be after confidential and highly classified information, trade secrets. They might be interested in revealing the names of the parties. Or they know that large companies with money are involved and they want to demand ransom or simply collapse their systems with a supply chain attack.

Who is the usual target of a cyber attack? Is each arbitration equally endangered to become a target of a cyber attack?

We cannot say it for sure. As mentioned, that is because we do not know what hackers or attackers want in general. There are different types of people that go about hacking. They can be "hacktivists", "state actors" and "criminal actors". They might be interested in making a statement against their government as much as obtaining financial gain. So, investment arbitration, state-state arbitration or commercial arbitration… they are all vulnerable when it comes to cyber security.

"THE TRUTH IS THAT 100% DIGITAL SECURITY OR SUFFICIENT PROTECTION DOES NOT EXIST."

How do I know if there was an attack on the arbitration proceeding?

This depends on the type of the attack. The sophistication of current attacks could allow hackers to be invisible on your systems and proceedings for a while until they define their target. Once you are officially a target, you possibly get a message telling you that you've been hacked and giving you directions to pay a ransom in cryptocurrency. There will be certain interruptions, if this was targeted at the proceedings to obtain certain information or gain. It is also possible to have your passwords changed, you may not be able to access certain platforms, your computer may

start acting a little bit weird having pop-ups or tabs being opened up. You may receive messages from your contacts saying that they were getting random notifications from you. Of course, these are just a few examples.

In a recent proceeding, a São Paulo court has stayed a partial award in a multibillion-dollar ICC dispute over the sale of a pulp maker. The reason was that the court considered allegations that the arbitration has been tainted by cyber hacking (see Global Arbitration Review, Brazilian pulp award leads to cyber hack challenge, April 12, 2021). Can you provide more details to this proceeding and what do we learn from cases like this?

In this case, Respondent found malware in its servers and alleged that Claimant hacked into its servers and revealed confidential information. At that time of the proceedings, there was a partial award and the Respondent challenged that award. Tribunal disregarded the challenge and found that there was no material harm. This led to the Respondent's request for disqualification. Later on, Respondent asked for the stay of enforcement proceedings arguing that the entire process was tainted. The court stayed the enforcement because it found that the arbitrator did not reveal its ties with Claimant.

"WE SHOULD STRICTLY ENSURE SECURITY SO THAT IT CANNOT INTERRUPT THE PROCEEDINGS."

This case shows something important. Cyber attacks may create effects that are beyond asking ransomware. A cyber attack may taint the proceedings by impacting the evidence or casting shadows on the impartiality of the arbitrators. However, the coin has another side. Just as we see with due process breach allegations, we may see cyber security breaches used as a strategic tool. Well, this does not mean that we should overlook cyber security. Quite the opposite! We should strictly ensure security so that it cannot interrupt the proceedings.

Is any additional case law out there dealing with the consequences of a cyberattack in an arbitration?

The Brazilian pulp case, as you mentioned, is an example. The other case laws that we are aware of do not particularly deal with cyber attacks but they rather address the issues of admissibility of evidence that is at the hands of the other party through illegal means. These cases are valuable to draw lessons as to the application of law to current issues involving cyber attacks. For a detailed discussion, I strongly urge our listeners to have a look at the article titled Consequences of Cyberattacks in International Arbitration published by TDM by co-authors of CyberArb leadership such as Sophie Nappert and Cemre Kadıoğlu.

Who in an arbitration proceeding is responsible to ensure that the appropriate security measures are in place?

That is something that we try to emphasize from CyberArb. Cyber security involves everyone. Everybody and every entity involved in the proceedings may become responsible for a cyber security breach. The consequences, of course, would have a direct impact on the parties, the award, and the course of the proceedings including the taking of evidence and challenge of arbitrators. The law firms or arbitration institutions or IT/technical service providers for the proceedings would also need to face the consequences as it will result in loss of trust, consumers and eventually, market share. So, everybody should take care of their cyber security.

Within the proceedings, we believe that this should be a joint effort of the parties and the tribunal. We advise them to have procedural order. For arbitrators, it is a good idea to keep track of their online identity in addition to security measures. CyberArb has a checklist for that as well. However, Arbitral Institutions are in a strategic position to take the leadership on the topic, not the responsibility.

What are the crucial and basic security measures that need to be implemented?

Security measures should be intact before, during and after the proceedings. And this should not be a one-time thing. Our CyberArb Roadmap suggests actions for each step. For instance, before the proceedings there should be cyber security protocols such as encryption, steps to take in case of an attack etc., all software and hardware should be updated, there should be a contact person for cyber security, and basic training can be held, and you can think of purchasing insurance. During the proceedings, we suggest following the

procedural order, limiting the access to data, keeping track of the data flow and continuously updating the cyber security protocol. After the proceedings, all documents with sensitive data should be returned, and all data could be achieved with encryption or securely deleted. This is just a caption of what can be done. The list is non-exhaustive as cyber security is a moving target! For more good practices, CyberArb Academy can provide further insights.

You mentioned the e-learning program "CyberArb Academy". Who is the right person to attend the workshop and what are the skills to be learned?

Yes. CyberArb has been partnering with ArbitrateUniversity.com and it is returning with an updated training session, which we put together considering the suggestions and critiques. Anyone who wants to learn more about cyber security in arbitration, consequences of cyber security breaches and tricks to avoid those are very welcome to attend the workshop. However, we believe it is particularly attractive for arbitrators.

The International Council for Commercial Arbitration ("ICCA"), the New York City Bar Association ("NYC Bar") and the International Institute for Conflict Prevention and Resolution ("CPR") established a Working Group on Cyber Security in Arbitration in April 2018. The Working Group released the 2020 Cyber Security Protocol for International Arbitration. What are the most important findings of the report?

This protocol is a good starting point which has to be regarded with the daily developments on the cyber security field. Schedules of the report are very informative and practical. The risk factors involved, in particular arbitration and sample languages to be adopted in an arbitration agreement, are really valuable.

Are there any guidelines on how to establish reasonable and sufficient security measures?

There are several technical guidelines and standards such as ISO27000 and NIST Cybersecurity Framework; however, they might be difficult to digest for non-technical profiles. Considering them as well as many other industry guidelines such as the 2020 Cybersecurity Protocol mentioned above, CyberArb is committed to help and mind the gap making the content simple and visual. As part of our toolkit, we also offer Template Procedural Order, CyberArb Roadmap for Proceedings, a Checklist for Arbitrators' Online ID, and e-learning programs as mentioned.

How can one stay up to date and make sure not to miss relevant updates?

"SECURITY MEASURES SHOULD BE INTACT BEFORE, DURING AND AFTER THE PROCEEDINGS."

There are good resources out there. The protocols and guidelines are being developed by the institutions and working groups. I also recommend following cyber security channels on LinkedIn or even the podcasts. We are too busy to invest our time in something that is not our day-to-day job. Well, cyber security should be our focus but for saving time, organizations like CyberArb are doing the job for you to highlight the most important things that you should pay attention to as in our regular LinkedIn Newsletter.

What do you expect to see in the future in terms of cyber security?

Cyber security will become our daily bread even more. From our smartwatches (IoT) to the double-edged sword AI joining cyber threat intelligence systems to fight cyber criminals. Without even considering our digital interactions at the metaverse level. More cyber adventures are to come but with few experts in the field, so a great new area of professional opportunities. So people/organizations who will be ahead must join forces with CyberArb to mind the gap together. Then, the team of CyberArb and its Board (Karina, Carolina, Cemre, Katherine, Ariana and Wendy) will be delighted to meet you, just email us at info@cyberarb.com

Thanks for joining me Wendy!