CYBERSECURITY RISKS IN ARBITRATION

QUERITIUS

Kyiv Arbitration Days

20 December 2024

Dragana Nikolić (Counsel)

Budapest | Kyiv | Warsaw | Zagreb

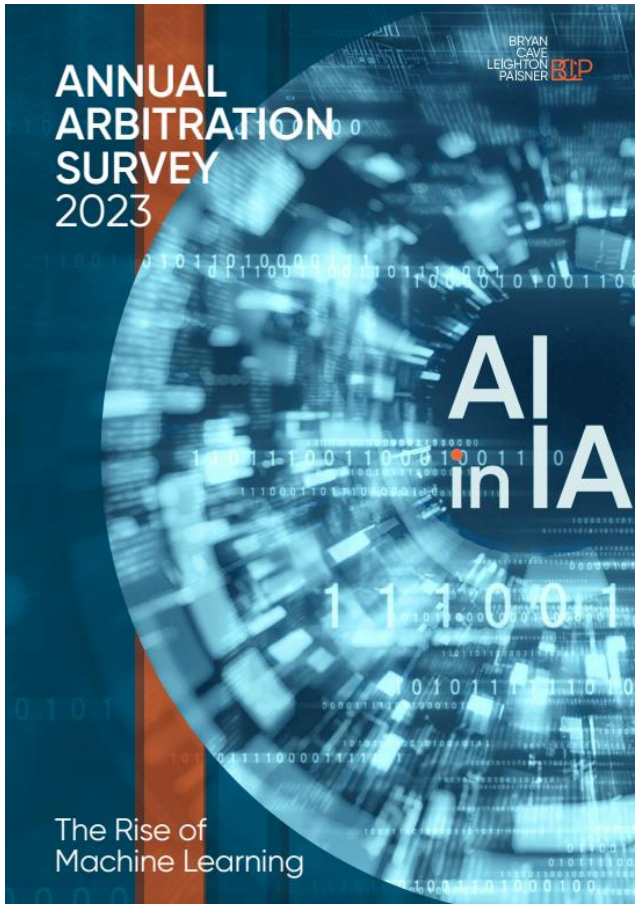
Cybersecurity Risks in Arbitration

- Why They Are Important?
- How to Recognize Cybersecurity Risks?
- How Common They Are?
- How to Prevent Cybersecurity Attacks?
- Way Forward?

Importance of Cybersecurity in International Arbitration

- **Definition**: Protection of digital data from theft, misuse and damage
- **Problem**: Arbitration proceedings are attractive targets for cyberattacks
- **Key aspects**: Confidentiality, data transmission, emerging technologies
- **Targets**: Parties, lawyers, arbitrators, tribunal secretaries, arbitral institutions, witnesses, supporting vendors
- **Consequences**: Business risks, private data leaks, criminal activities, national security threats

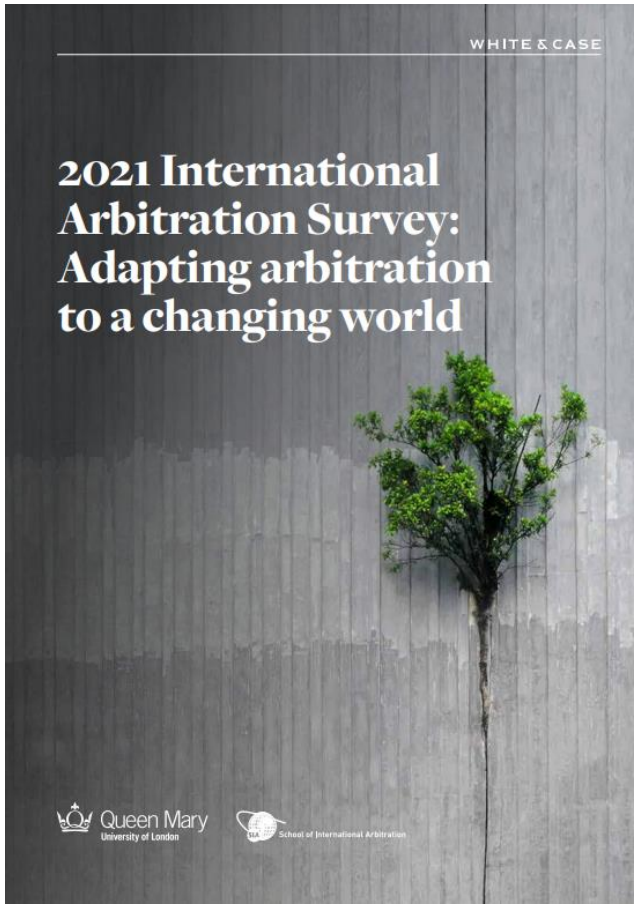
Importance of Cybersecurity in International Arbitration



BCLP

	VERY CONCERNED	SOMEWHAT CONCERNED	NEUTRAL	NOT CONCERNED	DON'T KNOW
Cybersecurity	38%	50%	8%	3.5%	0.5%
Breach of confidentiality	45.5%	42%	8%	4%	0.5%
Lack of transparency about the internal working of the technology	41.5%	37%	16%	5%	0.5%
Bias in the internal working of the technology	39%	35%	19%	6%	1%
AI Hallucination: risk of the technology conjuring up fictitious information	55%	33%	7%	3%	2%

Importance of Cybersecurity in International Arbitration



[Queen Mary]

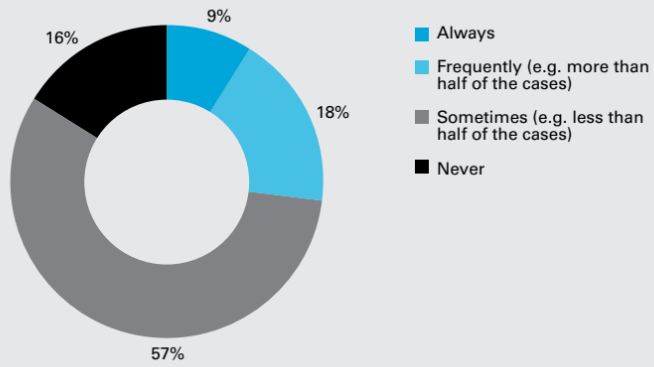
Only around a quarter of respondents said they have 'frequently' or 'always' seen cybersecurity measures being put in place in their international arbitrations. The majority (57%) encountered such measures in less than half of their cases.

Between a quarter and a third of respondents selected 'confidentiality and cybersecurity concerns' (30%) and the view that it is 'more difficult to 'read' arbitrators and other remote participants' (27%).

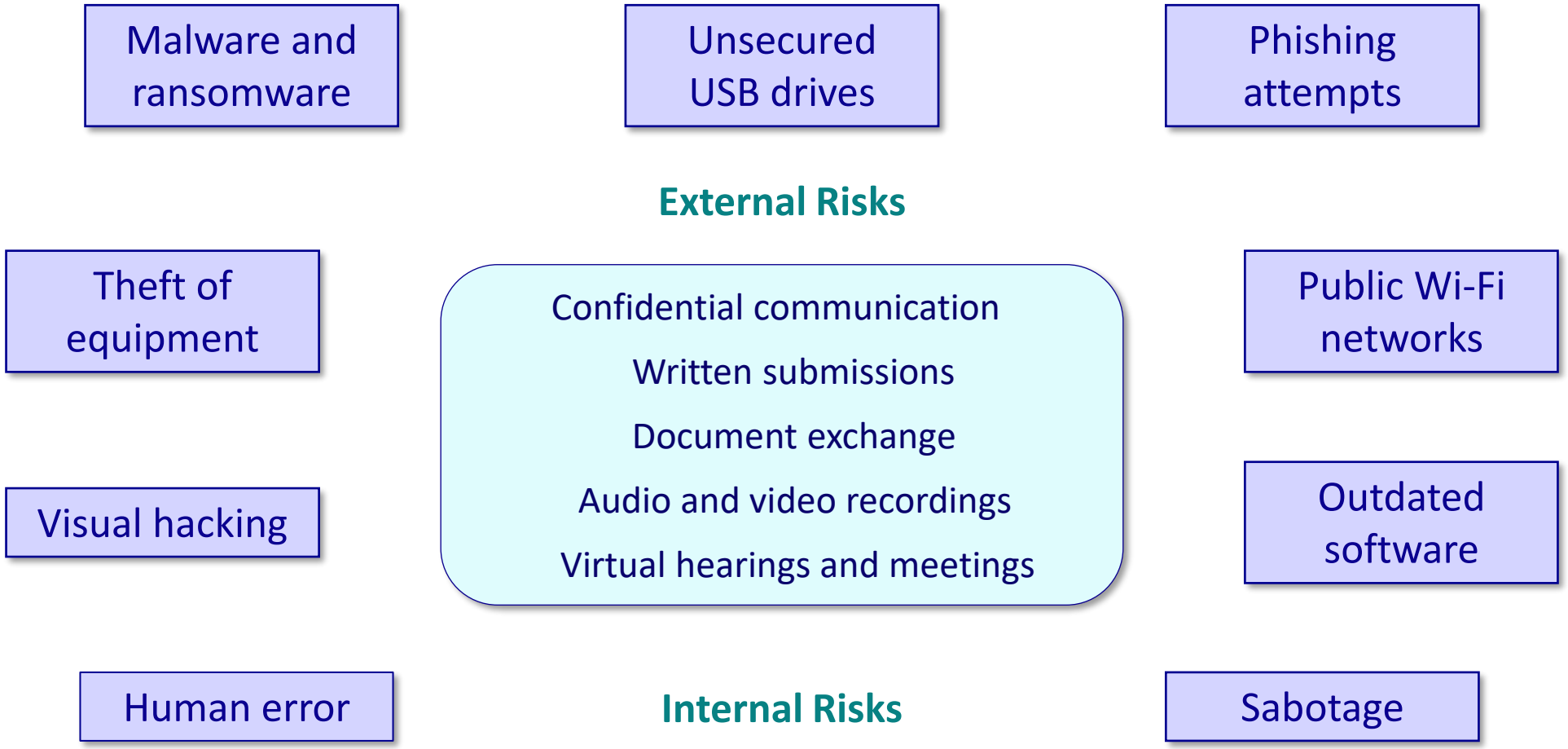
27%

of respondents have seen **cybersecurity measures** used in more than half of their cases over the past three years

Chart 21: In your experience over the past three years, how often have measures been put in place to protect the confidentiality and security of electronic or electronically submitted data in an international arbitration?



Cybersecurity Threats in International Arbitration



Cybersecurity Attacks in International Arbitration

- *The South China Sea Arbitration* (PCA website attack in 2015)
- *Caratube v. Kazakhstan II* (ICSID Case No. ARB/13/13)
- *ConocoPhillips v. Venezuela* (ICSID Case No. ARB/07/30)
- *Libananco Holdings Co. Limited v. Republic of Turkey* (ICSID Case No. ARB/06/8)
- *Gela Mikadze et al. v. Ras Al Khaimah Investment Authority et al.* (SCC Case No. V 2018/021)

Initiatives to Reduce Cybersecurity Risks in International Arbitration

- IBA Cybersecurity Guidelines (2018)
- ICC Leveraging Technology for Fair, Effective and Efficient International Arbitration Proceedings (2022)
- ICCA-NYC Bar-CPR Protocol on Cybersecurity in International Arbitration (2022)

Practical Tips to Reduce the Cybersecurity Risks

Pre-arbitration phase

- Preliminary risk assessment
- Internal cybersecurity protocols
- Cybersecurity clauses

Arbitration

- Cybersecurity due diligence
- Agreed measures (procedural orders or separate protocols)
- Expert instructions
- Terms of engagement of service providers
- Organizational checklists for virtual hearings

Post-arbitration phase

- Document destruction
- Encrypted archiving

RECOMMENDATIONS

Antivirus software

Encryption

Multi-factor authentication

Remote access protocols

Communications security

Confidentiality clubs

Audit logs

Anonymization

Backup and recovery procedures

Emergency response plans

Cybersecurity Risks in Arbitration

THANK YOU FOR YOUR ATTENTION!

Dragana Nikolić

dragana.nikolic@queritius.com