Article Information

Authors: McKenzie Moore, Tudor Filaret
Service: Arbitration, Commercial Disputes, Construction Litigation, Cyber Security, Dispute Resolution & Litigation, Intellectual Property & Technology
Sector: Electricity & Gas Regulation, Energy & Resources, Financial Services, Government, IT & Telecommunications, Mining, Oil & Gas, Power & Utilities, Renewables

---

Mitigating cyber security threats in international arbitration

As the prevalence of malicious cyber attacks on government, international and private organisations have become more profound, parties and practitioners involved in commercially and politically sensitive international arbitrations have expressed concerns about cyber security.

Advantages of arbitrations eroded by cyber security threats

Parties in a legal dispute may choose to commence arbitral proceedings to benefit from a number of procedural advantages. Parties involved in commercially and politically sensitive disputes however are likely to choose arbitral proceedings due to the confidentiality and privacy benefits it offers. But in today's environment, there is a real risk that these types of advantages can be altogether eroded by the profound and growing risk of cybersecurity attacks. Failing to protect the information collated, shared and retained in high-stakes and sensitive arbitrations could lead to the damage to the reputation of parties, liability under regulatory frameworks (including data protection regimes) and violation of the independence of arbitrators.

Arbitrations between governments and other private parties which transcend borders are not publicised, and often involve an exchange of classified government information and business trade secrets. This makes arbitrations a prime target for hackers. With law firms being one of the top four targets for cyber security attacks (according to a 2019 report by the Office of the Australian Information Commissioner), parties to international arbitrations have a right to be concerned about breaches of privacy and confidentiality.

How does one respond to cyber security threats?

To mitigate and respond to the growing cyber security concerns, parties may wish to consider implementing cyber security protocols in their arbitration agreements. One such protocol which was released in December 2019 for consideration is the *Protocol on Cybersecurity in International Arbitration* (**PCIA**). The purpose of the PCIA is twofold:

1. To provide a framework to determine reasonable information security measures for individual arbitration matters, including identifying the risks and measures that may be implemented to address these risks; and
2. Increase awareness about information security in international arbitrations.

Although the PCIA was prepared specifically for international arbitrations, it may also be a useful reference for domestic arbitration matters.

The PCIA is broken down into fourteen principles. Principles 2 and 6 bear the highest relevance on what parties must do and consider to manage and mitigate cyber security risks. It suggests that the consequences of a breach should be considered when deciding the risk profile of an arbitration, including:

1. risks of potential injury caused by loss of confidentiality, availability, integrity or authenticity of the information
2. risks to the integrity of the arbitration proceeding; and
3. financial loss, loss of privacy, destruction of value from release of confidential or proprietary data, injury to reputation or privacy of natural or legal persons, exposure of confidential, secret or proprietary data.

Principle 2: Baseline information security practices

Principle 2 of the PCIA mandates that each party, arbitrator and administering institution should consider the baseline information security practices (by reference to Schedule A of the PCIA). Schedule A of the PCIA outlines a number of suggested obligations, including:.

1. **Asset management** – which includes identifying categories of sensitive data and taking steps to minimise and protect the data, such as establishing document retention and destruction policies.
2. **Access controls** – such as considering password change intervals and user access to exchanged documents.
3. **Security for communications and encryption** –such as using secure share file services and avoiding attachments to emails and considering encryption standards and avoiding unsecured Wi-Fi connections.
4. **Information security incident response** – such as putting into place an information security response plan

Schedule C to the PCIA includes suggested wording to give effect to the information security practices in Schedule A.

Principle 6: Factors parties should have regard to when implementing cyber security measures

Principle 6 of the PCIA functions in tandem with Principle 2 and addresses factors parties and arbitrators should have regard to when assessing and mitigating cybersecurity risks (with reference to Schedule B of the PCIA). Principle 6 assists parties in understanding and evaluating the security risks factors presented in an arbitration, such as:

1. **Nature of the information** – including personal data will be processed (and whether this data is regulated or protected), and whether data is subject to express confidentiality agreements
2. **Subject–matter of the arbitration** – considering whether it involves parties to the arbitration handle large amounts of high-value confidential commercial information and/or classified government data, and whether it involves any public figure, high ranking official executives or celebrities
3. **Other matters** – such as the industry, subject-matter of the dispute, whether the matte is likely to attract public or media attention, quantity of confidential or sensitive data, and the nature and frequency of events that increase the risk of the breach

How does one implement the PCIA?

If parties wish to expressly implement the PCIA, the PCIA suggests the following language would be appropriate for inclusion in the arbitration agreement to achieve that end:

The Parties shall take reasonable measures to protect the security of the information processed in relation to the arbitration, taking into consideration, as appropriate, the ICCA-NYC Bar-CPR Cybersecurity Protocol for International Arbitration.

Conclusion

Although international arbitration offers the key advantage of confidentiality and privacy, this can be eroded by substantial cyber security threats. Accordingly, implementing information security measures such as the PCIA could help ensure your next arbitration maintains the advantages of confidentiality and privacy.

Key Takeaways

- With the growing threats in cyber security, parties to politically sensitive and high-value commercial arbitrations should consider implementing protocols to mitigate cybersecurity threats
- The *Protocol on Cybersecurity in International Arbitration* can be used to mitigate cybersecurity threats and preserve the confidentiality and privacy of an arbitration