INSIDE ARBITRATION: CYBERSECURITY MATTERS: ARBITRATION AWAY FROM PRYING EYES

16 July 2019 | Global
Legal Briefings

One of the many reasons that companies choose to resolve disputes through arbitration over court litigation is the ability to keep their disputes and the outcome of their disputes private. Arbitration is often chosen to resolve highly sensitive disputes, and being a truly international dispute resolution process, a single arbitration can involve participants from across the world.

Within the arbitral process those participants are likely to exchange information that is not in the public domain. That information may have the potential to cause commercial damage, influence share prices, corporate strategies or even government policy. The outcome of an arbitration could have significant repercussions in the financial markets, particularly for a listed company.

While arbitration is not on many client's radar as a potential source of cybersecurity risk, in reality the arbitral process is an obvious and attractive target for cyberattacks, particularly if hackers can identify a weak link in the chain of custody.

HOW CAN MY DATA BE TARGETED?

With so much information stored or transferred electronically, almost anyone and any organisation is susceptible to a cyber-attack.

The primary targets in international arbitration include:

- law firms acting as legal advisers, advocates or local counsel;
- past, present and prospective arbitrators whether in sole practice, in chambers or as a partner in a law firm;
- arbitral institutions;
- parties to disputes; and
- third parties holding information on any of the above, including experts, witnesses and service providers (the Participants).

Legal advisers and their clients generally share information and discuss drafting points and strategy by email. Pleadings, evidence, expert reports and witness statements are also often exchanged electronically with arbitrators, the other side's legal advisers, experts, witnesses, arbitral institutions and third party service providers. Document review and production regularly takes place on electronic data hosting platforms, usually owned by third party service providers. An award will be drafted, discussed and exchanged between the different members of an arbitral tribunal and may also be sent to the arbitral institution administering the arbitration, before being sent to counsel and the parties.

Each custodian represents a fresh target for cyber attackers and a potential point of weakness in relation to the security of arbitration data. Once data has been sent electronically in the course of an arbitration, the sender can no longer monitor or ensure its security. Law firms, particularly larger international law firms, have high levels of cybersecurity to protect their clients' data. Yet they can still be the target of cyberattacks. In 2016, three men were charged with making over US$4 million from insider trading with information stolen from the M&A teams of New York law firms. The perpetrators stole emails from partners who worked on the deals, bought shares in the target companies and then sold those shares after the deal was announced to the market. Accessing information that is otherwise held privately in the context of an arbitration may present similar appeal for hackers.

Arbitral institutions have access to a flow of data between a large number of parties and access to a steady stream of awards before they are issued, making them another obvious target for cybercriminals. There is precedent for successful attacks on arbitral institutions too: in 2015, the Permanent Court of Arbitration's website was hacked on the third day of a hearing involving a territorial dispute between the Philippines and China over the South China Sea.

Other participants, particularly those who are less likely to have implemented advanced cybersecurity measures, may also be seen as attractive targets for attack. While some arbitrators operate from within law firms or chambers, others are sole traders who may have in place more limited cybersecurity protections. The same could be said of expert witnesses and some fact witnesses who receive and store data on their personal devices. Careful consideration needs to be given by all stakeholders in an arbitration to avoid such participants being a weak link in the chain of custody.

WHO MIGHT WANT YOUR ARBITRATION DATA?

- Hacktivists are individuals or groups seeking to further a social or political cause. Depending on the subject matter of your arbitration, they might try to encourage environmental, economic, social or political reform and search for information they can use to advance their goals.

- State Actors pursue information to advance their own political agenda. In Libananco Holdings Co Ltd v Republic of Turkey the respondent state intercepted a number of the claimant's privileged emails through a money laundering investigation separate to the relevant arbitration proceedings.

- Cybercriminals generally perpetrate cyberattacks for monetary gain, either holding information for ransom or stealing information and selling it on to interested third parties. In 2016, a Russian cybercriminal was believed to have targeted 48 elite law firms in the United States to steal mergers & acquisitions information for the purposes of insider trading. Obtaining a draft form of an arbitral award before release to the parties themselves could be very lucrative for cybercriminals.

- Another potential source of cybersecurity threats are opponents in international arbitration proceedings. It is possible that commercial or individual parties to arbitration might attempt to obtain information unlawfully against their opponents to gain an advantage in the dispute resolution process.

WHAT MIGHT BE THE CONSEQUENCES OF A CYBERATTACK FOR A PARTY TO ARBITRAL PROCEEDINGS?

Cyberattacks may have severe legal, financial and reputational consequences for any party in relation to which (or whom) data is exchanged in arbitral proceedings.

Research published in 2018[1] analysed the long and short term share price effects of data breaches. The research found that the share prices of companies that had been hacked suffered in the short term following a data breach, hitting a low point after 14 days of trading (dropping -2.89% on average and underperforming the market by -4.6% over that period). In the long term, such a company's share price underperformed in the market by -3.7% (1 year), -11.35% (2 years), and -15.58% (3 years).

Damage caused by cyberattacks is not limited to share value. The breached data is likely to relate to one or more of the parties involved. It may be confidential or commercially sensitive information that was not intended to be shared with the wider market. It may be politically sensitive material which may show the party in a less favourable light and may cause considerable reputational damage to that party if leaked. The party whose data has been breached may also find themselves facing claims from other parties or individuals who are not involved in the arbitration but who were mentioned or discussed in the breached material.

[1.] Paul Bischoff, 'Analysis: How data breaches affect stock market share prices (2018 update)', Comparitech, 6 September 2018

Data flows in arbitration for one side

PRE-ARBITRATION OR ON RECEIPT OF REQUEST

1. INITIAL CYBERSECURITY RISK ASSESSMENT

Before commencing an arbitration (claimant) or immediately upon notification of commencement (respondent), the party in question and their legal advisors should consider carrying out a risk assessment into whether any commercially sensitive data is likely to be relevant to the dispute and what approach should be taken to the collation, storage and review of that data. A discussion should be had about whether access to that data, any particular pieces of information, the fact of the arbitration or its outcome could have a significant impact on the party's business.

Depending on the outcome of that risk assessment, a number of further steps may be necessary at the outset of the arbitration. The party and its legal advisers will need to discuss the retention of documents and the gathering and review of potentially relevant material with specific regard to any cybersecurity issues identified. At this stage, there is unlikely to be any agreement with the other side on appropriate cybersecurity measures, nor will an arbitral tribunal necessarily have been appointed. Where the content of initial pleadings or documentary evidence appended to it contains particularly sensitive information, legal advisors should send those submissions to, where relevant, arbitral institutions by the institution's electronic system (where secure) or via encrypted file transfer sites.

At this early stage, a party will also discuss with their legal advisors who to nominate as an arbitrator and may analyse the appointment made by the other side, an appointing authority or arbitral institution. Where cybersecurity is critical, it may be sensible to send a checklist of cybersecurity related questions to arbitrators before or immediately after nomination or appointment. The answers to such a checklist (or a failure to answer) might lead to security concerns that need to be addressed before the arbitrator's appointment is confirmed.

BEFORE FIRST PROCEDURAL CONFERENCE

2. ASSESSING CYBERSECURITY RISKS IN SHARING DATA WITH OTHER ARBITRATION PARTICIPANTS

Once the arbitration has commenced and the parties, legal advisers, institution and arbitrators are in place, it is helpful for each party to carry out a wider assessment of the cybersecurity risks posed by the sharing of data with the other participants in the proceedings. It may be helpful to map out a list of all the participants that will or may in future hold data related to the arbitration and identify what types of data each one will receive. The list can be added to when additional participants become involved.

In assessing those cybersecurity risks, the Draft ICCA Cybersecurity Protocol may give guidance in assessing whether the arbitration has a "low", "medium" or "high risk" profile. Parties may wish to consider:

- The participants, their status and location. Their technical resources and capability to comply with cybersecurity measures. For example:
    - Who are the parties?
    - Other law firms: large or small? Domestic or international? What security measures are they likely to have?
    - Experts: are they sole traders, academics, large professional services firms? What security measures are they likely to have?
    - Witnesses: will you be sending information to their work or personal email address?
    - Third party suppliers: what contractual arrangements will you have? Where will liability rest for cyber breach?
    - Arbitral institutions: any awareness of their security profile? Is there an online filing system?
    - Arbitrators: partner in large law firm, QC from chambers, academic or sole trader? Technical competence and experience?
- The dispute, its value and sector.

- What types of information will be shared in the arbitration.
- Who will hold the different types of data.
- How and where information will be stored.
- Consequences of breach and severity.
- Other regulatory requirements (such as the GDPR and other regulatory regimes related to personal data).

This analysis may enable a party to identify (and therefore seek to address) concerns about the suitability of cybersecurity measures put in place by other participants in the arbitration. That party may wish to take the initiative prior to the first procedural conference to seek agreement from the other party or directions from the tribunal (once appointed) about what cybersecurity measures should be put in place. This could include ensuring that data is encrypted in transit and at rest, setting up a secure online repository/data room to minimise email exchange/storage or the use of encrypted hardware to transfer data.

AT THE FIRST PROCEDURAL CONFERENCE

3. TRIBUNAL MANDATED CYBERSECURITY MEASURES OR CYBERSECURITY AGREEMENT

Under its procedural powers and discretion, an arbitral tribunal should be able to determine what security measures, if any, are reasonable in the circumstances of the case. Although it is not yet commonplace for tribunals to make directions or orders on cybersecurity without it being requested by one of the parties, this is likely to change, particularly as cybersecurity issues are being addressed by many arbitral institutions in their latest rule changes . The tribunal will usually wish to reach its determination in consultation with the parties and this may include prior submissions on cybersecurity risk. The tribunal may also wish to use the Draft ICCA Cybersecurity Protocol to guide its analysis.

Based on this analysis, the tribunal may wish to consider adopting or ordering reasonable cybersecurity measures such as:

- Specifying how communications will take place between the parties and the tribunal, between the tribunal members and with other participants; through password protected email or by secure file transfer systems.
- Using a secure platform for the transmission of large volumes of documents relating to the case or sensitive documents.

- Reducing the use of paper documents
- (which represent a confidentiality risk) and/or a protocol for their storage.
- Redaction of certain categories of data or particularly sensitive information unrelated to the dispute.
- Reducing access to certain categories of data.
- Reducing unnecessary disclosure.
- Breach detection, notification and mitigation.
- Allocation of liability and penalties that will apply in the event of a breach (although this may be hard to negotiate in practice).
- Insurance against breach.
- Document retention and destruction.

The tribunal will need to weigh up the costs associated with any proposed measures against the anticipated risks, whilst also factoring in the need for efficiency and effectiveness in the arbitral proceedings.

Alternatively, the parties, their legal advisors and the tribunal may wish to formalise these cybersecurity measures in a cybersecurity protocol or agreement. A document of this kind could be signed by the parties, legal advisors and tribunal (and potentially the arbitral institution) and other participants involved at that stage in the process.

THROUGHOUT THE ARBITRATION

4. ONGOING CONSIDERATIONS: NEW PARTICIPANTS AND MONITORING COMPLIANCE

If an agreement is entered into or measures are ordered or adopted, it is critical that the parties linked to or instructing witnesses, experts or third-party service providers later on in the process clarify the importance of cybersecurity and obtain those participants' agreement (or at least compliance) to the cybersecurity measures that have been instituted. This may include signature of a cybersecurity agreement. If they are unable to comply, consideration should be given to how the risks associated with their non-compliance can be managed and whether notification is required to the other participants involved in the arbitration.

A party (directly or acting though its legal advisors) will also need to be alert to failures in compliance from other participants. If there is a formal agreement on certain steps that must be taken, then failure of a participant to comply may be obvious. Similarly, if a participant has given responses to a cybersecurity questionnaire that appear not to be accurate on the basis of their performance, this may need to be flagged. The party and their legal advisers will then need to consider how to respond to this failure to comply.

5. WHAT TO DO IN THE EVENT OF A BREACH

Data breaches can be difficult to detect, especially where data has been accessed for the purpose of committing a financial crime such as insider trading. Herbert Smith Freehills has developed its own software to help clients respond to data leaks quickly and reduce the financial impact of a cyber-attack. The parties and their legal advisers should be alert to any suspicious activity, as should all participants in the arbitration.

Every party to the arbitration should have a plan in place in the event of a breach. Many companies will have a designated cybersecurity breach action plan based on specialist IT advice, although the action plan may be directed at an "in house" breach, rather than necessarily a breach of data held externally. Where the cybersecurity risk presented by an arbitration is high, it is advisable for the participants' IT teams to be involved at the outset to ensure that the right strategy is in place.

If a breach occurs, necessary steps may include:

- Identifying the breach – what type of breach has occurred and how far has it spread?
- Disconnecting any devices that have been affected by a breach.
- Informing the other participants in the arbitration, including the arbitrators, parties, institution, and third parties.
- Following a designated cybersecurity breach action plan.
- Seeking specialist IT advice.
- Informing insurers.
- Hiring crisis management professionals to manage any reputational fallout.
- Notifying the data breach to relevant regulators

Some arbitrations deal with issues that may put certain individuals at risk of harm. In cases where this kind of personal data has been breached, extra care should be taken to ensure the safety of those individuals.

[More Inside Arbitration]

KEY CONTACTS

If you have any questions, or would like to know how this might affect your business, phone, or email these key contacts.

NICHOLAS PEACOCK
PARTNER, LONDON

+44 20 7466 2803
Nicholas.Peacock@hsf.com

VANESSA NAISH
PROFESSIONAL SUPPORT CONSULTANT, LONDON
+44 20 7466 2112
Vanessa.Naish@hsf.com

CHARLIE MORGAN
DIGITAL LAW LEAD – UK, LONDON
+44 20 7466 2733
Charlie.Morgan@hsf.com
