Essential Tips on Cybersecurity for Arbitrators: Identify, Protect, Detect, Respond and Recover

Kluwer Arbitration Blog
February 6, 2019

Mauricio Duarte (QIL + 4 ABOGADOS / Universidad Francisco Marroquín)

Please refer to this post as: Mauricio Duarte, 'Essential Tips on Cybersecurity for Arbitrators: Identify, Protect, Detect, Respond and Recover', Kluwer Arbitration Blog, February 6 2019, http://arbitrationblog.kluwerarbitration.com/2019/02/06/essential-tips-on-cybersecurity-for-arbitrators-identify-protect-detect-respond-and-recover/

Parties to arbitration, just like "*millennials*", are dependent on digital data and network systems. Currently, most of the data created is used and stored in digital formats using internet and computer technology. This should not be surprising; the online world enables people to interact and behave in new and efficient ways. However, the resulting dependence on digital records creates significant cyber security vulnerabilities, which can result in major harm to the parties involved in an international arbitration.

In 2018, the White & Case – Queen Mary International Arbitration Survey: The Evolution of International Arbitration (***"Survey"***) revealed that the use of international arbitration is likely to increase in the technology sector. Furthermore, the Survey showed that technology is widely used in international arbitration and an overwhelming majority favours the use of hearing room technologies, cloud-based storage, videoconferencing, Artificial Intelligence and virtual hearing rooms.

However, as the digital environment continues to grow rapidly, it is time to acknowledge that any effort to achieve a successful relationship between technology and arbitration must also consider related privacy and data security concerns. This post discusses some essential tasks that can be undertaken by key players in international arbitration to protect privacy and data security and ensure a successful arbitration.

Cyber Security Scandals

In 2015, the Permanent Court of Arbitration's ("***PCA***") website was hacked as a result of a cyber-attack originated in China. Hackers placed a malicious code, infecting the computers of diplomats, lawyers, and others who visited the website, which caused the PCA to temporarily take the website down. This constitutes the first real example that cyber security is, in fact, becoming increasingly relevant in the context of international arbitration.

Other recent security incidents have made clear that no company is immune from cyber-attacks. For example, the Equifax cyber security scandal shocked data experts around the world in 2017. The incident involved the breach of a security protocol that was easy to decipher and "hackers" accessed sensitive information including: names, social security numbers, birth dates, addresses, driver's

licenses and credit card numbers taken from consumers' personal data.

As a result of this and many other cyber security incidents, the United States National Institute of Standards and Technology ("***NIST***") issued a

Framework for Improving Critical Infrastructure Cyber security. The framework defined high-level goals of any cyber security risk management program. ***Identify, Protect, Detect, Respond, and Recover*** are the 5 main goals for any successful cyber security program which could be considered in international arbitration. If these principles were adopted; 2019 could be the year in which there is an awakening for the international arbitration community regarding cyber security concerns in the field.

Cyber Security Protocol

International arbitration as a preferred choice of dispute resolution involves sensitive subject matters, which normally might require discovery of confidential information including trade secrets, financial information, and personal identifiable information. In order to preserve international arbitration as a preferred alternative to resolve disputes, arbitral institutions and arbitrators will have to identify critical data and software to protect valuable information. This will enable arbitrators to effectively build procedures that satisfy both cyber security and data privacy concerns at arbitral proceedings.

Parties, as users of international arbitration, expect arbitrators and arbitral institutions to take reasonable measures to protect non-public exchanges of information. This expectation derives from parties' awareness of the risk of cyber security incidents, which may result in a wide range of losses for them, including: **(a)** out-of-pocket expenses for legal advice and forensic investigators; **(b)** regulatory penalties imposed by authorities; **(c)** potential damages awarded in civil claims; and **(d)** damages to market reputation. For instance, Facebook is currently facing lawsuits and monetary claims for the recent scandal involving Cambridge Analytica.

In 2018, ICCA, the New York Bar Association and the International Institute for Conflict Prevention and Resolution released a draft of the Cybersecurity Protocol for International Arbitration ("***Cybersecurity Protocol***"). The Cybersecurity Protocol originated as an acknowledgement from practitioners that arbitration proceedings are not immune to increasingly pervasive cyber-attacks. This also meant that attention to cyber security is required and essential to ensure that international arbitration maintains the confidentiality of the dispute resolution process.

In a digital era, a variety of factors must be considered when adopting security protocols for the transfer of sensitive information. However, with the new Cybersecurity Protocol, arbitral institutions and arbitrators will have some principles and guidelines to *Identify, Protect, Detect, Respond, and Recover*data from cyber security incidents that might take place in the arbitration proceedings.

Identify

Parties, arbitrators and arbitral institutions will have to work actively to identify what information might be vulnerable to cyber threats. This means, there should be an exhaustive consideration of what type of information is likely to be exchanged by the parties in the case. Intellectual property; trade secrets or other commercially sensitive information; financial information; personal data; and information that is subject to express confidentiality agreements or other relevant obligations should be considered.

However, identifying the relevant data or information is the first step. The arbitral tribunal will also need to identify whether the risk of a cyber attack is high or low, and whether the consequences of a

breach are likely to be minor, moderate, or severe. This determination will depend on the identity of the parties; the industry/subject matter of the dispute; the size and value of the dispute; the prevalence of cyber threats and the severity of potential consequences if there is a breach of information security.

Protect

After identifying the data and potential risks, arbitrators will need to establish security protocols for the storage and transfer of sensitive data and information. This protection will require a digitally secure infrastructure that would contain or store the potential information. For instance, it is not recommendable to use a "*cloud service*" or similar services, such as Dropbox, with a fairly predictable password such as: "1234arbitration". In this regard, the NIST has recommended that passwords should be based on unique passphrases, at least 8 characters long, and easily remembered. In addition, common dictionary words, past passwords, repetitive or sequential characters and context-specific words should be avoided.

Encryption, pseudonymization, or anonymization of information before it is exchanged could be a reasonable measure, depending on the concerns. Moreover, other protection measures could also address the limiting of exchanges of confidential commercial information and personal data; restriction of access to arbitration-related information and the method of transmission of the information.

Hopefully, the future of a blockchain infrastructure can contribute to cyber security in international arbitration. Blockchain is a distributed and immutable ledger, which stores information, known as blocks. Blocks are structured in the form of a 'chain' sequence, stored on various nodes (i.e., computers), which ensure that no single person or entity can manipulate the ledger without everyone else knowing. In other words, a *blockchain protocol* could serve as a tamper-resistant and resilient repository of data, to modernize and increase cyber security.

Detect

After identifying and enabling protection measures, a tribunal would need to have tools to detect a possible cybersecurity breach. For instance, the use of a program that specializes in detecting both malware and non-malware forms of spyware could be helpful (anti spyware software). Also, the use of antivirus software's (not the trial versions) should enhance the process to detect a possible breach. Arbitral institutions could also adopt an enhanced digital infrastructure with a security service (i.e., intrusion detection system or intrusion prevention system) that monitors networks or systems for the purpose of finding or detecting, in real-time or near real-time, attempts to access system resources in an unauthorized manner.

Respond

Arbitrators would need to create a Cyber Incident Response Plan, providing instructions or procedures to respond and mitigate the consequences of a cyber incident. For instance, suspending the procedure until the cyber risk is addressed could be an option. Other options could include a strict mandatory 72-hour breach notification requirement; use of computer forensics to address the issue and alternatives to recover information; and the use cryptography for documents that have not been compromised in order to prevent anyone but the intended recipient from reading that data.

Recover

Although sometimes it might be difficult, if a cyber security incident occurs, a tribunal would have the responsibility to try to restore the data that has been lost, accidentally deleted, corrupted or made

inaccessible. However, a tribunal could also adopt protection measures (since the beginning) to have a data back-up system in which copy of files and programs is made in order to facilitate recovery, if necessary. This backup should be done routinely and even considering the so-called “3-2-1 rule”, according to which 3 copies of the data should be made, 2 should be stored locally in different storage media, and 1 copy should be stored offsite.

Conclusion

The Cybersecurity Protocol discussed in this post is designed to encourage practitioners to become more familiar with cybersecurity risks and to provide guidance on measures to be taken in light of those risks. Although the lack of regulation in a particular industry could be interpreted as something positive at times, this does not apply to situations in which there could be: **(a)** economic loss to parties, arbitrators, and arbitral institutions; **(b)** reputational damage to arbitral institutions, arbitrators and counsel, as well as to the system of international arbitration overall; and **(c)** potential liability under applicable laws and other regulatory frameworks.

As the frequency and sophistication of cyber-attacks grow, we will need to ensure the adoption of good practices to protect digitally stored information. The incorporation of new technologies will not dismantle arbitral proceedings. On the contrary, technology will boost the appeal of arbitration to resolve disputes, especially in the technology sector. Thus, as practitioners, we shall all be familiar with the need to *Identify, Protect, Detect, Respond, and Recover.*