Contents lists available at Science-Gate

International Journal of Advanced and Applied Sciences

Journal homepage: http://www.science-gate.com/IJAAS.html

Cybersecurity in international commercial arbitration (Legal vision)

Asmaa Saad Hussien *, Hani Mohamed Mounes

Department of Law, College of Business Administration, Northern Border University, Arar, Saudi Arabia

ARTICLE INFO

Article history:
Received 13 October 2023
Received in revised form
1 February 2024
Accepted 3 February 2024

Keywords:
Foreign investment
Arbitration
Information security
Confidentiality
Cyberattacks

ABSTRACT

Attracting foreign investment requires assurances from states to safeguard against infringements and losses. Arbitration serves as a crucial factor in enticing investors. However, for arbitration to be effective, ensuring information security is imperative. Maintaining confidentiality and preventing disclosure are vital, yet they pose challenges. International experiences indicate that companies might accept unjust settlements to prevent revealing their trade secrets. To tackle these obstacles, various arbitration bodies have endeavored to establish legal mechanisms for ensuring information security. This involves targeting individuals involved in arbitration proceedings and enhancing technical infrastructure. For instance, the International Council for Arbitration (ICCA), in collaboration with the New York State Bar Association (NYSBA) and the International Institute for Conflict Prevention and Resolution (CPR), devised an Electronic Security Protocol for Commercial Arbitration. These initiatives aim to shield participants in international commercial arbitration from the risks of divulging sensitive information due to breaches in information security. The protocol offers a framework of guidelines for arbitrators and parties on safeguarding confidential information throughout the arbitration process. It encompasses aspects like confidentiality agreements, data protection, access control, security measures for electronic devices and data, and procedures for handling incidents. By adhering to these guidelines, arbitrators and parties can uphold the protection of confidential information, thus ensuring that international commercial arbitration remains a secure platform for dispute resolution.

© 2024 The Authors. Published by IASE. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

1. Introduction

Arbitration is the preferred method of dispute resolution in international trade because it offers several advantages that are not available in national court litigation, including confidentiality, flexibility, neutrality, and expertise (Pauwelyn, 2023). One of the key benefits of choosing arbitration over court litigation is that it allows the parties involved to maintain a level of confidentiality that isn't available in public court proceedings.

The necessity of each party to an arbitration dispute submitting its documents and notes to the arbitral tribunal is inherent in the very nature of arbitration (Blackaby et al., 2023). This principle is known as document production and is essential for the arbitral tribunal to make a fair and informed decision on the merits of the case. Confidentiality in arbitration requires that none of the information provided by the parties to the dispute be disclosed to the arbitral tribunal (Singer, 2020). The submission of notes and documents in arbitration is most often done electronically, regardless of whether the arbitration is traditional or electronic. This can be done by requesting the arbitral tribunal to send a note or document by email or by requesting the arbitration center to submit notes and documents through an electronic platform under the supervision of the center. Therefore, this information may be exposed to electronic attacks, and there is no doubt that these electronic attacks, by aiming to disclose information about the arbitration dispute, undoubtedly affect the confidential nature of the arbitration.

In order to control information security in the field of arbitration, ICCA, in collaboration with NYSBA and the International Institute for Conflict Prevention and Resolution, has developed a cybersecurity protocol for commercial arbitration, which includes recommended best practices for

* Corresponding Author.
Email Address: asmaa.saad.elhadedy@gmail.com (A. S. Hussien)
https://doi.org/10.21833/ijaas.2024.02.023
Corresponding author's ORCID profile:
https://orcid.org/0009-0001-5560-6873
2313-626X/© 2024 The Authors. Published by IASE.
This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/)

securing information in the context of commercial arbitration (Awaisheh, 2023). The protocol in question operates under the premise that all participants in the arbitration process, including arbitrators, arbitration centers, experts, and others, share a responsibility to secure information and are equally vulnerable to cyberattacks. This protocol is not inherently mandatory; it only becomes applicable when the parties involved in the arbitration explicitly agree to adopt it within their arbitration agreement.

The aforementioned protocol deals with organizing communication processes between the elements participating in the arbitration, transmitting communications, pleadings, and evidence submitted by the parties, and storing information related to the arbitration.

The protocol addresses the type of information required to be secured against potential security attacks, the consequences of any potential information breach, and the security capabilities available to participants in the arbitration.

The Comparative Analytical Approach will be used, as international jurisprudence related to information security in international commercial arbitration will be exposed, whether it's the form of an electronic security protocol or not, which leads us to a comparative approach to compare the practices listed in the protocol in order to achieve information security in relation to information disclosed in an international commercial arbitration context, as well as an attempted comparison with national case law on electronic crimes.

2. Previous studies

Sussman (2018) studied the impact of information security breaches on arbitration, and it concluded that targeting arbitration is the ideal environment for resolving commercial disputes involving activities that violate information security. The study also found the duties of arbitrators with regard to preventing information security risks in the field of arbitration, as well as security precautions regarding documents submitted to the arbitral tribunal and the necessity of covering documents with a degree of documentation so that they are secured against the risk of breach. The study also examined the extent to which evidence derived from illegal amounts is acceptable.

Chaisse and Bauer (2019) also addressed the challenges of the digital age that have cast their shadows on all aspects of life, including international commercial arbitration as the ideal means of resolving international trade disputes. The study also reviewed international mechanisms to protect investors from the risks of violating privacy in arbitration. The study concluded that it is necessary to reach what is known as the principle of cyber peace to demonstrate information security in the field of commercial arbitration. This process involves creating bilateral or multilateral agreements that aim to establish protocols for regulating information security among the parties involved in the arbitration process.

The study's findings rely on the idea that all involved parties in arbitration disputes are responsible for safeguarding information and are susceptible to cyberattacks. It's crucial to understand that global arbitration regulations, while established by authoritative bodies, lack enforceability as they operate on voluntary compliance. To enforce information security measures, explicit agreement from the disputing parties is necessary within the resolution process documentation. This means that the parties must consent to adhere to information security protocols as outlined in the dispute resolution documents.

3. Arbitration and confidentiality

Confidentiality in arbitration aims to support trust by preventing the circulation of some information, and the commitment to ensuring confidentiality is one of the established principles in international commercial arbitration and is considered the cornerstone of the success of the arbitration process through what it ensures of securing mutual communications during arbitration procedures. Confidentiality is, therefore, an essential feature in international commercial arbitration (Cremades and Cortes, 2013). Practical practices in international commercial arbitration show that the obligation of confidentiality is of utmost importance to the parties, regardless of whether the obligation of confidentiality is a general obligation or not and regardless of the basis on which this obligation is based.

In order to regulate the obligation of confidentiality, the parties may include the aforementioned obligation in the arbitration agreement or conclude a separate agreement signed by them. Resorting to institutional arbitration is an essential guarantee in this regard, as arbitration institutions guarantee a commitment to confidentiality within their arbitration rules. For example, the appraisal rules of the London Chamber of International Arbitration (LCIA) and the Cairo Regional Center for International Commercial Arbitration (CRCICA, 2024) stipulate that all rulings and documents submitted in the procedures as well as the deliberations remain confidential in principle unless the parties expressly agree otherwise in writing (Article 30 LCIA Arbitration Rules, Article 37 CRCICA Arbitration Rules (CRCICA, 2024; LCIA, 2020).

The International Arbitration Rules of the American Arbitration Association (AAA, 2021) also included a text of the obligation of confidentiality (Article 34 AAA Arbitration Rules) and the International Trade Convention (ICC) in Paragraph 7 of Article 20 of the Arbitration Rules included allowing the arbitral tribunal to take all precautions to protect confidential information and trade secrets (AAA, 2021). The confidentiality rules of the World Intellectual Property Rights Organization (WIPO) are

notably detailed due to the organization's focus on disputes related to intellectual property and technology. These areas typically involve sensitive information like trade secrets, franchise rights, patents, and authors' rights, which necessitate a high level of confidentiality. (Landolt and Garcia, 2017).

Articles (75-78) of the WIPO Arbitration Rules stipulate that the existence of the arbitration, documents, and defenses presented in the arbitration, including witness testimony and awards, shall remain confidential, and this general and comprehensive commitment to confidentiality is binding on the parties, witnesses, arbitrators and the WIPO Arbitration and Mediation Center (Landolt and Garcia, 2017).

The principle governing the field of arbitration is confidentiality, which remains intact unless it becomes necessary for the parties to establish or serve a public interest. Some have put forth the argument that the nature and extent of the obligation to maintain confidentiality in electronic arbitration will rely on striking a balance between public and private interests. It is important to consider that electronic arbitration necessitates a heightened level of confidentiality due to the digital environment in which it takes place. Consequently, the obligation to maintain confidentiality must encompass case data, documents, communications, and procedures. Therefore, no party is permitted to unilaterally disclose any information pertaining to the existence of the arbitration, the involved parties, the award, or any documents or evidence obtained as a result of their participation in the arbitration proceedings, except in cases related to challenges against the arbitration award, requests for enforcement orders, or as mandated by a legal provision or an order from a competent regulatory authority. Providers of electronic dispute resolution services must employ encryption methods to ensure the confidentiality of procedures and secure electronic communications. Additionally, firewalls and passwords should be implemented to prevent unauthorized access to databases. (McKeon, 1994).

4. Confidentiality in institutional arbitration

The use of online platforms, electronic filings, and videoconferencing in arbitration proceedings has raised concerns about whether arbitral institutions and arbitrators are equipped to deal with cybersecurity and data protection compliance issues during the COVID-19 pandemic; In particular, most major arbitration institutions are bound by a duty of confidentiality. In the case of the International Center for Dispute Resolution (hereinafter referred to as "ICDR/AAA"), Rule 37 of the ICDR/AAA International Arbitration Rules imposes on the arbitrators and the Administrator a duty of confidentiality to preserve all matters relating to the arbitration or arbitration award. Confidentiality (ICDR/AAA, 2023) unless the parties agree otherwise or unless required under applicable law (Lee, 2020). This includes information disclosed by the parties or witnesses during the arbitration proceedings. Similar provisions can be seen in Section 4.18.2 of the Arbitration Rules of the ADR Institute of Canada, Inc., which requires the parties, the arbitral tribunal, the institution, and any third parties attending any part of the arbitration hearings or meetings to maintain their confidentiality rights. (ICDR/AAA, 2023). This requirement is dependent on the agreement of the parties or a mandate from the court or legislation. Similarly, Article 30(1) of the LCIA Arbitration Rules mandates that both the parties and the institution generally agree to maintain the confidentiality of all decisions, a principle particularly emphasized in Asia (ICDR/AAA, 2023; LCIA, 2020). There is a comprehensive duty to maintain the confidentiality of any recordings, transcripts, or documents used in connection with the arbitration proceedings (SIAC, 2016) and is imposed on all parties (the parties, the party, any arbitrator, including any emergency arbitrator, and any person appointed by the arbitral tribunal, including any Administrative Secretary and any expert) participating in the arbitration administered by the Singapore International Arbitration Centre. In the Oceania region, Rule 22 of the Australian Center for International Commercial Arbitration (ACICA) Rules 2016 requires parties to secure the same level of duty of confidentiality to witnesses attending arbitration proceedings as that imposed on the parties, the institution and the court (Yu, 2020; SIAC, 2016).

5. Arbitration confidentiality and cybersecurity

Cybersecurity has become increasingly important in arbitration as an alternative dispute resolution method, as a distinct dispute resolution option for parties involved in complex and sensitive international disputes. In these types of disputes, informational disclosure is inevitable and may include confidential information such as trade secrets, financial information, and personally identifiable information (Pastore, 2017). Therefore, attention must be paid to information security within the framework of international commercial arbitration, as the consequences that may result from not paying attention to information security are as follows (ICCA, 2020):

- Individuals may experience significant economic losses as a result of their business information or personal data being compromised.
- Cybersecurity incidents can lead to a loss of data integrity, raising concerns about the reliability and accuracy of the affected data.
- Disruptions caused by cybersecurity incidents can render data, networks, platforms, or websites unavailable.
- Parties involved may face potential legal liability under relevant laws and regulatory frameworks, including data protection regulations.
- The reputation of parties, arbitrators, administrative institutions, and third parties, as

well as the overall arbitration system, can be negatively impacted.

The efficacy of any system for resolving disputes hinges on upholding a reasonable level of protection of the information shared during the settlement process, irrespective of the confidentiality and integrity of said information (ICCA, 2020).

It is important to acknowledge that cyber intrusions into the arbitration process do not indicate a particular vulnerability to data breaches. However, it is evident that international arbitration proceedings are not immune to the growing prevalence of cyberattacks targeting companies, law firms, government agencies, officials, and other entities responsible for safeguarding large electronic datasets containing sensitive information. This issue came to light in July 2015 during a hearing held by the Permanent Court of Arbitration (PCA) in The Hague regarding maritime boundaries between the Philippines and China in the South China Sea. On the third day of the hearing, the court's website abruptly ceased functioning due to a cyberattack originating from China. The hackers had infected the site with malware, thereby exposing anyone visiting the site to potential data theft. It is worth noting that arbitration institutions seem to continue relying on relatively insecure storage and communication systems. Furthermore, institutional rules do not address cybersecurity concerns explicitly, as they permit the transfer of data between participants in the arbitration process through any electronic means. In fact, many arbitral institutions utilize unencrypted email and commercially available cloud data warehouses.

In the case of Libananco v Republic of Turkey (ICSID Case No. ARB/06/8), Turkey acknowledged its interception of Libananco's communication with its legal representatives and third parties, citing it as part of a criminal investigation (ICSID Case No. ARB/06/8). Similarly, in an unpublished order pertaining to Caratube International Oil Co. LLP and Devincci Salah Hourani v Republic of Kazakhstan (ICSID Case No. ARB/08/12, 5 Jun 2012), the court admitted certain documents into evidence that were obtained through the unauthorized access of Kazakhstan's government computer network (TENNANT ENERGY LLC Vs Government of Canada). This decision aligns with the court's acceptance of video evidence presented by TENNANT ENERGY LLC against the Government of Canada in their dispute. Furthermore, in the case of ConocoPhillips v. Bolivarian Republic of Venezuela (ICSID Case No ARB/07/30), additional relevant information was presented.

Law firms are increasingly falling victim to cyberattacks, as evidenced by a study conducted by LogicForce, a reputable cybersecurity consulting firm. The study, which analyzed 200 law firms during the first quarter of 2017, revealed that all surveyed firms had experienced hacking attempts. What is particularly concerning is that 40% of these firms were unaware of these attempts. Furthermore, a staggering 95% of law firms were found to be non-compliant with their cybersecurity protocols, highlighting a significant vulnerability. Alarmingly, only 23% of these firms had insurance coverage against cyberattacks. This information underscores the potential consequences of a sensitive data breach, such as the admission of illegally obtained or privileged evidence, which could severely compromise the integrity and legitimacy of the arbitration process, as demonstrated in the aforementioned cases (Cohen and Morril, 2017).

6. Cybersecurity protocol

ICCA (2020) has been established as a cybersecurity protocol in the field of international arbitration to serve as a recommended framework for the courts, parties, and institutions involved in the arbitration process, providing guidance on the necessary measures to ensure the security of information throughout the arbitration case. The protocol is structured into a series of principles and four annexes, offering a comprehensive approach to information security. It is important to note that the authors of the protocol acknowledge that it does not aim to provide a one-size-fits-all solution for all individuals and situations when it comes to securing information. Rather, the protocol seeks to establish a baseline of reasonable measures for information security in arbitration procedures. These measures are considered to be the minimum requirements for safeguarding information.

6.1. Principles of cybersecurity protocol

The Second Principle of the Protocol underscores the significance of active participation from all entities involved in the arbitration process (parties, arbitrators, and the institution) while considering reasonable information security practices. This includes individuals who have access to arbitration-related information. The principle of solidarity forms the basis of information security in arbitration, as any breach by a participant could potentially impact all parties involved and compromise the overall security of the arbitration. Therefore, it is crucial to recognize that actions taken by any individual, regardless of their operating environment or available infrastructure, can lead to incidents that compromise information security or become the "weakest link." In fact, many security incidents arise from individual behavior rather than system or infrastructure breaches (ICCA, 2020).

Furthermore, all entities participating in the arbitration process must have a comprehensive understanding of all information security policies. Violating any of these policies would have a detrimental effect on the entire information security system. For instance, policies that restrict communication through personal email addresses or prohibit the use of unencrypted disks (which can be accessed without additional steps, such as entering passwords for decryption). Individuals involved in

international arbitrations must ensure they are aware of and adhere to any applicable policies outlined in the ICCA (2020).

In spite of the advancements brought about by the digital transformation in the field of litigation and arbitration, it is imperative to exercise prudence with regard to cybersecurity, adherence to data protection regulations, training of arbitration participants, and comprehension of their respective roles in light of the growing reliance on electronic filing, videoconferencing, and email correspondence in arbitration proceedings. This is particularly crucial in relation to the interplay between data protection and arbitration institutions tasked with upholding confidentiality. Confidentiality remains a paramount concern in this context. (Yu, 2020).

ICCA (2020) mandates that individuals can only access arbitration-related information with the authorization of one of the parties authorized by the arbitral tribunal. This includes entities providing support services like translation, as well as experts preparing advisory reports commissioned by one of the parties involved in the case rather than the arbitral tribunal. Additionally, there may be other individuals who can view the information without permission from the arbitral tribunal, typically due to a contractual relationship with one of the parties or being under their actual control. However, these individuals will not be under the direct control of the arbitral tribunal and may not bear the immediate consequences of an information security incident. Given that these individuals, who have access to arbitration information beyond the control of the arbitral tribunal, can significantly impact the security of the information, the protocol emphasizes the importance of ensuring their awareness of the security measures in place. It recommends including a commitment to information security in an agreement between these individuals and any of the arbitration parties.

ICCA (2020) is not intended to supersede any applicable laws, arbitration rules, professional or ethical obligations, or other binding obligations. As such, the Protocol is designed to avoid any conflicts with other mandatory rules and guidelines. The Protocol is currently being applied in arbitration proceedings related to information security, which is particularly important given the varying data protection regulations across jurisdictions. These regulations are considered rules of public law due to their significance. Examples of such regulations include the General Data Protection Regulation in Europe (GDPR), the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the California Consumer Privacy Act of 2018 (CCPA), and the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA). The implementation of any regulation related to information security must be based on achieving the required level of information security. The Protocol also addresses institutional arbitration, as arbitration institutions have shown an interest in regulating information security controls through their rules. Some institutions have adopted secure platforms for transferring information and holding arbitration sessions. Therefore, the provisions of the Protocol are considered precautionary measures for information security in the event of failure. These provisions are applicable first, whether they are laws or rules of applicable arbitration institutions.

It is not appropriate to assert the existence of a unified system for information security. Therefore, the fifth principle of the ICCA (2020) emphasized the connection between information security in commercial arbitration and legal and contractual obligations. Consequently, the cost, technical capabilities, and level of risk associated with a particular case may influence the controls that need to be implemented in arbitration. The Protocol also states that its objective is to achieve a reasonable level of information security in arbitration, allowing parties to choose and implement controls based on the specific circumstances of each case. The sixth principle of the Protocol identifies the risk factors that impact security measures, while the seventh principle outlines the information security measures that should be considered in addressing each risk situation. This evaluation is based on several criteria, including asset management, access controls, encryption, communications security, operations security, and information security incident management. The sixth principle highlights the importance of evaluating specific elements to ensure information security in the arbitration process. Additionally, the eighth principle advises those involved in arbitration to develop information security measures suited to the specifics of the arbitration process. It is crucial to consider the methods used for data transfers in arbitration, such as through emails, external platforms or virtual data rooms, or via USBs and other portable storage devices. Considerations should be given to implementing measures for the storage of communications, pleadings, disclosure materials, and evidence. These measures may involve minimizing the processing of confidential business information, personal data, or other sensitive information associated with the arbitration. It may be necessary to restrict access to certain information to advocates only. Additionally, parties should agree to confidentiality provisions or implement protective orders as outlined in the ICCA (2020).

The tenth principle of the ICCA (2020) emphasized the importance of reaching an agreement on information security at the initial session of the arbitration. During this session, the following factors should be taken into consideration when determining information security procedures:

1. Engage legal representatives in a discussion regarding reasonable information security measures.
2. Assess the ability and willingness of all parties involved to adopt specific security measures.
3. Address any disputes that may arise concerning reasonable information security measures.

4. Disclose any information that could potentially impact the legitimacy and integrity of the arbitration process.

The eleventh principle further confirms that the arbitral tribunal possesses the jurisdiction to determine the information security measures implemented in the arbitration process. In all circumstances, the arbitral tribunal must adhere to the agreement reached by the parties, and it must promptly issue a procedural order outlining the necessary procedures concerning information security. The protocol includes Table No. D, which contains the standard language typically employed by arbitral tribunals in this regard.

Moreover, the Protocol grants the thirteenth principle the authority to address incidents that result in a breach of information security. In such cases, the authority is also empowered to allocate the costs associated with remedying the breach and determine the respective parties' share of those costs. Indeed, the arbitral tribunal possesses the right to impose penalties on the parties, taking into consideration the applicable law governing arbitration.

6.2. Tables of practical applications contained in the cybersecurity protocol

The cybersecurity Protocol includes four tables, which can be regarded as appendices. These tables are considered crucial in the protocol as they encompass practical applications in terms of identifying and evaluating the risks associated with arbitration. Furthermore, they provide a framework for prioritizing these risks and offer strategies to effectively address them. The final table in the protocol outlines procedural formulas that can serve as guidance for arbitral tribunals. These formulas can be utilized either for parties to agree on assigning the responsibility of managing information security risks to the arbitral tribunal or for issuing procedural orders.

6.2.1. Tables of practical applications contained in the cybersecurity protocol

The cybersecurity protocol related to arbitration comprises four tables, which may be regarded as appendices. In the researcher's assessment, these tables represent the most significant aspects of the protocol as they provide practical applications for identifying and prioritizing areas of risk that may be encountered in arbitration. Additionally, the tables offer guidance on how to confront these risks effectively. The final table contains procedural formulas that arbitral tribunals can use as a reference when addressing information security risks. These formulas may be used to facilitate agreement between parties to assign the task of confronting such risks to the arbitral tribunal or to issue procedural orders.

6.2.2. Table "A": General information security measures

Table "A" comprises a comprehensive checklist of information security measures that all custodians of arbitration-related information should contemplate incorporating into their daily use of technology for arbitration-related activities. It is important to note that these measures are primarily intended for security purposes and may not be obligatory, as previously stated. The Protocol encompasses all of these measures and takes into consideration the potential risks that may threaten the arbitration process (ICCA, 2020).

In the field of asset management, it is recommended to consider the following controls:

- Identify highly sensitive data and implement appropriate measures to safeguard and minimize its exposure.
- Restrict the creation of unnecessary copies of multiple documents.
- Establish secure methods for preserving and disposing of documents.
- Configure data backups and activate data wipe functions.

The protocol recommends considering the following measures pertaining to access control:

- Defining access control policies that include strong password requirements, password change intervals, and assigning responsibility for password management.
- Implementing multi-factor authentication.
- Separating the privileges of administrator and user accounts and regularly reviewing and reducing the privileges of user accounts.

The protocol recommends considering the following controls pertaining to encryption:

- Data encryption should be implemented during transfer. Additionally, it is crucial to consider the sensitivity level of the file that requires encryption.
- In addition to data encryption in the cloud and encryption through blockchain technologies, the feasibility of implementing comprehensive encryption should be taken into account.

The protocol recommends considering the following measures pertaining to information security:

- Exercise caution and prudence when handling attachments and links.
- Ensure that data and files are transferred using secure methods, such as utilizing cloud-based platforms, instead of relying on email for transmission.

- Refrain from utilizing public networks and prioritize the use of private networks whenever possible.

The protocol recommends considering the following measures pertaining to operational security:

- Utilize commercial and professional products and tools, thereby avoiding the use of non-original or counterfeit products.
- Refrain from sharing accounts and devices to ensure individual accountability and prevent unauthorized access.
- Promptly install software updates and patches while actively monitoring and addressing any identified security vulnerabilities.

6.2.3. Table "B": Information security risk factors related to arbitration

Table "B" provides a comprehensive analysis of information security risk factors associated with arbitration. Its purpose is to assist both parties and the arbitral tribunal in evaluating the potential risks involved in an arbitration case. This evaluation is crucial as the protection of information pertaining to the case, including details related to the subject matter and the participants, is of utmost importance. The table also considers other factors that contribute to the arbitration risk profile and outlines the potential consequences that may arise if this information is compromised. By paying close attention to the arbitration risk profile, it becomes possible to determine the appropriate and reasonable measures that should be implemented during the arbitration process. This protocol, known as the ICCA (2020), serves as a valuable resource in this regard.

The arbitration risk profile enables the assessment of information and the determination of the level of protection required. It is imperative to consider the sensitivity of information such as patient data, bank statements, trade secrets, and commercial books and provide the necessary protection accordingly. Additionally, if the lawsuit involves audio, visual, or intellectual property rights, it is crucial to ensure adequate protection. This is also applicable to information that is subject to confidentiality and non-disclosure obligations under the law, including intellectual property rights, trade secrets, health and medical information, ethnic origins, political opinions, and criminal records. Financial data, such as payment card information, and information subject to professional legal privilege, such as attorney-client or doctor-patient privilege, must also be protected. The nature of the subject matter of the arbitration or the identity of the participants may also impact the risk profile of the arbitration. When assessing the impact of these factors on information security risks, the following factors should be considered:

a. In the event that the Dispute involves a party or any other participant with a documented record of engaging in cyberattacks.
b. In the case where the dispute pertains to trade secrets or personal information, such as those held by a law firm, bank, or health care provider.
c. If the dispute involves a public figure or encompasses government information.

There are several additional factors that impact the assessment of the arbitration risk profile, which include:

a. The industry or subject matter involved in the dispute.
b. The magnitude and monetary value of the dispute.
c. The prevalence of cyber threats, encompassing those directed toward the industry, parties, or the type of data implicated in the arbitration.
d. The methods employed for data storage and transmission, encompassing network security measures.
e. The identification of individuals authorized to access the data processed during the arbitration proceedings.

When assessing the level of arbitration risk, it is crucial to take into account the potential consequences of a breach. These consequences encompass various aspects, including:

a. The potential harm that may arise from the loss of confidentiality, availability, integrity, or accuracy of the information involved.
b. The risks posed to the integrity of the arbitration process itself, as well as the potential impact on the nature and quality of the evidence presented in the claim.
c. The financial losses, loss of privacy, devaluation resulting from the disclosure of confidential or proprietary data, harm to the reputation or privacy of individuals or legal entities, and the exposure of secret or proprietary information.
d. In addition to evaluating the potential impact of a breach on the arbitral tribunal, the parties involved, and the administering institution, it is essential to consider the potential consequences for individuals outside the arbitration process. This includes individuals whose personal data may be implicated. An information breach suffered by one participant can lead to harm to other participants or third parties.

When implementing security protocols for the transfer of sensitive information, it is crucial to take into account a multitude of factors (Pastore, 2017).

First, it is a practical and useful step to identify categories of sensitive information that require enhanced cybersecurity measures. In fact, many cybersecurity measures often prove ineffective due to their excessive complexity or susceptibility to human error. Consequently, the endeavor to enforce stringent cybersecurity protocols on all data

implicated in arbitration proceedings may prove counterproductive. Such an approach risks excessively personalizing information, thereby causing practitioners to overlook crucial data. Moreover, it results in unnecessarily convoluted procedures for accessing information that requires minimal or no additional safeguarding.

Second, limiting the disclosure of sensitive information is crucial in mitigating the threat of cyberattackers in the context of arbitration. One effective approach is to restrict access to certain information to only those individuals who require it.

6.2.4. Table "C": Information security measures

Table "C" pertains to a subset of the information security measures prescribed in the cybersecurity protocol. The table encompasses instances of information security measures that may be mutually agreed upon by the parties or mandated by the arbitral tribunal as deemed necessary. It is not mandatory to implement all the measures outlined in the table. Instead, each case must be assessed on an individual basis, as certain measures may be considered as alternatives to others. The protocol emphasizes that Table "C" will be subject to periodic revisions in accordance with the evolving practical practices.

Among the information security measures recommended for asset management:

a. Restrict the exchange and access of conflict-related information to individuals who have a legitimate need for such information.
b. Prioritize the implementation of protective measures, such as redaction or pseudonymization, before sharing information that is considered to carry a higher risk within the arbitration context.
c. Categorize confidential or sensitive data into various classifications, such as "confidential," "top secret," or "for lawyers only," to ensure appropriate handling and protection.
d. Refrain from sharing disclosure materials with the arbitral tribunal or administrative institution unless it is necessary for resolving disclosure disputes or for evidentiary purposes. In such cases, only relevant and necessary materials should be shared to aid the arbitral tribunal's decision-making process.
e. Utilize a secure sharing site or cloud platform to facilitate the exchange of information and documents pertaining to the dispute.
f. Limit the use of public networks for accessing, storing, or transmitting arbitration-related information.
g. Establish an agreement that allows remote access to the networks of interested parties solely through a secure Virtual Private Network (VPN).
h. Maintain backup copies of arbitration materials throughout the duration of the case.
i. Clearly define the retention period for information related to the dispute after its conclusion and establish a procedure for returning such information to the original party or permanently destroying and deleting it, regardless of the storage method employed.

Recommended information security measures for access controls:

a. Access to arbitration-related information should be restricted to the least privilege, on a need-to-know basis, or limited to attorneys only.
b. Password submission to file-sharing sites should be agreed upon, passwords should be added to certain documents, and access expiration limits should be established.
c. Multi-factor authentication should be used for remote access or access to networks, systems, or platforms that may contain confidential or sensitive information related to the dispute.
d. Periodic reviews of access control lists for systems or networks in which conflict-related information will be stored should be conducted, and access should be disabled for persons who no longer need to know, such as those who leave the employment of a party.
e. Restrictions should be imposed on downloading and printing confidential documents.

Recommended information security measures are encryption:

a. Requesting that stored information be encrypted.
b. Consent to encryption of information during transmission.
c. Consent to encrypt devices (such as USB drives and hard drives) on which information relating to the matter is stored or exchanged.

It is noteworthy that Deloitte has reported on the promising innovations in the nascent field of blockchain technology that can assist organizations in addressing the challenges of immutable cyber risks, such as digital identities and maintaining data integrity (https://www2.deloitte.com). The fundamental properties of immutability, data encryption, and operational resilience inherent in blockchains make them effective in disrupting fraudulent activities and detecting data tampering, thereby enhancing cybersecurity. Unlike cloud computing, blockchains do not have a single point of failure, significantly reducing the likelihood of an IP-based DDoS attack disrupting network operation.

In the event of a node (i.e., a computer) being compromised, the data stored on the blockchain remains accessible through other nodes within the network. This is due to the fact that all nodes maintain a complete copy of the distributed ledger at all times, as highlighted on the Ethereum blog (https://blog.ethereum.org) and reported by Coin Telegraph (https://cointelegraph.com). While blockchain technology is generally considered to be resilient with no single point of failure, permissioned private blockchains with fewer nodes must ensure that their network is globally distributed and

resilient, with no single points of failure at the enterprise or platform level. This is necessary to ensure continuous operation, even in the event of a natural disaster or coordinated attack, as noted by Shehata (2018).

Furthermore, blockchain technology exhibits operational flexibility as it encompasses both public and private blockchains, each comprising numerous nodes. Consequently, in the event of a cyberattack, companies have the ability to render a node virtually redundant while maintaining uninterrupted business operations. Thus, even if a significant portion of the blockchain network falls victim to an attack, the technology's decentralized nature ensures its continued normal functioning. However, it is crucial to acknowledge that the fundamental characteristics of blockchain remain unaltered despite the aforementioned advantages (Shehata, 2018).

Information security measures recommended for communications security:

a. Establish protocols for the conduct of communications between the arbitral tribunal, the parties, and the administering institution to safeguard the confidentiality and integrity of such communications. This includes guidelines for the transmission of communications, pleadings, and evidence; communication channels between arbitrators; and communication channels between arbitrators and the administrative institution.
b. Ensure that all emails pertaining to this matter are sent using business or enterprise email accounts rather than free consumer or individual email services.
c. Utilize business or enterprise-level document-sharing systems or software for the sharing and storage of any documents related to the arbitration, avoiding the use of free consumer or personal storage or sharing platforms.
d. Exercise caution when using email files or attachments to transmit confidential or sensitive information. Unless the email is end-to-end encrypted and the attachments are password protected, refrain from transmitting such information through email. If necessary, passwords for protected attachments should be communicated through a separate means of communication, such as text messages or voicemail.
e. In the event of utilizing a shared third-party cloud platform, establish clear agreements regarding access privileges, duration of access, and user privileges concerning data. Additionally, implement measures such as user password requirements, multi-factor authentication, remote access restrictions, and regular monitoring of security vulnerabilities.
f. Employ a shipping method that incorporates a sign-and-track mechanism when delivering any packages, drives, devices, or printed materials relevant to the dispute.
g. Impose restrictions or prohibitions on the use of certain types of media, such as flash drives, for storing arbitration data. Alternatively, permit the use of only encrypted and password-protected flash drives.
h. Utilize secure communication channels for all voice calls pertaining to the arbitration process.

Information security measures recommended for physical and environmental security:

a. Ensure the implementation of measures to prevent the loss or theft of devices, including mobile storage devices, and establish the capability to remotely erase the data stored on such devices in the event of their loss or theft.
b. Take appropriate actions to safeguard the confidentiality of information contained in hard copies of data pertaining to the arbitration.
c. Evaluate and implement security protocols for any designated listening rooms or breakout rooms, particularly those situated in public buildings such as hotels.
d. Utilize privacy screens on laptops and mobile devices when accessing arbitration-related materials while in transit or in public areas.
e. Configure laptops and mobile devices to automatically activate screen lock after a specified period of inactivity.

It is important to highlight that there are significant repercussions associated with retaining outdated records that have surpassed their useful lifespan. In the field of cybersecurity, professionals often emphasize the phrase, "They can't hack what you don't own." While the process of mapping assets and architecture may present challenges, practitioners still find value in utilizing old records as references or examples for future projects. Therefore, completely eliminating old records may not be practical from a business standpoint. However, certain types of documents, such as exhibits containing personally identifiable information, may offer minimal or no future business benefits and can be disposed of without significant impact on operations (Pastore, 2017).

Information security measures recommended for operational security:

a. Ensure timely correction of all systems or devices housing arbitration-related information upon the issuance of corrections.
b. Continuously monitor system vulnerabilities and promptly notify other arbitration participants of any identified vulnerabilities in compliance with relevant laws, regulatory frameworks, or agreed incident response plans for the arbitration process.

Recommended information security measures for managing information security incidents:

a. In consideration of any relevant regulatory or professional ethical obligations and taking into

account the existing infrastructure of the parties, it is recommended that measures be implemented to address any potential information security incidents that may arise during the arbitration period. Table E provides resources that may be utilized in the development of an incident response plan.

b. It is advisable to establish clear procedures and expectations for notifying parties, arbitrators, arbitration institutions, or regulators of any information security incidents that may arise in connection with the arbitration. These procedures should include, among other things, a definition of what constitutes an "incident" triggering notification obligations, the timing of such notice (typically upon discovery of the incident), the method of notification, and the manner in which notice is provided. The recipient of such notice should also be specified.

c. The parties should agree to reasonably cooperate in any investigation and/or remediation of any information security incidents related to the arbitration.

d. The parties should also agree on their respective rights and obligations with respect to any public statements made regarding any information security incidents related to the arbitration.

6.2.5. Table "D": Examples of recommended formats for information security in arbitration

Please be advised that Table "D" contains the form of the arbitration agreement, should the parties mutually decide to incorporate a provision stating the utilization of reasonable security measures during the arbitration process. The prescribed format for such a statement is as follows.

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 (ICCA, 2020)."

In addition, Appendix "D" encompasses formulations of procedural orders that the arbitral tribunal may issue to effectively address cases necessitating its intervention and pertaining to matters of information security.

7. The extent to which evidence resulting from a cyber-breach is permissible

The arbitral tribunal encounters a predicament when confronted with evidence that has been obtained from an unlawful source, namely, in violation of the law. Subsequently, the court is confronted with the decision of either admitting or rejecting such evidence. This issue is progressively escalating, particularly with the proliferation of cyber intrusions in today's technologically driven world (Blair and Gojkovic, 2018).

In the case of Methanex v. United States, the arbitral tribunal faced the challenge of dealing with evidence that was obtained unlawfully. Methanex attempted to introduce documents they claimed to have found in waste and rubbish to support their position. However, the court decided not to admit this evidence. Further, the arbitral tribunal evaluated the unlawfully sourced evidence and found that it had minimal probative value, ultimately ruling against its admission.

In the Youkous ruling, which resulted in a $50 billion damages award, the court heavily relied on confidential diplomatic cables from the United States State Department that were unlawfully obtained and subsequently published on WikiLeaks (Hulley Enterprises Limited (Cyprus) v. The Russian Federation; UNCITRAL, PCA Case No. 2005-03/AA226, 20 Apr 2016). Notably, the court did not provide any analysis regarding the admissibility of illegally obtained evidence. However, other arbitration awards have addressed the issue of admitting evidence obtained through cyber intrusions, such as in the cases of Libananco Holdings Co. Limited v. Republic of Turkey (ICSID Case No. ARB/06/8, 2 Sep 2011), Caratube International Oil Company LLP v. The Republic of Kazakhstan (ICSID Case No. ARB/08/12, 5 Jun 2012), and ConocoPhillips Petrozuata v. Bolivarian Republic of Venezuela (ICSID Case No ARB/07/30).

These decisions by arbitral tribunals seem to establish the identity of the party responsible for the wrongful act, regardless of whether the documents were confidential or not and whether the disclosed information was material to the decision at hand or not.

8. Conclusion and recommendations

The study focuses on the crucial role of confidentiality in international commercial arbitration, highlighting it as a foundational element of the arbitration process. It discusses the threats posed by cyberattacks to this confidentiality and stresses the need for measures to secure information and documents shared during arbitration in digital environments. Additionally, the study offers recommendations for achieving effective cybersecurity in arbitration, drawing on established practices that protect against cyber threats.

It also addresses the issue of evidence obtained illegally and its admissibility in arbitration proceedings. The study emphasizes the importance of all parties agreeing to a common cybersecurity protocol, which serves as a collective action framework to achieve cybersecurity, while also noting that this protocol does not prevent the adoption of additional data protection measures required by local arbitration regulations.

The findings advocate for a comprehensive understanding of information security policies by all participants in the arbitration process, warning that any violation could compromise the entire information security system. The study suggests that electronic dispute resolution service providers implement encryption, firewalls, and passwords to

safeguard confidentiality and prevent unauthorized data access.

The ongoing threat of cyberattacks necessitates proactive defense strategies by arbitration participants, as outlined in the protocol. The study also recommends that insurance companies consider offering products that cover cyberattacks.

Furthermore, it proposes that the UNCITRAL Committee develop a model law on cybercrimes to guide international action and help harmonize national laws concerning information security, aiming to resolve issues arising from multiple legislative frameworks. For institutional arbitration, it is suggested that arbitration institutions engage with specialized information security firms with clearly defined responsibilities and liabilities outlined in their contracts. In ad hoc arbitrations, the parties should agree beforehand on who will handle information security.

These recommendations aim to foster a culture of information security among professionals in commercial arbitration, recognizing that individual adherence to security practices is critical in defending against cyber threats.

Acknowledgment

The authors gratefully acknowledge the approval and support of this research study by Grant No. BSAA-2022-11-1628 from the Deanship of Scientific Research at Northern Border University, Arar, KSA.

Compliance with ethical standards

Conflict of interest

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

References

AAA (2021). AAA rules, forms and fees. American Arbitration Association, New York, USA.

Awaisheh SM (2023). Digital justice in Jordan: The role of virtual arbitration sessions in modernizing the legal system. International Journal of Cyber Criminology, 17(1): 146-165.

Blackaby N, Partasides C, Redfern A, and Hunter M (2023). Redfern and hunter on international arbitration: Student version. Oxford University Press, Oxford, UK.

Blair C and Gojkovic EV (2018). WikiLeaks and beyond: Discerning an international standard for the admissibility of illegally obtained evidence. ICSID Review: Foreign Investment Law Journal, 33(1): 235-259. https://doi.org/10.1093/icsidreview/six030

Chaisse J and Bauer C (2019). Cybersecurity and the protection of digital assets: Assessing the role of international investment law and arbitration. Vanderbilt Journal of Entertainment and Technology Law, 21(3): 549-590.

Cohen S and Morril M (2017). A call to cyberarms: The international arbitrator's duty to avoid digital intrusion. Fordham International Law Journal, 40(3): 981-1022.

CRCICA (2024). Arbitration rules. The Cairo Regional Centre for International Commercial Arbitration, Cairo, Egypt.

Cremades BM and Cortes R (2013). The principle of confidentiality in arbitration: A necessary crisis. Journal of Arbitration Studies, 23(3): 25-38. https://doi.org/10.16998/jas.2013.23.3.25

ICCA (2020). ICCA-NYC Bar-CPR protocol on cybersecurity in international arbitration. International Council for Commercial Arbitration, New York, USA.

ICDR-AAA (2023). Rules, forms and fees. International Centre for Dispute Resolution, New York, USA.

Landolt P and Garcia A (2017). Commentary on WIPO arbitration rules. WIPO Arbitration and Mediation Center, Geneva, Switzerland.

LCIA (2020). LCIA arbitration rules 2020. LCIA, London Court of International Arbitration, London, UK.

Lee J (2020). The coronavirus pandemic and international investment arbitration-application of "security exceptions" clauses in investment agreements. Contemporary Asia Arbitration Journal, 13(1): 185-204.

McKeon RW (1994). Electronic data interchange: Uses and legal aspects in the commercial arena. UIC John Marshall Journal of Information Technology and Privacy Law, 12(4): 511-536.

Pastore J (2017). Practical approaches to cybersecurity in arbitration. Fordham International Law Journal, 40(3): 1023-1032.

Pauwelyn J (2023). The WTO's multi-party interim appeal arbitration arrangement (MPIA): What's New? World Trade Review, 22(5): 693-701. https://doi.org/10.1017/S1474745623000204

Shehata I (2018). Three potential imminent benefits of blockchain for international arbitration: Cybersecurity, confidentiality and efficiency. Young Arbitration Review. Available online at: https://ssrn.com/abstract=3290028

SIAC (2016). Arbitration rules of the Singapore International Arbitration Centre. Singapore International Arbitration Centre, Downtown Core, Singapore.

Singer DC (2020). Arbitration privacy and confidentiality in the age of (Coronavirus) technology. Alternatives to the High Cost of Litigation, 38(7): 107-108. https://doi.org/10.1002/alt.21849 **PMCid:PMC7361227**

Sussman E (2018). Cyber attacks: Issues raised in arbitration. New York Dispute Resolution Lawyer, 11(2): 10-12.

Yu HL (2020). 'Business as usual' during an unprecedented time-the issues of data protection and cybersecurity in international arbitration. Contemporary Asia Arbitration Journal, 13(1): 45-66.