

INTERNATIONAL ARBITRATION
SURVEY: CYBERSECURITY IN
INTERNATIONAL ARBITRATION

DON'T
BE THE
WEAKEST
LINK

BCLP'S INTERNATIONAL ARBITRATION GROUP

Over the last eight years, we have conducted a number of surveys on issues affecting the arbitration process:

- Unilateral Arbitrator Appointments (2017)
- Increasing Diversity on Arbitral Tribunals (2016)
- The Use of Tribunal Secretaries (2015)
- Choice of Seat (2014)
- Document Production (2013)
- Delay (2012)
- Conflict of Interest (2010)

The report on each of those studies can be found on our International Arbitration practice page at www.bclplaw.com

WORKING TOGETHER

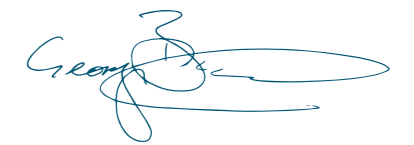
CYBERSECURITY IN INTERNATIONAL ARBITRATION

For this year's BCLP arbitration survey we wanted to consider the issue of cybersecurity. Are participants in international arbitrations sufficiently aware of the need to protect electronic data used in an arbitration against unauthorised access by third parties? Should more be done to promote risk assessment and the taking of active steps to enhance data protection?

In recent years there has been a dramatic increase in cyber-attacks on corporates, governments and international organisations. Media reports of such attacks are commonplace. Arbitration proceedings are not immune from these threats and debate on this subject raises a number of important issues that have yet to be navigated. The topic justifies considered examination by the arbitral community on how best to address the problem and who should take the lead in formulating a suitable cybersecurity strategy in individual cases.

We have once again canvassed the opinions of the many international arbitration practitioners and users with whom we work.

We would like to thank all those who responded to the survey.



GEORGE BURN
Head of International Arbitration



George Burn
Head of International Arbitration

Carol Mulcahy
Partner responsible for the BCLP
arbitration survey

Claire Morel de Westgaver
Senior Associate with particular
interest in cybersecurity in arbitration

WHY DOES CYBERSECURITY MATTER?

Cyber-attacks are an unfortunate but relatively common occurrence in today's world. There is no reason to assume that information collected, shared and used in an arbitration is immune from the threat of a targeted or opportunistic attack. Electronic documents and other information are introduced into arbitration proceedings in vast quantities.

Disputes referred to international arbitration have characteristics that can lead to an increased level of risk and adverse commercial consequences in the event of a security breach. These include the sharing of sensitive or commercially valuable information, the high volume of data transferred from one participant to another, the often high value/high stakes nature of the dispute, cross-border travel, and frequent use of mobile devices to access data.

Law firms are recognised as potential targets. A recent ethics opinion issued by the New York State Bar Association noted that...

"Law Cyber-security issues have continued to be a major concern for lawyers, as cyber-criminals have begun to target lawyers to access client information, including trade secrets, business plans and personal data. Lawyers can no longer assume that their document systems are of no interest to cyber-crooks."

Examples of cyber intrusion involving international arbitration include:



The attack on the website of the Permanent Court of Arbitration during the China-Philippines maritime boundary dispute.



The electronic surveillance undertaken in ICSID case Libananco v Turkey.

Carelessness with data by tribunal members, counsel, experts or witnesses can be as dangerous as targeted attacks - mobile devices left in public places or data loaded on to USB sticks and forgotten about when the dispute ends.

The consequences of a breach in data security can be significant. In many arbitrations one or more of the parties may have introduced into the proceedings commercially valuable data such as business models, distribution networks, technical formulae, or other proprietary information and commercial know how. If such data falls into the wrong hands it may result in economic loss.

Data loss may also result in reputational damage to the tribunal, to counsel and to any supervising institution. Parties to international arbitration expect to enjoy reasonable standards of privacy in relation to data used in the arbitration. Confidentiality of process is the reason many parties choose arbitration over other methods of dispute resolution.

In recent years the subject of cybersecurity has generated a fair amount of attention in the legal press. In addition to increased awareness of the problem, there appears to be a genuine appetite for engaging with the issues and arriving at a "best practice" approach that includes data protection steps, and protocols for data breach notification/return of data at the end of a dispute.

The most recent manifestation of this has been the Cybersecurity Protocol for International Arbitration published by ICCA (International Council for Commercial Arbitration), CPR (International Institute for Conflict Prevention and Resolution) and the New York City Bar.

The authors of that document intend it to be used as a framework that parties and arbitrators can consult in order to determine reasonable cybersecurity measures for their individual dispute. The Protocol will not apply unless it is adopted by agreement of the parties or a decision of the tribunal. Available only in draft at the moment, when published the Protocol will be a valuable addition to soft law on this topic.



Cybersecurity is a top priority to our clients and for most of us who sit as arbitrator. It is about defending the future of International Arbitration in a world increasingly dominated by technology.

Claire Morel de Westgaver



~~ONE
SIZE
FITS
ALL~~

Most commentators on cybersecurity in arbitration agree that there is no "one size fits all."

There are a range of security measures that may be put in place but those steps will only work effectively if all participants in the arbitration process "buy in" to them and take shared responsibility for their implementation. In practice, this may only be arrived at by consultation, discussion and a large measure of consensus on what will work.

RISK ASSESSMENT

A common recommendation is that participants start with a risk assessment. This involves thinking about the type of data likely to be introduced into the arbitration.

- Will it include highly sensitive/confidential information?
- How will participants store the data and who will access it?

The nature of the industry or subject matter of the dispute may inform the answers to these questions. Other factors may include the identity of the parties – for example:

- Is there a history of being targeted or a profile that may attract an attack?
- What are the likely consequences if there were to be a data breach?
- Would there be economic loss, damage to reputation and/or the potential for misuse by a third party?

If the potential consequences are relatively minor then the need for onerous security measures may be considerably less than in cases where the adverse consequences of a breach are very significant.

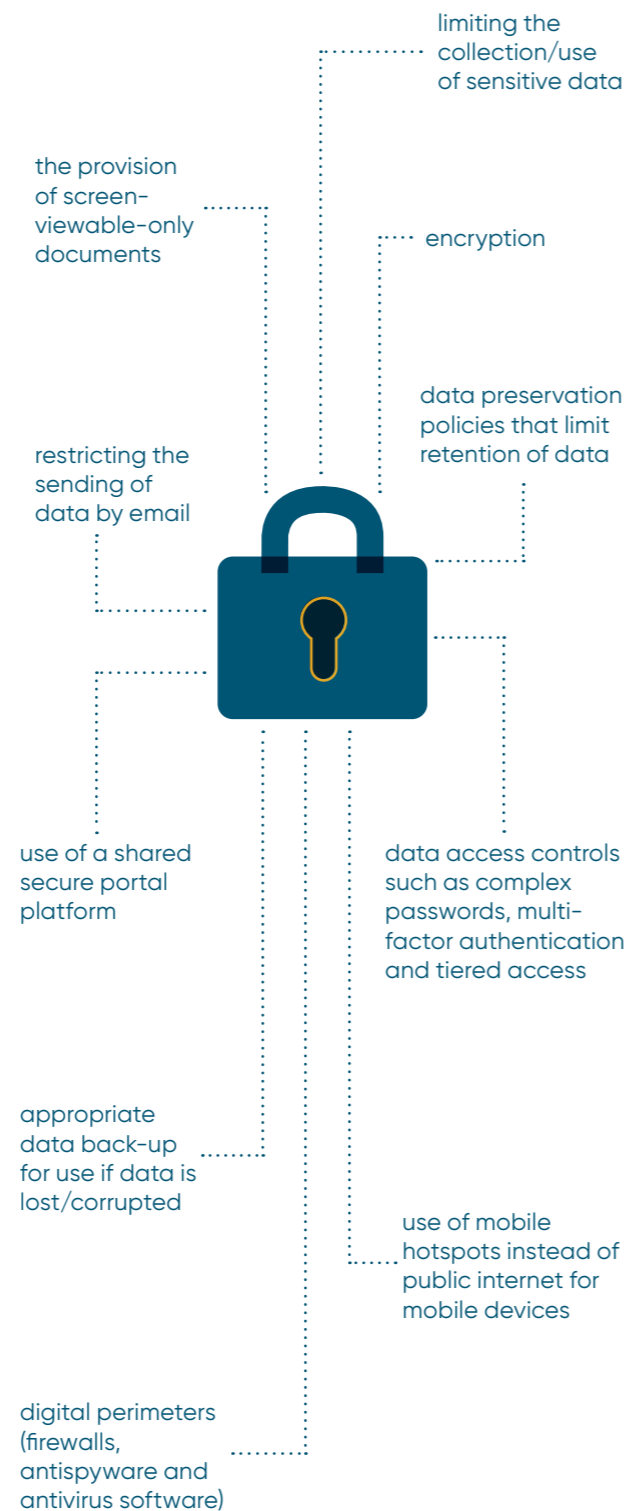
A risk assessment will inform a decision on what measures it is reasonable to take in an individual arbitration. However, there may still be significant differences between the parties in approach and perspective.

The data to which greater risk/sensitivity attaches may be on one side of the dispute. The parties may have different levels of risk tolerance. The value of the dispute may be relatively small, or a 'bet the company' case. Participants may have different working preferences relating to use/transmission of data, and the organisations within which they work may have different methods of organising data. In a large organisation where the IT and commercial/legal functions are separated there may be administrative and technical hurdles in tailoring data management to the needs of individual arbitration proceedings. Such factors may impact the relative ease with which the proposed security measures may be implemented and/or impose a different burden in time or costs on different participants to the process, each of whom may have different resources and capabilities. The measures may also have the potential to hinder efficiency. These factors lead to more difficult questions.

- How important are considerations of fairness and equality?
- To what extent should security measures be imposed on an unwilling party, or one simply unable to implement what is proposed?
- Are any additional costs incurred as a result of such measures to be treated as costs of the arbitration and allocated at the end of the arbitration in the usual way?

AVAILABLE MEASURES

Having identified the data landscape, participants must select appropriate security measures to address or mitigate the risks that exist. The available menu of measures is limited only by the technical knowledge and imagination of those involved. Relatively straightforward steps include:



WHO SHOULD TAKE THE LEAD?

TRIBUNAL

A further important issue is who should take the lead in initiating discussion on cybersecurity. The tribunal is an obvious contender. It is ideally placed to take an early lead by raising the issue of cybersecurity as part of routine discussions on case management and procedural timetable. If the tribunal has the necessary express or general power, it may then order the implementation of appropriate steps.

A related question is whether arbitration rules should be amended to include express provision for the tribunal to have such powers? Is existing provision on confidentiality (for example, Article 9.4 of the IBA Rules on the Taking of Evidence) sufficient or is there a distinction to be drawn between specific measures designed to protect the confidentiality of identified documents from misuse by one of the parties to the arbitration and broader measures intended to protect all data from possible attack by a third party.

- Should the tribunal's powers and responsibilities extend to the latter?
- Should the tribunal have power to impose sanctions in the event of a serious breach of measures agreed or ordered?
- Should there be a presumption against the admissibility of evidence obtained from a data breach?

In all cases, the tribunal is likely to have a role to play. If the parties cannot agree security measures there will have to be a determination on the competing considerations on each side. In addition to considerations of cost, efficiency and disparity in resources, it will be important to ensure that the measures put in place will not hinder a party in presenting its case. These are matters that may be said to be more suited to a judicial rather than an administrative function.

However, one criticism of leaving cybersecurity to the tribunal is that the arbitrator/s may not in all cases be best equipped to deal with it. Just as with parties and counsel, there are significant variations in the level of awareness, resources and technical knowledge of data security issues/risk abatement steps among arbitrators.

- Should arbitrators be required to take training in cybersecurity?
- Is cybersecurity a procedural matter falling within the scope of the tribunal's responsibilities?
- Is cybersecurity simply an administrative matter to be dealt with by the arbitral institution or by counsel?

INSTITUTIONS

Are institutions better placed than arbitrators to deal with issues of data security? Institutions can:

- make amendments to their rules;
- incorporate cybersecurity guidelines to be adopted;
- regulate the way in which data is stored and transferred;
- approach matters in a more systemic way thereby justifying investment of resources;
- encourage consistent "best practice"; and
- more easily address the issue of communications between tribunal members, and between institution and tribunal.

Institutions that seize the initiative on cybersecurity may gain a competitive advantage.

Is there a case to be made for institutions to retain dedicated cybersecurity consultants as part of the secretariat? If the institution were to take the lead on cybersecurity, the consultant could represent it in discussions with the participants in the arbitration. Alternatively, she or he could work with a tribunal to assist it supervising discussions between the parties on possible measures, and (to the extent necessary) the nature of the measures that it would be appropriate to impose. The consultant might also act independently of the tribunal as a resource available to the parties in discussions on the topic.

“Data security will only be as strong as the **weakest link**.”

THIRD PARTY CO-OPERATION

There may be issues around obtaining agreement from third party witnesses, experts and external service providers such as interpreters and data hosting agencies. Data security will only be as strong as the weakest link. What happens if one or more of these third parties is unwilling or unable to agree proposed measures that affect them? The tribunal has no jurisdiction over them.

WHAT WE ASKED

- Do respondents regard cybersecurity as an important issue?
- What measures have they used or consider desirable?
- Respondents' views on who should take the initiative in leading discussion on cybersecurity in an individual arbitration
- What support mechanisms would it be desirable to put in place?
- Respondents' opinion on some of the potential difficulties associated with organising cybersecurity measures
- How should the costs of such measures be distributed?

WHO WE ASKED

- Arbitrators
- Corporate counsel
- External lawyers
- Users of arbitration
- Those working at arbitral institutions
- Academics
- Expert witnesses

The geographical regions in which our 105 respondents work include Central and South America, North Africa, Western Europe, East and South East Asia, Australasia, the Middle East, Latin America and the Caribbean, Eastern Europe (including Russia and CIS), West and East Africa and North America.

KEY FINDINGS

AN IMPORTANT ISSUE

90% of respondents thought that cybersecurity is an important issue in international arbitration.

11% of respondents indicated that they had experience of a breach in cybersecurity (i.e. someone was able to obtain unauthorised access to electronic documents/other information) in an arbitration in which they had been involved.

A PROCEDURAL OR ADMINISTRATIVE MATTER?

Opinion was divided on whether the need for cybersecurity measures is a procedural or an administrative matter. Slightly more than half of respondents (52%) thought that it was a procedural matter for the tribunal. 42% felt that (in cases where there was a supervising arbitral institution) it was an administrative matter for the institution.

TRIBUNAL POWERS

52% of respondents felt that a tribunal should in all cases have the power to impose cybersecurity measures, and a very large percentage of respondents (71%) thought that a tribunal should have the power to impose sanctions for breach of measures either agreed by the parties or ordered by the tribunal.

A ROLE FOR ARBITRAL INSTITUTIONS

Respondents felt that arbitral institutions have an important role to play. 31% of respondents felt that the supervising arbitral institution (where there was one) should take the lead in initiating discussion on cybersecurity. 68% of respondents said that they would be more likely to use the arbitration rules of an institution that was able to provide advice and assistance on appropriate data security measures.

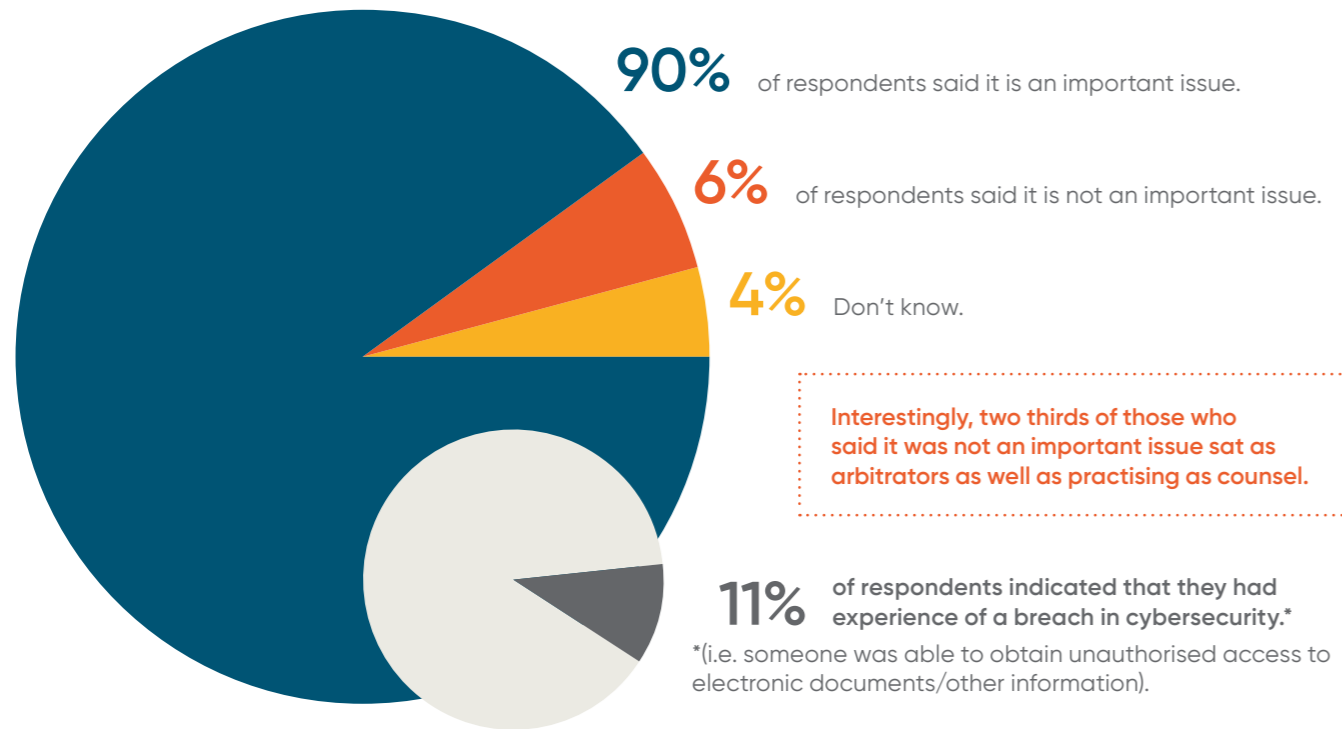
FACTORS RELEVANT TO A CYBERSECURITY STRATEGY

The two factors regarded by the largest number of respondents as being relevant to a cybersecurity strategy were the level of sensitivity/commercial value of the documents to be used in the arbitration (94%) and the consequences for the parties if someone gained unauthorised access to documents/information (78%). The extent to which security measures might hinder the ability of a party to present its case was considered relevant by only 61% of respondents.

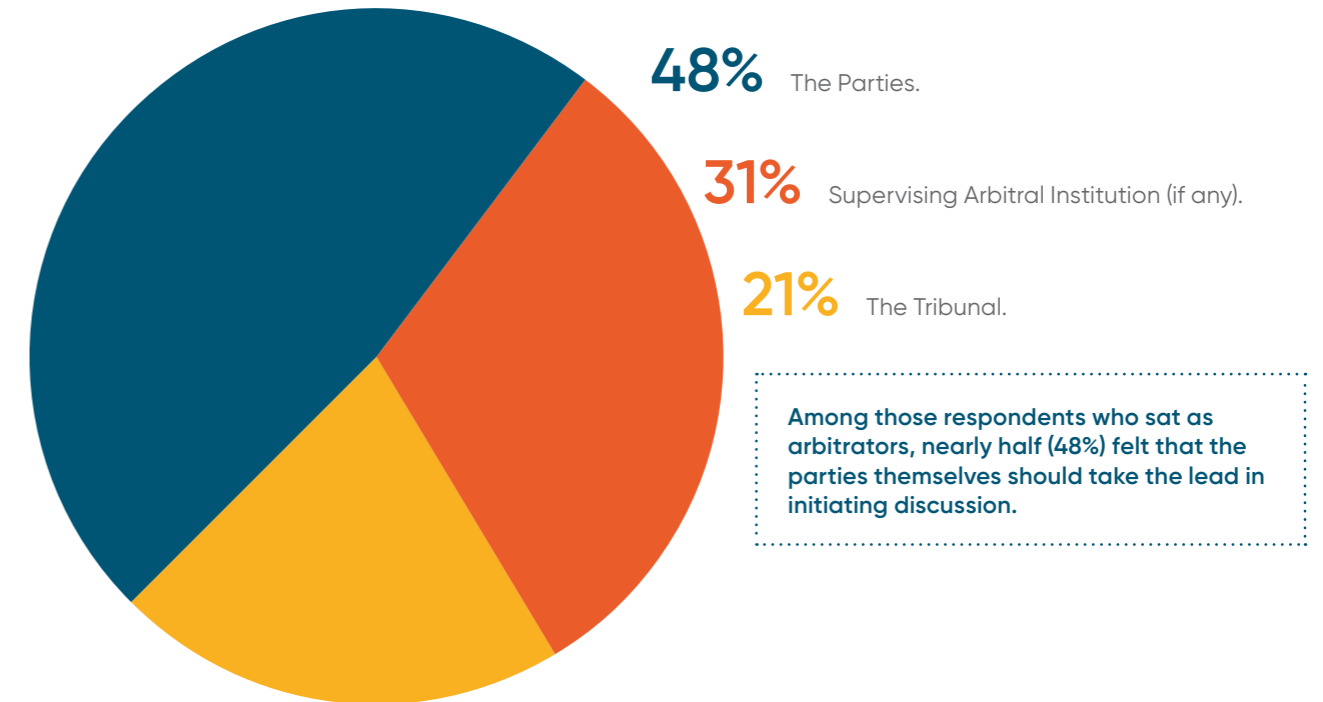


THE IMPORTANCE OF CYBERSECURITY AND WHO IS RESPONSIBLE

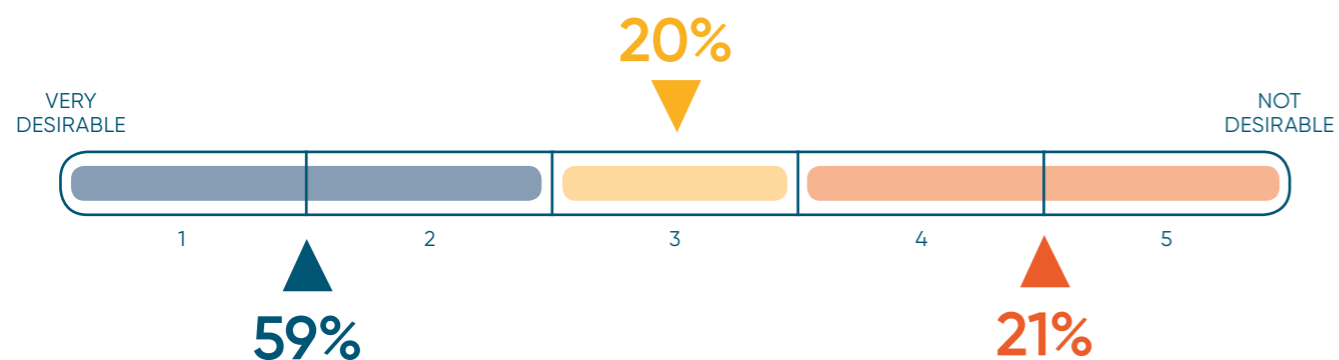
Q IS CYBERSECURITY IN INTERNATIONAL ARBITRATION AN IMPORTANT ISSUE?



Q WHO SHOULD TAKE THE LEAD ON INITIATING DISCUSSIONS ON CYBERSECURITY ISSUES?



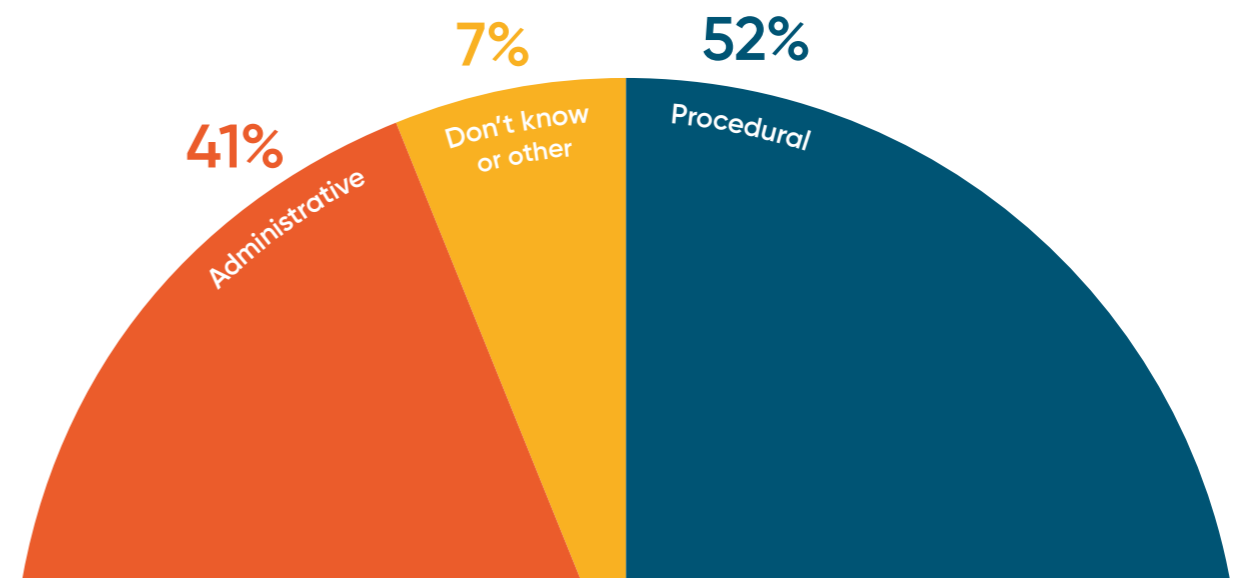
Q HOW DESIRABLE IS IT FOR PARTIES TO AN ARBITRATION TO CONSIDER AT AN EARLY STAGE IN THE PROCEEDINGS WHETHER IT IS APPROPRIATE TO PUT IN PLACE REASONABLE SECURITY MEASURES TO PROTECT ELECTRONIC DOCUMENTS AND OTHER INFORMATION IN THE ARBITRATION FROM UNAUTHORISED ACCESS?



Q IS CYBERSECURITY AN ADMINISTRATIVE OR PROCEDURAL MATTER?

Is the need to consider cybersecurity measures in an individual arbitration:

- An **administrative matter** - best handled by the supervising arbitral institution (assuming there is one)?
- A **procedural matter** - best handled by the tribunal after hearing submissions from the parties?

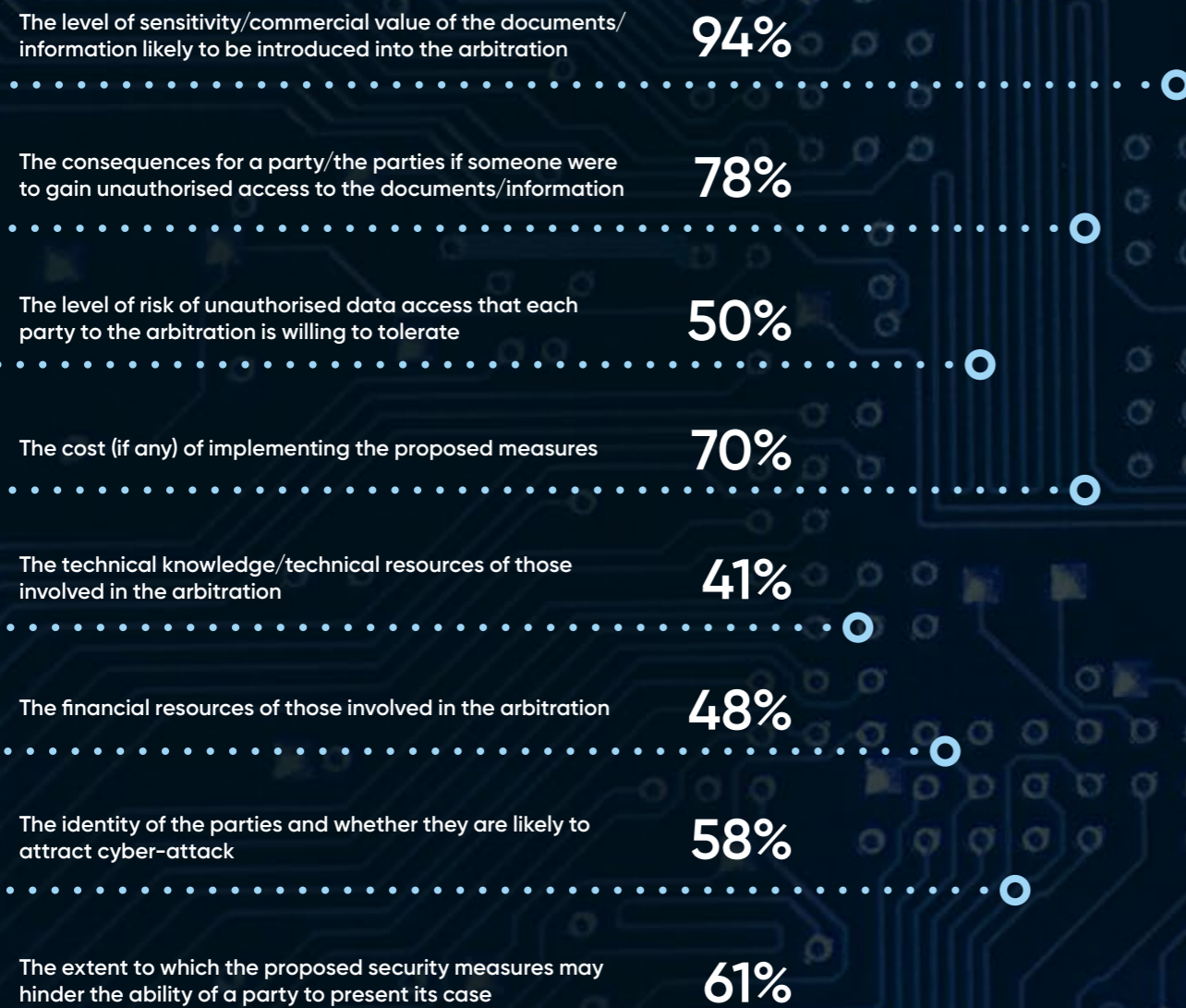


FORMULATING A CYBERSECURITY STRATEGY

Q WHAT FACTORS ARE RELEVANT TO FORMULATING A CYBERSECURITY STRATEGY?

We asked respondents to consider the factors that should be taken into account when deciding on the nature of measures (if any) that should be put in place to protect the security of electronic documents/other information in an individual arbitration.

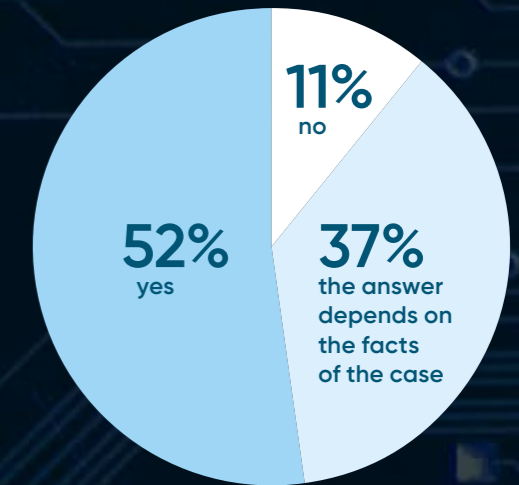
We asked respondents to select from a list of possible factors as many as they thought relevant to the decision on which measures to adopt:



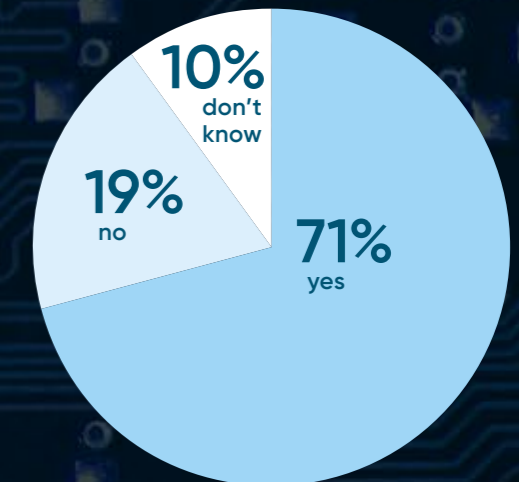
TRIBUNAL POWERS

We asked respondents for their opinion on tribunal powers to impose cybersecurity measures.

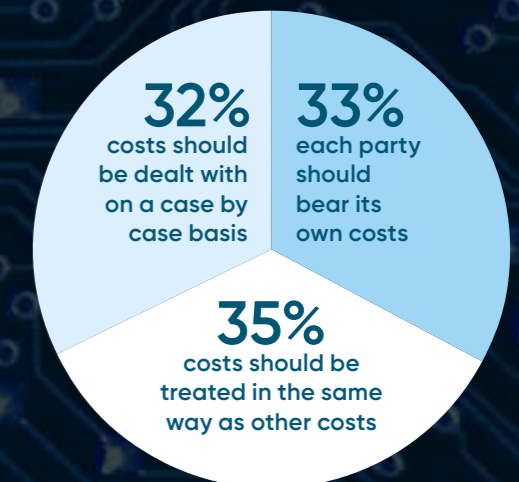
Q WHERE PARTIES CANNOT AGREE ON THE NATURE OF APPROPRIATE DATA PROTECTION MEASURES, SHOULD AN ARBITRAL TRIBUNAL HAVE THE POWER TO IMPOSE MEASURES ON THEM?



Q SHOULD THE ARBITRAL TRIBUNAL HAVE POWER TO IMPOSE SANCTIONS ON A PARTY THAT BREACHES DATA SECURITY MEASURES THAT HAVE BEEN AGREED OR ORDERED?



Q HOW SHOULD ANY ADDITIONAL COST BURDEN OF SECURITY MEASURES ORDERED BY AN ARBITRAL TRIBUNAL BE ADDRESSED?



CYBERSECURITY MEASURES: USED AND DESIRED

We were interested in exploring the correlation between cybersecurity measures that are adopted or imposed in practice and cybersecurity measures that respondents thought it would be desirable to adopt.

We asked respondents to indicate, by reference to a list of measures provided, which data security/mitigation steps to protect electronic documents/information had been agreed by the parties or imposed by the tribunal in arbitrations in which they had been involved.

For comparison purposes, we then asked respondents which of those same measures they thought it would be desirable to adopt in an arbitration.

In nearly all cases the percentage of respondents who felt a particular measure to be desirable was significantly higher than the percentage of respondents who had seen that measure used in practice in an arbitration in which they were involved.

The table opposite sets out the findings in full.

83%

of respondents thought it desirable for electronic documents to be transferred by means of a secure shared portal platform.

Opposed to **55%** who had seen the measure in practice.

50%

of respondents thought it desirable that steps be taken to verify that participants in an arbitration have in place appropriate firewalls and antispyware and/or antivirus software.

Opposed to **12%** who had seen the measure in practice.

50%

of respondents thought it desirable that data preservation policies be put in place that limit retention of electronic documents by a party after the arbitration is over.

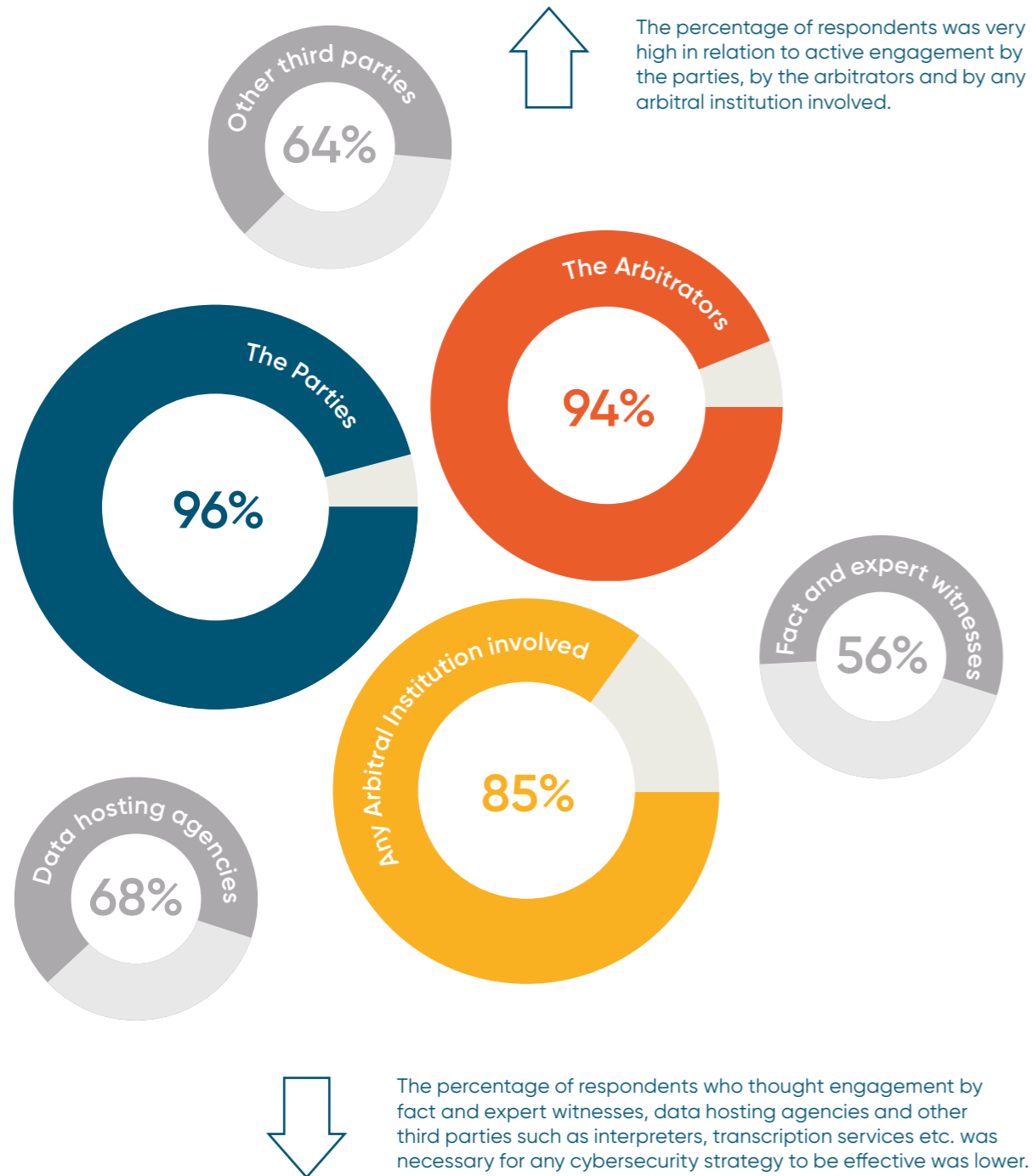
Opposed to **23%** who had seen the measure in practice.

CYBERSECURITY MEASURES	% WHO HAD SEEN THE MEASURE USED IN PRACTICE	% WHO THOUGHT THE MEASURE WAS DESIRABLE
Restricting the use of emails for sending electronic documents/other information.	16%	39%
Transfer of electronic documents by secure shared portal platform or similar.	55%	83%
Provision of screen-viewable-only documents.	8%	16%
Use of complex passwords/or multi-factor authentication to access electronic documents/information.	35%	56%
Encryption.	36%	63%
Restricting access to particular categories of electronic documents/other information to a limited number of individuals who have a demonstrated need to access that material (confidentiality clubs).	31%	46%
Restricting access to hard copies only of particular categories of document (usually kept in a single location).	22%	20%
Redaction of electronic documents before introduction in to the arbitration.	40%	30%
Agreement to limit use of public internet for mobile devices.	8%	34%
Verification that all participants to the arbitration have in place appropriate firewalls, antispyware and/or antivirus software.	12%	50%
Data preservation policies that limit retention of documents/ other information in electronic form after the arbitration is over.	23%	50%
Agreed notification procedures to be followed if a data security breach occurs.	12%	54%

ENGAGEMENT WITH CYBERSECURITY MEASURES

Q WHO WOULD NEED TO ACTIVELY ENGAGE WITH A CYBERSECURITY STRATEGY IN ORDER FOR IT TO BE EFFECTIVE?

Unsurprisingly, a majority of respondents thought that active engagement by all participants to an arbitration would be necessary if a cybersecurity strategy was to be effective.



Q HOW EASY WOULD IT BE TO OBTAIN AGREEMENT FROM THOSE PARTICIPANTS TO OBSERVE SECURITY MEASURES?

Respondents were asked to grade the degree of anticipated difficulty from 1 (very easy to obtain agreement) to 5 (very difficult to obtain agreement).



THE ROLE OF ARBITRAL INSTITUTIONS

We also asked respondents to consider the potential role of arbitral institutions and it was clear from their responses that arbitral institutions could play an important role in dealing with issues of cybersecurity.

Q WHAT POSSIBLE SUPPORT MECHANISMS PROVIDED BY AN ARBITRAL INSTITUTION MIGHT BE USEFUL?

70% of respondents felt that support from within an institution's secretariat would be useful to improve cybersecurity

62% thought that compulsory use of a secure platform hosted by the institution would be useful

Arbitration institutions to have a staff member within the secretariat experienced in data security measures and able to assist the parties/tribunal in deciding on appropriate security measures for an individual arbitration **70%**

Arbitration institutions to make compulsory the use of a secure platform hosted by the institution on which all communications and data sharing/storage would take place. The platform to have a discrete secure area for communication between members of the tribunal, and between the tribunal and the institution **52%**

Arbitration institutions or other organisations to offer cybersecurity training to arbitrators **61%**

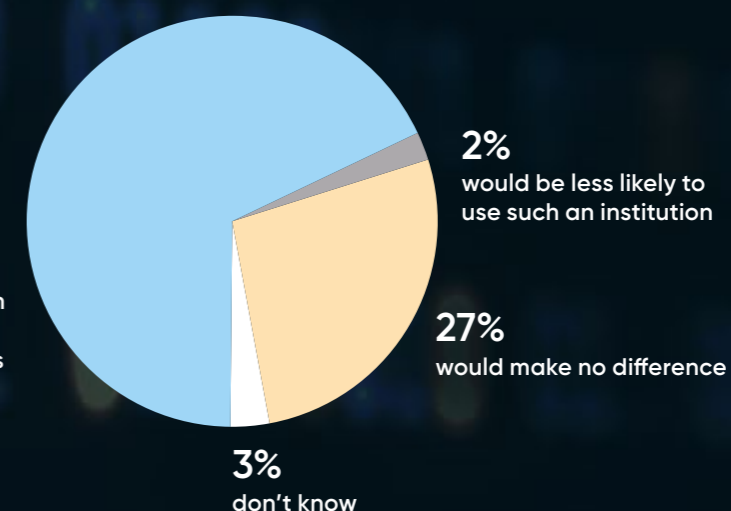
Arbitration institutions or other organisations to impose/offer cybersecurity certification to arbitrators **21%**

None of the above **5%**

Don't know **6%**

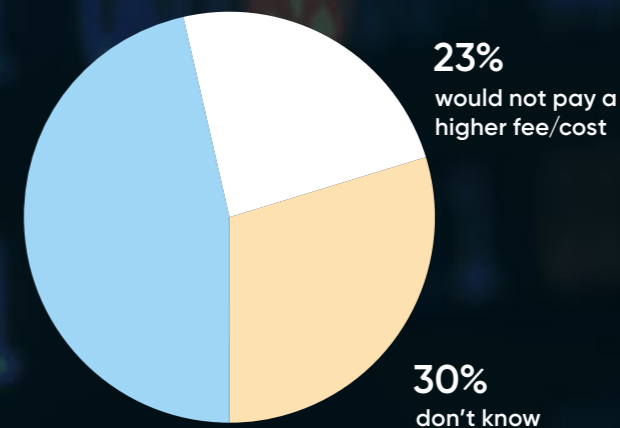
Q WE THEN ASKED RESPONDENTS WHETHER THEY WOULD BE MORE OR LESS LIKELY TO USE THE ARBITRATION RULES OF AN INSTITUTION THAT WAS ABLE TO PROVIDE ADVICE AND ASSISTANCE ON APPROPRIATE DATA SECURITY MEASURES FOR THE ARBITRATION.

68% would be more likely to use the arbitration rules of an institution that was able to provide advice and assistance on appropriate data security measures



Q WE ALSO ASKED WHETHER RESPONDENTS (OR, WHERE APPROPRIATE, THEIR CLIENTS) WOULD BE WILLING TO PAY A HIGHER FEE/INCUR AN ADDITIONAL COST WITH AN ARBITRATION INSTITUTION THAT PROVIDED ADVICE AND ASSISTANCE ON APPROPRIATE DATA SECURITY MEASURES AND/OR PROVIDED A SECURE PLATFORM (OR SIMILAR) ON WHICH ALL COMMUNICATIONS AND DATA SHARING/STORAGE IN THE ARBITRATION COULD TAKE PLACE.

47% would be willing to pay a higher fee/cost



GETTING IN TOUCH

When you need a practical legal solution for your next business opportunity or challenge, please get in touch.

London

Adelaide House, London Bridge
London EC4R 9HA England

GEORGE BURN

george.burn@bclplaw.com
T: +44 (0)20 3400 2615