Practical Law™

CYBER SECURITY ISSUES IN ARBITRATION

This document is published by Practical Law and can be found at: uk.practicallaw.com/**w-003-5790**
Request a free trial and demonstration at: **uk.practicallaw.com/about/freetrial**

This note sets out a checklist of cyber security risks for parties and arbitrators to consider at the outset of their arbitration. The checklist aims to help the parties, tribunal and arbitral institution to conduct an assessment of the information security needs of the arbitration and to adopt tailored safeguards which minimise the risk of a security compromise during the proceedings. The bespoke assessment also helps to avoid a more expensive and complicated security system than is necessary.

Hanna Roos and *Jennifer Archie, Latham & Watkins LLP*

RESOURCE INFORMATION

RESOURCE ID
w-003-5790

RESOURCE TYPE
Practice note

PUBLISHED DATE
15 December 2016

JURISDICTION
International

CONTENTS

- Scope of this note
- Why worry about cyber security?
- How and to what extent to safeguard your data during arbitration?
- Cyber security checklist
- Recommendations

SCOPE OF THIS NOTE

Cyber security breaches are now an everyday reality permeating all aspects of business and private life, including the world of international commercial and investment treaty arbitration. These breaches can relate to the subject matter of the dispute, communications between parties and their counsel or between tribunal members or the website and IT systems of the parties or the arbitral institution, among others. This note sets out the circumstances in which a cyber security breach may occur, the necessary tools to conduct a risk assessment and the appropriate safeguards to adopt to prevent a cyber security breach from occurring during an arbitration.

WHY WORRY ABOUT CYBER SECURITY?

Cyber security means keeping electronic data and IT systems safe from unlawful access, use, alteration, destruction and disclosure. Cyber security breaches have become the daily reality of high profile companies, law firms, persons and courts, including arbitral institutions, as well as a top priority for governments.

The results of a security compromise can be devastating and include loss of confidentiality of data, loss of integrity (where data is tampered with) and loss of availability (for example, when a website and internal IT system is rendered unavailable, known as a "Denial of Service"). This can further lead to:

- Contractual and tortious liability towards individuals seeking compensation for damage, distress, or both.
- Prosecution and regulatory sanctions.
- Reputational damage from adverse media coverage.

For more information, see *Practice note, Overview of cyber security*.

Reproduced from Practical Arbitration with the permission of the publishers. For further information visit practicallaw.com or call 0207 542 6664. Copyright © 2016 Thomson Reuters (Professional) UK Limited.. All Rights Reserved.

THOMSON REUTERS™

Cyber security is particularly relevant in commercial arbitration where parties often choose arbitration for its confidentiality. If the contract between the parties contains an agreement to keep data confidential, and to meet particular standards of care in data practices, a security breach could trigger contractual liability.

The rules of an arbitral institution may import additional confidentiality obligations. For example, Article 30 of the London Court of International Arbitration (LCIA) Rules 2014 (LCIA Rules), which the parties adopt when choosing an LCIA arbitration, provides, subject to certain exceptions, that "[t]he parties undertake ... to keep confidential all awards in the arbitration, together with all materials in the arbitration created for the purpose of the arbitration and all other documents produced by another party in the proceedings not otherwise in the public domain ...". Confidentiality extends to the tribunal ("[t]he deliberations of the Arbitral Tribunal shall remain confidential to its members") and to the LCIA ("[t]he LCIA does not publish any award or any part of an award without the prior written consent of all parties and the Arbitral Tribunal"). A leak into the public domain of the award, pleadings, witness and expert evidence, factual evidence produced by the other side and email deliberations among the tribunal would arguably breach these obligations.

Reputational damage can also be devastating. The reported breaches have been highly publicised. Examples include the hacking of the Permanent Court of Arbitration's (PCA) website during a hearing of a sensitive maritime border dispute between the Philippines and China, believed to be carried out by Chinese hackers (see *The Diplomat, Did China Just Hack the International Court Adjudicating Its South China Sea Territorial Claims?*). Security breaches can undermine the credibility of law firms, tribunals and arbitral institutions storing the data, and erode confidence in arbitration generally.

The PCA hack also illustrates the interconnectedness of the arbitral ecosystem. The hackers are understood to have exploited a flaw in Adobe Flash and created a malicious web address which visitors to the PCA webpages unknowingly loaded. If the visitors accessed the pages using computers installed with Adobe Flash, these computers too may have been affected, permitting the hackers to access their networks remotely. It is therefore important that everyone who is involved in proceedings protects its data and IT system adequately.

HOW AND TO WHAT EXTENT TO SAFEGUARD YOUR DATA DURING ARBITRATION?

It can be difficult to identify what specific set of cyber security standards are required or most appropriate.

Institutional rules tend to be silent on cyber security. However, various national cyber security regimes may be engaged depending on the jurisdictional nexus of the arbitration and which laws affect the parties, tribunal and institutions. For example, on 19 July 2016, the EU published its first cyber security directive 2016/1148, which imposes safeguarding obligations on operators of essential services, such as transport, health and finance, and for digital service providers, such as online marketplaces, search engines and cloud services (see *Legal update: archive, Cyber-security: Directive (EU) 2016/1148 on network and information security published in Official Journal*). In the United States, governmental authorities have the statutory authority to supervise cyber security plans and controls, for example for health care plans and organisations, financial institutions, critical infrastructure companies, defence contractors, and companies handling consumer data, among others.

Further, as a practical matter, there is no one-size-fits-all solution to protecting data, whether in arbitrations or otherwise. An off-the-shelf policy downloaded from the internet does not have regard to what is being protected and each institution's internal processes. A systematic risk assessment, based on an individualised inventory of sensitive data sets and systems, is the first step for any risk mitigation program.

The framework below (see *Cyber security checklist*) aims to help parties, tribunals and institutions to review their particular circumstances at the outset of the arbitration irrespective of the jurisdictions involved. The aim is to avoid the extreme alternatives which may see parties either ignoring the issue entirely or adopting a more expensive and expansive security plan than is necessary.

Reproduced from Practical Law Arbitration with the permission of the publishers. For further information visit practicallaw.com or call 0207 542 6664. Copyright © 2016 Thomson Reuters (Professional) UK Limited.. All Rights Reserved.

CYBER SECURITY CHECKLIST

1) What are the key assets?	2) Who may be after them?	3) Who is the softest target?	4) How may the target be hacked?	5) Likelihood of adverse consequences?	6) What safeguards to adopt?
The dispute relates to • **Commercially valuable assets** (trade secrets, IP) • **Assets that may be easily monetized** (bulk customer details, health or credit data, arbitrators' personal details stored by institute etc)	• Party's competitors • Specialised criminal outfits looking to sell data	• In how many places is the data located? • Is counsel's data management system used to store data in relation to the dispute? • As between the counsel and client, whose data system is less secure and therefore the likely target?	Data theft through unauthorised access. Attack vectors may include • Customised attacks designed to target specific data • Spear phishing and social engineering to gain access to credentials or data • Account takeovers	• How valuable is the data to third parties? • Is access to the systems tightly controlled, audited, alarmed and encrypted?	• Ring-fencing (separating data from the rest of the IT system)? • Software to track anomalous activity? • Encryption of data? • Encrypted transmission of sensitive data between client and counsel? • Written policies and procedures governing storage, access and transmission? • Legal requirements in the contract, institutional rules or national law?
Communications between • Party and its counsel • Tribunal members • Arbitral institute members e.g. in relation to arbitrator's disclosures of interest and independence, or draft award	• The other side? In *Libananco v Republic of Turkey (ICSID ARB/06/8)*, Turkey admitted to surveying Libananco's and its counsel's emails • An interested third party? If the parties or dispute are political or high profile, "hactivists" may be looking to expose communications to public scrutiny. A famous example is the leak of 11.5 million attorney-client documents of the Panama law firm Mossack Fonseca	• Which email server is the least protected? • Public email (web mail) accounts are particularly vulnerable to attack	Data theft through • Spear phishing and social engineering to gain access to credentials or data • Account takeovers	• Does the dispute involve a party or interested third party with a sophisticated cyber-capability, for example ability to intercept calls and emails? • How high profile or political are the parties and the dispute? • How embarrassing or damaging would interception or an online leak be?	• Software to track anomalous activity? • Tribunal not to use web email accounts? • Encrypted email? • Encrypted phone lines (e.g. designated mobile phones)? • Written policies and procedures governing communications? • Legal requirements in the contract, institutional rules or national law?
Materials created in the arbitration • Pleadings, witness and fact evidence in relation to the matters in dispute • Award and its draft versions	• Do these contain commercially valuable/monetizable information? See first row above. • Hactivists looking to cause embarrassment by leaking online confidential awards and pleadings held by institutions?	• In how many places is the data located? • Which email server is the least protected?	See above	• Is the matter of public interest and/or involve interested state parties? • If an arbitral institute's IT system is hacked, what is the degree of reputational damage and risk of liability for the institute from a leak of awards, evidence, pleadings and deliberations in relation to potentially hundreds of cases?	See above

Reproduced from Practical Arbitration with the permission of the publishers. For further information visit practicallaw.com or call 0207 542 6664. Copyright © 2016 Thomson Reuters (Professional) UK Limited.. All Rights Reserved.

1) What are the key assets?	2) Who may be after them?	3) Who is the softest target?	4) How may the target be hacked?	5) Likelihood of adverse consequences?	6) What safeguards to adopt?
Website and IT system of parties and arbitral institution	Hactivists looking to cause embarrassment by defacing a website or rendering IT system unusable (Denial of Service)? • The Permanent Court of Arbitration website was made unavailable in July 2015 by suspected Chinese actors in context of a dispute involving China • In November 2014, Sony's hackers rendered the company's entire IT system unavailable	• How difficult is it to gain control of the company's or arbitral institution's website? What about its social media page?	Unauthorised access leading to • Defacement of website • Unavailable IT system (Denial of Service) • Erasing data from servers	• Is the matter of public interest and/or involve interested state parties? • How damaging would defacement, Denial of Service or deletion of data be?	• See above • Ensure tight access controls to websites?

RECOMMENDATIONS

A tailored and systematic risk assessment along the lines of the checklist above will help parties map out the likelihood of risks and whether and which precautions are appropriate.

The assessment must also ask more broadly whether there are other legal areas which the cyber security policy needs to consider (see bullet "Legal requirements in the contract, institutional rules or national law?" in column six of the checklist). There may be regulatory cyber security obligations, for example imposed by the EU cyber security directive 2016/1148 discussed above (see *How and to what extent to safeguard your data during arbitration?*).

The parties, tribunal and institution should each also have a blueprint for responding quickly to a security breach and mitigating its effects, including making timely notifications required by law or contract.

A related consideration is whether the parties, tribunal and arbitral institution wish to request indemnities from one another to cover the expense of responding to breaches or follow-on governmental inquiries, or damages claimed by third parties (such as employees) flowing from cyber security breaches where one of the parties, arbitrators or institution is at fault.

The parties and tribunal should ideally address cyber security needs at the outset of the arbitration and no later than at the first procedural conference. This is an opportunity to allocate the responsibility to manage and mitigate legal and financial consequences of breach.

Arbitral institutions may also wish to differentiate their rules from those of other institutions by incorporating into the rules the obligation to adopt appropriate cyber security obligations.

Reproduced from Practical Law Arbitration with the permission of the publishers. For further information visit practicallaw.com or call 0207 542 6664. Copyright © 2016 Thomson Reuters (Professional) UK Limited.. All Rights Reserved.