Fordham International Law Journal

Volume 40, *Issue* 3 2017 *Article* 12

Practical Approaches To Cybersecurity In Arbitration

Jim Pastore*

PRACTICAL APPROACHES TO CYBERSECURITY IN ARBITRATION

Jim Pastore[*]

INTRODUCTION

In July of 2015, the Permanent Court of Arbitration in The Hague held a hearing over the dispute between the Philippines and China over territory in the South China Sea. On the third day of the hearing, the Court's website suddenly went offline, an event which turned out to be the result of a cyberattack that originated in China. The hackers had infected the site with malware, making it so that anyone who visited the site was subject to data theft.[1] With cyberattacks becoming increasingly more prevalent in all sectors of society, even a highly publicized and contentious international arbitration unfolding in the public eye was not immune.

Cybersecurity is in fact becoming increasingly relevant in the context of arbitration, which continues to be a popular choice of conflict resolution for parties involved in complex and sensitive international disputes. In these types of disputes, digital discovery is inevitable and may include confidential information including trade secrets, financial information, and personally identifiable information.

---

* Mr. Pastore is a litigation partner at Debevoise & Plimpton LLP, where his practice focuses on cybersecurity and data privacy matters, as well as intellectual property litigation. Mr. Pastore served for more than five years as an Assistant United States Attorney in the Southern District of New York, where he prosecuted a number of cybercrimes cases including *United States v. Monsegur, a/k/a* "*Sabu*"; Operation Cardshop; Operation Dirty R.A.T., and the Rove Digital organization as part of Operation Ghost Click. I wish to thank my associates, Max Shaul and Michael Brady, for their important contributions to this article.

1. Jason Healey & Anni Piiparinen, *Did China Just Hack the International Court Adjudicating Its South China Sea Territorial Claims?*, DIPLOMAT (Oct. 27, 2015), http://thediplomat.com/2015/10/did-china-just-hack-the-international-court-adjudicating-its-south-china-sea-territorial-claims/; *China Hacks the Peace Palace: All Your EEZ's Are Belong to Us*, THREATCONNECT (July 20, 2015), https://www.threatconnect.com/blog/china-hacks-the-peace-palace-all-your-eezs-are-belong-to-us/; David Tweed, *China's Cyber Spies Take to High Seas as Hack Attacks Spike*, BLOOMBERG TECH. (Oct. 15 2015), https://www.bloomberg.com/news/articles/2015-10-15/chinese-cyber-spies-fish-for-enemies-in-south-china-sea-dispute.

Despite the sensitivity surrounding such proceedings—where, unlike federal litigation in the United States, even the very existence of the arbitration may be highly confidential—cybersecurity has received perhaps less attention than it might deserve. Part I of this Essay explores the nature of the cybersecurity threat to arbitrations; Part II sets forth a few guiding principles that can be used to frame how to think about cybersecurity and the closely related field of data privacy; and Part III suggests practical steps that those involved in arbitrations might take to enhance cybersecurity and prevent violations of international data privacy laws.

I. UNDERSTANDING THE THREAT

Though hackers have proven to come in all shapes and sizes—from the so-called 400-pound man on the bed in his parents' basement[2] to highly sophisticated state-backed campaigns designed to influence political processes[3]—we suggest that they can be classified into three broad categories: hacktivists, state actors, and criminal actors motivated by financial gain. To be clear, these categories are not hard and fast, nor are they impermeable. A state actor could be motivated by financial gain (e.g., stealing intellectual property of manufacturers to establish competing plants in the home country[4]) or by ideological goals (e.g., distributed-denial-of-service ("DDoS") attacks launched against financial institutions in the United States[5]). The purpose of grouping the threats is not to exhaustively categorize the types of attacks, but rather to help build a framework that may be useful in identifying where attackers may be likely to strike.

---

2. Elizabeth Weise, *Tech crowd goes wild for Trump's '400-pound hacker'*, USA TODAY (Sept. 27, 2016), http://www.usatoday.com/story/tech/news/2016/09/27/tech-crowd-goes-wild-trumps-400-pound-hacker/91168144/.

3. Damian Paletta, *U.S. Blames Russia for Recent Hacks*, WALL ST. J. (Oct. 7, 2016), http://www.wsj.com/articles/u-s-blames-russia-for-recent-hacks-1475870371.

4. Erin Ailworth, *Chinese firm charged with stealing tech from Mass. Company*, BOS. GLOBE (June 27, 2013), https://www.bostonglobe.com/business/2013/06/27/feds-charge-chinese-firm-with-stealing-technology-mass-companyamsc/CTE66TzhtD19qvEfU35RQN/story.html.

5. Ellen Nakashima & Matt Zapotosky, *U.S. Charges Iran-Linked Hackers With Targeting Banks, N.Y. Dam*, WASH. POST (Mar. 24, 2016), https://www.washingtonpost.com/world/national-security/justice-department-to-unseal-indictment-against-hackers-linked-to-iranian-goverment/2016/03/24/9b3797d2-f17b-11e5-a61f-e9c95c06edca_story.html?utm_term=.f7f4ce2791b3.

A. Hacktivists

The term "hacktivist"—a portmanteau of "hacker" and "activist"—nicely captures the motivations of this often-unpredictable group. Simply put, they seek to hack not for financial gain, but instead to promote or further a social or political cause. These hackers may seek to use personal information to embarrass their targets, or launch disruptive attacks designed to harm their targets or draw attention to their behavior. One of the most famous examples of a hacktivist is Hector Xavier Monsegur, known as "Sabu," the founder of the international hacker group "Lulzsec," that became famous for a series of well-publicized publicity stunts and DDoS attacks on religious, government, and corporate websites including Visa, Paypal, and Mastercard. As part of a plea deal in 2012, Monsegur cooperated with government investigators and helped build a case against the five other hackers.[6] Parties of arbitration should be aware that these groups exist and should be cognizant of whether they might be transferring any information that could be of interest to these socially motivated hackers.

B. State Actors

Hackers who are arguably the most difficult to mitigate against are state actors. In May of 2014, the Justice Department indicted five members of the Chinese People's Liberation Army under charges of hacking into the networks of Westinghouse Electric, the US Steel Corporation, and other companies, copying their emails, installing malware, and generally stealing intellectual property and other information useful to their competitors in China, including state-owned enterprises ("SOEs"). These five men were identified as members of Unit 61398, the Shanghai-based cyber unit of the People's Liberation Army and home to various identifiable online hackers. These charges represent the first indictment of a state actor in

---

6. Press Release, U.S. Attorney's Office, Six Hackers in the United States and Abroad Charged for Crimes Affecting Over One Million Victims (Mar. 6, 2012), https://archives.fbi.gov/archives/newyork/press-releases/2012/six-hackers-in-the-united-states-and-abroad-charged-for-crimes-affecting-over-one-million-victims); Susan Candiotti, *Five Arrested In High-Profile Cyberattacks*, CNN (Mar. 7, 2012), http://edition.cnn.com/2012/03/06/us/new-york-hacker-arrests/.

a cyberattack.[7] Though not directly related to arbitration, this case involved the commercially motivated theft of intellectual property, information that can often be found in the discovery stages of arbitration proceedings.[8] It is thus important for parties to arbitration to recognize if the information they are sharing in discovery may include matters of interest to state actors conducting economic espionage.

C. Financially Motivated Criminals

The final category of cyber attackers is criminal actors. These hackers are usually interested primarily in commercial gain. To give a recent example, in March of 2016, a Russian hacker located in the Ukraine listed forty-six elite US law firms as targets in a phishing attack aimed at retrieving confidential information of clients to sell for purposes of insider trading.[9] Law firms, which store large amounts of confidential information about clients, are just one example of the types of entities targeted by criminal actors who seek to turn a profit off of stolen data. Given that arbitration often involves the transmission of sensitive commercial information that others might use for profit, parties to arbitration should be particularly cognizant of the threat of these types of hackers.

---

7. Press Release, Department of Justice, U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage (May 19, 2014), https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor; Michael S. Schmidt, *5 in China Army Face U.S. Charges of Cyberattacks*, N.Y. TIMES (May 19, 2014), https://www.nytimes.com/2014/05/20/us/us-to-charge-chinese-workers-with-cyberspying.html?_r=1; Devlin Barrett & Siobham Gorman, *U.S. Charges Five in Chinese Army With Hacking*, WALL ST. J. (May 19, 2014), http://www.wsj.com/articles/SB10001424052702304422704575957160406069653 2.

8. *See, e.g.*, Thomas Fox-Brewster, *U.S Accuses 7 Iranians of Cyberattacks on Banks and Dam*, FORBES (Mar. 24, 2016), http://www.forbes.com/sites/thomasbrewster/2016/03/24/iran-hackers-charged-bank-ddos-attacks-banks/#623b95417f8d. State actors might also engage in hacking as a form of cyber warfare or a terror attack but this activity is less of a risk in arbitration. *Id.*

9. Claire Bushey, *Russian Cyber Criminal Targets Elite Chicago Law Firms*, CRAIN'S CHI. BUS. (Mar. 29, 2016), http://www.chicagobusiness.com/article/20160329/NEWS04/160329840/russian-cyber-criminal-targets-elite-chicago-law-firms; Booz Allen Hamilton, Inc., *Cyberthreats to Law Firms*, CYBER4SIGHT 6-7 (Apr. 14, 2016), http://m.boozallen.com/content/dam/boozallen/documents/2016/05/Cyberthreats%20to%20Law%20Firms_new_header.pdf.

II. TOWARDS A FRAMEWORK: GUIDING PRINCIPLES

The examples above constitute only a tiny portion of the cyberattacks that can occur. The imperative to prevent the harms outlined above may seem self-evident, but the law also suggests that, aside from staving off reputational harm, there are affirmative obligations on both the tribunal and the parties appearing before it to pay heed to cybersecurity and take steps to protect client confidences in the digital world. For example, the Florida Bar Rules of Professional Conduct 4-1.1 states, "Competent representation also involves safeguarding confidential information relating to the representation, including, but not limited to, electronic transmissions and communications," and many other state bar associations use similar language surrounding precautions for cyber security.[10] By establishing procedures for the storage and transfer of sensitive information at the outset of arbitration proceedings, the parties and the tribunal may greatly mitigate the risk of future threats.

Before identifying the specific steps that practitioners may take to discharge what is increasingly viewed as an ethical duty and what is, at a minimum, a need to mitigate reputational risk, it is helpful to consider guiding principles for formulating the specific procedures that may be adopted in any particular matter. We suggest here that cybersecurity—and, relatedly, data privacy concerns—can most effectively be addressed once the practitioner knows her "assets" and "architecture." That is, the sensitive information that one has (e.g., customer lists of a client; sensitive trade secrets developed through substantial R&D expenditures; potentially market-moving information about future business plans) and where one stores it (e.g., with a third-party cloud provider; on portable (and easily lost) external media like thumb drives; on networks accessible by other practitioners in the firm without regard to whether they need access to such data).

Though this process may sound simple, it often poses unforeseen challenges, particularly for the practitioner who practices in a large firm where information decisions (such as where and how to store information digitally) often are made with little or no input from the practicing attorneys, but are instead delegated to information staff

---

10. *In re: Amendments to Rules Regulating the Fla. Bar 4-1.1 & 6-10.3*, 200 So. 3d 1225 (Fla. 2016); *see also* CA Eth. Op. 2010, Cal. St. Bar. Comm. Prof. Resp., 179 (2010); NY Eth. Op. 1019, N.Y. St. Bar. Assn. Comm. Prof. Eth. (2014).

whose primary focus is on keeping the data readily accessible. Indeed, in many ways, there is a tension between the cybersecurity concerns that have been pushed to the fore and the "always available" mentality that permeates law firm and law firm client expectations.

Layered on top of the cybersecurity concerns is the closely related field of data privacy. Even now, many information technology staff (and, perhaps, more than a few lawyers) remain only vaguely aware of data privacy laws—most prominently in the European Union—that forbid the exportation of sensitive data from the European Union to jurisdictions viewed as less secure, including, most notably, the United States. It is therefore possible that an entirely innocent measure taken by an information technologist (e.g., the transfer of data from a full server in London to an available one in the United States) may trigger liability for the practitioner.[11] Thus, it is helpful to identify the critical data assets and the architecture used to store them to effectively build procedures that satisfy both cybersecurity and data privacy concerns.

III. CYBERSECURITY IN PRACTICE

Once the parties and the tribunal have assessed the assets and architecture, the parties and the tribunal may then consider the following three thematic principles with respect to the threat of cyberattackers in the context of arbitration: (i) the establishment of security protocols for the storage and transfer of sensitive information, (ii) limiting of the disclosure of sensitive information, and (iii) in the event of any breach/attack, the process for notifying affected person(s) and for correcting/mitigating the breach/attack.

There are a variety of factors to consider when adopting security protocols for the transfer of sensitive information. First, identifying the categories of particularly sensitive information that merit enhanced cybersecurity procedures is a useful practical step. The reality is that much of cybersecurity fails because the mechanisms used are too cumbersome or subject to human error. Accordingly, trying to implement restrictive cybersecurity measures on *all* data involved in an arbitration proceeding may be counterproductive in

11. Boris Segalis, Christoph Ritzer, & Andrew Hoffman, *Hamburg DPA's Safe Harbor Fines Spell Further Uncertainty and Risk for Global Companies*, NORTON ROSE FULBRIGHT (June 8, 2016), http://www.dataprotectionreport.com/2016/06/hamburg-dpa-fines-three-companies-for-continued-reliance-on-safe-harbor/.

that it over-designates information (desensitizing practitioners to the truly critical information) and results in overly cumbersome processes for information that, in reality, needs little to no additional protections.

Once the key information is identified, procedures can be developed for the transfer of sensitive information between and among the tribunal and the parties. Such measures can include both endorsement of specific processes, as well as prohibitions on riskier procedures. For instance, particularly sensitive information might be disclosed using a secure portal rather than commercial email accounts that may be more easily subject to compromise. The parties who believe that such procedures are necessary might specifically endorse a secure portal platform (such as Accellion) while banning the use of free email accounts (such as Gmail or Yahoo). At a minimum, the parties may develop procedures whereby files containing sensitive information are password protected (and the password is separately transmitted through another channel, such as text messaging) when sent to a commercially available free email account.

Parties may also wish to pay particular attention to the vulnerabilities posed by frequent travel—a key concern for many international arbitration practitioners who often work in jurisdictions far from the home office and under less-than-ideal circumstances. For instance, the use of portable media such as thumb drives or locally stored copies of documents on laptop computers can pose significant risks if those easily portable media are lost, or worse, stolen by a bad actor intent on exploiting the information contained therein. For that reason, parties can consider the adoption of encryption standards for portable media so that, even if the drive or computer is lost or stolen, the data on it is nonetheless likely to remain secure. If the sensitivity of the data warrants it, parties also may choose to outright ban the local storage of such documents on easily lost media. Travel also poses risks for insecure networks accessed through public WiFi spots that may encourage snooping and data capture. Parties may consider a potential prohibition against the use of public WiFi to access sensitive information unless appropriate measures (e.g., use of VPN) are taken.

The second principle for mitigation of the threat of cyberattackers in the context of arbitration is limiting the disclosure of sensitive information. One way to minimize disclosure is to restrict the access of certain information to only those persons having a "need to know." Limiting the number of persons accessing data reduces the

potential for breach. Parties should also consider limiting the submission of sensitive information to only that information which is truly necessary for the arbitration.

In addition, we have recently seen the dramatic consequences of the practice of maintaining decades-old records that have outlived their useful life.[12] An oft-repeated adage for cybersecurity practitioners is that, "they can't hack what you don't have." Like mapping assets and architecture, however, this process may prove more difficult than it appears at first blush. Practitioners find old records useful as models or samples for future work product, so the wholesale destruction of older records may not be feasible from a business perspective. That being said, there are likely categories of documents (e.g., exhibits listing personally identifying information) that provide little or no future business value and can be destroyed with little impact on the business.

Finally, parties to arbitration should be prepared in the event of breach/attack, and thus may consider establishing the process for notifying affected person(s) and for correcting/mitigating any breach/attack. Ensuring that the parties have established policies and procedures related to detecting breaches, determining their scope, and notifying affected parties can help provide a clear path to follow if and when a data breach occurs. These procedures can take many forms but, at a minimum, it is helpful to identify a point-of-contact for each party (and, in tribunals with multiple arbitrators, the tribunal) responsible for coordinating communications in the event of a breach. All constituents of an arbitration should remain cognizant of legal obligations with respect to the reporting of any breach, whether to affected parties, regulatory agencies, or other governmental authorities. In this respect, international arbitration raises unique concerns due to varying legal regimes, which may also differ on a state-to-state basis.

CONCLUSION

As the frequency and sophistication of cyberattacks grow, so will the commensurate risks to arbitration. Though the threat is likely

12. Rishi Iyengar, *What to Know About the 'Panama Papers' Leak*, TIME (Apr. 4, 2016), http://time.com/4280302/panama-papers-leak-vladimir-putin-mossack-fonseca/.

never to be eliminated, it can be mitigated. And accepting the inevitable—that breaches have occurred (and will continue to occur)—in connection with arbitrations can help practitioners honestly explore the appropriate response to such breaches and how they can be mitigated. If all involved in arbitral proceedings approach these concerns with a shared sense of collective responsibility, we suggest that real gains can be seen in preventing and mitigating harm from the cybersecurity threat.