ADR in the age of CYBERSECURITY

By Steven A. Certilman
and Eric W. Wiechmann

Not too long ago, back when paper and pen ruled the world, the only things an arbitrator or mediator had to do in order to ensure the security of confidential case records was lock his office door and not leave his briefcase on the train. Unfortunately, this is not the case anymore.

Information security is a global challenge, and in light of the computer systems of some of our most vital national security agencies and corporations having been hacked, preventing data intrusion must be regarded by practitioners as a Herculean task. Many of us have sought to convince themselves that they are too small to be hacked, or that the risk is infinitesimal since there are so many more tempting targets. However, hiding behind such self-deceptions falls short of a reasonable effort to maintain cybersecurity. Even the solo and small firm practitioners among us must face the reality that reasonable steps are required and that the time to start is now.

STEVEN A. CERTILMAN, FCIARB, *is a Chartered Arbitrator, Accredited Mediator (CEDR) and attorney based in New York, NY and Stamford, CT. He concentrates his practice in the arbitration and mediation of international and domestic commercial disputes and particularly in the IT, IP, e-commerce, outsourcing and licensing areas. He is a frequent author, speaker and trainer in the ADR field, a former adjunct professor of law at Fordham University School of Law and a past chairman of the Board of Trustees of the Chartered Institute of Arbitrators. Mr. Certilman serves on the arbitration and mediation panels of dispute resolution organizations throughout the world including the ICDR, AAA, CPR, CAfA, HKIAC and AIAC.*

ERIC WIECHMANN *is an independent ADR neutral who has served as an arbitrator and mediator over the past 30 years. Eric was a partner at McCarter & English LLP where he served as the firm's managing partner. He serves on several AAA national arbitration and mediation panels, is a CPR Distinguished Neutral, a Fellow of the College of Commercial Arbitrators, a Fellow of the Chartered Institute of Arbitrators and a Member of the National Academy of Distinguished Neutrals.*

Why do we care?

Before a review of some of the many measures which may be adopted by alternative dispute resolution professionals as part of a cybersecurity strategy, a quick look at the professional reasons behind the need to care is warranted.

The community of ADR providers is a diverse lot, from partners in the largest firms to solo practitioners and non-lawyers. In a sense, we are a cross-section of the computing world. While those practicing in large firms may have delegates to address cybersecurity issues, doing so is far more challenging for solo and small firm practitioners. Nevertheless, those who find themselves in these smaller firm environments must resist the temptation to bury their heads. A paramount concern is the ethical obligation owed to clients. We are bound by the ethical duty to safeguard the confidences of the parties to our proceedings. This duty is independent of, and in addition to, the similar duty of those of us who are attorneys.

Looking back at arbitration practice a decade ago, it can be said that life used to be much simpler for arbitrators as we contemplated our confidentiality obligations under the Rules and ethical guidelines of the arbitral organizations and courts. Fifteen years ago, when these authors reviewed Rules R-23 and R-25 of the Commercial Arbitration Rules of the American Arbitration Association (AAA)[1] or Article VI(B) of the ABA/AAA Code of Ethics for Arbitrators in Commercial Disputes,[2] we focused on a few clear and obvious duties: to refrain from discussing the identities of the parties or the subject matter of the dispute and to keep confidential, and not lose, the pleadings, submissions or evidence of the parties. At that time, a little common sense and discretion seemed all that was required. The materials to be kept confidential were typically maintained and exchanged in a hard copy paper format. Even "native" electronically-stored information was typically produced for disclosure in paper format, and later through a CD-ROM or thumb drive. There was little if any focus on whether the document production might contain sensitive personal data.

However, times have changed. With the ubiquity of email usage and the explosion of electronically stored data, as well as electronic transmission of data and cloud-based data storage, the need for a new level of information security has become apparent. Examples of how easily this information can be unlawfully accessed by criminals, competitors, NGOs such as Wiki-Leaks, and governments have come with alarming regularity, causing a reassessment of business processes that are affecting the working environment of businesses, attorneys, government and others. Businesses, which now budget significant amounts to the protection of their sensitive information, have come to expect a similar focus of vigilance by

their attorneys. We, as arbitrators, must see ourselves as sharing the same responsibility for diligently protecting information entrusted to us for the resolution of disputes. To be sure, arbitrators today must take their confidentiality responsibilities to a whole new level. Administering bodies such as AAA, JAMS, CPR and the LCIA, to name just a few, have begun to impose specific cybersecurity duties on arbitrators,[3] and those arbitrators who are also attorneys must be equally focused on their obligations under the Rules of Professional Conduct of their states of admission and the ABA and state codes of ethics.[4] Prominent membership organizations in the field have done so as well.[5] Moreover, depending on the nature of their practices, arbitrators may also need to become familiar with, and comply with, state, federal and even international data protection laws such as HIPPA,[6] or the European Union General Data Protection Regulation (GPDR).[7] Many corporate and governmental parties impose their own data protection requirements as well.

The breach of confidential data or documents used in an arbitration or the unintentional release of such information can, in the absence of adequate precautions having been taken by the arbitrator, lead to serious professional consequences. With clients increasingly cautious about the dissemination of confidential data in their possession, a data breach caused by an arbitrator's failure to take reasonable precautions can form the basis of a grievance being filed against a lawyer-arbitrator, with sanctions being imposed by the arbitral organization administering the proceeding, loss of membership on an arbitration panel or in a professional membership organization. Even with the general immunity that arbitrators and mediators enjoy under the laws or court rules of many states[8] and the rules of many arbitral organizations,[9] a cybersecurity incident can lead to a lawsuit and can possibly threaten the career of a practitioner.

Our observations and suggestions designed to assist ADR professionals in avoiding, or at least minimizing, inadvertent or unauthorized disclosure of confidential party information are found below and are provided for consideration by the reader. While few readers will adopt every suggestion, it is recommended that they be considered globally when deciding whether you are taking reasonable steps to protect the sensitive material. In the interest of facilitating review and implementation, it is provided in outline format.

I. Storage of Data—Comparing the options

a. Internal hard drive or a connected external hard drive
   - *i. The least secure format*
   - *ii. Click on a link in the wrong email and you open a door for malware or unauthorized access*
   - *iii. If your computer has been infiltrated, this data likely will be as well*
   - *iv. Risk of ransomware, where you lose access to your data unless a ransom is paid*
   - *v. External drives have become very small and easy to use, but they can easily be lost if used portably*
   - *vi. Is the drive encrypted? Much better, but slows the computer down*
   - *vii. Generally, external drives need cables, which are easily forgotten*
   - *viii. These drives are subject to crashing (mechanical malfunction)*

b. Cloud-based (*e.g.* Google Docs, iCloud or Dropbox)
   - *i. The challenge is in finding the right balance between convenience and security*
   - *ii. How does the data get there? Services may be either encrypted or unencrypted. If encrypted, who holds the key?*
   - *iii. Look for services that have end-to-end encryption. This means data is encrypted getting to their servers and encrypted while residing on their servers*
   - *iv. Many services tell you in their Terms of Service that they have the right to "mine" your data and use for marketing or to sell to other marketers. Pay attention to these terms. Generally, e.g., iCloud, Google Docs do this, unless you pay for corporate service*
   - *v. With the very popular Dropbox, they hold the encryption key rather than you, so documents can be made available by them without your involvement, e.g., under court order. While you could encrypt your own documents individually, this is rarely done*
   - *vi. There are other services such as Tresorit (tresorit.com), a modestly-priced service which is similar to Dropbox except that it has end-to-end encryption and YOU, not they, hold the encryption key. This service is becoming increasingly popular for that reason. This is presently $20 per month for 1 TB*

of storage. They also offer a secure way to send attachments similarly to Dropbox

c. USB Drive
   i. Probably the worst choice for use. The military commonly disables USB drives in its computers. Risk outweighs convenience
   ii. Easy to lose. May carry viruses already built into the drive and invisible, especially freebies distributed at conferences, etc. for marketing purposes
   iii. Easy to misplace, or be used for a later purpose
   iv. If you must use one for data storage, make sure it is encrypted
d. Re-writable CD-ROM
   i. Dated and outmoded, almost not worth mentioning or using
   ii. Most portable computing devices do not even have CD drives any longer
   iii. At a minimum, password protect
e. Servers
   i. There are many kinds of illicit devices that are easily plugged into a server port and then will convey information to or enable access by a remote source.
   ii. Treat your server spaces as secure locations
   iii. Keep cables and hardware neatly organized to more readily expose hardware spyware.

II. Communications

a. Consider discussing confidentiality and security issues during your preliminary conference. It is an opportunity to bring a great deal of certainty to the security concern. There are various permutations of responsibility. See below
b. For you, with their information:
   i. Consider building into your first preliminary order a confidentiality and security agreement
   ii. Check the arbitration clause to determine whether the parties have already agreed to provisions which will bind you
   iii. See AAA Rule R-23(a): The arbitrator may issue order "conditioning any exchange or production of confidential documents and information, and the admission of confidential evidence at the hearing, on appropriate orders to preserve such confidentiality"
   iv. See ICDR Art. 37(2)
      1. Confidential information disclosed during the arbitration by the parties or by witnesses shall not be divulged by an arbitrator or by the Administrator. Except as provided in Article 30, unless otherwise agreed by the parties or required by applicable law, the members of the arbitral tribunal and the Administrator shall keep confidential all matters relating to the arbitration or the award.
      2. Unless the parties agree otherwise, the tribunal may make orders concerning the confidentiality of the arbitration or any matters in connection with the arbitration and may take measures for protecting trade secrets and confidential information
   v. If appropriate, consider including a clause such as the following, written by arbitrator Sherman Kahn:
   The parties are instructed to jointly consider methodologies to protect confidential and private data that may be exchanged in the arbitration and/or submitted to the Tribunal. Such methodologies should take into account the parties' need for information in the arbitration and whether such information must be provided to the Tribunal or exchanged among the parties in light of the sensitivity of the information and its relevance to the proceedings. The parties shall redact from information provided to the Tribunal any sensitive personal identifiers such as social security numbers (or other national identification numbers), dates of birth or financial account numbers, but may submit partially masked versions of such data if such masking is generally accepted for public use of such data (e.g., last four digits of credit card or social security numbers). The parties shall not submit to the Tribunal un-redacted documents containing personal identifying numbers, individual health information or financial information unless there is a demonstrated need for the Tribunal to have such information due to the matters at issue in the arbitration.
   vi. Agree when to use (or not use) unencrypted email. Encrypted email is readily available but use is cumbersome
   vii. An alternative is to password protect individual documents as necessary
   viii. Once you develop a preferred communication protocol, explain what it is and ask if any objections
   ix. If applicable, you may need to use a HIPAA-compliant process; have a plan
   x. Address when you will destroy the file and delete electronic records
c. The parties, with each other's information
   i. Consider addressing the partial or complete redaction of unnecessary personal confidential information such as Social Security numbers, dates of birth, financial account numbers, medical information, etc.
   ii. If exchanging documents on a CD, consider a format in

which the entire CD can be password protected and send the password separately

iii. To facilitate confirming all this in the order, you may wish to have "standing orders" for confidentiality (should include how witnesses, experts, consultants will be bound by confidentiality and cybersecurity measures and how that will be enforced)

d. As you referee issues related to discovery, and the hearing process, continue to have in mind the requirements of the governing rules such as AAA Rule R-23(a) and ICDR Art. 37(2)

e. General communication issues

i. Avoid the use of public Wi-Fi. If you must use it, as most of us do, use a VPN. Unsecured public Wi-Fi can be easily hacked, and the hacker, who technologically positions himself between you and the web, can capture your every keystroke and distribute malware to your computing device, without you knowing it. If you plan to use a public Wi-Fi network (e.g., hotel, airport, mass transit, Starbucks), purchase a Virtual Private Network service. With a VPN, your transmissions are encrypted and most hackers, who are looking for easily accessible information, will discard it.

ii. When browsing on the web, look at the address bar. If the internet address does not begin with "https://", it is not an SSL (Secure) connection. Use extreme caution before entering authentication information such as passwords into unsecured sites. The login page of most websites will be an SSL page. Always use the https:// option if given a choice.

iii. Keep Wi-Fi and Bluetooth off when not using them. Not only does this close the door to hackers, it will greatly extend your battery life.

iv. Protect your passwords. Take care not to fall victim to social engineering. No one should ever be asking you for your password by email or over the phone. Inform your staff about the problem

III. Use of Email

a. Reply-All Error

i. Take the time to ensure that you do not reply all. We are all busy, but you do not want to send confidential information to the wrong party.

ii. The ABA's stance on the ethics applicable to a party's accidental receipt of privileged information has evolved over time. Today's ABA rules ask attorneys simply to inform the sender that they've received the information

b. Any time you receive an unexpected email from a website urging you to click a link or open a document, put the process into slow motion and consider whether the request makes sense. An email that purports to be from a site you use, and says so in the sender box, may be a forgery. There are two easy things you can do to ensure the email is legitimate. If you are using Microsoft Outlook, roll your cursor over the link but do not click it. The email address or destination website of the link will appear on the lower left-hand corner of the Outlook window. If it is not the site you are expecting, hard delete (press shift + delete) the email. Also, you can double click on the sender's name to see the address from which it actually came. If it isn't the address you are expecting, hard delete as well.

IV. Concerns That Arise At Issuance of the Award

a. Confidentiality issues that come into play in the award-writing process

i. What if the award contains confidential information that a party would not wish to have filed in court in a confirmation or vacate proceeding? Some courts refuse to seal even those awards as part of the enforcement process. Can the arbitrator modify it?

ii. Not likely. See AAA Rule R-50 and ICDR Art. 33. Outside of permissible scope

iii. But see Section 11 of the Federal Arbitration Act (9 U.S.C. 11), under which the District Court is authorized as follows: "Where the award is imperfect in matter of form not affecting the merits of the controversy. The order may modify and correct the award, so as to effect the intent thereof and promote justice between the parties." Can an argument be made to modify to protect privacy under this language?

iv. Collaterally, do we have a duty to draft the award to avoid exposing party confidential information? Probably, at least where we know we are doing so

v. Underscores need to consider this issue when drafting the award

iv. Workarounds? (Show draft award to parties for review for confidential information)

V. Post-proceeding Concerns

a. There is a continuing duty to parties

b. Disposal of files

i. Is the paper file treated any differently from the electronic records?

ii. In its form award transmittal letter, the AAA says: "Pursuant to the AAA's current policy, in the normal course of our administration, the AAA may maintain certain electronic case documents in our electronic

records system. Such electronic documents may not constitute a complete case file. Other than certain types of electronic case documents that the AAA maintains indefinitely, electronic case documents will be destroyed 18 months after the date of this letter."

c. There is no hard and fast rule for how long to retain documents
   i. *Certainly for the modification period (See the FAA, 9 USC 9-11, state law (e.g. CPLR 7509) and the applicable rules)*
   ii. *Probably even long enough for the possibility of a vacatur proceeding to play out. In New York, that's 90 days for the vacatur period plus the duration of a pending proceeding. (See CPLR 7511)*

c. Securely delete your data files
   i. *A deleted file isn't really deleted. Initially it can be restored from the Recycle Bin, but even after deletion from the Recycle Bin deleted files can be undeleted (restored) using readily available software.*
   ii. *Electronic files should be deleted using file shredder software, some of which is available free. These programs all overwrite the deleted files several times with selected patterns to ensure that they are not recoverable. A good example is Eraser, which can be found at https://eraser.heidi.ie/.*

e. Decommissioning of equipment
   i. *When it's time to upgrade your computers, your best choice is to remove and destroy the hard drives. If you plan to make them available for use by others, the hard drives should be wiped clean using file shredder software, and then the operating system can be re-installed onto a clean hard drive.*
   ii. *It comes as a surprise to many that printers often have data storage capacity (like hard drives) for use in the printing process. To ensure that the memory is not accessible after your printers are taken offline, be sure to do a factory reset (found in the printer's menu settings) before disposing of the units.*

VI. Summary of Best Practices and Additional Tips

a. Take reasonable measures to avoid malware, including ransomware
   i. *Maintain anti-virus/anti-malware software and regularly monitor it to ensure that the definitions are up to date and that it has not been disabled*
   ii. *Maintain constant backup using a service such as Carbonite. Backing up data hourly would seem to be an appropriate level of protection*
   iii. *Avoid phishing attacks. A USDOJ report says that on average more than 4,000 ransomware attacks have occurred daily since Jan. 1, 2016.*
      1. Spear phishing attacks are emails that try to get you to click on a malicious link
      2. Whale phishing emails are similar, but they appear to come from a CEO or other VIP and ask you to deliver valuable information
      3. Use the mouse rollover technique to check the link and click on the sender's email address to verify that it really comes from the purported sender. Generally, this must be done on a desktop browser
      4. Secure your servers
      5. Delete data using file shredder software
      6. Be aware and keep your guard up.

b. Don't get *juice jacked*! This is a scam involving public chargers such as USB ports in hotels and free charging stations (such as in airports and malls) in which the cable is supplied. The problem is that malware can be hard-wired into the cable or the port and once you connect, the malware can be loaded onto your device. This in turn can open a gateway for malicious attacks such as spyware, stolen data and ransomware. Even cables given away as promotional gifts should be considered suspect. Best practice: carry your own wires and charge directly through a power outlet. If you rely heavily on public charging stations, use a charging cable that has had the data pin disabled.

c. Any public Wi-Fi is inherently insecure. Public Wi-Fi is any Wi-Fi you do not control. That includes hotel, airport and other public Wi-Fi networks. Avoid them unless you are sure it is legitimate and you are using a VPN with end-to-end encryption

d. Never connect your device to an insecure USB port to charge it. You don't know what is connected on the other end. Always use AC power(a standard power outlet) and the charger.

e. Cellular data is more secure, but you should still use a VPN as they too can be attacked.

f. Always use an end-to-end encrypted VPN any time you are out of the office.

g. With your own office Wi-Fi, use an inconspicuous network name, set it up for WPA2 encryption, change your network key regularly and make sure to change the router's password from the factory default.

h. Be careful of international travel with your iPad or laptop that has confidential arbitration information stored. In certain countries as soon as you activate your device on their cellular system your device may be penetrated by malware. Many people travel to these countries with a clean

device with nothing on it which is of any concern, and then wipe the device clean after leaving the country

i. Insurance—make sure your professional liability insurance policy includes cyber-liability and data breach response coverage. It is available as an add-on if not part of your basic policy. Even if you do not maintain an arbitrator malpractice insurance coverage, consider a separate policy for Cybercrime and Privacy claims. For instance, HUB International (https://www.hubinternational.com/) provides such coverage for a fairly nominal charge.
j. Upgrade your passwords
k. Consider using a password manager. It can store all your passwords
l. Update your software—older versions may lack security improvements and make it easier to infiltrate your system
m. Don't let your browser memorize your passwords (such as your password to the e-Center)
n. Use services which require (or opt to use) two-factor authentication wherever possible. You get an email or a text message which you have to enter to login
o. Encrypt your portable devices such as smart phones and tablets. The operating systems usually include the ability standard
p. Check the site www.haveibeenpwned.com to see if your account information is showing up on nefarious websites, which will mean at one point or another, your computer or an online account has been hacked. It's an identity theft early warning site. You input your email addresses and user names and the site will tell you if they come up in the sites database of known hacks.
q. Carefully handle and dispose of written documents (usually you do not need both an electronic and hard copy of the material)
r. Devices like the Amazon Alexa are always listening.
s. Don't pick up stray cables you may find as malware can be placed on microchips and inserted into the cable ends

---

For most of us in ADR—particularly full-time neutrals who typically are solo practitioners, focusing on our greatest vulnerabilities is likely the best first step. While this is a process, this article seeks to enable you as a practitioner to get started and stay safe in the age of cybersecurity. ⚖

This article is updated from one originally published in New York Dispute Resolution Lawyer, *Volume 12 No. 1 (Spring 2019) at page 14.*

Endnotes

1. American Arbitration Association Commercial Arbitration Rules and Mediation Procedures (2007)
2. The Code of Ethics for Arbitrators in Commercial Disputes, American Bar Association and American Arbitration Association (2004)
3. *See, e.g.,* JAMS Comprehensive Arbitration Rules & Procedures Rule 26; ICDR International Dispute Resolution Procedures Article 37; CPR Administered Arbitration Rules Rule 20; See also CPR 2018 Non-Administered Arbitration Rules Rule 9,3. "Matters to be considered in the initial prehearing conference, may include,…F. The possibility of implementing steps to address issues of cybersecurity and to protect the security of information in the arbitration."
4. ABA Model Rules of Professional Conduct, Rule 1.1 (Competence) and 1.6 (Confidentiality of Information); ABA Formal Opinions 477R and 483: Securing communication of protected client information (2017); New York State Bar Association Ethics Opinion 842 (2010) "Using an outside online storage provider to store client confidential information."
5. Examples include the Chartered Institute of Arbitrators and the College of Commercial Arbitrators.
6. Health Insurance Portability and Accountability Act, Pub.L. 104-191, 110 Stat. 1936.
7 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
8. *See, e.g., Austern v. Chicago Board Options Exchange, Inc.*, 898 F.2d 882, 885–86 (2d Cir. 1990) and *Calzarano v. Liebowitz*, 550 F.Supp. 1389, 1391 (S.D.N.Y. 1982); *Stasz v. Schwab* (2004) 121 Cal.App.4th 420.
9. *See, e.g.,* AAA Commercial Arbitration Rules R-52(d); ICDR International Dispute Resolution Procedures Article 38; JAMS Comprehensive Arbitration Rules & Procedures Rule 30(c); CPR Administered Arbitration Rules Rule 22.