CJM Working Draft: 03/22/19

Some Potential Checklist Items for Maintaining Cyber Security in Our Arbitration Cases

Charles J. Moxley, Jr.

Following is a checklist of some items to consider in our efforts to achieve and maintain cyber security for information we receive and transmit as arbitrators and mediators.

This checklist has been compiled based upon attending many panels on cyber security over the last several years and reflects a first effort at developing a Best Practices checklist for such matters.[1]

- **Target of opportunity/weakest link:** There's a wide consensus that, while protecting our information from a focused intruder determined to breach our security is quite difficult if not impossible, that. nonetheless, most cyber security failures result from people not following basic cyber hygiene. Specifically, most cyber intrusions are the result of the bad guys searching for targets of opportunity, as opposed to focusing particularly specifically intended targets.
- **Ethical as well as existential concerns:** There are numerous ethical obligations to which we are subject as attorneys with respect to maintaining cyber security, in addition the fact that a significant cyber security breach could pose a major problem to confidentiality in our cases, imposing substantial risks in numerous obvious regards.
- **No public WiFi:** Everyone agrees one should never use public WiFi. Essentially no exceptions.
- **The alternative to public WiFi:** Everyone should be using a 4G device or the like, which can be obtained from a cell phone provider, a little black box, that is apparently much harder to penetrate than public WiFi.
- **Virtual private networks (VPNs):** A VPN is a technical device that, as I understand it, disguises our actual location, encrypts our communications, and makes it harder for computer hackers to know who or where we are, hence ostensibly making it much harder for them to infiltrate our systems.
- **Good password hygiene:** This is a biggie. We should have long and complex passwords – and different passwords for each device.
- **Password protection systems:** Some such systems are available. We need to identify the most reliable ones. This is an area of concern where further exploration is necessary.

[1] I'd like to acknowledge ,Stephanie Cohen, Joseph DeMarco, Sherman Kahn, Mark Morrill, and many others who have advanced our understanding in this area. In preparing this checklist, I've drawn heavily on what I've learned from their presentations and the presentations and writings of many others. However, any areas that need further refinement in this regard are solely mine.

- **Anti-malware and other intrusion software:** We need to have good virus and malware protection for all our devices and have it always on. Malwarebytes (https://www.malwarebytes.com/lp/sem/en//?gclid=EAIaIQobChMI0LrhjfCV4QIVTD0MCh1GgwSREAAYASAAEgLl4fD_BwE), is reportedly one good such provider. We need to do additional work to identify reliable providers.
- **Protecting *all* our systems:** Again, we have to not be the weakest link. We have to be careful that *all* our systems, office, home, phones, iPads, whatever, are protected. The weakest link will be the way in.
- **Possible separation of our professional communications from our personal and recreational communications:** It seems prudent to separate our professional communications from our personal and recreational communications. There are various ways of doing this, including through having separate computers or, apparently, separate user accounts on individual computers, with separate strong passwords for each user on any particular computer. It may also be important to not access cites like Netflix, YouTube, and the like on the devices or user access accounts upon which we conduct our professional communications.
- **Importance of upgrades:** It is reportedly extremely important to install all upgrades on our systems on a timely basis. Under the "target of opportunity reality," there is an arm's race between the bad guys and the systems, making it essential that we take advantage of upgrades, which will often be designed to address emerging cyber threats.
- **Use enterprise not free levels of software:** This point is repeatedly raised. Apparently, the "free" versions of familiar systems are unreliable and often easily circumvented. It appears to be strongly advisable to use the more sophisticated, so-called "enterprise" versions of helpful software systems. We need to do more work to identify the most reliable systems in this regard.
- **Two point authentication:** This is current state of the art. We need to be establishing this approach in our professional systems, at least insofar as concerns remote access.
- **Laptop privacy screen:** We all sit on trains and planes and in conferences, etc. Laptop privacy screens apparently available on line and in business supply stores and the like can apparently protect our laptops and the like from being so readily readable to others around us.
- **Risk assessment:** We need to do a risk assessment as to the state of our cyber security and take proactive action as to areas of vulnerability that we identify.
- **Action plan if there's a breach:** There are all kinds of laws and professional obligations out there. We need to have a pre-thought-out action plan which we will have available to follow if any of our professional systems are breached.
- **Apple tracking and destruction of devices we lose:** There's a technical capability now to set up all Apple devices (and, presumably, other devices) with security such that, if they are lost or the like, we have the ability to destroy whatever is in them to avoid their contents' becoming available to inappropriate persons.
- **Burner laptops:** It soon will be, if it is not already, the standard of care that, if we're traveling internationally, we need to have a "burner," which, as I understand it, means a computer that has a very limited amount of confidential

information on it, and that, perhaps, is subject to our destroying the data contained in it if we lose control of the device. The same would appear to be the case as to our cell phones.

- **Thumb drives:** Many commentators seem to believe thumb drives are very risky, such that we should "never" use them.
- **Having our backup systems "unplugged:"** The point has been made that, if we have a backup system which is attached to our actual computer, such as a desktop, that, if intruder sgets into the computer, they will also be able to get into the backup materials, which could be a problem with ransomware and the like. Accordingly, measures need to be taken, including, apparently, having our external backup device not physically connected to the computer, except on a periodical basis under safe circumstances. This area needs to be studied further.
- **A secure system for sending sensitive emails:** Various software systems we regularly use enable us to specifically encrypt emails and documents transmitted by email. Obviously, this is a good idea.
- **Sending passwords as to encrypted emails through a separate email system:** It seems evident that, if we're going to the trouble of encrypting our emails and attachments thereto, we should also consider sending the password through a separate email systems or the like so as to have a redundant level of protection.
- **Owning one's server versus using an outside provider:** The view is often expressed that enterprise versions of the major providers, such as Microsoft, Amazon, Google, and the like, are potentially more secure, given hopefully the sophistication of such entities, than private servers in our homes or offices, unless we have them professionally supported.
- **Monitoring the access logs on our computers:** Specialists know how to monitor the access logs on computers so as to ascertain, in various ways, whether an intruder seems to have access to our computers.
- **Protecting us against receiving information we don't want to receive:** The point is increasingly emerging that we need to be very protective as to the information we let ourselves receive. Specifically, the point has been made that, in our cases, we should, in many circumstances, require counsel or parties to "scrub" documents and other information they provide us so as to preclude our receiving highly sensitive personal information when that is unnecessary.
- **Available redaction tools:** With respect to the above-discussed topic of unnecessarily receiving highly confidential information, there are apparently some redaction tools that are now commercially available – something that needs to be looked into further.
- **GDPR privacy regulations of the EU:** There's a widespread concern about the new EU regulations in this regard – regulations that can potentially have severe consequences for violations. This is a scenario as to which we have to educate ourselves and, perhaps, question counsel in cases involving EU parties or the like where the GDPR privacy regulations may be applicable so as to make sure we follow practices that avoid violations.
- **Potential use of provider websites for case information:** The AAA and potentially other providers will likely, in the near future, be increasingly open to

more extensive use by case participants of provider websites for maintain case information of a confidential nature.

- **Deleting old electronic records as well as arranging for the shredding of old hard copies:** This is another area of self-protection. We need to be much more self-protective as to what information we maintain over the long haul and hence expose to unauthorized access. We need to work on protocols on this as to when we get rid of hard copies and as to when, and the extent to which, we get rid of electronic copies – and how to do this effectively and securely.
- **Upgraded security as to hard copies of documents:** We shouldn't lose track of the fact that we also have security obligations as to hard copies. There is an increasing awareness of the risk that bad guys will try to penetrate our secure information by accessing our offices or work spaces, perhaps as cleaning people or delivery persons or the like. There appears to be a growing concernt that we need to consider having "clean desks," locked offices, and the like as reasonable steps to maintain security.