DRAFT CYBERSECURITY PROTOCOL
FOR INTERNATIONAL ARBITRATION

CONSULTATION DRAFT

ICCA
INTERNATIONAL COUNCIL FOR COMMERCIAL ARBITRATION

NEW YORK
CITY BAR

CPR
International Institute for
Conflict Prevention & Resolution

Announcement of Cybersecurity Protocol Consultation

International arbitration in the digital landscape warrants consideration of what constitutes reasonable cybersecurity measures to protect the information exchanged during the process.

Recognizing this need, the International Council for Commercial Arbitration (ICCA), the International Institute for Conflict Prevention and Resolution (CPR) and the New York City Bar Association have established a Working Group on Cybersecurity in Arbitration (the "Working Group"). The Working Group has promulgated a Draft Cybersecurity Protocol for International Arbitration (the "Protocol") and is now pleased to proffer this draft Protocol for public consultation. The draft Protocol is attached hereto.

The consultative period will last until 31 December 2018. All interested parties are encouraged to provide detailed thoughts and comments on the draft protocol, or to provide general feedback. The Working Group will hold a number of public workshops in different parts of the world to solicit and discuss the views of interested parties. In addition, the Working Group welcomes written comments from interested parties which should be submitted no later than 30 September 2018, through the Working Group's page on ICCA's website at <http://www.arbitration-icca.org/projects/Cybersecurity-in-International-Arbitration>.

In anticipation of the public consultation, which the Working Group anticipates will include input from a variety of sources with differing views, the draft Protocol refrains in Schedule A from offering specific cybersecurity measures for possible inclusion in arbitration agreements or procedural orders. Instead the Protocol suggests a procedural framework for developing specific cybersecurity measures within the context of individual cases, recognizing that what constitutes reasonable cybersecurity measures will vary from case-to-case based on a multitude of factors. Depending on the feedback received, the final Protocol may or may not include such proposed measures in Schedule A.

Following the consultation period, the Protocol will be revised, refined, and finalized in accordance with the input and comments received. After that time, the Working Group anticipates that there will be an ongoing review and revision process, as cybersecurity issues will evolve with changing technology, new cyberthreats, changing laws and regulatory schemes, and emerging consensus as to best practices.

The Working Group is chaired by Brandon Malone (Chairman of the Scottish Arbitration Centre and the principal of Brandon Malone & Company). Its members include Olivier André (CPR), Paul Cohen (4-5 Gray's Inn Square Chambers), Stephanie Cohen (independent arbitrator), Hagit Elul (Hughes Hubbard & Reed), Lea Haber Kuck (Skadden, Arps, Slate, Meagher & Flom LLP), Micaela McMurrough (Covington & Burling), Mark Morril (independent arbitrator), Kathleen Paisley (Ambos Law) and Eva Y. Chan (Skadden, Arps, Slate, Meagher & Flom LLP) as Secretary to the Working Group.

Draft Cybersecurity Protocol for International Arbitration[*]

I. Introduction: Importance of Cybersecurity in Arbitration

A. Most exchanges of information[1] today are digital, including in international arbitration and other forms of dispute resolution.

B. Parties expect that the providers of dispute resolution services and other participants in the dispute resolution process will take reasonable measures to protect non-public exchanges of information, including reasonable cybersecurity measures, to safeguard digital information from unauthorized access and disclosure.

C. Cybersecurity may be legally mandated when the information at issue is personal or industry-regulated data, or if the information is relevant to national security or other matters of public interest.

D. In an increasingly digital landscape, the credibility of any dispute resolution system, including arbitration, depends on maintaining a reasonable degree of protection of the digital information exchanged during the process, except where the parties intend for the information to become public. Arbitration proceedings are not immune to increasingly pervasive cyberattacks against businesses, law firms, governmental actors, educational institutions and other custodians of large electronic information repositories. This means that attention to cybersecurity is required in international arbitration as it is in other sectors.

E. Arbitration has the benefit over other dispute resolution processes of enabling parties to maintain the confidentiality of the dispute resolution process itself where they want to, and the information exchanged within it. Reasonable cybersecurity measures are essential to ensure that international arbitration maintains this advantage.

F. Even where an arbitration has not been made confidential by agreement of the parties or by application of arbitration rules or law, maintaining the legitimacy of the process may require that certain aspects of the arbitral process remain confidential. For example, interactions between an administering institution and the parties, tribunal deliberations, and draft awards are generally intended to remain private and secure.

G. Although a reasonable degree of cybersecurity is critical for international arbitration in the digital world, what is reasonable in any given circumstance depends on various factors discussed herein.

[*] Proposed by the Working Group on Cybersecurity in Arbitration established by the International Council for Commercial Arbitration (ICCA), the International Institute for Conflict Prevention and Resolution (CPR) and the New York City Bar Association. Pending a period of public consultation, the Protocol is being issued as a draft for debate and comment. The Working Group anticipates that a final version of the Protocol will be released in 2019.

[1] This Protocol uses the broad term “information” to include all types of electronic and non-electronic information of any type and in any form, including both commercial and personal information. When referring to personal information specifically, we use the term “personal data” employed in many data protection laws and regulations. This is also a very broad term and typically includes all information of any nature whatsoever that individually or collectively could be used to identify an individual (including for example, work-related emails, lab notebooks, agreements, handwritten notes, etc.).

H. Cybersecurity is a shared responsibility of all Participants[2] in the international arbitration process. Security of information ultimately depends on the responsible conduct and vigilance of individuals. Many breaches arise from individual conduct; any individual actor can be the "weak link", no matter how robust the security of its infrastructure.

I. The Participants in international arbitrations are, to a large degree, digitally interdependent, because the process typically involves the transmission and hosting of information and collaborative elements such as communications relating to the arbitration. Consequently, any break in the custody of arbitral information has the potential to affect all Participants. Indeed, since Participants will frequently host not only their own arbitral information, but also the information of others, intrusion into the information held by one Participant may injure another more than the one whose information security was compromised.

J. All Participants should take into consideration their own, regular cybersecurity practices and digital infrastructure as a threshold matter, because Participants' day-to-day security practices and infrastructure pre-exist individual arbitrations, and therefore have an immediate and continuing impact on the security of arbitration-related information. Schedule C hereto highlights general cybersecurity practices that all Participants in an international arbitration should take into consideration.

II. Cybersecurity Risks in International Arbitration

A. Cybersecurity refers to the means employed to protect digitally stored information from intrusion by threat actors not authorized to have access to that information.

B. As a matter of good practice, reasonable cybersecurity measures should be employed whenever large amounts of digital information are processed. This includes international arbitration.

C. While not unique, the need for reasonable cybersecurity measures in international arbitrations is highlighted by:

1. the litigious backdrop, which can lead to targeting of information;

2. the high-value, high-stakes nature of disputes, which increases the risk of breaches and the likelihood that those breaches will cause significant loss;

3. the exchange of information that is often sensitive or high-value confidential commercial information and/or regulated personal or other data; and

4. the cross-border nature of the process, which creates heightened challenges in complying with applicable legal requirements and makes the consequences of a breach more substantial.

[2] The term "Arbitral Participants" or "Participant" refers to anyone who receives information that s/he would not otherwise have as a result of the arbitral process. Hence, it includes the parties, counsel, arbitrators, arbitral institutions, experts, and Vendors. Capitalized terms not otherwise defined herein are defined in the Glossary attached as Schedule D, which also includes a general glossary of terms relevant to cybersecurity that are not used in this Protocol.

D. The specific consequences that may result include:

1. economic loss to parties, arbitrators, institutions, witnesses or other persons/entities whose commercial information or personal data is compromised;

2. reputational damage to arbitral institutions, arbitrators and counsel, as well as to the system of arbitration overall; and

3. potential liability under applicable laws and other regulatory frameworks.

E. With respect to the legal and regulatory framework, the vast amounts of digital information available today have led to increasing regulation of the security and use of information, particularly personal data. These data protection regimes require, among other things, reasonable cybersecurity measures whenever personal data is exchanged. This legal infrastructure has the potential to apply to, and shape how, information is managed in international arbitrations.

F. Applicable law may vary from jurisdiction to jurisdiction, and non-compliance with applicable law may result in substantial penalties and/or litigation risk. Furthermore, data protection enforcement and other legislative risk may be inconsistent in different jurisdictions and create obstacles to trans-border information exchanges and indirectly international arbitration.

G. However, the determination of what law(s) apply(ies) in a particular arbitration may be a complex issue and it may be difficult to reconcile requirements of different jurisdictions.

H. Given the substantial risk of non-compliance, we can expect that parties will increasingly drive data protection compliance in all fields, including international dispute resolution, with the starting point being that reasonable cybersecurity may be required as a matter of law, whenever personal or other regulated data is exchanged, and good practice, whenever important information is exchanged during an arbitration. The baseline reasonableness standard will ensure consideration of the facts and circumstances of individual cases, including the parties' preferences and resources.

III. Purpose of the Cybersecurity Protocol

A. The Draft Cybersecurity Protocol for International Arbitration set forth in Section IV (the "Cybersecurity Protocol" or the "Protocol") is intended to encourage Participants in international arbitration to become more aware of cybersecurity risks in arbitration and to provide guidance that will facilitate collaboration in individual matters about the cybersecurity measures that should reasonably be taken, in light of those risks and the individualized circumstances of the case to protect information exchanged in the arbitral process.

B. The Protocol is intended to provide a framework that parties and arbitrators can consult in order to determine reasonable cybersecurity measures for their individual matters. The Protocol will not apply in any given case unless it is adopted by agreement of the parties or an arbitral tribunal determines that it will apply.

C. Although following the Protocol may assist in identifying applicable legal requirements, it does not supersede applicable laws or regulations which may require that specific cybersecurity measures be implemented. Furthermore, it is solely addressed at cybersecurity and does not attempt to address any other potentially applicable data protection or other measures that may be required.

D. The Protocol therefore purposefully does not adopt a one-size-fits-all approach, but rather guides parties and arbitrators in undertaking a risk-based approach to determine reasonable cybersecurity measures for a particular matter.

E. Rather than obligating the parties to follow a specific and immutable set of cybersecurity measures, the Protocol provides flexibility to accommodate party preferences and risk tolerance in light of the individual circumstances of each case.

F. It is expected that the Protocol will necessarily evolve over time in light of:

1. Changing technology;

2. New and prevalent cyberthreats;

3. New laws/regulations;

4. Any consensus that might emerge as to reasonable measures/arbitration best practices; and

5. New cybersecurity initiatives by institutions or others.

G. Although the Protocol is drafted with international commercial arbitrations in mind, Arbitral Participants may find it a useful starting point for domestic arbitration matters and/or investor-state arbitrations.

IV. Cybersecurity Protocol for International Arbitration

A. The Cybersecurity Protocol is structured as follows:

1. Articles 1-3 address general issues;

2. Articles 4-6 address the tribunal’s authority to order cybersecurity measures and the potential scope of such measures;

3. Articles 7-12 address the factors to be considered when determining what cybersecurity measures to adopt;

4. Articles 13-17 suggest a procedural framework for adopting cybersecurity measures during an arbitration;

5. Article 18 addresses cybersecurity breaches; and

6. Article 19 clarifies what is not covered.

General Provisions

1. This Cybersecurity Protocol governs issues of information security in an arbitration where the parties have agreed to follow it, or the arbitral tribunal has determined to employ it.

Commentary to Article 1

(a) Article 1 recognizes the importance of party autonomy in the conduct of international arbitrations, as well as the important role played by the tribunal in determining what cybersecurity measures are reasonable in any given case. Among other things, the arbitral tribunal may have to interpret any agreements reached by the parties, resolve any conflicts with applicable arbitration rules or mandatory provisions of law, consider the interests of other Participants such as third parties or administering arbitral institutions, and fulfill its own responsibility to maintain the integrity and legitimacy of the adjudicatory process.

(b) Subsequent Articles more fully address the role played by Arbitral Participants. In particular, Article 4 addresses the tribunal's authority over issues of cybersecurity in the arbitration, and Article 13 addresses when and how parties are recommended to enter into an agreement addressing cybersecurity.

(c) The Protocol has been prepared as a unified set of guidelines and is not intended or recommended to be applied in a piecemeal fashion.

2. The Protocol does not supersede applicable law, regulations, professional or ethical obligations.

Commentary to Article 2

(a) The Protocol is not intended to ensure compliance with any applicable law or regulation and adherence to the Protocol does not provide any liability shield or presumptions.

(b) Article 11 reminds Participants that, in determining what cybersecurity measures are reasonable for their individual matter, applicable law and regulations should be taken into account.

(c) There are multiple sources of mandatory cybersecurity regimes including those contained in many of the more than 100 national data protection laws, regulations, and industry norms applicable across the globe to certain types of personal data and data of public importance, including, for example, the European Union General Data Protection Regulation ("GDPR") and the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") in the United States.

(d) The GDPR, for example, includes a broad-reaching set of mandatory legal requirements applicable to the collection and processing of individuals' personal data. There is no exception for arbitrations and the penalties for breach may be substantial.

(e) The Protocol is limited to cybersecurity, and purposefully does not address the broader subject of how the application of data protection rules to any personal or other data exchanged in an arbitration will impact the process. However, while the security required differs among jurisdictions, to the extent personal data is exchanged during an arbitration, under the GDPR and virtually all extant data protection regimes, keeping that information secure, including implementing reasonable and proportionate cybersecurity adequate to such purpose, is mandatory.

(f) Legal requirements may apply to all who either process or control the information, including personal data, which may include all Arbitral Participants.

(g) It is therefore important in each case for all the Arbitral Participants to understand their obligations under the law(s) that may be applied to the processing of the information, including personal data. Counsel's obligations in some instances may extend to informing other relevant actors of applicable legal requirements and how they will be addressed.

(h) It is also important for counsel and arbitrators to be aware of any ethical and professional obligations of their own that have implications for cybersecurity.

3. The Protocol does not establish any liability standard for any purpose, including, but not limited to, liability in contract, for professional malpractice, or negligence.

Commentary to Article 3

(a) Article 3 makes clear that the Protocol is not intended to establish any liability standard.

(b) The Protocol proposes a mechanism for the adoption of reasonable case-specific cybersecurity measures, rather than providing what those measures should be.

(c) Article 3 is not intended to limit the rights of the parties to make agreements with respect to cybersecurity as set forth in Article 13 or the right of the arbitral tribunal to issue directives regarding cybersecurity as set forth in Article 4.

Authority to Order Cybersecurity Measures and their Potential Application

4. The arbitral tribunal has the authority to determine what security measures, if any, are reasonable in the circumstances of the case, taking into account the views of the parties (and the other Arbitral Participants, to the extent the tribunal considers to be appropriate) and to order the implementation of such measures.

Commentary to Article 4

(a) Article 4 recognizes the tribunal's express authority to determine the cybersecurity measures, if any, that are reasonable in the case. This authority is implied in the tribunal's general powers, but is expressly recognized in Article 4.

(b) In making any determination on cybersecurity, the tribunal shall take the parties' views into account.

(c) As further set forth in Article 13, in cases of party agreement, the tribunal should respect the parties' agreement on the cybersecurity measures to be employed, unless other significant countervailing factors exist that in the tribunal's view outweigh the significant weight to be given to party autonomy.

(d) Article 4 also recognizes that in some cases, third parties as well as Arbitral Participants other than the parties, also may have an interest in the cybersecurity measures to be employed, and recognizes the tribunal's right to take such views into account where appropriate.

5. In administered arbitrations, counsel and the arbitral tribunal should consider whether the application of certain cybersecurity measures may depend upon the consent of the arbitral institution or may need to be adapted to respond to the institutional rules, practices or capabilities.

Commentary to Article 5

(a) If an arbitration is administered by an institution, it may be necessary for the parties and the arbitral tribunal to consult and coordinate with that institution prior to adopting cybersecurity measures, in order to ensure that the measures are consistent with, and can be implemented pursuant to, the institution's rules, practices and technical capabilities.

(b) Depending on the degree of confidentiality of the information involved, it may be necessary to coordinate with the institution when the arbitration is being commenced (e.g., to determine whether the secure notification of a request for arbitration or request for emergency relief can be made or if a more limited filing is appropriate initially; or, to request institutional attention to the secure handling of confidential information by potential arbitrators.)

(c) As cybersecurity receives increasing attention, some arbitral institutions may adopt their own rules or practices relating to information security. For example, an institution might adopt or endorse a hosting platform for some or all of the information related to arbitrations they administer, such as a secure hosting platform for the transmission of communications and documents between the parties, the tribunal and the institution.

(d) The institution's rules and practices may or may not be deemed mandatory by the institution.

6. In determining what information security measures will be adopted in the arbitration, consideration may be given to establishing procedures for the following:

i. the transmission of communications, pleadings, disclosure materials and evidence by the parties;

ii. communications among arbitrators and between the arbitrators and any administering institution;

iii. storage of arbitration-related information;

iv. sharing arbitration-related information with authorized third parties such as experts, interpreters, stenographers, and tribunal secretaries;

v. vulnerability monitoring and breach detection;

vi. security breach notification and risk mitigation; and

vii. post-arbitration document retention and destruction.

Commentary to Article 6

(a) With respect to the transmission of communications, pleadings, disclosure materials and evidence, the following measures, among others, may be considered:

(i) limiting all exchanges and transfers of confidential commercial information and personal data in relation to the arbitration;

(ii) without prejudice to disclosure obligations, limiting the disclosure of confidential commercial information and personal data (i.e., in addition to the narrow standard generally applied to document exchange in international arbitration, the parties may consider protective measures such as redaction, pseudonymization, or anonymization of information before it is exchanged);

(iii) restricting access to arbitration-related information on a least privilege and need-to-know basis, or limiting certain information to attorneys' eyes only (e.g., under ordinary circumstances, disclosure material need not be shared with the arbitral tribunal or the institution, except in respect to disclosure disputes, in which event the material shared should be limited to what is relevant to the tribunal's resolution of the dispute); and

(iv) the method of transmission (e.g., e-mail, third-party platform or virtual data room, USB drive or other portable storage device) and corresponding protective measures (e.g., encryption; procedure for transmitting the password for a portable storage drive separately from the drive itself).

(b) If a third-party data storage platform is being considered, counsel should seek to agree on the party or other individual or entity that will host it, who will have access to the platform, and for how long.

(c) In considering which data storage platform to use, if any, counsel should consider the nature and amount of information, the amount of time it will need to be stored, whether it includes personal or other regulated data or confidential commercial information, and other issues related to the data being stored.

(d) Security breaches are addressed in Article 18 and accompanying Commentary.

(e) Issues to be considered with respect to post-arbitration document retention and destruction may include:

(i) whether to require that arbitration-related information be returned or safely disposed of (or certified as having been safely disposed of); and

(ii) the timing of any such requirement, with due consideration for applicable legal or ethical obligations, award recognition/enforcement proceedings, and legitimate interests in retaining work product.

Factors to be Considered in Developing Cybersecurity Measures

7. The cybersecurity measures to be adopted for the arbitration shall be those that are reasonable, taking into consideration: the nature of the information at issue; the potential security threats and consequences of a potential information breach; the available security capabilities of Arbitral Participants; applicable rules and legal obligations; the Purpose of the Protocol as set forth in Section III supra, and other relevant circumstances of the case.

Commentary to Article 7

(a) Article 7 sets out the elements of a risk-based approach to determining what cybersecurity measures are reasonable in individual arbitration matters. Articles 8-12 provide more detailed guidance as to each aspect of the risk analysis.

(b) By assessing risk according to the individual circumstances of a case and adopting a standard of reasonableness, Article 7 recognizes that there is no one-size-fits-all approach to cybersecurity in arbitration matters.

(c) The reasonableness standard adopted by the Protocol is consistent with an emerging global trend in favor of requiring “reasonable”, “reasonable and proportionate”, or “appropriate” cybersecurity measures when attention to cybersecurity is legally or ethically required.

(d) This approach provides flexibility to accommodate changes in technology, best practices and threats current at the time of an actual dispute, rather than obligating the parties to follow a specific and immutable set of steps.

(e) This individualized approach recognizes that implementation of cybersecurity measures entails balancing potentially competing considerations (such as cost and convenience) and that similarly situated parties may make different but equally legitimate choices based on their own preferences, including considerations of cost and proportionality, risk tolerance and technical capabilities, among others.

(f) Article 7 recognizes that there will exist categories of cases where enhanced data security protection will be necessary in light of the sensitivity of information, legal considerations, special risks or other factors. Provided it is legally permissible, there may also be cases in which parties consider that information security protection somewhat below a baseline standard is sufficient and appropriate (e.g., due to the parties’ lack of resources or infrastructure or the low-value nature of the case).

8. With respect to the nature of the information in the arbitration, the following factors, among others, may be considered:

i. what information is likely to be relevant and material in the arbitration;

ii. whether confidential commercial information will be exchanged;

iii. whether personal data will be exchanged;

iv. how much confidential commercial information and personal data is likely to be exchanged in the arbitration;

v. who has or should have access to the information exchanged during the arbitration;

vi. who “owns” the information;

vii. where the information is stored; and

viii. whether the confidential commercial information and/or personal data is subject to express confidentiality agreements or other relevant obligations, such as legal/regulatory restrictions relating to data protection/privacy, cross-border data transfer, breach notification, and/or privilege.

Commentary to Article 8

(a) Article 8 seeks to identify what information might be vulnerable to cyberthreats or increased legal risk in an arbitration.

(b) Consideration of what information is likely to be relevant and material in the arbitration can be useful in identifying types of data that are likely to be exchanged by the parties in the case.

(c) Examples of types of confidential commercial information and/or personal data that may require special care include:

(i) intellectual property;

(ii) trade secrets or other commercially sensitive information;

(iii) health or medical information;

(iv) payment card information;

(v) non-payment card financial information;

(vi) personal data, which is also referred to as personally identifying information ("PII");

(vii) information subject to professional legal privilege;

(viii) information related to or belonging to a government or governmental body (including classified data and politically sensitive information); and

(ix) information that is subject to express confidentiality agreements or other relevant obligations, such as legal/regulatory restrictions relating to data privacy, cross-border data transfer, breach notification, and/or privilege.

9. With respect to the potential cybersecurity threats and consequences of a potential breach, the following factors, among others, may be considered:

i. further to the analysis conducted under Article 8, the nature of the information likely to be involved in the arbitration;

ii. the identity of the parties, key witnesses, and other Arbitral Participants;

iii. the industry/subject matter of the dispute;

iv. the size and value of the dispute;

v. the prevalence of cyberthreats;

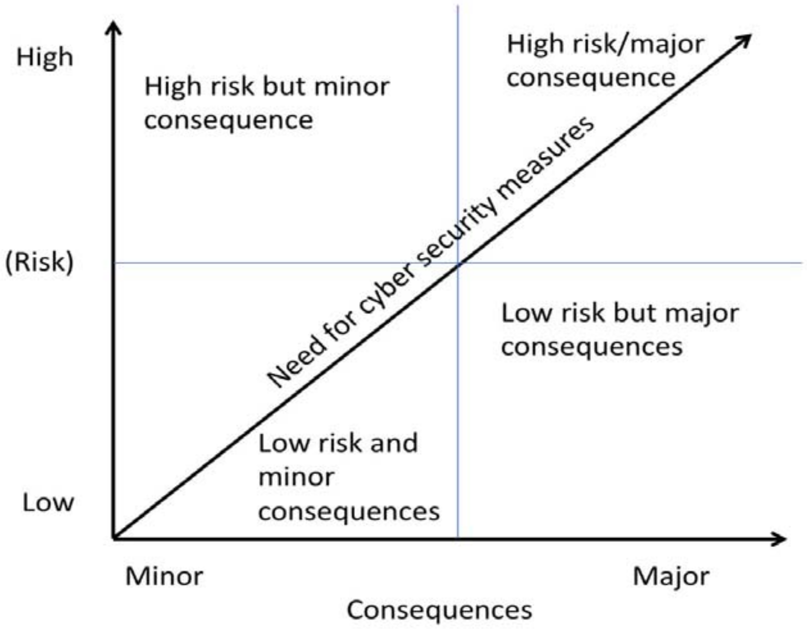
vi. the nature and frequency of international travel likely to be required for the arbitration; and

vii. the severity of potential consequences if there is a breach of information security.

Commentary to Article 9

(a) Article 9 sets out some factors that may be relevant in analyzing information security risk in the arbitration. The risk is a function of the likelihood of a cybersecurity breach and the consequences of that breach. Typically, parties and/or the tribunal will wish to determine whether the risk of a cyberattack or other information security breach in the particular circumstances of the arbitration is high or low, and whether the consequences of a breach are likely to be minor, moderate, or severe.

(b) The threat of a cyberattack and consequent desirability of cybersecurity measures can be plotted on a chart as follows:


High
(Risk)
Low
High risk but minor consequence
High risk/major consequence
Need for cyber security measures
Low risk but major consequences
Low risk and minor consequences
Minor
Major
Consequences

(c) A case with a large counsel team, for example, will have more points of vulnerability and may necessitate stricter cybersecurity measures.

(d) Some issues to consider in analyzing the information security risk that may attach to the identity of the parties, key witnesses, and other Arbitral Participants (including the arbitral institution, experts, and counsel) include:

(i) Whether the matter involves a party or other Arbitral Participant with a history of being targeted for cyberattacks;

(ii) Whether the matter involves parties that handle large amounts of high-value confidential commercial information and/or personal data;

(iii) Whether the matter involves a public figure, high-ranking official or executive, or a celebrity; and

(iv) Whether the matter touches upon any government, government information, or government figure.

(e) Travel tends to increase information security risk. Consideration should be given to how often and to where Participants are likely to travel with arbitration-related information and whether there are particular risks associated with a particular destination. Some jurisdictions may assert the right to access information on portable devices as a condition of entry, for example. Consideration should also be given to how arbitration-related information is likely to be transported (e.g., whether it will be downloaded on portable devices or accessed via a secure server).

(f) Some questions to consider in analyzing the consequences and severity of a potential breach of information security may include:

(i) The value of the information to the parties;

(ii) The value of the information to third parties;

(iii) The nature, type, and amount of personal data being processed and whether it is legally regulated;

(iv) Potential embarrassment or damage caused by public disclosure of the information;

(v) Whether and how the information could be (mis)used by a third party (e.g., politically, for extortion purposes, for insider trading purposes, or to obtain a competitive advantage).

(g) In addition to considering the potential impact of a breach on the Arbitral Participants, consideration should be given to the potential impact on persons outside of the arbitration process, including but not limited to the persons to whom personal data relates. An information breach suffered by one Arbitral Participant may cause injury to other Participants or third parties.

10. With respect to the available security capabilities, the existing digital infrastructure of Arbitral Participants and any potential technical impediments to implementing cybersecurity measures should be considered.

Commentary to Article 10

(a) Once parties and the tribunal have assessed the seriousness of the cybersecurity threat in the circumstances of the particular arbitration and the desirability of cybersecurity measures, it is then necessary to weigh the degree of cybersecurity measures suggested by the threat against practical considerations, including what measures are proportionate to the size and value of the dispute.

(b) Article 10 recognizes that the Arbitral Participants, including the parties, counsel, the arbitrators, and administering institutions, may have differing technical resources and constraints on their technical capacity that will influence what may be reasonable in a particular case.

(c) General cyber awareness by the Participants, including their day-to-day security practices and digital infrastructure, may also determine what security measures may be warranted in any given arbitration matter. For example, when all Participants already employ a high level of cybersecurity, additional measures may not be needed. Schedule C highlights general cybersecurity practices that all Arbitral Participants should take into consideration.

(d) While the limitations of a party’s resources are an important factor, consideration also should be given to the security needs of the case, the accessibility and affordability of security resources, and measures that may be taken without significant expenditure.

11. Applicable rules and legal obligations may dictate that certain types of cybersecurity measures be adopted regardless of the threat inherent in the individual circumstances of the arbitration. Among the factors that may be considered are the following:

    i. contractual obligations such as confidentiality agreements;

    ii. relevant arbitration rules;

    iii. ethical and professional obligations; and

    iv. regulatory obligations including those that are industry-related (e.g., HIPAA) and those that are information-related, including those applicable to personal data (e.g., GDPR and other data protection laws and other privacy rights).

Commentary to Article 11

(a) As discussed in the Commentary to Article 2, the Protocol is not intended to assure compliance with, and does not supersede, applicable law, regulations, professional or ethical obligations.

(b) Arbitrators and parties may also be faced with differing or conflicting mandatory obligations. The arbitral tribunal will have to determine how to harmonize such obligations, taking into consideration the consequences of non-compliance as well as due process considerations for all concerned.

12. Other relevant considerations in determining what measures are reasonable may include, but are not limited to:

    i. workflow needs and preferences;

    ii. cost;

    iii. proportionality;

    iv. burden/relative resources; and

    v. efficiency.

Commentary to Article 12

(a) Article 12 recognizes that if proposed cybersecurity measures would be so onerous as to prevent the arbitration from proceeding in an orderly fashion, then the balance of “reasonableness” may weigh against their adoption.

(b) In particular, cybersecurity measures that are too strict or difficult: (i) risk being ignored or evaded; and (ii) may have a negative impact on the ability of Participants to accomplish necessary tasks.

Procedural Considerations When Adopting Cybersecurity Measures

13. In the first instance, the parties should attempt to agree on reasonable cybersecurity measures, if any. Any agreement is subject to approval by the arbitral tribunal.

Commentary to Article 13

(a) Article 13 recognizes the importance of party autonomy. Normally, counsel should be responsible in the first instance to meet and confer on the information security protection measures to be implemented in a particular arbitration, taking into account existing cybersecurity measures already employed by the Arbitral Participants.

(b) Issues that counsel should consider discussing with their clients and opposing counsel may overlap with issues ordinarily considered in the context of disclosure and document preservation.

(c) In principle, where possible, the parties should agree on the cybersecurity measures to be employed, which should be reasonable taking into account the factors discussed above in Articles 7-12.

(d) Notwithstanding the principle of party autonomy, the parties cannot bind the arbitral tribunal. Nor can the parties bind the institution administering the arbitration. Any preliminary agreement should be formalized only after consultation with the tribunal and, where appropriate or required, the arbitral institution.

14. The tribunal should consider issues of cybersecurity, including any agreement that may have been reached by the parties, as early as practicable, which ordinarily will not be later than the first case management conference.

Commentary to Article 14

(a) The expectation generally is for issues of cybersecurity to be discussed with the parties in preparation for, and during, the initial case management conference or procedural hearing, and then to be incorporated in a procedural order.

(b) However, in certain cases, the initial hearing or conference may either be too late or too early; hence, any party may raise cybersecurity measures for consideration at any time.

(c) At the initial conference, the arbitral tribunal should be prepared to:

(i) discuss the ability and willingness of its members to adopt specific security measures;

(ii) engage counsel in a discussion about reasonable cybersecurity measures;

(iii) resolve any disputes about reasonable cybersecurity measures;

(iv) express its own interests in preserving the integrity of the arbitration process, taking into account the parties’ concerns and preferences, the capabilities of any administering institution and other factors discussed in this Protocol; and

(v) render an appropriate order or include cybersecurity provisions in an early procedural order.

(d) Cybersecurity measures may also be set forth in a stipulation of the parties approved by the tribunal.

(e) Ordinarily the tribunal should defer to the parties' agreement, but there may be circumstances for departure. Such circumstances may include but are not limited to:

(i) measures to protect third-party interests, including other Arbitral Participants or third-party witnesses;

(ii) applicability of mandatory legal and regulatory requirements and other rules;

(iii) capabilities of the arbitrators and administering institution;

(iv) the tribunal's own interest in protecting the integrity of the process, including the security of its own communications and deliberations.

(f) The procedures adopted at the outset of the arbitration should allow for modification as necessary throughout the course of the proceeding, including updates as to: (i) what qualifies as the nature of the information being processed; (ii) required procedures based on the specific circumstances of the case as it develops; and (iii) changed circumstances, such as changes in applicable law, risks in the proceeding, institutional rules/requirements, or technological developments. Such updates should be made after consultation with the parties and any administering arbitral institution.

(g) The tribunal may modify the measures previously agreed to by the parties or determined by the tribunal at the reasoned request of any party, or on its own initiative in light of the evolving circumstances of the case.

15. Arbitral Participants and fact witnesses should be informed of the cybersecurity measures in place and shall agree in writing to comply with such measures before receiving any arbitration-related information, provided that where an essential third-party expert, fact witness or Vendor is unable or unwilling to comply with the agreed standards, the matter shall be referred to the tribunal for consideration, and, if necessary, direction.

16. The technical capability of Vendors should be no less than the minimum requirements designated by the parties.

Commentary to Articles 15-16

(a) Third parties present a difficult area for the protection of confidential information in general and electronically stored information in particular. They are not under the control of the tribunal and may not suffer directly from the consequences of a cybersecurity breach. Nevertheless, there is little point in agreeing to stringent cybersecurity measures for the parties, counsel, the tribunal and institution if the same information is to be sent to third parties without adequate safeguards. Further, to the extent that legal requirements apply, these may require third parties to agree to adequate safeguards before the information is shared.

(b) Where possible, counsel should obtain the written agreements of third parties to abide by cybersecurity measures that have been agreed or ordered by the tribunal.

(c) Where third parties either cannot or will not agree to comply, the tribunal shall be informed and direction given where appropriate.

17. Cybersecurity is the shared responsibility of all Arbitral Participants involved in an arbitration. Arbitral Participants are responsible for ensuring that all personnel directly or indirectly involved in an arbitration are aware of, and follow, cybersecurity measures being adopted in a proceeding as well as the potential impact of a cybersecurity breach.

Commentary to Article 17

(a) The security of information in an arbitral proceeding ultimately depends on the decisions and actions of all individuals involved, and any individual actor can be the cause of a cybersecurity breach. Many security breaches result from individual conduct rather than a breach of systems or infrastructure.

(b) In a case with multiple parties and large counsel teams, for example, it is necessary for Arbitral Participants to make persons directly or indirectly involved aware of any cybersecurity measures, and of their agreement to be bound by them, whether by express agreement or as part of their employment conditions or consulting agreement.

(c) The Arbitral Participant providing access to arbitral information covered by cybersecurity measures is responsible for ensuring that the persons with whom it is shared are aware of those measures and agree to follow them.

(d) This may involve a large number of people, each of whom could prove to be the weak link.

(e) Arbitral Participants should identify the various team members who support them and have access to digital information. For example, counsel appearing on behalf of a party in an arbitration may be supported in the background by additional lawyers who are not known to the other party or tribunal, administrative staff, and legal assistants or law clerks.

(f) Similarly, within an arbitral institution, case administration may involve a team of case management personnel, administrative support staff, and members of the institution's standing court of arbitration practitioners. To mitigate the risk of data breaches, cybersecurity awareness must permeate organizational structures and extend beyond the core Participants in the arbitral process to such team members and support personnel.

Cybersecurity Breaches

18. The cybersecurity measures adopted for the arbitration may address material issues related to possible information security breaches, including, among other things:

i. what constitutes a security breach;

ii. who shall be notified of a breach;

iii. timing of the notification; and

iv. specific steps to be taken to mitigate any information breach.

Commentary to Article 18

(a) Steps that may be taken to mitigate any information security breach may include, depending on the circumstances:

(i) implementing measures to identify the specific source of the breach;

(ii) taking steps to correct any weaknesses in security systems in order to mitigate the impact of a breach and/or prevent further breaches;

(iii) informing all affected parties that a breach occurred, consistent with any applicable legal obligations, in a timely manner and in a manner best preserving the confidentiality of the arbitration;

(iv) if appropriate, taking systems and applications offline to prevent further loss of information;

(v) taking steps to retrieve lost information and to ensure that unauthorized recipients delete or return information;

(vi) if appropriate, enlisting Vendors to manage effects of breach; and

(vii) if appropriate, involving law enforcement.

(b) Applicable laws may dictate the required procedures for addressing cybersecurity breaches. The GDPR, for example, includes strict mandatory 72-hour breach notification requirements. Some U.S. states have also adopted harm triggers; for example, if a lost laptop has full-disk-encryption-enabled, no notification would be required.

(c) There may also be a need to assess the nature of the breach, whether there has been unauthorized access to information, and whether there is an urgent need to take corrective action to prevent further breaches.

(d) Until a breach occurs, it may not be possible to determine what breach notification obligations exist as a matter of law even if compliance may require swift action.

Matters Not Covered by the Protocol

19. The following matters are beyond the scope of this Protocol:

i. the allocation of costs arising from the implementation of the Protocol and/or from any data breach or alleged failure to implement information security measures as directed by the arbitral tribunal; and

ii. the nature and scope of any authority of the arbitral tribunal to impose sanctions in the event of a data breach or alleged failure to implement information security measures as directed by the arbitral tribunal.

Commentary to Article 19

(a) The Protocol purposefully does not address either the allocation of costs or the tribunal's authority to order sanctions arising from data breaches or an alleged failure to implement information security measures as directed by the arbitral tribunal.

(b) However, while the Protocol does not expressly address such issues, it is not intended to negate authority otherwise available to the tribunal to allocate costs or impose sanctions.

Schedule A
Arbitration Agreement

It is not recommended that parties specify particular cybersecurity measures in their arbitration agreement because technology may change materially by the time the dispute arises, and the circumstances of the subsequent dispute may inform the cybersecurity measures that the parties choose to adopt. However, the parties may want to provide generally in their arbitration agreement that the arbitration shall be conducted in a secure manner in line with the Cybersecurity Protocol for International Arbitration. The following language would be appropriate for inclusion in the arbitration agreement:

> The parties agree that the arbitration shall be conducted in a secure manner as determined by the arbitral tribunal, taking into consideration the views of the parties and the Cybersecurity Protocol for International Arbitration.

Schedule B
Model Language for Specific Cybersecurity Measures*

Article 13 of the Protocol provides that parties should in principle agree on the cybersecurity measures to be employed, but that these measures should not be adopted without the approval of the tribunal. Further, Article 14 provides that the tribunal should typically adopt such language into a procedural order or by stipulation of the parties after the first case management conference, to be updated as the case proceeds.

The language set forth below providing for specific cybersecurity measures and related issues may be considered for inclusion in party agreements and/or tribunal orders. The adoption of case-specific cybersecurity measures whether by agreement of the parties, which will typically require tribunal approval, or by tribunal order, may include the language set forth below or some variation thereof depending on the circumstances.

1. [Model Language Re: Baseline Cybersecurity Measures]

2. [Model Language Re: Enhanced Cybersecurity Measures]

3. [Model Language Re: No Additional Cybersecurity Measures]

4. [Model Language Re: Notification of Data Breach and/or Breach of the Cybersecurity Measures]

5. [Model Language Re: Cybersecurity Dispute Resolution]

6. [Model Language Re: Use of Special Expert on Cybersecurity Issues]

7. [Model Language Re: Damages for Breach of Cybersecurity Measures]

8. [Model Language for inclusion in Vendor Agreements]

9. [Model Language Re: Agreement to Share Expenses of Cost of Enhanced Cybersecurity Measures]

10. [Possible Model Procedural Order (standard provisions subject to adaptation in individual cases)]

* Inclusion of Model Language to be considered based on feedback from the Consultation Process.

Schedule C
General Cybersecurity Practices

1. Because the Participants in international arbitration are, to a large degree, digitally interdependent, all Participants (including counsel, witnesses, experts, arbitrators, Vendors and arbitral institutions) involved in the arbitration should be conscious of good general cybersecurity practices for storing and processing information obtained during the arbitral process.

2. All Participants should be conscious of their own, regular cybersecurity practices and digital infrastructure as a threshold matter, because Participants' day-to-day security practices and infrastructure pre-date individual arbitrations, and therefore have an immediate and continuing impact on the security of arbitration-related information.

3. Depending on the circumstances, examples of good general cybersecurity practices may include:

   (a) Creating access controls, such as strong, complex passwords and multi-factor authentication when appropriate and secure password storage and controls.

      (i) Access controls, including user account management, passwords, and multi-factor authentication, determine who has authority to access information and what privileges s/he has to use it.

      (ii) In June 2017, the National Institute of Science and Technology ("NIST") substantially revised longstanding password guidance (see NIST Special Publication 800-63B). Key recommendations include that passwords should be based on unique passphrases, at least 8 characters long, and easily remembered ("memorized secrets"). In addition, common dictionary words, past passwords, repetitive or sequential characters, and context-specific words (such as derivatives of the service being used) should be avoided, and mixtures of different character types are unnecessary. The NIST further recognizes that in many cases, password managers increase the likelihood that users will choose stronger memorized secrets.

      (iii) Multi-factor authentication allows a user to safeguard a digital account (such as an e-mail account) from unauthorized access by requiring that the user provide additional proof of identity beyond a password. Given the frequency with which Participants in international arbitrations travel, to the extent they consider it is warranted to use multi-factor authentication, they may wish to ensure that any method they use is available offline.

   (b) Guarding digital "perimeters" using measures such as firewalls, antivirus and antispyware software, operating system updates and other software patches.

   (c) Adopting secure protocols, such as encryption for the storage and transmission of arbitral information, that are reasonable, taking into account the nature of the data and its required use within the arbitral process.

      (i) Arbitral information should generally be protected during transmission using industry-standard encryption technology, which prevents communications from being intercepted and read as they travel from end-to-end. It may also be appropriate under certain circumstances and depending on the nature of the data to encrypt individual file attachments.

(ii) To guard against unauthorized access of digital information due to loss or theft of a laptop or other mobile devices, it may be reasonable to enable full disk encryption (which is often built into device operating systems) to protect all data stored on the device while it is at rest.

(iii) If information is stored in the cloud, depending on the nature of the information, it may sometimes be appropriate to encrypt the information before it is uploaded and to keep control of the encryption key out of the hands of the cloud provider.

(d) Being mindful of public internet use in hotels, airports, coffee shops and elsewhere and considering protective measures such as personal cellular hotspots or virtual private networks (VPNs) where warranted in light of encryption and other measures being employed. Public Wi-Fi may provide hackers with access to unsecured devices on the same network, allow them to intercept password credentials, or to distribute malware. As an alternative to public Wi-Fi, Arbitral Participants may wish to use a mobile hotspot to establish an internet connection. Where appropriate, other protective measures could include using a VPN to encrypt communications traveling on the unsecured network connection and/or avoid connecting to any websites that fail to use HTTPS security.

(e) Being mindful to download programs and digital content only from legitimate sources and not to open attachments from unknown email senders.

(f) Keeping mobile devices close and making use of available protective measures in case of loss or theft, possibly including full disk encryption and remote tracking and wiping.

(g) Making routine secure and redundant data back-ups. Redundant data back-ups allow users to recover information in the event data is lost or corrupted due to human error, hardware failure, ransomware attack, or otherwise. One possible approach is to follow the so-called 3-2-1 rule, which means there should be 3 copies of the data, 2 should be stored locally on different storage media, and 1 copy should be stored offsite.

(h) Knowing one’s data security infrastructure, including professional and personal networks, computers and portable devices, cloud services, software program and apps, remote access tools and back-up services.

(i) Implementing document and data preservation policies to minimize storage of data no longer required.

(j) Making reasonable on-going efforts to be educated about evolving cybersecurity risks and best practices.

4. All Arbitral Participants should have an understanding (if not a written inventory) of where data resides in, and flows through, their digital infrastructure, in order that appropriate controls and safeguards may be implemented. An arbitrator who regularly uses a personal tablet to review pleadings and exhibits, for example, should know whether the documents will be stored locally on the tablet by default, on servers for the application(s) used to review the documents, and/or personal cloud storage.

5. Once Arbitral Participants are cognizant of their own digital architecture, they can take steps to mitigate the risk of data breaches from basic security vulnerabilities. More often than not, data breaches arise from malicious actors who look for and find security vulnerabilities to exploit rather than from targeted attacks. Many of these security vulnerabilities arise from a failure to implement and/or maintain basic, well-established security practices that do not require any significant financial resources, technological support, or infrastructure investment.

Schedule D
Glossary

(Please note that not all of the terms defined below appear in the draft document.)

Access Control – The process of granting or denying specific requests to: (i) obtain and use information and related information processing services; and (ii) enter specific physical facilities.

Antispyware Software – A program that specializes in detecting both malware and non-malware forms of spyware.

Antivirus Software – A program specifically designed to detect many forms of malware and prevent them from infecting computers, as well as cleaning computers that have already been infected.

Attribution – The process of tracking, identifying and laying blame on the perpetrator of a cyberattack or other hacking exploit.

Authentication [includes multi-factor authentication and dual-factor authentication] – Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

Backing Up – The act of making a copy of files and programs to facilitate recovery, if necessary. (See also *Data Backup*.)

Breach Notification – Notification of the unauthorized movement or disclosure of sensitive information to a party, usually outside the organization, that is not authorized to have or see the information.

Business Continuity Management – The documentation of a predetermined set of instructions or procedures that describe how an organization's mission/business processes will be sustained during and after a significant disruption.

Chief Information Security Officer (CISO) – The individual responsible for overseeing and implementing an entity's cybersecurity program and enforcing its cybersecurity policies.

Cloud – A model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Computer Forensics – The application of computer science and investigative procedures involving the examination of digital evidence – following proper search authority, chain of custody, validation with mathematics, use of validated tools, repeatability, reporting, and possibly expert testimony.

Cyberattack – An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.

Cybersecurity – The ability to protect or defend the use of cyberspace from cyberattacks.

Cyber Exercise – A simulation of an emergency designed to validate the viability of one or more aspects of an IT plan. (See also *Information Technology (IT)*.)

Cyber Incident – Actions taken through the use of an information system or network that result in an actual or potentially adverse effect on an information system, network, and/or the information residing therein.

Cyber Incident Response Plan – The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a cyber incident involving an organization's information system(s).

Cyber Risk – The potential of loss or harm related to technical infrastructure or the use of technology within an organization.

Data Backup – A copy of files and programs made to facilitate recovery, if necessary.

Data Breach – The unauthorized movement or disclosure of sensitive information to a party, usually outside the organization, that is not authorized to have or see the information.

Data Integrity – The property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing, and while in transit.

Data Loss – The exposure of proprietary, sensitive, or classified information through either data theft or data leakage.

Data Privacy – Assurance that the confidentiality of, and access to, certain information about an entity or individual is protected.

Data Recovery – The process of restoring data that has been lost, accidentally deleted, corrupted or made inaccessible.

Data Storage – Retrievable retention of data. Electronic, electrostatic, or electrical hardware or other elements (media) into which data may be entered, and from which data may be retrieved.

Data Transfer – The act of electronically sending information from one location to one or more other locations.

Data Wiping – Overwriting media or portions of media with random or constant values to hinder the collection of data.

Decryption – The process of transforming ciphertext into plaintext using a cryptographic algorithm and key.

Denial of Service – Actions that prevent a system from functioning in accordance with its intended purpose. A piece of equipment or entity may be rendered inoperable or forced to operate in a degraded state; operations that depend on timeliness may be delayed.

Digital Perimeter – A physical or logical boundary that is defined for a system, domain, or enclave, within which a particular security policy or security architecture is applied.

Document Destruction – Destroying, overwriting, deleting, or otherwise rendering digital, electronic, or physical documents unusable.

Document Retention – The identification, storage, retrieval, and maintaining of digital, electronic, or physical documents, files, or records pursuant to legal, specific contract, or other obligations.

Encryption – Any procedure used in cryptography to convert plaintext into ciphertext to prevent anyone but the intended recipient from reading that data.

Endpoint Monitoring – Automated tools, software, and procedures that track and ensure the security of network devices and systems.

Firewall – A gateway that limits access between networks in accordance with local security policy.

Full Disk Encryption – The process of encrypting all the data on the hard drive used to boot a computer, including the computer's operating system, and permitting access to the data only after successful authentication with the full disk encryption product.

General Disruption – An unplanned event that causes an information system to be inoperable for a length of time (e.g., minor or extended power outage, extended unavailable network, or equipment or facility damage or destruction).

Hacker – Unauthorized user who attempts to or gains access to an information system.

Hacking – The act of gaining unauthorized access to a digital device, network, system, account or other electronic repository. (See also *Hacker*.)

Identity Theft – Wrongfully obtaining and using another person's personal data in some way that involves fraud or deception, typically for economic gain.

Incident Response – The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a cyber incident involving an organization's information systems(s). (See also *Cyber Incident Response Plan.*)

Information Technology (IT) – Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an entity or individual. The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.

Intrusion Detection System (IDS) – A security service that monitors and analyzes network or system events for the purpose of finding, and providing real-time or near real-time warning of, attempts to access system resources in an unauthorized manner.

Intrusion Prevention System (IPS) – A system that can detect an intrusive activity and can also attempt to stop the activity, ideally before it reaches its targets.

Keyboard Logger (also "Keylogger") – A program designed to record which keys are pressed on a computer keyboard, often used to obtain passwords or encryption keys and thus bypass other security measures.

Malware – A computer program that is covertly placed onto a computer with the intent to compromise the privacy, accuracy, or reliability of the computer's data, applications, or operating system. Common types of malware threats include viruses, worms, malicious mobile code, Trojan horses, rootkits, and spyware.

Managed Services – A service provider that remotely manages a customer's IT infrastructure and/or end-user systems, typically on a proactive basis and under a subscription model.

Multi-Factor Authentication (MFA) Proxy Server – Authentication using a server that services the requests of its clients by forwarding those requests to other servers and uses two or more different factors to achieve authentication. Factors include: (i) something you know (e.g., password/PIN); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric).

Password – A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization.

Payment Card Industry (PCI) – Commonly refers to the Payment Card Industry Data Security Standard (PCI DSS), which is a set of policies and procedures developed to protect credit, debit, and cash card transactions and prevent the misuse of cardholders' personal information. PCI DSS compliance is required by all card brands.

PCI Forensic Investigator (PFI) – Companies, organizations or other legal entities charged with investigating cyber incidents related to Payment Card Industry information; organizations in compliance with all PFI Company requirements (as defined by the Payment Card Industry Security Standards Council (PCI SSC)) and have been qualified as PFI Companies by PCI SSC for purposes of performing PFI Investigations.

Personal Cellular Hotspot – A mobile hotspot is an *ad hoc* wireless access point created by a dedicated hardware device or a smartphone feature that shares the cellular data.

Personally Identifying Information (PII) – Information which can be used to distinguish or trace the identity of an individual (e.g., name, social security number, biometric records, etc.) alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual (e.g., date and place of birth, mother's maiden name, etc.).

Phishing – Tricking individuals into disclosing sensitive personal information by claiming to be a trustworthy entity in an electronic communication.

Ransomware – A type of malware that is a form of extortion. The malware works by encrypting a victim's hard drive, thus denying the victim access to encrypted files. The victim must then pay a ransom to obtain a key to decrypt the files and gain access to them again.

Remote Desktop Protocol (RDP) – Provides remote display and input capabilities over network connections for Windows-based applications running on a server. RDP is designed to support different types of network topologies and multiple Local Area Network (LAN) protocols.

Remote Tracking – A tool designed to help remotely and proactively monitor mobile devices, laptops, or other systems.

Server Message Block (SMB) – A network protocol used by Windows-based computers that allows systems within the same network to share files. It allows computers connected to the same network or domain to access files from other local computers as easily as if they were on the computer's local hard drive.

Software Patch – A software component that, when installed, directly modifies files or device settings related to a different software component without changing the version number or release details for the related software component.

Spoofing – Faking the sending address of a transmission to gain illegal entry into a secure system.

Spyware – Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code.

Trojan Horse – A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program.

Virtual Private Network (VPN) – A restricted-use, logical (i.e., artificial or simulated) computer network that is constructed from the system resources of a relatively public, physical (i.e., real) network (such as the internet), often by using encryption (located at hosts or gateways), and often by tunneling links of the virtual network across the real network.

Vulnerability – Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

Worm – A computer program that can run independently, can propagate a complete working version of itself onto other hosts on a network, and may consume sources destructively.