ADR in CYBER, PRIVACY and DATA BREACH RELATED DISPUTES

Jean M. Lawler
Lawler ADR Services, LLC
Los Angeles, CA

Keith A. Langley
Langley Attorneys & Counselors
Dallas, TX

So now that a data breach has been contained, a ransom paid, insurance claims submitted, and lawsuits pending – what's next? Mediation and, if not settled, either Arbitration or Litigation. There is money to be recovered by the insurer, person or entity who incurred the expense of recovering from a data breach and/or paying a ransom, subrogating against the allegedly negligent entities that allowed the threat actors into the company's network. There may be privacy lawsuits by consumers or state agencies waiting to be settled. There may be insurance coverage issues needing to be resolved – including "silent cyber" issues. Ultimately, there are businesses involved that need to get back up and running. In an era defined by digital interconnectedness, the realm of cybersecurity has become a critical focal point for legal practitioners. As cyber threats continue to evolve, the need for efficient and effective resolution mechanisms is paramount. How to resolve these disputes using ADR processes?

General Types of Alternative Dispute Resolution Processes

First and foremost, there is not a one-size-fits-all approach to resolve these disputes. Every situation is unique, with its facts in turn dictating dispute resolution approaches that might work. That said, what might some of those options look like?

1. EDR – Early Dispute Resolution

Early Dispute Resolution is a form of ADR that focuses on approaching the dispute early, as it says in its name, without need for formal discovery. It is intended as a way of getting the parties together as early as possible to work out a resolution in an expeditious and economical way. The stated goal of EDR, by The EDR Institute, is to resolve most disputes within 30-60 days of inception. It is a process that is gaining national attention, with more businesses embracing it.

A form of Mediation, the EDR process is also meant to be confidential. The EDR process consists of four steps: (a) Initial Case Assessment; (b) Information and Document Exchange (including, if appropriate, EDR Experts); (c) Risk-Benefit Analysis; and (d) Final Resolution.[1]

2. Traditional Mediation

This is the most typical approach. In cyber and data breach/ransomware cases, mediation is often held before suit or arbitration is even filed. Mediation can be held in

[1] The EDR Institute, www.EDRinstitute.org, EARLY DISPUTE RESOLUTION PRACTICE PROTOCOLS, page 5, sec. 2.7

person or online. The parties in mediation typically include the company that was the victim of the data breach and its vendor(s) alleged to have been responsible for the data breach, along with each of their respective insurers and/or risk managers. These vendors often include Managed Service Providers who may host and maintain a company's website, its IT Techs, some equipment or software suppliers, and others. A vendor's vendor is increasingly seen as a target in mediation of these cases. The insurers may include cyber insurers, technology or management liability insurers, D&O (Directors & Officers) and/or professional liability insurers, Crime insurers and those insuring related first party coverages.

On the Claimant's side, there may be multiple claimants participating in multiple businesses that may have experienced a breach because of the negligence or other liability of a particular respondent/defendant. For example, the managed service provider may be managing and maintaining the servers for many businesses, especially if small businesses or professional service firms are involved. Not every company with a loss has presented a claim and the applicable statute of limitations has not yet expired.

At its core, for mediation these cases present questions typical to product liability, insurance cases, professional liability, breach of contract, breach of fiduciary duty, D&O, and the like. If there are multiple claimants, or the potential for multiple claimants, an insurer of a defendant will be hesitant, if not outright unable, to exhaust its policy paying a claim for only those parties in the mediation. There may also be insurance coverage issues on the part of the defendant(s) as to which policies pay and/or how to allocate between multiple policies. Excess insurance may also be involved. Coverage for certain exposures or types of damage may be excluded. The defendant may be looking at a potential bankruptcy or may have already filed.

There are just so many variables that it is critical that companies involved in a data breach, regardless of which side of the situation they are on, notify their insurers immediately, get their damage claims documented as quickly as possible, and get into mediation as early as possible. Ideally this can happen pre-suit or pre-arbitration, but at the very least, even if suit or arbitration is filed, get the matter into mediation as soon as possible.

3. Mandatory Mediation Clauses and Court Ordered Mediation

Many vendor contracts require the parties to mediate prior to going to Arbitration or filing a lawsuit, with a consequence for not doing so. Many of these terms will provide that the failure to do so will result in the inability to collect attorney fees and costs, for example. It is imperative that parties and their counsel read the fine print on the vendor contract before proceeding to suit or arbitration. If they do not, they moved forward at their peril.

Most courts, especially the federal courts where many of these cases will end up, have mandatory court ordered mediation programs, including requiring early mediation. Whether using a court's panel mediator or a private mediator, early mediation should be embraced.

4. Mandatory Arbitration Clauses

Risk avoidance is the best form of risk management. Many, if not most, vendor contracts these days include mandatory arbitration clauses. It is very important at the negotiation stage that those involved consider all aspects to create a clause that is as clear as possible. The “who”, “what”, “when”, “where” and “how” questions should all be answered. Once a claim arises, as it very likely will, the vendor contract (along with the applicable insurance policies) is one of the first contracts to be reviewed in terms of dispute resolution. Crafting arbitration clauses with precision is a foundational step. In cybersecurity cases, specificity is crucial. Parties should delineate the scope of disputes covered, identify the applicable laws and regulations, and stipulate the qualifications of arbitrators with expertise in cybersecurity matters. If there is a mandatory arbitration clause, or a mandatory mediation clause, those clauses will direct next steps. A well-crafted clause sets the stage for a smoother ADR process.

5. Arbitrating Cybersecurity Cases

Arbitration offers a compelling avenue for resolving cybersecurity disputes, providing a framework that aligns with the dynamic nature of technology. Among other things, arbitrating cybersecurity cases necessitates a deep understanding of both legal and technical aspects. Lawyers should cultivate a multidisciplinary approach, engaging with cybersecurity experts to bridge the gap between legal frameworks and technological intricacies. This collaboration is indispensable in ensuring a comprehensive assessment of the issues at hand.

Cybersecurity disputes can be highly nuanced, requiring a tailored procedural approach. Lawyers should be adept at adapting traditional arbitration procedures to accommodate the unique characteristics of these cases. This may involve expediting proceedings in the face of imminent threats, allowing for technical experts' testimonies, or facilitating remote hearings to accommodate global stakeholders. Navigating the evidentiary landscape in cybersecurity cases poses distinctive challenges. Lawyers must grapple with digital forensics, complex technical reports, and rapidly evolving threat landscapes. It is imperative to engage experts capable of translating technical data into a format comprehensible to arbitrators, ensuring a well-informed decision-making process.

Preserving the confidentiality of sensitive information is paramount in cybersecurity cases. Lawyers must diligently address confidentiality concerns, incorporating robust protective measures into the arbitral process. This may include employing secure communication channels, implementing encryption protocols, and establishing strict access controls.

The landscape of cybersecurity is continually evolving, introducing new threats and regulatory frameworks. Lawyers involved in arbitrating cybersecurity cases must remain vigilant and adaptive, staying abreast of emerging trends, technologies, and legal precedents. This proactive approach enables practitioners to effectively advocate for their clients in a rapidly changing environment. Arbitrating cybersecurity cases demands a unique set of skills and considerations. Lawyers specializing in this field must join legal acumen with technical expertise, navigate intricate evidentiary challenges, and remain agile in the face of emerging threats. By adopting a multidisciplinary approach, crafting tailored arbitration clauses, and prioritizing confidentiality and security,

practitioners can adeptly navigate the complex terrain of cybersecurity arbitration. In doing so, they contribute to a more secure digital landscape for individuals, businesses, and society at large.

Typical Types of Cyber Disputes Going through ADR Process

Keep in mind that there are cyber incidents and data breaches. They do not necessarily mean the same thing and they do not necessarily mean the same types of issues are at play. If there has been an incident but no extraction of private personal information (e.g., employee records, patient, student, client, or customer information, etc.), then it is a very different situation than one where there has been extraction of personal information.

1. Ransomware or Data Breach Subrogation and/or Contractual Indemnification Suits for a Cyber Incident without Extraction of Private Personal Information

These cases generally involve vendors and vendor contracts. Interesting and able to be resolved relatively easily, they involve the payment of money by one party (or its insurer) to another party, parties, or insurers. It is straightforward. A loss happened. Liability is often attributable to the vendor. Damages can be ascertained. The pool of companies with direct claims against the vendor can be identified and the vendor will ideally have insurance that responds to the claims. These suits can also be characterized as subrogation suits, with the Claimant or its insurer having paid out on the loss for which they then seek to recover the money paid. The key to resolving these types of disputes is to mediate early and have the financial records in place to share with the other party to substantiate the damages being sought. If liability is not clear, then causation documents and expert reports will be needed. But that said, the goal for the Company that is a victim of a data breach or ransom demand is to get their systems back up and running as quickly as possible and with as little interruption to their customer-facing systems as possible.

2. Data Breach with Extraction of Private Personal Information

These cases are much more complicated to resolve, but resolvable. One difference will be in the nature of the Claimants as in addition to the Company, there will likely be individuals making claims. These individuals will be employees, customers, clients, patients, students, etc. whose personal information has been taken. In these cases, there will be economic damages, but also probable state and/or federal regulatory laws and protocols with which to comply, depending on the data breach.

3. Class Actions

Most class actions settle – we have all received those postcards advising of a settlement and our rights to opt out or in. That said, these are complex cases with multiple parties and issues, involving multiple mediation sessions to resolve. The same basic principles apply, but just with more parties, people, issues, claims, contracts, and insurance involved. They will also often involve federal statutory violations and, with more states adopting privacy regulations, state violations.

4. Administrative Proceedings vis-à-vis Privacy-Related Regulatory Violations

There are many federal privacy regulations that range from protecting children to consumers from things like spam. On the state level, many states have enacted privacy-related regulations, and more are jumping on this bandwagon every day. As of the writing of this article, President Biden has issued an executive order that includes a request for enactment of a federal regulation as to artificial intelligence (AI) and privacy. Each statute provides its own regulatory process, including how violations are to be handled. Negotiation of the fine or penalty that may be imposed and/or actions that will be taken to "fix" the non-conforming situation for the future is certainly something to consider. An ADR process can be helpful in this regard.

5. Insurance Coverage Disputes

These often arise in data breach, privacy, and cyber cases. Not every company carries cyber insurance or other types of insurance that would provide coverage for its insured's liability arising out of cyber incidents and data breaches. Every policy will have terms and conditions required for coverage to apply. It may be that conditions were not complied with. Maybe the IT department was never even advised of the insurance conditions. That said, whether a particular policy of insurance applies to provide coverage for the loss at hand will be determined by the facts of the loss and the terms and conditions of the policies. It may be that more than one policy provides coverage. If so, is one primary to the other? Is there allocation between the policies that needs to be done? Oftentimes the parties will have insurance coverage attorneys attend and participate in mediation because the availability, or not, of insurance proceeds is crucial to there being a source of funding for a settlement. Alternatively, insurer vs. Insurer disputes may arise after the underlying claim has been resolved, presenting in the form of subrogation, contribution, or indemnification claims. Generally, insurers will want to resolve differences between themselves sooner than later. That said, each policy is unique, and each loss is unique. Hence, mediation is most helpful in these claims.

6. Directors & Officers and Professional Liability

D&O issues arise when a Board of Directors (BOD) has allegedly perhaps not paid sufficient attention to the company's cyber needs and/or exposures. Insurance brokers and agents, lawyers and other professionals may face exposure in this area for not procuring the appropriate insurance. Lawyers and other professionals can be at risk for not properly maintaining their files and records. Most professional liability policies specifically exclude cyber related claims at this point, but again, each claim is unique, and it will turn on the facts of the situation as to whether there might also be a professional liability claim.

Benefits of, and Best Practices for, Using ADR to Resolve these Types of Disputes

The landscape of cybersecurity is continually evolving, introducing new threats and regulatory frameworks. Lawyers involved in mediating and arbitrating cybersecurity cases must remain vigilant and adaptive, staying abreast of emerging trends,

technologies, and legal precedents. This proactive approach enables practitioners to effectively advocate for their clients in a rapidly changing environment.

In a nutshell, ADR procedures allow the parties an opportunity to come together early in the dispute, to be able to speak candidly and share documents, and to negotiate an early resolution that will let them get back to their lives and the business of the business. Litigation is costly and takes years. Arbitration is less costly and is generally a more expedited process than litigation. Mediation is at the cornerstone of any dispute and able to resolve the dispute with even less cost and in less time. Conflicts in the world of cyber and privacy are very personal, and it is in everyone's best interests to find the common ground that can resolve the dispute as early as possible.