PARR BROWN GEE & LOVELESS
ATTORNEYS AT LAW

BRADEN W. JOHNSON
ATTORNEY AT LAW
bjohnson@parrbrown.com

February 24, 2020

A Lawyer Walks into a Dataroom: Getting the most from your Dealsite

---

There's no way to avoid it: Corporate transactions require the sharing of documents and information. For prior generations of lawyers, this *sharing* could involve creating a "dataroom" – a physical space somewhere on the globe filled with items for disclosure. Parties would pilgrimage to these datarooms to perform due diligence for the transaction. When inside the dataroom, cameras and photocopies were typically banned, marking or highlighting documents was a serious offense, and cell-phones (to the extent they existed) were usually forbidden. Some dataroom parties were even asked to consent to a search or metal detector scan in order to enter or leave the dataroom.

Fast-forward to the present day where the cloud is more than just a weather phenomenon and virtual dealsites like Intralinks, Ansarada, Firmex, ShareVault, SecureDocs, and Merrill Dealsite are common. With these advances, the typical dataroom structure has shifted from a physical space to a virtual document repository. These virtual datarooms (also called "dealsites") allow for instantaneous sharing among unlimited users and without the limitations of time or location. And these virtual datarooms often include powerful organizational, analytical and safety tools that would be impossible for physical datarooms.

When properly utilized, virtual datarooms provide greater convenience, efficiency, and security than physical datarooms. But, to avoid the fate of the proverbial lawyer who walked into a bar after failing to duck, attorneys should be thoughtful and deliberate when walking (or, more likely, logging) into a virtual dataroom. The following tips can help:

Use a Document Index Strategy when Creating or Accessing a Dataroom:

When logging into a dataroom, the user is typically greeted by a list of file folders with names like "*Organizational Documents*" or "*Financials*". Clicking on these root folders allows access to subfolders and, eventually, a collection of digital files. The specific folder structure will vary based on the subject matter of the transaction. But, if structured in an intuitive way, the list of folders and subfolders can become the functional equivalent of a table of contents outlining the structure of the dataroom.

Given the importance of the folder structure, users should avoid folder names with overlapping subject matter like "*Environmental*" and "*Phase I Reports*". To this end, a folder named "*No Relevant Category*" is more descriptive than the typical "*Miscellaneous*" folder (which folder often degrades into a random collection of new, unusual, or irrelevant items anyway). Rather than deleting items from the dataroom, a "*Delete*" folder allows the user to quickly re-categorize these items in the future as needed. Such a delete folder also keeps a record of potential deletions, whereas deleting the file typically removes any record that the document ever existed. For the same reasons, a "*Duplicates*" folder is often better than deleting perceived duplicated uploads.

Using sequential numbers at the beginning of each named folder and subfolder can also be helpful. First, it allows the user to determine the order in which the folders are shown so long as they are sorted in alphanumeric order. For example, naming a folder "*3. Intellectual Property*" will typically be listed before a folder called "*4. Tax*". And second, when identifying a document's location within the dataroom, numbered folders allow the user to share a numeric folder address (e.g. 1.7.4) rather than a long string of folder and subfolder names.

Considering document index strategy is also helpful when reviewing a dataroom prepared by a third party. Rather than frivolously searching for document names or aimlessly scrolling through all folders, the user can direct the document search based on the folder index. The folder index can also help an experienced user determine what categories of information may be missing. This can lead to helpful requests like: "I saw the folder for Leased Real Property; is there any owned real property that should be disclosed?"

Leverage the Automatic and Analytic Features:

Keep in mind that all datarooms are not created equal. There are several free web applications that allow document sharing, but they lack some of the important functionality and security features offered by the more powerful dataroom tools. Thus, depending on the specific needs of the transaction, users should consider whether it is appropriate to suggest a different dataroom tool.

Notwithstanding the variations between dataroom providers, nearly all datarooms track the date, time, and author of each uploaded document. This feature makes it unnecessary to include names and dates as part of the filename. For example, "*1-28-2020-BWJ.Prepared-Purchase.Agreement.docx*" can be titled simply "*Purchase-Agreement.docx*" without losing any identifying information. Some datarooms also track who has opened a document or, conversely, which documents have not been viewed by a given user. Sorting documents by date, author, or viewed status can help a user identify what diligence items still need to be reviewed.

Rather than just sorting documents according to certain variables, some datarooms can create reports and export lists of documents fitting certain criteria. For example, the user can run a report to identify all unopened documents, all documents uploaded by certain user, or even all documents uploaded after the user's last log-in to the dataroom. These reports and lists can be used as a diligence summary, an informal checklist, an agenda for a conference call, and much more. And further, these reports and lists can prevent the inefficient practices of scrolling through the entire dataroom looking for specific document types.

Some of the more powerful datarooms can compile usage statistics and prepare visual depictions as to the activity level for specific users or documents. This can give the dataroom owner some insight as to what documents are particularly concerning to the parties in the transaction. When a user is shown as not regularly accessing the dataroom, the dataroom owner may consider cutting off access for that person to limit the number of parties who have access to sensitive data. Or, at a minimum, the dataroom owner may infer (rightly or wrongly) that users who rarely access the dataroom are less interested in completing the transaction.

Finally, some datarooms allow for multiple versions of the same document to be uploaded. This allows users to upload negotiated changes to a transaction document without saving wholly separate versions each time. This keeps the folders organized and focuses the user's attention on the newest version of a given document. But notwithstanding this, the text of prior versions is still available within the dataroom as needed.

Pay Attention to Security Features:

Most datarooms have nuanced access rules that can be changed at any time. This allows dataroom owners to expand or limit access for certain individuals, and to stop access completely for parties that drop out of the transaction. In some cases, dataroom owners can set a date on which all permissions expire unless otherwise renewed. This feature is helpful when there are transaction-specific deadlines, after which access will probably need to change. Conversely, for documents that are meant to be circulated broadly, some datarooms allow anyone with the appropriate link to access the relevant document. That way, the dataroom owner can circulate multiple or large files without needing to create specific log-in credentials for every party who wishes to access certain non-confidential documents.

An increasing number of datarooms support two-factor authentication. This is primarily designed to confirm that the person accessing a dataroom is, in fact, the person who is authorized to do so. But it also provides benefits for users who lose their password or users who want push notifications with respect to new uploads. Moreover, two-factor authentication can be used to verify the location of the party trying to access the dataroom. For example, if a user's cellphone is in the United States but the log-in request comes from another country, access can be temporarily denied.

Some datarooms restrict certain documents from being downloaded, saved, or printed; rather, the document can only be viewed within the dataroom application. This can be particularly helpful in a transaction involving competitors, since it makes the information harder to store or duplicate. Other datarooms add an indelible watermark on certain highly sensitive items. The watermark can identify the name of the person who downloaded the document to create a paper trail for investigation and punishment of any misuse. The watermark can also make it more difficult to edit or digitize a sensitive document, or to infringe upon a copyrighted image.

Speak Up about Risk Issues and Mitigation Strategies:

Anyone with the proper credentials can examine files posted within a dataroom. But attorneys have an additional responsibility to advise clients about the relevant legal risks and mitigation strategies. For example, allowing a third-party to download information from a dataroom confers a vague possessory right. And, absent a contract defining this possessory right, the dataroom owner may struggle to terminate the right, limit the way the information can be shared, or require the return of the information. This risk is commonly mitigated by a contract between the parties, whether in the form of a non-disclosure agreement or a terms of use agreement. Building these provisions into the underlying transaction documents is not recommended, since the provisions wouldn't be applicable unless and until the transaction concludes.

There are other ways to mitigate the risk of unauthorized disclosure of information found in a dataroom. For example, attorneys can advise dataroom owners to closely monitor the security permissions for the dataroom. Additionally, attorneys can suggest dataroom providers who log information as to who accesses or edits documents. At a minimum, this can help the dataroom owner unwind situations where a file is inadvertently changed or deleted. But it can also help the dataroom owner understand who is accessing the information, when, and – potentially – why.

Clients will also need advice as to how the underlying transaction documents affect a dataroom. For example, the transaction documents typically set the boundaries for what categories of documents must be shared. In the absence of either a provision requiring a company to disclose something or a specific disclosure request, it is unlikely that the company will want to share it. Or, in M&A transactions, a so-called "anti-sandbagging provision" may stop a buyer from recovering on false representations and warranties from the seller if the problematic information was disclosed by the seller in the dataroom. In theory, this could allow a seller involved in litigation to make a representation that there are no active lawsuits, but avoid a claim from the buyer that the seller breached its representation so long as the seller uploads the relevant lawsuit documents in the dataroom sometime before closing. Lawyers who limit their role to simply perusing the dataroom miss huge opportunities to serve their clients.

Finally, datarooms come with typical tech-related risks like viruses, ransomware, and data breaches. To mitigate these risks, some datarooms have special features like automatic virus scanning, the aforementioned two-factor authentication, strict password requirements, and more. Bigger and more powerful dataroom providers often have an edge here, but some dataroom providers take security more seriously than others. Attorneys should consider involving their IT department or other data security resources to evaluate the strengths and weaknesses of a given dataroom.

Final Thoughts:

Virtual datarooms have created a tectonic shift in the due diligence process for commercial transactions. But rather than basking in the convenience of virtual datarooms, attorneys should focus on mitigating risk and leveraging their powerful built-in features. This can add significant value for clients, while streamlining the due diligence process for all parties.