

Ironclad Security

Five Keys to Ironclad Security in Your M&A Transactions

Keeping security front and center
when using a virtual data room





Contents

The importance of data security	3
Navigating VDR choices	3
Key 1: Security-based business model	4
Key 2: Multi-layered data security	5
Key 3: Seller-based security controls	5
Key 4: Secure viewer and interface	6
Key 5: Security verification	6
Highest VDR security in the industry	7
A Merrill DataSite™ for your company	7

Introduction

Of all the critical elements that make up a successful deal, security is the one component that allows no room for error.

The importance of data security

M&A transactions are characterized by a series of complex, detailed activities that must be carefully orchestrated in order to achieve success. Sellers need to engage as many qualified buyers as possible to drive the best valuation for the deal. At the same time, they must prepare for a due diligence review. Large volumes of strategic information must be gathered and made available in a responsive, collaborative manner. A confidential due diligence environment must be established, and all of these activities need to be handled skillfully, so that the seller is ready to strike when market conditions are favorable.

Inadequate levels of security can have disastrous consequences and companies need to ensure that their sensitive business information is well protected. The loss of confidential information can harm a company financially, damage its reputation and result in a lack of trust that disrupts the transaction. Of all the critical elements that make up a successful deal, security is the one component that allows no room for error.

For years, the solution to this dilemma has been to set up a physical data room, monitored by a security staff, where investors spend hours, one group at a time, poring over the information. This process, although tedious, was a seller's best bet for addressing the need for document security while allowing potential investors to conduct due diligence. However, even the tightest physical security measures can fail. Documents can be misplaced, damaged or even hidden or stolen by unscrupulous individuals.

Recently, technology, in the form of the online virtual data room (VDR), has emerged as a solution. Virtual data rooms or datasites take the concept of the physical data room and make the information available in a secure electronic environment. Professionally installed online security measures have proven more effective than physical measures, and in the past five years, VDR technology has become the norm in the M&A marketplace for transactions of all sizes.

However, as with any technology, not all VDR solutions are alike. What is the best way to keep information safe and secure? What factors should be considered? You do not have to be an information technology specialist to make the right choice – as long as you keep a few key requirements in mind as you're reviewing your options.

Navigating VDR choices

Some companies, unfamiliar with VDR or datasite technology, often cite security concerns as a main reason for not adopting a virtual data room. This may be because online security measures are harder to see and touch – they are certainly less visible than security measures in the physical world. Virtual security, if professionally installed, is often far more effective than anything available in the physical world. Indeed, it is one of the main reasons for setting up the room in the first place.

Just as home security involves looking at door locks, windows and alarm systems, M&A security requires an integrated approach. The following five keys to security must be in place for the highest level of data protection:

1. Security-based business model
2. Multi-layered data security
3. Seller-based security controls
4. Secure viewer and interface
5. Security verification



Security considerations must factor into the chain of custody of documents during the datasite set-up to ensure that the chain of custody is intact at all times.

Key 1: Security-based business model

Vendors that focus exclusively on M&A activities are security experts. They have security embedded throughout the development, deployment and termination of the datasite. Work with an expert VDR consulting team that knows the industry, its security needs and due diligence requirements.

The VDR solution must provide a range of security and access choices during set-up, including flexible system tools and a responsive staff who can assist at any time if a security or control issue arises. Project managers should be available 24 hours a day to handle all aspects of setting up the VDR, including onsite deployment with prompt data uploading, applying desired access control and addressing vital security concerns.

Data acquisition and setup considerations

The documentation residing in the virtual data room must be protected from the start as it is highly sensitive and often strategic in nature. Security considerations must factor into the chain of custody of documents during the datasite setup.

Some clients may choose to control the entire chain of custody themselves, using internal staff to scan and upload documents and administer the site. If this is the case, the user should look for the vendor that can provide comprehensive training and adequate levels of security. Other clients may rely on the vendor to scan and upload documents to the datasite. If this is the case, it is important to find out if the vendor outsources any aspects of the process, since doing so introduces a potential break in the chain of custody of information and thus a breach in security.

The ideal solution is to choose a vendor that manages the entire process with its own staff and equipment. This is the best way to ensure that the chain of custody is intact at all times. The entire process of capturing paper or electronic documents, from the project management process to the actual server hosting of the client's documents, should all be handled by the vendor's staff, using the vendor's equipment.

In addition to choosing how you want to manage the set up process, you can also choose how involved you want to be in managing the datasite once it is "live." Some sellers rely on the VDR vendor to administer and maintain the site for them; others take a more hands-on approach in which they are given the necessary tools to handle much of the process themselves.

In such cases, a VDR provider should have the flexibility to customize the level of control and administrative access to meet the seller's needs. However, the VDR provider must also be available at a moment's notice to step in and address security issues throughout the life of the datasite. For example, if you accidentally give document access to the wrong person or group of people, the VDR provider must be able to instantly step in, assess and interpret the data, and provide the client with a detailed report of which pages of documents were viewed, by whom, and then swiftly adjust the access controls to correct the situation.

Key 2: Multi-layered data security

Data security is at the heart of ensuring that the due diligence portion of an M&A transaction remains confidential. While the specific terminology can be technical, the two key concepts are simple:

- **Multiple layers multiply the protection.** Safeguarding data requires multiple layers of software and hardware protection around sensitive information. No single feature should be relied on as a defense against a breach of security.
- **Page-level security.** VDR providers must have the ability to audit users' current document-level rights in order to provide the highest level of protection possible.

For the highest security levels possible, virtual data room security features should at least include the following:

- Strong username and password control to prevent unauthorized users from gaining access
- End-to-end encryption using Secure Sockets Layer (SSL) protocol
- Deterrence features, such as watermarking all documents on the computer screen to prevent photographing or printing of sensitive data

Key 3: Seller-based security controls

When it's your data, you know best how it should be viewed and accessed. That's why the best VDR solutions give the seller control over who can view and print information. Not only does this provide actionable information to help optimize deal-making, but it also ensures that only authorized parties are looking at your documents.

Seller-based security controls allow you to set usage permissions based on job title, level or department; so, for example, the accounting team can only access the files they need to see. Even if an individual user has access to view certain documents, he or she may not be given permission to print, allowing for more specific, detailed control.

Just as circumstances can change in an instant during the M&A process, usage permissions must have the flexibility to be changed as needed. For example, best-in-class VDRs provide real-time reporting regarding exactly who has viewed documents, when and for how long, as well as which documents have been printed, down to the page level. If it becomes apparent that a supposed suitor is simply trolling for competitive data, a VDR should allow for the swift disablement of that user's access.

The VDR provider should allow you to:

- Control who is allowed to view data
- Control who is allowed to print data
- Assign users to groups with common access settings
- Terminate access for any user or group in real time
- Report exactly who is viewing what content, when and for how long – in real time

When it's your data, you know best how it should be viewed and accessed. The best VDR solutions give the seller control over who can view and print information.



Key 4: Secure viewer and interface

Not all viewers are the same. Some require that you install additional software, some request that you deactivate ActiveX controls as a security measure and some allow users broad ability to download documents beyond the seller's control. The optimal solution:

- **Offers not only the most secure viewer but one that is the most convenient to use.** The optimal solution should not require installation or rely on plug-ins on the user's computer. Plug-ins create a security hassle since many companies restrict the download and installation of these types of programs by employees onto their desktops. Instead, choose a solution with a viewer based on a secure, no-installation-required, Java applet.
- **Aggressively manages the downloading of data and prevents it from being stored on a user's computer after he or she logs off the virtual data room.** Some VDR solutions recommend or suggest that bidders manually clear their computer cache, but this is unenforceable by the seller. For best security practices, choose a VDR solution that does not use viewer systems that allow the pages to be cached on a Web browser.
- **Is fully encrypted from the Web site to the workstation.** Once pages are closed or printed, the VDR viewer should clean up any traces they may have left on the desktop.
- **Retrieves only one page at a time.** This is called page-level viewing and limits the amount of data on a desktop at any given time for better security.

Key 5: Security verification

Cross-border transactions demand international verification

The growth within M&As is focused on international transactions, which demand the speed of closing the deal, access to more bidders and a streamlined buying experience offered by datasites. VDRs are a more efficient and cost-effective approach to making thousands of pages of data available to viewers over a wide variety of geographic and political borders. Yet, international privacy and security standards are higher, particularly for firms looking to do business in the European market.

International transactions demand an international standard. The highest internationally recognized review is the **ISO 27001 certification**, a stringent security standard. This involves an initial analysis of security protocols and follow-up auditing and testing to ensure practices evolve to meet new threats. ISO 27001 certified VDR providers are also required to have an approved security plan in place that ensures data will be protected, data storage facilities are protected and VDR employees are background checked.

Additional security verification measures

Ensuring data security also requires that the VDR provider should continually test their system and have it reviewed by outside experts to provide objective verification of the system. Routine tests performed by a VDR provider must include monthly vulnerability scanning and penetration testing, or so-called "ethical hacking."

How secure are the VDR provider's solution and services? Don't simply take the VDR provider's word on their level of security – demand certification by respected third parties to ensure peace of mind, and bear in mind that not all certifications are alike.

International transactions demand an international standard. The highest internationally recognized review is the ISO 27001 certification, a stringent security standard.

Merrill DataSite is currently the only VDR provider in the industry to earn ISO 27001 certification, the most highly recognized security certification.

Highest VDR security in the industry

Merrill DataSite™ is the leading global provider of turnkey VDR solutions. We combine the industry's leading technology with highly secure technical and operational environments, and a professional staff dedicated to customer success. Merrill DataSite has hosted virtual data rooms for thousands of clients, representing transactions totaling trillions of dollars in asset value.

Merrill DataSite is currently the only VDR provider in the industry to earn ISO 27001 certification, the most highly recognized security certification.

Merrill DataSite ensures the security of client information by:

- Supplying dedicated project managers 24/7 to assist with security needs
- Offering turnkey options for complete service or “do it yourself” options for sellers who need to minimize exposure of sensitive documents
- Utilizing only in-house staff and equipment to ensure the chain of custody
- Providing layered security down to the page level for maximum security
- Tightly controlling access for viewing or printing information based on seller preferences
- Ensuring sensitive information is accessed one page at a time and leaves no trace on the bidder's computer after log-out
- Verifying security through ongoing testing and meeting the highest international standards for data security and data privacy

A Merrill DataSite for your company

With systems capable of getting the datasite up and running within two hours, setting up a Merrill DataSite for your company can be accomplished rapidly. Our team can scan, upload and organize thousands of pages of content from any source in 24 hours or less. We are ready to answer any questions you may have and make your M&A process as secure, efficient and successful as possible.

To learn more about how Merrill DataSite can transform your next transaction, call your Merrill representative today or visit us at www.merrillcorp.com/datasite.



About Merrill DataSite

Merrill DataSite™ is a comprehensive virtual data room (VDR) solution that accelerates the due diligence process by providing a secure online document repository for confidential time-sensitive documents. Merrill DataSite overcomes the many limitations of a traditional paper data room by enabling companies to maintain and share critical business information in a secure online environment, streamlining all stages of the document and communications process. Accessible via the Internet, Merrill DataSite dramatically reduces transaction time and expense by allowing prospective buyers to participate concurrently in the due diligence process.

Merrill DataSite is designed for rapid deployment and can be up and running in two hours or less. Every aspect of the process, from document scanning to VDR hosting and project management is delivered by Merrill's multilingual staff, available 24 hours a day worldwide. Currently, Merrill DataSite is the industry's only ISO 27001 certified VDR solution, providing assurance that the most stringent security standards for business transactions are followed.

As a leading provider of VDR solutions worldwide, Merrill DataSite has empowered more than 500,000 unique visitors to perform electronic due diligence on thousands of transactions totaling trillions of dollars in asset value.

About Merrill Corporation

Founded in 1968 and headquartered in St. Paul, Minn., Merrill Corporation is a leading provider of outsourcing solutions for complex business communication and information management. Merrill's services include document and data management, litigation support, branded communication programs, fulfillment, imaging and printing. Merrill's target markets include the legal, financial services, insurance and real estate industries. With more than 6,300 people in over 70 domestic and 15 international locations, Merrill empowers the communications of the world's leading companies.

Merrill Corporation

225 Varick Street
New York, NY 10014
866.399.3770

Corporate Headquarters

One Merrill Circle
St. Paul, MN 55108
800.688.4400

*Offices in major cities
throughout the world*

www.merrillcorp.com/datasite

©Merrill Communications LLC. All rights reserved. MD0108_1

