brainloop

WHITEPAPER

# Protecting Sensitive Information in Life Sciences Organizations:
## Top Three Misconceptions that Put Companies at Risk


Executive Summary »

Critical business processes in biotech and pharmaceutical companies involve highly confidential, important documents that need to be safely accessed by external partners and potential licensees. Poor security measures based on a "traditional" view of data security have lead to high-profile, significant security breaches.

The technology implemented to ensure security in this new era of business must change. What's needed is a shift in the way business users think about security. Putting confidential information outside the firewall is actually safer and more expedient for all parties involved. Fortunately, there are solutions today that understand this new paradigm and are providing new ways to conduct important business securely without being impeded by IT complexity.

Whitepaper

# Protecting Sensitive Information In Life Sciences Organizations: Top Three Misconceptions that Put Companies at Risk

## Introduction

It's no secret: More than any other industry, life sciences depends on intellectual property (IP). A company's IP is generated through the investment of hundreds of millions of dollars and years of development. One or two drugs may represent the entire future earnings stream for a biotech start-up, and even pharmaceutical companies with a large number of products attribute a significant proportion of their revenues to a relatively small handful of drugs.

Because of the tremendous value of their IP, as well as the large amounts of clinical trial information they generate, biotech and pharmaceutical companies face security risks far greater than those in other industries. Several business processes expose life sciences companies to potential loss of IP or breach of clinical trial data, and require strict security measures:

- **Drug and technology licensing:** Biotech firms share their discovery and clinical trial information with a number of potential licensees in a controlled manner, and retract it from unselected partners once the licensee is selected.
- **Research and development:** Increasing complexity in drug development is driving drug research companies to outsource specialized functions to a network of contract research organizations. In addition to accessing confidential information, these vendors must be able to provide, update and modify clinical trial plans, data and analyses securely.
- **Alliance management:** When biotech firms and licensees both have a financial interest in a drug's approval and commercialization, both parties must work closely to coordinate development and measure progress against defined milestones. Partners must have complete access to shared IP, and must be able to document each partner's changes to the information. Additionally, communication processes that accelerate development, such as document forwarding and online discussions, need to be secured.

security breaches in the news:

A new Silicon Valley start-up recently raised about $30 million in three rounds of venture funding after receiving a valuation of $150 million. Unfortunately, the company's VP of sales mistakenly leaked the company's sales spreadsheet. In a matter of hours, screenshots of the start-up's sales figures were available to anyone and everyone on the web.

Or how about the 2007 – 2008 streak of security breaches in the pharmaceutical industry? Two companies suffered four high-profile breaches exposing information on more than 70,000 employees and former employees, while another company reported the theft of two laptops containing more than 68,000 patient records.

- **Regulatory reporting:** Regulatory staff members, often in conjunction with outside consultants, need to organize and streamline the filing process in a secure environment. Project members preparing presentations and application materials require versioning support, commenting, and the ability to lock documents when the final version is complete.

Because of the massive capital investment at stake, many companies still use non-electronic means of sharing data in these processes, resulting in expensive information-sharing costs, gross inefficiencies, the inability to share documents in parallel with multiple partners, and increased exposure to risk.

The press offers a wealth of evidence that ensuring confidentiality and control over business-sensitive data is no easy task. Why? Because business is moving faster than ever, and sensitive documents are being shared in ways that executives can no longer assume are protected by traditional IT measures.

This white paper will discuss the enormous cost of security breaches, the risks end users introduce through common business practices, and misconceptions that exacerbate the problem of protecting a company's most important and confidential information. It will look at traditional IT approaches and reveal why they are no longer adequate. It will suggest a change in how companies view security, and explore new technologies that meet the needs of the new enterprise.

case study:
Drug Licensing

challenge:
A drug research firm needed a way to share highly confidential research information, including clinical trial data on a new drug with pharmaceutical firms interested in licensing the drug. Protecting their IP, while expediting the process, was paramount.

solution:
This firm designated a secure virtual data room as the central repository for all facets of the drug review stage and licensing documents. They controlled access to all documents, and placed further restrictions on the most sensitive ones to prevent them from being downloaded, saved, forwarded or printed without authorization. An audit trail captured all accesses for each document, so the firm was able to easily measure interest level by reviewing which pharmaceutical companies were accessing the documents. This approach allowed the firm to secure a profitable partnership, while protecting IP and expediting the review and agreement process.

## Confidential Documents in the Wrong Hands: What It Costs, Why It Matters

Confidential documents can fall into the wrong hands in a variety of ways. Intentional data theft from either inside or outside the company is an all-too-frequent occurrence. Unintentional breaches happen as well, due to poor security measures, human error, or both. The imperative of "getting the job done" compels individuals to forward business-sensitive information, whether or not airtight security measures are in place. Regardless, the costs associated with data security breaches can be enormous.

## Hard and Soft Costs

According to the US Chamber of Commerce, IP theft results in a loss of $200 - $250 billion a year for US companies and represents a loss of 750,000 jobs[1]. Forrester Research recently estimated the cost per record for security breaches at $90 to $305, meaning that the *total cost of a single breach may run into millions or even billions of dollars.*[2] The research firm surveyed 28 companies that had recent data breaches. Hard costs cited included outside legal fees, notification costs, response costs and lost employee productivity. Other significant hard costs Forrester warned of that were not part of the estimate included regulatory fines and additional security and audit costs.

There are significant non-quantifiable costs to a company whenever a data breach occurs, including inadvertent disclosure of key assets, decrease in investor value, unfavorable press, and more. These costs can be even more detrimental than hard costs, given their implications, and can eventually run into the tens of millions of dollars.

## The Cost of Non-Compliance

Life sciences companies are required to meet stringent documentation and compliance requirements, or pay a high price. Regulations such as electronic access to patient information (HIPAA) and the newly amended E-Discovery rules (Rule 26 of the Federal Rules of Civil Procedure) underscore the fact that airtight data security is critical in today's highly regulated business environment. Moreover, as is the case with all industries, life sciences companies that are subject to regulations such as the Sarbanes-Oxley Act (SOX) now require a fully documented information flow for critical corporate information, creating a need for tamper-proof and persistent audit trails.

case study:

Alliance Management

challenge:

A biotech firm had recently signed a drug licensing and collaboration agreement that included substantial payments for clinical and regulatory milestones and for achieving sales targets. The biotech needed to manage information exchange as the two companies worked together to complete development and commercialization of the product.

solution:

The firm had used a secure virtual data room to conduct the initial transaction, and used their familiarity with virtual data rooms to set up a secure online work space for collaboration. Employees from both companies, as well as outside suppliers and consultants, can access the work space from any location, at any time. Fine-grained access controls allow each employee to access only the relevant information. Participants can safely send document links to each other, so they enjoy ease of communication without the risk of their documents being accessed without authorization. The result: Seamless collaboration in a secure environment.

## Protection of Confidential Documents: More Critical Than Ever

Developing and bringing drugs to market is becoming more complex over time. The late 1990s and early 2000s saw the rise of contract research organizations as pharmaceutical companies outsourced processes to achieve increased efficiency and competitiveness. Many different outside organizations may be used in the development of a single drug to manage preclinical and clinical trials, provide monitoring, toxicology and lab services, and prepare the New Drug Application (NDA) or Biologic License Application (BLA). The economic turbulence of 2008 accelerated the trend among pharmaceutical companies toward an alliance orientation, with particular emphasis on acquiring companies with expertise in large molecule research, as evidenced by Pfizer's recent acquisition of Wyeth, with its focus on biologicals and vaccines.

Leading industry analyst firm Gartner refers to groups of individuals who collaborate together outside the corporate boundaries as "communities of trust." According to Gartner, there is a rapidly growing need for ways to *"meet the communications and security needs for the ongoing sharing of sensitive data across the Internet between multiple organizations."*[3]

This trend will continue to grow as more and more collaboration occurs among innovation networks around the globe. These processes need to be secure; additionally, they can't be impeded by an unwieldy IT security infrastructure that slows down the job that needs to be done.

### case study:

Regulatory Filing

### challenge:

A drug research firm with a pipeline of several drugs hired a consulting firm to help prepare for its upcoming filings. The consulting firm needed access to highly confidential, rapidly changing information to create the company's presentations. Protecting the company's confidential information, as well as tracking the changes to the evolving application materials, was crucial to optimizing the application process.

### solution:

The company set up a secure online work space to give the consultants 24/7 access to application materials and documentation for each of the candidate drugs. They controlled access to the documents to ensure that only authorized employees would be able to view or modify them, and to prevent unauthorized forwarding and printing. Versioning and an integrated audit trail inform users from both companies of changes to the materials and allow them to roll back to a previous version if necessary. The result: A secure collaboration procedure that allows the company to leverage the consulting firm's expertise while accelerating application preparation.

## Common Misconceptions about Data Security

Protecting confidential information in today's dispersed environment is a much more daunting task than it was in the past. Part of the problem is the prevalence of commonly held ideas about data security that simply are not true. Below are three of the most common misconceptions that jeopardize organizations' implementation of truly secure solutions:

## Misconception #1: Data Security is IT's Problem

Most biotech and pharmaceutical executives want to know that confidential documents are protected without having to worry about the mechanism by which this is achieved. As a result, data security is delegated to IT. But this "hands-off" approach can lead to a number of problems.

First, IT departments are primarily concerned with security from an infrastructure perspective, producing solutions that focus primarily on internal employee desktops and exclude external partners. They may build a company-wide solution for every desktop, which is not necessary and can take years to develop. Or, on the other extreme, an IT solution may not be good enough, and have its own security loopholes.

Additionally, these infrastructure solutions may not focus on the end-user experience. IT departments may spend significant time and resources devising a solution that is cumbersome for end users; for example, they may implement encrypted email or encrypted hard disks, diminishing employee productivity while doing nothing to protect documents once they have been sent to external partners.

In short, users themselves need to find a way to conduct confidential business that is efficient, includes outside approved participants, and meets stringent security requirements without being at the mercy of a cumbersome IT infrastructure. **Because executives are held accountable for security breaches, security must be a management concern.**

## Misconception #2: If it's Behind the Firewall, it's Safe

Highly confidential documents are in fact more vulnerable *behind* the firewall than outside. Why? Because there are so many individuals behind a company firewall who could gain inappropriate access.

Perpetrators of data security breaches are often disgruntled employees, "super users" with high access permissions, or individuals who have left the organization, but whose access privileges have not been updated.

The firewall does not take into account the selectiveness and breadth of individuals in collaboration-heavy business processes. Only a select few individuals should have access to sensitive documents. For this reason, file servers, document management systems, and email are vulnerable repositories for storing and managing confidential documents.

The best and safest solution is one that seamlessly connects authorized users on *both* sides of the firewall while preventing unauthorized access by individuals both inside and outside your organization.

## Misconception #3: Traditional Security Measures are Good Enough

Biotech professionals who are tasked with important, deadline-driven projects generally trust that the security measures in place are enough to protect the documents they are working with. However, as stated above, some IT security measures are not in fact bullet proof. It is dangerous to assume that any data security measure is better than nothing. The reality is that *partial security equals essentially no security.*

For example, the practice of sending emails with a disclaimer is widespread, and yet completely unsecure; the disclaimer does absolutely nothing to "protect" the security of the data or email attachments from unauthorized access. It's equivalent to putting a sign on your wallet that says "If you're a pickpocket, please don't steal this" before getting on a crowded train.

Another example of partial security is encrypted emails, whose information and attachments are only truly "safe" while encrypted. Once they are unencrypted at the desktop, they are vulnerable. Hard-disk encryption also only solves part of the problem, because it only protects information "at rest." Once documents are in transit, whether from one laptop to another or from one person to another, the information is vulnerable since the encryption does not travel with the document.

## A New Security Model

These misconceptions illustrate the need for a major transformation in the way businesses view data security. Traditional approaches to data security like firewalls and encrypting data on the server or in email are insufficient. They assume that highly confidential business information remains in a tightly controlled, definable environment. That assumption is false. The reality is this: In order to be fully utilized, information must be shared. Therefore, data protection has to be attached to the document itself and it has to follow the document wherever it goes. This is known as *persistent document security.*

The new model sees important documents as safer when placed in a repository outside the firewall, a place that is highly secure, accessible anytime, anywhere by a select number of individuals, and allows users to easily control exactly what documents are viewed, accessed, and updated. In this paradigm, documents are stored on a highly protected, encrypted server outside the firewall. Workflows are managed by authorized end users, rather than by IT, so that sensitive documents are shielded from internal or external IT personnel. Documents can only be accessed via strong authentication methods that ensure only authorized access, and a complete audit trail captures all activity. Access rights can be easily managed at a group level or down to an individual level. With these measures in place, business users can freely collaborate and share information, knowing their documents remain secure in the repository.

## Best-Practice Data Security Strategies

As important information moves farther and farther from the physical boundaries of the IT infrastructure, the technology required to keep that information secure becomes paramount.

According to Gartner, "The traditional security mechanisms provided by the operating system or network are just not suitable for meeting this need. However, effective solutions can be found in security technology that overlays the existing infrastructure, instead of being dependent on it."[3]

Network-based solutions to the problem of keeping electronic data secure, such as file servers and the corporate firewall, are inadequate for documents that must be shared with external partners. Traditional encryption measures are cumbersome for end users and can hinder collaborative business processes while providing security only to the point of unencryption.

Below is a brief synopsis of two strategies available today that solve the need to provide end-to-end data security for all confidential documents as they travel throughout the extended enterprise.

## Enterprise Rights Management Software

Enterprise rights management software (ERM) provides security that "travels" with the document, from the server to the desktop. Recipients can view or modify documents only as allowed. While ERM software is an important step in the direction of end-to-end data security, such a system by itself often requires proprietary software on both the server and the desktop, and can be a relatively expensive solution. It imposes a burden on users: Access privileges need to be assigned to each document individually. Also, by itself it does not allow "anywhere, anytime" access that would foster collaborative business processes.

Thus, ERM software addresses the security of moving documents better than does deploying only server and/or email encryption, but with greater use of resources and decreased user productivity.

The key to successful adoption of an ERM infrastructure within the extended enterprise, therefore, is to enable users both inside and outside the enterprise to benefit from such an infrastructure while minimizing the users' administrative burden.

## A Different Approach: Secure Online Work Spaces

Secure online work spaces, or virtual data rooms (VDRs) are web-enabled applications that operate outside of the corporate firewall, and enable document sharing with highly secure access and viewing controls without requiring proprietary server and client-side software. These online document vaults are offered as a web-based service, and so require no IT infrastructure; however, they can also be integrated with an ERM infrastructure to provide even greater functionality.

The most sophisticated of these secure work spaces offer the highest security standards, including two-factor authentication, encryption, and tamper-proof audit trails. Extremely important features to look for are operator shielding, in which software and operating processes ensure that the VDR operator is not able to read customer data, and end-to-end security, in which documents can be access-controlled even after delivery to users' desktops. VDRs combine these security functions with communications and administration tools that allow the end user to efficiently set access rights, organize workflow, and ensure complete control over everything that happens in the data room, from beginning to end.

A secure VDR provides a central repository for confidential documents located outside the IT infrastructure. It gives business executives control over highly sensitive documents, regardless of where documents "live," in a way that facilitates business rather than hinders it. VDRs are device-agnostic, so any authorized individual can enter the data room anytime, with any web-enabled device, wherever they are.

## Summary

Critical business processes in biotech and pharmaceutical companies involve highly confidential, important documents that need to be safely accessed by external partners and potential licensees. Poor security measures based on a "traditional" view of data security have lead to high-profile, significant security breaches.

Business will go on, with or without the proper controls. Documents will be shared, and the farther they move from the corporate boundaries the more imperative it becomes to keep them secure, wherever they reside. A company's most important information cannot be vulnerable; the cost in real dollars, non-compliance, and business risk is simply too high. Executives need to ensure that their most important data is not only secure, but also easily accessible by those individuals who need such access. Security cannot be achieved at the expense of business goals.

The technology implemented to ensure security in this new era of business must change. What's needed is a shift in the way business users think about security. Putting confidential information outside the firewall is actually safer and more expedient for all parties involved. Fortunately, there are solutions today that understand this new paradigm and are providing new ways to conduct important business securely without being impeded by IT complexity.

## About Brainloop

Brainloop, with offices in Boston and Munich, was founded in 2000 and is the leading provider for software solutions that enable the secure management of confidential documents across the extended enterprise. Brainloop Secure Dataroom is a hosted service for managing confidential documents and for enabling document sharing and collaboration for authorized users, while best-in-class security technology prevents any access by unauthorized users. Examples of application areas are biotech licensing, contract negotiations, project executions, generation of quarterly reports, and other communications that involve documents with sensitive and confidential information. Brainloop Secure Dataroom is used in hundreds of companies around the world.

For more information, or to request for a free trial, please visit the Brainloop website at www.brainloop.com.

1. US Patent and Trade Office, "Small business - FAQ - USPTO Stopfakes.gov"
2. Kark, Khalid; "Calculating The Cost of a Security Breach" (Forrester Research, April 2007)
3. Heiser, Jay; "The $10 Billion Market for Communities of Trust" (Gartner, January 2007)
4. Heiser, Jay (Ibid)