

DATA SECURITY IN AN OUTSOURCING ENVIRONMENT

A LexSphere Whitepaper

I. Abstract

In-house data is generally presumed to be safe: data entrusted to others is always a source of anxiety with respect to its security. This is not only natural but also justified in some ways. Even with comparable security practices at client and vendor premises, loss of co-location increases risk by adding the dimension of transportation. In addition to stored data there is now, also, data in transit that needs protection.

If, however, advantage is to be taken of the promise inherent in the model of outsourcing business processes to wherever they are done best, it becomes necessary to reconcile to the requirement of entrusting data - to a greater or lesser extent -- to others. What remains then is to select one's collaborators carefully, evolve the most secure architecture for a distributed data process, and bring to bear the optimum technology package.

Three principal models can be visualized in connection with data security in an outsourcing environment, namely:

Case 1: Main Database Hosted by the Client

Case 2: Main Database Hosted by LexSphere

Case 3: Main Database Hosted by Independent Data Center (IDC)

Each approach has its advantages and drawbacks, and the choice in a particular case will emerge by balancing the requirements of (a) desired security-level (b) criticality of throughput (c) economy (d) specialized training (e) etc. The advantages and disadvantages of each model are evaluated below.

2. Dimensions of Data Security

In an outsourcing environment data, in general, needs to be secured against three modes of loss:

- (a) Data theft
- (b) Disabling attacks
- (c) Accidental disasters

Data theft may have the purpose of causing dislocation through erasure, in which case it is detectable; or it may be industrial espionage, in which case it may remain undetected for long. It can take the form of copying data to removable media such as floppies, CD's, pendrives etc., and extend to electronic transfer via email or ftp.

Disabling attacks are typically mindless, broadbased, and without specific targets. They are carried out through viruses, worms, trojans, etc.

Accidental disasters are typified by fire, floods, and the like, which destroy the hardware on which data is stored.

The technologies involved in parrying these threats range from electronic surveillance, through firewalls and anti-virus software, to disaster recovery systems. They can be very complex at the high-end, requiring a high level of training for maintenance and system administration.

3. The Security Process

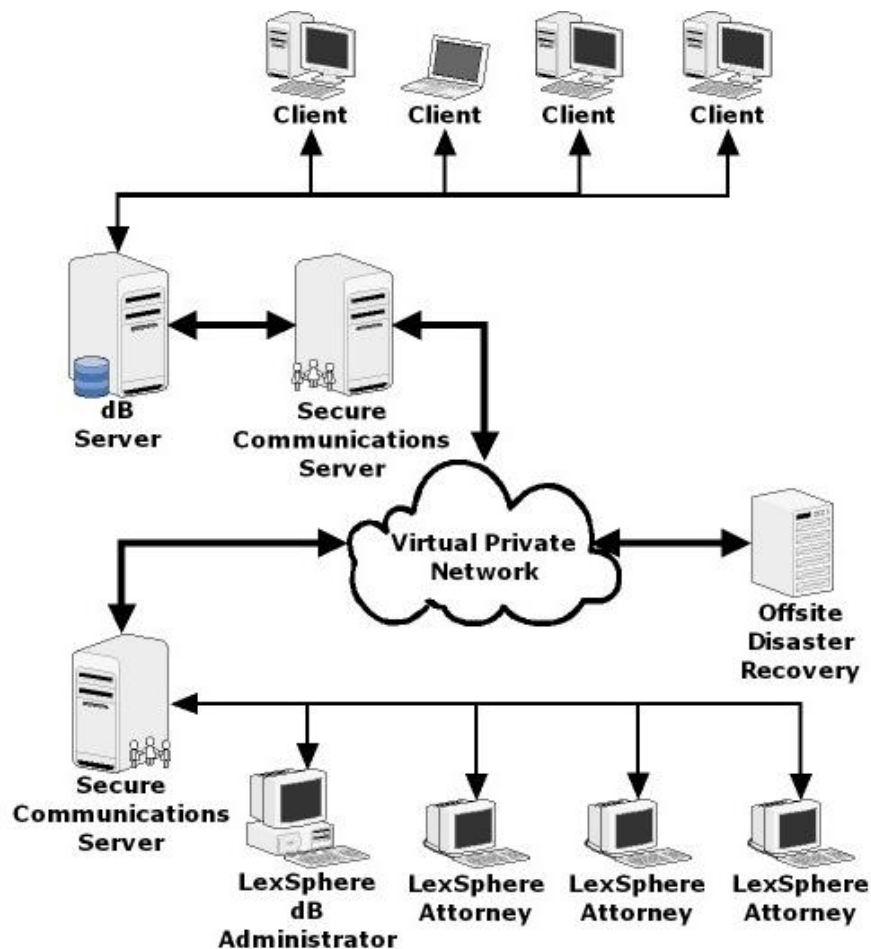
The process of constructing a security environment consists of the following steps:

- (a) Formulation of a Security Policy
- (b) Design of Security Architecture
- (c) Choice of Principal Technologies
- (d) Calculation of Principal Specs (incl telecom requirements)
- (e) Selection of Security Softwares
- (f) Selection of Security Hardwares
- (g) Selection of Telecom Service Provider
- (h) Selection of IDC for Hosting (possibly)
- (i) Selection of Principal Suppliers
- (j) Personnel Selection & Training
- (k) Institution of Periodic Review and Audit

While elaboration of these items is out of place in an outline note such as this, one topic may be profitably discussed due to its importance viz. the choice between Case 1, Case 2, and Case 3 as given in section 1. To begin with, a comprehensive security process may already be a part of the client's established workflow, with LexSphere being required to conform to it. In such an event, the choice between Cases 1, 2 and 3 would have been already made. On the other hand, if LexSphere is required to propose and design a new workflow, and related security process, *ab initio*, we must consider the relative characteristics of the three possibilities.

Database Hosting Models

Client Hosted - In some circumstances, a client may choose to take on the responsibility for hosting the database and allowing service providers like LexSphere to access the data via a virtual private network or leased line. Such a network can be portrayed as follows:

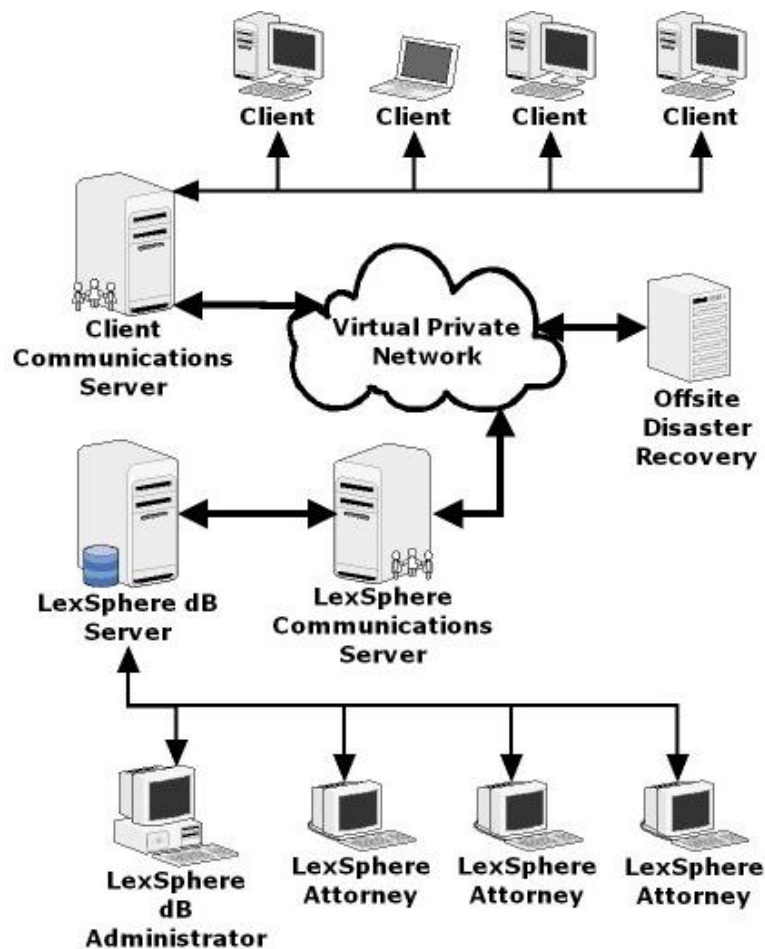


For the client, a Client Hosted Database may afford maximum comfort with regard to data security. This model may, in fact, be best for large companies with comprehensive IT strengths, who have established security procedures and trained manpower. Alternatively, onsite hosting may be mandated by the company's regulations.

The main disadvantage of this model is that it leads to separation of the process flow: some activities are located on the client's premises, while the rest is at LexSphere. This bifurcation of outsourced services can increase costs and decrease operational efficiency.

Furthermore, since the client's corporate data server and IT department will, in all likelihood, be located at the Head Office, that part of the process which is done at the client's premises must also be so located. This can be an undesirable distraction from the core operations of the average company.

LexSphere Hosted - As an established service provider, LexSphere is capable of securely hosting sensitive databases at its own facilities. A typical network layout is shown below:

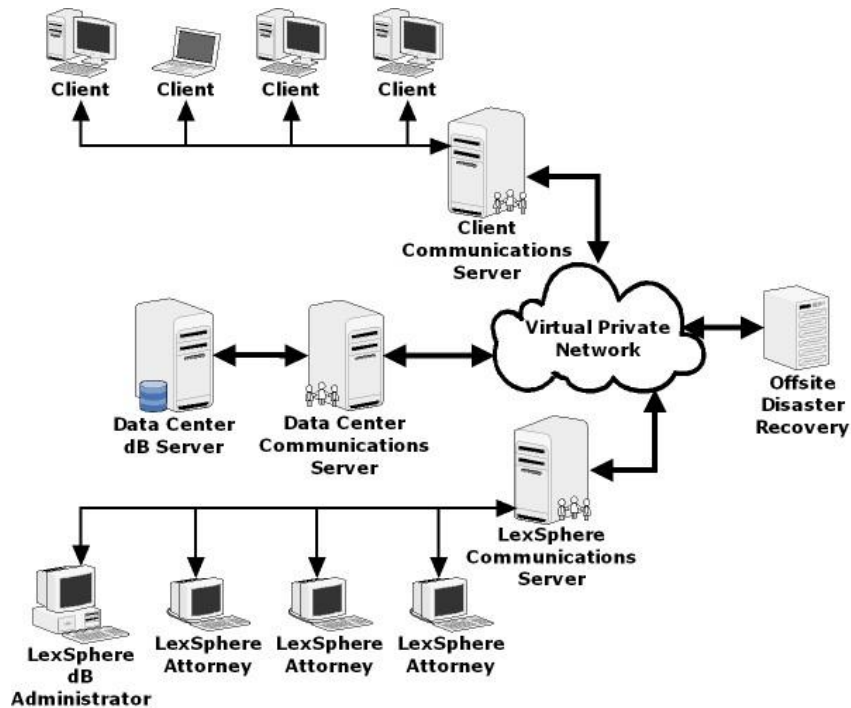


A LexSphere Hosted Database can optimize the workflow configuration, and thereby lead to the lowest process costs. The security environment itself could be made more focused to specific project needs. It could draw the best from the client's practices as well, while including his mandated requirements. Due to its smaller size compared to the client, LexSphere can react quickly to new threats.

The primary disadvantage of LexSphere hosting is the physical location of the database off the client's site. This approach may conflict with corporate policies and preferences.

Since LexSphere services other clients concurrently, the issue of security walls between projects may naturally raise a client's concern. LexSphere recognizes this potential disadvantage and maintains complete process transparency to the client for his assurance. LexSphere's technology package, as a matter of fact, ensures four-fold isolation to a client with (a) hardware walls (b) software walls (c) work-area layout walls (d) information walls or need-to-know.

IDC Hosted - Databases can also be hosted by third party independent data centers, who communicate and share data with the client and service provider over a VPN or leased line.



In theory, this model makes available the highest security tools with the least fixed-costs. This approach potentially has benefits both for the client as well as for LexSphere. IDC's of quality generally have excellent protection against disabling attacks. They also maintain comprehensive data backup, including dual-redundant Disaster Recovery Systems.

The downside is that it introduces a third party into the security equation. Also, data transportation volumes would increase (since data would now move between three nodes in place of two) which, again, has security implications.

LexSphere has tailored security systems that allow for adoption of any of the above three alternatives.

4. LexSphere's Security Environment

The security environment at LexSphere covers all potential vulnerabilities, at several levels, so as to make a practical, effective, and watertight system. An outline description, given in point form, is as follows:

- a. *Process Logs*
Structured process logs which are regularly audited highlight any unusual IT activity, including data transfers to non-legit addresses as well as failed attacks from outside the network.
- b. *Identity Determination*
Digital identity cards, customized for process and function, restricts migration of personnel.
- c. *Personnel Segregation*
The work flow on the floor is arranged in a way that makes it difficult for collusion that can lead to systematic and planned data theft.
- d. *Premises Segregation*
Functional areas are segregated as required to restrict access to authorized persons only.
- e. *Process Segregation*
All process information, including training, are limited on a need-to-know basis
- f. *Hardware Security*
All storage media, stand alone or integrated, are immobilized against physical removal.
- f. *Security Against Copying*
Only thin clients are used (unless otherwise mandated by the function) with no removable media.
- g. *Security of Stored Data*
All data on HDD, CD/DVD, Network Drives, USB drives, etc are encrypted with 128-bit keys.
- h. *Security of Data in Transit*
All data transfers are under Public/Private Key encryption, with PKI and Digital Certificates.
- l. *Security of Web Based Data*
Web based data is secured with SSL technology based on 128-bit keys.
- j. *Security of Email and FTP*
Email and FTP data are secured with SSL technology based on 128-bit keys.
- k. *Security of Telecom Channels*

LexSphere, its Teaming Partners, and the Client are linked on a VPN. Where so mandated, a Leased Line is used for dedicated point-to-point secure data transfer.

l. Network Segmentation and Firewalls

Segmentations of all LAN/WAN are done not only to optimize throughput but also for maximum security as well as damage-limitation in case of infiltration. Firewalls guard the peripheries of all networks.

m. Security Products Used by LexSphere

LexSphere's security arrangements are built with products from such internationally reputed companies as VeriSign, Checkpoint, PGP, Nokia, etc. All websites within the LexSphere system are "VeriSign Secured".

5. Security System Architecture

LexSphere always proposes a security architecture which it believes to be in the best interests of the client with regard to cost as well as effectiveness. However, it realizes that a client may wish to depart from this proposal for its own reasons. In such an event, LexSphere is amenable to reworking the solution as required, with the proviso that the concomitant alterations in system specifications and cost are mutually agreed upon.

5. Conclusion

Data security is, in general, of compelling interest to both clients and vendors. It is of importance for direct practical application, and its failure can have serious commercial implications. Nevertheless, it is a complex subject and has several independent dimensions. So much so, that genuine security specialists are few even among IT professionals.

LexSphere recognizes that companies who own the data, and thereby have most to lose by data loss, are usually far removed from this esoteric science. Therefore, companies often make data security an integral part of their business process outsourcing services. LexSphere has not only in-house competency but also has alliances with some of the world's leading companies in this area. Thus, LexSphere's expertise, backed by the best security products, is inbuilt into the process that brings you all the advantages of the outsourcing business model.

LexSphere's security environment covers *all* needs ---- stored data or data-in-transit, wired transport or wireless, text or audio/video, physical and electronic, hardware-centric, software-centric, process-centric, personnel-centric ---- and more.

When you are with LexSphere your data is safe!