

## Database Security and I-O

Jeffrey Worst

Private I-O and IT Consultant

R. Jason Weiss

Development Dimensions International



It has long seemed inevitable that databases will replace paper as a means of storing various types of corporate data, including HR data. As we know, data such as hiring process information and personnel records are very sensitive and need to be carefully protected. When these data were stored on paper in a file room, the human resources department maintained various policies and procedures to ensure that only authorized personnel had access to the files. This protected the files from people outside the organization and also ensured that only authorized personnel *within* the organization had access to the data. When HR data is migrated to a network-accessible database, these layers of protection must still be maintained. This edition of **Leading Edge** discusses strategies for protecting HR data.

### What is a Computer Network?

Before delving into database security, it would be helpful to consider how computers in a networked organization connect to each other and to the Internet. These connections are depicted graphically as Figure 1. Let's begin with the notion of a *client-server* network. The left portion of Figure 1 illustrates a small client-server network. The *server* is a computer that provides a wide variety of services to client computers. For example, servers can provide access to e-mail, instant messaging, shared file directories, or desktop applications. A *client* draws on the services provided by one or more servers on a network. There are other types of network structures (e.g., token ring), but this is the network structure or typology used in most organizations today.

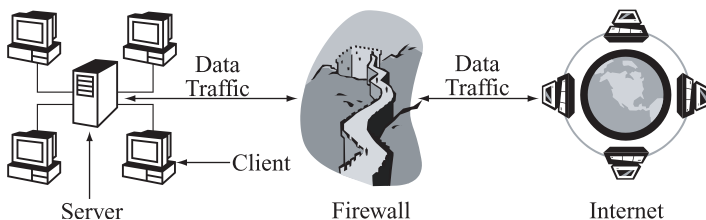


Figure 1. Very simple client-server network

Typically, a corporate client-server network has many clients and more than one server. For example, a single server within an organization may be dedicated to handling e-mail, another to payroll, and another to general storage space (i.e., hard disk) for clients to store various types of files on the corporate network. Servers are usually connected to each other so they can forward requests from clients to the appropriate server. From a database perspective, the obvious advantage of a client-server network is that it provides many users access to a single copy of a database. Hence, a database of job applicants need only be kept on one server rather than being duplicated repeatedly across individual clients. Maintenance of the data is therefore much easier and more accurate because all changes are made directly to a single database.

A company's network of servers is often referred to as an *intranet* or *corporate intranet*. An intranet is different from the Internet (where the World Wide Web exists). An intranet is an organization's private internal network. The Internet is a public collection of interconnected networks. To provide access to the World Wide Web and other Internet tools, the corporate intranet needs to connect out to the Internet. Most companies use what is called a firewall to prevent unauthorized users entering the corporate intranet via the Internet connection (see Figure 1). A firewall is a combination of hardware and software that tries to determine if network traffic coming from and going to the corporate intranet from the Internet is authorized and not malicious.

In some respects, the whole arrangement seems somewhat fragile. For example, the Nimda virus outbreak of September 2001 took down a number of corporate networks, paralyzing many organizations. Fortunately, we I-O psychologists don't have to worry about maintaining network security—that's the role of the network administration department and/or information technology department. However, I-O psychologists *do* have to consider the security of HR data, and it is important to understand how corporate networks function so that we can effectively define our needs and communicate them to the IT staff.

### **Limiting Database Accessibility**

We trust the network administration department to maintain the firewall that keeps the intranet secure from outsiders. What concerns us more directly is the matter of internal security—ensuring that only authorized people from *within* the organization have access to a particular database. If the database to be secured is maintained by HR, then both the HR and network administration staff need to meet and discuss how that security and maintenance will be implemented.

A necessary first step in securing databases is to limit access to them. Modern database software commonly allows for the creator of the database to set up an account directory containing the names and passwords of everyone allowed access to the database. The person with ultimate authority over the database, typically known as the database administrator, maintains this

directory. Only the database administrator should have permission to add and delete user access to the database. By using the account directory, we reduce access to the database from everyone on the network to only those people with names and passwords recognized by the database software.

We needn't stop with merely limiting access to the database. We can also control which activities are available to particular users. There are only four activities that an authorized user can perform on the data in a database:

- Create a record
- Read or view data
- Update or edit currently existing data
- Delete data or records

These activities are colloquially known by the acronym *CRUD*. One of a database administrator's most important responsibilities is to keep tabs on who has the ability to perform CRUD-related activities and which activities they can perform.

The detailed level of control described above is accomplished through *permissions*. A permission is something an authorized user is allowed to do with the database. For example, the database administrator may give an authorized user only the permission to view data in the database. This typically includes the ability to run already established queries and reports (see Weiss & Worst, 2002, for definitions of these terms). A user with these permissions is not permitted to perform any of the other CRUD activities. For example, this user cannot delete data or records in the database. This level of permission is typically given to people who need access to the queries and reports of a database but are not involved in day-to-day maintenance of the database. Limiting who has authority to do what with a database greatly enhances quality control and accountability.

To illustrate the management of permissions, let's take a look at how they are implemented in Microsoft Access 2000. Below are some of the permission levels found in Access.

*Delete*—View and delete data.

*Insert*—View and insert data.

*Update*—View and modify data.

*Read*—View data only, run established queries and reports.

*Administer*—Total access to all aspects of a database such as assigning permissions; revising tables, queries, and reports; setting database password; adding and deleting authorized database users.

Permissions are additive. A user whose only permission is *Update* cannot insert or delete data but by default has permission to read data (you can't edit what you're not allowed to see!). On the other hand, giving the user *Delete*, *Insert*, and *Update* permissions permits unfettered access to the data. Figure 2 below illustrates the Access permissions dialog box.

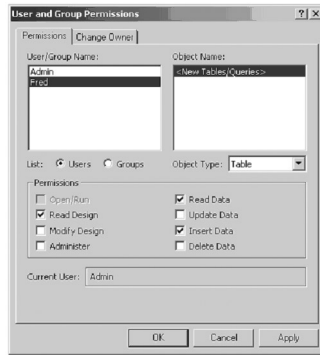


Figure 2. Permissions dialog box for Microsoft Access 2000

The Current User is Admin, which is the default user name for the database administrator. The User/Group Name box shows that there are currently only two users allowed access to the database: the database administrator and a user named Fred. The database administrator has given Fred permission to insert new data (or *create* new records in CRUD terms) but is not allowed to revise (i.e., update) or delete data from the database. Fred is also allowed to look at the design of the database but is not allowed to make any changes to the design. Only the database administrator is allowed to make permission changes. When Fred logs into the database, he would not be allowed to see the dialog box in Figure 2. Note the “Object Name” and “Object Type” listboxes on the right side of the dialog box—these permit the database administrator to set permissions for specific objects within the database such as individual forms, reports, and queries.

As this brief overview illustrates, modern database software allows tremendous control and flexibility in implementing policies regarding who will have access to a database and what level of access they will be permitted. We’ve said it earlier, but it bears repeating: Those responsible for the privacy of the data need to play a very active role in determining these policies. It is interesting to note that once the above security features are in place, not even your corporate network administrators will have access to the data!

Though permissions represent an important level of security for databases containing sensitive data, that security can be compromised. For example, what if the username and password of a person having full CRUD permissions falls into the wrong hands? A malicious user could easily access the database and revise data or make other unauthorized changes. Because of this risk, it may be necessary to take security one step further and implement a small, HR-specific client-server network that is not physically part of the overall corporate intranet. This approach would obviously entail added expense over simply limiting user access and permissions. However, it is

usually not all that expensive to implement, especially when compared to the potential costs associated with compromised HR data.

### **Developing a Data Security Strategy**

Overall data security is a combination of technology and policy. Below are some guidelines to consider when contemplating the development of a new database:

1. There are substantial security concerns when HR data is migrated from paper to databases located on servers. Make data security the first, not the last thing you discuss with your clients, contractors, and/or network administrators when considering the development of a new database. If reasonable data security cannot be assured or fit into the budget, then you probably should not be developing the database. The cost of a security breach is probably much higher than the convenience and data reporting features of a database.

2. The level of security needed is dependent on the sensitivity of the data. For some data, the development of an authorized user directory with permissions may be more than adequate and involves almost no additional cost. Consult with others in your organization or outside consultants, if necessary, to help you make this decision.

3. Leading-edge data security technology can easily be rendered moot by poor policy guidelines or enforcement. A good data security policy should include, but not be limited to, very careful consideration of the following questions:

- Who will be the database administrator? Has the administrator been trained and made aware of their responsibilities?
- Who will be allowed access to the database?
- Who will have permission to make CRUD-level changes to the database? Have they been trained in proper procedures for making changes to the database?

We hope that this column has helped awareness of some critical concerns with HR data security. However, there is much more to know about database security than we have described here. A good Web site for readers interested in learning more is available at <http://databases.about.com/cs/security/>.

We invite readers with questions or comments on this edition of **Leading Edge** to contact us at [kensei@comcast.net](mailto:kensei@comcast.net) (Jeffrey Worst) or [jason.weiss@ddiworld.com](mailto:jason.weiss@ddiworld.com) (Jason Weiss).

### **Reference**

Weiss, R. J. & Worst, J. (2002). Databases and I-O. *The Industrial-Organizational Psychologist*, 40(2), 49–56.