DM Review

intelligent solutions

Managing the Business Intelligence Infrastructure

by jonathangeiger

My last three columns dealt with governance, which is one of the six major sets of activities that must be performed to ensure that the business intelligence (BI) environment operates smoothly, performs cost-effectively, and increases in value to the organization as the business learns to leverage and expand its application.

In this column, I will address a second function: infrastructure management. Infrastructure management consists of the people, processes and technologies that ensure the environment operates smoothly and complies with the regulations and policies concerning data access and use.

BI infrastructure management is a challenge because: 1) the task is rarely within the responsibility of a single group, and 2) the data access and usage patterns vary widely.

The infrastructure consists of the server platform, operating system, database management system, communications facilities, performance tools, BI tools and security tools. The BI team is often held responsible for the performance of the environment but does not directly manage all of it. This requires a collaborative environment for success. Some of the areas that need to be addressed include capacity planning, performance tuning, BI tools and security.

Capacity planning for the BI environment differs from that for the operational environment. Capacity planning must factor in the data warehouse load requirements (primarily batch), the data mart load requirements (primarily batch) and the access requirements (primarily interactive). With the movement to right-time BI, batch cycles are moving from daily to intraday, with some migrating to real time. Capacity planning must consider more than just processing cycles – it needs to consider the storage requirements (which are easier to anticipate) as well as the telecommunications needs. For capacity planning, the BI team must take the lead on anticipating needs and work with other groups to ensure that appropriate facilities are in place.

Performance tuning is important as well. Service levels should be established, and close coordination is needed among the technical systems, database administration and operations personnel to ensure that these levels are met. The BI team must work closely with these groups and may need to serve as a liaison with the business areas to negotiate requirements and explain deviations from expectations.

BI tool requirements are unique. Specialized tools are needed for extract, transform and load (ETL), data query and access, data visualization, etc. With input from the business areas and the technical support area, the BI team needs to coordinate the selection of these tools and determine when upgrades should be installed. While other groups are often tasked with the physical installation, the BI team should create the verification plan and coordinate the testing prior to the production implementation.

Security in the business environment requires some of the same tools needed for the operational environment. Due to the varied usage patterns, additional tools, such as encryption tools for data downloaded to personal computers, may also be needed.

The data access and usage patterns certainly have an obvious impact on the required tools and facilities to be provided to the business users. However, what happens once the data is delivered to the business user?

Data protection has always been important to companies. Companies have traditionally been concerned with ensuring that their trade secrets and other strategic information are not disseminated to competitors. Today's regulatory environment does not leave data protection decisions in the company's hands. Companies with access to personally identifiable information are required to take measures to ensure it is not disclosed except as permitted by law.

Policies, procedures and education provide instructions on handling information once it is viewed or printed. Infrastructure management needs to address what happens to the information as long as it is transmitted and stored in electronic form. Sometimes this requires ensuring that information cannot be accessed in its raw form (i.e., the personal identification must be removed). The greatest exposure exists when the information is accessed outside the corporate walls.

For the person accessing data on a home computer, consider some of the potential pitfalls – for example, others, including children, may also be using that computer. Additionally, the computer may be lost or stolen and its contents viewed by whoever finds it if the data is not properly protected. In addition to ensuring that the data is encrypted during transmission, the receiving computer must also be equipped with security features such as a firewall, antispyware, encryption facilities and other features that ensure that only the authorized people access the sensitive information.

The BI team needs to work with data security to understand the exposures and the options for mitigating them so that the sensitive data is fully protected.

Infrastructure management is sometimes treated as a stepchild within BI. BI methodologies emphasize issues related to capturing and integrating data and to delivering that information to the business community. Infrastructure management is one of those behind-the-scenes functions necessary to ensuring the environment meets the performance expectations and that the company's information is appropriately protected. Strong collaboration with other IT areas is critical for this function to be successfully performed. DMR

Jonathan G. Geiger is executive vice president at Intelligent Solutions, Inc. He may be reached at jgeiger@intelsols.com.