Database Security

Database security is of utmost importance to the organization. Databases contain all of an organization's data (information) vital to the organization's well being and continuity. The organization's sensitive information including financials, customers, sales, payroll, intellectual property, etc. is stored in the database.

Threats in the form of bad actors are both within the organization and outside of the organization. Much of the time the bad actors are from within the organization both intentional and unintentional.

Phishing is a frequent tactic that bad actors employ in order to coax names, accounts, credit cards, and passwords from unsuspecting employees from seemingly authentic sources. The ill-gotten accounts and passwords may also be used to login to the database where the sensitive information can be viewed or downloaded.

The refreshing of data from a production database into a lower level non-production database provides access to production data occurs frequently and is often overlooked. Lower level non-production databases generally have more liberal policies wherein a wider audience is able to access data that it does not otherwise have access to.

There are several tools at our disposal to help thwart attempts to gain access to an organization's sensitive information both vendor supplied and DHS supplied. We have a number of processes to protect and secure your information. Limiting a user to logging into the database from specific hosts will prevent account/password stealing and using it from a different host than what is specified for the account. We have a process to identify sensitive data and scramble it as it is copied to a lower level non-production database. This prevents non-production users from accessing production data in non-production databases.

We also have expertise installing, implementing, and configuring vendor supplied routines to assist with security concerns.