PROTECTING SENSITIVE DATA IN NON-PRODUCTION ENVIRONMENTS

Christopher Carriero

Guardian Applications

Introduction

Sensitive human resource, payroll, credit card, and banking information exist in multiple modules within the Oracle E-Business Suite. While responsibilities control access to sensitive data in a production environment, developers, testers and other IT staff have access to environments cloned from production. These individuals have access to ALL your sensitive data. This is a HUGE risk to a corporation.

With identity theft legislation being enacted in multiple states, corporations must begin to take measures to prevent identity theft or face stiff fines from state and federal governments. This does not even include the cost to a corporation in order to clean up after a security breach. By not protecting the data, even from internal personnel, the corporation opens themselves up to a potential security breach.

The presenters will create an awareness of the problem and then demonstrate to the audience how a corporation can mitigate the risk in their Oracle Applications. The audience will learn how to incorporate a strategy to create another layer of security within their supporting environments and what they need to do to their supporting Oracle E-Business Suite's in order to prevent a potential breach of sensitive data.

Trends

A trend is a general universally accepted evolutionary change. Some are short lived; some are here for the long haul. Sometimes, a trend is something that should be followed. Security is not a trend, it is a necessity. The organization that can adopt the trends quickly and implement them can gain significant market share.

In previous years, network security was the hot button issue. Corporations needed to prevent viruses from entering the corporate environment. Now, most companies have multiple levels of network security. Around the year 2000, compliance was another trend that made corporations create corporate governance business models to prevent insider wrong doing. The latest trend is Risk Management. How does a corporation mitigate all risk in the technology without hindering work? If achieved, the corporation stands to gain significant competitive advantage.

What about the data in our non-production ERP systems?

Non-Production Data

Data in non-production environments is cloned from production in everyday business settings. Therefore, the data is still production data. This is great for the IT staff. They get to use real data while working on everyday problems and enhancing existing systems. The problem is, IT'S REAL DATA. Real data means social security numbers, credit card numbers, and bank account numbers. But that's not all. What about data that no thinks about. Marital status, citizenship information, passport information, drivers license information, salary, salary history, child support payments, and alimony. There are many pieces of data that can be deemed "sensitive".

Targeted Data

Of all the data contained in databases, 90% of the data is contained in HR and Payroll data. Corporations need to care to shield this information in all databases as 61% of data leaks come from inside an organization (McAfee Datagate). And IT does not need access to production to get this information. The information is handed to them.

Security Direction

Prior to 2000, security was all based on preventing access from external sources. With the usage of more outsourcing firms, the concern over access to sensitive data has become heightened. Now, people are looking at the back end applications used and have determined there is a huge potential for data leaks.

What To Do

Organizations can start by auditing who has access to sensitive information. This must be comprehensive and every role in the organization must be looked at. This includes DBA's. Every database environment must be evaluated too. As stated above, data is cloned from production to non-production environments. Who has the APPS password for these environments? Who queries the database regularly?

After your audit, you should have a comprehensive list of individuals in your organization and determine the risk for each. All risk must be mitigated.

Start by educating your staff on secure coding practices. This is a new concept that prevents code theft.

Encrypt or scramble data as necessary. Determine the sensitive fields and using a vendor or home written scripts encrypt or scramble the data so it is not recognized.

Truncate tables as necessary

The scramble routines must be able to determine the primary keys, foreign keys, values sets, lookups, referential integrity, and historical data. All data must still tie out in order to accurately develop new IT projects and maintain existing ones.

Conclusion

The best in class organizations are usually in innovators in society. They are the organizations who are early adopters of technology. These organizations have recognized the problem and are implementing solutions. They look at this as a business incentive to protect data that is considered an asset. All data is protected in all environments without affecting the usage of the data.