



These days, organizations are managed with ones and zeros rather than printed-paper. Networks of computers hold critical data and run essential processes that keep an organization in operation. This combination of interconnected computers and critical data creates a real area of concern— computer security. If an organization’s computers are connected to a network, users of that network can easily misuse unprotected computers. If critical computers are connected to the Internet, they become susceptible to hacking by anyone in the entire world who may want to steal information, modify data, or disrupt operations. Anyone. Anywhere. Anytime.

Most organizations have taken steps to secure computer information and operations. The computer room doors are locked, a firewall has been placed on the network or some software has been configured to detect intrusion. These measures and many more address the physical security of the machines and the logical security of the internal network.

But what information would an intruder want—credit card numbers, social security numbers, private personal information, salary amounts, etc.? Where would an intruder find these things—in a database.

What many companies fail to realize is that most security breaches occur from employees or trusted entities within the internal network of the organization. Suppose a disgruntled employee wants to get even, or a greedy staff member desires to commit fraud, or a quality employee accidentally exposes confidential information, or a curious student wants to test his abilities. Whatever the reason or whoever the person, the goldmine of information they seek most likely resides in or around a database.

How can an organization protect itself from the risks of an exposed database? A complete Oracle database assessment can identify risks within an organization’s databases (due diligence). Having identified the risk, due care can be taken mitigate the risks.

Inplexus an accomplish the management security mandate of due diligence and due care. Inplexus will examine each database for vulnerabilities and notify key staff members in confidence.

This examination takes three steps: (1) interviews with key employees, (2) a penetration test of database systems, and (3) vulnerability tests in the database and the Oracle environment on the operating system. Once these tests are accomplished, Inplexus will produce a confidential and detailed report of the findings along with recommendations for risk mitigation.

If you would like more information about an Oracle database system assessment from Inplexus, please call 770-864-7222 or send an email to [info@inplexus.com](mailto:info@inplexus.com).