



“We wanted to look at the environment from both a tactical perspective and also from a more strategic viewpoint to see where we stood in terms of an overall security posture.”

*Virgil Vaclavik
Technical Services Manager
Hydril*



Hydril Company

Industry: Oil & Gas, Manufacturing
HQ: Houston, TX

Problem: Prepare for SOX audit
Solution: Perform vulnerability assessment and IT Controls Review

Accudata Systems
7906 N. Sam Houston Parkway
West, Suite 200
Houston, TX 77064
281.897.5000
800.246.4908
www.accudatasystems.com

Accudata Systems Aids Hydril to Assess Its IT Environment

THE CHALLENGE

Network security has never been more important to today's businesses. Implementing secure solutions is complex and requires sophisticated approaches, both strategic and tactical.

So when Hydril, a company engaged worldwide in engineering, manufacturing and marketing premium connections and pressure control products used for oil and gas drilling and production, needed to prepare for a SOX audit, it decided to take a larger, more strategic view of the process and issues involved. Hydril determined it wished to examine its network for vulnerabilities and review the overall IT control infrastructure in place. The Company engaged Accudata Systems, Inc. (ASI) in August 2005 to perform an in-depth vulnerability assessment and an IT Controls Review of its network.

“A vulnerability assessment scans the IT environment identifying each vulnerability and misconfiguration at a point in time,” stated Virgil Vaclavik, Technical Services Manager. “We wanted to go a step further. We wanted to look at the environment from both a tactical perspective and also from a more strategic viewpoint to see where we stood in terms of an overall security posture.”

“We had performed previous service work for Hydril,” said Brian DiPaolo, Assessment Practice Manager for Accudata Systems. “When they came to us, they wanted help preparing their environment prior to a SOX audit and as part of this effort they also wanted to do an IT Controls review. How is a controls review different from an assessment? In simple terms, an assessment involves vulnerability scanning and penetration testing of systems. An IT Controls review is similar to an audit of the environment and supporting processes. In this case Accudata Systems used an internationally recognized standard, ISO17799, to examine the status of IT controls in place within the Hydril IT organization.”

THE SOLUTION

Vulnerability Assessment

Hydril engaged ASI to perform a vulnerability assessment of its enterprise. This included an external and internal vulnerability scan and control assessment, a wireless security assessment, and a dial-up systems discovery assessment. The project included complete documentation of findings and recommendations and the presentation of findings to the Hydril management team.

“A lot of tactical issues are discovered during a vulnerability assessment,” Brian stated. “Basically, examine your network at a specific point in time and, by doing so, discover the vulnerabilities. We may identify some strategic issues that need to be addressed; for instance, we find a lot of systems that are not patched. The strategic issue there is you need to make sure you have a patch management system in place, a strategy to deal with patching. But the tactical issue is this server simply isn't patched.”

“We try to extrapolate out of that data some strategic goals,” he continued. “But at the same time we’re saying here are the tactical issues – you need to patch that server, you need to change this configuration, you need to alter specifics in the environment to make it more secure.”

The data collected during the vulnerability assessment was used to generate a report detailing all vulnerabilities found, categorized by risk and effort. Recommendations were made specific to each asset to remediate discovered vulnerabilities based on industry best practices.

IT Controls Review

To attain that larger more strategic view of its environment, Hydril requested an IT Controls review, an interview-based assessment that looks at issues within the organization’s environment to ensure that adequate processes and controls exist based on recognized frameworks and best practices.

“Hydril needed the tactical piece to identify security holes that require resolution in a short time frame,” stated Brian. “But they also wanted to know the overlying strategic issues so they could put projects and efforts in place to strengthen security longer term.”

The IT Controls review gathered data from two main components.

- ◆ A Host Configuration Review – examined critical servers for proper hardening and implementation against best practices. All gaps were documented with recommendations.
- ◆ A Gap Analysis Against ISO17799 – reviewed configurations, processes, and procedures and interviewed required personnel to evaluate existing controls against the ISO17799 standard. This covered the following areas included in the framework:
 1. Access Control
 2. Business Continuity Management
 3. Human Resources Security
 4. Physical and Environmental Security
 5. Communications and Operations Management
 6. Information Systems Acquisition, Development, and Maintenance
 7. Information Security Incident Management
 8. Security Policy
 9. Organization of Information Security
 10. Asset Management
 11. Compliance

Based on the ISO17799 standard, Accudata Systems created a set of open-ended questions for each of the individuals interviewed, including general questions on the perceived current state of security within Hydril and specific questions relative to the individual’s area of responsibility. Personnel included in these reviews included human resources, facilities and business units in addition to IT focused staff to better understand the security needs and integration of the organization.

Once the questionnaires were finalized, they were pre-populated as much as possible with data provided by Hydril personnel. Data included audit reports, policies, procedure documents, network diagrams, organizational diagrams, and other relevant material. The questions were grouped into sections that corresponded to control groups within the ISO17799 standards.

This process produced a composite scorecard for all categories. The scorecard was used to identify areas of strength and weakness, and to help identify recurring themes for deficiencies. The resulting common sources of root cause were summarized into gaps, and these in turn represented discrete projects and/or management action items.

THE RESULTS

From these two assessments, Hydril received a holistic view of the current state of its network security and its vulnerabilities, as well as best practices for remediating and maintaining a steady security posture.

“Hydril had a very good overall picture. They understood the tactical issues that needed to be addressed immediately,” Brian said. “Both assessments dealt with risk and resolution – we associated what the risk to their environment was as well as relating this to the resolution effort. The outcome identified the priorities and low hanging issues for Hydril.”

“Accudata Systems created one deliverable, tying it all together in a single report organized with an executive portion and technical details allowing the appropriate information to be supplied to management as well as the technical IT resources,” concluded Virgil Vaclavik. “The outcome delivers what needs to be done. You prioritize these issues, put a cost around them and a timeframe, and you have a security plan.”

“Both assessments dealt with risk and resolution – we associated what the risk to their environment was as well as relating this to the resolution effort. The outcome identified the priorities and low hanging issues for Hydril.”

*Brian DiPaolo
Assessment Practice Manager
Accudata Systems*