Assess security risk at the plant level

Chemical plant cyber risk and security assessment

Addressing plant security vulnerabilities

As chemical companies have grown through mergers and acquisitions, the number and diversity of plant operations and supporting information technologies have grown. Any comprehensive enterprise cyber-security assessment must address the unique risk profiles of a chemical company's many plant environments.

IBM offers a four-phase solution to help chemical companies assess their plant cyber risk at a given site:

Phase 1 - ISO 17799 Gap Analysis
IBM's multidisciplinary team of security experts evaluates the plant site according to the International Security Standard ISO17799. Areas addressed include:
- Security policy
- Security organization
- Asset classification and control
- Personnel safety
- Physical and environmental security
- Computer and network management
- System access control
- System development and maintenance
- Business contingency planning
- Domains

Phase 2 - Network Security Assessment
In order to realize the benefit from investments in enterprise systems, chemical companies have implemented networks to facilitate the integration of business processes and the sharing of information. These networks are part of a comprehensive strategy to gain competitive advantage. However, their resilience must be appropriate for the unique requirements of the business.

IBM's Network Security Assessment focuses on the security controls implemented for your internal, trusted plant networks. The assessment will be custom-designed to cover whatever system platforms, routers, bridges, switches, or other network components provide the security within your organization.

The technology review component consists of "intrusion tests" and configuration analysis to give you a thorough understanding of the strengths and weaknesses of your internal network components.

Highlights

- Assesses cyber risk, single points of failure, and workplace security at the individual plant site
- Identifies existing threats and vulnerabilities in physical and cyber security
- Addresses information, information systems, and process controls
- Quantifies the potential business impact of identified risks
- Recommends risk reduction measures and mitigation initiatives
Phase 3 - Information Systems Risk Analysis
The Information Systems Assessment conducts a risk analysis and vulnerability assessment of your information systems, including data centers, facilities, networks and plant sites. This analysis helps identify which security measures are most cost effective.

IBM's System Security Assessment is designed to help you identify vulnerabilities that might exist on your key, internal operating system platforms, such as UNIX,® Windows/NT®, MVS,™ AS/400,® etc. and any core “middleware” components, such as Microsoft® Exchange,™ Lotus® Notes,® DB2,® CICS,® MQ Series,® Sybase, DCE, Netware, CORBA, Tivoli,® etc. Both technology and management controls are reviewed.

The technology review assesses each component's mechanisms for identification and authentication, access control, confidentiality, integrity, non-repudiation, audit and alert in the context of your organization's documented policies, standards and processes. The management review consists of interviews with administrators and management and reviews of documented security policies, standards and processes related to the components included in the scope of the review.

Phase 4 - Quantitative Risk and Workplace Security Assessment
IBM's Quantitative Risk and Workplace Security Assessment examines a select plant site to determine its current physical condition, to identify possible single points of security failure, to determine existing workplace security risks and to recommend actions for risk mitigation. The site will be measured for compliance with applicable corporate and industry security standards. Risks are quantified in terms of business impact and risk level. Risk reduction measures and mitigation alternatives are proposed and prioritized. The alternative recommendation may be based upon intangible factors specific to the culture, business practices, and policies of your plant.

For more information, contact your IBM representative or visit:
http://www.ibm.com/services/security