invensys™

Services Profile

Cyber Security – Oil & Gas Client Successes

Summary

At Invensys, developing a successful, comprehensive cyber security portfolio for our clients is critical. We always focus on the overall protection and safety of our clients' facilities.

Business Value

Invensys cyber security solutions are tailored to unique industrial distributed control systems to meet regulatory compliance requirements, industry regulations and best practices. Our cyber security solutions are platform and system agnostic and are based on Invensys' unique cyber security lifecycle methodology that fits with any client's program and includes:

- Assessment
- Development
- Implementation
- Management

Real Collaboration.
Real-Time Results.™

CRITICAL INFRASTRUCTURE & SECURITY PRACTICE

Invensys' Critical Infrastructure & Security Practice (CISP) specializes in cyber security solutions for the Oil & Gas, Power, Nuclear, Chemicals, and Water Industries, focusing on the unique needs of each of these industries' distributed control systems (DCS). Just as every facility is different, so are the issues that drive cyber security. In some cases, it is government regulatory requirements or industry regulations, and, in others, it is a need to comply with best practices. To optimally address such diversity, CISP developed a unique methodology.

CYBER SECURITY LIFECYCLE METHODOLOGY

The cyber security lifecycle methodology takes a holistic approach to cyber security based on the four tenets of critical infrastructure compliance: information security, physical security, plant safety and business continuity. Cyber security solutions developed by this approach are unique because they provide not only security for critical infrastructure, but they also integrate seamlessly between manufacturing operations and corporate IT networks – Invensys solutions address all the needs of a comprehensive cyber security solution.

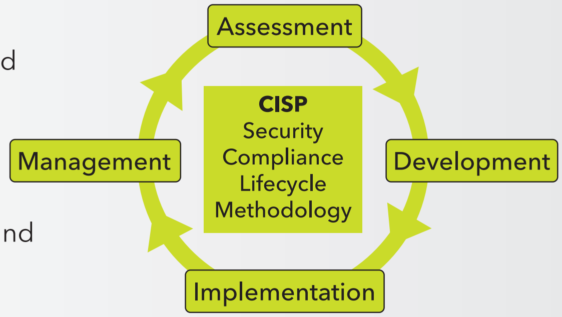
The four phases of the lifecycle methodology are shown in the diagram which illustrates the basic approach for every client engagement. The methodology gives CISP the flexibility to engage a client at any point in their program's own lifecycle.

Stage 1 – Assessment

CISP reviews the current network, identifies any problems or issues, and suggests areas for improvement.

Stage 2 – Development

CISP identifies what needs to be implemented from the assessment and develops the remediation plan.



Stage 3 – Implementation

CISP installs networks, from design to installation and commissioning.

Stage 4 – Management

CISP closely manages the network and provides a mechanism to improve and optimize the continuously changing landscape of network usage.

OIL & GAS INDUSTRY CYBER SECURITY SUCCESSES

Below are concise, illustrative examples of how CISP has successfully applied in-depth cyber security knowledge and extensive industry experience, using the cyber security lifecycle methodology, for our Oil & Gas Industry clients.

Large Global Refining Company

Problems	Actions	Results
• Client had very specific corporate security policies and standards. • Client wanted to limit employee access to systems based upon policies. • Client's network was comprised of dissimilar DCS and networking equipment.	• CISP deployed an Off-Mesh Active Directory (AD) solution. This solution provided flexibility by bringing third-party equipment under a common domain. • A Patch Management Server solution was provided to maintain and push updates out to the network on a client-defined schedule.	• Met client's specific needs and corporate policies. • Overall design deployment was an investment optimization. The existing dissimilar equipment was able to be reused and the scope of the overall network was kept in check. • Enhanced cyber security posture.

Large Global Refining Company

Problem	Actions	Results
• Client needed to ensure that all the I/A servers were at the same level of compliance.	• CISP performed I/A workstation hardening, removing all unnecessary services and baselining the systems to develop a profile. • CISP provided additional security work such as patch updates and password update.	• Client has a complete baseline and full documentation for all I/A workstations at that facility. • Client has enhanced their security profile and reduced one cyber security attack vector.

Mid-Tier Refining Company

Problem	Actions	Results
• Client required enhanced security between the corporate network and the plant control network.	• CISP designed and deployed its Secure Zone solution, an implementation of firewalls that support functionality in different zones, such as the corporate and plant control zones.	• Client has secured the plant control network from the corporate network and can still pass critical business information to and from both sides. • Enhanced security posture.

Mid-Tier Refining Company

Problem	Actions	Results
• Client had an identified need for cyber security, but lacked the necessary personnel and skill sets required to sustain and maintain a cyber security solution 24/7/365.	• CISP designed and deployed its Secure Zone solution to isolate and secure the corporate network from the plant control network. • CISP deployed an Anti-Virus updating and Patch Management server to manage all critical updates for the network. • CISP hardened the I/A workstations to provide a common baseline. • CISP deployed a Network Management server to monitor the I/A workstations, traffic, utilization per port, statistics and reporting. • CISP deployed Managed Secure Services for 24/7/365 monitoring, reporting and critical event alerting.	• Client received a comprehensive cyber security solution. • The entire solution can be maintained without the need for additional highly skilled technicians. • The client has greatly improved their cyber security posture and reduced a number of cyber security attack vectors.

INVENSYS CYBER SECURITY SOLUTION MATRIX

Component	Functionality	Benefits
Network Assessment Tools	Network and Software Tracking & Change Management	Detailed analysis of what is happening on the network; visibility of applications installed, state of hardware and security on your network. Provides history of network changes and change notifications
	Cyber Assets Inventory	Creates an inventory of IP devices essential to plant operation, to be protected
Patch Management	Identify & install missing Operating System and Third Party software updates	Scanning profiles to identify missing patches for specialized mission specific cyber assets such as DCS HMIs. Patch remediation tracking
Network Performance Monitoring & Alarming	Monitor Protected Cyber Assets	Quickly detect, diagnose and resolve network performance problems; real-time dashboards enable at-a-glance network performance tracking
Centralized AV Management with ePO	Apply AV protection to Protected Cyber Assets	Centralized AV management, controls and updates to protected Cyber Assets
Centralized Host Access Controls for HIDs, DLP and Whitelisting	Apply access controls to Protected Cyber Assets	Centralized Host Access Controls and management for protected Cyber Assets
Event Logging and Reporting	Security Information and Event Management	Provides centralized event monitoring services collecting data from various systems, archiving events and providing notification capabilities with a central repository of data logs
Centralized Backup Storage	Protected Cyber Asset backup management and controls. Repository for protected Cyber Asset backups and storage.	Enables quick backup, restore and testing for protected Cyber Assets
Remote Relay Access Server	An intermediate device such that the Cyber Asset initiating interactive remote access does not have direct access to protected Cyber Assets.	Remote Access to establish relay bastion host for relaying remote connections to protected Cyber Assets. Ability to deliver Read Only—Administrative function; diagnostics and configuration; non-operator observation
Protected Cyber Assets Identification Workshop	Identify and classify Protected Cyber Assets and identify potential Electronic and Physical Security Perimeters for easier management and maintenance.	Identify Protected Cyber assets with an identified repeatable methodology. Identifies exactly what is protected and why
Technology Roadmap Workshop	Identify network strategy for connecting DCS networks to business networks	Establish security methodology for connecting dissimilar networks. Establish technology plan and requirements for DCS network
Managed Secure Services	Designed specifically for process control networks; 24/7/365 monitoring of security devices with timely identification and remediation of security vulnerabilities	Eliminates need for expensive full-time security expertise; maximizes reliability and uptime; continues data analysis to identify existing and predict future security challenges; enforces policy management and change control
AD Workshop	Identify staffing, security and access control requirements for protected cyber assets	Implementing of active directory structure capable of meeting compliance requirements for protected cyber assets
Supporting Services	Gap analysis; assessments; incident response; documentation policy and procedure creation, updates and assessments; network management	Customizable services that complement any Cyber Security compliance program; services can be leveraged individually to identify and fill any gaps in client's compliance program or against their internal security posture
Engineer Operating Instructions	Detailed instructions for performing task associated with maintaining compliance for Protected Cyber Assets	Task instructions developed for DCS staff to perform task required for implementing, changing and updating Protected Cyber Assets

To learn more about Invensys' Critical Infrastructure and Security Practice solutions, contact your sales representative or visit: http://iom.invensys.com/CyberSecurity.

Invensys • 5601 Granite Parkway III, #1000, Plano, TX 75024 • Tel: (469) 365-6400 • Fax: (469) 365-6401 • iom.invensys.com

Rel. 08/12 PN IN-0231