invensys™

Services Profile

Cyber Security Best Practices

Summary

The Invensys Critical Infrastructure and Security Practice (CISP) has developed a comprehensive lifecycle approach that includes these core best practice tenets:

- Assessment
- Development
- Implementation
- Management

Business Value

- Dependable and repeatable process
- Easily maps to any standard regulation
- Implementable at any process roadmap stage
- System agnostic and platform independent

Real Collaboration. Real-Time Results.™

Comprehensive Cyber Security programs have never been more needed than they are today. In addition to the traditional hacker targets – large corporations and banks – the utilities sector is increasingly a focus. Hackers now target SCADA systems for weaknesses, seeking to exploit these industrial control systems and publishing related information online. Numerous standards organizations help companies develop effective Cyber Security compliance strategies, including these:

- North American Electric Reliability Corporation Critical Infrastructure Protection (NERC-CIP)
- Nuclear Energy Institute (NEI)
- Internet Engineering Task Force (IETF)
- National Institute of Standards and Technology (NIST)
- Chemical Facility Anti-Terrorism Standards (CFATS)
- Department of Homeland Security (DHS)
- International Society of Automation (ISA)
- International Organization for Standards (ISO)

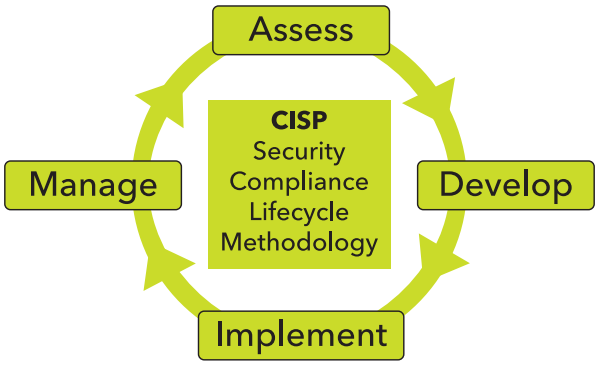
While these organizations have different approaches, they all have a common element – to establish a "best practice" approach to Cyber Security. Invensys' Critical Infrastructure and Security Practice (CISP) builds on the best practice approach through its lifecycle methodology, which ensures that the solutions are network and control system agnostic. The lifecycle of any network system is divided into four distinct stages:

Stage 1: Assessment & Planning – CISP reviews the current network, identifies any concerns and suggests areas for improvement.

Stage 2: Development of Architecture & Design - CISP builds on the assessment to identify what needs to be implemented and develops the detailed designs required to make it happen.

Stage 3: Implementation & Modernization - CISP takes the network design and turns it into reality through procurement, staging and commissioning of the new system or upgrades.

Stage 4: Management & Optimization – CISP works closely with network management, providing a mechanism to improve and optimize the continuously changing landscape of network usage.



CISP CYBER SECURITY BEST PRACTICES

Component	Functionality	Benefits
	Network and software tracking and change management	Detailed analysis of network; visibility of installed applications, state of hardware and security; history of changes & notifications
Network Assessment Tools	Cyber assets inventory	Creates an inventory of IP devices on the ESP network
Patch Management	Identify and install missing operating system and 3rd-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 performance problems; real-time dashboards enable at-a-glance performance tracking
Centralized Anti-Virus (AV) Management with ePO	Apply AV protection to cyber assets	Centralized AV management, controls and updates to ESP 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 ESP 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 data log repository
Centralized Backup Storage	Protected repository for cyber asset backup management and controls	Enables quick backup, restore and testing for ESP cyber assets
Remote Relay Access Server	An intermediate device so the cyber asset initiating remote access does not have direct access to cyber asset(s) within the ESP	Remote access to establish relay bastion host for relaying remote connections to ESP 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	Identifies protected cyber assets with a repeatable methodology; identifies exactly what is protected and why; easier management and maintenance of compliance
Technology Roadmap Workshop	Identify strategy for connecting DCS and business networks	Establish security methodology for connecting dissimilar networks; establish 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
Active Directory (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 complement any cyber security compliance program; 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	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

Rev. 06/12 PN IN-0226