



BETTER SAFE THAN VULNERABLE TO PLANT SYSTEMS CYBER ATTACK

Holistically managing your enterprise risk protects business value.

- Ensure that compliance becomes part of business as usual
- From policy to operations — security is a cohesive whole
- Gain shared insight into the probable business impact of actual/anticipated security incidents
- Understand the shareholder value of information risk
- Align security expenditures with business priorities and compliance imperatives
- Get protection commensurate with value-at-risk — don't under protect, or over spend

- How will you address the complex and unique problems of cyber security in manufacturing process control systems?
- How can you be sure your manufacturing plants are ready for regulatory cyber security inspections?
- What will you do to manage the differing requirements for IT and manufacturing cyber security, in addition to those of wireless networks and other vulnerabilities?

“Today the Department of Homeland Security has identified terrorist-based cyber security threats to manufacturing process control systems as the highest risk scenario to the chemical industry.”

Source: Department of Homeland Security, 2009

Cyber security threats have become very real for chemical manufacturers. The recent Stuxnet worm, called by security analysts “one of the most sophisticated and unusual pieces of malicious software ever created,” was targeted to directly attack manufacturing control systems. In addition, the Department of Homeland Security (DHS) has begun inspecting chemical plants against the Chemical Facility Anti-Terrorism Standards (CFATS). The cyber standards in CFATS are primarily focused on manufacturing real time systems, such as DCSs, PLCs and SCADA packages, their multiple egress points and integration with physical security elements, such as surveillance systems and bar-coded access management systems. Process engineers and site IT personnel are challenged to effectively define the risk and develop mitigation plans and designs. To make things even more difficult, they must address two opposing requirements — how to provide access to the plant floor systems to facilitate connectivity with business systems, while simultaneously protecting them from cyber attack.

While IT professionals have long been familiar with standard practices for securing routers and web access to ERP and other applications and networks, these techniques and technologies do not translate directly to the manufacturing floor.

How can you adapt and harmonize them with process control systems?

What is the most effective way to manage in this environment?

What can you do today to secure your manufacturing environment?

Achieving and sustaining CFATS compliance can be a costly affair. The DHS estimates that each Site Security Plan will consume 200 man-hours to prepare, and will have to be completed within 120 days of DHS notification. The traditional approach of allowing individual sites to create their own plans is ineffective — resulting in gaps and inefficiencies that drive up costs and produce sub-par outcomes. An enterprise-wide approach is really the only realistic path forward.



CFATS Plant Cyber Security Services

The combination of rapidly evolving cyber threats to manufacturing systems (like Stuxnet) and the quickening pace of DHS CFATS Site Inspections are a “call to action” to invest in chemical plant cyber security readiness. Cyber Security in chemical plants is complex due to the differences between business and manufacturing systems — as a result, most plants are not prepared for a cyber inspection. Meeting these challenges requires combined domain expertise in IT Security and Plant Control Systems, and the ability to apply that expertise consistently from the Business Data Center to the Plant Control Room.

CSC’s CFATS Plant Cyber Security Services will enable you to secure your plants and be ready to meet the DHS inspection challenge by:

- Creating a comprehensive inventory of consequence-based risks for all plant automation and process control systems.
- Documenting a Gap Analysis of the plant systems versus required standards around cyber security policies, practices, and technologies.
- Building a Roadmap of prioritized remediation projects to close the Gaps, with rough order of magnitude cost estimates.

CSC combines world-class Cyber Security skills with deep Manufacturing domain knowledge to meet the challenge of securing your manufacturing facilities against the growing threat of cyber attack and the increasing requirements of government regulations.

About CSC

The mission of CSC is to be a global leader in providing technology-enabled business solutions and services.

With the broadest range of capabilities, CSC offers clients the solutions they need to manage complexity, focus on core businesses, collaborate with partners and clients and improve operations.

CSC makes a special point of understanding its clients and provides experts with real-world experience to work with them. CSC is vendor independent, delivering solutions that best meet each client’s unique requirements.

For more than 50 years, clients in industries and governments worldwide have trusted CSC with their business process and information systems outsourcing, systems integration and consulting needs.

The company trades on the New York Stock Exchange under the symbol “CSC.”

CSC

3170 Fairview Park Drive
Falls Church, Virginia 22042
+1.703.876.1000
www.csc.com

Copyright © 2010 Computer Sciences Corporation. All rights reserved.

What Sets Us Apart?

- More than 1,200+ full-time security professionals
- Client base including: CIA, Department of Defense, and other top government agencies and commercial customers on continents in all industries
- Extensive domain expertise and experience in Chemical Manufacturing processes and systems
- Recognized by analyst research as providing “best customer service”
- Secured Enterprise portfolio of services



If you want to reduce the cost of compliance, while simultaneously improving the effectiveness and thoroughness of your security programs, we can help.

Learn more about our iRisk and Protected Enterprise/Protected Plant by contacting us at poweryourperformance@csc.com.

CSC’s Chemical, Energy and Natural Resources Group is a global leader in helping companies achieve strategic business objectives through the application of industry-specialized business solutions and services.

To learn about our Enterprise Compliance and Sustainability solutions, visit www.csc.com/sustainable_compliance.