Securing Industrial Control Systems in the Chemical Sector

ROADMAP AWARENESS INITIATIVE – A CASE FOR ACTION

Developed by the Chemical Sector Coordinating Council in partnership with the U.S. Department of Homeland Security

September 2012

Homeland Security

WHAT IS THE ROADMAP AWARENESS INITIATIVE?

Through the Chemical Sector Coordinating Council (CSCC), the chemical industry is working in partnership with the Department of Homeland Security (DHS) to address Industrial Control System (ICS) security. Published in September 2009, the Roadmap to Secure Control Systems in the Chemical Sector ("Roadmap") is the result of the collaborative effort of DHS and representatives from the chemical industry, as well as the vendor community. The document defines key milestones over a 10-year period designed to advance the security of ICS in the chemical industry. This awareness initiative targets several key milestones noted in the first two years of this process.

The Roadmap Implementation Working Group, composed of DHS and industry volunteers, has collected a wealth of reference information designed to assist owners and operators in addressing ICS security. Key resources include:

Cyber Security Evaluation Tool (CSET) – DHS offers the CSET for companies interested in an assessment methodology. This tool is provided free of cost in the Roadmap Awareness Initiative.

Cybersecurity Tabletop Exercise – This exercise is scalable and adaptable for your company allowing you to explore and address cybersecurity challenges. It includes an option of two scenarios – control systems and business systems. All materials and templates are provided for a minimal planning effort.

The Industrial Control Systems – Cyber Emergency Response Team (ICS-CERT) - The Industrial Control Systems – Cyber Emergency Response Team (ICS-CERT) is a key resource for situational awareness for the process control and automation industries. The Roadmap Awareness Initiative contains several resources from ICS-CERT, including an overview of national ICS incident reporting as well as the most prominent cyber threat trends and vulnerabilities pertinent to ICS.

Industry Standards, Relevant Guidance, and Additional References – The Roadmap Implementation Working Group developed *Industry Standards, Relevant Guidance and Additional References*. This guide is designed to facilitate research on existing standards in the area of control systems security. The guide highlights two resources for industry standards, as well as five resources for relevant guidance, and several additional reference resources on ICS security topics.

Procurement Language – The *Department of Homeland Security: Cyber Security Procurement Language for Control Systems* provides sample recommended language for control systems security requirements. The document provides example language to incorporate into procurement specifications. ICS asset owners and users can change or modify document language as needed to meet individual procurement needs.

Training Resource – The Roadmap Implementation Working Group developed the *Chemical Sector ICS Security Training Resource*. This guide of available training is designed for professionals who work in areas relevant to the process control and automation industries. The information is organized by levels of difficulty – introduction; intermediate; advanced. For ease of access, the guide includes links to relevant Web sites.

All of this information and more is available through the Roadmap Awareness Initiative DVD. To obtain a copy of this DVD, please email **chemicalsector@dhs.gov.**

Why should I care?

The chemical industry dedicates immense time and resources toward ensuring the safety of its personnel, customers, and surrounding community but, in today's environment of growing cyber threats, a chemical plant is not safe unless its systems are secure.

Over the past decade, ICS vendors, not unlike companies in the chemical industry, have undergone mergers and acquisitions and have implemented cost efficiencies. One of the trends emerging from this marketplace is the move from delivery of ICS on "proprietary" system platforms to "open" system platforms. These open platforms carry a greater level of cyber risk due to the rapid growth of cyber threats against them. ICS environments that once required specialized expertise to penetrate are now exposed to the vulnerabilities of open platform environments, including both specific ICS threats and more general attacks against the platform itself that could contribute to an ICS incident.

Potential consequences of an ICS incident are listed below. Note the similarities of consequences that could result from either a control systems security breach or a safety protocol breach.

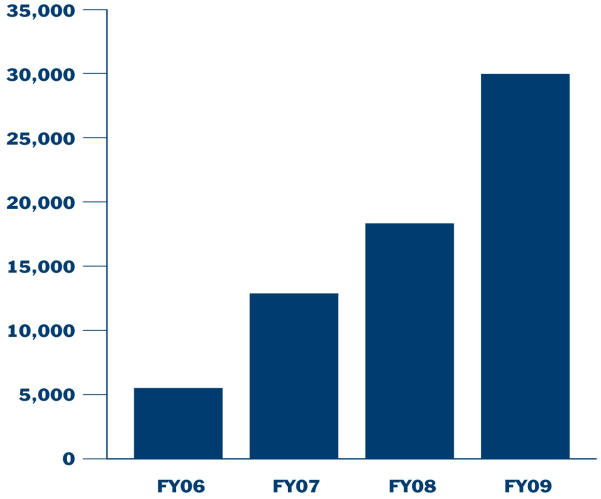
- Reduction or loss of production at one site or multiple sites simultaneously;
- Injury or death of employees;
- Injury or death of persons in the community;
- Damage to equipment;
- Release, diversion, or theft of hazardous materials; and
- Impact to company's reputation in the community.

When connectivity and speed of communications are vital to efficient business operations, it is essential that every company understand and assess both the safety and security issues related to ICS.

Is the risk real?

Yes. Since the summer of 2010, media reports highlighted a number of incidents where computer viruses and worms specifically targeted ICS. Systems can be infected though USB drive usage, remote access, and wireless connectivity. Like a personal computer, a plant automation system could potentially shut down if infected. Although the information technology community has been actively addressing threats to computer systems for a number of years, the control systems community faces an uphill battle to proactively protect against this new threat environment.

Cybersecurity Incidents Reported to US-CERT in Fiscal Years 2006 to 2009[1]



Source: GAO analysis of US-CERT data.

According to the DHS ICS-CERT 2010 Year in Review[1], 2010 saw an increase in advanced persistent threat activity affecting organizations across all critical infrastructure sectors. In addition, a June 16, 2010 Government Accountability Office (GAO) report[2] found that Federal agencies reported approximately 30,000 incidents to US-CERT in fiscal year 2009, representing an increase of more than 400 percent compared to 2006. In most cases, these attacks focus on corporate espionage with the intent to gain a competitive advantage in regional or global markets. Although control systems are not the typical target, all pathways from a business network should be considered if a compromise has breached the control network.

Moreover, 2010 also represented an unprecedented year for the control systems community. The emergence of Stuxnet, the first malware created specifically to target ICS, signaled a paradigm shift. Stuxnet demonstrated that organizations must be operationally prepared with tools, systems, and personnel to detect malicious activity and effectively mitigate the impact to their control systems. Stuxnet highlighted the interdependencies and vulnerabilities that exist in legacy control system environments and demonstrated that motivated groups are interested in attacking critical infrastructure. Stuxnet is a wake-up call to many that "security through obscurity" is no longer an option.

Control systems are increasingly interconnected to other plant and business systems to share valuable data using standard communications protocols. Also, most ICS vendors are incorporating standard information technology into their systems at a rapid pace that exposes these systems to modern malware threats, even if those threats are not intended for the plant floor.

[1] *DHS ICS-CERT 2010 Year in Review*, Washington, D.C.: Department of Homeland Security, January 2011: p. 2.

[2] GAO, *Cybersecurity: Continued Attention is Needed to Protect Federal Information Systems from Evolving Threats*, Washington, D.C.: June 2010: p. 3.

The real risk associated with the interconnected nature of our plants requires specific attention to:

- ***Securing connectivity between business systems and ICS within corporate networks*** The objective is to restrict the highest probable attack path to ICS. In the recent past, cyber attacks on ICS have most often been initiated through the Internet to the business system and then to the ICS.
- **Securing communication between remote access devices and control centers** The objective is to deter cyber attacks from remote location via legitimate and surreptitious access points. Remote access includes wireless communication devices that have access to the control system, such as personal communication devices that have access to the control system and system state sensors, senders and receivers. It also includes virtual private network (VPN) connections, and authorized vendor and system support access.

Guidance to addressing these vulnerable areas can be found in section 2.15 of the *Catalog of Control Systems Security: Recommendations for Standards Developers*, authored by DHS with representatives from the National Institute of Standards and Technology, as well as the Department of Energy. The catalog can be found at: **http://www.us-cert.gov/control_systems/csdocuments.html.**

Are Industry Control Systems regulated?

In addition, high risk chemical companies are required to secure ICS under the Chemical Facility Anti-Terrorism Standards (CFATS). DHS has issued security regulations for any facility that manufactures, uses, stores, or distributes certain chemicals at or above a specified quantity.

Risk-based performance standard (RBPS) 8 states that regulated facilities must "Deter cyber sabotage, including preventing unauthorized onsite or remote access to critical process controls, such as Supervisory Control And Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), Process Control Systems (PCS), Industrial Control Systems (ICS); critical business systems; and other sensitive computerized systems.

For more information on CFATS, please visit **www.dhs.gov/chemicalsecurity**.

WHAT CAN I DO?

The chemical industry must work together to ensure that a control systems security breach does not occur. This requires increasing awareness, education, and communication between the engineering, security, information technology, process safety, and manufacturing operations communities.

The ultimate responsibility for ensuring a secure ICS environment lies with the owner/operator. Companies should do the following:

- Ensure one person takes ownership of ICS security and is accountable.
- Open the lines of communication between engineering, security, IT, process safety communities, and manufacturing operations communities within your own company.
- Conduct an audit of current ICS security measures and implement obvious fixes.
- Follow-up with an ICS security vulnerability analysis (risk assessment) for a complete identification of vulnerabilities and recommendations for corrective action.
- Implement an ICS security management program that is integrated with existing company management systems for security, safety, quality, etc.
- Email **chemicalsector@dhs.gov** to obtain additional information including the Roadmap Awareness Initiative DVD.

Look through the information provided, bring it to your company management, ask key questions about how your company is addressing ICS security, and become an advocate in your company on this important issue!

Prepared by the Chemical Sector Roadmap Implementation Working Group, September 2012

The Chemical Sector Coordinating Council (CSCC), the U.S. Department of Homeland Security's Office of Infrastructure Protection (IP), and the National Cyber Security Division (NCSD) of the DHS Office of Cybersecurity and Communications (CS&C) facilitated the development of these materials, with volunteers from Chemical Sector and industry stakeholder organizations.

Working Group Members

Christine Adams, Catalyst 35

Marc Ayala, AkzoNobel

Randy Black, Ineos

Eric Cosman, Dow Chemical

Terry Deo, Infineum

Tom Dion, DHS

Bill Erny, American Chemistry Council

Tom Good, DuPont

Amy Graydon, DHS

Mark Heard, Eastman Chemical

Lisa Kaiser, DHS

Robert Kirk, DHS

Esther Langer, DHS

Blake Larsen, Western Refining

Theresa Miller, Energetics, Inc.

Johan Nye, Exxon Mobil

Dan Rozinski, CSC

Steve Salvo, Air Products

Mike Sauer, Ashland

Jonathan Schreiter, Air Products

Dan Strachan, National Petrochemical and Refiners Association

Michael Sweet, Energetics, Inc.