

Cyber Preparedness in Industrial Control Systems: Beyond CFATS

Edward J. Liebig

MsIT/IA, CISM, CISSP, CIPP, CBCP, CHS-III

CTO Commercial Security Consulting (CSC²)

CSC

Legal Notifications

No Endorsement Notification

Any reference on this website or materials on this website to any specific commercial products, processes, or services by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the Department of Homeland Security or the United States Government.

Hyperlinks Web sites do not constitute endorsement by DHS of the Web site or the information, products, or services contained therein. DHS does not exercise any editorial control over materials on this website or the information on non-DHS Web sites.

Disclaimer Notification

The views, opinions, findings, conclusions, or recommendations expressed in the materials on this website are those of the authors and do not necessarily reflect the official policy or position of the Department of Homeland Security (DHS) or the United States Government. The publication of these views by DHS does not confer any individual rights or cause of action against the United States. Users of information in the materials assume all liability from such use.

Call to Action: Industrial Systems are under Cyber Attack

Shodan, an internet search tool, highlights the exposure of ICS environments to cyber threats as they become more connected and as tools to exploit them become increasingly available.

A sophisticated worm designed to *steal industrial secrets and disrupt operations* has infected at least 14 plants, according to Siemens.

Called Stuxnet, Iran. *It is one of*

The worm... has is worrisome new *significant amount*

Researchers at *built not only*

Flame, a more complex descendant of Stuxnet, shows the continuing exposure of ICS environments to cyber attacks and the growing sophistication of those attacks.

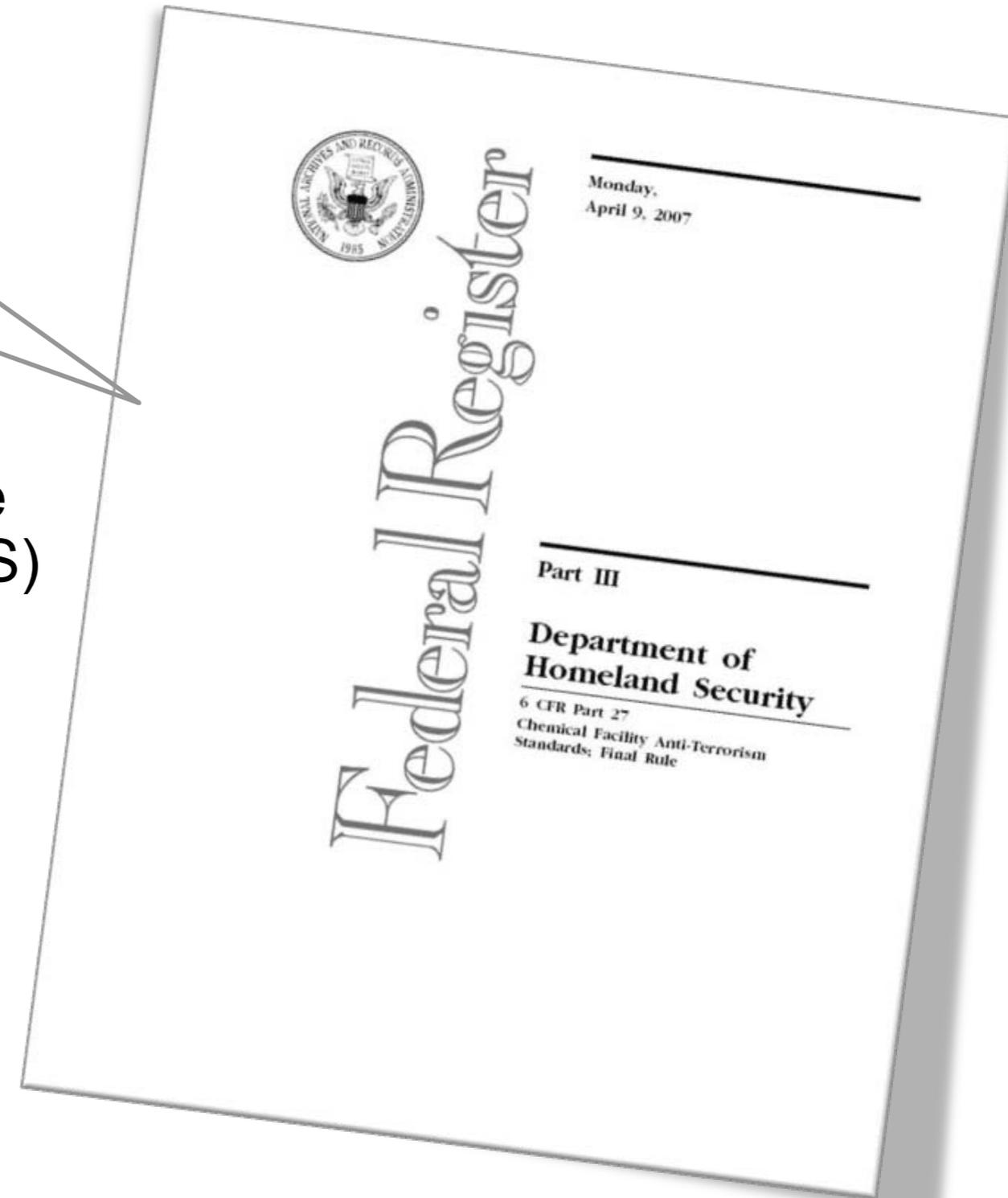
The Cyber threat to industrial systems is real and growing

Call to Action: CFATS - Getting Serious About Security

“This rule establishes risk-based performance standards for the security of our Nation’s chemical facilities.

It requires covered chemical facilities to prepare Security Vulnerability Assessments (**SVAs**), which identify facility security vulnerabilities, and to develop and implement Site Security Plans (**SSPs**), which include measures that satisfy the identified risk-based performance standards (**RBPS**).”

- 6000+ U.S. Chemical Plants have been designated “in scope” for CFATS by the Department of Homeland Security (DHS)
- CFATS process:
 - Site Vulnerability Assessments
 - Site Security Plans
 - Site Inspections (by DHS)
 - Implementation or Correction of Plan
 - Compliance and Recordkeeping



This is where we are now in the CFATS process

We Believe ...

- CFATS Site Inspections were a “call to action” to invest in cyber security readiness at the plant ICS level.
- But the **imperative for action** goes “beyond CFATS”; we need to make sure we understand - and can describe - the risk to global manufacturing operations from the increasing cyber threat to ICS.
 - **Consequence-based risk assessments** in **global** manufacturing operations
 - **Gap analysis** against CFATS and enterprise IT security policies and standards
 - **Prioritized** action plans to close gaps and **reduce the risk** to manufacturing operations
- Cyber Security in chemical plants is challenging due to the differences between enterprise-business and plant-control systems.
 - As a result, many plants are not prepared for a cyber inspection
 - ...or, much worse, a major incident with operational and/or SHE impact
- Meeting this challenge requires combined domain expertise in IT Security, ICS and Manufacturing Operations, with consistent cyber policy from the Enterprise Data Center to the Plant Control Room.

Compliance is not enough – we must go “Beyond CFATS” to meet today’s cyber threats to manufacturing operations.

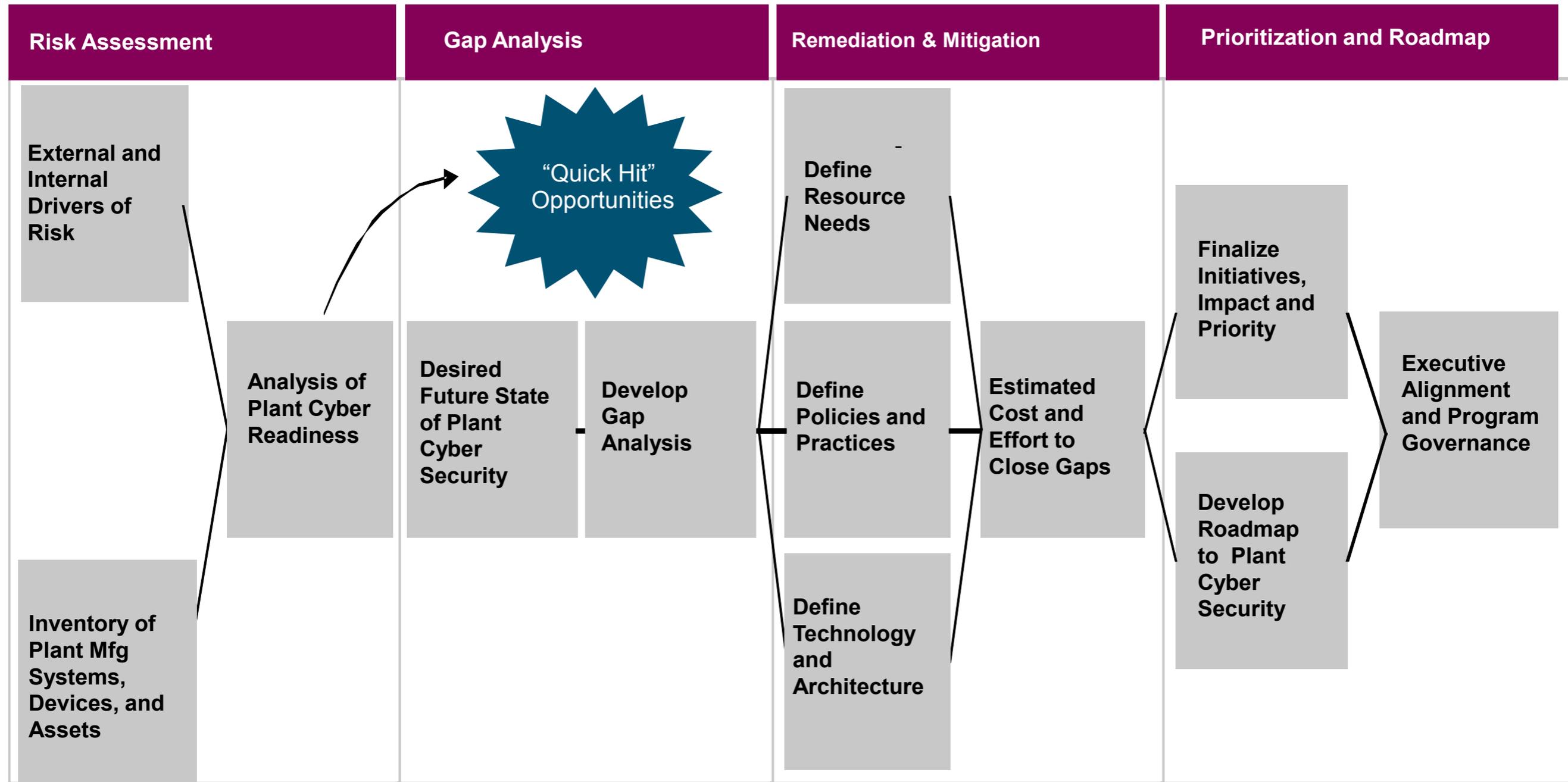
Meeting the Imperative for Action: ICS Cyber Security Readiness Assessments - *CFATS and Beyond*

- Cyber Security Inspection and Risk Assessment of Assets
- MTSA, Responsible Care, and Global Standards Assessments
- Automation & Control System Cyber Risk Reduction



CSC combines world-class Cyber Security skills with deep Manufacturing domain knowledge to meet the challenges of ICS Security and beyond

Building the ICS Cyber Security Roadmap



Critical Success Factors for ICS Cyber Security Assessments

- Engage the plant process owners, operations staff, and technical support staff in the plant directly.
- Give real world examples of exploit techniques and concerns as part of the information gathering and assessment activities.
- Intentionally build cyber security awareness training for the plant operations and engineering staff into the assessment process.
- Understand that cyber security gaps will be a combination of people, process, and technology and actively engage all three aspects to assess and close gaps (including ICS suppliers).
- The engagement and awareness better aligns IT, Security and Operations stakeholders in understanding of how cyber risk is measured and managed.

Key Learnings from ICS Cyber Security Programs

- A standard framework for assessing consequence-based risk is critical to making informed decisions on plant cyber security investments:
 - Assessments should be done at the ICS device level.
 - Consider the impact on Safety/Health/Environment, Operations/Cost, and Company Image/Brand.
 - Measure gaps against compliance requirements, company IT security policies, and industry standards.
- The uptime and process safety needs of Manufacturing Operations **and** the discipline and rigor of IT Security should be included in the Program.
- Common ICS cyber security gaps that need to be addressed include:
 - Hardening operating systems
 - Locking down removable media ports
 - User account and password management
 - File transfer security

Case Study: ICS Cyber Assessments for a Global Chemical Company

- Client Challenge

- Their manufacturing plants were slow to respond to Cyber Security requirements, resulting in unknown (assumed high) cyber risk and CFATS compliance issues

- Client Call to Action

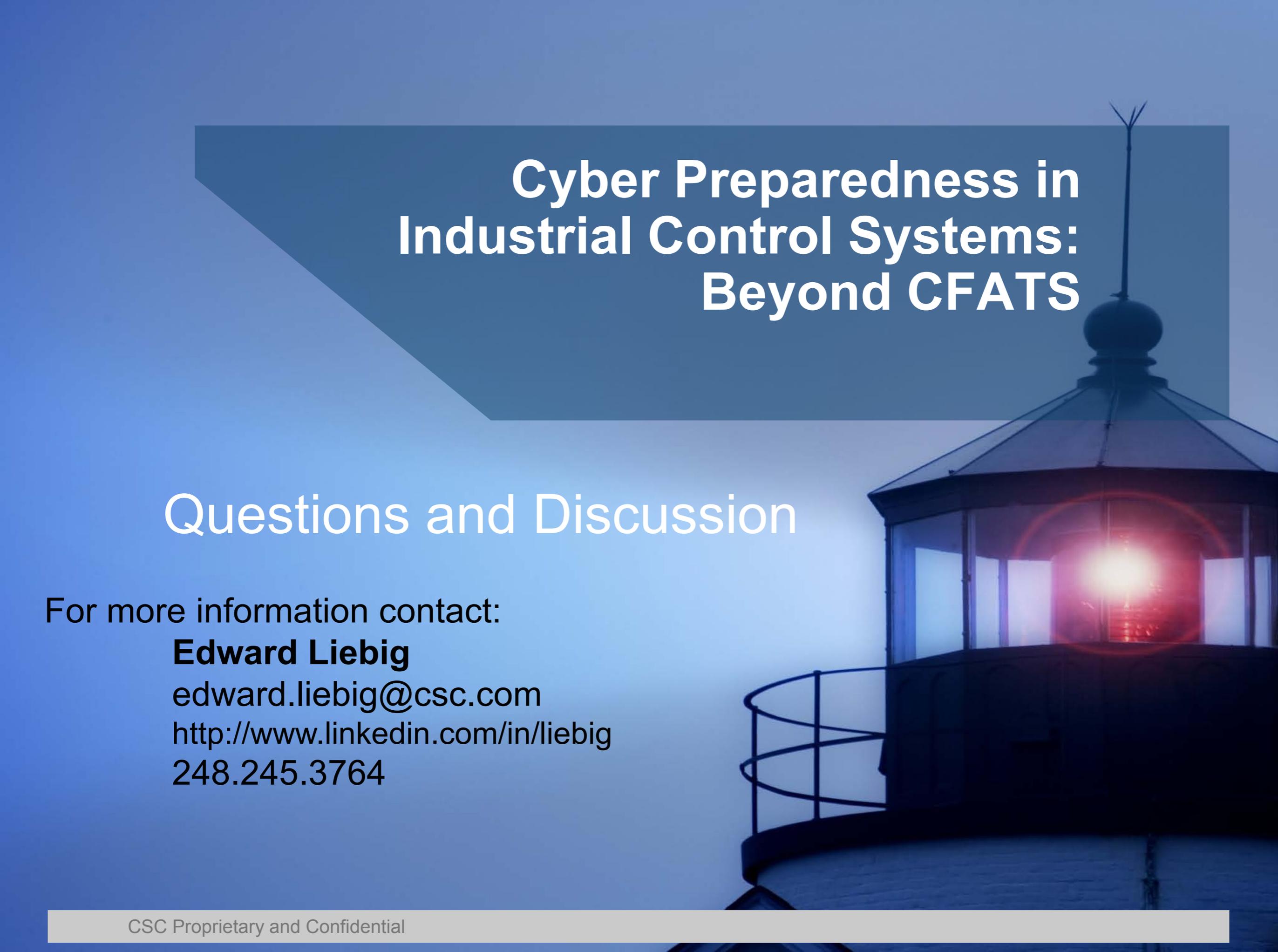
- DHS announced CFATS Site Security Inspections were commencing in the 2nd Half of 2010; this impacted 30+ manufacturing sites for this client.
- Senior Operations Executives requested a report on the cyber risk to manufacturing operations and an estimate of cost to reduce the risk.

- CSC Solution

- Plant Cyber Security Assessments for the plant sites (using CFATS sites as a priority), combining CSC's deep domain knowledge in Chemical Manufacturing Systems with world-leading Cyber Security expertise to lead the plants in delivering:
 - Consequence-based risk assessment of all plant Automation and Control Systems
 - Gap Analysis of the plant systems' cyber security vs required (regulatory and policy based) standards
 - Remediation Roadmap with cost estimates to close the identified gaps

- Client Value delivered:

- Complete Risk Assessment & Remediation Plans to meet Security Policy and CFATS requirements.
- Clear understanding of risk to Manufacturing Operations across key plants.
- Comprehensive approach to rolling out Plant Cyber Security Standards globally.



Cyber Preparedness in Industrial Control Systems: Beyond CFATS

Questions and Discussion

For more information contact:

Edward Liebig

edward.liebig@csc.com

<http://www.linkedin.com/in/liebig>

248.245.3764