Introduction to Securing Critical Infrastructure

Keith Frederick
CISSP, CAP, CRISC, Author

securenok.com
Topics

• Attacks on the Oil and Gas Industry.
• Executive Order 13636 (February 12, 2013).
• Presidential Directive 21 (February 12, 2013).
• Cybersecurity Framework (February 12, 2014).
Evolution of Cyber Attacks

1998: MORRIS (First Internet Worm)

2000: IDENTITY THEFT (Malware, Phishing)

2003: WORMS (Worst worm year)

2007: WEB WAR 1 (DDoS attack on Estonia over three weeks)

2011: FLAME DUQU (Cyber espionage)

2015: Power Blackout? Oil/Gas pipeline explosions?

1999: MELISSA (I love you, Minda, Slammer, Blaster, SoBig, MyDoom)

2002: DDOS (First successful attack against critical infrastructure)

2004: BOTNETS (Attacks change and becomes more hidden)

2010: STUXNET (Embedded systems)

2012: GAUSS, SHAMOON
Why the Focus on O&G?

- Energy is fundamental to the nation’s economy and defence and pervasive throughout critical infrastructure.

- Represents the political direction of the government and future war efforts aimed at country/corporate economics.

Hacker ability to take over “Control Systems”.

2014 © Secure-NOK AS, all rights reserved.
Threats to the Energy Industry

• In 2013, 53% of attacks against the critical infrastructure in the United States targeted the “Energy Industry”.
  • **Continues to increase annually.**

• Motivation behind:
  • Executive Order 13636,
  • Presidential Directive 21 (PD-21), and
  • Cybersecurity Framework (CSF).
Executive Order 13636:
Improving Critical Infrastructure Cybersecurity

• Develop a technology-neutral voluntary cybersecurity framework.

• Promote and incentivize adoption of cybersecurity practices.

• Increase the volume, timeliness, and quality of cyber threat information sharing.

• Explore the use of existing regulation to promote cybersecurity.
Presidential Policy Directive 21:
Critical Infrastructure Security and Resilience

• Develop a situational awareness capability that addresses both physical and cyber aspects of how infrastructure is functioning in near-real time.

• Understand the cascading consequences of infrastructure failures.

Update the National Infrastructure Protection Plan.

Evaluate and mature the public-private partnership.
Cybersecurity Framework (CSF)

- The Cybersecurity Framework (CSF) is a living document and will continue to be updated.

- The CSF uses risk management processes to enable organizations to inform and prioritize decisions regarding cybersecurity.

- It supports recurring risk assessments and validation of business drivers.
CSF Overview

- CSF is a risk-based approach to managing cybersecurity risk, and is composed of three parts:
  - The CSF Core,
  - The CSF Implementation Tiers, and
  - The CSF Profiles.

Each CSF component reinforces the connection between business drivers and cybersecurity activities.
CSF Core

• The CSF Core is a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors.

• The Core presents industry standards, guidelines, and practices in a manner that allows for communication of cybersecurity activities.
## CSF Core Chart

<table>
<thead>
<tr>
<th>Function Unique Identifier</th>
<th>Function</th>
<th>Category Unique Identifier</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Identify</td>
<td>ID.AM</td>
<td>Asset Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.BE</td>
<td>Business Environment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.GV</td>
<td>Governance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.RA</td>
<td>Risk Assessment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.RM</td>
<td>Risk Management Strategy</td>
</tr>
<tr>
<td>PR</td>
<td>Protect</td>
<td>PR.AC</td>
<td>Access Control</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.AT</td>
<td>Awareness and Training</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.DS</td>
<td>Data Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.IP</td>
<td>Information Protection Processes and Procedures</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.MA</td>
<td>Maintenance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.PT</td>
<td>Protective Technology</td>
</tr>
<tr>
<td>DE</td>
<td>Detect</td>
<td>DE.AE</td>
<td>Anomalies and Events</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DE.CM</td>
<td>Security Continuous Monitoring</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DE.DP</td>
<td>Detection Processes</td>
</tr>
<tr>
<td>RS</td>
<td>Respond</td>
<td>RS.RP</td>
<td>Response Planning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.CO</td>
<td>Communications</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.AN</td>
<td>Analysis</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.MI</td>
<td>Mitigation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.IM</td>
<td>Improvements</td>
</tr>
<tr>
<td>RC</td>
<td>Recover</td>
<td>RC.RP</td>
<td>Recovery Planning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RC.IM</td>
<td>Improvements</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RC.CO</td>
<td>Communications</td>
</tr>
</tbody>
</table>
CSF Implementation Tiers

• “Tiers” provide context on how an organization views:
  - Cybersecurity risk and
  - The processes in place to manage that risk.

• Tiers describe the degree to which an organization’s cybersecurity risk management practices exhibit.
CSF Implementation Tiers

• The Tiers characterize an organization’s practices over a range, from Partial (Tier 1) to Adaptive (Tier 4).

• These Tiers reflect a progression from informal, reactive responses to approaches that are agile and risk-informed.
CSF Implementation Tiers (continue)

- An organization should consider its:
  - Current risk management practices,
  - Threat environment,
  - Legal and regulatory requirements,
  - Business/mission objectives, and
  - Organizational constraints.
CSF Profiles

• A “Profile” represents the outcomes based on business needs that an organization has selected from the Framework:
  • Categories and
  • Subcategories.

• The Profile can be characterized as the alignment of:
  • Standards,
  • Guidelines, and
  • Practices.
CSF Profiles (continue)

• To develop a Profile,
  • An organization reviews all of the categories and subcategories and,
  • Based on **business drivers** and a **risk assessment**, 
  • Determine which are most important.
CSF Profiles (continue)

- Profiles can be used to identify opportunities for improving cybersecurity posture by comparing:
  - “Current” Profile (the “as is” state) with a
  - “Target” Profile (the “to be” state).
Risk Management and the CSF

• Risk management is the ongoing process of:
  • Identifying,
  • Assessing, and
  • Responding to risk.

• To manage risk, organizations should understand the:
  • Likelihood that an event will occur and
  • The resulting impact.