Continuous Improvement: Supply Chain Risk Management

By Sam Ciccone, Principal Reliability Consultant

The Journey to Security, Resilience and Reliability

"Risk comes from not knowing which cog in your supply chain is in trouble." – Warren Buffett

Supply Chain Risk Management (SCRM) of all assets, cyber and power, is a critical topic in the electric utility industry, as well as almost every industry. The JBS and Colonial Pipeline attacks show how important it is to proactively identify supply chain cyber risks and have a plan to mitigate those risks. Also, the SCRM process must get buy-in from the top. The recent supply chain attacks "demonstrate that your organization needs to make cybersecurity a Boardroom priority, if you haven't done so already."[1]

NERC Standard CIP-013-1 Cyber Security - Supply Chain Risk Management was implemented to "mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems."[2]

As the industry takes additional reliability measures to meet this standard, this article will explore the importance of continuously improving, training on, and maturing your SCRM program.

SCRM DMAIC Continuous Improvement Concept, Process Maturity and SCRM Standards

Supply chains (e.g., cyber, fuel, contractor, etc.) introduce risks due to External Interdependencies (EXID) with third-party products, components and services necessary to maintain grid reliability. The RF maturity model framework defines EXID as "a management practice designed to implement organizational processes to manage external stakeholders, such as suppliers, that may impact grid reliability and resilience."[3]

Best practices include activities, such as identifying and assessing risks, entailing both existing and emerging risks being identified and assessed with fully quantitative impact analysis. Another EXID activity is to mitigate the risks identified and assessed with best practices that include performing internal audits or third-party assessments of the interdependencies.

Additionally, there are more general frameworks you can familiarize yourself with, such as the Capability Maturity Model (CMM),[4] ISO 9001, Common Criteria, and SOC 2. There also is an accreditation you can achieve for Certified Supply Chain Professional (CSCP) provided by the Association for Supply Chain Management.[5]

Standards and SCRM Maturity

Several industry Standards are a great resource for SCRM maturity. NIST Special Publication 800-161, "Supply Chain Risk Management Practices for Federal Information Systems and Organizations," describes the four critical system level domains in SCRM[6]:

- Frame – Define system-level SCRM requirements
- Assess – Conduct SCRM Risk Assessment, including Criticality Analysis for individual systems and determine current risk posture
- Respond – Select, tailor and implement appropriate system-level controls, and document SCRM controls in System Security Plan

[1] https://www.industryweek.com/technology-and-iiot/article/21165692/hackers-getting-hooks-into-crucial-supply-chains
[2] https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-013-1.pdf
[3] https://rfirst.org/KnowledgeCenter/Risk%20Analysis/InternalControls/Assessments/Management%20Practice%20Abstracts.pdf
[4] https://resources.sei.cmu.edu/asset_files/TechnicalReport/2010_005_001_15287.pdf
[5] https://www.ascm.org/learning-development/certifications-credentials/cscp/
[6] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf

Continued on page 5

Continuous Improvement: Supply Chain Risk Management

Continued from Page 4

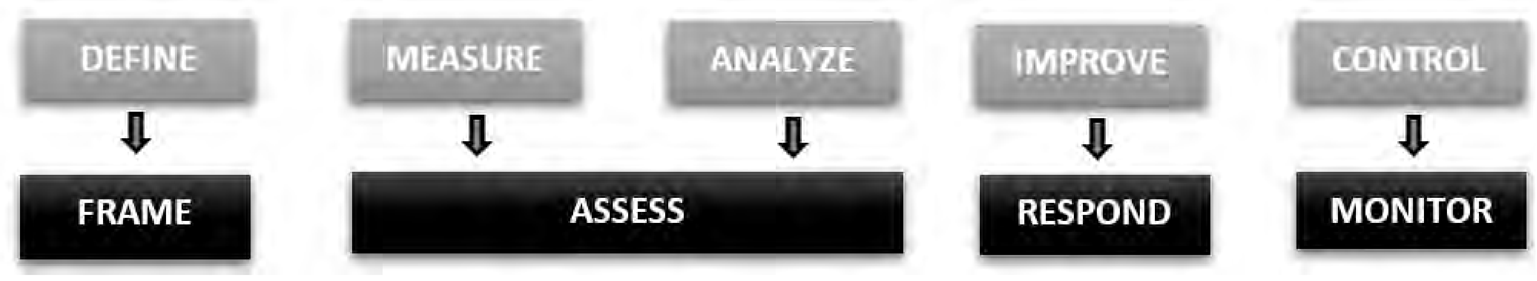
- Monitor – Monitor and evaluate system level requirements and risks for change and impact, and Monitor effectiveness of system level risk response

Entities are encouraged to review this standard and apply the framework for their SCRM maturity.

DMAIC Continuous Improvement Concept

DMAIC, (pronounced “dah-may-ik”) is a “Six Sigma data-driven process improvement framework that … was developed to guide manufacturers in their efforts to minimize defects and improve quality performance for existing business processes. DMAIC is rooted in the Plan-Do-Check-Act cycle and is a core project methodology used to drive Six Sigma project results”[7]. Following each phase of DMAIC described below can improve your SCRM process:

- Define – Define your Supply Chain goals
- Measure – Measure the performance of your SCRM process with KPIs
- Analyze – Analyze relevant data to determine areas for improvement in your SCRM process
- Improve – Determine solutions to fix and prevent issues in the SCRM process
- Control – Ensure improvements keep the SCRM process on course



The Connection

The DMAIC Continuous Improvement (CI) process improvement concept can be mapped to the NIST 800-161 maturity domains Frame, Assess, Respond and Monitor as follows:

Utility Case Study – Cyber Supply Chain

An example of supply chain risks in the utility industry involves SCADA and Industrial Control Systems. “SCADA systems are increasingly under attack, illustrating a growing vulnerability in the electricity grid. To better secure the power sector, organizations must: 1) anticipate the evolution of SCADA functionality and deployment; 2) understand the supply chain risks they face; and 3) take proactive measures to mitigate these risks.”[8]

To mitigate SCADA and other critical utility infrastructure supply chain risks, a utility industry entity implemented a Cybersecurity SCRM process that focuses on the following:[9]

- Addresses supply chain risk through extended definition of supplier, including the entire supply chain ecosystem of vendors and their suppliers, service providers and third parties

- Cross-functional vendor management including supply chain, security, legal and IT representatives to assess contract terms and conditions and ensure that appropriate contract controls are in place

- Use of vendor security questionnaires related to vendor cyber supply chain policies, process and controls

- Adoption of specific security control and audit provisions in vendor contracts

[7] https://www.industrystar.com/blog/2017/03/leveraging-six-sigma-dmaic-solve-supply-chain-challenges/

[8] https://www.odni.gov/files/PE/Documents/11---Supply-Chain-Risks-of-SCADA-Industrial-Control-Systems-in-the-Electricity-Sector_Risks-and-Mitigations.pdf[

[9] https://protectourpower.org/2020-cyber-risk-report.pdf

Continued on Page 6

Continuous Improvement: Supply Chain Risk Management

Continued from Page 5

We encourage Entities with best practices and lessons learned to engage in discussions with fellow Entities to help each other improve SCRM processes. RF can help with these introductions among Entities.

SCRM E-Learning Module

Humans are important assets in SCRM, and ongoing training and education helps reduce risks. A SCRM case study on DuPont shows that "one of the unique aspects of the DuPont transformation was its focus on people. A core tenet of the program was that people are simultaneously the key barriers and key enablers of the new culture of excellence needed to cope with increased global competition and operational risks. DuPont established new training and skills development programs to effect the cultural change and collaborative approaches of the DuPont Production System."[10]

In an effort to train and educate, RF and SERC Reliability Corporation (SERC) partnered to create a CI learning module for SCRM. The module is a good primer for understating CIP-013-1 fundamentals, CI techniques and CI Applications for SCRM. We urge every Entity to review this module at Supply Chain Risk Management: Continuous Improvement Techniques.

Conclusion

To tie this discussion to the quote at the beginning of the article, "be aware that the weakest department within your link and the weakest link in your supply chain will drive performance."[11] SCRM will become more challenging as our global environment evolves and more sophisticated cybersecurity, fuel supply, contractor and other threats emerge. It's critical that you don't become complacent, but instead keep improving as you monitor and mitigate your supply chain risks.

For more information on SCRM, maturity assessments and CI, please contact Brian Thiry, RF Entity Engagement Manager at brian.thiry@rfirst.org. For questions on the e-Learning module, you can contact Banna Underland, SERC Technical Writer & Training Coordinator at bunderland@serc1.org.

[10] https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/case_studies/USRP_NIST_DuPont_071315.pdf

[11] https://multichannelmerchant.com/operations/the-top-10-supply-chain-improvement-strategies/