SAND2015-10232C

Supply Chain Decision Analytics: Application and Case Study for Critical Infrastructure Security

Nathan J. Edwards[1], Gio K. Kao[1], Jason R. Hamlet[1], John Bailon[1], and LTC Shane F. Liptak[2]
[1]Sandia National Laboratories, Albuquerque, NM, USA
[2]U.S. Army Retired (former member of U.S. Strategic Command J6 -- Command, Control, Communications and Computer Systems), USA
njedwar@sandia.gov
gkkao@sandia.gov
jrhamle@sandia.gov
jbailo@sandia.gov

Abstract: Today's globalized supply chains are complex systems of systems characterized by a conglomeration of interconnected networks and dependencies. There is a constant supply and demand for materials and information exchange with many entities such as people, organizations, processes, services, products, and infrastructure at various levels of involvement. Fully comprehending supply chain risk (SCR) is a challenging problem, as attacks can be initiated at any point within the system lifecycle and can have detrimental effects to mission assurance. Counterfeit items, from individual components to entire systems, have been found in commercial and government systems. Cyber-attacks have been enabled by suppliers' lack of security. Furthermore, there have been recent trends to incorporate supply chain security to help defend against potential cyber-attacks, however, we find that traditional supply chain risk reduction and screening methods do not typically identify intrinsic vulnerabilities of realized systems. This paper presents the application of a supply chain decision analytics framework for assisting decision makers in performing risk-based cost-benefit prioritization of security investments to manage SCR. It also presents results from a case study along with discussions on data collection and pragmatic insight to supply chain security approaches. This case study considers application of the framework in analyzing the supply chain of a United States Government critical infrastructure construction project, clarifies gaps between supply chain analysis and technical vulnerability analysis, and illustrates how the framework can be used to identify supply chain threats and to suggest mitigations.

Keywords: Supply chain risk management, supply chain security, risk analysis, decision support systems, security, critical infrastructure

1. Introduction

The United States Government (USG) is dependent on supply chains that are highly complex and geographically diverse, presenting a risk to national security. Modern supply chains are large-scale, globalized conglomerations of interconnected networks. This complexity reduces transparency and visibility into supply chains at every level of involvement, including people, organizations, processes, services, products, and infrastructure. This reduces understanding of how technology and products are acquired, developed, integrated, deployed, and decommissioned. Currently, there is a general lack of visibility, understanding, and control over supply chains.

For example, according to the director of the United States Department of Defense's (DoD) Defense Microelectronics Activity (DMEA), "the defense community is reliant critically on a technology that becomes obsolete every 18 months, and is made in unsecure locations over which the USG does not have market share influence" (Levin 2013). As a result, DoD is limited to utilizing independent distributors and brokers that are highly susceptible to counterfeit threats and malicious subversions. Many DoD supply chains have already been compromised by counterfeit electronic parts, posing a risk to the security and reliability of U.S. defense systems (Levin 2012; Levin 2013). In addition, suppliers' lack of security have enabled cyber attack which have resulted in significant loss (Kassner 2015).

The United States Government Accountability Office found that many USG departments are inadequate in countering the supply chain threat. Lacking are protective measures, policies, and monitoring capabilities to verify compliance with and effectiveness of countermeasures (GAO 2012). Furthermore, the U.S. Department of Commerce (2010) states that electronic manufacturers often do not discover counterfeit parts until after defective parts are returned. Industry is not able to detect counterfeits as the required testing, qualification, and verification requires significant effort (Hanlon 1996; Lebron et al., 2000).

It is extremely challenging to fully comprehend supply chains and their vulnerabilities due to inherent complexities in systems, corporate structures, and distribution networks. These complexities provide attackers opportunities to hide malicious insertions within individual components, assemblies, and systems comprising of entire buildings and facilities; they pose threats that impact confidentiality, integrity, or availability of the end system. Therefore, a supply chain decision analytics framework is needed to support organizations in reducing complexity of identifying and mitigating SCRs.

Section 2 provides a brief survey of related work, and finds that there is a lack of lifecycle focused approaches to manage SCR. We introduce a decision support framework for analyzing supply chains across the system lifecycle in Section 3, and the application of this framework for a military construction project with results from the analysis are presented in Section 4. We also show how the results were used to target specific aspects of the supply chain for a detailed analysis, and present recommendations for reducing the risk of this supply chain. Section 5 provides a brief discussion on challenges and future work, and Section 6 offers conclusions.

2. Related Work and Motivation

2.1 Related Work

Much of the existing national guidance on SCR focuses on information and communication technology (ICT). For instance, NIST released a series of reports that suggest high-level SCR mitigation measures (Boyens et al., 2012; Boyens et al. 2013; NIST 2013). Suggested controls include trusted shipping and warehousing and engaging independent penetration testing teams. These reports do not address detailed SCR analysis which is needed to correlate a system's supply chain and lifecycle to prioritized and optimal mitigation strategies. For example, a recently developed cyber supply chain tool based on NIST guidelines enables construction of a flow-of-goods view of the supply chain and presents the user with a small set of questions about each transaction and node (Boyens et al., 2012; UMD 2015). The answers to these questions are combined with data from the national cyber vulnerability database and are translated into an overall risk score for the supply chain map. The tool has a strong ICT focus but does not consider product lifecycle or optimization of mitigation actions. Another common approach for SCR management (SCRM) is to use data aggregation and analysis tools to collect and categorize information on suppliers so that an analyst can make subjective risk determinations (Palantir 2015).

2.2 Motivation

We find that current SCRM approaches are incomplete and do not provide a holistic lifecycle perspective. Supply chain vulnerabilities exist at every stage of the lifecycle process, from initial development of concepts and requirements through design, procurement, manufacturing and construction, and eventual deployment, operation, sustainment, and decommissioning. Each stage of the lifecycle consists of many process steps and sub-processes which incorporate internal and external actors, information and material flows, and supporting infrastructure. Altogether these elements constitute the supply chain, and any of them can introduce risk and vulnerabilities. In order to reduce risk we must understand processes, vendor and supplier involvement, and supporting infrastructure. We must incorporate material flows, including logistics and supplier networks, and information flows, including business processes and operation, to comprehensively evaluate supply chains. Considering only cyber risks or only analyzing suppliers and vendors is insufficient.

To address these issues we developed a decision support system to enable risk informed cost-benefit prioritization of security investments and mitigation approaches to help manage SCR. We have used this framework to analyze the supply chain of a critical infrastructure system (CIS) under construction by the DoD. The repeatable and structured nature of our process is important because the supply chain problem is large

and complex. It also aids in reducing the complexity of supply chain analysis by reducing the required subject matter expert (SME) input lifecycle activities and processes with which they are already familiar.

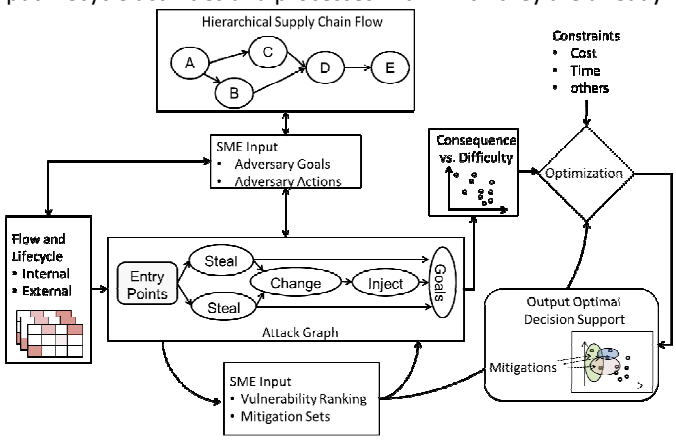

Figure 1: Our supply chain lifecycle decision analytics framework supports gathering and representing the supply chain and lifecycle processes at any level of detail; risk assessment of the process steps, suppliers, and infrastructure in the supply chain; generation of attack graphs to understand potential sequences of adversary actions, and assessment of the difficulty and consequences of each attack graph; and optimal selection of mitigations. In this case study we focus on representing the supply chain, identifying locations that warrant further analysis.

3. Supply Chain Lifecycle Decision Analytics

The goal of our framework is to provide decision-support analytics that enable risk-based cost-benefit prioritization of security investments to manage SCR. Key challenges are the complexity of the end-to-end supply chain lifecycle problem, and the scalability of the supply chain representation. To overcome this complexity we developed a hierarchical decomposition methodology, Figure 1, for examining the supply chain lifecycle. It consists of (1) information-based mapping of the supply chain lifecycle, (2) vulnerability and mitigation modeling, (3) risk assessment via application of difficulty and consequence security risk metrics, and (4) mathematical optimization models that evaluate threats and mitigations based on the security metrics. We leverage a security risk metric based on the difficulty adversaries will encounter when attempting to execute attack scenarios and the consequences of those attacks (Wyss et al., 2010). These metrics enable decision makers to overcome the complexity of quantifying security risk, and are suited for cost-benefit optimization. The methodology enables flexibility to evaluate the supply chain at various depths (e.g., system, sub-assembly, component, etc.), and to leverage each decomposition to address system or enterprise level supply chain vulnerabilities. Additionally, this approach helps identify emergent behaviors and their global effects.

A brief description of the framework is provided below. Section 4 illustrates an example use-case application.

3.1 Supply Chain Mapping

The first component of the framework is supply chain representation. This requires mapping material and information flows across the lifecycle. Our representation is a directed graph that can represent high level flow diagrams to detailed processes, and is scalable based on the level of fidelity provided by SMEs. The purpose of the supply chain mapping is to provide a thorough understanding of the risk associated with the processes, suppliers and infrastructure throughout the supply chain and across the lifecycle.

The mapping includes a high-level risk assessment of the process steps and entities within the supply chain. SCR is partition into a set of eight indicators. These indicators are the amount of *control and influence* over a process step or entity, information and material *exposure*, the *diversity* or redundancy of a process step or entity, the *temporal access* of an entity to the system, *visibility* into a process step or entity, the *rapport* between the system owner and entity, and the *reputation* and *financial strength* of an entity. Moreover, we have developed an assessment protocol to aid analysts in assessing each indicator. For each indicator we developed a series of qualitative and quantitative questions that can be easily answered for assessing the risk

from the category and can accommodate varying levels of detail. At this level, we can begin to identify risk of individual process steps and entities, and identify locations of elevated risk based on relative scores. Elevated risk scores also identify appropriate locations in the supply chain for detailed analysis. Additionally, the structure of the directed graph helps us to identify nodes where there is a convergence of information or materials.

3.2 Vulnerability and Mitigation Modeling

The second component of the framework, vulnerability and mitigation modeling, provides a structure for analysts to systematically identify potential vulnerability insertion points. Once the insertion points are identified, SMEs can develop attack scenarios based on adversary goals. However, this type of vulnerability assessment can be highly subjective and the supply chain vulnerability space is far too large for manual analysis to provide comprehensive coverage. To streamline SME effort and reduce subjectivity of red-teaming based attack path generation, we developed a functional ontology describing both adversary and mitigation actions within the supply chain. The ontology consists of a set of actions that can be applied to each node of the directed graph. As an example, an adversary can acquire (action) the product design (object) at the design house (location). Sequences of these (action, object, location) triplets form attack graphs. This ontology allows generation of attack scenarios represented by directed graphs which enables more comprehensive representation of the attack surface. Ultimately the ontology encapsulates the problem into manageable elements.

Mitigation actions can be evaluated in a similar manner. By generating and representing attack scenarios and mitigation options in this manner, we free analysts from having to manage individual vulnerabilities and empower them to analyze the supply chain holistically and comprehensively. This may help them to identify mitigation strategies that address multiple vulnerabilities, for example, by identifying nodes that appear in multiple attack scenarios.

3.3 Risk Assessment

Risk assessment consists of ranking and prioritizing the vulnerability space generated in the vulnerability and mitigation modeling component. We leverage a risk assessment methodology that enables evaluation of attack scenarios based on difficulty and consequences (Wyss et al., 2010). Mapping the attack scenarios to the difficulty and consequences space further enables optimization techniques for risk-based cost-benefit decision analysis.

3.4 Optimization

The fourth part of the framework, optimization, enables prioritization of mitigation strategies while our risk assessment methodology enables ranking of the attack scenarios. The objective of the optimization problem is to find optimal mitigation strategies for the attack space generated by the vulnerability modeling subject to various constraints such as cost, time, and capabilities. Kao et al (2014) provides a more detailed discussion of this framework.

In this case study, we focus our analysis on high-level risk assessment mapping of the supply chain. Using the mapping we identify locations warranting in-depth analysis, and identify structures in the supply chain that are good candidates for applying mitigations. We then perform a detailed technical analysis of a small collection of products found within the supply chain.

4. Case Study

4.1 Scope

As described in Section 3, the main purpose of the framework is to provide effective SCR decisions analysis and to select mitigations to satisfy organizational constraints. We use this decision analytics framework to analyze the supply chain of a DoD critical infrastructure system under construction, highlight the complexities of SCR, and give examples of how to address the challenges of applying SCRM for national security.

Many SCRM approaches are applicable only to early stages of procurement or engineering efforts (e.g., initial contract, qualification) with the assumptions that a good screening process provides a more secure system. This case study highlights the applicability of the framework when the supply chain and contracts have already been established, and the limitation of supplier screening. In this case study, the construction project was well underway – equipment vendors and contractors were already selected before our team was engaged. In particular, this study identified the need for SCRM approaches to accommodate for operational security issues that are introduced by well-screened original equipment manufacturer (OEM) within trustworthy supply chains and during post-contract support or later in a system's lifecycle.

We analyze the supply chain lifecycle and identify weaknesses or vulnerabilities where an adversary might have opportunity to affect the fielded product. Our analysis includes business entities and relationships, the federal contracting process, pre-bid information distribution processes, company and personnel screening processes, OEM hardware equipment and software, network and protocol implementations, engineering and integration processes, and critical infrastructure industry practices.

4.2 Data Collection

We acquired much data through document collection and on-site interviews since the framework's focus is to identify vulnerabilities in the supply chain and lifecycle. In particular, our data collection included DoD information controls used for the Request For Information (RFI) and contract process, construction site controls, contractor knowledge of facility mission, manufacturer knowledge of component end-use, manufacturer quality and procurement practices, hardware and software components, and military construction (MILCON) program testing and acceptance processes. During a construction site visit we met with the government program management office (PMO), government oversight teams, prime contractors, subcontractors, and system integrators to understand the current state of the program, supply chains, and entities involved in the large construction effort.

Additionally, we engaged with MILCON security representatives and the responsible DoD Civil Engineering Center to better understand the process for security testing and verification of the system. The civil engineering unit applies a battery of security tests and provides the recommendation for an Authority to Operate. It also provides early feedback on the security of specified equipment.

To validate use of the framework and to acquire detailed risk data, we procured equipment and integration engineering services similar to that specified for the DoD facility and constructed a test system. This provided opportunity to apply our detailed SCRM risk indicator protocol, an extensive questionnaire similar to that described by Lin et al. (2012), and validate its applicability for establishing the SCRM risk metrics used in the framework. Through procurement we better understood practices within industry and OEM specific configuration details of interested equipment. Furthermore, we gain insights to the OEM's manufacturing quality control, supply chain, and customer data collection practices.

We compiled the large data set into a directed graph of material and information flow, representing the supply chain lifecycle for this construction process. Using the graph we were able to identify key weaknesses in the supply chain and system integration process (Figure 2).

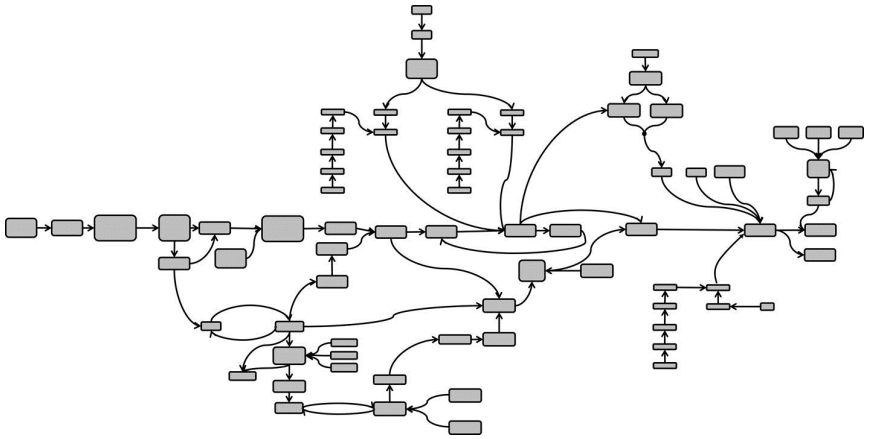

Figure 2: An illustration of the supply chain representation and flow for the entire CIS construction and commissioning process. 104 process steps or entities within the supply chain were identified, highlighting its complexity. Although not shown in this diagram, the color of the nodes can be used to represent level of potential risk.

The SCRM system-level analysis led us to conduct an in-depth analysis on the OEM hardware equipment, software, network and protocol implementations. This deep-level analysis identified integrated circuits, circuit board designs, software, network equipment, and included other traditional vulnerability assessment data to provide a holistic view of the CIS system lifecycle security risks.

Note that while the collection of specific data can be different for each system analysis, the approach is the same: identify the process, entities, and artifacts dependencies, complete assessment questionnaires, evaluate risk, and perform deep dive where appropriate and possible.

4.3 Results

Our data collection identified operational processes, entities, and supporting infrastructure of the DoD program. The business characteristics, operational practices and process steps of the various entities were evaluated through 24 questions categorized into eight indicator categories of SCR. For each question we assign lower and upper bounds for each entity's score, allowing us to accommodate for uncertainty in the responses. We transform the entity's responses into risk scores by normalizing the response of each question to the maximum reported responses to those questions. This provides a relative scoring of risk. Then, individual scores are combined with a weighted average to determine an overall risk score, as shown in Figure 3.

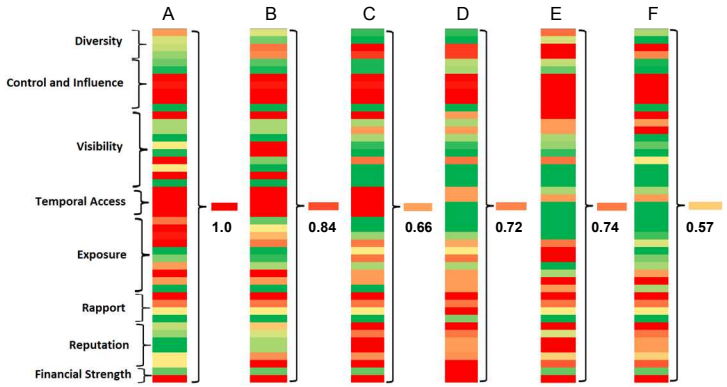

Figure 3: The SCR indicators heatmap for various entities and their overall relative risk score. In this example, each column represents various DoD contractors that have some impact on the CIS system. The questions are grouped by indicators. Adjacent bands indicate upper and lower bounds of the risk from a single question. Adjacent bands of opposite color indicate a lack of information whereas adjacent bands of similar color indicate high confidence in the information. An average of the scores provides an overall risk score for the entity.

Note that these SCR scores are relative scores among the entities in question; the values themselves are less important than the ordinal comparison which provides analysts a way to evaluate areas of higher risk. It is also noteworthy that independent risk scores can be highly subjective, and establishing baselines for such scores can be extremely difficult.

Figure 4 provides another perspective of the data in Figure 3 by plotting the risk score for each indicator. This view allows analysts to quickly make determinations on specific risks, whether to collect more information or potentially work with a supplier to improve their risk posture.

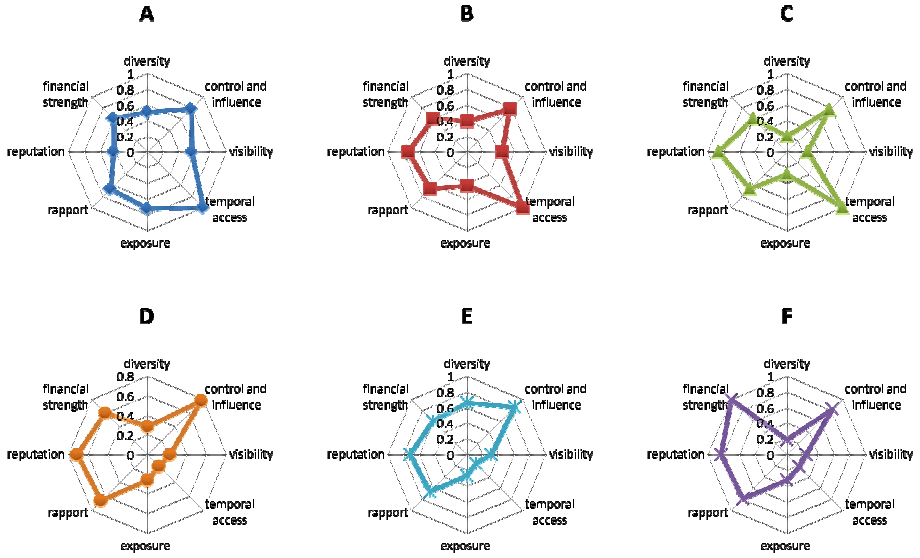

Figure 4: The SCR for entities A through F with each indicator showing magnitude of risk. Larger areas and indicator values further from the center imply greater SCR. This chart allows analysts to more easily identify and better characterize supplier risk. This represents the same data as Figure 3, but emphasizes risk from individual indicators.

Supply chain weaknesses and vulnerabilities can exist at any stage of a system's lifecycle. Our analysis can identify critical nodes in the supply chain for the CIS. For example, there are areas in the supply chain where several predecessor nodes in Figure 2 converge into single nodes. These aggregation points indicate important, potentially high-risk nodes. Large edge density in the supply chain graph indicates complexity and potentially suggests more risk. The convergence also indicates that a detailed analysis of the node is warranted and identifies it as a potential location for applying mitigations to have broad impact in reducing SCR.

Since the decision to analyze the SCR of the DoD system occurred well after contracts were awarded, the opportunity to apply early-stage mitigations was significantly reduced, and many late-stage mitigations would add significant cost and delays to the construction program. Ultimately, late-stage supply chain analysis emphasizes the importance of operational system security characterization followed by comprehensive acceptance testing with detailed cybersecurity plans. The high level analysis of Subsections B and C helped to identify components for this more detailed analysis, which is presented in the following section.

4.4 Further Analysis

We determined that the components, communications, and protocols used in the CIS meet national standards specifications. However, the OEM implementations of the specifications, and proprietary extensions, create vulnerabilities.

Our analysis begins with identifying the hardware and software technologies used in the control system. We checked for signs of illegitimacy, poor quality, and opportunities within the supply chain or quality processes for malicious adversary insertions. Overall, our analysis revealed that the OEM had high regard for quality and reliability, and manufactured most assemblies in-house. The OEM's quality process evaluates suppliers on quality, cost, service, and capability, and allows insertion of equivalent components or specified components

from qualified alternate suppliers. The use of alternate suppliers is one of the key risk areas identified by the U.S. Department of Commerce (2010). While the OEM had a reasonable process for selecting and qualifying suppliers and components, qualification was only performed once using a cost-driven model. Other security factors, periodic sampling and audits were not considered.

We partially validated the output of the OEM quality system with deep hardware and software inspection. In the devices we observed many complex programmable logic devices, ARM processors, and other commercial off the shelf (COTS) components that affect the digital data flow and controls. Using standard COTS reliability screening technology such as x-ray imaging, the ICs appeared to be consistent across packages, suggesting that their lineages are from single sources. This does not necessarily rule out grey or black market components, but it does suggest the OEM has processes that allow for some traceability back to the manufacturers. Analysis of the system's software included embedded firmware, programmable logic, Windows CE applications, human machine interface (HMI) workstation, and general Windows operating system applications, which did not produce any significant findings. Using open-source or COTS software designed to interact with the system's network protocol, we observed that the OEM fully implemented the protocol standard. However, similar to many other vendors, we observed a large number of proprietary extensions and data objects.

4.5 Gaps Between SCR and Technical Vulnerability Analysis

Security characterization of the working test system revealed that system behavior, proprietary protocol implementations, and other extensions lead to a number of operational weaknesses and vulnerabilities of the system. This highlights the fact that even with good SCR reduction, system implementations must be considered in securing a system. Initial risk might be mitigated through SCR reduction or during initial commissioning of a system; however CIS typically operate for several decades and are serviced on a regular basis. Mitigations for contemporary security challenges may not be applicable in the future, and SCR should be monitored continuously. The system lifecycle must be considered in the overall risk analysis.

From our detailed analysis, one recommendation for reducing risks introduced from the CIS supply chain is to apply cybersecurity best practices such as network security and monitoring, including out of band monitoring, and establishing stringent procedures for system upgrades, security testing, and audits.

Additionally, this case study offers a pragmatic perspective on three aspects of supply chain security: criticality analysis, threat analysis, and mitigation courses of action (COA). Criticality analysis prioritizes some risks, but our results show that it is also important to understand the overall supply chain and system risks. Threat analysis and mitigation options often focus on procurement, supplier analysis, and components testing. Screening does not account for future risks or threats introduced during operation and maintenance. System hardening should be routine to reduce risks throughout the system lifecycle. Finally, guidelines for mitigation COAs need to consider the cost-benefit of SCR throughout system lifecycle. This is especially true for existing programs where SCRM analysis is performed in later stages of the lifecycle when it can be costly to implement some mitigation options.

5. Challenges and Future Work

A key challenge of SCRM is the difficulty of collecting accurate and useful data. Some approaches use online information, Dun and Bradstreet reports, or systems similar to Palantir's product. However, experience from this case study reveals that these results were sometimes inaccurate or outdated, and more importantly did not correlate with the operational security issues identified by our SCR indicators. Consequently, supply chain security approaches cannot rely solely on such data.

Additionally, government entities are constrained by fair business opportunity regulations and may not be able to interact with potential suppliers or collect detailed SCR information prior to issuance of RFIs or contracts. Even when such provision were requested, this case study identified that some suppliers have loose interpretation of the requested information, which reduces data quality, while others choose not to respond at all. Ultimately, the lack of information could potentially result in lower-quality suppliers with additional security risks to the system.

Another industry accepted approach to gain detailed supplier information is through non-disclosure agreements (NDAs). This case study identified that some suppliers are not willing to establish NDAs unless there exist significant financial incentives or established contracts. In addition, NDA does not oblige the supplier to disclose any information for SCR assessment.

Regardless, the challenges of collecting accurate data can be overcome. Establishing professional and courteous business relationships with suppliers can be more effective than formal information request processes. Such relationships must still be mindful of laws, procurement regulations, and operational security concerns of the end system.

The work presented in this paper only illustrates only part of our decision analytics framework. Future work will include application of the complete framework to additional case studies. Future work will include applying the framework within small business constraints, and addressing regulations such as Buy America Act and other trade laws.

6. Conclusion

This paper provided a brief description of a systematic supply chain decision analytics framework that enables holistic understanding of SCR, including vulnerabilities across the system lifecycle. We introduced a risk assessment methodology that evaluates internal and external entities, processes, supporting infrastructure, and other elements of the supply chain with a collection of risk indicators. Relative evaluation of the supply chain elements against each other via these indicators allows high-level, visual risk assessment with heat maps, and also permits analysis of the risk contributions from individual indicators using spider charts. This framework aims to help decision makers perform risk informed cost-benefit prioritization of security investment and mitigation approaches to manage SCR. We have successfully applied part of this framework, namely supply chain mapping, risk evaluation, and vulnerability assessment, to a DoD CIS project case study.

We have shown that this framework is effective at various stages of the system lifecycle. In particular, this analysis occurred during the development phase of the CIS project. The assessment results identified areas of immediate risk and provided a high-level comparison across entities. Furthermore, it helped focus the analysis towards areas where further in-depth studies were needed.

As part of the data collection and information mapping of the supply chain lifecycle, we validated the use of SCRM questionnaires for supplier screening. We also found that establishing relationships with vendors seems to be more fruitful in collecting valuable SCR analysis data than other methods, as it lends itself to pragmatic risk reduction methods.

This case study clarified gaps between SCRM practices and operational security. We found that most SCRM guidelines do not account for systems that lack security options. Many SCR reduction methods would not likely identify or block an adversary from operating within normal specification of the system. Existing supply chain security practices do not holistically address security risk, especially for CISs that operate for several decades. This framework helps enable government and industry to make decisions concerning SCR, and to help them select mitigation approaches including technical vulnerability analysis and system security testing. Ultimately, our analysis of this case study highlights that a system's security has strong dependencies between supply chain security and traditional cybersecurity practices.

Acknowledgement

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND2015-XXXX.

References

Boyens, J. et al. (2012) “Notional SCR management practices for federal information systems.” (NISTIR 7622). [online] http://dx.doi.org/10.6028/NIST.IR.7622.

Boyens, J. et al. (2013) “SCR management practices for federal information systems and organizations.” (NISTSP 800-161). Initial Public Draft.

Hanlon, J.T. (1996) “The Future of Components for High Reliability Military and Space Applications,” Sandia National Laboratories

Kao, G. et al. (2014) "Supply chain lifecycle decision analytics." *Security Technology (ICCST), 2014 IEEE International Carnahan Conference on*. IEEE

Kassner, M. (2015) “Anatomy of the Target data breach: Missed opportunities and lessons learned” ZDNet Security and Privacy: New Challenges [online] http://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/

Lebron, R.A., Rossi, R., and Foor, W. (2000) “Risk-Based COTS Systems Engineering Assessment Model: A Systems Engineering Management Tool and Assessment Methodology to Cope with the Risk of Commercial Off-the-Shelf (COTS) Technology Insertion During the System Life Cycle,” *Strategies to Mitigate Obsolescence in Defense Systems Using Commercial Components*, Budapest, Hungary.

Levin, C. et al. (2012) “Inquiry into Counterfeit Electronic Parts in the Departement of Defense Supply Chain”, Committee on Armed Services United States Senate. [online], http://www.gpo.gov/fdsys/pkg/CRPT-112srpt167/pdf/CRPT-112srpt167.pdf

Levin, C. U.S. Senator of Michigan. (2013) “Background memo: Senate armed services committee hearing on counterfeit electronic parts in the DoD supply chain.” [online], http://www.levin.senate.gov/newsroom/press/release/background-memo-senate-armed-services-committee-hearing-on-counterfeit-electronic-parts-in-the-dod-supply-chain

Lin, H. et al. (2012) “Leveraging a Crowd Sourcing Methodology to Enhance Supply Chain Integrity”. *Proceedings of 2012 IEEE International Carnahan Conference on Security Technology (ICCST)*

National Institute of Standards and Technology (2013). “Security and privacy controls for federal information systems and organizations.” (NIST SP 800-53r4).

Palantir (2015) [online] https://www.palantir.com/

UMD (2015) “CyberChain”. [online], https://cyberchain.rhsmith.umd.edu/

U.S. Government Accountability Office (GAO) (2012) “IT supply chain: National security-related agencies need to better address risks.” (GAO-12-361), [online], http://www.gao.gov/assets/590/589568.pdf

U.S. Department of Commerce, Bureau of Industry and Security Office of Technology Evaluation (2010) “Defense Industrial Base Assessment: Counterfeit Electronics”

Wyss, G. et al. (2010) “Risk-based cost-benefit analysis for security assessment problem.” In Security Technology (ICCST), *2010 IEEE International Carnahan Conference on*, IEEE