SAND2015-2587C

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

Nathan J. Edwards, *Member, IEEE*, Gio K. Kao, *Member, IEEE*, Jason R. Hamlet, *Member, IEEE*, and John Bailon, *Student Member, IEEE*
Sandia National Laboratories
Albuquerque, NM, USA 87123
Email: {njedwar, gkkao, jrhamle, jbailo}@sandia.gov

LTC Shane F. Liptak
J673 Cybersecurity Branch Chief
Supply Chain Risk Management Program Manager
U.S. Strategic Command, Offutt AFB, NE, USA 68113
Email: shane.f.liptak.mil@mail.mil

***Abstract*— Today's globalized supply chains are extremely complex. They are systems of systems and 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, sources, products, and infrastructure at various level of involvement. Fully comprehending supply chain risk is a very challenging problem as supply chain attacks can be initiated at any point within the product or 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. This paper overviews a supply chain decision analytics framework that will assist decision makers and stakeholders in performing risk-based cost-benefit prioritization of security investments to manage supply chain risk, and presents results from a case study along with discussions on quality data collection and pragmatic insight to approaches in supply chain security. This case study considers application of the framework to analyzing the supply chain of a United States Government critical infrastructure construction project, and illustrates how the framework can be used to identify supply chain threats and suggest mitigations for addressing those threats.**

***Index Terms*—Supply chain risk management, supply chain security, risk analysis, decision support systems, security, integrity, critical infrastructure**

I. Introduction

The United States Government (USG) is dependent on supply chains that are highly complex and geographically diverse which presents a risk to national security. Modern supply chains are large-scale, globalized conglomerations of interconnected networks. This complexity reduces transparency and visibility into the supply chain at every level of involvement, including people, organizations, processes, services, sources, products, and infrastructure. This reduces understanding of how technology and products are acquired, developed, integrated, and deployed. 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" [5]. 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 the reliability of U.S. defense systems [5].

The United States Government Accountability Office (GAO) issued a report which found that many USG departments, including the DoD and the Department of Homeland Security (DHS), are inadequate in countering the information technology (IT) supply chain threat. Lacking are protective measures, policies to address the threat, and monitoring capabilities to verify compliance with and effectiveness of any counter measures [4]. Furthermore, the U.S. Department of Commerce states that manufacturers of electronic subsystems often do not discover counterfeit parts [10]. Rather, they are discovered primarily after the parts had been returned as defective. Industry simply does not have the capability (staff, equipment, processes, or budget) to detect counterfeits as the required reliability testing, qualification, and verification requires a large effort [11][12].

It is extremely challenging to fully comprehend supply chains and their vulnerabilities due to inherent complexities in systems, corporate structures, and distribution networks. Examples include the number of unique components in a system and the complexity of the components themselves; difficulty in identifying suppliers and sub-suppliers and their processes; understanding internal processes and how they interact with external suppliers; and understanding the material and information flows to and from outsourced vendors (including a vendor's internal processes.) This complexity impacts all aspects of systems and possibly provides more adversarial opportunities to hide a malicious insertion: from individual components, to the assemblies and systems composed of these components, to systems-of-

systems and entire buildings and facilities. Owing to this complexity, a supply chain decision analytics framework is needed to support system owners and decision makers to identify and mitigate supply chain risks.

Supply chain vulnerabilities pose threats ranging from quality issues, such as counterfeits that impact the reliability of the end system, to malicious actions by sophisticated actors with intent on compromising the confidentiality, integrity, or availability of end systems.

Section II provides a brief survey of related work. We find that there is a lack of lifecycle focused approaches to supply chain analysis, which is part of the motivation for our efforts. We introduce a decision support framework for analyzing supply chains across the system lifecycle in Section III, and the application of this framework for a military construction project and results from the analysis are presented in Section IV. In addition, we show how the results were used to target specific aspects of the supply chain for a detailed analysis. We also present recommendations for reducing the risk of this supply chain. Section V provides a brief discussion on challenges and future work, followed by the conclusion in Section VI.

II. Related Work and Motivation

A. Related Work

Much of the existing national guidance for addressing supply chain risk focuses on information and communication technology (ICT). For instance, NIST has released a series of reports that suggest high-level supply chain risk mitigation measures [1]-[3]. Suggested controls include guidelines such as using trusted shipping and warehousing, and also engaging independent penetration testing teams. These reports do not indicate how one should analyze and prioritize deployment of mitigations or how best to map a system's supply chain and lifecycle to support supply chain risk analysis. For example, a recently developed a cyber supply chain tool based on some of the NIST guidelines [1][6], permits construction of a flow-of-goods view of the supply chain which aids in mapping a product's prominence and presents the user with a small set of questions about each transaction and node. The answers to these questions are combined with data from the national vulnerability database for assessing cyber vulnerabilities and are translated into an overall risk score for the resulting cyber 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 supply chain risk management (SCRM) is to use data aggregation and analysis tools to collect and categorize information on suppliers and vendors [7] so that an analyst can make risk determinations.

B. Motivation

We find that most of the 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 a concept and requirements through design, procurement, manufacturing and construction, and eventual deployment, operation, sustainment, and decommissioning. Each stage of this lifecycle consists of many process steps, each of which contains sub-processes, and each of these incorporates 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 need to understand processes, vendor and supplier involvement, and supporting infrastructure. We must incorporate both 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 have developed a decision support system to enable decision makers to perform risk informed cost-benefit prioritization of security investments and mitigation approaches to help them manage supply chain integrity and risk. We have used this framework to analyze the supply chain of a new critical infrastructure system (CIS) under construction by the DoD.

Our framework provides a repeatable and structured process for capturing and representing complex supply chains across the system lifecycle, and accommodates both material and information flows. The repeatable and structured nature of our process is important because the supply chain problem is too large and complex. Budget constraints often limit the analysis and effectiveness of mitigation strategies to be developed, analyzed, and deployed without a formal approach for understanding the problem. Additionally, this further aids in reducing the complexity of supply chain analysis by reducing the required SME input to the knowledge of lifecycle activities and processes with which they are already familiar.

As part of our framework, we have developed a generalized approach for analyzing risk within supply chains. This approach evaluates risk along a number of distinct categories discussed in Section III, and can be used to characterize suppliers, processes, and infrastructure. By organizing the risk assessment along these dimensions we can evaluate the risk of any entity or element in the supply chain using information at any level of detail that is available. This permits a hierarchical approach to the analysis and allows us to perform more detailed analyses of selected portions of the supply chain without requiring the same level of detail in other portions. For example, after an initial supply chain mapping and high-level risk analysis, we can identify critical portions of the supply chain that warrant a more thorough analysis. For instance, a node in the supply chain where many information or material items converge may indicate that a detailed analysis of the risk at that node is warranted.

This hierarchical approach not only reduces the amount of information that must be collected and the SME effort required for collecting it, but it also reduces the cost of the analysis. Furthermore, it helps to identify areas where data might be either unavailable or unnecessary for analysis. The hierarchical supply chain and lifecycle process mapping is then used to identify weaknesses and potential vulnerabilities in the supply chain. For instance, it can help identify locations where information loss occurs; bottlenecks where there is a convergence of information or materials (i.e. indicating potential high-risk locations); and nodes where testing or evaluating materials may be most helpful. Weaknesses in the

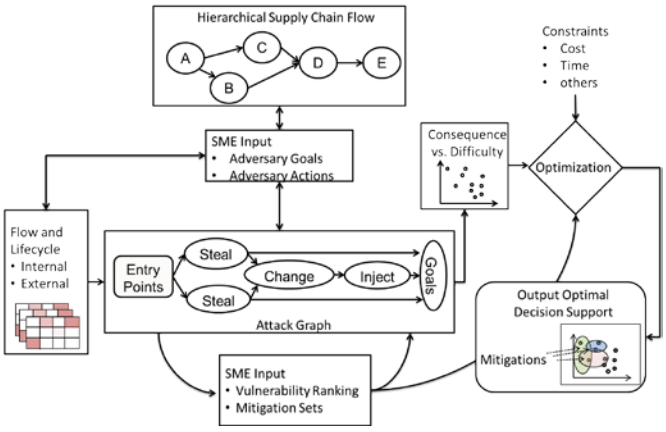

Fig. 1. Our supply chain lifecycle decision analytics framework supports gathering and representing the supply chain and lifecycle processes at any level of detail; risk assessment of the process steps, suppliers, and infrastructure in the supply chain; generation of attack graphs to understand potential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

supply chain must be understood in order for effective mitigations to be easily identified. Our framework helps decision makers understand their complex supply chains, allowing them to deploy mitigations with confidence and with a defensible basis for why particular mitigations were selected.

III. Supply Chain Lifecycle Decision Analytics

The goal of our framework is to provide a decision-support analytics that enables decision makers to perform risk-based cost-benefit prioritization of security investments to manage supply chain integrity and risk. The 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 for examining the supply chain lifecycle. The decomposition, illustrated in Fig. 1, consists of (1) information-based mapping of the supply chain lifecycle and flow representation, (2) vulnerability and mitigation modeling, (3) risk assessment via application of difficulty and consequence security risk metrics that can be used to evaluate vulnerabilities throughout the supply chain lifecycle, and (4) solving mathematical optimization models that evaluate threats and mitigations based on the security metrics. This approach systematically examines the lifecycle phases of supply chains and assesses risk using various metrics including the leveraging of a security risk metric based on the degree of difficulty an adversary will encounter when attempting to execute attack scenarios [8]. These metrics enable decision makers to overcome the complexity of quantifying security risk, and it is suited for cost-benefit optimization. The methodology enables the decision maker to have the flexibility to scale the problem and to evaluate the supply chain at various depths (e.g., components, sub-component, sub-assembly, systems, etc.), and to leverage each decomposition to address system or enterprise level supply chain vulnerabilities. Additionally, this approach enables decision makers to recognize emergent behaviors and their global effects.

The first component of the decision analytics framework is representation of the supply chain. This includes mapping of both the materials and information flow of the supply chain across the lifecycle phases. We have developed an information-based approach that enables a hierarchical decomposition of the supply chain. The 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 representation mapping is to enable the analyst to have a complete understanding of the risk associated with the processes, suppliers and infrastructure throughout the supply chain across the lifecycle.

After generating the supply chain mapping we perform a high-level risk assessment of the process steps and entities within the supply chain. For this, we have partitioned supply chain risk into a set of eight indicators. These indicators are the amount of *control and influence* over a process step or entity, the information and material *exposure* during a process step or to an entity, the *diversity* or redundancy or 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 the entity. Moreover, we have developed an assessment protocol to aid analysts in assessing each indicator. For each of these indicators, there is a series of qualitative and quantitative questions that can be easily answered for assessing the risk within each indicator category. Aggregating risk across the indicators provides a first measure of the risk of individual process steps and entities. At this level of detail we can begin to identify locations of elevated risk within the supply chain by noting higher risk scores. Elevated risk scores may also identify appropriate locations in the supply chain for further, more detailed analysis. Additionally, the structure of the supply chain graph can help us to identify nodes where there is a convergence of information, materials, or both. Organizing risk into sets of indicators enables the hierarchical nature of the analysis, and furthermore provides the flexibility to overcome the problem of missing or unavailable data. We can evaluate the risk at different portions of the supply chains and with different levels of detail by varying the types of questions we answer about them. As long as these questions are consistently categorized by the indicators, we can accommodate varying levels of detail within our analysis.

The second component of the framework, vulnerability and mitigation modeling, provides analysts with the ability to perform vulnerability and mitigation assessment on the supply chain. The end-to-end supply chain representation in combination with lifecycle phases, 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 to subvert the supply chain. However, this type of vulnerability assessment can be highly subjective and the supply chain vulnerability space is too large for manual analysis to provide comprehensive coverage. To streamline SME effort and to reduce the subjective nature of red-teaming based attack path generation we developed a functional

ontology for both adversary and mitigation actions that relates actionable functions to the supply chain. The ontology consists of a set of actions that are applied to the set of objects (materials and information) that exist in the supply chain at their defined locations in the supply chain. 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 helps to encapsulate the problem into manageable elements. This also enables an efficient method of automatically inferring attack scenarios against the supply chain and of representing them by directed graphs. By generating a rich attack space in this manner we can measure the overall supply chain risk with our difficulty and consequence risk metrics.

The mitigation space can be evaluated in a similar manner. Mitigation actions can be applied at locations within the supply chain, or to specific objects at specific locations. 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, identifying common nodes that are part of multiple attack scenarios could provide broader mitigation.

Once the supply chain vulnerabilities have been identified, the third component of the framework provides risk assessment of the vulnerabilities. This process enables the analysts to rank and prioritize the vulnerability space of the supply chain. We leverage Sandia National Laboratories developed risk assessment methodology that have been previously applied for physical security. This risk assessment methodology enables the evaluation of attack scenarios based on difficulty and consequences [8]. Mapping the attack scenarios to the difficulty and consequences space further enables optimization techniques to be applied for risk-based cost-benefit decision analysis.

The fourth part of the framework, optimization, provides decision support for the decision maker to select the best mitigation strategies to counter the discovered vulnerabilities. Optimization models enable decision makers to perform risk-based cost-benefit prioritization of mitigation strategies, while our risk assessment methodology enables ranking of the attack scenarios and provides input for optimal prioritization. The goal of the decision support component is to find the best set of mitigation strategies such that attack scenarios become more difficult for the adversary, reduce the consequences if the attack is successful, or both. A more detailed discussion of this framework can be found in [9].

In this use case we focus our attention on an initial high level mapping of the supply chain, and then use the mapping to identify locations warranting more detailed analysis and to identify structures in the supply chain, such as convergence points, 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.

IV. Use Case

A. Scope

As described in Section III, the main purpose of the framework is to enable government or business entities to make decisions concerning supply chain risk, and to help them select mitigation approaches that might be most effective, provide broader coverage, reduce cost, or satisfy some other constraint. In this research we use this decision analytics framework to analyze the supply chain of a DoD critical infrastructure system under construction and highlight the complexities of supply chain risk and give real examples of how to work through the challenges of applying supply chain risk management for national security.

Many SCRM approaches are applicable only to early stages of procurement or engineering efforts, and many of these approaches consider mitigations that are effective only during an early stage contract or qualification process. In this use case we wanted to highlight the applicability of the framework when the supply chain and contracts have already been established. In this example, the overall DoD contracted construction project was well underway – equipment vendors and contractors were already selected before our team was engaged. Similarly, many SCRM approaches assume that if a good screening process is used, then the system will be more secure. Yet, as we will discuss in this manuscript, a comprehensive SCRM approach must also accommodate for operational security issues that are introduced by well-screened original equipment manufacturer (OEM) implementations from trustworthy supply-chains. The approach must also account for other security issues introduced during post-contract support or later in a system's lifecycle.

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

B. Data Collection

Since the focus of the framework is to identify vulnerabilities in the supply chain and lifecycle of a program, we acquired much data through document collection and on-site interviews. 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 end-use, manufacturer quality and procurement practices, hardware and software components, and military construction (MILCON) program testing and acceptance process of the system. 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 (ATO). They also provide early feedback on specified equipment whether its security posture acceptable for the DoD facility.

To validate use of the framework and to collect more granular data on the CIS case study, we procured equipment similar to that specified for the DoD facility from another local integrator (within another U.S. region) and constructed a working test system. This provided the opportunity to apply our SCRM risk indicator protocol, an extensive questionnaire similar to [13], and validate their applicability for establishing SCRM risk metrics used in the framework. Under this procurement contract our team spent much time with the local integrator to understand normal practices within this industry and OEM specific configuration details of this control systems domain.

The procurement also helped established a communication channel with the OEM regional manager of the CIS equipment; through procurement we moved from a third-party role and became a customer. While keeping in mind the operational security (OPSEC) considerations, we exercised this relationship to understand the manufacturing quality control, supply chain, and customer data collection practices of the OEM. The DoD site location was not disclosed to the OEM, making sure that an inadvertent correlation would not increase the supply chain risk due to our analysis efforts.

We compiled this data into a directed graph representation of the lifecycle, processes, and supply chain interactions, including both material and information flows, for the supply chain established for this construction process and helped identify key weaknesses in the supply chain and system integration process (Fig 2). This analysis also identified the

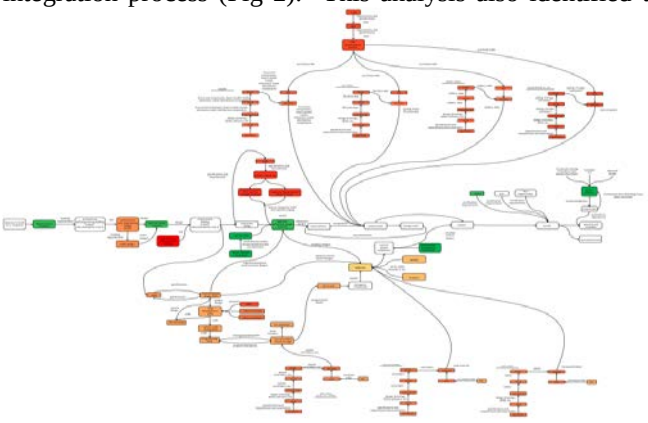

Fig. 2. An illustration of the supply chain representation and flow for the entire CIS construction and commissioning process. 104 process steps or entities within the supply chain were identified, highlighting its complexity. The color of the nodes represents varying level of potential risk.

limitations of traditional approaches to supply chain security risk mitigation – primarily due to our late engagement in the construction/procurement process. For this SCRM case study the limitations significantly emphasized the importance of operational system security characterization followed by acceptance testing with detailed information assurance test plans.

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

C. Results

Thorough data collection and analysis of the DoD program, roles, and responsibilities helped identify operational processes, entities involvement, and supporting infrastructure. We studied the business characteristics, operational practices and process steps in relation to this construction project of the various entities that have impact on the critical infrastructure system. A total of 24 questions, categorized into our 8 indicator categories, were used to evaluate the supply chain risk. 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 to 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, which is also shown in Fig. 3.

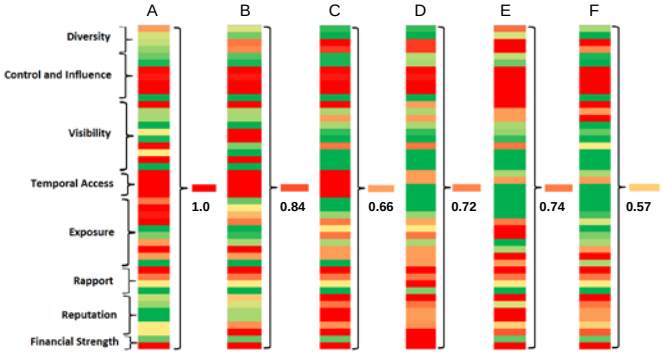

Fig. 3. The supply chain risk indicators heatmap for various entities their overall relative risk score. In this example, each column represents various DoD contractors that have some impact on the CIS system. Adjacent bands of a category indicate upper and lower bounds on the score. Adjacent green and red bands indicate a lack of information whereas adjacent bands of the same or similar color indicate high confidence in the information.

It is important to note that these supply chain risk scores are relative scores among the entities in question; the value of the score in itself is less important than the ordinal comparison which provides analysts a way to evaluate areas of higher risk. It is also noteworthy to point out that an independent risk score can be highly subjective, and establishing a meaningful baseline can be extremely difficult.

Figure 4 provides another perspective of the data offered by spider charts (aka radar charts), which identify an entity's strengths or weaknesses in several of the risk indicator areas. This view allows an analyst to quickly make determinations

on specific risks, whether to collect more information or potentially work with a supplier to improve their risk posture.

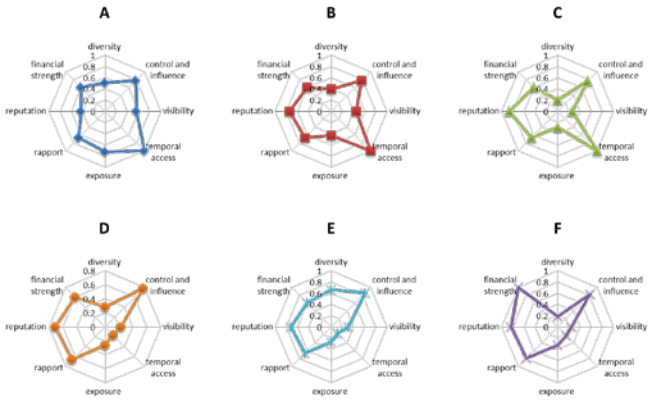

Fig. 4. The supply chain risk for entity A through F represented in a spider chart. Larger areas or indicator values further from the center mean greater supply chain risk. This chart allows analysts to more easily identify and better characterize supplier risk.

As mentioned in Section II, there are supply chain weaknesses or vulnerabilities at any stage of a system's lifecycle process. One of the analysis goals was to use this SCRM decision analytic framework to identify critical nodes in the supply chain for the CIS. Of the 104 nodes identified (Fig. 2), there are areas in the supply chain where several predecessor nodes converge into single nodes – this indicates high-risk nodes. A greater edge density of the supply chain directed graph means more complexity and suggests more risk. The convergence also indicates that a detailed analysis of the node is warranted (Subsection D) and identifies it as a potential opportunity to apply mitigations that can have broad impact in reducing supply chain risk.

Since the decision to analyze the supply chain risks of the DoD system occurred well after contracts were already awarded, the opportunity to apply many early-stage SCRM mitigations, such as advanced vendor screening, were significantly reduced. If many of the potential mitigations were to be applied in this late-stage, they would add significant cost and delays to the program as the SCRM problem boundaries and complexities were too large and uncontrolled. Ultimately, late-stage supply chain analysis emphasizes the importance of operational system security characterization followed by comprehensive acceptance testing with detailed information assurance security plans. The high level analysis of Subsections B and C helped to identify components for more detailed analysis while Subsection D provides details of our deeper-level SCRM analysis and operational security testing which help clarify gaps between SCRM security practices and operational security.

D. Further Analysis

One of the assumptions of security professionals and many supply chain security methodologies is that adversaries will use advanced techniques to access or compromise a system. We determined that the components, communications, and protocols used in this CIS meet national standard specifications. However, the OEM implementation of the specifications, along with proprietary extensions, created many simple attack vulnerabilities.

Our deeper-level analysis began 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, including printed circuit assemblies. The OEM quality process allows insertion of equivalent components or specified components from alternate but qualified suppliers. The use of alternate suppliers is one of the key risk areas identified in [10]. Some of the factors that the OEM uses to make the supplier decisions include:

1) *Quality Performance* - acceptance testing, responsiveness to issues.
2) *Cost and Service Performance* - price, on-time delivery, lead time and cycle time, ease of doing business, accuracy and timeliness of documentation.
3) *Supplier Capability* - production capability, infrastructure.

Aside from their supplier selection, the components are verified and validated through the hardware development and quality assurance (QA) departments listing of all acceptable alternate sources and suppliers. The purchasing department then chooses which prequalified supplier to use based on price, lead times, availability, payment terms, and other factors. While this OEM process is reasonable, it follows a cost-driven model of qualifying once, and does not include a schedule for continued component sampling, audits of the supplier, or other security factors.

We partially validated the output of the OEM quality system with a deep-level hardware and software inspection. In the devices we observed many complex programmable logic devices (CPLD), ARM processors, and other 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 market or black market components, but it does suggest the OEM has processes that allow for some traceability back to the component manufacturers. Analysis of the system's software included embedded firmware, programmable logic, Windows CE applications, and general Windows OS applications for the human machine interface (HMI) workstation. Cursory static analysis of the software 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.

Security characterization of the working test system procured during this process 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 and reasonable supply chain risk reduction, the system implementations must be considered in securing a system. A

number of findings might be mitigated during the supply chain risk reduction steps or during initial commissioning of a system; however critical infrastructure systems typically operate for several decades and are serviced or tuned on a regular basis. Ultimately, this means that mitigations for today's security challenges may no longer be applicable in the future life of the system. The 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 information assurance 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 course of action. 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 and screening of vendors or randomly selected COTS components. Screening does not account for future risks and threats introduced during normal operation and maintenance of the system. Practitioners need to account for system hardening to reduce risks throughout the lifecycle of the system. Finally, guidelines for mitigation courses of action need to consider the cost-benefit of SCRM risk reduction efforts as well as the system's lifecycle. This is especially true for existing programs where SCRM analysis is performed in later stages of the acquisition process when it can be costly to implement some mitigation options.

V. Challenges and Future Work

One characteristic that distinguishes a mature approach to supply chain security is its appreciation for the challenges of collecting accurate and quality supply chain data. Some approaches use online information, Dun and Bradstreet reports, or systems such as [7]. However, our experience in this case study reveals that these results were sometime inaccurate or outdated, and more importantly they did not directly correlate to the operational security issues introduced by supply chain factors. Consequently, supply chain security approaches cannot rely solely on such indicators.

It can be challenging to collect accurate data which helps build a holistic view of the system's supply chain. For example, government entities are constrained by fairness of business opportunity regulations and may not be able to interact with potential suppliers or to collect detailed supply chain risk information prior to issuance of the RFI or contract. It may be possible to specify such provisions in the RFI, use pre-bid questionnaires, or with contract language. However, our experience in this case study demonstrates that suppliers may have a loose interpretation of the requested information, which leads to a reduction in data quality. If the supply chain information requests are too extensive in a pre-bid environment, some suppliers may choose not to respond. This could result in lower-quality suppliers earning the contract and introduces more security risks to the system.

Another industry accepted approach to gain detailed supplier information is through non-disclosure agreements (NDA), which legally bind both parties to protect the other's disclosed information. This process can take much time and usually involves legal staff or top-level company representatives. Again in our experience, suppliers are not as willing to establish an NDA unless they have a contract in place or have significant financial interests at stake. When establishing an NDA to gain specific vendor supply chain information, it is also important to realize that the NDA does not oblige the supplier to disclose information.

Regardless, the challenges of collecting accurate and quality supply chain data can be overcome. Establishing professional and courteous business relationships with suppliers will at many times have more gains than formal information request processes. The relationships must still be mindful of laws, procurement regulations, and the operational security concerns of the end system.

The work presented in this paper only illustrated part of the decision analytics framework, which have already demonstrated it's usefulness. As such, future work will include application of the complete framework to additional case studies. Additional supply chain decision analytics will include considerations of how to apply the framework within small business constraints, and also how to address the Buy America Act and other trade laws.

VI. Conclusion

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

We have shown that this framework will work at various stages of a system lifecycle. In particular, this analysis was done during the development phase of the CIS. As a result, detailed characterization and vulnerability assessment would be the most cost-effective and best option for mitigating supply chain risks. The assessment results identified areas of immediate risk, and provided a high-level comparison across the 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 and flows, we validated the use of SCRM questionnaires for supplier screening. The relevant

companies seem to be compliant, but we also noted some nuances of such data collection methods. We also found that establishing relationships with vendors seems to be more fruitful in collecting valuable supply chain risk analysis data than other methods, as it lent itself toward a stronger correlation of pragmatic and beneficial risk reduction methods, keeping in mind that using one type of information source or risk indicator is insufficient for overall system security.

This case study clarified gaps between SCRM security practices and operational security. Supply chain security practices do not holistically solve all security problems, especially for critical infrastructure systems that operate for several decades. This framework helps enable government or business entities to make decisions concerning supply chain risk, and to help them select mitigation approaches including technical vulnerability analysis and system security testing. In addition, we found that most SCRM guidelines do not account for the limited functionality of systems that lack security options. Many supply chain risk reduction methods would not likely identify or block an adversary from operating within normal or OEM specification of the system. Ultimately, our analysis of this case study highlights that a system's security has strong dependencies on both supply chain security and traditional information assurance practices. It also emphasizes the need for detection and prevention mechanisms to be specifically tailored for each OEM implementation and overall system integration.

ACKNOWLEDGMENT

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.

REFERENCES

[1] J. Boyens, C. Paulsen, N. Bartol, R. Moorthy, and S. Shankles. Notional supply chain risk management practices for federal information systems. (NISTIR 7622), October 2012. http://dx.doi.org/10.6028/NIST.IR.7622.

[2] J. Boyens, C. Paulsen, R. Moorthy, N. Bartol, and S. A. Shankles. Supply chain risk management practices for federal information systems and organizations. (NISTSP 800-161), August 2013. Initial Public Draft.

[3] Computer Security Division. Security and privacy controls for federal information systems and organizations. (NIST SP 800-53r4), April 2013.

[4] GAO. IT supply chain: National security-related agencies need to better address risks. (GAO-12-361), March 2012 http://www.gao.gov/assets/590/589568.pdf [Online; accessed 29-September-2013].

[5] C. Levin U.S. Senator of Michigan. Background memo: Senate armed services committee hearing on counterfeit electronic parts in the DoD supply chain. http://www.levin.senate.gov/newsroom/press/release/background-memo-senate-armed-services-committee-hearing-on-counterfeit-electronic-parts-in-the-dod-supply-chain [Online; accessed 15-September-2013].

[6] UMD, CyberChain. https://cyberchain.rhsmith.umd.edu/ [Online, accessed 10-March 2015].

[7] Palantir. https://www.palantir.com/ [Online, accessed 10-March 2015].

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

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

[10] U.S. Department of Commerce, Bureau of Industry and Security Office of Technology Evaluation, "Defense Industrial Base Assessment: Counterfeit Electronics," Jan. 2010

[11] R. A. Lebron, R. Rossi, and W. Foor, "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," in Strategies to Mitigate Obsolescence in Defense Systems Using Commercial Components, Budapest, Hungary, 2000.

[12] J. T. Hanlon, "The Future of Components for High Reliability Military and Space Applications," Sandia National Laboratories, Feb. 1996

[13] H. Lin, M. Schwartz, J. Michalski, M. Shakamuri, P. Campbell. *Leveraging a Crowd Sourcing Methodology to Enhance Supply Chain Integrity*. Proceedings of 2012 IEEE International Carnahan Conference on Security Technology (ICCST), 2012.