Securing the Supply Chain - A Hybrid Approach to Effective SCRM Policies and Procedures

Daniel Carbonaro

Securing the Supply Chain - A Hybrid Approach to Effective SCRM Policies and Procedures

Author: Daniel Carbonaro, decarbonaro@gmail.com

Advisor: *Johannes Ullrich*

Accepted: *October 18, 2019*

Abstract

Organizations' supply chains are growing increasingly interdependent and complex, the result of which is an ever-increasing attack surface that must be defended. Current supply chain security frameworks offer effective guidance to organizations to help mitigate their supply chains from attack. However, they are limited in their scope and impact and can be extremely complex for organizations to adopt effectively. To further complicate issues, the ability of an organization to identify the scope of their supply chains may be a complicated endeavor.

This paper seeks to give context not only to the challenges facing security within the ICT Supply Chain, but attempts to give a hybrid framework for any business regardless of size or function to follow when attempting to mitigate threats both to and from within their supply chain.

1. Introduction

To establish motives for attacking or defending an organizational supply chain, one needs to look no further than approaches militaries have made in attacking an enemy's supply lines. As General Omar Bradley once famously quipped: "As amateurs debate strategy, professionals discuss logistics" (Singer, 2014). Simply put— without the ability to properly supply a military body, would collapse and cease to operate as a fighting force.

A nation that cannot sustain its military to protect or expand its borders cannot continue to exist, just as a business cannot function without the means to exchange goods and services for profit. Consequently, an attack on a business' supply chain is an attack on its core reason for existence. Businesses and organizations must answer this rising existential threat with an effective means of defense.

2. Supply Chain Overview

The result of today's increasingly complex and integrated environments is an evolving attack surface that is going unacknowledged. The increased use of third-party components (Whitney, 2019) has literally introduced foreign objects into corporate ecosystems. While they bring functions to products that otherwise would not exist, they can also have the potential to introduce vulnerably that otherwise would not exist.

The service industry has also increased foreign access to organizations. The human side of these services come in the form of external product support, human resources, and security services. These human operators are often given both on-premise and remote access to endpoints for the purposes of their jobs. Examples of this can include product troubleshooting support and information security services.

A central issue with the large-scale integration is that an organization is directly inheriting another company's supply chain and potentially any security issues therein. This, in turn, increases the inheriting organization's own attack surface. Security devices and monitoring teams are no exception to this, especially in the case with outsourced

incident response teams, known as Managed Information Security Service Providers (MISSP's). These teams install and monitor devices which, at times, are given unfettered access to an organization's most sensitive areas. If an unpatched update server belonging to one of these security appliances was compromised, malicious actors could potentially access the 'crown jewels' of the monitored environment. After all, who is monitoring the monitors? In April 2019, Carbon Black published their Incident Response Threat Report in which they sighted increased use of targeting these service providers to then pivot into the monitored network (Carbon Black, 2019). This 'island hopping' technique can potentially be used for lateral movement into other organizations if a route is exposed and made available to an attacker.

3. Supply Chain Attacks Past, Present, and Future

Supply Chain attacks either to or from within the Information Communications and Technology (ICT) Supply Chain have occurred with regularity, only having made headlines relatively recently.

One of the first well-published examples was the 2013 data breach which crippled Target's POS systems. The credit and debit card information of an estimated 40 million customers was subsequently compromised as a result of the breach (Alumni, B 2017). While it has been reported that the chosen vector was network authentication mechanisms of Target's third-party HVAC provider, the exact attack technique remains unknown. Thorough mapping and auditing of transitive access rights is a key security technique that should be employed on a frequent basis.

A more recent technique utilized by attackers is to move laterally and inject malware into the update servers themselves upon gaining system access. This enables them to utilize the update mechanisms themselves as the vector to infect their victims. Avast's newly acquired CCleaner and Asus' Live Update utility, were victims of this tactic in 2018 and early 2019 (Newman, L. H., 2018). Even more interesting is that, in both cases, although numerous victims were reportedly infected, only a select few devices phoned home to their gates to pull down additional malware.

The attack on Asus, later known as ‘Shadow Hammer' appears to have been customized to target a specific set of specific MAC addresses for compromise. This invariably leads to the conclusion that the attackers knew exactly who and what they wanted to target.

Looking to the future, a recent attack highlighted an even more down-level attack with the insertion of malware to source code then being rendered by high-level compiler runtime libraries such as C/C++ (Mokbel, M. 2019). Supply chain attacks techniques such as this adds yet another level of complexity to mitigating attacks within the supply chain.

Current supply chain attacks are extremely complex in their preparation and execution. Thus, these attacks will typically favor those who have the resources at their disposal to conduct such coordinated attacks. In time, the industry may see nation-states and other highly funded and coordinated groups using these tactics with increased frequency and more devastating consequences.

4. Approach to Methodology

A critical mistake which organizations tend to make in approaching the concept of information security, is that they attempt to monitor and defend all assets within the organization with the same criticality, often deploying too many tools across large swaths of the organization (Muresan, 2019). Additionally, this approach is undertaken many times with limited resources for proper implementation of the associated controls. To further complicate this issue, the ICT supply chain is a mechanism which will invariably ‘touch' every part of an organization. So how do you defend everything in your business from malicious attacks? Simply attempting to use a single blanket SCRM policy across your entire organization will most likely be ineffectively monitored and controlled. Moreover, this approach is unrealistic for most large enterprise organizations, from both a resource and time allocation perspective. Furthermore, challenges can arise not only from identifying and scoping the supply chain, but from attempting to identify the areas to

defend. To this end, an organization must look to how its goods and services are sourced and provided in order to define their own unique supply chains.

To address these areas, various risk management policies will be examined. The policies will include not only supply chain risk management polices but other policies that are not directly related to traditional supply chain risk management. This research is proposing that organizations must identify the critical components of its supply chain first, using NISTIR 8179 to accomplish this goal. Once these areas are identified, a baseline SCRM practices must be established for them. For this research, ISO 28001 will be used in establishing these security best-practices within the example organization. After the critical components have satisfactory supply chain defenses established, targeted controls for these components will be identified and established using the NIST 800-161framework. Subsequently, the less critical components should then be focused on. These components will then be factored into the Business Continuity Plan (BCP) and the Disaster Recovery Plan (DRP), integrated within the context of the supply chain in sequence. It must be noted that the critical mechanisms must be incorporated first, as their loss will have the greatest impact on the organization.

NISTIR 8179 is a framework adopted for existing infrastructures and not necessarily for the supply chain. To add clarity, a fictitious company named "Acme" will be used as a hypothetical example to show what implementation would look like. Acme is a company which specializes in the design and development of 'next-generation' network security appliances. These examples will be listed as the conclusion of each *Adoption* section under a section titled, '*Example'.*

5. Supply Chain Security Frameworks

6.1 NISTIR 8179 - Criticality Analysis Process Model

The NIST Internal Report (IR) 8179 was developed out of recognizance of the challenges faced by organizations in identifying and protecting their most critical assets. The NIST 8179 guideline recognized that each organization is unique, and consequently, their attack surface and defense capabilities are as well. Therefore, each organization

must effectively self-assess and build defenses catering to their unique needs. NIST 800-161 states in its *Risk Response* Section, "Provide tailoring decision for selected controls, including the rationale for the decision″ (Boyens, J., Paulsen, C., Moorthy, R., & Bartol, N., 2015) The "rationale" is what NISTIR 8179 will be able to provide to the organization in conjunction with NIST 800-161.

6.2 ISO 28001:2007 - *Best Practices for Implementing Supply Chain Security Assessments and Plans*

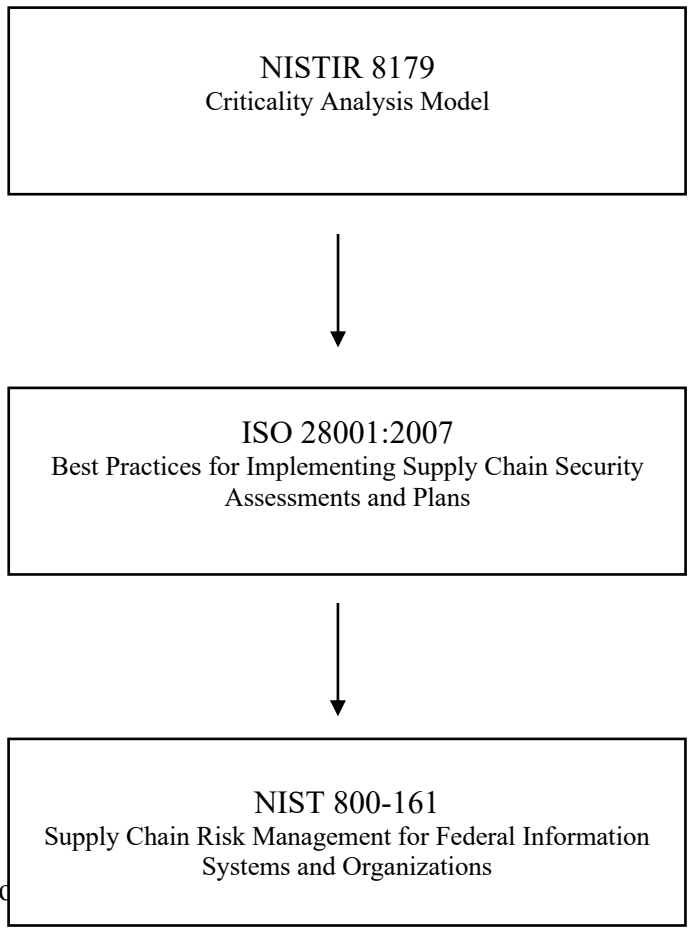
The ISO 28001:2007 standard was developed to outline best practices for establishing and implementing security strategies and techniques for an organization's ICT supply chain. The best practices will establish the basic and core defenses that, without their implementation, will nearly guarantee a compromise at some point in its future. Like Maslow's hierarchy of needs, the basic and core components for a business to survive must be established. The techniques establish by the International Standards Organization for this task is preferred, as the approach takes care to examine the unique and differentiating challenges it faces. The NIST 800-161publication states that "…[FIPS 199] "high-impact" systems should already have these foundational practices established" (Boyens, J., Paulsen, C., Moorthy, R., & Bartol, N., 2015). It should be noted that this guidance is the primary purpose for the inclusion of the ISO 28001:2007 standard. It gives a brief and high-level guideline for an organization to quickly identify gaps and provide security guidance that is appropriate for the organization. It will be noted that further, more targeted security control guidance can be re-examined according to NIST 800-161 security controls at a later date.

6.3 NIST 800-161 – Supply Chain Risk Management for Federal Information Systems and Organizations

For years, the National Institute of Standards and Technology (NIST) has published incredibly useful guidelines and standards for institutions to follow. Their standards are primarily adopted by US-based organizations, with particular emphasis within the public sector. In 2015, NIST published a supply chain security guideline for US agencies in their selection technology vendors.

Recognizing that security controls may not be applicable to every component of a business, relevant controls are outlined through a tiered structure. NIST 800-161 borrows from FIPS 199 *Standards for Security Categorization of Federal Information and Information Systems*, and FIPS 200 – *Minimal Security Standards for Federal Information and Information Systems,* eighteen (18) security control families. An additional '*Provenance*' family for components was then added to help give additional insight into the needs of the supply chain. These nineteen (19) control families are structured from specific controls that are either directly related or are 'relevant' to supply chain risk management (SCRM) of an organization's mission or business processes.

It should also be noted that the framework does an outstanding job of giving examples of possible scenarios for a number of its controls. Organizations that may be relatively new to these controls can look to Appendix D, page D-1 of the publication. It is recommended that organizations cater to these scenario outlines and develop their own scenario 'run-books' to reference in the event such an occurrence does happen.



7. Framework Adoption

The following proposed hybrid framework methodology utilizes a combination of guidance from the documents below and borrows strengths from each in successive order:

1. NIST IR 8179 - *Criticality Analysis Process Model*
2. ISO 28001:2007 – *Best Practices for Implementing Supply Chain Security Assessments and Plans*
3. NIST 800-161- *Supply Chain Risk Management for Federal Information Systems and Organizations*

The hierarchical structure scales vertically, with defense mechanisms for critical infrastructures emphasized initially, then progresses to less critical infrastructures as the processes continue. These frameworks, in combination with supplemental strategies, will produce a targeted, yet holistic guideline for organizations to consider when creating supply chain security policies. This paper recognizes that while there may be areas of overlap between frameworks, the proposed guideline will increase the efficiency and effectiveness of the implementations of these security standards.

The purpose of the following section is to give the reader an overview of the sections targeted for inclusion in the hybrid framework. It should be noted that the following sections should not solely be taken as summaries of the referenced procedures, but rather should be taken as contextual applications of the control methods within the organization's supply chain. Additional reading and research of these frameworks is both implied and encouraged. This framework should be used not only in securing existing infrastructures, but also in examination scaling future components if they fall under one of the nineteen (19) NIST 800-161 control families. These families will be discussed in further detail in Section 7.3.

To adopt this framework, a working-group led by a program manager should be formed consisting of both technical and managerial representatives from the departments in scope.

Example: *Recently, The Acme Corporation suffered from a supply chain attack which ultimately cost the company over $1.5 million dollars in liquid assets. As a result, the executive leadership team at Acme has made the decision to undertake a project to create policies and procedures to help reduce the risk of another such attack. This has been communicated to Acme's shareholders in their quarterly briefing, post-incident.*

An official project has been designated and an interim funding budget of $200,000 has been approved and allocated for the effort. A senior project manager has been selected by the CISO to lead the effort. The project manager has now assembled a 'tiger team' to include representatives from their Corporate Security Team, Supply Chain, Legal, Software and Hardware Development, Manufacturing, and senior managers for their business units. It is the executive leadership's understanding that representatives may be brought in on an 'as-needed' basis.

7.1 NISTIR 8179 - Criticality Analysis Process Model

While NIST 800-161 does briefly approach the idea of identifying a baseline criticality of components, suggestions on how to approach this identification is only briefly discussed (Boyens, J., Paulsen, C., Moorthy, R., & Bartol, N., 2015). The issue with establishing a baseline for supply chain risk is the majority of the two-hundred and thirty-four controls comprise what is identified as the SCRM 'baseline' within NIST 800-161 sections A-1-A-9 (Boyens, J., Paulsen, C., Moorthy, R., & Bartol, N., 2015). This framework will argue that all three tiers should be considered, as identified in the process. However, the ability to establish these baseline controls will be difficult in that nearly all the controls will need to be examined. Additional emphasis on this needs to be placed on this aspect as the failure of mission critical components can cripple an organization. NIST 8179 can be used to bridge these gaps.

The following sections are high-level overviews of the five processes and sub-processes that go to the heart of the Criticality Analysis Process Model. The purpose of this identification is to locate the critical components of the organization. The intent is to

examine the components, sub-components and any entailed processes and or applications not from a static-state, but rather in the context of their supply chain ecosystems. For instance, a database server may or may not arrive with unwanted configurations made to its storage media. However, given the criticality, diligent checking should be performed to ensure this has not occurred nor can occur in the future if not authorized to do so. If the organization has policies and procedures these need to be recorded for later reference.

It should also be noted that this process is similar to the 'Framing' process step in NIST 800-161. The results of this should be documented for later reference if using NIST 800-161 in more in-depth applications (Paulsen, C., Boyens, J., Bartol, N., & Winkler, K., 2018).

The following section is located on page 7 of NISTIR 8179 (Paulsen, C., Paulsen, C., Boyens, J., Bartol, N., & Winkler, K., 2014).

1.*Define Criticality Analysis Procedure(s) where the organization develops or adopts a set of procedures for performing a criticality analysis* (Paulsen, C., Boyens, J., Bartol, N., & Winkler, K., 2018). This phase is the initial procedural step for the organization in defining their mission-critical components. The need is defined, and the group is formed to oversee the tasks' execution. The group should be formed with a number of representatives with technical knowledge of the organization's architecture.

***Example**: The team has now met over the past few weeks and has gathered any existing corporate policies and procedures as well as distributed copies of the NISTIR 8179 and NIST 800-161 documents into a secured, document repository location for their review and collaboration. Licensed copies of ISO 28001 have also been purchased and distributed.*

2.*Conduct Program - Level Criticality Analysis where the program manager defines, reviews, and analyzes the program to identify key activities that are vital to reaching the objectives of the program and for reaching the overall goals of the organization* (Paulsen, C., Boyens, J., Bartol, N., & Winkler, K., 2018).

An essential aspect of this process is the program manager's ability to effectively gather input from their respective technical resources and identify the areas for scrutiny. These systems will then be assigned controls according to the Tier 2 controls of NIST 800-161 and will discussed further in Section 7.2.

Example: *The Acme team has now identified their next-generation firewall product line as their use-case for this project. All components related to the product lifecycle will be examined from a supply chain perspective. They chose this system not only because they use the devices for perimeter security in their own infrastructure, but because its embedded software and firmware is designed to interact with other security products which Acme sells. This NGFW line also is also Acme's most popular customer offering and would have devastating branding consequences if it were to be compromised from a low-level supply chain attack.*

3.*Conduct System/Subsystem – Level Criticality Analysis where the system designer reviews and analyzes the system or subsystem from the point of view of its criticality to the overall organizational goals* (Paulsen, C., Boyens, J., Bartol, N., & Winkler, K., 2018).

In this step, the system is selected based on its criticality-relationship to the organization. Its assemblies are examined and analyzed to identify the critical components and will be eventually assigned Tier 3 controls of NIST 800-161. Examinations of supply risk factors such as system component provenance, or maintenance needs will occur in the later steps of the following sections.

Example: *The Acme team asks their product engineers to examine the overall system-level design components of their NGFW products. They have identified the high-level hardware and software assemblies that will be further scrutinized in later steps. An example of this is the core behavior-based intrusion detection application. How this application functions at the system level should be examined.*

4. *Conduct Component/Subcomponent - Level Criticality Analysis where the system or component engineer reviews and analyzes component or subcomponent from the point of view of its criticality to a specific system or subsystem of which these components and subcomponents are a part.* (Paulsen, C., Boyens, J., Bartol, N., & Winkler, K., 2018).

Special care should also be taken when assigning controls to these system components and subcomponents. The potential to overlook these areas remains a risk during this step. It is recommended that the system designer (architect) should work closely with the engineer to ensure this does not happen. Again, these will ultimately be assigned Tier 3 NIST 800-161 controls.

Example: *The Application decoding engine, for instance, will be examined later at the sub-component level. Since Acme enjoys the luxury of developing this sub-component, it can be examined in-house. If this was not the case, ACME should utilize a vendor questionnaire as discussed in Section 8.2 'Supplier-Trust Audits'.*

5*.Conduct Detailed Review of Criticality for Processes B, C, and D where the program manager or a collaborative group analyzes the baseline criticality analysis results to create final criticality levels for Systems/Subsystems and Components/Subcomponents* (Paulsen, C., Boyens, J., Bartol, N., & Winkler, K., 2018).

A careful review of the steps 1-4 is critical to ensure that no areas are overlooked nor undervalued. The program manager needs to ensure that these analyses are done from the context of the supply chain and the results are documented for later reference.

Example: *Acme's program manager along with the team reviews all material gathered in this phase to ensure the project scope was properly adhered to and the data gathered is accurate.*

7.2 Step 2: ISO 28001:2007 – *Best practices for implementing supply chain security assessments and plans*

After the careful examination and identification of these critical components are completed, an assessment of existing supply chain security controls will be performed. NIST 800-161 explicitly states that baseline security measures should already be in place for critical components (Boyens, J., Paulsen, C., Moorthy, R., & Bartol, N., 2015). Find. An expeditious assessment needs to be performed to ensure no major gaps exist. An examination of the ISO 28001 document will give the organization a roadmap to verifying or, if needed, adding security countermeasures to these critical areas.

Section 5.3 *'Conduction of the security assessment'* outlines the high-level approach to assessing the security of these areas. The initial assessment process outlines that organizations will evaluate the suppliers of the components through an examination of any security declarations made by the supplier. Both the detail and the validity of the supplier claims need to be examined (BSI, 2007). Risk and likelihood of compromise should also be taken into consideration when examining these components.

If vulnerability scans are conducted within the organization, the results of any in-scope components should be examined by the security team. If scans have not been performed, it is highly encouraged that scans be performed immediately, if possible. Again, the purpose of this step is to not to completely harden the critical systems, but rather to ensure a security baseline is established, with further controls being identified later in Step 3.

7.3 Step 3: NIST 800-161 – *Supply Chain Risk Management for Federal Information Systems and Organizations*

Once the critical components are identified, and a baseline of security is established, the main focus will now shift to the more detailed implementation of security controls from NIST 800-161. As previously stated in Section 6.3, NIST 800-161 is a robust, three-tiered risk management framework that examines all areas that can be considered an ICT supply chain. At two-hundred and eighty-two pages (282), the work is

by far the most comprehensive. Spread across nineteen control families, the two-hundred and thirty-four (234) directly-related and indirectly-related security controls are each mapped to their applicable families (Boyens, J., Paulsen, C., Moorthy, R., & Bartol, N., 2015).

The first of the three tiers to be examined is the tier responsible for the parent policies which will ultimately map to the child tier-two and tier-three policies. This tier describes control policies that need to be in place at the Executive or "*Organizational*" level. These polices "Define corporate strategy, policy, goals and objectives" (Boyens, J., Paulsen, C., Moorthy, R., & Bartol, N., 2015). It is important that these policies are identified and mapped to their respective 'child' policies so that both a logical policy flow can be easily referenced by users, and that the ability to ensure appropriate compliance mappings is actionable.

On reference page A-1 of the NIST 800-161 guideline, a control chart with the applicable controls is listed for users to reference. The chart will list, according to the control, the tiers at which they are applicable. In most cases, controls are mapped to multiple tiers with the context changing at each tier. For instance, the control *Identification, and Authentication Policy and Procedures* will map from the Executive (tier 1) level, Business Unit (tier 2) and Component level (tier 3), while the *Authentication Management* control will only apply to the tier 3 control as it is managed at the component level.

Each control criteria can be found under Section 3.5 *ICT SCRM Security Controls* (Boyens, J., Paulsen, C., Moorthy, R., & Bartol, N., 2015). Each identified critical component will be mapped to any of the applicable control families. The nineteen (19) control families are:

> *Access Control, Awareness and Training, Audit and Accountability, Security Assessment and Authorization, Configuration Management, Contingency Planning, Identification and Authentication, Incident Response, Maintenance, Media Protection, Physical and Environmental Protection, Planning, Program Management, Personnel Security, Provenance, Risk Assessment, System and*

Services Acquisition, System and Communications Protection, System and Information Integrity.

It is also recommended that components that share commonality amongst each other, either at the component or policy level, are identified and documented for further risk mitigation. This reason for this is that if these shared components were to become compromised, they can potentially act as a single point of failure for multiple critical components. Once all critical components are mitigated to a level of risk deemed acceptable by the organization, less-critical components can be identified for NIST 800-161 security control implementations.

8. Joining Forces

8.1. Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) Integration

The critical components identified in *Step 1 - NIST IR 8179 – 'Evaluation'* (Paulsen, C., Boyens, J., Bartol, N., & Winkler, K., 2018) should be incorporated into a company's disaster recovery program with the appropriate care and consideration warranted by its designation. An evaluation of the Business Impact Analysis (BIA) on these assets is a crucial component in demonstrating the need to protect an organization;s critical components. This analysis will help demonstrate the potential monetary damages incurred in the event of a supply chain attack to these components.

The Annualized Loss Expectancy (ALE) formula gives both standardized and quantifiable measurements of the impact a successful compromise has on a given organization. The ALE is the calculated Annual Rate of Occurrence (ARO) and Single Loss Expectancy (SLE).
ALE is determined by the following formula: (Chapple, M., Stewart, J. M., & Gibson, D., 2018):

$$ALE = SLE \times ARO$$

- The Single Loss Expectancy (SLE) is defined by the incurred monetary loss of a single compromised asset. The formula is as follows:

  SLE = Asset Value (AV) x Exposure Factor (EF)

- The Exposure Factor (EF) is a measurement of the negative impact which a negative event would have on an asset.
- The Annualized Rate of Occurrence (ARO) is the estimated annual frequency of occurrence for a threat or event.

  (Chapple, M., Stewart, J. M., & Gibson, D. 2018).

The quantitative view is that the Business Impact Assessment gives does not take into account many of the nonmonetary items that are difficult to assign a value. The monetary and reputational damage suffered by Bloomberg's dubious SunMicro article cannot be challenged (Leswing, K. 2018,) However, given sheer attack surface of an organizational supply chain, both short and long-term nonmonetary damages can be difficult to quantify. These items include (Chapple, M., Stewart, J. M., & Gibson, D., 2018):

- Loss of goodwill among your client base
- Loss of employees to other jobs after prolonged downtime
- Social/ethical responsibilities to the community
- Negative publicity

These potential effects also need to be taken into account when examining organizational risk to supply chain attacks.

8.2. Supplier-Trust Audits

NIST 800-161, along with a number of other additional controls, added the 'Provenance' control family to help track the traceability and origin of components in the ICT supply chain (Boyens, J., Paulsen, C., Moorthy, R., & Bartol, N., 2015). This pertains to both hardware and software components alike. It is of the utmost importance that security teams work intimately with procurement teams to ensure that new components are only introducing a level of risk that is acceptable to the organization.

Vendors should always be evaluated for their security practices before they are approved. Not only should their products and practices be evaluated, but their infrastructures should be appropriately evaluated as well. Special consideration to third-party components should be given as well.

Products and/or components which are under consideration for purchase should be evaluated by a risk management professional working in tandem with the sales team. An information security officer (ISSO) would be an example of an appropriate person for this task. It should be noted that business and organizational needs should be considered appropriately in this regard. It is commonly echoed that Information Security is an art, not a science (P. C. 2013). The balancing act between business needs and robust security measures is a common issue across organizations. Supply chains exist to supply the fundamental needs of the business and adding security overhead will directly impact this concept, making a case for "art" all the more ostensible.

A common practice that organizations use when selecting vendors is to submit questionnaires to potential business partners. Questions can be targeted to the suppliers based on the product type and integration point. Be it hardware, software or firmware, the answers given should be auditable and/or contractually binding to the organization. These questionnaires can be an effective solution to dependencies an organization may face, and that otherwise wouldn't be addressed. For instance, if an organization needs to buy an offsite-data storage solution to maintain records containing personal identifiable information (PII), specific questions can be directed at how the database servers are maintained, updated, and monitored. Questions can be posed about any third-party software used, physical security of the storage locations, back-up procedures, etc. The questions asked can be finetuned for the needs of the customer. The answers given should be reviewed and if need be, the organization should clarify the vendor's answers before any agreements are reached. For optimal results, the questionnaire should be resubmitted to query for changes made on a re-occurring basis.

9. Conclusion

Given the current capabilities of today industry, the security of the ICT Supply Chain is unfortunately too vast and complex to tackle. After all, everything in your organization was sourced and supplied to you in some fashion. If there was ever an argument for a ‘journey' versus a ‘destination', the security of the products and services traversing the ICT Supply Chain would be it. While steps to ensure integrity should be undertaken as often as possible, the integrity of an organization's critical components and their management systems should be prioritized once an acceptable security baseline has been established. Afterward, priority should be placed on mitigating supply chain threats to other areas should be untaken from a descending level of importance.

It should be noted that threat-modeling can be used to determine the likelihood of an attack. This likelihood should be taken into consideration, within this stream as well. Critical components cannot, and must not, share this same luxury of consideration.

An organization can only control what it can control. Interdiction of software and hardware components can occur at simply too many points within its journey. Each point of a component’s ingestion should be re-assessed an assessment of its purpose. An example of this is an app store, where employees are able to download applications on their laptops. The mechanism of how these apps are distributed needs to be assessed with the purpose of the application should be examined. Controls then should be placed on the employee's ability to install these applications only to allow approved or whitelisted applications. A critical database server probably should not have access to any application store in any capacity, much less a web-browser at all.

If there is a single word that should define supply chain security, it should be “*distribution."*. Trusting and verifying integrity is a constant battle in the IT industry, but an especially challenging issue within the ICT Supply Chain, as integrity goes to the heart of the problem. Both software and hardware need to be continuously re-evaluated whenever possible, especially given the various points of interdiction in the global supply chain. It is because these controls scrutinize both the product lifecycles and infrastructure of the supplying company.

Daniel Carbonaro, decarbonaro@gmail.com

The process of hardening the defenses of critical distribution mechanisms only serves to help augment existing security controls throughout the organizations. The 'crown jewels' will only be further protected, which should make any CISO or public investor sleep better at night. The demand for demonstrated supply chain security from vendors can help serve as a catalyst for greater security throughout the IT industry as a whole. Customer demands for such are entirely justified as well. After all, their purchase can one day compromise their organization.

Appendix

The Case for Blockchain

Blockchain technology was developed out of a need to better track and manage high fidelity transactions. It has since evolved into other uses outside of this initial application. One current use for blockchain architecture is its deployment as a tracking solution for traditional supply chain teams. Both IBM and Microsoft have developed great solutions for this. The fact that this software is already being integrated into supply chains is an advantage and could help augment security teams in analyzing their supply chains. The 'Provenance' control specifically calls for "methods for tracking relevant purchasing, shipping, receiving, or transfer activities, including reviewer signatures for comparison" (Boyens, J., Paulsen, C., Moorthy, R., & Bartol, N., 2015). If applied in an augmented fashion, with emphasis on security and integrity checking, could have far

reaching effects. Integrity checking at scale could very well thwart many of the attacks discussed earlier in Section 3 with regard to the delivery of compromised updates.

With Blockchain advantages are huge; both the smart contract and hyper ledger can be configured within the required parameters to meet the needs of the organization. Any proposed change to the shared distributed ledger must be approved through a group consensus. Unfortunately, there is a great deal of misunderstanding around this issue. It is widely misunderstood that the node consensus threshold for blockchain is 51%, and this is categorically incorrect. (Gazdecki, A., 2019). The 51% consensus rate exists currently because that was the rate that was designed for the initial crypto currency application. The rate of consensus is entirely customizable for the end purpose. Again, it is entirely possible to architect a block chain solution with a custom ledger and smart contract dictated by the end user. The only potentially limiting factors are potential latency times and the needs of application with regard to dataset sizes. If mechanisms were in place to customize a blockchain solution with consensus requirements (for example 85%) perhaps other ledger criteria can be examined.

A potential use case for issues discussed in this paper could be a smart-contract consensus for hash digest accuracy and/or provenance for application updates. An agreement immediately prior to release could prove to be a useful deterrent.

References

(2019, April). Global Incident Response Report. Retrieved from https://www.carbonblack.com/global-incident-response-threat-report/april-2019

Alumni, B. (2017, November 12). Target under Attack. Retrieved from https://digital.hbs.edu/platform-rctom/submission/target-under-attack

Newman, L. H. (2018, April 17). Inside the Unnerving Supply Chain Attack That Corrupted CCleaner. Retrieved from https://www.wired.com/story/inside-the-unnerving-supply-chain-attack-that-corrupted-ccleaner/

Seals, T. (2019, April 2). ThreatList: Half of All Attacks Aim at Supply Chain. Retrieved from https://threatpost.com/half-all-attacks-supply-chain/143391/

Mokbel, M. (2019, April 22). Analyzing C/C Runtime Library Code Tampering in Software Supply Chain Attacks. Retrieved from https://blog.trendmicro.com/trendlabs-security-intelligence/analyzing-c-c-runtime-library-code-tampering-in-software-supply-chain-attacks/

Singer, P. W. (2004, April). Warriors for Hire in Iraq. Retrieved from https://www.brookings.edu/articles/warriors-for-hire-in-iraq/

Daniel Carbonaro, decarbonaro@gmail.com

Paulsen, C., Paulsen, C., Boyens, J., Bartol, N., & Winkler, K. Criticality analysis process model: prioritizing systems and components, Criticality analysis process model: prioritizing systems and components1–94 (2018).

Boyens, J., Paulsen, C., Moorthy, R., & Bartol, N. Supply Chain Risk Management Practices for Federal Information Systems and Organizations, Supply Chain Risk Management Practices for Federal Information Systems and Organizations1–282 (2015).

B. S. I. ISO 28001:2007 SECURITY MANAGEMENT SYSTEMS FOR THE SUPPLY CHAIN -- BEST PRACTICES FOR IMPLEMENTING SUPPLY CHAIN SECURITY, ASSESSMENTS AND PLANS -- REQUIREMENTS AND GUIDANCE, ISO 28001:2007 SECURITY MANAGEMENT SYSTEMS FOR THE SUPPLY CHAIN -- BEST PRACTICES FOR IMPLEMENTING SUPPLY CHAIN SECURITY, ASSESSMENTS AND PLANS -- REQUIREMENTS AND GUIDANCE 1–27 (n.d.). LBK.

Chapple, M., Stewart, J. M., & Gibson, D. (2018). *11. (Isc)2 Cissp Certified Information Systems Professional Official Study Guide* (8th ed.). Indianapolis, IN: John WIley & Sons.

Robitalle, D. (2014, February 12). Self-Certification Is Not a Real Thing. Retrieved from https://www.qualitydigest.com/inside/quality-insider-column/self-certification-not-real-thing-021214.html

Leswing, K. (2018, October). The company accused of selling Apple and Amazon data servers compromised by Chinese spies is getting crushed - it's lost half of its value today . Retrieved from https://www.businessinsider.com/supermicro-share-price-crushed-by-report-it-sold-servers-compromised-by-chinese-spies-2018-10

P. C. (2013, June 13). Infosec Risk Management: Art, Science or Philosophy? Retrieved from https://www.tripwire.com/state-of-security/risk-based-security-for-executives/risk-management/infosec-risk-management-art-science-or-philosophy/

Whitney, Lance. “Why Third-Party Providers Pose a Security Risk to Organizations.” *Tech Republic*, Apr. 2019, https://www.techrepublic.com/article/why-third-party-providers-pose-a-risk-to-organizations/.

Muresan, Razvan. “Even with the Greater Emphasis on Cyber Security, Many Organizations Still Struggle to Protect Themselves.” *Security Boulevard*, June 2019, https://securityboulevard.com/2019/06/even-with-the-greater-emphasis-on-cyber-security-many-organizations-still-struggle-to-protect-themselves/

Gazdecki, Andrew. “Proof-Of-Work And Proof-Of-Stake: How Blockchain Reaches Consensus.” *Forbes*, 28 Jan. 2019,

https://www.forbes.com/sites/forbestechcouncil/2019/01/28/proof-of-work-and-proof-of-stake-how-blockchain-reaches-consensus/#1faea52668c8.

Last Updated: December 15th, 2019

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS Miami 2020	Miami, FLUS	Jan 13, 2020 - Jan 18, 2020	Live Event
SANS Threat Hunting & IR Europe Summit & Training 2020	London, GB	Jan 13, 2020 - Jan 19, 2020	Live Event
SANS Tokyo January 2020	Tokyo, JP	Jan 20, 2020 - Jan 25, 2020	Live Event
SANS Anaheim 2020	Anaheim, CAUS	Jan 20, 2020 - Jan 25, 2020	Live Event
Cyber Threat Intelligence Summit & Training 2020	Arlington, VAUS	Jan 20, 2020 - Jan 27, 2020	Live Event
SANS Amsterdam January 2020	Amsterdam, NL	Jan 20, 2020 - Jan 25, 2020	Live Event
MGT521 Beta Two 2020	San Diego, CAUS	Jan 22, 2020 - Jan 23, 2020	Live Event
SANS San Francisco East Bay 2020	Emeryville, CAUS	Jan 27, 2020 - Feb 01, 2020	Live Event
SANS Vienna January 2020	Vienna, AT	Jan 27, 2020 - Feb 01, 2020	Live Event
SANS Las Vegas 2020	Las Vegas, NVUS	Jan 27, 2020 - Feb 01, 2020	Live Event
SANS Security East 2020	New Orleans, LAUS	Feb 01, 2020 - Feb 08, 2020	Live Event
SANS Northern VA - Fairfax 2020	Fairfax, VAUS	Feb 10, 2020 - Feb 15, 2020	Live Event
SANS New York City Winter 2020	New York City, NYUS	Feb 10, 2020 - Feb 15, 2020	Live Event
SANS London February 2020	London, GB	Feb 10, 2020 - Feb 15, 2020	Live Event
SANS Dubai February 2020	Dubai, AE	Feb 15, 2020 - Feb 20, 2020	Live Event
SANS Scottsdale 2020	Scottsdale, AZUS	Feb 17, 2020 - Feb 22, 2020	Live Event
SANS San Diego 2020	San Diego, CAUS	Feb 17, 2020 - Feb 22, 2020	Live Event
SANS Brussels February 2020	Brussels, BE	Feb 17, 2020 - Feb 22, 2020	Live Event
Open-Source Intelligence Summit & Training 2020	Alexandria, VAUS	Feb 18, 2020 - Feb 24, 2020	Live Event
SANS Training at RSA Conference 2020	San Francisco, CAUS	Feb 23, 2020 - Feb 24, 2020	Live Event
SANS Secure India 2020	Bangalore, IN	Feb 24, 2020 - Feb 29, 2020	Live Event
SANS Manchester February 2020	Manchester, GB	Feb 24, 2020 - Feb 29, 2020	Live Event
SANS Jacksonville 2020	Jacksonville, FLUS	Feb 24, 2020 - Feb 29, 2020	Live Event
SANS Zurich February 2020	Zurich, CH	Feb 24, 2020 - Feb 29, 2020	Live Event
SANS Secure Japan 2020	Tokyo, JP	Mar 02, 2020 - Mar 14, 2020	Live Event
SANS Munich March 2020	Munich, DE	Mar 02, 2020 - Mar 07, 2020	Live Event
ICS Security Summit & Training 2020	Orlando, FLUS	Mar 02, 2020 - Mar 09, 2020	Live Event
SANS Northern VA - Reston Spring 2020	Reston, VAUS	Mar 02, 2020 - Mar 07, 2020	Live Event
Blue Team Summit & Training 2020	Louisville, KYUS	Mar 02, 2020 - Mar 09, 2020	Live Event
SANS Jeddah March 2020	Jeddah, SA	Mar 07, 2020 - Mar 12, 2020	Live Event
SANS St. Louis 2020	St. Louis, MOUS	Mar 08, 2020 - Mar 13, 2020	Live Event
SANS Paris March 2020	Paris, FR	Mar 09, 2020 - Mar 14, 2020	Live Event
SANS Austin Winter 2020	OnlineTXUS	Jan 06, 2020 - Jan 11, 2020	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced