SUPPLY CHAIN RISK MANAGEMENT ASSESSMENT SERVICES

Second Renaissance ®

This whitepaper includes data that shall not be disclosed outside the intended recipient and shall not be duplicated, used, or disclosed – in whole or in part – for any purpose other than to inform customers and potential customers of Company techniques and procedures. This restriction does not limit the recipient's right to use information contained in these data if they are obtained from another source without restriction. The data subject to this restriction are contained within all sheets.

EXECUTIVE SUMMARY

In an increasingly outsourced world, where cloud and managed services are displacing owned and operated IT, the end user has almost no visibility into the supply chain of hardware, software, and processes that comprise the services received. While the benefits of these services are irrefutable, there is an increasing risk to organizations' missions through the IT and Communications Supply Chain.

In June 2018, hackers exploited automated software update systems for technology company ASUS to push out backdoor trojans to over 500,000 users. The trojan was pushed out through trusted, legitimate ASUS systems, which bypassed traditional security checkpoints[1]. Supply Chain attacks have continued to increase in sophistication and impact, and are quickly becoming a favorite tactic of Advanced Persistent Threats[2].

To combat this increasingly used threat vector, organizations must consider and assess their supply chain within risk management. By assessing essential organizational elements and functions, a comprehensive understanding of the organizations' preparedness and resilience against supply chain attacks is formed, with actionable strengths and weaknesses. Additionally, by performing supply chain threat hunting, tangible impacts of supply chain threats are identified and ultimately remediated.

[1] Read more on the ASUS supply chain attack on the Symantec Threat Intelligence Brief.
[2] Read more on the increased use of supply chain attacks by Advanced Persistent Threats on Wired.

SUPPLY CHAIN RISK MANAGEMENT ASSESSMENT SERVICES

Cybersecurity Supply Chain Risk Management (C-SCRM) is the process of identifying, assessing, and mitigating the risks associated with the global and distributed nature of Information and Communication Technology product and service supply chains (as defined by NIST SP 800-161). Incorporating C-SCRM into organization processes includes participation and leadership within acquisitions, enterprise architecture, and cybersecurity programs. Assessing C-C-SCRM includes evaluating performance of multiple organizational elements and functions using the NIST Risk Management Framework (RMF) and supplemental guidance within NIST SP 800-161r1, as well as performing supply chain threat hunting. Aspects of an organization to be assessed include:

- Acquisition
- Threat intelligence
- Risk management planning
- Supply chain visibility and tracking
- Incident response

By assessing these five organizational elements and functions, a comprehensive understanding of the organizations' preparedness and resilience against supply chain attacks is formed, with actionable strengths and weaknesses. By performing supply chain threat hunting, tangible impacts of supply chain threats are identified and ultimately remediated.

PURPOSE

The purpose of this document is to establish the need and authorities for organizational C-SCRM, identify key aspects of a C-SCRM program, and establish a methodology for comprehensive assessment of an organization's resiliency against cybersecurity threats through the supply chain.

NEED AND AUTHORITY

All organizations that use information and communication technology should be aware of supply chain risk. Private sector businesses are increasingly targeted for their proprietary data and access to their customers. Breaches lead to loss in customer confidence with serious financial implications[3]. In June 2018, hackers exploited automated software update systems for technology company ASUS to push out backdoor trojans to over 500,000 users. The trojan was pushed out through trusted, legitimate ASUS systems, which bypassed traditional security checkpoints[4]. Supply Chain attacks are increasing in number and sophistication, and are quickly becoming a favorite tactic of Advanced Persistent Threats (APTs)[5]. APTs target private organizations, as well as state and local governments. As such, those

[3] Read more regarding the cost of cyber breaches on https://www.cmswire.com/information-management/the-cost-of-a-cyber-breach/.
[4] Read more on the ASUS supply chain attack on the Symantec Threat Intelligence Brief.

[5] Read more on the increased use of supply chain attacks by Advanced Persistent Threats on Wired.

organizations must be aware of supply chain risk and should implement C-SCRM programs to protect against such threats.

Federal organizations should implement C-SCRM for the same reasons as private sector organizations; as well as to comply with Federal mandates on the subject. Office of Management and Budget (OMB) Circular A-130, published July 28, 2016, describes Government organizations' requirements for C-SCRM. OMB A-130 specifies that Government organizations must:

1. Consider supply chain security issues for all resource planning and management activities throughout the system development life cycle;
2. Analyze risks (including supply chain risks) associated with potential contractors and the products and services they provide for all IT acquisitions; and
3. Allocate risk responsibility between Government and contractor when acquiring IT.
4. Develop, implement, document, maintain, and oversee agency-wide information security and privacy programs; and
5. Implement supply chain risk management principles to protect against the insertion of counterfeits, unauthorized production, tampering, theft, insertion of malicious software, as well as poor manufacturing and development practices throughout the system development life cycle;
6. Develop supply chain risk management plans as described in NIST SP 800-161 Rev1 (C-SCRM Practices) to ensure the integrity, security, resilience, and quality of information systems.

Beyond OMB Circular A-130, the NIST Cyber Security Framework (CSF) includes 6 controls within a C-SCRM family, and NIST 800-161 includes a C-SCRM control overlay to the NIST 800-53 controls typically used for information security and privacy assessment.

KEY C-SCRM FUNCTIONS

Comprehensive C-SCRM programs cut across an organization, including acquisitions, threat intelligence, risk management planning, supply chain visibility and tracking, and incident response. Each of the five key elements of C-SCRM are integral to organization resilience, and have associated controls from NIST 800-53 and/or 800-161.

Acquisition

Organizations obtain IT systems and services through acquisitions. During the process of acquisition, the government has the responsibility to *analyze risks (including supply chain risks) associated with potential contractors and the products and services they provide for all IT acquisitions*, and *allocate risk responsibility between Government and contractor when acquiring IT (OMB A-130)*. NIST groups all acquisition-related controls into the System and Services Acquisition (SA) control family. Organizations should consider C-SCRM when determining systems and services to acquire. This includes the acquisition

FIVE ELEMENTS OF SCRM

Incident Response for supply chain attacks involves multi-organization information sharing and response.

Supply Chain Visibility is the continuous monitoring of technologies, processes, and technologies that impact end products and services supporting the organization's mission.

Threat intelligence gathering and analysis feds threat hunting, improves supply chain visibility, and prepares incident responce teams.

Supply chain risks must be included in the organization's risk management processes, including supply chain risk management plans.

Acquisition strategy includes assessment of supply chain risk prior to contract award, and writing in cybersecurity requirements within awards.

SECOND RENAISSANCE

This image shall not be duplicated, used, or disclosed – in whole or in part – without written concent from Second Renaissance Incorporated.

Incident Response

As cyber attacks throughout the supply chain increase, organizations' incident response capabilities should include procedures for handling supply chain incidents. Addressing an organization-wide threat that is built into the hardware of 10,000 laptops requires a vastly different incident response plan than a network-based distributed denial of service attack, which is also vastly different from handling the fallout of an incident that originated from a supplier's external information system.

Relevant Controls: *IR-1, IR-4, IR-6*

Risk Management Planning

Supply chain risks should be considered alongside other risks to the organization's mission. OMB A-130 requires federal organizations to *develop supply chain risk management plans as described in NIST SP 800-161 (C-SCRM Practices) to ensure the integrity, security, resilience, and quality of information systems*. The risk management program should be designed to incorporate supply chain risk in its assessments, in the overall risk management planning, in handling of external information systems, and in handling interconnections.

Relevant Controls: *PM-1, CM-10, CA-2, CA-3, AC-20*

Supply Chain Visibility

Supply chain visibility is the most stand-alone element of C-SCRM. While this element of an C-SCRM program can be incorporated into asset and inventory programs, it can require additional resources to implement the requirement to create visibility and tracking of portions of information and communication technologies' supply chains outside of the organization. To address this unique challenge, the Provenance Control Family was created in NIST 800-161. Aspects of Provenance controls, along with Maintenance, Physical and Environmental Security, Contingency Planning, and Configuration Management controls combine to provide the organization with visibility into its supply chain, and associated risks.

Relevant Controls: *PV-1, PV-2, PV-3, MA-7, PE-16, PE-18, PE-20, CP-8, CM-8*

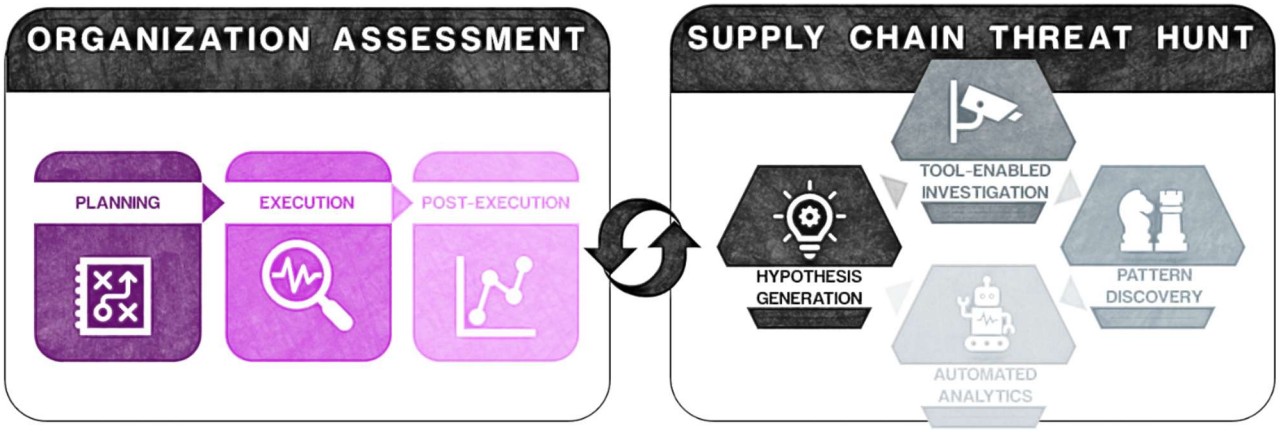
Threat Intelligence

Cybersecurity Threat Intelligence feeds the organization with vital information on threats so that resources can be prioritized efficiently. For C-SCRM, the supply chain threats must be included in the threat intelligence program's capabilities; from research, analysis, recognized TTPs (Tactics, Techniques, and Procedures), and briefings. The information sharing from threat intelligence equips acquisitions, operations, and security assessment teams with information needed to deal with supply chain risks.

Relevant Controls: *PM-12, PM-16*

C-SCRM ASSESSMENT METHODOLOGY

Second Renaissance approaches C-SCRM assessments in two phases: an organization assessment, and supply chain threat hunting. The organization assessment provides an understanding of organizational maturity regarding supply chain risk management, and recommended improvements based on Federal requirements. Threat hunting provides validation of the organization assessment, as well as targeted areas of improvement based on practical testing and evaluation.



Phase 1: Organization Assessment

Second Renaissance performs information systems security assessments using a flexible methodology that accommodates a wide range of differing scopes and timelines. While the methodology only has three phases – Planning, Execution, and Post-Execution – the processes and templates for each phase are robust and numerous. Our Security Assessment Methodology is aligned to NIST 800-115, and is flexible enough to accommodate all information security assessment requirements, including assessing supply chain risk management.

PLANNING – All assessments are initiated once research of the organization and associated systems/programs has been identified. The *Kickoff Deck* is tailored for C-SCRM assessments, associated programs, and relevant controls; and the assessor team holds the kickoff meeting to initiate the kickoff with relevant stakeholders. *Rules of Engagement forms* are signed at the conclusion of the kickoff meeting, and appropriate populations (also referred to as sample size) are agreed upon with system personnel. While Second Renaissance uses a simple *Sample Size Formula* to determine the appropriate volumes to test, organization personnel may have pertinent information that can change the desired or available sample population to use for testing.

Following the kickoff, the assessor team builds a Security Assessment Plan (SAP) aligned to the C-SCRM Methodology and the Five Key Elements of an C-SCRM Program, and the Requirements Traceability Matrix (RTM) of controls to assess from the *RTM Template* (See Appendix A).

EXECUTION – The assessor team starts the Execution phase once all stakeholders are ready – assessors prepared, system personnel available, and the programs/systems are in an assessable state (e.g. not during an upgrade). Multiple stakeholder groups will likely be involved in an C-SCRM assessment, as the five key elements of an C-SCRM program are typically managed by separate divisions within an

organization. During this portion of the organization assessment, the assessment team is focused on identifying and validating weaknesses through scanning, examination, testing, interviewing, and reviewing documentation. The assessment team uses the RTM populated with C-SCRM controls specified in Appendix A, to assess the organization's C-SCRM capability in five key areas:

- Acquisitions
- Incident Response
- Risk Management Planning
- Supply Chain Visibility
- Threat Intelligence

POST-EXECUTION – The Post-Execution phase begins once all execution tasks are completed. The assessor team analyzes results captured within artifact evidence and assessment results within the RTM. The Security Assessment Report (SAR) is populated within this information. The SAR includes strengths, as well as prioritized weaknesses the organization should address to improve its resilience against supply chain exploits.

In addition to the SAR and included Executive Summary, Second Renaissance also develops an *Outbrief Deck* from our Outbrief Deck Template. The Outbrief meeting mirrors the kickoff meeting and includes the same participants. The SAR is reviewed at a high level, and the assessors answer any questions about their findings and recommendations.

Phase 2: Supply Chain Threat Hunting

Supply chain threat hunting follows our Threat Hunting Methodology, which consists of hypothesis generation, tool and technique enabled investigation, pattern and TTP discovery, and automated analytics. The primary difference between a typical threat hunting exercise and a supply chain threat hunt is that typical hunting is confined to the bounds of the organization's networks and systems. To hunt throughout the organization's supply chain involves coordination and partnership with other organizations and external information systems.

HYPOTHESIS GENERATION – A hunt starts with creating a hypothesis, or an educated guess, about a potential area of the supply chain that may be susceptible to exploit. Hypotheses can come from any number of sources and are best when aligned to recent cyber intelligence. Formulating and tracking hypotheses includes preparation activities and mission analysis. Threat Hunters prepare by developing a deep understanding of the organization's supply chain, authorized assets, configurations, and critical data located on their network. Threat Hunters also perform mission analysis to understand potential value targets for adversaries. This information is used to focus Threat Hunters and ultimately give them direction needed to hunt for adversaries who may already be exploiting the organization's supply chain and its data.

TOOL AND TECHNIQUE ENABLED INVESTIGATION –Second, hypotheses are investigated via various tools and techniques, including Linked Data Analysis and visualizations. Effective tools will leverage both raw and linked data analysis techniques such as visualizations, statistical analysis, or machine learning to fuse disparate cybersecurity datasets. Linked Data Analysis is particularly effective at laying out the data necessary to address the hypotheses in an understandable way, and so is a critical component for a

hunting platform. Linked data can even add weights and directionality to visualizations, making it easier to search large data sets and use more powerful analytics. Many other complementary techniques exist, including row-oriented techniques like stack counting and datapoint clustering. Analysts can use these various techniques to traverse the supply chain and identify exploitable areas as well as malicious patterns in the data and reconstruct complex attack paths to reveal an attacker's Tactics, Techniques, and Procedures (TTPs).

PATTERN AND TTP DISCOVERY – Next, tools and techniques uncover new malicious patterns of behavior and adversary TTPs. This is a critical part of the hunting cycle. An example of this process could be that a previous investigation revealed that a user account has been behaving anomalously, with the account sending an unusually high amount of outbound traffic. After conducting a Linked Data investigation, it is discovered that the user's account was initially compromised via an exploit targeting a third-party service provider of the organization. This TTP (initial compromise via a third-party system via particular type of malware) should be recorded, shared (both internally and externally), and tracked within the context of a larger attack campaign. Linked data relationships will also contextually reveal what other accounts were associated with the compromised third-party service.

Threat Hunters receive the greatest return on their efforts by focusing on uncovering adversary TTPs. TTPs reflect an attacker's behavior, and behavior requires a significant time and monetary investment to modify. By focusing on detecting and responding to adversary TTPs, Threat Hunters gain an advantage by operating directly on adversary behaviors, rather than adversary toolsets.

AUTOMATED ANALYTICS – Lastly, successful hunts form the basis for informing and enriching automated analytics. Once a successful technique to find adversary behavior has been uncovered, the technique is automated within the security operations toolset and/or the supply chain visibility capability and tools. There are many ways this can be done, including developing a saved search to run regularly, creating new analytics using tools like Apache Spark, R, or Python, or by even providing feedback to a supervised machine learning algorithm confirming that an identified pattern is malicious.

The hunting methodology is a simple but effective process that can radically enhance an organization's understanding, visibility, and resiliency towards supply chain attacks. It is most effective when it is used together with C-SCRM organization assessment of an organization with an existing cybersecurity program; complementing existing cybersecurity risk management efforts that most organizations already have in place.

ABOUT SECOND RENAISSANCE

Second Renaissance Inc. was founded in 2012 to bring a unique style of cybersecurity and IT consulting to the Federal, State, and Local governments of the United States. We believe that art and science are connected, and that bringing well-rounded expertise to the table unlocks greater levels of value for our customers. Data without a message is just a bunch of numbers. Information without a story can be confusing. Words without visualization can tell an incomplete story. Second Renaissance empowers clients to communicate actionable information to leadership, align action to strategy, and build a high-performing action-oriented culture.

We provide cybersecurity and IT transformation management services; developing strategies and executing against mission objectives to strengthen our nation locally and globally. We work hand-in-hand with our customers to build robust cybersecurity programs that continually improve to integrate with and support the greater mission. Second Renaissance provides security assessments, managed security operations, threat hunting and incident response, organizational change management, cybersecurity risk management, and information system continuous monitoring services.

REFERENCES

1. OMB Circular A-130, *Managing Federal Information as a Strategic Resource*: https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf
2. NIST SP 800-53 Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*: https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final
3. NIST SP 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*: https://csrc.nist.gov/publications/detail/sp/800-161/final
4. Symantec, *Threat Intelligence Brief*: Symantec Threat Intelligence Brief
5. Wired, *A Mysterious Hacker Group is on a Supply Chain Hijacking Spree*: https://www.wired.com/story/barium-supply-chain-hackers/
6. CMS Wire, The Cost of a Cyber Breach: https://www.cmswire.com/information-management/the-cost-of-a-cyber-breach/

APPENDIX A: C-SCRM CONTROLS

The C-SCRM Assessment Methodology identifies 63 controls, which are described within NIST 800-53 and further tailored in supplemental guidance captured within 800-161. The Supply Chain Risk Management controls related to assessing Supply Chain Visibility were originally created specifically for 800-161, and have been added to the 800-53 catalog in Revision 5. Of the 63 controls, 45 are high priority for any organization trying to build a solid understanding of their supply chain risk.

Control Family	CTRL ID	CTRL NAME	PRIORITY
Supply Chain Risk Management (SR)	SR-1	Policy and Procedures	High
	SR-2	Supply Chain Risk Management Plan	High
	SR-3	Supply Chain Controls and Processes	High
	SR-4	Provenance	High
	SR-5	Acquisition Strategies, Tools, and Methods	High
	SR-6	Supplier Assessments and Reviews	High
	SR-7	Supply Chain Operations Security	High
	SR-8	Notification Agreements	Moderate
	SR-9	Tamper Resistance and Detection	High
	SR-10	Inspection of Systems or Components	Moderate
	SR-11	Component Authenticity	High
	SR-12	Component Disposal	Moderate
Access Control (AC)	AC-2	Account Management	High
	AC-3	Access Enforcement	High
	AC-6	Least Privilege	High
	AC-17	Remote Access	High
	AC-20	Use of External Systems	High
Awareness and Training (AT)	AT-2	Literacy Training and Awareness	Moderate
	AT-3	Role-Based Training	Moderate
Audit and Accountability (AU)	AU-2	Event Logging	High
	AU-3	Content of Audit Records	High
	AU-12	Audit Record Generation	High
Assessment, Authorization, and Monitoring (CA)	CA-2	Control Assessments	High
	CA-3	Information Exchange	Moderate
	CA-7	Continuous Monitoring	High
	CA-8	Penetration Testing	Moderate
Configuration Management (CM)	CM-2	Baseline Configuration	High
	CM-3	Configuration Change Control	High
	CM-4	Impact Analyses	Moderate
	CM-8	System Component Inventory	High
Contingency Planning (CP)	CP-2	Contingency Plan	High
	CP-9	System Backup	High

Control Family	CTRL ID	CTRL NAME	PRIORITY
Incident Response (IR)	IR-4	Incident Handling	High
	IR-6	Incident Reporting	High
Maintenance (MA)	MA-3	Maintenance Tools	Moderate
	MA-4	Nonlocal Maintenance	High
	MA-5	Maintenance Personnel	Moderate
Media Protection (MP)	MP-6	Media Sanitization	High
Physical and Environmental Protection (PE)	PE-3	Physical Access Control	High
	PE-16	Delivery and Removal	Moderate
Planning (PL)	PL-2	System Security Plan	High
	PL-8	Security and Privacy Architectures	High
Program Management (PM)	PM-9	Risk Management Strategy	High
	PM-30	Supply Chain Risk Management Strategy	High
Risk Assessment (RA)	RA-3	Risk Assessment	High
	RA-5	Vulnerability Monitoring and Scanning	High
	RA-7	Risk Response	High
	RA-9	Criticality Analysis	High
System and Services Acquisition (SA)	SA-4	Acquisition Strategy	High
	SA-5	System Documentation	Moderate
	SA-8	Security and Privacy Engineering Principles	High
	SA-9	External System Services	High
	SA-10	Developer Configuration Management	Moderate
	SA-11	Developer Testing and Evaluation	Moderate
	SA-15	Development Process, Standards, and Tools	High
	SA-16	Developer-Provided Training	Low
	SA-22	Unsupported System Components	High
System and Communications Protection (SC)	SC-7	Boundary Protection	High
	SC-18	Mobile Code	Moderate
	SC-38	Operations Security	Moderate
System and Information Integrity (SI)	SI-3	Malicious Code Protection	High
	SI-4	System Monitoring	High
System and Information Integrity (SI)	SI-7	Software, Firmware, and Information Integrity	High