Leveraging a Tailorable Holistic Perspective of Supply Chain Risk

to Deliver Trustworthy IoT Systems

2022-07-27

Author:

Robert Martin
MITRE Labs, MITRE Corporation
ramartin@mitre.org

CONTENTS

FIGURES

TABLES

1 DEFINING SUPPLY CHAIN AND SUPPLY CHAIN SECURITY

Today supply chain and supply chain security topics have received unprecedented attention and coverage in our national discourse. These topics are discussed by many, but interpretations can differ in the minds of those involved in the conversation. In these discussions, we must be clear about which aspects associated concepts are included when conversing about a "supply chain" and which ones we are addressing. As shown in Figure 1-1, a supply chain moves items from initial ingredients and design to production, distribution and use by the customer, whether it be for fish, chips, or software.

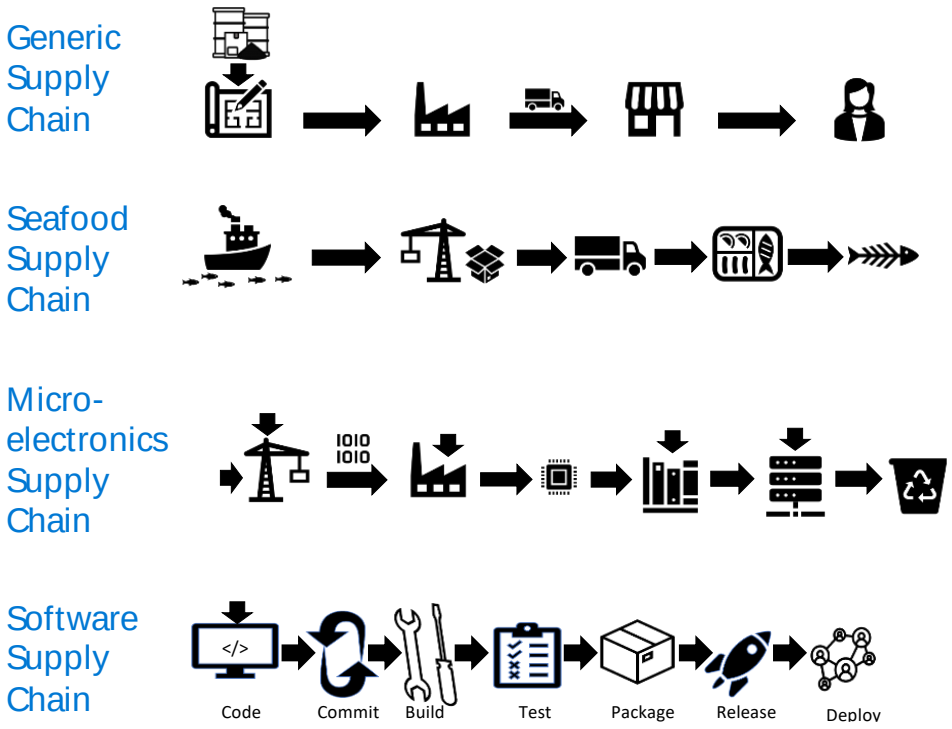

Figure 1-1. Examples of supply chains.

For example, when using the term supply chain, some will want to discuss the resilience of connected supply chains against disruptions from shortages of common elements, shared supply chain partners, transportation issues, or regional impacts. Others will be looking to map or illuminate the supply chains of a specific type of product. Some will wish to gain awareness about the management practices of the organization they deal with as well as mission risks caused from those suppliers and the suppliers' supply chains. Yet others will be focused on addressing domain specific supply chain risks (e.g., cyber-based capabilities, pharma, food stuffs, etc.).

Certain supply chain discussions will cover the acquisition and procurement activities to help organizations see and manage risks from supply chains. Then there are those that want to define and promote standards and norms for third-party risk management due diligence regarding

suppliers, supplies, and service providers but also consider aspects covered in domains identified above. All these things generally apply to the term "supply chain" while supply chain security focuses on the robustness, trustworthiness and resilience aspects of this broad topic.

Within the Industry IoT Consortium (IIC) Trustworthiness Task Group activities the focus on supply chains comes from their influence on the assurance of trustworthiness and impact on the trustworthiness of the IoT systems and their operations from the flow of assurance to the operational user, from the systems builder and the component builders as illustrated in Figure 1-2 below, which comes from the IIC's Trustworthiness Framework Foundations July 2021 document [*References*, 17].

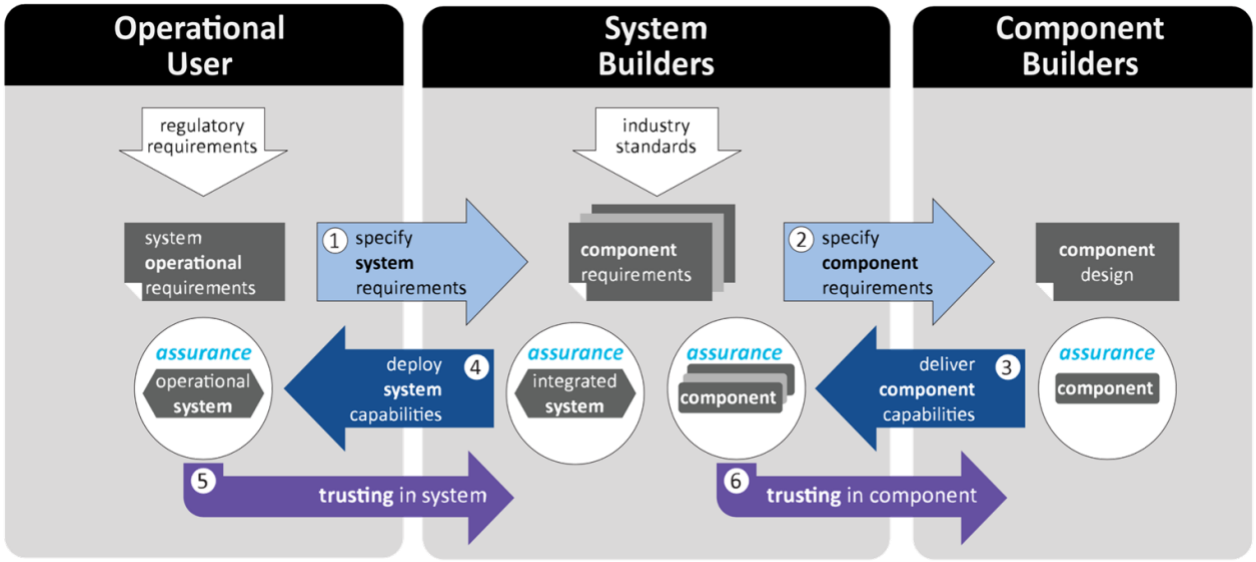

Figure 1-2. Integration and commonality of trust in the lifecycle of a complex system.

The remainder of this article will address the challenge of delivering trustworthy IoT systems in the face of supply chain risks, offering a comprehensive, tailorable and scalable holistic approach that industry and government can adopt to address this pressing issue.

2 BACKGROUND

The MITRE Corporation has been engaged for decades supporting the national and homeland security communities on supply chain risk issues and working with national and international standards organizations to reduce risks in global supply chain security. We have also been deeply engaged in projects that specifically focus on supply chain security for Information Communications Technology (ICT), cyber physicals systems, and IoT systems, including national security systems.

These projects also include highly sensitive nuclear and intelligence systems and safety critical systems and the "trustworthiness" of these systems, vendors and products. With today's

increased focus on the need for robust and resilient supply chains, trustworthy partners, and trustworthy components and systems that are globally manufactured, a reliable path to an understanding of the risks that can impact trustworthiness is essential. This path must be broadly understood, shared, and usable at scale.

As a method for addressing these supply chain security challenges, MITRE developed and introduced the System of Trust™ Framework. This framework is aimed at defining, aligning, and addressing the specific concerns and risks that stand in the way of organizations' trusting suppliers, supplies, and service providers.

More importantly, the framework offers a comprehensive, consistent, and repeatable methodology — for evaluating suppliers, supplies, and service providers alike — that is based on our decades of supply chain security experience, deep insights into the complex challenges facing the procurement community of interest, and a broad knowledge of the relevant shared thinking on this topic in literature and standards.

Here we describe the different components of the System of Trust framework [*References*, 1-3] and how they relate and integrate with industry and government efforts [*References*, 4-16]. This framework enumerates supply chain risks in the areas of suppliers, supplies, and services, and provides a methodology to assess those risks in a common, repeatable way for organizations to effectively communicate with each other about supply chain risks.

3 THE IMPETUS FOR A SYSTEM OF TRUST

Today there is wide diversity across organizations and practitioners in identifying the list of risks and approaches to risk assessment and conveying results of such assessments. From among identified aspects of supply chain security, the MITRE System of Trust (SoT) focuses on identifying and assessing the risks from your supplier, their supply items, and their service offerings. SoT is aimed at collecting, organizing, and sharing a common baseline of the supplier, supplies, and services risks that an organization may need to consider.

This collection of identified risks can begin as something unworkably large, highlighting the need for a methodology for selecting an operationally relevant sub-set of the body of knowledge of supply chain risks. This empowers organizations to conduct assessments in a practical, timely, and cost-efficient manner that focuses on the needs of the organization and allows for broad adoption, training, and automation.

4 SOT'S STRATEGIC GOAL

The goal of System of Trust is to offer a comprehensive and consistent methodology that can be tailored to meet industry and company needs to address supply chain security issues, leading to better traceability, reliability, and security of supply chains. MITRE's deep experience, as well as

investigations and discussions with a broad set of stakeholders in government, industry, and academia, have led to the discovery of several key elements that will enable SoT's goal, including:

1. Having a common taxonomy of supply chain risks for suppliers, supplies and services.
2. Creating consistent supply chain security assessments and risk discussions.
3. Informing data driven decisions about supply chain risks.
4. Supplying a broad understanding of the available sources for supply chain risk assessment information.
5. Supporting and promoting use of automation.
6. Providing for cost-efficient assessments.
7. Establishing pathways for broad adoption and training of supply chain security practices across diverse communities.

5 SYSTEM OF TRUST APPROACH

Progressing towards SoT's stated goal, in a manner that can scale and allows for a wide variety of uses by different industries, organizations, and types of supply chain domains, requires a comprehensive body of knowledge (BoK) that details the specific supply chain security risks from suppliers, supplies, and services. SoT hosts this BoK in an automation platform that enables organizations to develop sub-sets of the most relevant of these resources as profiles that can be used to perform assessments in a standardized and consistent fashion - thereby creating opportunities for comparable discussions and assessments of supply chain security issues internally and with external partners.

The tension between seeking the broadest, most inclusive capabilities and resourcing versus servicing needs that are tailored to prioritized requirements, has motivated much of the approach to implementing MITRE's System of Trust. A comprehensive and holistic body of knowledge describing every supply chain risk from suppliers, supplies, and services available to an organization, as illustrated in the left part of Figure 5-1 below, is unworkable on its own. Instead, we need a way to create a more narrowly defined, yet highly relevant, set of supply chain risks can be effectively evaluated to guide operational choices, activities, and decisions, as shown on the right side of Figure 5-1.

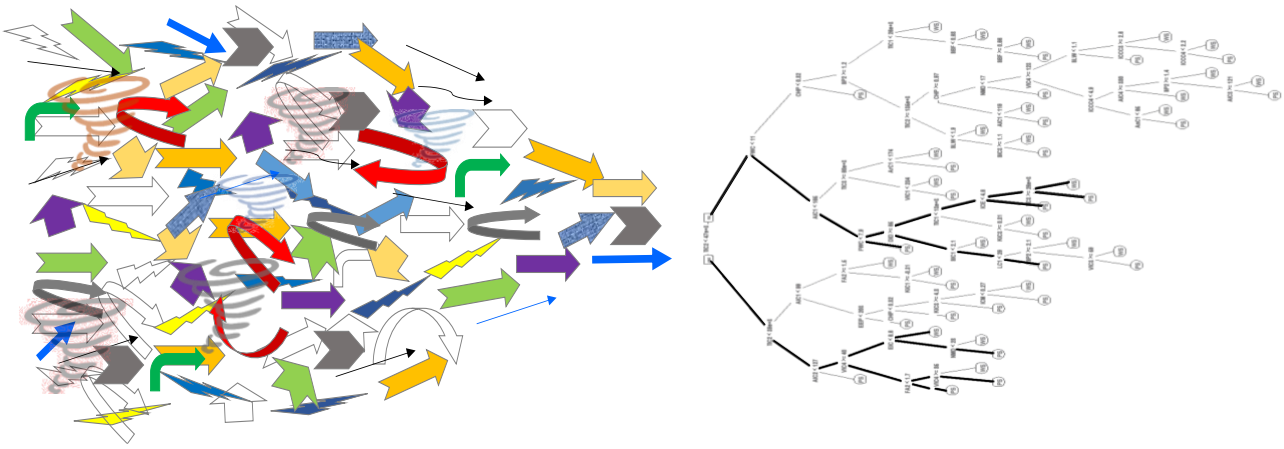

Figure 5-1. Address Chaos, Align & Organize, and then Simplify, Tailor & Use.

Specifically, we decided to develop the content of the SoT BoK in a managed data store that could be actively trimmed to an appropriate subset. That subset would be used as the basis of the evaluations and assessments driving decisions and choices. Until now, no known content management capabilities fit the needs for active BoK curation, tailoring, and assessment that could be shared and synchronized appropriately for separate deployments by a variety of organizations.

This challenge resulted in the development of the Risk Model Manager (RMM) - a cloud-native capability that provides the core underpinnings for developing a sharable supply chain risk taxonomy that is grounded in industry and government best practices, open-source components, cloud-native services, standards, and policy. The RMM was specifically developed to allow for active tailoring of the BoK into profiled sub-sets for use in assessment activities. While the current instantiations of the RMM are native to Amazon Web Services (AWS) environments, the architecture, and components of the RMM technical platform can form the basis of versions usable in other cloud or non-cloud container environments.

In order to support assessments that leverage subsets of the supplier, supplies, and services risks, each risk must include knowledge of its contribution to a risk scoring approach as well a scoring method that can adjust weighting to differing sets of risks in each profile. Additionally, each must support tailoring of those weights as part of the profile creation. We envision a variety of profiles created over time and plan to roll them into the baseline SoT BoK so that all RMM deployments can leverage them and, if they so choose, to share back for community use.

Finally, to foster broad adoption and understanding of how the System of Trust functions, MITRE will be providing a functional copy of the SoT RMM capability for public usage on the SoT website. Since evaluating products and services for specific risks can quickly become sensitive, the version of RMM provided will only allow for viewing the SoT BoK and selecting or creating a profile of the BoK. A spreadsheet export capability will provide a mechanism for downloading the resultant sub-set of the SoT BoK for evaluation on an organization's systems where they can protect the assessment appropriately.

6 SYSTEM OF TRUST BODY OF KNOWLEDGE

The current SoT BoK starts with the three top-level aspects of trust – suppliers, supplies, and services, shown in Table 6-1.

Trust Aspect	Definition
Supplier	Risks related to characteristics of a supplier of products or services, including their supply chain, that may potentially impact consumers of those products or services.
Supply	Risks related to characteristics of supplies (products), including their supply chain provenance and pedigree, that may potentially impact consumers of those products.
Service	Risks related to characteristics of services, including their supply chain provenance and pedigree, that may potentially impact consumers of those services.

Table 6-1. Supply chain security trust aspects.

These have seven, three, and four risk categories covering each of them respectively. For suppliers the top categories of risks are as shown in Table 6-2 below. The top categories for supplies and services are shown in Table 6-3 and Table 6-4 below.

Risk Category	Definition
External Influences	Risks related to characteristics of a supplier that affect its potential to be negatively influenced by external motivations or allegiances. In a nation-state context this is typically an issue of foreign influences and in the commercial context this would typically be a competitor's influence on a supplier.
Financial Stability	Risks related to financial health and stability characteristics of a supplier that affect its potential ongoing existence, operation, integrity, growth, technological advancement, and consistent supply/service delivery.
Maliciousness	Risks related to characteristics of a supplier that can negatively impact its customers, clients, partners or market through explicit intent, whether internally or externally driven, to violate legal/business norms or to cause harm.
Organizational Security	Risks related to characteristics of a supplier's personnel, facilities, transport and cyber security capabilities, policies, and practices that affects its potential to resist malicious actions and their impacts on their customers.
Organizational Stature	Risks related to geographical, geopolitical, structural or operational characteristics of a supplier that affect its potential to operate in an efficacious and resilient manner.
Quality Culture	Risks related to characteristics of a supplier's ability to reliably deliver quality supply item(s) and/or service(s).
Susceptibility	Risks related to characteristics of a supplier (industry sector, location, customers, etc.) including proactive management of such risks that affect the likelihood of them being targeted, compromised, or otherwise adversely affected by malicious actors causing risk to their customers.

Table 6-2. Supply chain security top-level risk categories for suppliers.

Risk Category	Definition
Counterfeit	Risks related to the authenticity of supplies (products) or services.
Hygiene	Risks affecting the ability of supplies (products) or services to perform as expected. This involves characteristics related to quality, security, resilience, etc.
Malicious Taint	Risks related to the integrity of supplies (products) or services.

Table 6-3. Supply chain security top-level risk categories for supplies.

Risk Category	Definition
Service Integrity	Risks related to the service being delivered unaltered.
Service Quality	Risks related to the service being delivered as specified.
Service Reliability	Risks related to the service being delivered consistently.
Service Security	Risks related to the service being delivered as expected in the face of malicious action.

Table 6-4. Supply chain security top-level risk categories for services.

Together with the elaborating sub-categories one level down, Figure 6-1 below illustrates the top of the SoT BoK.

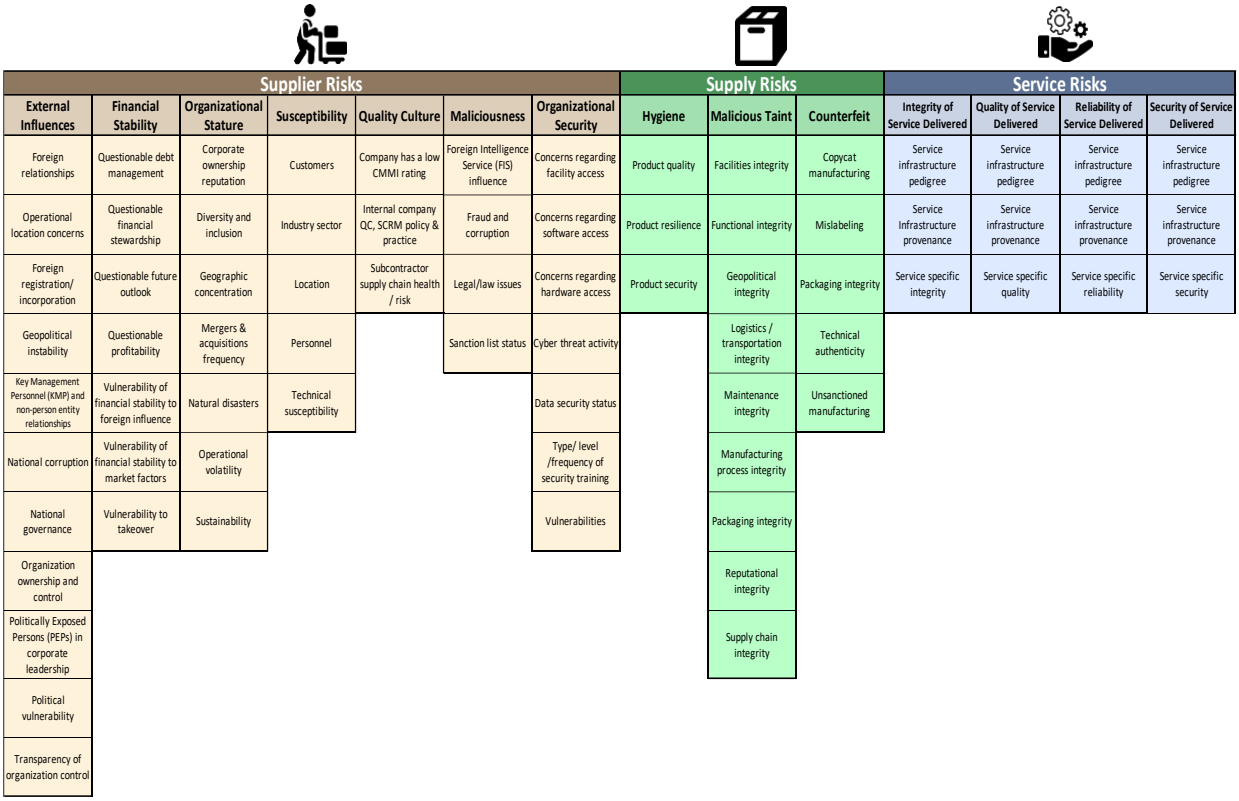

Figure 6-1. Top-Level set of supply chain security risks in the SoT BoK.

Beyond these top-level risk categories, the SoT BoK expands down to the specific risk factors that compose these concern categories. The organization of the taxonomy goes from the common to the specific. For example, the concern for counterfeits is *common* while the ways of identifying whether counterfeits are in your supply chain are *specific* to the type of supply item.

Detecting counterfeit micro-electronics would have different risk measures than, for example, counterfeit software, handbags, or sushi, yet for those specific businesses that focus on each of these types of products, the need to identify and address their industry's counterfeit items is critical to their businesses viability. The fuller scope of the SoT BoK includes more than 2,200 possible supply chain risks from suppliers, supplies, or services within the 14 top-level risk categories.

7 DRIVING FOR CONSISTENCY

One of the main elements required to achieve SoT's goal is consistency – whether that be consistency of:

- A specific organization's assessments over time and across their different groups that are doing evaluations,
- Across the various members of a supply chain as they each perform their due diligence in assessing their own suppliers, and the supplies and services they get from them; or
- Across an industry that has similar concerns and constraints.

Providing a path towards achieving differing types of consistency will require engagement and participation from all parts of our collective marketplace. There is business value in understanding the expectations and needs of your customers and having consistent expectations across industry sectors. This identified value offers a strong incentive for businesses as does having colleges and universities educate the future work force and leaders about supply chain risks in a manner that prepares graduates for varied career paths and professional endeavors.

Having an explicit methodology for scoring the individual risks, especially one that is supported by evidence, is a critical part of the System of Trust capability. This includes addressing how risk assessment findings are collected and can reflect incomplete data or missing information. Additionally, it must allow for reflection of the risk tolerance or sensitivity of an assessing organization to the different risk areas.

For example, foreign ownership of an entity can be a deal-breaker for some organizations in government but less of a concern for those in industry (unless of course that entity plans to supply those that have those concerns). For some types of transactions an organization may be highly concerned with whether a supplier's infrastructure is located in an area susceptible to weather or political events. The significance of these risks must be tailorable to reflect an organization's approach to assessing and addressing risks.

A final aspect of the SoT scoring approach is in addressing issues coming from aggregating many individual risk measurements together. There could be strong risk findings in a few items that get diluted by low-risk findings in others. But if strong risk findings point to risks that are critical to the organization then those findings cannot be hidden by a scoring approach that does not account for this use case. We are addressing all of these issues in the SoT scoring approach.

8 AWARENESS OF INFORMATION SOURCES FOR SUPPLY CHAIN SECURITY INSIGHTS

Another dimension of SoT's approach is to establish a broad understanding in the community regarding where information can be found to answer the various questions surrounding supply chain security risks. Some information about specific supply chain risks is readily available from government or other public sources. Examples include public filings, public information on

sanctions, news stories on indictments and security issue publications. Other risk questions require access to non-public or proprietary information and can involve resourcing the information directly from the supplier or by assessing the service or item of supply directly.

The ICT SCRM Task Force's Vendor Template is an example process that answers questions that could be collected directly from a supplier and used to answer SoT risk questions. There are additional risk questions that can be answered by looking at other sources, such as analyses of certifications and accreditations done on an organization, their workforce, facilities, and products. If, for example, an organization has been certified by a trusted 3rd party to have met one of these standards for security practices by their facilities, it would qualify as addressing SoT risk questions on that topic.

Finally, there will be restricted sources of information that could be used to gather insights on some supply chain risks. For government this may include law enforcement resources or information gathered by the intelligence community. In private industry it maybe information from past work with a supplier or service provider. SoT provides for the use of these types of sources as "general research."

SoT is exploring a mechanism for conveying examples of all the above as part of the SoT BoK and making them accessible as assessment information sources within the RMM tool itself. SoT is also working to incrementally expand the lists of sources in collaboration with industry and those providing the certifications and information sources. Similar to MITRE's established compatibility programs for initiatives like Common Vulnerabilities and Exposures (CVE) and Common Weakness Enumeration (CWE), the SoT program is establishing a process to allow organizations to share their adoption and use of the SoT taxonomy of risks.

This will enable the community at-large to see where market offerings fit into the strategic landscape of supply chain security capabilities and needs. SoT offers a consistent framework for identifying the scope and nature of issues requiring review and issues that have been addressed. This framework provides the insights necessary to construct the appropriate set of capabilities required to address individualized supply chain security needs.

9 COMMUNICATING RESULTS OF SOT ASSESSMENTS

Communicating the findings from a supply chain assessment is something that calls for careful planning and detailed execution. While there are lots of risks to consider when investigating your supplier, the supplies they offer, and services being provided, the key to managing those risks is to understand which ones represent a showstopper if they manifested and which ones would have strong impacts to the organization.

Reflecting the potential for impact in the scoring and weighting of the individual risks, as well as in the presentation of the findings from an assessment, is key to providing consistent, usable

results that are supported by data. When the data is questionable or incomplete, the uncertainty in the findings must be clearly indicated as a part of the results.

Additionally, the 14 top-level risk areas in SoT are separate areas of risk that do not easily or usefully combine. A healthy and financially stable supplier that has great facilities, personnel, and cyber security does not offset or mitigate the risks to your organization if they consistently deliver tainted, counterfeit, or substandard goods. Results have shown that SoT assessments are best represented in a series of nested radar diagrams[1] with explanatory text that describes the evidence of risk. Figure 9-1 shows the top-level of a notional assessment result in the RMM of two suppliers or items of supply.

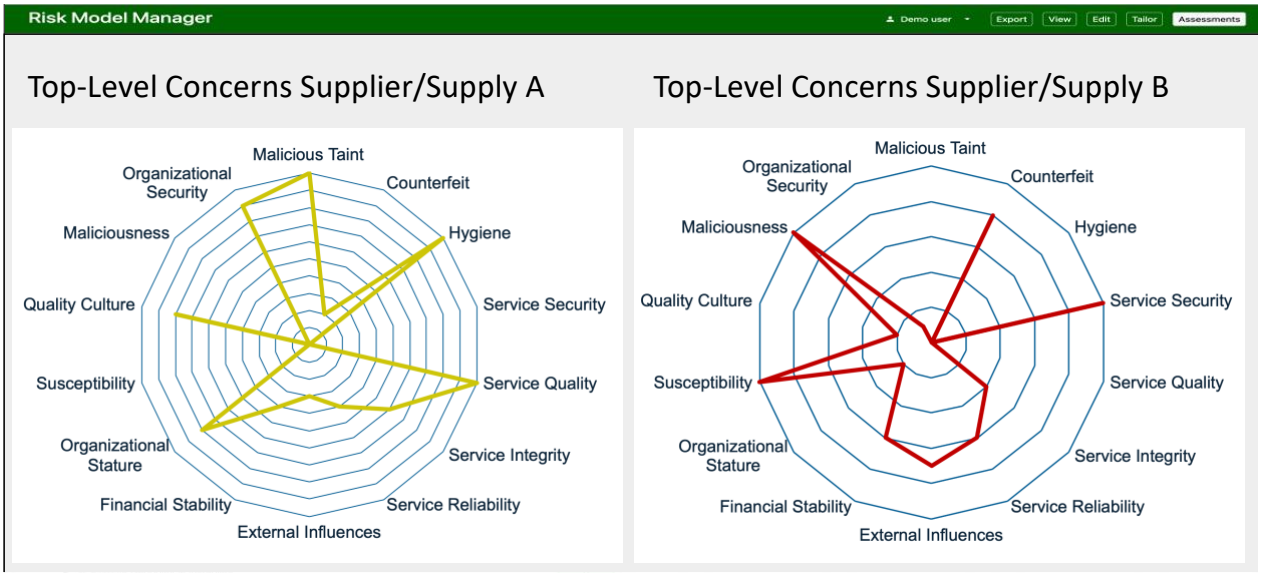

Figure 9-1. Top-level set of supply chain security assessed risks.

As part of the assessment process, the SoT RMM capability supports capturing the information obtained to determine the absence or presence of each particular risk. Given the general lack of historical statistics for supply chain security risks SoT offers measures for the different risk factors so that a series of observations about different aspects of the risk can be substantiated or refuted. Collectively these measures can be used to convey whether the risk in question is present to a degree that requires mitigation or avoidance.

The scoring mechanisms in SoT support a running evaluation of the top-level and underlying risk categories that show the number of risks assessed out of the total in scope for the assessment. This gives a measure of the completeness of the assessment and the range of possible final scores, from lowest to highest, once the remaining risks are assessed.

[1] Also referred to as kiviat charts or spider diagrams.

10 An Example IoT Supplier Assessment

As part of our exploration of all of the above, we conducted an initial set of assessments of a group of IoT component suppliers that were critical to one of our sponsors. These suppliers provided critical IoT-related capabilities crucial to the operational activities of the sponsor and the supplier's continued ability to be a trusted, reliable provider of the IoT capabilities were an important factor to the sponsor and their ability to do their job.

The focus of concern about these suppliers centered upon a "Supplier and Public Data Profile" with risks from the External Influences, Financial Stability, Maliciousness, Organizational Security and Organizational Stature sub-categories of the Supplier Trust Aspect and 26 specific risk factors that we could obtain publicly available data about. There were 11 suppliers in the group that was evaluated but we are showing the initial finding for three of 11 in radar plots shown in **Error! Reference source not found.**. Figure 10-2 shows the full details for supplier 10 along with the sub-categories of five of the seven supplier risk categories from Table 6-2 above.

From the perspective of a IoT supplier to an organization, the overall set of risks that Company 1 and Company 7 present are of a different level from those presented by Company 10. All three show no indications of External Influence risks as the assessment from public sources showed nothing beyond Green, when plotted as a stop-light chart for the sub-categories 13-19 listed in Figure 10-2 for External Influence. Similarly for Company 1 there was nothing to indicate that Maliciousness was present in the sub-categories 10-12, with Maliciousness plotting to zero for Company 1, but to non-zero for Company 7 and 10.

More disturbing, for Company 10, there was information available indicating that it had security issues that could make it a conduit of attack to its customers (sub-categories 8 & 9) and that it had financial stability issues (sub-categories 1-7).

When choosing your IoT suppliers, those that are providing the components for making Trustworthy IoT Systems, security and financial issues raise the possibility of undermining and disrupting your own capabilities and should be something to consider in choosing your suppliers.

Figure 10-1. Three suppliers of interest from set of 11 using SoT supplier and public data profile.

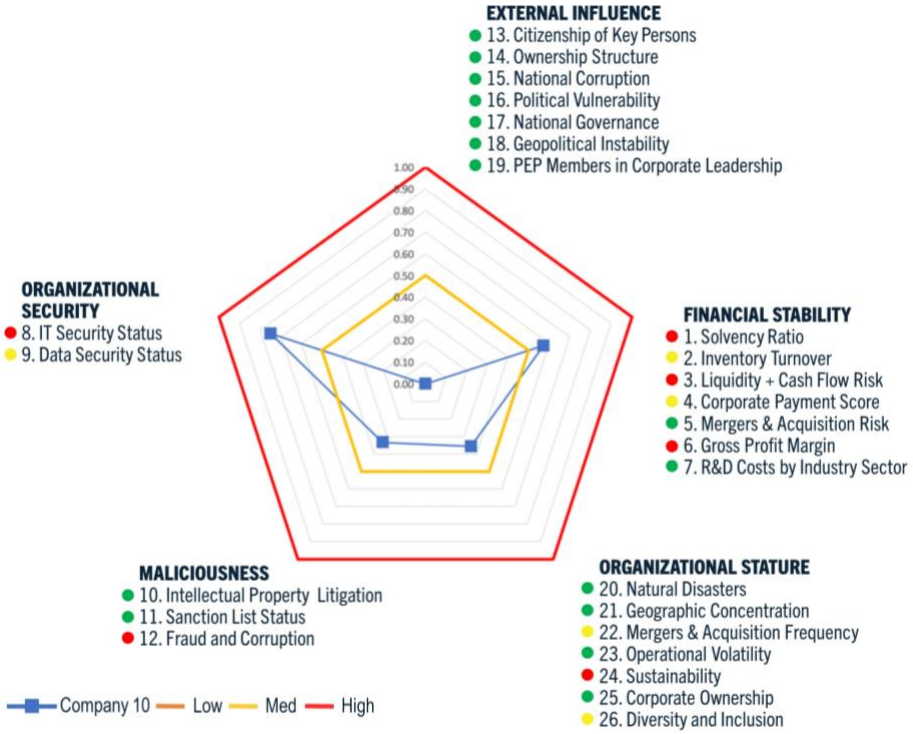

Figure 10-2. Supplier 10 assessment using the SoT supplier and public data profile.

The implications to your organizations of these findings and the need for mitigation or deciding to reduce your risk by going with a different supplier would be supported by this type of assessment and the supporting evidence it provides.

11 THE VISION

With the introduction and adoption of SoT vocabulary and concepts, the nature of interactions with others regarding supply chain security will simplify, become teachable, and become more efficient while at the same time the processes and practices surrounding day-to-day supply chain assurance work will be more consistent, automatable, and supported by evidence for all industries including those incorporating and leveraging IoT systems.

We believe SoT is the foundation needed for understanding supply chain risks, that IoT systems trustworthiness depends upon those supplying its constituent parts, and that it will be the key to securing robust and resilient supply chains, trustworthy partners, and trusted components and systems that are globally manufactured.

12 REFERENCES

1. MITRE, “The Supply Chain Security System of Trust: A Framework for the Concerns Blocking Trust in Supplies, Suppliers, and Services”, Cutter Business Technology Journal, Nov 2020.

2. MITRE, “Defining a System of Trust (SoT) as a Keystone Tool for Supply Chain Security”, American Bar Association SciTech Lawyer, Volume 17, Number 2, January 2021.
3. MITRE, “Trusting Our Supply Chains: A Comprehensive Data-Driven Approach”, January 2021.
4. The Open Group, “An Approach to Assessing Vendors to Lower Potential Risk of Outsourced Network Services”, Mar 2020.
5. The Open Group, “Open Trusted Technology Provider Standard (O-TTPS) – Mitigating Maliciously Tainted and Counterfeit Products - Parts 1 and 2 and ISO/IEC 20243-1:2018”, Version 1.1.1, 2018.
6. Department of Defense (DoD), “DoD Instruction 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks”, October 2018.
7. Department of Defense (DoD), “DoD Instruction 5000.90, Cybersecurity for Acquisition Decision Authorities and Program Managers”, Section 3.4. Cybersecurity in the Supply Chain, December 2020.
8. Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force, “ICT SCRM Task Force Threat Scenarios Report (Version 3)”, July 2021.
9. ICT SCRM Task Force, “ICT SCRM Task Force Vendor SCRM Template”, April 2021.
10. Israel National Cybersecurity Directorate, “Supply Chain Risk Management”, September 2021.
11. NIST, NISTIR 8276, “Key Practices in Cyber Supply Chain Risk Management: Observations from Industry”, February 2021.
12. NIST, Special Publication (SP) 800-161, Revision 1, “Supply Chain Risk Management Practices for Federal Information Systems and Organizations”, May 2022.
13. NIST, SP 800-218, "Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities", February 2022.
14. NIST, “Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products”, NIST Whitepaper, February 2022.
15. NASA, “NASA’s Information & Communications Technology (ICT) Supply Chain Risk Management (SCRM)”, May 2019.
16. Telecommunications Industry Association (TIA) Quality Excellence for Suppliers of Telecommunications (QuEST) Forum, “TIA QuEST Forum SCS 9001® Supply Chain Security Management System Handbook”, SCS 9001:2021.
17. IIC, “Trustworthiness Framework Foundations”, July 2021.

13 ACKNOWLEDGEMENTS

The views expressed in the IIC Journal of Innovation are the author’s views and do not necessarily represent the views of their respective employers nor those of the Industry IoT Consortium®.

➢ Return to *IIC Journal of Innovation landing page* for more articles and past editions.