TRUSTING OUR SUPPLY CHAINS: A COMPREHENSIVE DATA-DRIVEN APPROACH

By Robert A. Martin

Trust and trustworthiness of supply chains is an issue confronting communities around the world, including U.S. government agencies and the thousands of commercial enterprises that support them.

The COVID-19 pandemic has brought supply chain security (SCS) into sharpened focus, and many inadequacies have surfaced regarding timely access to reliable stocks of personal protective equipment, medical devices, and food supplies, to name a few.

This is not a new challenge. In the 2000s, many U.S. government practices related to supply chain logistics management, dating from the Cold War era, were extended into the broader commercial information and communications technology (ICT) marketplace as those technologies and the efficiencies they brought to business and government became key enablers of the information economy.

For many suppliers providing the Department of Defense with commercial goods, the concept of a "cleared industry partner" became part of their way of life.

At the same time, the computerization of everything gave rise to pervasive cyber threats – including those stemming from vulnerabilities inherent in repurposed software of often dubious provenance. Further complicating this picture is the increasingly globalized nature of service support for ICT systems. Our adversaries seek to inject themselves into every conceivable stage of technology development, for both disruptive and intelligence objectives.

Congressional Actions

Since 2013, Congress has passed several National Defense Authorization Acts and laws that contain more than 100 references to supply chain security. Many of these still remain to be implemented by their target agencies. More recently, in 2018, the executive branch and Congress worked to pass new legislation to improve executive branch coordination, supply chain information sharing, and actions to address supply chain risks. The Federal Acquisition Supply Chain Security Act of 2018 (Title II of Pub. L. 115-390), signed into law on December 21, 2018, established the Federal Acquisition Security Council (FASC). The FASC is an executive branch interagency council, chaired by a senior-level official from the Office of Management and Budget (OMB), and includes representatives from the General Services Administration, Department of Homeland Security, Office of the Director of National Intelligence, Department of Justice, Department of Defense, and Department of Commerce. This new interagency council, with its multiagency leadership and broad mandate for both cyber and SCS policy, could become the much-needed coordinating mechanism for federal agencies seeking to answer questions about vendor and product trustworthiness.

Supply Chain Security System of Trust (SoT) Framework

MITRE 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. We have also been deeply engaged in projects specifically focusing on supply chain security for ICT systems, including highly sensitive nuclear and intelligence systems, and the "trustworthiness" of vendors and products. With today's increased focus on the need for trustworthy supply chains, trustworthy partners, and trusted systems globally, a reliable path to an actionable understanding of the risks that can impact trustworthiness is essential – and this path must be understood, shared, and usable at scale.

As a result, we have developed the Supply Chain Security System of Trust (SoT) 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 broad knowledge of the relevant standards organizations.

How it Works

The SoT framework is organized into categories that include suppliers, supplies, and services. It addresses 12 top-level decisional risk areas associated with trust that agencies and enterprises must evaluate and make choices about during the full life cycle of their acquisition activities. Leveraging the full breadth and depth of our expertise, industry efforts, and government research, the SoT framework drills down into these 12 top-level risk areas, investigating as many as 76 risk sub-areas by addressing over 400 detailed questions. For example, as highlighted in Figure 1: Does a supplier make use of a standard service bill of materials—a list of all the serviceable parts needed to maintain an asset while it's in operation? Is the supplier using high assurance and integrity capabilities to track where software "supplies/components" came from, who crafted them, and whether it is verified that they have been through the expected assurance and validation steps necessary to address the risk of malicious taint?

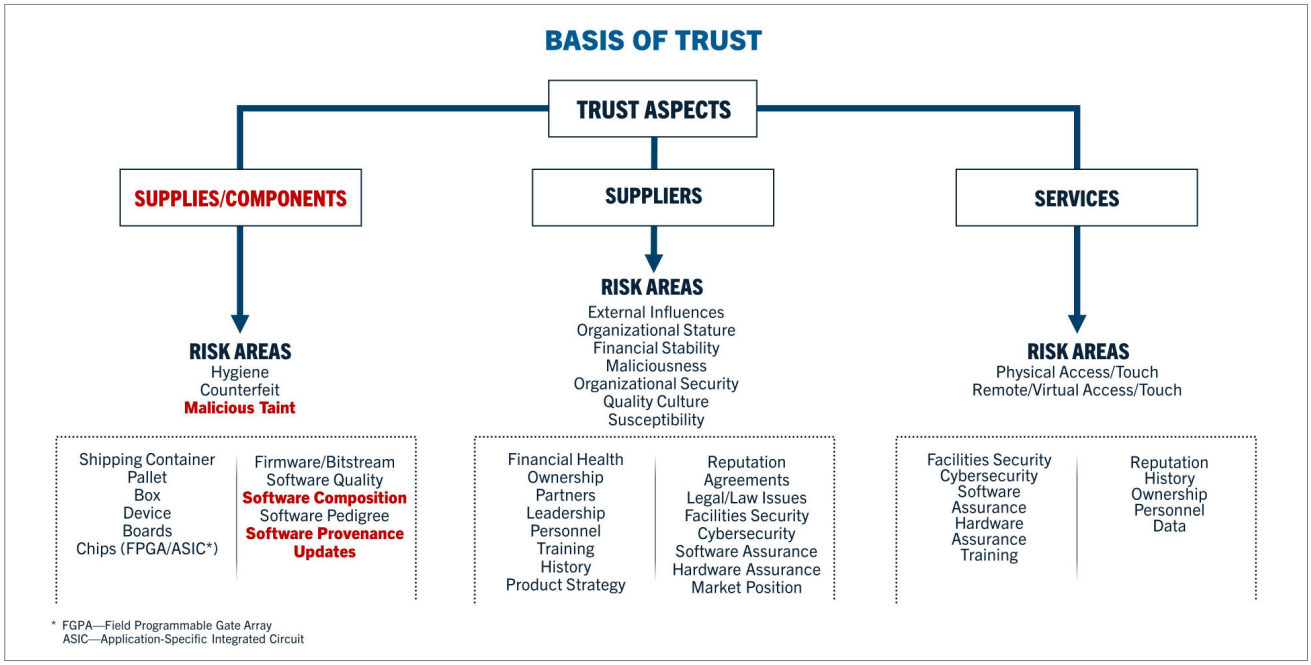

Figure 1. System of Trust, showing key risk areas for suppliers, supplies/components, and services

In addition, the framework draws upon numerous validated data repositories to advance a probabilistic risk assessment of the trustworthiness of a product, service, or supplier. This SoT analytical system is positioned to enable an acquirer to make a clear, well-informed decision about whether to purchase from a particular entity, and whether to purchase a specific item/part number from that entity. Figure 1 shows a high-level depiction of the SoT framework.

How to Apply It

The SoT assessment starts with asking a few scoping questions to narrow down the SoT content to something appropriate to the product, service, or supplier in question. This subset will be aligned to the assessing organization's assessment focus, resources, available time, and legal authorities, and to its present acquisition challenge. During the evaluation process, subject-specific questions are posed to establish the presence or absence of individual aspects of concern and to align with best practices from government and industry. Risks are scored using a set of contextually driven, tailorable, weighted measurements that are used as inputs into a scoring algorithm. The scoring results are then used to identify supplier strengths and weaknesses against the applicable risk categories, enabling an acquirer to analyze and evaluate one or more suppliers' relative "trustworthiness" for supplying components or services.

Early Pilots Show Promising Results

In late 2020, we conducted an initial set of pilots that assessed: (1) a set of companies for general concerns, (2) a specific company as a supplier of critical infrastructure systems, (3) a product for use by a specific community within the federal government, and (4) an industrial base assessment for an organization dependent upon a specific technology and the industry capable of supplying it.

The preliminary results for Pilot 1 are illustrated below in Figure 2, an unweighted bar chart depicting the overall risk scores for the 11 companies reviewed in the pilot, and in Figure 3, which presents radar plots of five data-driven scores from the supplier risk categories (leveraging 52 questions in those areas) for three of the 11 companies of interest. Figure 4 offers a deeper look

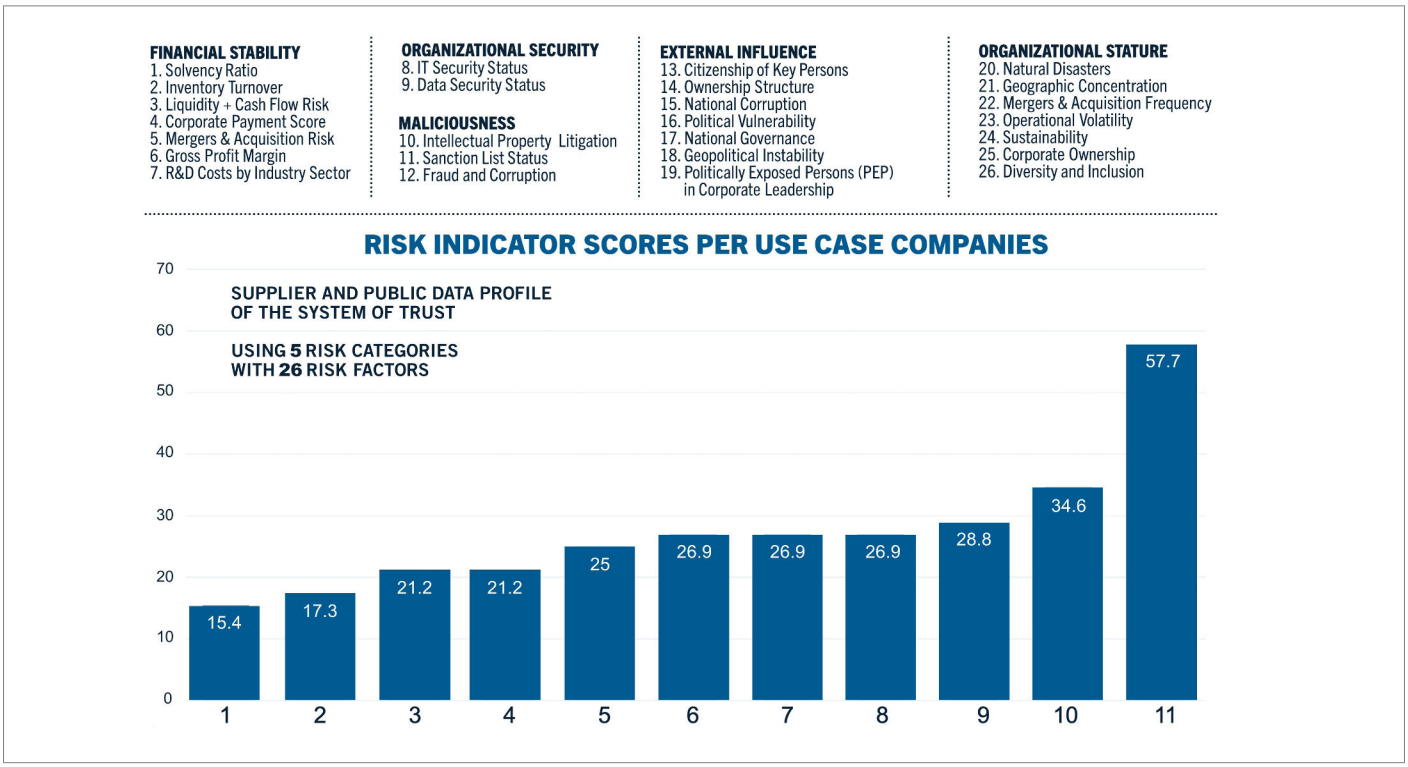

Figure 2. Risk scorecard based on the preliminary System of Trust scoring methodology for 5 top-level categories and 52 risk measure questions for 26 risk factors

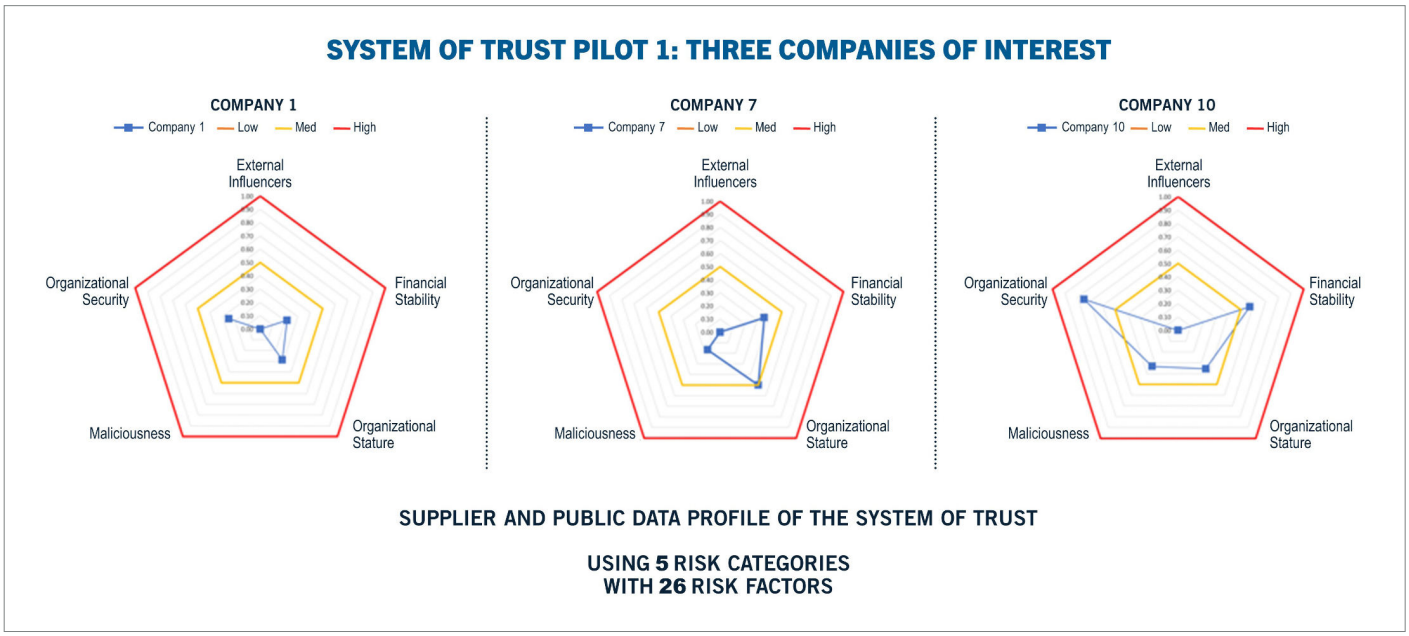

Figure 3. Radar plots of 5 data-driven scores for 3 of the 11 companies reviewed in Pilot 1

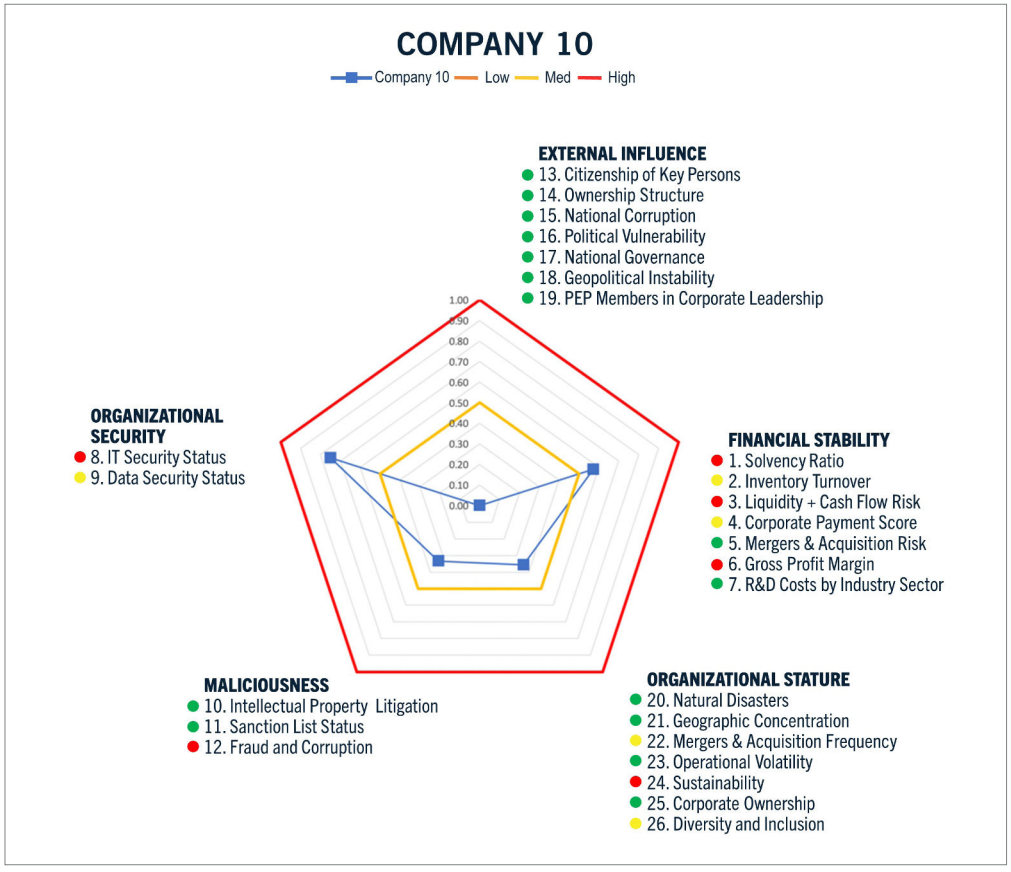

Figure 4. Specific risk scores for one company involved in Pilot 1, in the form of a radar plot

into the risk scores that generated the radar plot for one of the companies involved in the pilot (Company 10).

These examples all use data sources the SoT leveraged to generate the analytical assessments, which clearly show a larger risk profile for Company 10 compared to the others. This pilot provided a proof of concept that offers early evidence of this tool's utility, with deeper and broader analysis to follow as the SoT is completed. The other three pilots had similar insights.

In the next phase of the SoT effort, we will use the full array of data sources envisioned and tailor weighting and score contributions to fine-tune the emphasis on specific sub-risk areas used in any given assessment. Although the pilots only used a subset of the public, private, and restricted access data sources the SoT is anticipated to leverage, we are cataloging and capturing the numerous sources of potential utility in conducting such analyses.

Next Steps and Recommended Actions

Continued tuning of the Supply Chain Security SoT Framework through additional pilots and real-world application is expected to result in enhancements that will position the SoT framework to become the generally accepted framework for supply chain security – similar to the generally accepted accounting principles (GAAP) used in all U.S. businesses, or the globally equivalent international financial reporting standards (IFRS).

There are a number of actions that agencies, the newly organized FASC, Congress, and industry can take now:

- Agencies should explore the application of this framework to their supply chain risks. This participation would also enhance the framework. In addition, data sharing of the results of these assessments between federal agencies should be explored to strengthen the management of government-wide risks to our nation's supply chain.
- The FASC, working under the direction of OMB, should actively examine the use of a comprehensive framework like the Supply Chain Security SoT Framework to improve agencies' supply chain risk management, and move towards adopting a consistent, repeatable, data-driven analytical approach for addressing supply chain concerns.
- Congress, both in its oversight role and in the context of future legislation associated with execution of the Federal Acquisition Supply Chain Security Act of 2018, should consider the potential benefits of having the FASC utilize a comprehensive approach like the Supply Chain Security SoT Framework.
- Industry should support and contribute to the continued legislative and executive branch efforts to better understand and secure our nation's supply chains. Such actions will encourage companies to be conscious of their trust rating if they want to do business with the federal government and to take steps to ensure they're securing their supply chain systems.

About the Author

Robert A. Martin, as senior staff in the MITRE Labs Cyber Solutions Innovation Center, leads Supply Chain Security efforts within MITRE and with industry and is the elected chair of the Industrial Internet Consortium Steering Committee. Mr. Martin created the community standard for software security weaknesses used throughout the world as well as over 40 global standards addressing the interplay of enterprise risk management, cybersecurity, and critical infrastructure protection.

For more information about this paper or the Center for Data-Driven Policy, contact policy@mitre.org