BlueVoyant

Booz | Allen | Hamilton®

SUPPLY CHAIN CYBER RISK MANAGEMENT

AN END-TO-END SOLUTION FROM BOOZ ALLEN HAMILTON AND BLUEVOYANT

CONSULTING | ANALYTICS | DIGITAL SOLUTIONS | ENGINEERING | CYBER

SUPPLY CHAIN CYBER RISK MANAGEMENT CONTENTS

EXECUTIVE SUMMARY

Supply chain risk has become one of the most vital national security challenges for the federal government today. In the age of digital transformation and globalization, suppliers and contractors who form the government's supply chain are increasingly becoming globally distributed, complex, and difficult to manage. This has led to supply chain vulnerabilities that are actively under attack from various threat actors causing disruption of critical mission operations, loss of sensitive data and intellectual property, and increased harm to the lives of our citizens.

Furthermore, cybersecurity risk is increasingly becoming a larger component of the overall supply chain risk landscape as expanding the digital footprint of supply chain increases the attack surface of the government's critical infrastructures. As our government clients work tirelessly to protect against supply chain cybersecurity attacks and breaches, we have identified the following challenges they must address to effectively manage risk:

- Supply chain visibility is critical to knowing and understanding who and what your suppliers are and their potential threats.
- Due diligence must be performed effectively (and at scale) to cover the broad range and tiers of suppliers and the types of cyber risk they may pose as a supplier.
- Risk assessment should include multi-dimensional and holistic view of supplier risk profile—not just a compliance checklist.
- Monitoring must be done continuously to assess the dynamic and increasingly sophisticated threat actors and environment, rather than at a point in time.
- Remediation is essential in reducing identified and prioritized risks and requires the right set of tools and resources to implement actionable steps.

The Booz Allen team has been designing and delivering supply chain cyber risk management solutions tailored for nearly every major U.S. government organization. Leveraging our proven approach to supply chain cyber risk management, we help our clients solve their key supply chain security challenges, as highlighted in Figure 1. With our best-in-class supply chain domain expertise, managed services, and innovative and emerging technologies, such as artificial intelligence (AI)/machine learning, we deliver a customized and differentiated end-to-end supply chain cybersecurity solution.

KEY CHALLENGES

- Many organizations have **poor supply chain visibility** and do not clearly understand the extent of their supply chains
- As the sheer number of suppliers explodes, organizations face **gaps in due diligence** with lack of expertise in cyber risk management
- **Limited approach to assessment**, often based on basic compliance, does not provide a holistic picture of the organization's broad risk landscape
- Most organizations do not monitor their suppliers continuously, but rather conduct **point-in-time reviews**
- Even when supplier risk is identified, organizations are challenged with **lack of remediation and validation** due to resource constraints

OUR APPROACH

- Clearly **knowing your vendors** helps to identify critical supplier attributes and intelligence data to monitor for potential supply chain threats
- **Prioritizing risks** from supply chain deficiency based on their criticality and impact to your organization's missions is essential
- **Conducting multifaceted, ongoing monitoring** and assessments is vital as supply chain cybersecurity threats are dynamic
- **Driving remediations quickly** with detailed, actionable instructions for implementation and confirmation is critical
- **Taking a programmatic approach** allows supply chain cybersecurity risk to be integrated into enterprise risk management

Figure 1: The Booz Allen team's approach to supply chain cyber risk management

SITUATION

"You can't assume that [supply chains] defend themselves. That's the principal failure that we're observing in SolarWinds." – Chris Inglis

SUPPLY CHAIN VULNERABILITIES LAID BARE…

Securing the federal government's supply chain from cyber-attacks has become a vital national security challenge. The services, technology, and industrial base that forms the backbone of the government's capabilities to deliver services, procure essential goods, and maintain continuity of operations is strategically crucial and bewilderingly complex. For example, in the defense industrial base (DIB) alone, experts estimate that the number of companies that directly contract with the Department of Defense (DoD) range up to at least 300,000, and there are many more subcontractors.[1] A similarly overwhelming breadth exists for civilian government agencies.

The Booz Allen team recently performed external cybersecurity assessments across a 300-company sample of the DIB—in essence, the DoD supply chain—and found 48% of the suppliers, vendors, partners, and third parties represented had significant and exploitable deficiencies.[2] These findings are consistent with our team's assessments of thousands of private commercial firms across the world. ***The supply chain is vulnerable.***

There are several specific reasons for this vulnerability:

01 Poor Supply Chain Visibility: Most government entities[3] do not understand the extent of their supply chains. This is, essentially, flying blind. Until the government knows who and what its suppliers are, identifying, prioritizing, triaging, and monitoring risk is a near-impossible task.

02 Lack of Due Diligence Scalability: As the sheer number of suppliers explodes, inundation sets in. Organizations often fail to perform adequate due diligence on new suppliers and allow long-term suppliers' due diligence to become stale. Moreover, when due diligence is performed, it often happens through a procurement department that lacks expertise in cybersecurity and cyber risk management.

03 One-Dimensional "Assessments": Rather than incorporating various supplier data and assessments to gain a holistic view of their supply chain, organizations often select only one of the following: vendor questionnaire, external assessment, or internal program assessment. Even more problematic, these rudimentary assessments are basic compliance checklists (and often self-attestation) rather than a rigorous study of the supplier's real exploitability profile from a cyber adversary's perspective.

04 Point-in-Time Reviews: Supplier assessments are mostly conducted at a point in time.[4] Followups, if any, occur at another point in time some months later. In a world where cyber threat actors evolve daily and hourly, episodic and static snapshots don't cut it. Continuous, real-time monitoring is needed.

05 Lack of Remediation and Validation: Monitoring for and detecting cyber threats is only the first step in managing supply chain risks. Risks must then be mitigated to ensure organizations are protected from potential supply chain breach or attack. In particular, vulnerabilities need to be discovered and fixed before adversaries can discover and exploit them. However, many organizations[5] lack the resources to quickly detect and validate the issues with suppliers—let alone work with the supplier to remediate and confirm that the issue has been fixed.

---

[1] Cybersecurity Maturity Model Certification (CMMC), Carnegie Mellon University and The Johns Hopkins University Applied Physics Laboratory LLC, 18 March 2020, v1.02. https://www.acq.osd.mil/cmmc/docs/CMMC_ModelMain_V1.02_20200318.pdf

[2] "BlueVoyant Review: Defense Industry Supply Chain & Security," BlueVoyant, 2021. https://www.bluevoyant.com/resources/cyber-attacks-against-smb-defense-contractors-report-bluevoyant/

[3] The visibility challenge is not limited to the government. According to our [recent year] survey of 1,500 chief information security officers, chief information officers, and chief procurement officers around the globe, 77% of respondents reported to having limited visibility into their third-party vendors.

[4] In our survey of 1,500 organizations, 0% monitor suppliers in real time or daily.

[5] According to our survey, 40% of organizations simply inform the suppliers of any issues and hope they fix them.

...AND RUTHLESSLY EXPLOITED BY CYBER ADVERSARIES

Cyber threat actors have discovered the usefulness of the supply chain (and the federal supply chain in particular) to gain access to even the most well-defended targets. Attackers have honed capabilities to detect security deficiencies through scanning and metadata analysis are adept at quickly capitalizing upon those deficiencies to gain access, and are increasingly capable of operating at a greater scale. When the intended target is too hard to penetrate directly, adversaries quickly move to vendors, suppliers, and partners.

SolarWinds, Microsoft Exchange, and Kaseya are the biggest (but certainly not the only) validators that this adversarial strategy works and that attackers are outpacing defenders. We expect adversaries to double down on supply chain exploitation, especially as pandemic-driven remote work and vast federal information technology (IT) and digital modernization greatly expand every department and agency's third-party digital ecosystem. The supply chain is a network of networks, and cyber threat actors are navigating it better than we are.

THE NEED

The good news is that the government and industry have begun to recognize the magnitude of the problem and the importance of solving it. The White House and Congress, through the May 2021 Cybersecurity Executive Order and copious legislation, have codified supply chain security as a priority. Industry players who serve the government are also recognizing that they own many of the weak spots and need to act. As a result, new cottage industries of cyber supply chain vendors and service providers have emerged—many positioning themselves as a panacea.

Unfortunately, there is no magic bullet widely available on the market today. The scale, complexity, and malleability of supply chains, and the constantly morphing ways adversaries exploit their vulnerabilities, mean that none of the tools traditionally available (e.g., security ratings services; governance, risk, and compliance methods; and traditional threat intelligence) will deliver comprehensive security and durable resilience at scale. Classic approaches to cyber risk management, which tend to focus on a well-bounded enterprise IT footprint and emphasize compliance with longstanding control regimes, often fail to "see" the entire supply chain and third-party ecosystem, and as such, just perpetuate the previously defined problem with lack of visibility.

WHAT GOOD LOOKS LIKE

We need a transformatively different approach. The answer is not to do the same things better; it's to tackle cyber supply chain security in a fundamentally different way. In the same way that a 24/7 Security Operations Center provides the cyber defense for a single company, the government needs a similar, continuous detection and response capability for the supply chain. There are several additional attributes of the supply chain solution the government needs to adopt:

Knowing Your Vendors: The starting point for defending the supply chain is maintaining full awareness of the suppliers—including third, fourth, and fifth parties—who participate in the design, development, implementation, maintenance, and disposal of all products and services. This awareness is the pre-requisite to protecting and defending the supply chain; what's invisible isn't securable. The key here is data: gleaning robust, diverse information about individual suppliers and the supplier ecosystem overall, and rapidly turning that data into actionable intelligence that drives risk mitigation actions.

Prioritizing Risks: Every organization has a unique risk profile, which means every risk from a supply chain deficiency isn't created equal. Departments and agencies need to clearly understand and define their mission-critical functions and processes, highest-value assets, and the threat scenarios that would cause the greatest damage. This should result in a clear stratification of suppliers based on criticality. It is also crucial that government organizations clearly identify supplier attributes that are most critical to monitor.

Conducting Multifaceted, Ongoing Monitoring and Assessments: Supply chain cybersecurity threats are dynamic. Continuous monitoring is vital because point-in-time snapshots become obsolete within days or even hours. Similarly, assessments of suppliers need to evolve beyond self-attestations and compliance checklists to include independent, external cybersecurity program reviews conducted by independent parties and the review of critical tools like software composition analysis. The rigor and depth of monitoring and assessment should be commensurate with the criticality of the supplier.

Driving Remediations Quickly: This is critical—risk identification and prioritization is meaningless without a "machine" to rapidly execute remediations. Most cyber supply chain security efforts stop at reporting on risks and often rely on simply making suppliers aware there is a problem. What's needed is detailed, actionable instructions for implementing remediations and a process and mechanism for confirming that remediation occurs in a timely fashion.

Taking a Programmatic Approach: Fundamentally, this is about codifying cyber supply chain security as a durable function within a department or agency's cybersecurity and/or risk management program. It is about recognizing that durable supply chain security and resilience requires much more than purchasing new tools or intelligence subscriptions. It demands well-trained people, clear processes, and cutting-edge technology and automation—all tightly integrated into a programmatic approach.

THE SOLUTION

We have coupled the federal services and supply chain expertise of Booz Allen with the agility and world-leading data and technology of BlueVoyant to deliver a customized, end-to-end cyber supply chain security solution for the federal government that pairs decades of professional services experience with bleeding-edge technology products and managed services.

OUR SOLUTION FOUNDATIONS

Our team's solution rests on ***three foundational tenets:***

01 First, that we can ***detect, prioritize, and remediate supply chain deficiencies as fast as anyone else***—and before adversaries can exploit them. Our fundamental view is that this is a race—currently being won by cyber threat actors, but winnable by defenders if they bring the right combination and integration of data, tools, and mitigations to bear. ***This is about reducing immediate-term supply chain risk.***

02 Second, that triaging supplier deficiencies isn't sustainable, and thus, it is critical ***to address underlying systemic weaknesses across the supplier ecosystem.*** This includes examining supplier networks for signs that vulnerabilities have been exploited prior to the repair (also called threat hunting). Also, we seek to elevate the vigilance and efficacy of the security program at suppliers showing poor performance. We find suppliers generally fall into one of two categories: They have good security programs and have a few blind spots or errors, or they have never properly invested the energy and resources to have a vigilant, effective cybersecurity program.

We have teams ready to deploy professional services for security operations program uplift, quickly modernizing cybersecurity programs to ensure emerging issues are properly dealt with. ***This is about creating durable long-term security improvements across the supplier ecosystem.***

03 Third, that we can bring an ***unmatched understanding of government missions and the digital backbone that supports them.*** Our team's decades-long work across nearly every U.S. government department and agency means that we know what matters most and what is most critical to protect. Our solution, therefore, is not a generic installation of more novel technology. It is fit-for-purpose cyber supply chain program design, development, and operations that meet the unique needs and priorities of each customer. ***This is about building lasting supply chain security capabilities into every government department and agency.***

OUR APPROACH AND CAPABILITIES

Our comprehensive solution approach and capabilities is illustrated in *Figure 2*.

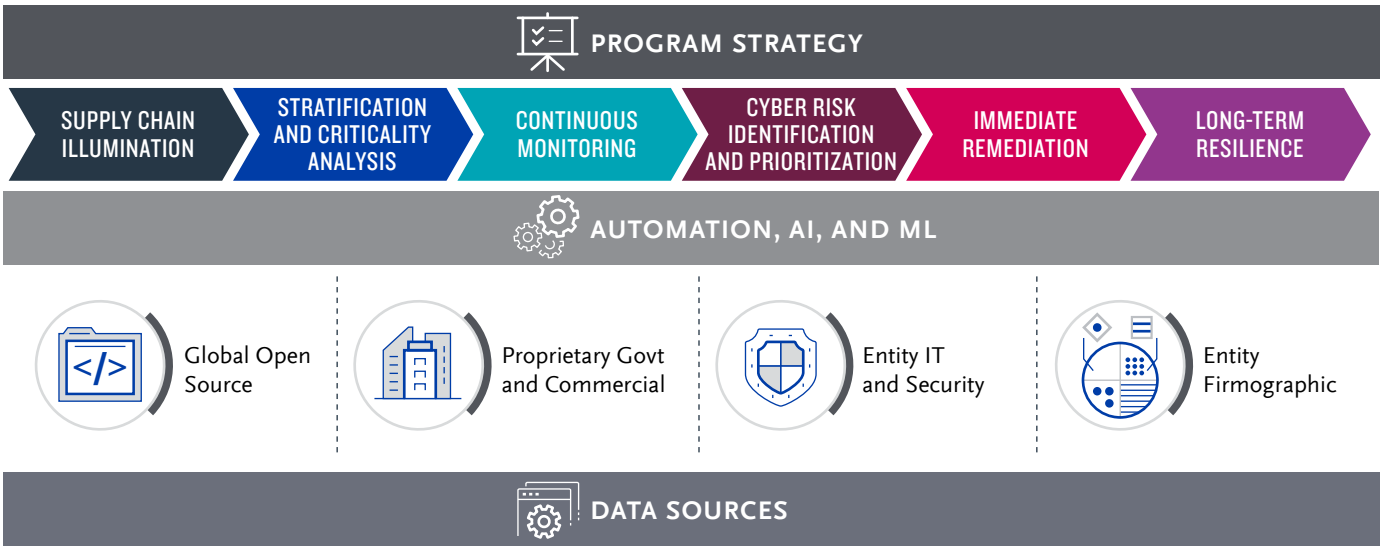

Figure 2: The Booz Allen team's comprehensive solution

Program Strategy and Design

Our team provides program diagnostic assessments to evaluate the maturity and effectiveness of the client's supply chain cyber risk management program. We utilize a program dashboard tool to provide customized data analytics and visualization of the organization's score with benchmarks against peers in the industry sector. We view this as a critical service enabling clients to quickly assess and understand their program maturity and whether their supply chain is highly secured or likely vulnerable to cyber attacks.

We also collaborate with clients to develop enterprise-wide strategies to design, develop, and execute a cyber supply chain security risk management program consistent with the organization's defined risk appetite and tolerance.

Supply Chain Illumination

Our team helps clients identify and map their supply chain by collecting and analyzing suppliers, products, and services data. Where clients lack visibility or awareness, we utilize cutting-edge technology to illuminate supply chains and identify sub-tier (down to fifth or sixth party) suppliers.

Critical to illumination is the quantity and quality of accessible data. Our team has some of the best data outside the U.S. intelligence community for this problem set with more than 40 data sources. We have exclusive commercial rights to numerous data feeds; we process 17 million data points per second; and we have processed firmographic information (e.g., company data such as size, employees, websites, subsidiaries, and M&A history) on more than 17 million suppliers—800,000 of which we actively monitor daily for cybersecurity risks.

Crucially, our data comes from sources external to the suppliers under assessment. We can illuminate supply chains and identify suppliers from the outside-in, using open-source data and commercial data sets with no government data or handholding by clients (or permission from suppliers) to get started. This approach guarantees that we see suppliers as adversaries see them, not as they see themselves.

Supplier Stratification and Criticality Analysis

A key component of risk management is mission understanding. Our team performs a criticality analysis of our client's missions and business functions, and identifies the digital assets that most directly enable the performance of those missions and functions. We use that information to subsequently stratify and categorize suppliers—identifying and prioritizing those that have the greatest impact on the organization's mission-critical functions and assets, as well as identifying suppliers that may appear to be unremarkable, but if compromised, would provide strategic access to a government target. By stratifying vendors in this way, we're able to provide prioritized alerting and rapid remediation to the areas of highest risk.

Continuous Monitoring of Suppliers

The starting point for supplier monitoring is the footprint: an inventory of the supplier's internet-facing infrastructure. The footprint (also called the attack surface) includes the domains and Internet Protocol addresses belonging to each supplier. Creating accurate supplier footprints is extremely challenging; our team has invested heavily to build automated, intelligent footprinting technologies, with roadmaps to improve accuracy over time. This is significantly different than many other firms, which use primarily manual analysis to generate a (hard-to-update) supplier footprint. These manual approaches will not scale to the size and scope of the government's supply chains, nor to the dynamic nature of footprint changes.

In addition, we built and employ custom analytics to continuously monitor for risk indicators. These analytics generate actionable alerts and findings based on client-defined priorities for dissemination and followup.

Cyber Risk Identification and Prioritization

Our team's cybersecurity experts defined an advanced taxonomy of more than 200 risk measures organized into 45 factors and four overall categories. This comprehensive risk taxonomy is the basis for identifying, organizing, and prioritizing specific deficiencies within the monitored supplier environments. The main risk categories are:

- Under ***IT Hygiene,*** we assess indicators that the firm is being vigilant in cybersecurity to include email protections, use of outdated software versions, configuration control, non-business application usage, and technology vendors.
- Under ***Vulnerabilities,*** we consider known vulnerabilities such as those with Common Vulnerabilities and Exposures (CVEs), emerging software vulnerabilities, and encryption weaknesses to include security certificate vulnerabilities.
- For ***Threats,*** we consider indicators of probing from known malicious sources, phishing email traffic, brute force attack attempts, and domain lookalikes.
- Finally, ***Malicious Activity*** encompasses indicators of outbound traffic going to known malicious infrastructure, traffic to known phishing sites, company assets on blacklists, and credentials for sale.

Not all risks are equal in severity. While the taxonomy allows us to identify and organize a supplier's deficiencies logically and clearly, our team overlays that view with the criticality analysis conducted previously. This ensures our remediation insights and activities (see next step) are focused on the most important risks given an individual client's unique mission, business, and critical asset profile.

Immediate Remediation

We are the leader in the industry that combines supply chain risk analysis with mitigation services. Through our Risk Operations Center—a virtual entity available to all our clients—we provide clients and suppliers with detailed, actionable information (through findings and alerts) on deficiencies to help them remediate quickly. Our reports explain why the finding matters and what it tells us in relation to overall cybersecurity risk for the supplier. Our approach is to provide systems administration tasks that in many cases can be implemented quickly. Our analytics follow up on the repair to ensure the vulnerable condition has been fixed prior to closing out the issue. With our client's approval, we engage directly with suppliers to provide these actionable findings and accomplish remediations within their systems. Our team maintains a mean-time-to-remediate of less than 1.5 hours per deficiency finding. This is unparalleled in the industry.

Long-Term Resilience

The real-time remediations accomplished via our Risk Operations Center reporting and follow-ups are necessary, but not sufficient. Our team provides additional services typically delivered in a more robust, hands-on way with suppliers to drive durable improvements to the supplier's cybersecurity program and operations. This often begins with threat hunting (which can be conducted remotely and delivered as a service) to ensure we "won the race" and that any identified vulnerability was not exploited prior to the repair. Beyond this, we deliver deep consulting and technical services to raise the level of cybersecurity performance. This work is often focused on security architecture and engineering: for example, implementing zero trust principles and best practices, upgrading core protective security controls or cyber defense operations, and helping suppliers more proactively prepare for and prevent cyber attacks on their networks and systems.

OUR TEAM PROVIDES ADDITIONAL SERVICES TYPICALLY DELIVERED IN A MORE ROBUST, HANDS-ON WAY WITH SUPPLIERS TO DRIVE DURABLE IMPROVEMENTS TO THE SUPPLIER'S CYBERSECURITY PROGRAM AND OPERATIONS.

About Booz Allen

For more than 100 years, business, government, and military leaders have turned to Booz Allen Hamilton to solve their most complex problems. As a consulting firm with experts in analytics, digital, engineering, and cyber, we help organizations transform. To learn more, visit BoozAllen.com.

About BlueVoyant

At BlueVoyant, we recognize that effective cyber security requires active prevention and defense across both your organization and supply chain. Our proprietary data, analytics and technology, coupled with deep expertise, works as a force multiplier to secure your full ecosystem. Learn more at BlueVoyant.com