BlueVoyant®

BLUEVOYANT REVIEW

Defense Industry Supply Chain & Security

2021

Table of Contents

Executive Summary

Businesses in the defense industrial base (DIB) are high-value targets for nation-state adversaries and other cybercriminals. As prime contractors and other large companies have developed more robust security defenses, attackers have pivoted towards targeting small to medium-sized businesses (SMBs) that are subcontractors within the same supply chain. This attack strategy is based on the expectation that SMBs will have fewer and less sophisticated defenses[1] and will thus provide an easier entry point to all entities within the entire supply chain. The news is replete with examples of how these third-party attack strategies have been devastatingly effective, including the recent SolarWinds attack.

A number of government regulations have set standards designed to raise the baseline of cybersecurity requirements. Regulations can help reduce the attack surface, but compliance with regulations are typically measured at points in time and are thus not necessarily synonymous with ongoing effective cybersecurity.

BlueVoyant set out to independently test the security of SMBs within the DIB using our third-party datasets and proprietary analytics and techniques that provide insights into the security of companies using only externally available data. **The rest of this report provides a detailed description of our findings and makes recommendations based on those findings.**

A FEW NOTEWORTHY AND SURPRISING RESULTS INCLUDE:

- **Manufacturing and R&D companies had the highest risk profiles** and industry type was more predictive of risk than company size alone, although industry modified by size yielded the strongest findings.
- **Over half of the 300 SMB defense contractors** examined in this report had critical vulnerabilities to ransomware[2].
- Almost **one-tenth of the companies** analyzed had critical vulnerabilities, evidence of intentional and **targeted threat activity**, and evidence of compromise.
- **28% of the companies** analyzed showed evidence indicating they **would fail** to meet the most basic, tier-1 CMMC requirements

SUMMARILY STATED:

Defense supply chains are only as strong as their weakest link,

Evidence suggests that cybercriminals are increasingly adept at locating and exploiting the weakest link within a supply chain/set of trusted third parties, and

Results of this study provide ample evidence that exploitable cyber weaknesses within the defense supply chain are abundant.

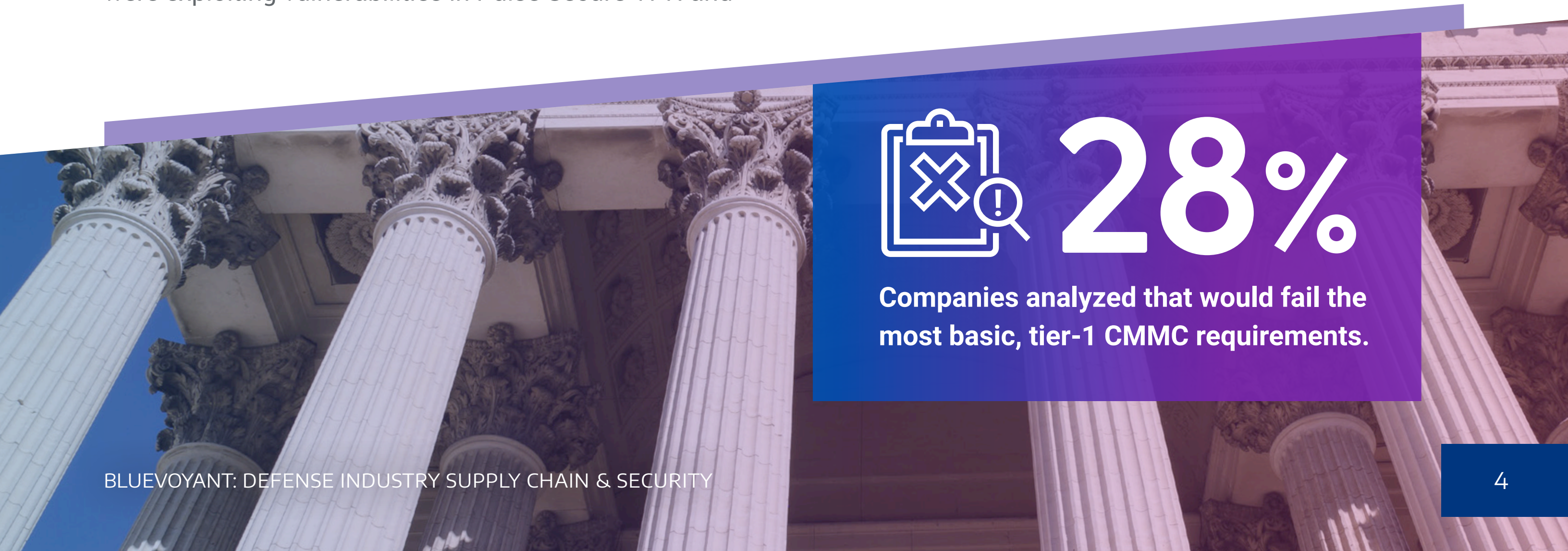
The Defense Industry's Cybersecurity Problem

In the United States, securing the defense industrial base is one of the critical national security objectives of our time. Spanning thousands of companies, forming a many-layered multinational chain, and comprising everything from machine shops of a few dozen employees to billion-dollar prime contractors, the industrial base that forms the backbone of the U.S. defense industry is strategically integral and bewilderingly complex. It is also under attack. Defense companies face the same opportunistic cyber threats of any business. BlueVoyant has reported extensively on the rising threat of ransomware and in just the last year, U.S. defense contractors have been hit by the Babuk[3], Ryuk[4], Maze[5,6], and DoppelPaymer ransomware groups[7], not to mention dozens of instances where the details were not fully reported[8]. Two contractors were shut down by ransomware and at least two other defense contractors were attacked using recently-disclosed zero-day vulnerabilities in 2021 (F5 and Microsoft Exchange)[9].

Most worrisome, however, is pressure on the defense industry from persistent, sophisticated foreign actors for the purposes of espionage and theft of vital intellectual property. **In 2011, after 24,000 terabytes of data had been exfiltrated from a large Department of Defense (DoD) contractor, then-Deputy Defense Secretary William Lynn stated, "It is a significant concern that over the past decade, terabytes of data have been extracted by foreign intruders from corporate networks of defense companies."**[10] Fast forward to October 2020, the NSA issued an advisory noting that Chinese APT groups were exploiting vulnerabilities in Pulse Secure VPN and F5 Networks' cybersecurity software to target defense contractors.[11] In April 2021, Chinese APT groups were reportedly exploiting another software vulnerability to attack defense contractors: vulnerabilities in Microsoft Exchange servers.[12]

As the larger companies have improved their cyber defenses, attack strategies have shifted away from direct attacks on the crown jewels of prime contractors toward initial attacks on trusted vendors and subcontractors to enable stealthier access to primes and other companies within the supply chain. Attackers commonly leverage weaknesses in SMBs to insert malicious software into less-defended points that then proliferate, or they socially engineer employees downstream, search for reusable credentials or otherwise victimize less prepared supply chain members just to get a foothold in the network.

Often referred to as third party attacks, one of the largest breaches in defense history, which affected every branch of the U.S. military and Pentagon, as well as the State Department, Treasury, and dozens of other government agencies and corporations, succeeded because a Russian APT group compromised SolarWinds, a software company. SolarWinds sells the Orion network monitoring platform, software used by hundreds of corporations and government bodies. **When the Russian cyber threat group APT28 or 'Cozy Bear' were able to exploit a vulnerability in SolarWinds and then laterally access the popular Orion platform, they were able to gain access to Orion customers including over 18,000 organizations.**



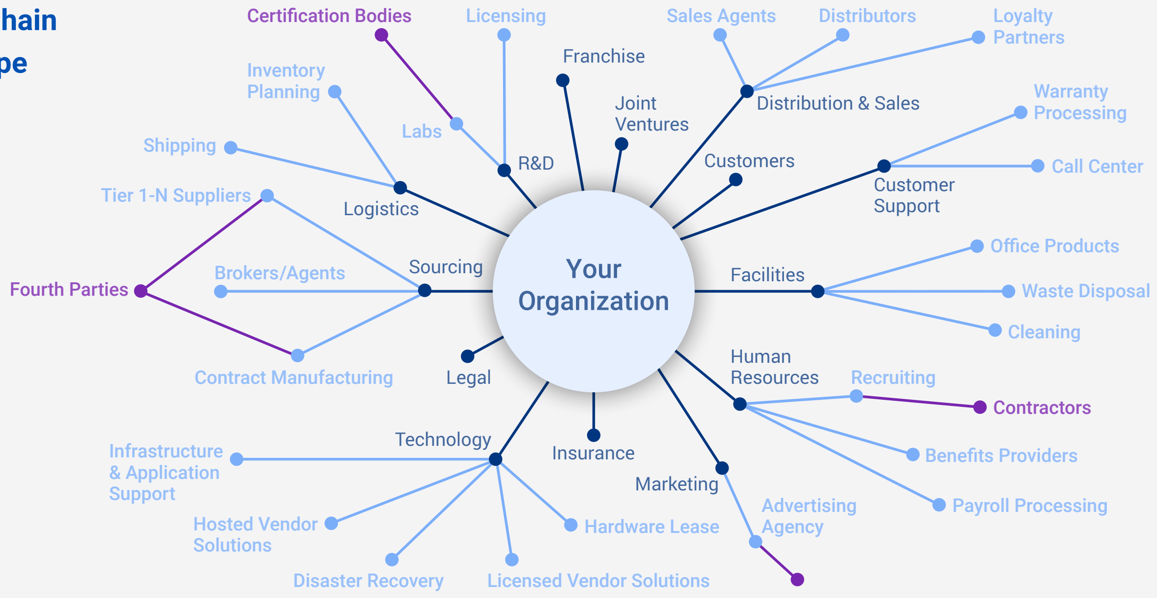
28%

Companies analyzed that would fail the most basic, tier-1 CMMC requirements.

Defense Supply Chain Structure as an Attack Enabler

The DIB is an enormous and complex ecosystem. **Estimates of the number of companies that directly contract with the DoD range from 100,000[13] to 300,000[14],** with even less clarity on the number of subcontractors, since primes commonly have multiple layers of subcontractors and those subcontractors often have their own complex network of subcontractors. The production of a submarine, for example, involves development of multiple components across multiple industrial sectors. There may be separate subcontractor networks around communications, each physical component, various weapons systems, accommodations design, etc. Each component has sub-components and it's not unusual for each new subcomponent to involve the introduction of another vendor.

Supply Chain Landscape



What makes the DIB even more complex is that the supply chain for any given contract is not linear. Defense supply chains overlap: a prime contractor on one contract may be a sub on another contract, and different prime contractors may use the same subsidiaries along with a range of their own independent contractors. Over many contracts, these networks proliferate and grow more interconnected.

A primary driver of cyber risk in the defense industry is a combination of the complexity of the networks as described above, along with general changes in production processes over the last few decades. Adoption of lean manufacturing processes and just in time delivery practices have helped ensure that the quality of a single component is consistent, material waste is minimized, and employee efficiency is maximized. For this approach to work effectively, communications between and among supply chain members have been streamlined and improved with a focus on ease of data transfer. This emphasis on ever improving efficiencies in communications has eclipsed concerns over network and transmission security, leaving gaping holes at every connecting point across any given supply chain.

Supply chains are only as strong as their weakest link. In interconnected networks, vulnerabilities appear at any point where information or connections are shared. As with all industries involving intellectual property (IP), the DIB faces increasing cybersecurity challenges due to the adopted production process and interorganizational communications and production dependencies.

Current Defense Cybersecurity Efforts

Policymakers are painfully aware of the high stakes with cyberattacks. Cybersecurity regulations and compliance standards have been developed and improved for decades. **In 2019, the DoD announced that they were launching the Cybersecurity Maturity Model Certification (CMMC) regulation as an expansion of, and improvement upon, the National Institute for Standards and Technology (NIST) SP 800-171**[15]. The theoretical model upon which CMMC is based represents an improvement over earlier standards by providing a tiered framework for security, the requirement for evidence of maturity, and third-party verification of standards. Essentially, CMMC is designed to help apportion compliance and responsibility in appropriate measures throughout a complex ecosystem and to also ensure third party verification that controls are, in fact, in place.

Despite the discipline reflected in the CMMC regulations, many challenges remain for smaller firms, which are increasingly targeted for cyberattack. These smaller firms are suddenly facing a requirement that demands significant investment in new controls without necessarily having either the budget or the in-house expertise to implement the controls.

Prime contractors, on the other hand, are under enormous pressure to reduce the attack surface of the entire supply chain without having complete visibility into the vulnerabilities that exist. While the primes are large and sophisticated enough to maintain their own cybersecurity, the challenge of designating which of their subcontractors falls into which tier and ensuring compliance for each represents a substantial cost - financial and logistical - and may even seem impossible without visibility or insight into subcontractor network security. Additionally, since compliance requirements are contract specific, a subcontractor that needs to comply at Level 1 for one contract may need to comply at Level 3 for another contract with the same prime. Accordingly, primes are predisposed to "level up" on their expectations of subs, resulting in added pressure and cost to the SMBs.

In parallel, the Cyberspace Solarium Report calls for substantial changes to the structure and organization of the national cyber ecosystem, especially with respect to partnering between government and the private sector to protect supply chains.

Most recently, of course, are the two Executive Orders: one on American Supply Chains, which orders the DoD to identify areas of critical risk and dependency in its defense supply chains, and one on Improving the Nation's Cybersecurity, which orders a review of cybersecurity practices in federal agencies and also states,

> "Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector."

More legislation is coming: the currently proposed Infrastructure Plan may include significant funding aimed at military technology, and the 2022 Defense Authorization Act is just around the corner.

This suite of emerging legislation across multiple spheres directs much-needed attention and funding to cybersecurity in the defense supply chain. The price of cybersecurity regulation is a burden not only for SMBs who often lack the necessary resources or organizational management, but also for prime contractors who bear responsibility for enforcing compliance.

Compliance is a key first step toward baseline security for all, but more is needed. How can we create a secure environment for the defense industrial base, while also supporting the development of a large and diverse ecosystem for business? How do we close the gap between periodic measures of compliance with regulations and ongoing, perpetual monitoring and management of systems security throughout an entire supply chain?

Research Goals

Given that compliance efforts are a necessary but insufficient approach to cybersecurity, BlueVoyant set out to analyze real time and ongoing evidence of the security practices of a wide cross section of subcontractor firms within the DIB. BlueVoyant employed proprietary tools and analytical methods to identify evidence of cybersecurity gaps in the subcontractors' security practices using only externally available data and resources (i.e., no access to internal data or systems was required).

THE GOAL OF THIS RESEARCH WAS TO:

Garner a better understanding of the security posture of less visible members of the very complex defense supply chain;

To the extent possible, identify specific vulnerabilities of the SMBs studied;

Identify addressable concerns for those DIB members with the least organizational cybersecurity capability;

Gain a better understanding of those DIB members most likely to leave the defense supply chain.

BlueVoyant partnered with Professor Steven Melnyk and his team at Michigan State University, the number-one ranked supply chain management teaching and research program in academia[16] to consider alternative and meaningful ways to review and analyze the collected data. Together, the team agreed that **it would be interesting to look at the data through the lens of industry segment. Specifically, companies were categorized as manufacturing, research and development (R&D), or services.**

MICHIGAN STATE UNIVERSITY

THE NUMBER-ONE RANKED SUPPLY CHAIN MANAGEMENT TEACHING AND RESEARCH PROGRAM IN ACADEMIA

Research Methodology

Dataset - Broad-based analysis of DIB businesses

First, BlueVoyant identified and assessed a sample set of 300 SMBs in the DIB. For the purposes of this analysis, SMB refers to any business below revenues of $1B annually. For analytic purposes, the dataset was divided into four different size ranges - determined by employee count, not revenue, due to the preponderance of private companies and the challenge of verifying revenue figures.

Size (# of employees)	Number of Companies
Group 1: 1-50	113
Group 2: 51-200	105
Group 3: 200-500	37
Group 4: 500+	45

Table breakdown - size

The companies were also separated into four different industry segments, as follows.

Size (# of employees)	Number of Companies
Group 1: R&D	76
Group 2: Manufacturing	130
Group 3: Services	77
Group 4: Other	17

Table breakdown - industry

BLUEVOYANT IDENTIFIED AND ASSESSED A SAMPLE SET OF

300

SMBs IN THE DIB

Vulnerabilities, Threats, and Compromises

BlueVoyant uses a range of proprietary and open-source datasets and analytics in order to determine cyber risk and track threats. We rank businesses as high risk, higher risk, or highest risk based on evidence of one, two, or all three of the following indicators of risk:

- Evidence of security **vulnerabilities**
- Evidence of identifiable **threats** from malicious actors, and
- Evidence of **compromise**

Vulnerabilities that were analyzed in this study include identifiable gaps in network, software, and email security. BlueVoyant focused on the following key indicators:

- **Unsupported software:** was the company running unsupported or unpatched software? This refers to outdated software that is no longer supported with security patches to fix known vulnerabilities. As a result, unsupported software is frequently vulnerable to exploit, and not patching software is a sign of poor cybersecurity management.
- **Unsecured ports:** the biggest threats to companies today, ransomware and data breaches, use attacks that target unsecured ports - especially, unsecured remote administration or RDP ports and unsecured datastore ports.
- **Email security:** is there evidence of DNS-based or other email security software, to mitigate against phishing attacks?

Threats refer to evidence of targeted attack activity - i.e., threat activity above the level of mere broad-based scanning which appears to target vulnerable web pages.

Compromise refers to evidence of malicious outbound traffic - i.e., any communication from a company's systems that appears to be directed towards a command-and-control (C&C) server or malicious online infrastructure. Often, this is a sign of a compromised device or network.

Analysis against the CMMC framework

The primary analysis for this study was conducted using proprietary analytics with findings mapped to the CMMC framework for context. Using the CMMC lens for mapping cyber risk provides a clearer understanding of the sophistication of security controls in place. For example, vulnerabilities identified that map to CMMC level 1 controls indicate that basic cyber hygiene controls are missing.

Specific vulnerabilities, threats, and compromises were also mapped to CMMC domains within each CMMC level. For example, for the Access Control CMMC domain, evidence of access from prohibited types of devices, insecure remote practices and evidence of insecure email practices are applicable to identify if companies are actually providing effective access controls. Similar mappings were applied across all of the CMMC domains and organized by CMMC level.

Study Findings

Our research yielded interesting findings including the following revelations that some industry segments are at higher risk than others:

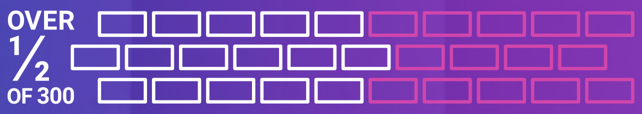
- Breaking down the defense supplier base into different industry segments reveals that company type, not size, is the greatest predictor of cyber risk. Companies in the R&D segments are at highest risk;
- When size and industry are combined, patterns become even clearer. Small companies in the Manufacturing and R&D segments are at significantly higher risk than companies in any other size group or industry;
- Risk factors are highly correlated, meaning that companies with more than one risk factor often have many. This also suggests that actions which target certain vulnerabilities should also affect other larger firms within the supply chains;
- Understanding that risk is concentrated and frequently segment-dependent provides useful insights for managing those risks.

Research findings also revealed less surprising facts, including the finding that security regulations, while necessary, are still insufficient:

- 28% of the companies analyzed showed evidence indicating they would fail to meet the most basic, tier-1 CMMC requirements, let alone the more stringent NIST 800-171 requirement with which they should already comply. Additionally, some security issues identified are considered 'high' or 'critical' according to security industry standards.

Perhaps the most jarring findings involved hard statistics about the overall insecurity of the companies included in the study:

1. Over half of the 300 small- to medium-size defense contractors examined in this report had unsecured ports that are critically vulnerable to ransomware attack[17].



2. 48% (146 of 300) of the companies examined had ports vulnerable to ransomware as well as other severe vulnerabilities, including unsecured data storage ports, out of date software and OS, and other vulnerabilities rated severe according to NIST frameworks. These are 'high risk' companies.

48% VULNERABLE

3. Almost 20% (49 of 300) had multiple vulnerabilities as well as evidence of threat targeting - network vulnerabilities, including open ports, and unsupported software. These are higher risks.

20% MULTIPLE THREATS

4. Roughly 7% (19 out of 300) of the companies were identified as critical risk: these businesses had evidence of vulnerabilities, evidence of targeting, and some evidence of compromise, all together.

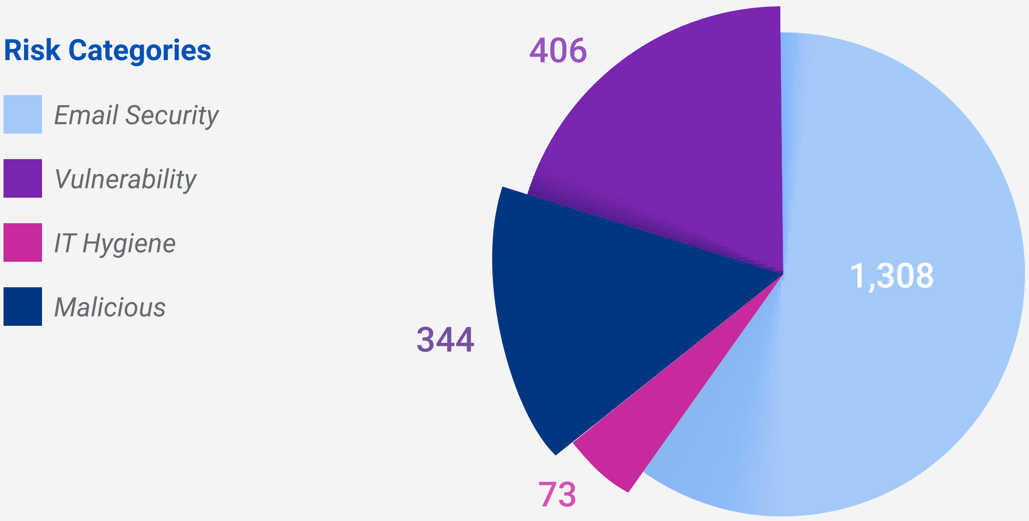
7% CRITICAL RISK

5. More than six months after the announcement of the F5 and the Microsoft Exchange vulnerabilities, nine companies in the database still had the vulnerabilities present on their networks. All of the nine companies were either small manufacturers or large R&D companies.

9 COMPANIES STILL HAD VULNERABILITIES IN THEIR NETWORKS 6 MONTHS LATER

To better understand the nature of the data used for the analysis, the following chart provides an overview of what we found. The number of email security issues is the sum of all of BlueVoyant's observations of domains that 1) belong to one of the companies studied and 2) either lacks evidence of standard security or exhibits evidence of a misconfigured or incomplete security policy implementation. The vulnerability count reflects the total number of observations of software with known vulnerabilities as tracked by NIST and the IT Hygiene category includes a variety of issues ranging from open ports to observations of outdated software as identified using proprietary BlueVoyant methods. Finally, malicious activity counts observations of indicators that suggest company resources are involved in anomalous or criminal activity, as tracked and measured by BlueVoyant's proprietary combination of tools and methods.

Most of the issues we identified related to email security protocols. The next-most prevalent issue related to the presence of unsupported software, suggesting absence of organizational patch policies.



Exploring the Findings

Despite an initial hypothesis that smaller, under-resourced companies would carry the most risk, in this limited study, there was little to no correlation between risk and size without moderating for other factors. Rather, risk was more strongly correlated with industry and stronger still with industry moderated by size. In other words, risk could be best predicted taking into consideration industry and size together.

Overall, manufacturing companies had elevated levels of risk compared to service, R&D, or other industries. There was a stronger correlation between manufacturing and risk than there was between company size and risk.

There were more exciting discoveries when tracking risk across industry and size, however. When size was introduced, the correlation between risk and small (<200 employee) manufacturing firms was stronger than the correlation between risk and manufacturing as a whole. **The number of small manufacturing firms with critical risks (i.e., had evidence of vulnerabilities, threats, and compromises), was almost 14%, which is double the percentage across all industries and sizes.**

The strongest correlation found in this study, however, was the identification of risk with the subset of large (>200 employees) R&D companies. In fact, of those companies, all were high risk: they had network vulnerabilities. 66% were higher risk - they had network vulnerabilities and evidence of targeting. 37.5% had all three (network vulnerabilities, evidence of targeting, and evidence of compromise) and were rated highest risk - almost six times the percentage across the group of 300 companies examined.

Smaller manufacturers often have less resources to address cybersecurity and can lack senior-level management roles tasked solely with information security. Moreover, despite being deeply integrated - often providing parts that are then tracked through the entire supply chain - manufacturers are often not affected by attacks that occur farther down the supply chain and have little incentive to grow more secure[18].

R&D firms have a different profile. Not only are R&D firms vulnerable, they are particularly attractive to attackers. R&D firms work on cutting-edge products, develop valuable IP, and often create and sell software and tech that become components in larger and more important systems - making them attractive as points of entry for malicious insertion or IP theft.

The study identified the risk with the subset of large R&D companies (>200 employees)

66% HIGH RISK

THEY HAD NETWORK VULNERABILITIES AND EVIDENCE OF TARGETING

37.5% HAD ALL 3 RISKS

(network vulnerabilities, evidence of targeting, and evidence of compromise) and were rated highest risk - almost six times the percentage across the group of 300 companies examined.

6X THE PERCENTAGE ACROSS THE GROUP OF 300 COMPANIES EXAMINED

While our analysis was undertaken without the benefit of participation by the subject companies, and therefore is not fully sufficient to determine compliance with either the currently prevailing NIST 800-171 or the pending CMMC requirements, it is an indicative and therefore a powerful tool in the daunting process of identifying ongoing risks and for understanding overall supply chain health, as mapped to the framework of CMMC. As companies get certified with CMMC compliance, we hope that a follow up study will reveal improvements in reduction of risks to the overall attack surface. Regardless, the **third-party security monitoring techniques used for this study will continue to be powerful resources for monitoring and managing supply chain risk.**

Insights from this report are important because they can help the DoD and defense primes focus their attention. They can also be used to support several recommendations that can significantly improve the cost, and overall effectiveness of supply chain security in the DIB. Finally, the following supports and extends **recommendations that are already present in the 2017 DSB Task Force report and in the 2020 Cyberspace Solarium Commission Report.**

1 **Continuous cybersecurity monitoring is a key component of a secure supply chain.** This is critical to supplement additional point-in-time measures of compliance and to ensure continuous security and protection against novel threats.

2 **Primes can reduce their risk exposure by focusing on the most high-risk segments** of their supply chain. This study indicates that manufacturing and R&D companies are at greatest risk, but additional research is needed to confirm and extend these initial findings. However, our findings align with the conclusions of prior reports that R&D companies are particularly vulnerable points for malicious insertion in the supply chain[19] and focusing on them can reduce risk to all segments.

3 **More research is needed.** This report suggests that predictive analysis is possible based on quantitative measures but the sample size of 300 companies is only a small fraction of a huge industry. More analysis incorporating a wider set of variables and a larger sample size will likely produce greater insights to help the DoD and prime contractors identify and more effectively manage risk.

THE THIRD-PARTY SECURITY MONITORING TECHNIQUES USED FOR THIS STUDY WILL CONTINUE TO BE

POWERFUL RESOURCES

FOR MONITORING & MANAGING SUPPLY CHAIN RISK

Conclusion

The U.S. defense supply chain is a vital national security asset. A secure and diverse supply chain is a strategic necessity, especially in the face of persistent and successful cyber espionage. **Prime contractors need to be empowered to secure their supply chains; subcontractors of all sizes need to be supported in achieving compliance; and compliance and security measures must be implemented in tandem, such that the DIB can grow in both size and security.**

There has been a great deal of public discourse about the pending burden of CMMC to SMBs - both the financial burden and the technological burden on companies that may not have in-house IT, let alone security expertise. As challenging as this hurdle is to the success of CMMC, there has been even less clarity regarding how prime contractors will manage their responsibilities pertaining to flowing down requirements and managing security of defense information throughout their networks of subcontractors.

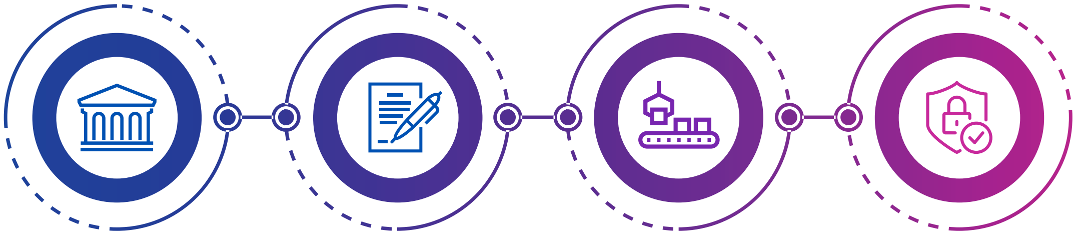
As described in this report, SMBs are increasingly the top initial target of attackers but, more often than not, the end goal is to leverage access to a SMB's network in order to attack the prime via a third-party attack. CMMC represents an opportunity to improve cybersecurity and reduce risk across the entire defense industrial base. However, many questions still remain regarding how subcontractors can quickly get up to speed, how defense primes can best designate into which tiers their supplier base should fall, and how the primes will track and manage the flow down of risk that ultimately affects everyone. In the end, the primes are responsible for ensuring compliance with the security of information they share within their subcontractor network. The financial and logistical obligations that primes face are complex and substantial.

Another important consideration is that compliance is not security. This report shows that the DIB is in a deeply vulnerable state. While CMMC is an improvement on prior regulations that lacked the maturity component, the assessment of compliance is still focused on singular points in time. A company that meets expectations during an assessment may fall out of compliance a year, months, or even weeks later. Continuous monitoring, and a proactive risk model, are absolutely necessary for assurances of a genuinely secure defense industrial base.

This report proves that this is possible. Risk can be proactively identified. Further, our study indicates that risk is not based on a company's size. Instead, risk depends on a complex interaction between industry and size, and between resources and vulnerability and attractiveness to attackers. By proactively identifying pockets of risk, the DoD and primes together can ensure not only a more compliant supply chain, but a more secure one. Primes should implement continuous risk monitoring programs to move beyond compliance to a more persistently secure environment for contractors. Additional research is needed (and called for) to develop a more robust, repeatable, and accurate risk prediction model.

Change needs to be implemented today. The health and security of the U.S. defense sector as a whole is at stake. **Accessible compliance frameworks, robust and proactive risk tracking, continuous external monitoring - all of these steps will help support a more vibrant, diverse, and secure defense sector.** They are complex challenges, but absolutely achievable at the policy level and with closer cooperation between the DoD and the private sector.

Change needs to be implemented today. The health and security of the U.S. defense sector as a whole is at stake.



SOURCES

1 https://dtc.org.au/wp-content/uploads/2020/04/SADILP-2019-Concept-paper-Cybersecurity-Report-FINAL.pdf

2 https://us-cert.cisa.gov/ncas/current-activity/2021/05/19/update-cisa-fbi-joint-cybersecurity-advisory-darkside-ransomware

3 https://therecord.media/ransomware-gang-leaks-data-from-us-military-contractor-the-pdi-group/

4 https://www.cybersecurity-insiders.com/ransomware-attack-on-us-dod-contractor/

5 https://www.bankinfosecurity.com/st-engineering-confirms-maze-ransomware-attack-a-14399

6 https://threatpost.com/nuclear-contractor-maze-ransomware-data-leaked/156289/

7 https://www.fifthdomain.com/2020/03/02/a-hacker-group-says-it-has-major-defense-companies-data/

8 https://techcrunch.com/2020/03/05/cpi-ransomware-defense-contractor/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAABxMFkO06oL02pI0ZFk_FLPr8Q6--apt0p6tghTa7_4HtO3k2gOu449ZeJ8E55iw4Ct0iCxmGRUxmS317pOJ84aLhL0ghjB3_t3QWoqSdcl6U26kLw8d1ReEoCVo9lDXkCryJBhc_2F5XNNSXtyuDWbhcJYnWBttJpeUBqfO2uG0

9 https://searchsecurity.techtarget.com/news/252500356/US-defense-contractor-BlueForce-apparently-hit-by-ransomware

10 https://phys.org/news/2011-07-stolen-defense-contractor-pentagon.html

11 https://www.cyberscoop.com/defense-contractors-chinese-government-hacking-nsa/

12 https://www.washingtonpost.com/national-security/chinese-hackers-compromise-defense-contractors-agencies/2021/04/20/10772f9e-a207-11eb-a7ee-949c574a09ac_story.html

13 https://www.cisa.gov/defense-industrial-base-sector#:~:text=The%20Defense%20Industrial%20Base%20partnership,Department%20of%20Defense%2C%20and%20government%2D

14 https://www.acq.osd.mil/cmmc/docs/CMMC_ModelMain_V1.02_20200318.pdf

15 BlueVoyant has written extensively on CMMC regulations and their implications for companies that must comply at each level. More information available at https://www.bluevoyant.com/cmmc-services

16 https://www.michiganstateuniversityonline.com/resources/supply-chain/king-of-supply-chain-still-reigns/#:~:text=U.S.%20News%20%26%20World%20Report%20ranks,and%20undergraduate%20supply%20chain%20programs.

17 https://us-cert.cisa.gov/ncas/current-activity/2021/05/19/update-cisa-fbi-joint-cybersecurity-advisory-darkside-ransomware

18 https://webarchive.nationalarchives.gov.uk/20160902161433/https:/www.cert.gov.uk/wp-content/uploads/2015/02/Cybersecurity-risks-in-the-supply-chain.pdf

19 https://dsb.cto.mil/reports/2010s/DSB-CyberSupplyChain_ExecutiveSummary_Distribution_A.pdf

About BlueVoyant

At BlueVoyant, we recognize that effective cybersecurity 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.

Accuracy. Actionability. Timeliness. Scalability.

Founded in 2017 by former Fortune 500 and former government cyber officials, BlueVoyant is headquartered in New York City and has offices in Maryland, Tel Aviv, San Francisco, Manila, Toronto, London, Latin America, and Budapest.

Visit www.bluevoyant.com.

BlueVoyant®

To learn more about BlueVoyant, please visit our website at **www.bluevoyant.com** or email us at **contact@bluevoyant.com**