Cybersecurity in Software Supply Chain And the role of SLTT Governance

[DOI 10.5281/zenodo.7847284]

André Garrett

Georgetown University

December 14, 2022

Review Committee:

Professor Kathleen Moriarty

Professor Matthew Shabat

Professor Matthew Halvorsen

Dr. Frederic Lemieux

Acknowledgements

To my parents,

†Martha R. Garrett and †Kenneth Garrett who instilled in me a passion for learning, exploration, advocacy and to never ever be afraid to question and ask “why”

Acknowledgements

I would like to acknowledge and thank a number of individuals who provided invaluable insights, support, and guidance throughout this research study, especially Kathleen Moriarty, Matthew Shabat and Dr. Frederic Lemieux.

I would like to also thank and express sincere appreciation and gratitude to the companies and individuals who contributed their time, experience, and knowledge to this research:

1. AWS, Dave Rogers
2. CIS, Karen Sorady
3. CIS, Kathleen Moriarty
4. Cybeats, Dmitry Raidman
5. FedEx, Nik Puri
6. IBM, Kelvin Coleman
7. Microsoft, Adrian Diglio
8. NIST, Jon Boyens
9. Redhat, Luke Hinds
10. SLTT, Gary Coverdale

Executive Summary

On May 12, 2021, Executive Order 14028, Improving the Nation's Cybersecurity, was published. It acknowledged for the first time the growing importance of software security in today's supply chain in the federal government and the nation. Moreover, with vulnerabilities exposed by SolarWinds and Log4J posing a severe threat to consumer products, enterprise software, and web applications, the role of cybersecurity in today's software supply chain has taken on new meaning. Software supply chains are now an essential component of networks used by State, Local, Territory, and Tribal organizations (SLTT) providing services and products to communities they support, including critical infrastructures like hospitals, schools, and libraries. Hence, the SLTT governance's role in software supply chain cybersecurity becomes just as important.

With rapidly expanding technologies and the explosive growth of IoT devices, the role of software in supply chains has increased tenfold over the past decade. Various reports have identified the vulnerabilities and threats to software supply chains, which mostly point to open-source software, issues of integrity, exploitation of the software supply chain process, and third-party risks. However, research needs to be more extensive when examining software supply chains with their many dependencies and the role of SLTT governance in mitigating risk.

This study used qualitative research to collect data to analyze common trends, themes, gaps, and opportunities. In over 11 hours of interviews with participants from various software supply chain fields, the study examines vulnerabilities, threats, and challenges facing those responsible for software supply chains today. Commonalities identified include addressing weaknesses in human capital, processes, and SLTT governance, as well as limitations in funding and today's security architecture.

Solutions to combat attacks and threats in vulnerabilities in today's software supply chain are only now coming to fruition. Moreover, while there has been incremental progress, our findings show that the continued rapid growth of emerging technologies will outpace efforts to prevent and mitigate cybersecurity risks in software supply chains. New and bold ideas, as well as additional research, are warranted to address this growing gap.

Table of Contents

List of Charts and Tables

Introduction

The growing awareness and importance of today's supply chain became evident as businesses and everyday consumers experienced shortages of everyday staples to computer chips during the Covid-19 pandemic and thereafter. From the newsroom to the boardroom, the significance, sometimes overlooked, of today's supply chain was front and center.

With the rapid evolution of technology and a 24/7 online world, software now propels the multiple facets of the physical components of supply chains, and hence making software supply chains essential, as well as providing an opening for nefarious actors, from cyber criminals to nation states for cyber attacks. According to Sonos (2022) malicious software supply chain attacks have increased 633% YoY and charting the next generation of software supply chain attacks from 2019-2022, indicates a 742% YoY average growth rate.

Executive Order 14028 (EO) on Improving the Nation's Cybersecurity released in May 2021 and the OMB Memo M-22-18, dated September 14, 2022 on "Enhancing the Security of the Software Supply Chain through Secure Software Development Practices," both acknowledge the increasing number of software security risks throughout the supply chain. Federal

departments and agencies become exposed to cybersecurity risks through the software and services that they acquire, deploy, use, and manage from their supply chain (which includes open source software components). Acquired software may contain known and unknown vulnerabilities as a result of the product architecture and development life cycle. This in turn may pose severe risks to the critical infrastructure that State, Local, Territorial, and Tribal organizations have a role in protecting in ensuring the safety and security of the communities they support.

As per the aforementioned, the U.S. Government has only just begun taking steps to address software supply chain cybersecurity. And while the expected growth of IoT devices has slowed due to the COVID-19 pandemic and supply chain disruptions, it is anticipated there will be approximately 27 billion connected devices by 2025 which will only lead to an increase in cyber attacks as hackers seek ways to exploit weak cybersecurity measures (Hasan, 2022).

"The increasing dependency on computing and communications backbones is changing how supply chain mechanisms operate and interoperate. The devastation caused by exploiting a vulnerability in a military supply chain can have consequences beyond economics, effectively endangering human lives" (Sobb et al., 2020).

This research aims to answer the following two questions: a.) Cybersecurity Governance is essential to mitigating risk in today's software supply chain. Is there a baseline governance approach that would benefit all SLTT organizations? And b.) What is the best solution for software supply chain cybersecurity with the rapid digital transformation in supply chains?

Due to limited research in software supply chain cybersecurity and the role of SLTT governance in cybersecurity effectiveness, the qualitative research methodology was selected for this study. Over eleven hours of interviews with 10 participants were conducted over seven days, and the data analysis from those interviews and various source information follows. The research also includes preliminary observations and recommendations that emphasize the need for new and bold actions by the government and private sector if there is the expectation of being able to prevent and mitigate cybersecurity risks that exist today and those unforeseen in the future.

Review of Literature

This review aims to synthesize the concentrated analysis and discussion of Supply Chain Cybersecurity governance in risk management benefiting State, Local, Tribal and Territorial organizations (SLTT). The Information Technology sector has become indispensable to supply chains worldwide and will help provide a framework for understanding today's opportunities, vulnerabilities, and cybersecurity risks.

The Cybersecurity & Infrastructure Security Agency (CISA) has identified the Information Technology (IT) sector as 1 of 16 critical infrastructure sectors "whose assets, systems, and networks, whether physical or virtual, are considered fundamental to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof" (CISA, 2019). Software supply chain is integral to IT performance and is essential to the management of data.

II. Overview of Traditional Supply Chains and Logistics

The unexpected COVID-19 pandemic brought supply chains under the microscope of everyone from heads of states to boardrooms to the average consumer unable to purchase everyday goods and services. It was a critical

warning about the importance of supply chains and how disruption can impact the daily lives of citizens living in towns and cities across the globe. According to Sherman, (2012) “The supply chain impacts virtually every financial metric included in the company's balance sheet and income statement". And with the rapid evolution of advanced technologies, software and software procurement increase the efficiencies, speed as well as vulnerabilities of supply chains. But precisely, what is a supply chain and the impact of its evolution?

Supply chains have existed since the dawn of man when humans began trading and have evolved tremendously since the turn of the century. According to Gomez, (2022), during the Industrial Age, approximately between the late 1800s to early 1900s, most goods were produced locally or regionally due to the limited availability of transportation options which resulted in manufacturing taking place close to the source of raw materials to ensure businesses could produce goods skillfully and quickly. Move forward beyond the 1920s, and we see the assembly line and mass production rise to the adopted method for manufacturing goods. The further maturation of the railroad (and late highway) systems in the U.S. and Europe further enabled supply chains to elongate such that raw material sources and manufacturing sites no longer required much coupling.

According to Sobb et al. (2020), the traditional supply chain is a network of systems, processes, and organizations that produce valuable goods and services and their delivery to their end-user. Supply chains are the binding link of nations, physical distribution networks, and transport systems that, in totality, create a global network. Supply chains comprise flows of materials, goods, and information, which pass within and between organizations, linked by tangible and intangible facilitators, including relationships, processes, activities, and integrated information systems. Their foundational technologies are transport systems, communication platforms and networks, and physical distribution networks. Supply chains can be viewed in three phases; a procurement phase, a production phase, and a distribution phase. Supply chains integrate software procurement, manufacturing, and distribution activities as a continuous and cohesive process. Supply chain logistics is the "point-of-origin to point-of-consumption " component of essential business operations.

Post-World War II, American manufacturing had learned a great deal during the war regarding design to production cycle reduction, quality control, learning curves and operations research. Sadly, the majority of this knowledge was set aside after the war as it was felt to be unnecessary. Unbeknownst to many today, but after the war, the United States remained

the only "significant production capability in the world." Essentially, all goods the U.S. purchased and used were manufactured in the U.S. In addition, practically all manufactured goods sold around the world were being supplied by the U.S.; competition was non-existent (Pope, 2011).

According to MacCarthy et al. (2016), over the course of history supply chains have emerged to meet the diverse needs of human societies, to exploit natural resources and to enable humans to engage profitably in commerce and trade

Moving forward to the 21st century, we see the rise of e-commerce, the buying and selling goods and services over the internet, which has tremendously impacted businesses and the global supply chain. The sourcing of goods and products is now from suppliers the world over. This global supply chain has led to a more intricate network of suppliers and logistics providers interconnected via rapidly advancing information technology. Consumers, businesses, State, Local, Tribal and Territorial governments are now dependent upon a global supply chain that has become more complex and robust than ever in human history.

Information Technology (IT) now plays a significant role in U.S. elections. Computers have become essential to the democratic process where the

software supply chain takes center stage. Moreover, the software is a critical component in efforts to manage cybersecurity-related supply chains. Moreover, the prominent role that software now plays in cybersecurity has prompted organizations such as the Center for Internet Security (CIS), National Institute of Standards and Technology, and National Counterintelligence and Security Center (NCSC) all publishing guidance to help vendors manage software supply chain attacks.

III. Information Technology and Software Supply Chain

There is a general consensus in literature that the rise of Information Technology in the 1980s had a significant impact on supply chains. The rapid technological advances led to an expansion in the use of computers and other electronic devices. This in turn improved an organizations ability in the tracking of inventories and management of shipments resulting in improved efficiencies in the flow of goods worldwide. It would soon become a necessity for companies to utilize IT techniques and methods for integrating their internal business functions which would improve efficiencies, productivity and rapid responses to an increasingly changing consumer demands. IT would become the backbone of supply chain information

systems for strategic planning, warehousing, inventory control, manufacturing, logistics and transportation, supplier and customer management. Enterprise Resource Planning (ERP) and Customer Relationship Management (CRM) systems would emerge as key to being able to exploit advances in IT techniques and methods. These systems allow for the broadening of connectivity between business partners, suppliers and customers (Marinagi et al., 2014).

The three core components of today's computers and systems identified by cis (2022) are hardware, software, and firmware. Each component has a role in IT used by SLTT government agencies at all levels, especially during elections. As described by the Center for Internet Security, "hardware includes the physical components of a computer system, which may wear out over time and require replacement. The software includes sets of instructions that allow a variety of inputs from the user. Firmware is a specific type (or subset) of software designed to act as the intermediary between the software and hardware or for operating single-purpose embedded systems, such as printers or routers. End users typically have limited interaction with firmware, modified infrequently when it comes to vulnerabilities. Software vulnerabilities are the simplest to remediate,

typically via regularly scheduled updates but remain the "primary vector cyber threat actors use to exploit systems” (cis, 2022).

Software supply chain’s role in IT enables companies to collect transactional data and information and analyze it to determine the best decisions in achieving their mission and objectives. The software companies use in IT enables various processes that help manage client and supplier relationships. Software is a critical component in Client Relationship Management (CRM), Supplier Relationship Management (SRM), and Internal Supply Client Relationship Management (ISCM) together, all considered the macro-processes of a supply chain.

According to Pressman (2005), in just over 50 years, computer software has undergone rapid and radical change. Extraordinary improvements in hardware performance, unfathomable changes in computing architectures, vast increases in memory and storage capacity, and a wide array of novel input and output options have all accelerated more sophisticated and complicated computer-based systems. Sophistication and complexity can produce astonishing results when a system succeeds, but they can also become problematic for those who must build complex systems and an opening gateway to the new world of cybersecurity threats and vulnerabilities we see in software supply chains today.

IV. Software Supply Chain Vulnerabilities

There is a general consensus in literature today, that software is truly the most vital enabler of the modern world. As industries continue to rapidly expand the benefits of connectivity via the Internet of Things (IoT), the cloud, and mobile device penetration, it also expands the software supply chain's size, depth, complexity, and attack surface. This crossroad of factors has elevated cybersecurity to new heights. According to Woods & Bochman (2018) "All systems fail; complex systems fail in complex ways. Software has a defect rate measured in the number of flaws per 1,000 lines of code." General computing components provide channels for incidents and nefarious actors to undermine their reliability and safety. Eliminating all security vulnerabilities is often not possible in the software development process. Over 10,000 security vulnerabilities are detected yearly in standard off-the-shelf components. They appear in global supply chains, including many critical infrastructure sectors that keep global economies moving.

Woods & Bochman, (2018), also state that software design vulnerability and weaknesses can multiply unknowingly or deliberately throughout the multiple steps in supply chains. Add to these common occurrences is the challenge that one single software component can compromise an entire system that supply chains rely upon.

And an example provided by Korolov, (2020) is the NotPetya supply chain attack attributed to Russia compromised Ukraine's accounting software to target the country's infrastructure. However, the malware spread rapidly to other countries causing more than $10 billion in damage while disrupting major multinational corporations such as Maersk, FedEx, and Merck.

The National Vulnerability Database (NVD) of the US National Institute of Standards and Technology (NIST) maintains a collection of Common Vulnerabilities and Exposures (CVEs) reported by security experts, researchers, and vendors. In 2021, the NVD disclosed approximately 20,157 security vulnerabilities, more than in any other year (CSCC Labs & NIST, 2022).

Cyberattacks are carried out via cyberspace and target an organization's use of that cyberspace with the sole intent of obstructing, disabling, damaging, or maliciously controlling a computing infrastructure or destroying the integrity of the data, or stealing controlled information. Lately, cyberattacks such as those executed against SolarWinds and its customers discovered in 2020 "and exploits that take advantage of vulnerabilities such as Log4j expose weaknesses within software supply chains. This issue transcends commercial and open-source software and impacts private and Government enterprises. Cyberattacks such as this demonstrate the increased need for

software supply chain security awareness and realization regarding the potential for software supply chains to be weaponized by nation-state adversaries using similar tactics, techniques, and procedures (TTPs)" (ESF, 2022).

Section 4 of Executive Order 14028 on Improving the Nation's Cybersecurity, signed by President Biden in May 2021 specifically underscores the need for "enhancing software supply chain security" due to critical importance to the Federal Government in its ability to function. It also highlights the "security and integrity of "critical software" — software that performs functions critical to trust (such as affording or requiring elevated system privileges or direct access to networking and computing resources) "— as a major concern (The White House, 2021).

According to Zhu et al. (2021), due to the global distribution of the IoT software supply chain, the structure of the network chain, purchasers, and users, the risk control capabilities of the IoT supply chain are gradually reduced as the transparency of the supplier decreases. Malicious functions, data leakage, and critical product interruptions exist in any link or service provision will destroy the continuity of related business and bring uncontrollable security risks.

And the NCSC (2021) describes improved cybersecurity postures across most networks and computers have made software supply chain attack vectors increasingly attractive because many software development and distribution channels lack sufficient protections. Software supply chain attacks can be used for espionage as well as to manipulate or destroy data and provide difficult to detect access for future attacks.

There has been significant vulnerabilities discovered that can lead to attacks. DeRusha (2022) comments that in 2020, a number of Federal agencies and large corporations were compromised by malicious code that was added into SolarWinds software. This small change created a backdoor into the digital infrastructure of Federal agencies and private sector companies. This incident was one of a string of cyber intrusions and significant software vulnerabilities over the last two years that have threatened the delivery of Government services to the public, as well as the integrity of vast amounts of personal information and business data that is managed by the private sector. And By strengthening our software supply chain through secure software development practices, we are building on the Biden-Harris Administration's efforts to modernize agency cybersecurity practices, including our federal 'zero trust' strategy, improving our detection and response to threats, and our ability to quickly investigate and recover from

cyber-attacks. It is part of a larger enterprise cybersecurity and information technology (IT) modernization plan that ensures we can deliver a simple, seamless, and secure customer experience.

V. SLTT Cybersecurity Governance Opportunities

There is not an abundant of research or case studies examining the role and effectiveness of SLTT Cybersecurity Governance. But with the given events of cyberattacks by Nation States such as Russia, China and North Korea, there is growing alarm by U.S. Congress and both the private and public sector.

Due to the critical infrastructure at the State Local Territory Tribal level and subsequent impact on businesses and communities at large, there has been ongoing efforts to improve cybersecurity. In June 2019, Thomas Duffy, SVP Operations and Security Services & Chair of the MS-ISAC Center for Internet Security, testified in Congress that cyber protections at all levels of government are critical, and central to the fiduciary responsibility to protect the data that is entrusted to government by our citizens and businesses. Local governments connect to state governments, state governments connect to the federal government. All levels of government have a shared

responsibility for safeguarding information. Data on citizens is tracked from cradle to grave, from the issuance of your birth certificate, to the filing your death certificate. Regarding the question “has the cybersecurity posture of and local governments improved?” – the answer is yes. There are, however, other related and equally important questions that should be asked. If the question is “have and local governments kept pace with advancing threats and the rapidly expanding cyber infrastructures that need to be protected?”, the answer is probably not. If the question is “are state and local governments prepared to build, maintain and evolve their cybersecurity programs commensurate with the risks that they will face in the future?”, the answer is again, probably not. Both state and local governments continue to make news for ransomware, cybercrime and other cybersecurity-related issues every week” (USHOR, 2019).

MS-ISAC, the Multi-State Information Sharing & Analysis Center “mission is to to improve the overall cybersecurity posture of U.S. State, Local, Tribal, and Territorial (SLTT) government organizations through coordination, collaboration, cooperation, and increased communication” (cis, 2022b). According to USHOR (2019) MS-ISAC members include all 56 states and territories and more than 5,000 other state and local government entities. In it’s annual cybersecurity maturity assessment called the Nationwide

Cybersecurity Review (NCSR) of state and local governments it identified the following top five security concerns:

- Lack of sufficient funding
- Increasing sophistication of threats
- Lack of documented processes
- Emerging technologies
- Inadequate supply of security professionals

In providing an understanding of this assessment, USHOR (2019) commented the assessment uses a scale of 1-7 to measure cybersecurity maturity, and establishes a score of 5 as the minimum-security level organizations should strive for. The state average in 2018, was 4.7, with 44% states achieving the baseline of 5. The local government average is 3.4, with only 18% achieving the baseline minimum of 5. There have been improvements over time, with the states improving by 5% over the past 3 years and local governments improving by 17%. And while improvements have been achieved, there is still significant opportunities existing to improving sustainable cybersecurity.

The above analysis points to the role SLTT Cybersecurity Governance can have in helping to mitigate cyber risks. Though there is limited studies in the role of governance in SLTT cybersecurity, there is growing literature which argues that the government should play a more significant role. Gilligan (2017) makes a case for government oversight and comments that the government should establish mandatory minimum standards for security, for they are the largest procurer of products and services. A government-defined minimum standard for cyber security that the vendor must demonstrate prior to purchase can significantly impact ensuring that these products are available to everyone. A standard against which SLTT can hold vendors liable for delivering insecure products is needed.

Government systems that are funded by taxpayer monies should be examples of excellence. The OPM (Office of Personnel Management) breach and every other government security breach highlight the failure of government organizations to provide basic cybersecurity hygiene.

The Center for Internet Security (CIS) has worked with hundreds of collaborators to develop the CIS Controls — a consensus-based roadmap for implementing basic cyber hygiene. The CIS Controls were developed to address 80+% of cyber-attack threats based on information provided to the project by the National Security Agency.

Many CIS Controls address technical and management practices and related tools fundamental to any well-managed cyber operation. However, many government organizations have not implemented this basic cyber hygiene. Government should be setting the example, and senior officials in government need to hold government managers accountable for providing basic cyber hygiene.

The government is the only organization with the authority and clout with product providers to make the rapid progress needed to improve cybersecurity.

Highlights from a 2018 study of all 50 states of the CISO's role, governance, reporting workforce, and operations, Deloitte-NASCIO (2018) provides the following insight:

> Most states have a formally approved governance process delineating a central vision and guidelines for cybersecurity across the state enterprise. CISOs have also increased their reporting frequency to governors and senior state officials and furthered their collaboration with federal and state governments. As CISOs continue to build a cybersecurity practice, they report gaining more confidence in their abilities to combat cyber threats. However, these governance strides and establishing the CISO role's legitimacy have not resulted in significant progress in overcoming the top challenges US states face in implementing effective cybersecurity programs.

Various studies show trends that software supply chain attacks are rising and impactful. As Herr et al. (2020) point out, these attacks exploit natural seams between organizations and abuse relationships where users expect to find trustworthy code. Targeting the supply chain for code can help magnify the value of a breach and sow distrust in widely used open-source projects. Second, these attacks can drive compromise deep into an organization's technology stack, undermining development and administrative tools, code-signing, and device firmware. Furthermore, third, software supply chain attacks have strategic utility for state actors and have been used with substantial impact, especially by Russian and Chinese groups. This trend is likely to continue and should motivate action from US policymakers.

One of the few reports and case studies discovered below provides a limited view into cybersecurity governance at the state level.

As published, cisa (2017) State Cybersecurity Governance Case Studies Cross-Site Report is a collaboration between the Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Division and the National Association of State Chief Information Officers (NASCIO) to examine how states govern cybersecurity. The Homeland Security Systems Engineering and Development Institute (HSSEDI), a DHS-owned Federally

Funded Research and Development Center (FFRDC), developed the case studies.

This report and supporting case studies examine how five states, identified by the Department of Homeland Security (DHS) and the National Association of State Chief Information Officers (NASCIO), govern cybersecurity as an enterprise-wide, strategic issue across state government and other public and private sector stakeholders in these six areas (cisa, 2017) :

- Strategy & Planning Governance Trends
- Budget & Acquisition Governance Trends
- Risk Identification & Mitigation Governance Trends
- Workforce & Education Governance Trend
- Incident Response Governance Trends
- Information Sharing Governance Trends

The report and case studies explore cross-enterprise governance mechanisms used by states across a range of common cybersecurity areas and offer insight into trends and concepts beneficial to other states and organizations that face similar challenges.

Research Gaps

While the aforementioned reports and case studies provide an overview of governance trends in managing SLTT cybersecurity, there does not appear to be a metric or measurement to determine the success of a risk mitigation strategy or impact of identified trends ongoing. How are the various cybersecurity controls, whether from CIS, CISA, NIST, ISO or other validated frameworks being utilized? And as the cost of cyber attacks continue to rise, how will SLTTs integrate or expand involving tools and standards such as Software Bill of Materials (SBOM) and Information Sharing to help mitigate risk?

Carter (2020) research indicate two-thirds of security breaches result from supplier or third-party vulnerabilities. Moreover, organizations increasingly provide third parties access to their IT infrastructure for business reasons. However, IT and security leaders need to help their business leaders understand the risks of third-party access and take steps to help manage these risks to an acceptable level."

As information technology continues to evolve, challenges for software supply security become even more intricate and sophisticated, as well as the technologies used to mitigate them.

Consider Gartner (Hippold, 2022) predicts that by 2026, more than 75% of commercial supply chain management application vendors will deliver embedded advanced analytics (AA), artificial intelligence (AI), and data science. Furthermore, 25% of supply chain execution (SCE) vendors will have rewritten their core application to a microservices architecture, but only 5% of supply chain organizations will have adapted to true composability.

And as Dolci et al. (2017) points out Supply Chain Governance (SCG) is a topic that has been widely studied in recent years for analyzing inter-organizational relations as a multi-dimensional phenomenon embedded in the company's structures and processes. Studies analyzing all aspects of SCG at the same time, however, have not been found. Moreover, there are a number of performance indicators, but there is a lack of consensus on what determines the performance of these supply chains. Furthermore, few studies have attempted to understand the effects of SCG on supply chain performance.

There are even less studies analyzing all aspects of SCG for SLTTs as well as their role in software supply chain security.

Methodology

In 2016 the Federal Cybersecurity Research and Development Strategic Plan coordinated by the National Science and Technology Council was released as part of then-President Obama's Cybersecurity National Action Plan (CNAP). It was the most comprehensive federal cybersecurity research and development (R&D) plan. It challenged the cybersecurity R&D community to provide the techniques and tools for "deterring, protecting, detecting, and adapting to malicious cyber activities." It stated that software defects are common and lead to multiple vulnerabilities that require scientific and technological advances to implement software, firmware, and hardware resistant to malicious cyber activities. The plan also noted, "whether in government, academia, or the private sector, organizations that sponsor research, perform research, or advise on such investments have an opportunity to contribute" (The White House, 2016).

Five years later and after the devastating SolarWinds cyber attack, Section 4 of Executive Order 14028 on Improving the Nation's Cybersecurity, signed by President Biden in May 2021, underscored the need for "enhancing software supply chain security" due to the critical importance to the Federal Government in its ability to function. It also highlights the "security and

integrity of "critical software" — software that performs functions critical to trust (such as affording or requiring elevated system privileges or direct access to networking and computing resources) "— as a significant concern (The White House, 2021).

Cybersecurity research is now one of the fundamental tools for improving cybersecurity in software supply chains and may provide insights for improvements in SLTT Cybersecurity governance.

The following three components outline the methodology and research design to be used for conducting this research study. The Qualitative approach is best suited to respond to the research questions in this study and consider the limitations outlined in the closing section. Though the terms to describe a cyber attack, such as computer virus, Trojan Horse and the Morris Worm came into being in the 1980s, it was not until the 1990s and 2000s which saw the significant growth and development of the internet along with the growth of the cybersecurity industry and cyber crime. With limitations in research in the areas of software supply chain cybersecurity and role of SLTT governance, qualitative research was selected in being able to yield the most data for analysis within the allocated timeframe for research.

I. **Approach** - Qualitative Research

Cybersecurity is a vast research area that can include various aspects from organizational to technical, sociology, as well as psychological, legal to other undefined characteristics. Many researchers have examined Cybersecurity with various research methods (e.g., observational, mathematical, descriptive, experimental, and applied). As Fujs et al. (2019) have pointed out, using qualitative methods provides complementary insights and may produce rigorous, insightful, and consequently highly cited papers. Qualitative methods refer to naturalistic inquiry, interpretive, and inductive research methods developed to gain a deeper insight into studied topics.

Moreover, as Statswork (2021) underscores, the purpose of qualitative research is to estimate market research and analytics based on the insights of people who will participate in the set of questions or interviews conducted, which provides qualitative data which gives the familiar and genuine opinions of people regarding market insights. Furthermore, as Wolf (2019) suggests, Qualitative designs not only enable but also encourage flexibility in the content and flow of questions to challenge and probe for deeper meanings or follow new leads if they lead to a more profound understanding of an issue. The first step in Qualitative research is data

collection, followed by a segment of analysis where the collected data has to be analyzed by researchers for accurate results and outcomes.

In selecting this research methodology it was important to select the analysis method (or methods) which aligns with the research's overall goals and objectives. And as Crossman (2020) points out qualitative researchers use their own eyes, ears, and intelligence to collect in-depth perceptions and descriptions of targeted populations, places, and events. The two methods used for conducting this study were:

- In-depth Interviews (Face-to-Face)
- Content Analysis

And for data analysis and organization which included filing, sorting and coding, the following tools were used:

- ATLAS.TI
- EVERNOTE
- ROAM

II. **Sources and Data**

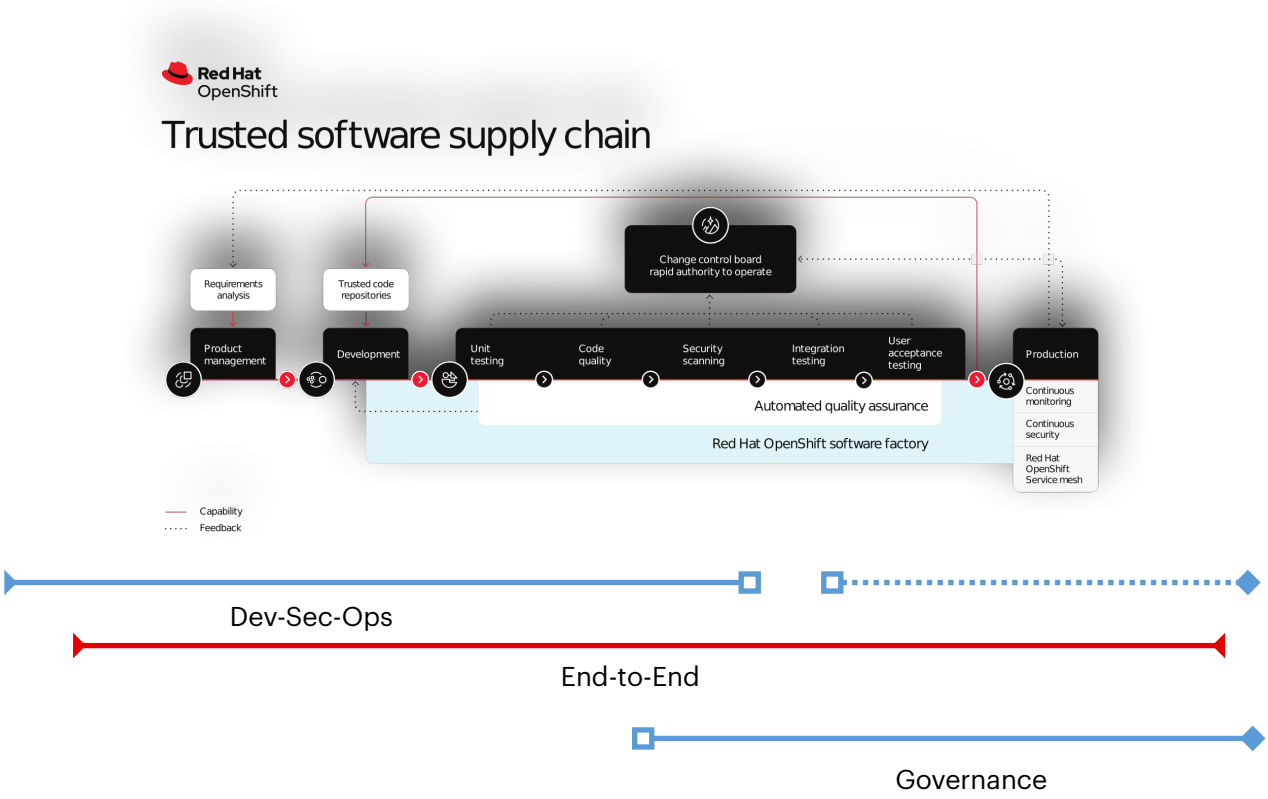


Figure 1. Acquisition and deployment segmentation

Sources and data collection process were approached from viewing the software supply chain as identified from the following three segments in acquisition and deployment:

End-to-End

Dev-Sec-Ops

Cybersecurity Governance

Utilizing the above segmentation approach helped in drafting the matrix of variables, as well as the analytical design and overall methodology.

Primary Data

Data pulled from face-to-face interviews served as the primary source for this qualitative study; as Sileyew (2019) suggests, primary data acquired from the original source of information can be more reliable and have a more confident level of decision-making with the trusted analysis having direct contact with the occurrence of the events.

Sample size: The study's number of participants, as Wolf et al. (2019) recommended, suggests that Qualitative samples are typically small and purposive. In-depth interview informants are usually selected based on unique characteristics or personal experiences that make them exemplary for the study, if not typical in other respects. Key informants are selected for their unique knowledge or influence in the study domain.

For in-depth interviews, 10-13 participants (subject matter experts) were chosen to participate in face-to-face one-hour interviews over a two week time period. The matrix of variables or category of questions were sent to participants in advance.

In addition, participants were selected based on their knowledge, expertise, and current work in the cybersecurity supply chain, software supply chain,

and SLTT governance, as well as the following criteria: 1.) Key area of focus, 2.) Type of Organization, and 3.) Level of Engagement.

Principal Interview Data Coverage:

Table 1 Interview Data Coverage

Instrument	Planned Participants	Verified coverage	Success Level
Interviews / discussion	10	10	100%
Observation	10	10	100%

Interview participants for the study are from organizations representing a broad section of society experienced in multiple facets of facilitating cybersecurity in software supply chains, including academic, government institutions, and for-profit and non-profit entities in technology, cybersecurity, policy, and risk management. Entities selected were evaluated in their ability to elicit and gain keen insights into the following key areas: Cyber and Supply Chain Risk, Supply Chain Cybersecurity, Software Supply Chain Security, Role of SLTT Governance, the impact of emerging technology, Threats, and Vulnerabilities.

Below is a representative sample of the principal data coverage from a cross-section of enterprises and organizations:

Table 2 Interview Participants Overview

Organization	Problem Statement Key Area Focus	Org Type	Level of Engagement
AWS	Software Supply Chain Cybersecurity	For Profit / Multinational	Product Sr. Mgr
Center for Internet Security (CIS)	Software Supply Chain Cybersecurity, Governance	Non-Profit	CTO
cybeats.com	Software Supply Chain Cybersecurity, Governance	For Profit	Co-Founder/CTO
FedEx	Cybersecurity, Supply Chain, Software Supply Chain Cybersecurity, Goverance	For Profit / Multinational	SVP IT
IBM	Cybersecurity, Supply Chain, Software Supply Chain Cybersecurity, Goverance	For Profit / Multinational	Executive Partner
Microsoft	Software Supply Chain Cybersecurity, Governance	For Profit / Multinational	Principal Program Manager
Multi-State Information Sharing & Analysis Center® (MS-ISAC®)	Cybersecurity, Software Supply Chain Cybersecurity, Governance	Non-Profit	VP/Former CISO
National Institute of Standards and Technology (NIST)	Software Supply Chain Cybersecurity, Governance	Government	Deputy Chief
RedHat	Software Supply Chain Cybersecurity	For Profit / Multinational	Software Engineer
SLTT West Coast	Cybersecurity, Software Supply Chain Cybersecurity, Governance	Non-Profit	CISO

Secondary Data

Secondary data will include existing case studies, white papers, research papers, consultant reports and blogs from organizations who currently participate in this vector. Sources for this data include but not limited to: Academia, U.S. Government, Non-profit and For-profit organizations, e.g. Center for Internet Security (CIS), National Institute of Standards and Technology (NIST), Cybersecurity & Infrastructure Agency (CISA), Gartner, McKinsey, CSCC Labs, and Deloitte.

In addition, existing databases such as the National Vulnerability Database (NVD) of the US National Institute of Standards and Technology (NIST) and the MITRE ATT&CK® Common Vulnerabilities and Exposures were explored to evaluate current software supply chain threats and vulnerabilities to determine potential for data mining for relevant implications and historical trends within the current research analysis timeframe.

III.Analytical Design

This study focuses on the following areas of Supply Chain Cybersecurity and the role of State, Local, Territory, and Tribal (SLTT) organization governance:

- Software Supply Chain
- Rapid evolution in IT impact, e.g., Supply Chain 4.0

- Cybersecurity threats, vulnerabilities, existing solutions, and opportunities
- SLTT Cybersecurity governance comparisons

In-depth interviews provided a significant amount of data for analysis in helping to identify key themes, weaknesses and opportunities in current software supply chain cybersecurity approaches in preventing and mitigating risks across industries.

In addition, a comparative analysis of the below case studies along with participant interview data provided additional evidence in helping to identify trends, themes, commonalities, gaps, and opportunities that exist in examining the role of cybersecurity and governance in SLTT organizations

As Njie & Asimiran (2014) suggests, qualitative research is generic and needs a direction that is mainly decided by the specific aim and type of study one chooses to conduct to arrive at a result. The Case study is one such direction that is prompted by the need to thrust deep into a specific unit, person, program, or institution for a greater understanding which would not have been possible through other means.

Table 3 Case Studies Analyzed

Year	Case Study
2017	SCGCS - State Cybersecurity Governance Case Studies - DHS - NASCIO (Department of Homeland Security and the National Association of State Chief Information Officers
2018	DNCS - Deloitte-NASCIO Cybersecurity Study - 2018
2020	National Institute of Standards and Technology Case Studies in Cyber Supply Chain Risk Management
2021	NCSR - Nationwide Cybersecurity Review -Multi-State Information Sharing and Analysis Center (MS-ISAC®) and Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC®)

Limitations

There is limited in-depth public research or information available evaluating software supply chain cybersecurity, and there is even less so when gauging the overall effectiveness of SLTT Cybersecurity governance. This short supply of resources results in notable limitations to accomplishing a rigorous review to obtain accurate results. Moreover, the current timeframe constraints prohibit a much deeper dive and broader qualitative review from a more exhaustive resource pool. As Njie & Asimiran (2014) indicate, qualitative research "is not the approach to take if you are looking for quick results and easy answers." It involves enthusiasm and the determination to dig deep to understand a situation or process. It often needs a longer time and further inquiry to better understand a situation through observation, interviews, and follow-up sessions.

Furthermore, as Dolci et al. (2017) point out, Supply Chain Governance (SCG) is a topic that has been widely studied in recent years for analyzing inter-organizational relations as a multi-dimensional phenomenon embedded in the company's structures and processes. Studies analyzing all aspects of SCG at the same time, however, have not been found. Moreover, there are several performance indicators, but there is a lack of consensus on what determines the performance of these supply chains. The lack of studies inhibits existing research from drawing information and conclusions.

Finally, studies still need to understand the full impact of cybersecurity on Software Supply Chain performance and the impact of risk in SLTT's role in Cybersecurity governance.

Analysis and Discussion

This section analyzes the research findings from face-to-face one-hour interviews with ten participants over two weeks and selected case studies on SLTT Cybersecurity preparedness and governance. It begins with an overview of questions, themes identified, and participant responses, followed by an analysis of three case studies conducted between 2017 and 2019. The research compares and contrasts participant responses and critical elements identified in the case studies. Below represents the broad knowledge, expertise, and experience of the participants who lend their time to this study.

Table 4 Participants and Levels of Engagement

Participant	Level of Engagement
Participant One	Sr Mgr Product Development
Participant Two	SVP IT
Participant Three	Executive Partner
Participant Four	Principle PM Secure Software Supply Chain
Participant Five	CTO
Participant Six	Deputy Chief
Participant Seven	Former CISO
Participant Eight	CISO
Participant Nine	Software Engineer
Participant Ten	CTO/Co-Founder

Table 5 Interview Questions and Coding		
Question#	Question Code	Question
1	Q-BiggestCSC	What is your biggest Cybersecurity Concern
2	Q-VendorAccess	Do you have a complete inventory of vendors and third parties with access to data, the company utilized on a daily basis?
3	Q-SoftwareSecurity	How do you currently effectively assess software security, enabling an approved list (e.g., allowlist) of software and libraries on distributed systems across your organization effectively?
5	Q-ZeroTrust	Is current software security, especially around application security testing, sufficient from a scale and speed perspective to handle the move to zero-trust network architectures? Feelings toward Zero Trust Architecture
7	Q-SBOM	Software Bill of Materials or SBOM has risen to be an important building block in software security and supply chain risk management. Do you feel SBOMs are the solution and what do you think the future holds? E.g. the EO focuses on critical software, do you see this extending to all software
8	Q-CSCRankings	Please rank the following top five security concerns identified by the Nationwide Cybersecurity (NCSR) of state and local governments and explain your ranking; 1.) Lack of sufficient funding 2.) Increasing sophistication of threats 3.) Lack of documented processes 4.) Emerging technologies. 5.) Inadequate supply of security professionals
9	Q-SLTTreadiness	Do you feel state and local governments have kept pace with advancing threats and the rapidly expanding cyber infrastructures that need to be protected?
11	Q-911cyber	911 was a major wake-up to the nation in terms of threats and vulnerabilities. Do you feel State, Local, Territorial and Tribal organizations are prepared from a Governance perspective, should a significant Cyber attack occur simultaneously in locations across the U.S.?

DATA COLLECTION ANALYSIS

The data collection analysis began with **question 1**, - What are your biggest Cybersecurity concerns? According to the respondents, the main themes identified were a coordinated cyber attack by nation-states, the complexity of technology, and software, the limitation of resources, and human capital. As one respondent alluded,

> *what I'm worried about in the most scary scenario, it would be a powerful nation-state with those resources (kinetic conflict like warfare combined with cyber-attacks). When you coalesce those multiple attacks in different domains, it is of the biggest concern because those start to have exponential impact compared to something that could be isolated to a single domain and managed more effectively.*

And in terms of State, Local, Territory and Tribal Organizations (SLTTs), one CISO related the impact of limited resources is multifold leading to 1.) Purchase of software not reviewed for meeting standards as well security review, 2.) Unable to support with existing resources leads to elevated security risks 3.) Short term review of systems doesn't allow for proper security review, 4.) Software whether internal or vendor are frequently developed without appropriate security life cycle development tools, which means no security oversight 5.) Connected data bases are not properly configured with security in mind for data transfers, exchange, north/south

flows that utilize unsafe software, 6.) Unapproved software acquisition and deployment (including shadow IT).

And when it comes to human capital, 80% of respondents indicated that people are a major concern when it comes to cybersecurity; either due to the limited talent pool, knowledge, weakness due to human errors or as an adversary. As one senior executive lamented,

> *we have tightened the algorithm that has to be used for passwords but I still believe that phishing emails, spamming, spared phishing emails, all of this points to the weakest link, which is people, because they still click on a link and give their password and logins away, without doing their due diligence and any amount of awareness still is not sufficient. Awareness campaigns continue, but I still believe people remain our weakest link.*

Another executive also echoed this same sentiment, saying,

> *again, our products are really sound, when implemented properly, they're very effective. We actually have really good processes as well as government and private sector is working close together. And then, you know, really honing in on best practices which goes into those processes the big, biggest weakness we have happens to be people right, and so it has nothing to do. Well, of course, it has something to do with technology, but it really is a people issue or people challenge that we have to do a better job on like, everything from education, awareness, coordination, collaboration and communication.*

He added,

> *And you know the cliche of the weakest link holds true. Right? You know the adversary, in this case hostile adversary only has to find that weak link to be able to penetrate your system. And then all mitigation strategies, as it relates to supply chain will generally break down from there, because you know the weakest link just provided the biggest vulnerability. Therefore you know, the adversary has that opportunity. And again, that usually comes to a human era, right.*

In attempting to understand the risk associated with software supply chains and third party risk, **question 2** asked "Do you have a complete inventory of third parties and vendors assessing your data? Responses were mixed with only 20% of participants affirmatively acknowledging processes in place to identify vendors assessing their data. Participant 6 responded

> *Federal agencies they're supposed to, whether they do or not, I think we will know over the next year. DoD (Department of Defense) has been leading as they should. But ever since I've started in this area, DoD has been the lead, because their mission is so incredibly important, and they do have the resources. At least a couple of years ago, I believe, have started the process of trying to get an understanding of who all of their suppliers are.*

Participant 7 indicated,

> *that will vary state by state, but i'd say in general, it's probably safe to say that that a complete inventory is still a ways away. There's been*

great strides that have been made in that area, and there's certainly a greater recognition within government leadership of the risks of the connectivity with those third parties and vendors.

Echoing this point, Participant 5 commented,

so we don't have this for SLTTs and work towards this type of solution is important. One of the hurdles is the economic model. If you think about it, we're talking about a population with far fewer resources. And so how can they manage that complete inventory? That's intensive. If there were a third party that worked with SLTTs would that be government funded? But if you thought about this on a per MS-ISAC model, we get into trouble there because there isn't funding for every single MS-ISAC. Some ISAC's are funded from the community members, and if those community members don't have resources they would wind up in the same place. There's a lot of work and opportunity here, and I don't think anybody quite has that answer yet, but it's a good challenging problem to pursue.

In today's digital world, it has become more important than ever to have full knowledge of whose handling an organization's sensitive data. A large percentage of breaches have been attributed to third-party vendors.

With the release of Executive Order 14028 Improving the Nation's Cybersecurity in 2021 there has been a major focus on software supply chain. **Question 3,** asks How do you currently effectively assess software security, enabling an approved list (e.g., allowlist) of software and libraries

on distributed systems across their organization effectively? As noted, software security is an evolving arena, so responses were reflective of its infancy and noted areas of opportunities as well as cybersecurity concerns. Participant 2 commented,

> *I would not say that we have a blacklist or a white list approved list or a non-approved list that is global in nature. We have a list of approved or trusted vendors that we use through a firewall, disable access to downloading of certain vendors. So there is a vendor level download prohibition that takes place because it also impacts asset management, license usage and associated elements. Being a global enterprise there is always some risk that there is software being deployed which may not be the best in the world and for that we have a very strong software asset management team stood up over the last three years which proactively looks at software running in our endpoint devices and makes judgements based on the risk.*

Participant 7 remarked,

> *that's gonna to vary depending on the security maturity of the SLTT organization and some are at the point where they have an allow list, I wouldn't say a lot are there yet. Traditionally, they try to address software security through contracts or requirements. They put in their request for proposals when they're going to do a purchase. But again, that can be a challenge, because agencies will do their own contracts. You want to make sure that you're educating your um business leaders as well as your procurement people. The need to have security clauses*

> *in those contracts and request for proposals. I'd say plenty of organizations that aren't doing any of these things in terms of software security. And you know that's a little frightening.*

And to illustrate that point, Participant 8 indicated,

> *software security is really probably the lowest priority while agencies chase their tails from a security perspective. We all are wishing and hoping that our software vendors have taken the appropriate approach to insure security is properly baked into their software that we use. There are about 26 different 'businesses' in a County or City. Law, legal, public health, mental health, building, fire/ems, tax, financial, HR and many others all independently want to deploy software from vendors (perhaps develop in house) that will help their respective departments... where a 'bank' only has to worry about financial systems (and HR).*

And while Participant 4 has published a guide on this topic, Participant 6 indicated *DHS (Department of Homeland Security) binding operational directives require departments and agencies do what you're asking.* Perhaps there is overlap or synergy with both of these publications or at the minimum sharing of information could be beneficial.

And while **question 3** elicited similar responses, there were two very contrasting view points worth a mention. Participant 9 responded,

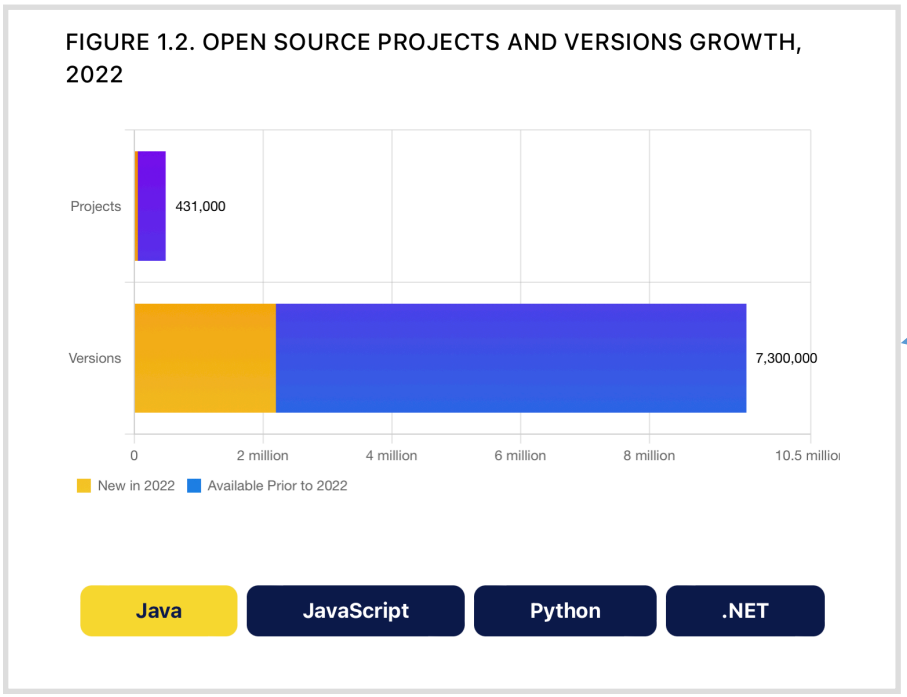
I only know open source, so I would go by the people generally building the software. Are they active? Is it maintained? Is it updated. I would also utilize some sort of scanner to check if there's known vulnerabilities. If its an open source project that is popular, you know more eyes are on that code, because we've open source the code readable to anybody. It's transparent. So generally a more popular project will have more people that are looking at the code working on the code, and we will discover vulnerabilities and so forth. If it's a proprietary code where if it is proprietary software where you do not have that insight into the code. Then I imagine it's a lot more difficult, really. So again, that's where I see open source as having a strong case for security really is that it's transparent. It's observable.

Participant 4 responded,

so developers use open source pervasively in software development today. So whether that's a docker container or they're pulling in like newgit or Npm or PyPi or whatever sort of open source packages and they're consuming it into their their software development workflow. Open source has seen a rise of 742% attacks specifically targeting open source over the last three years, on average.

FIGURE 1.1. SOFTWARE SUPPLY CHAIN STATISTICS, 2022

Ecosystem	Total Projects	Total Project Versions	2022 Annual Request Volume Estimate	YoY Project Growth	YoY Download Growth	Average Versions Released per Project
Java (Maven)	492k	9.5M	675B	14%	36%	19
JavaScript (npm)	2.06M	29M	2.1T [1]	9%	32%	14
Python (PyPI)	396K	3.7M	179B [2]	18%	41%	9
.NET (NuGet)	321K	4.7M	96B [3]	-5%	23%	15
Totals / Avgs	**3.3M**	**47M**	**3.1T**	**9%**	**33%**	**14**



Exponential growth in Open Source Software

Figure 2. Above Figures 1.1 and 1.2 per Sonatype 2022 8th Annual State of Software Supply Chain indicate continued growth in Open Source Software

"With more open source being consumed than ever before, attacks targeting the software supply chain have increased as well, both in frequency and complexity. This year's research revealed a 633% year over year increase in malicious attacks aimed at open source in public repositories–equating to a 742% average yearly increase in software supply chain attacks since 2019" (Sonatype, 2022)

To sum up the concern of assessing software security , Participant 10 commented, *So I wouldn't say that you know It's been happening effectively. I'm sure there that there are organizations that doing that right? It's really hard to enforce and keep track of everything*.

Highlighted in the Sonatype State of the Software Supply Chain Report was the statement,*"Organizations think they have their software supply chains under control, but the data disagrees - 68% of survey respondents were confident that their applications are not using known vulnerable libraries, but in a random sample of enterprise applications, 68% contained known vulnerabilities. One needs to look no further than SolarWinds and Log4J and the ensuing impact. It is evident given the responses, opportunities exist in effectively assessing software security.

Executive Order 14028 and the OMB guidance "Enhancing the Security of the Software Supply Chain to Deliver a Secure Government Experience" both take aim at software supply chain security and the significance of a software bill of material (SBOM). **Question 4,** asked since, Software Bill of Materials or SBOM has risen to be an important building block in software security and supply chain risk management. Do you feel SBOMs are the solution and what

do you think the future holds? E.g. the EO focuses on critical software, do you see this extending to all software? While the general consensus amongst respondents was the SBOM is an important tool participant responses offered a more nuanced viewpoint. As Participant 7 responded,

> *so I wouldn't say they're the solution. They're certainly an important tool to have in our security to box, I guess, but they're not going to be the panacea and security is all about layer defense right? No one thing is going to protect you against everything that we're facing.*

Participant 5 echoed this point of view.

> *I think, as some are only part of the solution, so they enable an ability to assess more easily, especially if there's an accreditation signature on a SBOM, right? But they don't necessarily solve the problem themselves. It's it's an essential building block. And now we have to do the right thing with that building block, we could go totally in the wrong direction and make it burdensome for every organization or we could make this more seamless. The ownness needs to be on the vendor because the vendor owns the responsible disclosure process. The responsible disclosure process is that if some researcher finds the vulnerability in software they notify the vendor with a reasonable amount of time.*

Participant 4 responded,

> you should want to have SBOMs for all of your software because that'll give you insight into your supply chain dependencies that you never

> knew you had before. So when Log4J happened, that was the wake up call that everybody needed to go like. Gosh, I don't even know if i'm affected when Log 4J happen, because nobody had SBOM for their stuff. And so the best thing about SBOM like as a consumer, you can answer the question, am I affected, and what is affected? So if you know what is affected, you can look at your network architecture and go, Ok, that application is deployed here. It's behind two firewalls, so the risk might be somewhat reduced. Maybe, I don't have to think that my hair is on fire, you know.

And there are tools to support the SBOM initiative which Participant 4 demonstrated and commented that *the SBOM is famously compared to the ingredients list on food packaging right? It just tells tells consumers about what's inside this piece of software at build time.*

However 30% of respondents offered a more nuanced response. Participant 10 remarked,

> *now there is the problem for software consumers. Now I i'm going to change my hat, you know and i'm going to put myself in the head of software consumer. And these guys, they don't produce software. They buy software, but now they need to receive a SBOM from multiple vendors. So know they're working with three hundred vendors. They need to get all of these SBOMs flying into them, and somehow keep them somewhere organized. And in the same way monitor vulnerabilities because they want to take their own fate in their own hands. The problem is not to generate and create them. The problem is to manage them at scale and also to extract value out of it, right? And values could be like three different things. I want to optimize my*

problems, I want to kind of create savings of money of for profit. I want to do things much faster and more efficient than I have done it before, which definitely you can.

Participant #6 elaborated even more so,

*Typically, I don't like the Government coming out with requirements on aspirational things, but it has been long recognized that there is a need for some sort of, what we have always called a component inventory. They kind of trademarked the whole software bill of materials thing. There's actually many ways to do component inventories. And we've long advocated for component inventories. **Part of the problem has always been is SBOMs or component inventories are not a new thing. They've been around for forty, fifty years, but more in the development side, and they're usually protected with nondisclosure agreements between the third parties.*

The more of the issue that we have now, I think, is bringing SBOMs into more of an end user Consumer area and then from a consumer perspective, the question always has to be asked, what is it useful for? Does it increase my security? Right? So if you give me a list of what those components are, what am I going to do with it. So I think it's more mature on the the issuing side which is going fast and strong on developing the formats, and the information that will be contained in the the standardized formats. But on the consumption side, I think that's a little bit again. More more aspirational. I do think it has a lot of potential depending on if we can actually consume it in an automated way, actually allows us to proactively use the information. So what I predict initially that we're going to be consuming SBOMs on a reactive

basis, and we're gonna be stacking those up in a repository of some sort and probably won't be using the information in there proactively until there is an incident, right?

Participant 6 offered more insight when indicating,

The National Cyber director has prioritized open source software and an initiative in line of effort one which is again "left of center" on looking how open source software is developed and trying to get it to be developed more securely. Part of this effort was co-chaired with NSF (National Science Foundation). They recently held workshop with output I think you would be interested in. There workshops are conducted very differently as NSF invites thirty, thirty-five specialists in a very narrow field to come in and talk. And so the fact that they had experts and open source software, different areas of it is pretty cool, and there is a discussion of SBOMs in there very briefly, and Cves and kind of what the contextualization, I think, and I don't want to miss quote somebody, but essentially, I think they said a SBOMs without contextualization is security theater and useless. But this is why I'm saying, I want you to go back and look at that workshop report to verify.

Upon verification, we found the following as reported in the Open-source Software Security Initiative (OSSI) Final Report - Recommendations from the Workshop on Open-source Software Security Initiative, "SBOM can be a key component of any solution, but the associated tooling for creating, manipulating, and generally integrating with development and management processes and workflows is currently viewed as immature. Anecdotally,

workshop attendees expressed the opinion that the majority of SBOMs are "worthless" or "security theater". What is needed is canonicalization of software names/references, and tools for managing/maintaining and checking the dependencies in an SBOM. At a minimum, software manifests should include transitive dependencies. Ideally, the SBOM functionality should be integrated into the build tools by default; a targeted R&D effort could yield great results in this space."

Zero Trust Architecture - NIST defines Zero Trust as an evolving set of cybersecurity paradigms that move defenses from static, network- based perimeters to focus on users, assets, and resources. A zero trust architecture (ZTA) uses zero trust principles to plan industrial and enterprise infrastructure and workflows. Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or based on asset ownership (enterprise or personally owned). Zero Trust continues to gain ground as a defense for software supply chain cybersecurity. **Question 6**, asked, "Is current software security, especially around application security testing, sufficient from a scale and speed perspective to handle the move to zero-trust network architectures?" There was a general consensus as to the

move towards Zero Trust Architecture as a positive one, though with varying viewpoints. Participant 5 responded,

> *So I think in the next few years we're going to see great change, and it will trickle through from the vendors where they will have better management options, so as you acquire new software we will start to see some change. Will it be dramatic, I don't know yet. I think that's too hard to tell. But I think we will see initial improvements. And we've seen some pretty cool things like the Okta attack, while not ideal, they caught it within twenty-five minutes because they have zero trust implemented. Vendors like Akamai have zero trust on their infrastructure. Google has your trust on their infrastructure. So the big players have been able to do this. I think the hurdle will be if the vendors producing zero trust products, if they are producing them with the architectural patterns that we've used for ever. Where we expect lots of the individual organization, then this is just not going to work. But if we see the vendors built it in more because of things like the Solar Winds attack and the impact and the realization that we have to do better in terms of scale, then it will just start to happen with infrastructure, refresh cycles, and move to cloud environment.*

Participant 7 echo similar sentiments,

> *So are they moving towards Zero Trust, I'd say Yes, absolutely. Are they moving at the scale and speed that we need them to. Probably not. I mean, there's just still far too many vulnerabilities in in our software and applications as a whole. And those vulnerabilities are constantly increasing. But we really need people to adopt more of the basics of*

cybersecurity, inventory in your systems, hardening your systems, limiting administrative rights just to get them prepared to move to Zero Trust.

Participant 6 expressed a somewhat contrasting viewpoint, similarly echoed by 30% of participants.

At the moment I think Zero trust architecture is still in the aspirational stages, "At the moment I think Zero trust architecture is still in the aspirational stages. And so in some instances it could be a little bit of pulling the cart before the horse. It is good principally, but in actuality, I would just highly recommend talking to sophisticated organizations that are trying to implement zero Trust and see the challenges that they're having. I have read some critiques of Zero Trust and one of the the biggest kinks I think in the Zero Trust armor is the supply chain piece, and it's the technology that is being utilized in any zero trust environment. And as we all know there's no such thing as a one hundred percent security, and there's no such thing as is a technology without vulnerabilities, and that's just the way that's the life we're living. So there's always going to be vulnerabilities even in a Zero Trust, that the name Zero Trust, unfortunately, that's the name that uh was given to it. But it's It's kind of a misnomer. because I don't think there will ever be you know Zero Trust, I mean, is it? There's always going to be risk.

With continuously rapidly expanding technology and the widening of attack surfaces due to the growing use of devices and associated software,

question seven asked, Do you feel state and local governments have kept pace with advancing threats and the rapidly expanding cyber infrastructures that need to be protected? According to 60% of respondents, the answer was no.

> *Laughter, I think we fell behind in the last twenty years. From what I see today I think we are keeping that gap. We're not necessarily allowing the gap to open, we're maybe closing it, but there is a gap. It's like the Federal government is paving the way and the state governments are applying the effort to keep up and the local governments are kinda just hanging on. I haven't observed any significant enough closure to those gaps, industrial controllers and data vulnerabilities for example and that's a concern.*
>
> *No, we're, we're always a phase behind what's going on. We're doing the best we can. What's really helping is our collaboration with other agencies, and with MS-ISAC to kind of stay slightly ahead of zero day exploits and things like that that pop up that we can put defenses in as soon as we possibly can, or update our patching schedule for certain applications and things like that. But no, I don't think we have kept pace.*
>
> *Yeah, no, laughter, I can stop you right there. You biggest strength is generally your biggest weakness. We have fifty States and six Territories right? Each has the autonomy to govern themselves, and that's in our Constitution. It should be that way. Right, States are the laboratories of democracy. We have a a great deal of innovation*

happening at the States that generally bubbles up to the Federal level right? As someone said today, States created the Federal Government not the other way around right Federal Government didn't create States? And so the States they do a lot of great things. That's the blessing. The curse is that they're different, Right? So the blessing is that you know the weaknesses. The strength is that they're all different. You've seen one State. You've seen one state right. You've seen California. Well, you can't compare California to Michigan or Nebraska or Texas, because California alone is the six largest economy in the world. Right like California would be, could be a country in itself, and be top ten. But you can't compare that to Delaware, one of our smallest states. When it comes to your question, the reason I stopped you, you know. Have they kept pace? Again, it goes back to the question of well, what state are we talking about? And who's leading that state at the time?

Does this not elicit commentary on the role of governance and leadership within an organization? Additional responses provided varied viewpoints on SLTT keeping pace as well as some of the root causes inhibiting progress in this important preventive measure

Well, they've shown improvements year over year with the NCSR, results right? And so I mean nobody's keeping pace necessarily with the advancing threats. The industry as a whole, we've gotten a lot better in the last decade, where detections of attacks were at two and a half years for dwell time, and now they're a lot smaller, depending on the attack. Right? For a SLTT, It might be a longer time before detection, although they're getting hit with ransomware, so detection

of ransomware is quick. But the problem with it is that their systems are already locked up, and you know, by the time they're notified. So, even though it might be a short dwell time, they already have the full impact of the attack. So you know. There they're not keeping pace, I think, with the advancing threats right because they are getting hit. I do think we have to push this back to the vendors because we just can't expect the SLTTs to do it.

It's really really hard in the small world of under resource governments, you know, maybe not so much in the States. But again, you know, as I mentioned some of the smaller accounting cities, libraries, those kinds of things where you have, maybe the school bus drivers is also the person responsible on the side for cyber security, and it you know the the person in charge of city public works also has that on their plates, so they're not necessarily IT Cyber Professionals, but it's been added to the expectations of them, and that makes it very, very challenging for them.

Though there was general consensus that the Federal government has made considerable progress.

I believe the Federal Government has done a good job in publishing standards as well as creating communities of large corporations to keep us updated on the landscape. We are part of some of these consortiums, forums, meetings that take place. I have personally visited leadership at NSA and in the previous administration in the White House, so I know the right level of Federal leadership exist. So

my point is that the Federal Government has done a very good job. Can they do more absolutely?

With the alarming rise of cyber attacks, many in the cybersecurity community are asking is cybersecurity still an afterthought? To put this into context, one of the last questions evoked a great deal of conversation as well as reflection. **Question 8** referenced 911 as a major wake-up to the nation in terms of threats and vulnerabilities. Do you feel State, Local, Territorial and Tribal organizations are prepared from a Governance perspective, should a significant Cyber attack occur simultaneously in locations across the U.S. Fifty percent of respondents indicated "no," they did not feel we were prepared. Though all respondents indicated it as a challenging question to answer and offered reflective responses such as,

Yeah, there's couple of areas that i'm concerned about, one area is specific to the public sector, and our ability to react quick enough and get feedback from other agencies as well as MS-ISAC staying on top of things to notify us.

There answer is no. I mean we've just seen that, Colonial Pipelines, you know you don't need to go far, like the example is right here, and I think, like the funny thing is that the executive order. I think that's kind of what you know the straw that broke the camel's back. But when Colonial Pipeline happened, that was like, Okay, that was like the straw. I'm absolutely sure, we're not prepared.

I'd say No, but we're making progress. I think 911 certainly showed us the interdependencies of a cyber attack and a physical attack, and it did so improve some of the planning and governance across the nation, but I think there's more to do. That event was actually the impetus for the the start of MS-ISAC, as the State Cisco's realized that, Hey, we need to do better at information sharing and making each other aware of the threats that are happening, because you know, they're not geographic, right? What's happening in one area can easily happening in another. It certainly increased the planning, but I think there's more to do there. I don't think every state has a cyber security annex to their Homeland Security plan. But I know a number have, and the number of working towards that. And then, you know, testing those plans on a regular basis is important. It's not enough to just have them. You need to test them regularly. And then we need to start considering, and I think we are starting to consider the larger scale significant attacks, and how the governments across the nation are going to be responding in time.

And to bring this full circle to current events, the following response was offered,

I think about what we are seeing in Ukraine. Ukraine was a lot more prepared than lot of countries I know. They had their entire electrical, water and gas network has been knocked off due to a cyber attack. We have seen similar effect in the U.S., where attacks were made to Colonial gas pipeline, not too long ago. Some of the local governments have been impacted by it. So I would say that there are definitely pockets in the Federal, State, and local level that have the capabilities to react, but it will be like Swiss cheese. There will be gaps.

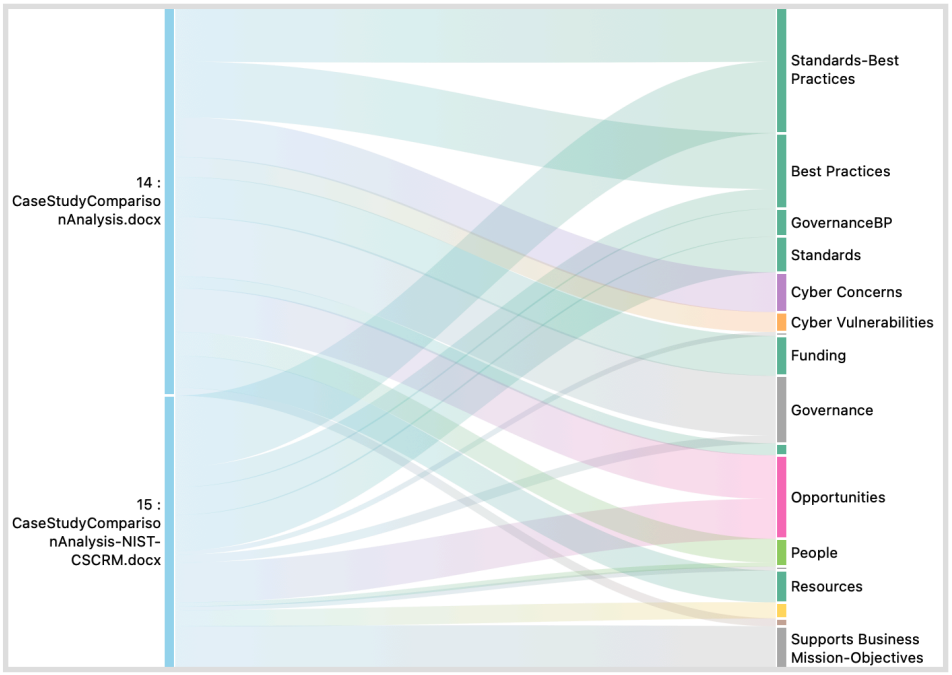


Figure 3. Color coded Common occurrences identified across all case studies

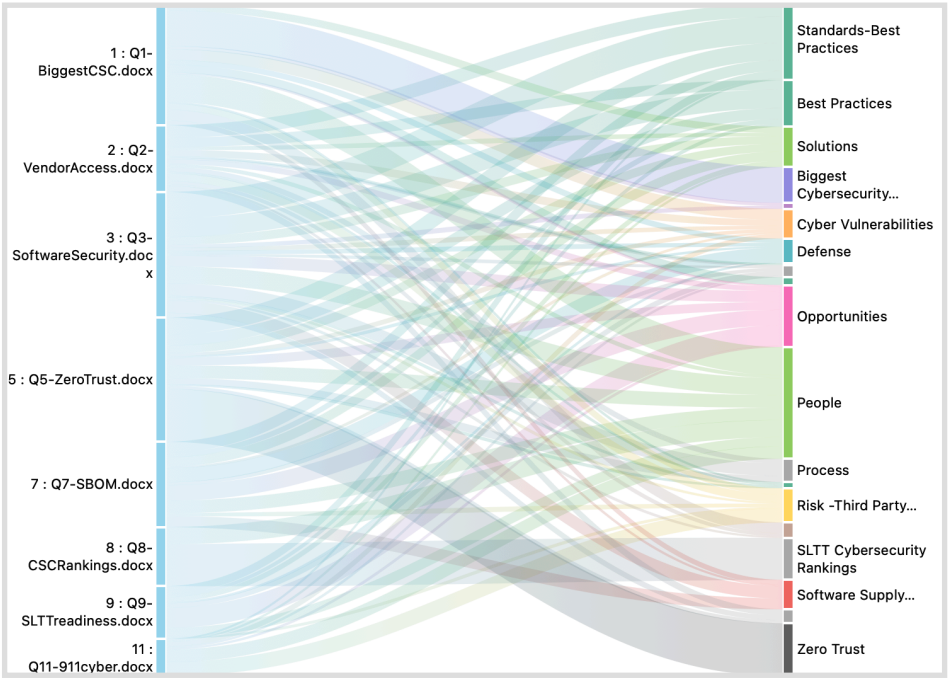


Figure 4. Color coded Common occurrences identified across selected interview questions

Case Studies and Interview Questions Common Occurrences Comparison

Case Studies

The following three case studies were selected for comparison analysis as well as how they aligned with the qualitative interviews.

Table 6 Case Studies Analyzed

Year	Case Study
2017	SCGCS - State Cybersecurity Governance Case Studies - DHS - NASCIO (Department of Homeland Security and the National Association of State Chief Information Officers
2018	DNCS - Deloitte-NASCIO Cybersecurity Study - 2018
2021	NCSR - Nationwide Cybersecurity Review -Multi-State Information Sharing and Analysis Center (MS-ISAC®) and Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC®)
2020	National Institute of Standards and Technology Case Studies in Cyber Supply Chain Risk Management

Top cybersecurity concerns identified in all three case studies have been consistent and continuous throughout from 2017 through 2021 and can be consolidated under the below main categories:

1. Governance
2. Resources
    a) Funding
    b) People
3. Information Sharing
4. High percentage of cyber incidents
5. Compliance with established Cybersecurity Frameworks and basic cyber hygiene

While considerable progress has been made, there still exists tremendous opportunities for improving overall cybersecurity risk management. As reported in the Nationwide Cybersecurity Review, SLTTs reported key security concerns that they face. The top five reported concerns remained the same for the fifth consecutive year:

- Lacking of sufficient funding, increasing sophistication of threats
- Increasing sophistication of threats
- Emerging technologies
- Lack of documented processes
- Inadequate availability of cybersecurity professionals

The above cybersecurity concerns were listed in **question 7** - Please rank the following top five security concerns identified by the Nationwide Cybersecurity (NCSR) of state and local governments and explain your ranking;

1. Lack of sufficient funding
2. Increasing sophistication of threats
3. Lack of documented processes
4. Emerging technologies.
5. Inadequate supply of security professionals

According to the respondents, all agreed with the concerns as listed and while all provided varying viewpoints in their responses, 100% of responses elaborated on the challenges of limited or insufficient resources (funding and people) —

> *So you know it's It's something we take every year. I do agree with them. I think I would probably put them in a little bit of a different order to me. I think the inadequate supply of security professionals is number one, because without this, without professionals, the other issues are going to be hard to address. It always starts with the people right? Lots of sufficient funding is number two. There's so many governments out there that don't even have the basics, and that are severely disadvantaged, and that are in desperate need of funding.*
>
> *I am actually on the committee. I'm actually the co-chair of the committee that developed the NCSR. And it's a report back to Congress and all that. But I would, I would say, here's how I would measure it. #1 Lack of funding is number One, #2 inadequate supply or ability for us to hire more security professionals, #3 increasing sophistication of threats, four, and five essentially in that order, three being increasing sophistication of threats, four lack of documented processes and five, emerging technologies. But our inability to either hire security professionals which we have a hiring challenge out there, and we're not getting the appropriate people that are applying for the jobs, we're not paying enough to bring in the appropriate people that are uh to to apply for the jobs. We really have a serious lack of security*

professionals within our organization. And I hear that's pretty much across the country.

So I think that they kind of all quite connected right, because lack of sufficient funding will probably bring you inadequate supply of security professionals, right?" "These are definitely the top five concerns. I wouldn't address them in this order, and I wouldn't right now because of how we design things. Yes, we have an inadequate supply of security professionals. I don't think the answer is just to solve. That is explicitly. As stated, I think we have to change how we deliver and deploy emerging technologies and current technologies. We have to push more to the vendor, and that will reduce the number of security professionals needed to serve in these functions. It will also help with the increasing sophistication of threat actors, because we will have more secure products by default, and if we are able to have them manage securely over time. That will also increase the cost for those sophisticated threat actors and have them target their threats more directly instead of the broad based attacks that they're having right now. I would not address them as individual items, because I think you don't get to the correct result in that way, right? If you just throw more funding at it.

So there's caveats with all of them right? I mean, for example, sufficient funding, in general resources, which would be, (1) and (5) are all dependent right? So that is an issue. But even if you give them that, and they don't have good processes. So it's not a lack of documented processes. It's a lack of good processes. I would put #2 last, because again you can't control the threat. And you actually want technologies

that emerge, right, or we're going to be on a horse and buggy, laughter. We talked about It's not the fact that there are emerging technologies. It's the more the fact that there's a lack of understanding of the impact on those emerging technologies which has a lot to do with the resources and getting the right professionals, right? So if they're all linked together, that's a tough one.

And a resounding theme of "people" being a major cybersecurity concern jumps right off the page illustrated by the last response,

but these things are the glue that really makes it go right. I mean as a colleague said, it's like baking a cake. Everyone wants to talk about the icing. No one wants to talk about the little things in it. Yeah, who talks about the butter or anything else that holds it together. But these are the things that really need to be focused on, NASCIO, itself. Arguments can be made for all of them, so i'm putting all on the same level right now. But again, look at it. three out of there top five, nothing to do with technology. And that's where (people) I think you need to really take a strong look at.

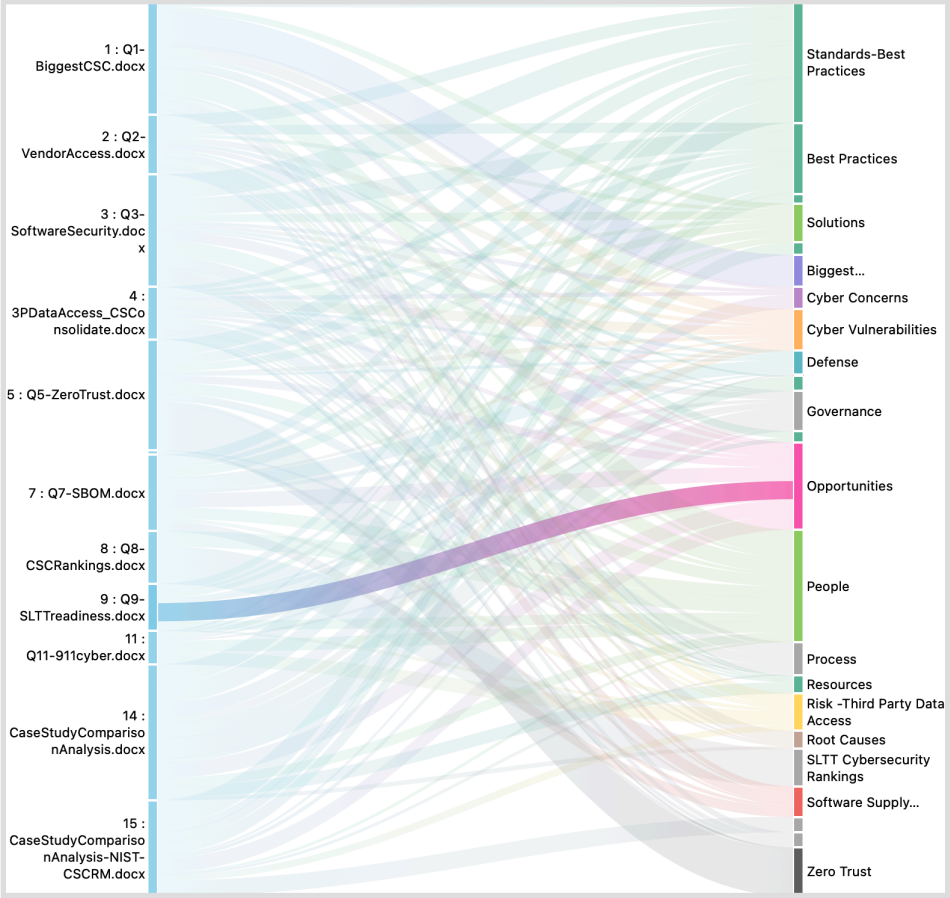


Figure 5. Color coded Common occurrences identified across case studies and interview questions

Figure 6. Case Studies Common Themes

Figure 7. Interviews Common Themes

DISCUSSION

The data analysis reveals multiple long term gaps and cybersecurity risks that left unchecked can have an insurmountable negative impact on the nation at large should a large cyber attack occur. From, insufficient funding, gaps in processes, governance issues, identified vulnerabilities, information sharing, communications, coordination and a multitude of cyber concerns. Yet, at the same time there are a multitude of best practices, standards and solutions being utilized that if more broadly known could support the Nation's efforts defenses against cyber attacks.

That 64% of respondents in the NCSR Case Study reported experiencing a cyber incident in the past year and the the five key security concerns remain unchanged over the last five years, indicate the need for change.

Based on the research conducted, two areas which became prominent were governance and the need to architect security so it scales. Governance is responsible for resources, whether its human capital or software. A continued focus on design and development of security architecture can be beneficial in the many shortfalls in human capital which will only continue to grow without new and bold initiatives.

The tables below provides preliminary observations and recommendations for discussion and further review and analysis:

Table 7 Observations and Recommendations

Category	Recommendation
1. Governance	a) Concerns referencing resources, human capital and funding limitations were a reoccurring theme throughout all interviews. How are organizations determine cyber budgets, addressing shortfalls, benchmarking with peers or evaluating current organizational cybersecurity posture. b) Leadership is the cornerstone every organization. Review of best practices for organization governance provided under key established guidances. NIST, ISO, and MS-ISAC were most mentioned by participants. Identify standards per organization maturity and share. Are there other standards beneficial to governance that could be utilized, e.g. COBIT c) Formation of formal Cybersecurity Partnerships with Government, Private Sector and select Non-Profits (modeled from new AUKUS security partnership)

1. Governance	d) Re-evaluation of the CISO role. The CISO role is deemed an important function in organizations for raising awareness and implementing solutions to mitigate cyber risk. But without adequate funding and resources, has it become more of a bandaid for prevention? Every organization needs someone responsible for technology and appropriate resources for managing risk or security regardless of what that title is. Can this be a shared responsibility across SLTT organizations with the right resources allocated? e) Ensure Supply Chain Cybersecurity strategies align to an organization's core mission and objectives. It was vaguely mentioned in most conversations outside of the two multinational companies and the one NIST CSCRM study f) Build economic models for helping to determine R.O.I. as well as better metrics to evaluate reliability, sustainability and cybersecurity risks. 1. In mature organizations, cybersecurity funding is allocated as the cost of doing business. Economic models would lend support to this model as well as aid less mature organizations g) How is governance measured and communicated within an organization? What are key metrics to determine success or failure rates. Include Metric attributes to an organization's scorecard tied to accountability, performance reviews and compensation if it does not already exist.

1. Governance	h) How are the obstacles to using Cybersecurity Frameworks being addressed? In 2017 per Bitchkei, S. (2017) 95 percent of organizations said they face significant challenges in trying to implement cybersecurity frameworks, according to a survey of 319 IT security decision makers by Dimensional Research on behalf of CIS and Tenable Network Security. [NIST, ISO, CIS CSF] i) Cybersecurity contains a broad area of skillsets. Identify key skills based on position, org type (e.g. stand alone SOC) and organization maturity level. Establish key processes, standards and measurements of performance. Engagement and collaboration with functional groups can a tremendous value add, e.g. H.R., Training, Marketing, Finance
2. Labor Pool (Human Capital)	a) Inclusion and Diversity. Collaborate with human resources and marketing to design demographically targeted recruiting and AD campaigns. Expand outreach to marginalized communities and other educational institutions such as community colleges, trade schools and high schools. b) Raise the profile and prestige of working in the Cybersecurity arena, akin to the military attributes in supporting the Nation. Identify or establish key benefits in addition to compensation. Evaluate compensation tiers to current private sector market rates
3. Technology / Security Architecture	a) Design and development of architect security so it scales to optimize security and minimize risks

4. 911 Model Cyber Attack	a) Overall the U.S at large is not prepared should a major cyber attack occur. SLTTs readiness paint a mosaic picture of strengths and weaknesses that overall could put the communities they serve at risk. What is the National plan for cybersecurity risk management and how is it being communicated to both government agencies and the private sector?

The following are additional research areas identified which would enable a deeper dive into many of the opportunities presented in this study as well as provide a path forward in helping to design and develop new and bold ideas to support the pressing need for improving software supply chain cybersecurity.

Table 8 Additional Research Areas

Human Capital Constraints	Cybersecurity Economic Modeling
Evaluation of CSF and Organizational Maturity Levels	Cybersecurity Risk Management Measurements and Metrics
Business and IT/Cybersecurity Alignment	Impact of growth of Open Source Software
Recruitment Cybersecurity National Education and Awareness Campaign	Benchmarks from NIST-NASCIO Case Studies
Cybersecurity impact of emerging technologies, e.g. Quantum computing	Software Supply Chain Third Party Risks
Benchmarks from NIST Secure Software Development Framework (SSDF) - NIST SP 800-218	Adoption of a Formal Audit and Compliance Certification Program

Conclusion

The awareness and importance of software supply chain cybersecurity are only beginning to receive the attention it desperately needs. In reality, businesses and consumers pay little attention to the need for a secure and trusted software supply chain to deliver the products and services they have come to depend on every day. Moreover, incremental progress is only beginning in developing workable solutions to prevent and mitigate vulnerabilities and risks inherent in today's software supply chain used by the private sector, government agencies, and the communities they support.

Many SLTT and business organizations have yet to fully understand the implication of the expansive growth of IoT devices and the inherent need to protect against threats and vulnerabilities in their software supply chains. Moreover, while Cybersecurity is not new, starting in the 1990s, its importance to software supply chains has grown with the explosion of computers, networks, and how we work, play, and live; its importance can not be understated. Any sustainable Cybersecurity solution combines people, processes, culture, and technology.

Multiple applaudable efforts are underway in various vectors to improve software supply chain Cybersecurity. Unfortunately, many silos and barriers exist to formulating a more holistic approach to Cybersecurity that would strengthen efforts at preventing and mitigating the continued growth of vulnerabilities and threats that will most likely always exist in software supply chains. Furthermore, while the rapid expansion of technology will continue unabated, what can we learn from the past to serve us better now and in the future? After all, as the saying goes, "all new ideas are only old ideas repackaged?”

“Cybersecurity is a team sport”

References

Bailey, T., Greis, J., Watters, M., & Welle, J. (2022, September 19). Software bill of materials: Managing software cybersecurity risks. Retrieved October 15, 2022, from mckinsey.com website: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/software-bill-of-materials-managing-software-cybersecurity-risks

Carter, S. D. (2020, July 2). Hackers Putting Global Supply Chain at Risk. Www.nationaldefensemagazine.org. https://www.nationaldefensemagazine.org/articles/2020/7/2/hackers-putting-global-supply-chain-at-risk

cis. (2022). Cybersecurity Spotlight - Hardware, Software, and Firmware. Center for Internet Security. https://www.cisecurity.org/insights/spotlight/cybersecurity-spotlight-hardware-software-and-firmware

CISA. (2019). Critical Infrastructure Sectors | CISA. Cisa.gov. https://www.cisa.gov/critical-infrastructure-sectors

CISA. (2017, October). Cybersecurity Governance | CISA. Www.cisa.gov. https://www.cisa.gov/cybersecurity-governance

CISA. (2022, October 3). CISA Issues Binding Operational Directive 23-01: Improving Asset Visibility and Vulnerability Detection on Federal Networks | CISA. Www.cisa.gov. https://www.cisa.gov/uscert/ncas/current-activity/2022/10/03/cisa-issues-binding-operational-directive-23-01-improving-asset

CSCC Labs, & NIST. (2022). NIST security vulnerability trends in 2021 Report from CSCC labs. NIST NVD. https://cscclabs.com/reports/NVD_vulnerabilityTrends.pdf

Chukwuemeka, E. S. (2022, August 31). Limitations and Weaknesses Of Qualitative Research. Bscholarly. https://bscholarly.com/limitations-and-weaknesses-of-qualitative-research/

Crossman, A. (2020, February 2). What Is Qualitative Research? ThoughtCo. https://www.thoughtco.com/qualitative-research-methods-3026555

Deloitte-NASCIO. (2018). 2018 Deloitte-NASCIO Cybersecurity Study: States at Risk: Bold Plays for Change – Press release. Deloitte United States. https://www2.deloitte.com/us/en/pages/about-deloitte/articles/press-releases/2018-deloitte-nascio-cybersecurity-study-states-at-risk-bold-plays-for-change.html

DeRusha, C. (2022, September 14). Enhancing the Security of the Software Supply Chain to Deliver a Secure Government Experience. The White House. https://www.whitehouse.gov/omb/briefing-room/2022/09/14/enhancing-the-security-of-the-software-supply-chain-to-deliver-a-secure-government-experience/

Dolci, P. C., Maçada, A. C. G., & Paiva, E. L. (2017). Models for understanding the influence of Supply Chain Governance on Supply Chain Performance. Supply Chain Management: An International Journal, 22(5), 424–441. https://doi.org/10.1108/scm-07-2016-0260

ESF. (2022). DEVELOPERS RECOMMENDED PRACTICES GUIDE FOR SECURING THE SOFTWARE SUPPLY CHAIN 1 Enduring Security Framework. In cisa.gov. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/uscert/sites/default/files/publications/ESF_SECURING_THE_SOFTWARE_SUPPLY_CHAIN_DEVELOPERS.PDF

Fujs, D., Mihelič, A., & Vrhovec, S. L. R. (2019). The power of interpretation; Qualitative methods in cybersecurity research. Proceedings of the 14th International Conference on Availability, Reliability and Security. ACM Digital Library. https://doi.org/10.1145/3339252.3341479

Gilligan, J. M. (2017, September 19). The Government Role in Improving Cyber Security. GCA | Global Cyber Alliance | Working to Eradicate Cyber Risk; Global Cyber Alliance. https://www.globalcyberalliance.org/the-government-role-in-improving-cyber-security/

Gomez, A. (2022, August 25). History and Evolution of the Global Supply Chain. AJG Transport. https://www.ajgtransport.com/ajg-blog/2022/8/25/history-and-evolution-of-the-global-supply-chain

Hasan, M. (2022, May 18). State of IoT 2021: Number of Connected IoT Devices Growing 9% to 12.3 Billion globally, Cellular IoT Now Surpassing 2 Billion. IoT Analytics. https://iot-analytics.com/number-connected-iot-devices/

Herr, T., Loomis, W., Scott, S., & Lee, J. (2020, July 27). Breaking trust: Shades of crisis across an insecure software supply chain. Atlantic Council; Atlantic Council. https://www.atlanticcouncil.org/in-depth-research-reports/report/breaking-trust-shades-of-crisis-across-an-insecure-software-supply-chain/

Hippold, S. (2022, April 20). How Supply Chain Technology Will Evolve in the Future. Gartner. https://www.gartner.com/smarterwithgartner/gartner-predicts-the-future-of-supply-chain-technology

Köhler, T., Smith, A., & Bhakoo, V. (2021). Templates in Qualitative Research Methods: Origins, Limitations, and New Directions. Organizational Research Methods, 25(2), 109442812110607. https://doi.org/10.1177/10944281211060710

Korolov, M. (2020, October 29). What is a supply chain attack? Why to be wary of third-party providers. CSO Online. https://www.csoonline.com/article/3191947/supply-chain-attacks-show-why-you-should-be-wary-of-third-party-providers.html

MacCarthy, B. L., Blome, C., Olhager, J., Srai, J. S., & Zhao, X. (2016). Supply chain evolution – theory, concepts and science. International Journal of Operations & Production Management, 36(12), 1696–1718. https://doi.org/10.1108/ijopm-02-2016-0080

Marinagi, C., Trivellas, P., & Sakas, D. P. (2014). The Impact of Information Technology on the Development of Supply Chain Competitive Advantage. Procedia - Social and Behavioral Sciences, 147, 586–591. Science Direct. https://doi.org/10.1016/j.sbspro.2014.07.161

Moriarty, K. (2022). Software Assurance: Approaching Allowlisting for Code. Center for Internet Security; CIS. https://www.cisecurity.org/insights/blog/software-assurance-approaching-allowlisting-for-code

NCSC. (2021). Software Supply Chain Attacks. In The National Counterintelligence and Security Center. Office of the Director National Intelligence. https://www.dni.gov/files/NCSC/documents/supplychain/Software_Supply_Chain_Attacks.pdf

Njie, B., & Asimiran, S. (2014). Case Study as a Choice in Qualitative Methodology. IOSR Journal of Research & Method in Education (IOSRJRME), 4(3), 35–40. https://doi.org/10.9790/7388-04313540

NIST. (2021). Software Supply Chain Security Guidance. NIST. https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/software-supply-chain-security-guidance

nitrd. (2019). FEDERAL CYBERSECURITY RESEARCH AND DEVELOPMENT STRATEGIC PLAN. The Networking and Information Technology Research and Development (NITRD) Program. https://www.nitrd.gov/cybersecurity/

OMB. (2022, March 7). OMB Statement on "Enhancing The Security Of Federally Procured Software." Retrieved October 7, 2022, from The White House website: https://www.whitehouse.gov/omb/briefing-room/2022/03/07/omb-statement-on-enhancing-the-security-of-federally-procured-software/

Pope, J. A. (James A. (2012). Supply-chain survival in the age of globalization (1st ed.). Business Expert Press. https://doi.org/10.4128/9781606491645

Pressman, R. S. (2005). _Software engineering : a practitioner's approach_. Mcgraw-Hill

REVERSINGLABS. (2022, December). The State of Software Supply Chain Security. ReversingLabs. https://www.reversinglabs.com/the-state-of-software-supply-chain-security

Rose, S. W., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture. Www.nist.gov. https://www.nist.gov/publications/zero-trust-architecture

Sherman, R. J. (2012). Supply chain transformation practical roadmap to best practice results (1st edition). John Wiley & Sons

Sileyew, K. J. (2019). Research Design and Methodology. Text Mining - Analysis, Programming and Application [Working Title], 1–12. Intechopen. https://doi.org/10.5772/intechopen.85731

Sonatype. (2022). 8th Annual State of Software Supply Chain. Www.sonatype.com. https://www.sonatype.com/state-of-the-software-supply-chain/open-source-supply-demand-security

Sobb, T., Turnbull, B., & Moustafa, N. (2020). Supply Chain 4.0: A Survey of Cyber Security Challenges, Solutions and Future Directions. Electronics, 9(11), 1864. https://doi.org/10.3390/electronics9111864

Statswork. (2021, May 18). Qualitative Data Collection Techniques for Persona Development– Recent Insights. Statswork. https://statswork.com/blog/qualitative-data-collection-techniques-for-persona-development-recent-insights/

The White House. (2016, February 9). National Challenges and Goals for Cybersecurity Science and Technology. Whitehouse.gov. https://obamawhitehouse.archives.gov/blog/2016/02/08/national-challenges-and-goals-cybersecurity-science-and-technology

The White House. (2021, May 12). Executive order on improving the nation's cybersecurity. The White House. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

The White House. (2021, May 12). Executive order on improving the nation's cybersecurity. The White House. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

USHOR. (2019). Testimony of Thomas Duffy Senior VP of Operations and Security Services & Chair of the MS-ISAC Center for Internet Security Hearing on Cybersecurity Challenges for State and Local governments: Assessing How the Federal Government Can Help Subcommittee on Cybersecurity, Infrastructure Protection and Innovation of the House Committee on Homeland Security. In homeland.house.gov. House

Committee on Homeland Security. https://homeland.house.gov/imo/media/doc/Tetsimony-Duffy.pdf

Wolf, B., Mahoney, F., Leena Lohiniva, A., & Corkum, M. (2019). Collecting and Analyzing Qualitative Data. CDC. https://www.cdc.gov/eis/field-epi-manual/chapters/Qualitative-Data.html

Woods, B., & Bochman, A. (2018, May 30). Supply chain in the software era. Atlantic Council. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/supply-chain-in-the-software-era/

Young, S. (2022). EXECUTIVE OFFICE OF THE PRESIDENT OFFICE OF MANAGEMENT AND BUDGET M-22-18 MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES FROM. Office of Management and Budget. https://www.whitehouse.gov/wp-content/uploads/2022/09/M-22-18.pdf

Zhu, Z., Lan, K., Rao, Z., & Zhang, Y. (2021). Risk assessment method for IoT software supply chain vulnerabilities. Journal of Physics: Conference Series, 1732(1), 012051. https://doi.org/10.1088/1742-6596/1732/1/012051

Appendix

Below are all questions used during interviews conducted but numbering may differ from the numerical color coding assigned used in the data analysis software:

1. What is your biggest Cybersecurity Concern? In Software Supply Chain?

2. Do you have a complete inventory of vendors and third parties with access to data, the company utilized on a daily basis?

3. How do you currently effectively assess software security, enabling an approved list (e.g., allowlist) of software and libraries on distributed systems across your organization effectively?

4. Do you have a complete inventory of third parties and vendors assessing your data? What do you see as the biggest vulnerability or threat in software supply chain?

5. Is current software security, especially around application security testing, sufficient from a scale and speed perspective to handle the move to zero-trust network architectures? Feelings toward Zero Trust Architecture?

6. Software Bill of Materials or SBOM has risen to be an important building block in software security and supply chain risk management. Do you feel SBOMs are the solution and what do you think the future holds? E.g. the EO focuses on critical software, do you see this extending to all software

7. Please rank the following top five security concerns identified by the Nationwide Cybersecurity (NCSR) of state and local governments and explain your ranking;

1.) Lack of sufficient funding 2.) Increasing sophistication of threats 3.) Lack of documented processes 4.) Emerging technologies. 5.) Inadequate supply of security professionals

8. Do you feel state and local governments have kept pace with advancing threats and the rapidly expanding cyber infrastructures that need to be protected?

9. What do you think are the minimal testing requirements for an organizations software supply chain?

10. 911 was a major wake-up to the nation in terms of threats and vulnerabilities, do you feel State, Local, Territorial and Tribal organizations are prepared from a Governance perspective, should a significant Cyber attack occur simultaneously in locations across the U.S.?