Unraveling Incentives: Understanding the Adoption Barriers of SBOM in the Software Supply Chain

Obtaining novel insights into how a current misalignment of (dis)incentives among business stakeholders in the software supply chain can explain the limited adoption of SBOM.

Master Thesis

Berend Kloeg

NORTHWAVE
CYBER SECURITY

TU Delft

Unraveling Incentives: Understanding the Adoption Barriers of SBOM in the Software Supply Chain

Obtaining novel insights into how a current misalignment of (dis)incentives among business stakeholders in the software supply chain can explain the limited adoption of SBOM.

by

Berend Kloeg

Student Name	Student Number
Berend Kloeg	4700171

First Supervisor (TU Delft):	Yury Zhauniarovich
Second Supervisor (TU Delft):	Aaron Ding
Chair (TU Delft):	Michel van Eeten
Supervisor (Northwave Cyber Security):	Sjoerd Pellegrom
Project Duration:	February 2023 - August 2023
Faculty:	Technology, Policy and Management, Delft

TU Delft

Executive Summary

In today's business landscape, virtually all companies operate as some form of software companies. Development cycles are increasingly accelerated to keep up with the demand for rapid innovation. As a result, software is increasingly built by incorporating numerous third-party software components, resulting in applications and systems consisting of a lot of dependencies. However, the lack of visibility and transparency within this complex web of dependencies poses significant challenges. It creates a breeding ground for security issues, with the main concern being the potential for vulnerabilities to lurk throughout the entire software supply chain (SSC), spreading widely without detection. To address these challenges and enhance transparency in the SSC, the concept of Software Bill of Materials (SBOM) has emerged. The SBOM serves as an ingredient list for software, containing relevant data about each software component, including its dependencies, version numbers, and supplier names, among other details.

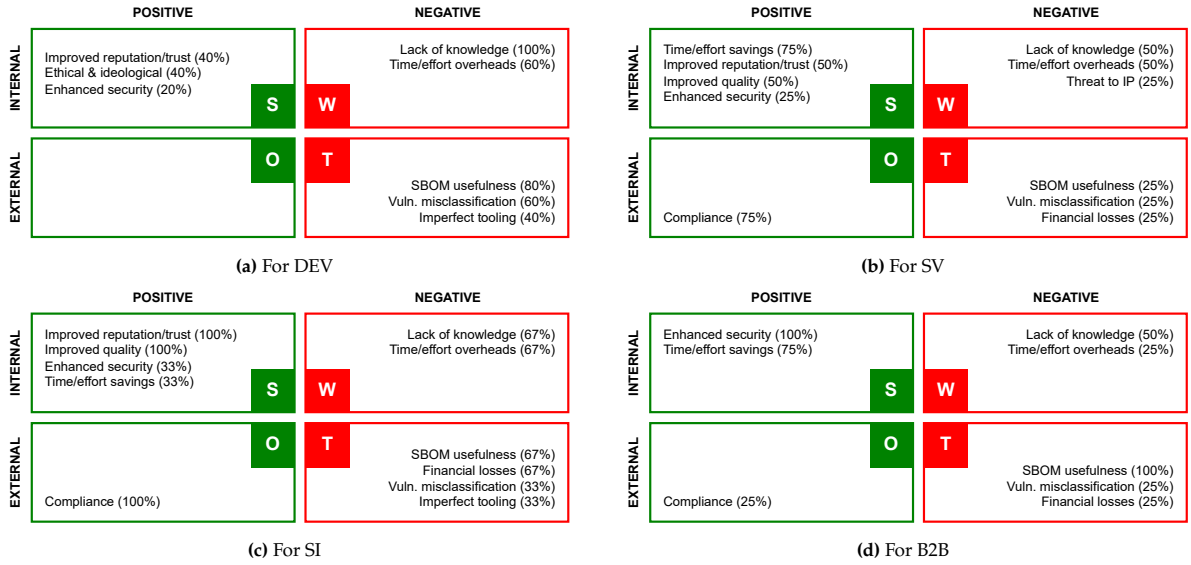
While the concept of SBOM has been around for several years, its adoption and widespread implementation across the SSC and its stakeholders have been relatively limited. Despite the increased attention following SSC attacks such as Log4j and SolarWinds, the literature at the beginning of this research provided little insight into the various interests and concerns surrounding SBOM. Addressing these gaps in both technical and stakeholder considerations became the primary focus of this study. To contribute to the current scientific knowledge gaps regarding the interests involved, empirical data was collected. The main research question was formulated as follows:

What are the main (dis)incentives regarding SBOM among stakeholders in the SSC, and how do these impact its adoption?

To systematically address the research question, it was divided into four sub-questions, each requiring its own research approach and methods. The initial step involved identifying the key stakeholders in the SBOM ecosystem. After thoroughly examining cross-functional processes and value streams, the decision was made to focus solely on stakeholder groups directly involved in the SBOM lifecycle. These groups included developers, software vendors, IT system integrators, and B2B customers. For each of these four stakeholder groups, interview question sets were developed using a bottom-up approach. While the questions were slightly tailored to each stakeholder group, the majority remained the same. The gathered data could later be aggregated to identify general patterns and relationships. Initially, the questions comprised open-ended inquiries regarding participants' anticipated benefits, most impactful (dis)incentives, and significant concerns. Subsequently, more specific questions were posed, exploring predetermined (dis)incentives identified through extensive literature research. Finally, the interviews concluded with an ordinal preference ranking method to obtain a somewhat quantified assessment of participants' perceptions of the specified (dis)incentives.

Following 16 one-hour interviews, a substantial amount of raw empirical data was gathered. To derive meaningful insights from this data and address the research questions, multiple analyses were performed on the dataset. The primary analysis involved a thematic analysis combined with a frequency analysis. Initially, only the themes were extracted from the transcriptions, being the majority of the dataset. To better understand their significance, a frequency analysis was conducted to determine how many participants addressed each theme. The data obtained from the ordinal preference ranking method was subsequently used to validate the preceding findings. Furthermore, a validation session was organized with a field expert possessing extensive SBOM experience. The aim of this session was to share knowledge and gather insights from the expert's perspective on the obtained results. Subsequently, a voluminous amount of findings emerged, which proved intricate to comprehend and clearly differentiate among stakeholder groups within the research scope. Several steps were undertaken to facilitate a more comprehensive analysis of the research questions. Initially, the extensive array of themes was aggregated once again to a more manageable quantity. These were then incorporated into a SWOT analysis for each stakeholder group, precisely delineating the incentives (as strengths

and opportunities, in green) and the disincentives (as weaknesses and threats, in red). The cells in which they are situated visualize how they impact the adoption behavior of the respective stakeholder group and to what extent.



(a) For DEV **(b)** For SV **(c)** For SI **(d)** For B2B

Figure 1: SWOT Matrices

For the B2B sector, the promise of incorporating SBOMs lies in the expectation of achieving **enhanced security** and **time or effort savings**. However, the current reality indicates that SBOM integration may actually require increased **time and effort overheads**, with uncertain benefits. Recent high-profile cyberattacks like Log4Shell underscore the critical need for SBOMs in identifying vulnerabilities and reducing response times. B2B stakeholders perceive SBOMs as having **limited usefulness**, likely due to a **lack of knowledge**. This group is apprehensive about the relevance of SBOMs and foresees cognitive challenges in implementation, leading to reduced internal motivation.

The pursuit of SBOM adoption is notably stronger among the SI and SV groups, primarily driven by **regulatory compliance**. However, under strict compliance regulations, SBOMs may be seen as a procedural requirement. These groups also recognize the value of SBOMs in **enhancing their reputation, trustworthiness, and the quality of the supplied software**. Despite these advantages, they are aware of potential **financial losses** and increased **time or effort overheads** associated with adoption. Consequently, these stakeholder groups are poised to drive widespread SBOM adoption due to their strong motivation and awareness of the technology's benefits.

Developers, much like the B2B group, exhibit hesitance towards SBOM adoption. Their motivation primarily arises from **ethical and ideological principles** and from **enhance their reputation and trustworthiness**. Sustaining internal motivation without corresponding rewards poses a challenge, as financial contributions to popular software projects are typically low, and developers in this study have not cited financial incentives. Furthermore, as many developers work on projects as a hobby, they are not bound by specific requirements. Implementing SBOM would necessitate additional investments due to a **lack of knowledge** and increased **time or effort overheads**. The perceived **limited usefulness** of SBOM for developers remains a concern, resulting in minimal interest in its adoption.

Acknowledgements

Completing this research project marks the culmination of my studies. My educational journey has equipped me with the skills to analyze and address complex problems, devise a robust research plan, and execute it effectively. This project has provided me with an opportunity to push my boundaries by exploring a topic closely aligned with my growing interest in cybersecurity, specifically in the areas of SBOM (Software Bill of Materials) and supply chain security. From start to finish, this endeavor has felt like a seamless process, requiring hard work, but with a clear direction guiding my path.

I would like to express my sincere gratitude to all those who played a significant role in supporting and guiding me throughout this research project. First and foremost, I am deeply indebted to my two supervisors who have been instrumental in this journey: Dr. Yury Zhauniarovich (internal, TU Delft) and Sjoerd Pellegrom (external, Northwave). Their supervision and mentorship over the past few months have been invaluable in helping me navigate the world of SBOM and comprehend its associated incentives. Through our extensive discussions and weekly meetings, they consistently provided me with fresh insights and perspectives, enabling me to structure and enhance my research. The combination of their distinct expertise has created a holistic guidance, which was essential for conducting research in such a novel and emergent domain. From TU Delft, I received immense assistance in comprehensively understanding the technological background and future prospects of SBOM. Dr. Yury Zhauniarovich's shared interest in the topic and the outcomes of my research served as a constant source of motivation and enthusiasm whenever I shared my new findings. At Northwave, the practical business and governance aspects of SBOM were expertly illuminated based on their extensive experience. Within the organization, I was able to fine-tune my interview approach through pilot interviews with various employees from different perspectives. Additionally, with the help of several colleagues, I had the opportunity to engage with interview participants who provided valuable insights.

Furthermore, I extend my thanks to Prof. Dr. Michel van Eeeten for serving as the chair of my research process. Despite his busy schedule, he dedicated his time to provide insightful feedback. I initially approached him with my broad ideas about SBOM and software supply chain security, and our meetings consistently offered valuable insights to ensure the comprehensibility and direction of my research. Additionally, I would like to thank Dr. Y. Aaron Ding for serving as a formal second supervisor and providing feedback on my work. This is the second time I have received guidance from him, following his support during my Bachelor's final project. His involvement may have been less active this time, due to the role of second supervisor, but my gratitude remains unwavering. I would also like to express my appreciation to all the experts I had the privilege of speaking with, who graciously shared their knowledge and expertise.

Last but not least, I want to express my gratitude to Northwave, and particularly the Business Security team. Their involvement has made the otherwise solitary process of individual research significantly more enjoyable. Right from the beginning, I have been fully engaged and warmly welcomed, which has made a tremendous difference.

I hope you find this report enjoyable and informative.

Warm regards,
Berend

Contents

Acronyms vii

1 Introduction 1
- 1.1 Problem Introduction . . . 1
- 1.2 Key Concepts of Related Work . . . 3
  - 1.2.1 Search and Selection Method . . . 3
  - 1.2.2 Selected Articles . . . 3
  - 1.2.3 Benefits of SBOM . . . 3
  - 1.2.4 Adoption of SBOM . . . 4
  - 1.2.5 (Dis)incentives Concerning SBOM and Similar Matters . . . 4
- 1.3 Knowledge Gap and Research Objectives . . . 5
- 1.4 Main Research Question . . . 5
- 1.5 Research Sub-questions . . . 5
- 1.6 Societal Relevance . . . 6
- 1.7 Application to CoSEM . . . 6
- 1.8 Thesis Outline . . . 7

2 Theoretical Background 8
- 2.1 Software Supply Chain Attack . . . 8
  - 2.1.1 Lifecycle of a SSC Attack . . . 9
- 2.2 Technical Breakdown of SBOM . . . 10
  - 2.2.1 Core Elements . . . 10
  - 2.2.2 SBOM Generation . . . 12
  - 2.2.3 SBOM Consumption . . . 13
- 2.3 Regulatory Context . . . 15
  - 2.3.1 Network and Information Systems Directive 2 . . . 15
  - 2.3.2 Cyber Resilience Act . . . 16
  - 2.3.3 Digital Operational Resilience Act . . . 16
  - 2.3.4 Regulatory Context for the U.S. . . . 16

3 Research Methodology 17
- 3.1 Research Approach . . . 17
- 3.2 Data Collection and Analysis Methods . . . 18
  - 3.2.1 Reflection on Research Methods . . . 20
- 3.3 Data Requirements . . . 20

4 Stakeholder Analysis 22
- 4.1 Identifying SBOM Stakeholders . . . 22
  - 4.1.1 SBOM Lifecycle: Cross-Functional Processes . . . 23
  - 4.1.2 Stakeholder Values . . . 24
- 4.2 Determining Key SBOM Stakeholders . . . 25
  - 4.2.1 Excluded Stakeholder Groups . . . 26
- 4.3 Stakeholder Group Distinctions . . . 27
  - 4.3.1 Stakeholder Groups Without Distinctions . . . 27
  - 4.3.2 Stakeholder Groups With (Potential) Distinctions . . . 27
  - 4.3.3 Distinctions in Job Functions . . . 28
- 4.4 Conclusion of Chapter 4 . . . 29

5 Gathering Empirical Data **30**
5.1 The Incentives To Research; Identified Ex Ante . . . 30
5.1.1 Economic . . . 31
5.1.2 Time . . . 31
5.1.3 Regulatory . . . 32
5.1.4 Trust . . . 32
5.1.5 Intellectual Property . . . 32
5.1.6 Awareness . . . 33
5.1.7 Technical Capabilities . . . 33
5.2 Interview Setup . . . 34
5.2.1 Generating the Interviews: The Roadmap . . . 34
5.2.2 Generating the Interviews: The Content . . . 35
5.2.3 Ordinal Preference Ranking . . . 36
5.3 Conclusion of Chapter 5 . . . 37

6 Data Analysis and Findings **38**
6.1 Thematic Analysis: Setup . . . 39
6.1.1 Six Steps of a Thematic Analysis . . . 39
6.1.2 Results of the Main 3 Questions . . . 40
6.1.3 Results of the More Specific Questions . . . 47
6.1.4 Interesting Results in General . . . 58
6.1.5 Participant-specific Results: Micro-level . . . 62
6.2 Ordinal Preference Ranking: Results . . . 64
6.3 Data Validation with Expert . . . 65
6.3.1 Validation of Findings from Main Three Questions . . . 65
6.3.2 Validation of the remaining findings . . . 66
6.4 Stakeholder-Specific (Dis)incentives Overview . . . 68
6.4.1 Aggregation and Frequency Overview . . . 68
6.4.2 Matchup Against Ex-ante Identifified (Dis)incentives . . . 69
6.4.3 SWOT Analysis . . . 70
6.5 Conclusion of Chapter 6 . . . 71

7 Discussion **72**
7.1 Discussing and Comparing the Empirical Results with Existing Literature . . . 72
7.2 Feasibility of SBOM: Inclusions, Responsibilities, and Use Cases . . . 73
7.3 The Role of Governmental Agencies and External Security Companies . . . 74
7.4 Limitations of the Research . . . 74
7.5 Reflection . . . 76

8 Conclusion **77**
8.1 Addressing Sub-Research Questions (1-3) . . . 77
8.2 Addressing Main Research Question . . . 79
8.3 Scientific Contributions . . . 80
8.4 Practical Contributions . . . 80
8.5 Recommendations for Further Research . . . 81

References **83**

A Appendix: Search and Selection **86**

B Appendix: Results of Gathering Empirical Data **89**
B.1 Summaries of Interviews . . . 89
B.1.1 Summary 1 . . . 89
B.1.2 Summary 2 . . . 90
B.1.3 Summary 3 . . . 91

B.1.4 Summary 4 . . . 92
B.1.5 Summary 5 . . . 92
B.1.6 Summary 6 . . . 93
B.1.7 Summary 7 . . . 95
B.1.8 Summary 8 . . . 96
B.1.9 Summary 9 . . . 97
B.1.10 Summary 10 . . . 98
B.1.11 Summary 11 . . . 99
B.1.12 Summary 12 . . . 100
B.1.13 Summary 13 . . . 101
B.1.14 Summary 14 . . . 101
B.1.15 Summary 15 . . . 102
B.1.16 Summary 16 . . . 103
B.2 Ordinal Preference Ranking: Results . . . 105

C Appendix: Data Analysis **106**
C.1 Main 3: Thematic Analysis . . . 106
C.2 Specific Semi-structured Questions . . . 108
C.3 Generally Interesting Findings from Thematic Analysis . . . 112

D Appendix: Data Validation **113**
D.1 Summary of Data Validation with Field Expert . . . 113

Acronyms

Abbreviation	Definition
2FA	Two-Factor Authentication
API	Application Programming Interface
B2B	Business-to-Business
CBS	Centraal Bureau voor de Statistiek
CI/CD	Continuous Integration and Continuous Deployment
CoSEM	Complex System Engineering and Management
CRA	Cyber Resilience Act
COTS	Commercial Off-The-Shelf
CVE	Common Vulnerabilities and Exposures
DEV	Developer
DNB	De Nederlandsche Bank
DORA	Digital Operational Resilience Act
EdTech	Educational Technology
EO	Executive Order
EU	European Union
GDPR	General Data Protection Regulation
IP	Intellectual Property
IT-SI	IT System Integrator
NIS	Network and Information Security
NIST	National Institute of Standards and Technology
NVD	National Vulnerability Database
NTIA	National Telecommunications and Information Administration
OSS	Open Source Software
OWASP	Open Web Application Security Project
ROI	Return on Investment
SaaS	Software as a Service
SBOM	Software Bill of Materials
SCA	Software Composition Analysis
SMEs	Small and Medium-sized Enterprises
SOC	Security Operations Center

Abbreviation	Definition
SSC	Software Supply Chain
SV	Software Vendor
TU	Technical University
UUID	Universally Unique Identifier
US	United States
VEX	Vulnerability Exploitability eXchange

1

Introduction

This research was conducted at Delft University of Technology in collaboration with the cybersecurity firm Northwave, with primary guidance from their Business Security team. The objective of the thesis is to provide new insights into the current distribution of (dis)incentives concerning the Software Bill of Materials (SBOM) among key stakeholders in the software supply chain (SSC), and how these (dis)incentives could be inhibiting the adoption of SBOM. The results of this study will be used to identify potential solutions and recommendations for further research, in order to contribute to the overall adoption of SBOM. The exploratory research approach is used to gather empirical data from the four main stakeholder groups, consisting of (respectively from the beginning to the end of the SSC) software developers, software vendors, IT system integrators (IT-SIs), and B2B customers. The research starts with gathering empirical data at the end of the SSC, being those B2B customers of the third-party software supplied by stakeholders higher up in the SSC. After, the research gradually progresses higher up the SSC to extract (dis)incentives to adopt SBOM from the other relevant stakeholders. In the end, this should give us a complete understanding of the set of (dis)incentives in place at the SSC, and how this set causes an inhibition of the adoption of the concept. Furthermore, for this research, participants from stakeholder groups besides developers will primarily consist of customers of Northwave's services.

This chapter forms the basis of this research project. The primary research problem, which is introduced in Section 1.1, revolves around the challenges and barriers that limit the adoption of SBOM in the SSC. To provide a clear understanding of the core concepts regarding SBOM, Section 1.2 discusses its benefits, adoption, and the importance of (dis)incentives involved. To address these challenges, the main knowledge gap from the literature review is identified in Section 1.3. The knowledge gap relates to the limited understanding of the (dis)incentives regarding SBOM among stakeholders in the SSC and the impact of the set of these (dis)incentives on SBOM adoption. Based on the knowledge gap, the main research question, which is introduced in Section 1.4, is formulated as follows: *What are the main (dis)incentives regarding SBOM among stakeholders in the SSC, and how do these impact its adoption?* To answer this research question constructively, sub-questions are identified in Section 1.5. The sub-questions aim to provide a more in-depth understanding of the (dis)incentives that drive SBOM adoption and the factors that hinder its adoption in the SSC. Additionally, the sub-questions seek to identify the impact of these (dis)incentives on the adoption of the technology. Next, Section 1.6 discusses the societal relevance of the issue. Here the research will delve into the threats of the current lack of transparency in SSCs and what consequences it may have for numerous different stakeholders. Section 1.7 then states how the research relates to the CoSEM master's program. It gives examples of how certain core courses (and lessons from them) are incorporated into the research process for this thesis. Finally, Section 1.8 visually depicts the outline of this thesis in a Research Flow Diagram, where the different phases are linked to the sub-questions, research methods, and deliverables.

1.1. Problem Introduction

Organizations across all industries are becoming increasingly dependent on third-party software products and services within their businesses (Okafor et al., 2022). In the software, derived from commercial software vendors, 85 to 97% of the code originates from OSS repositories, including APIs, libraries, packages, binaries, and so on (Martínez & Durán, 2021). The OSS is developed by open source developers who themselves include a lot of open source components into their own code development processes. This results in their software components being dependent on other software components and havign a lot of, so-called, dependencies. Software vendors include OSS components into their solutions too, which creates dependencies that have dependencies. The trend of increasing software dependencies, driven by developers' inclining towards incorporating more third-party components, is fueled by the industry's growing demand

for faster software development cycles (Pashchenko et al., 2021). Between software vendors and B2B customers there is often an IT systems integrator (IT-SI) who assembles the developed software application elements into a ready-to-use software product for the B2B customer (Hertweck & Bouché, 2006; Scacchi & Alspaugh, 2019). A vendor supplies to many different customers, and conversely, customers buy from many different vendors. All in all, this structure of software progressing from developers, to vendors, to IT-SIs, to customers, forms the SSC (Viega & Michael, 2021). The combination of all these different applications and services with their differently composed software and all their dependencies makes the dependency trees of SSCs very complex. An issue within that complex SSC is that most stakeholders involved keep little to no record of what they use and import when developing their software. This results in a lack of transparency into those dependencies, and therefore the composition of all software brought into a B2B organization, as well, cannot be determined (Zajdel et al., 2022). As organizations bring in a lot of third-party software from multiple vendors and IT-SIs, and create larger software stacks, their security or IT teams, as a result, have very little insight into what is in the software they have running in their stack (Viega & Michael, 2021; Wang, 2021). A simplified conceptual representation of an SSC and the lifecycle of software within is shown in Figure 1.1. The arrows in the figure represent the progression of software through the SSC, primarily indicating the direction of flow. The figure is simplified, which means that in practice, the chain may consist of significantly more links, resulting in greater complexity and layering.

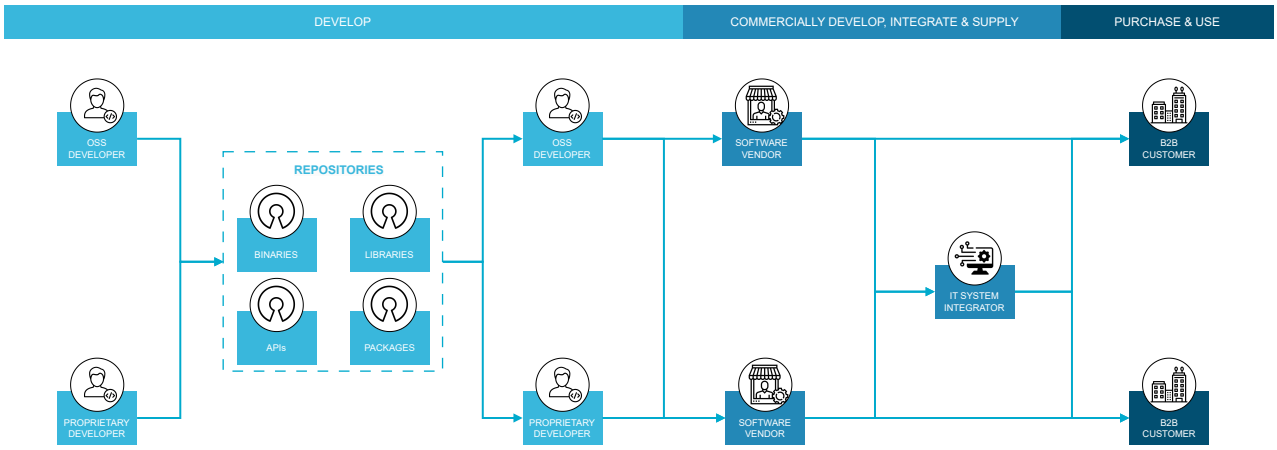


Figure 1.1: The lifecycle of software products through the SSC (own illustration)

To contribute to enhancing transparency in software (supply chains), SBOM is frequently cited in current literature as a promising technological solution envisioned to effectively address issues related to transparency. An SBOM is a comprehensive list consisting of metadata and technical information on software components, and relationships between the latter (Girdhar, 2022). For example, it contains information such as the version number, licensing, and dependencies of all the components that make up a software component. The primary benefit, as highlighted by Martínez and Durán (2021) and Okafor et al. (2022), is the envisaged contribution of the SBOM concept to transparency and visibility. As a consequential positive effect, others argue that it should also facilitate the expedited identification of vulnerabilities, offer an improved comprehension of licensing, security, and quality dimensions, and potentially enhance compliance with legal and regulatory frameworks (GitHub, n.d.-a; Romanosky & Welburn, 2022; Xia et al., 2023). Collectively, these diverse benefits are anticipated to empower stakeholders within the SSC to more effectively manage and potentially mitigate their security risks. Further insights into the technical construction of SBOMs and the engagement of various stakeholders throughout its lifecycle will be expounded upon in 2.

Despite these theoretically promising purposes of SBOM technology, widespread adoption of the concept within the SSC remains limited. Research conducted by Xia et al. (2023) explicitly demonstrates that at least 81.3% of the organizations they surveyed reported not receiving SBOMs for third-party software or components. In theory, as depicted by state-of-the-art researchers, SBOM holds considerable promise. However, whether the directly involved stakeholders share the same perspective on SBOM has received little attention. Only Xia et al. (2023) have engaged with direct practitioners, uncovering SBOM uncertainties concerning its use cases, benefits, and apprehensions about its production quality. They posit that these factors may contribute to inhibiting its adoption. Nevertheless, these findings remain general and lack linkage to stakeholder-specific (dis)incentives. Similarly, the work of Moroz (2022) and Allan Friedman, a notable figure from the National Telecommunications and Information Administration (NTIA) and a key figure in SBOMs, merely state that misalignment of (dis)incentives can hinder adoption but do not delve into the specifics (Elias & Jones, 2022; Owen, 2022). The researchers also consider the classical *network externalities* theory as a reason to explore this further, deeming it relevant to the study. Accorrding to Top et al. (2011) the theory states that an entity's utility for a particular good depends on the

number of other entities consuming the same good. Without the alignment and elimination of the stakeholder-specific (dis)incentives, the technology has a low potential for widespread adoption. The lack of SBOM adoption among different stakeholder groups means that, in terms of the theory, the critical mass is currently absent. Consequently, there are primarily costs for adopters and relatively few benefits. The researchers consider it highly likely that this currently hinders the acceptance of the technology as a whole. Therefore, investigating the (dis)incentives that impact adoption is considered relevant.

This thesis aims to bridge this gap through empirical practice-based research, focusing on each relevant stakeholder group to ascertain their primary (dis)incentives. Moreover, it seeks to investigate the issue from a socio-technical perspective. In doing so, it furnishes novel insights into how and which of these factors exert the most impactful influence on SBOM adoption, encompassing both positive and negative aspects.

1.2. Key Concepts of Related Work

To identify the state-of-the-art literature and define the knowledge gap of the problem domain introduced above, a literature review is conducted on the available literature on SBOM, its benefits, its current adoption, and on (dis)incentives regarding SBOMs and similar cyber security challenges. The literature review is guided by these three concepts identified during the problem demarcation. It is crucial to create a shared understanding of these fundamental principles early on in order to further scope the thesis. The next sections introduce the concepts and their definitions.

1.2.1. Search and Selection Method

The articles that are to be reviewed must be of an adequate scientific level. Therefore, searches were done through search engines such as Scopus and Google Scholar (Google Scholar, n.d.; Scopus, n.d.). Figure A.1 in Appendix A visualizes what search strings and screenings eventually lead to a selection of 18 articles.

Initially, a 'LIMIT' is set for the search strings of a publication date of 2020. This means that through those search strings, only articles published after this year can be found. This was a deliberate decision, because while reading up on the thesis, it turned out that most of the relevant research had taken place after. Many of the (relatively) few publications available before 2020 are also exclusively healthcare-related. Furthermore, very little research from these years has been cited in post-2019 studies. Still, in order not to neglect the research from before, a backward snowballing method was applied through the articles found. This facilitated one extra relevant source and was also included in the literature review.

1.2.2. Selected Articles

Figure A.1 depicts the search process well, but it does not indicate which sources were actually chosen. For that, this section and especially Table A.1 serve their purpose. Here, the title, author(s) and publication date of each article are first shown. Then, for all literature, a distinction is made between three different categories. From left to right, it determines whether the article addresses the relevance of SBOM as a solution against the current lack of transparency and visibility within software systems, whether it addresses the lack of SBOM adoption, and/or whether it addresses misaligned (dis)incentives between key players in the SSC.

1.2.3. Benefits of SBOM

What emerges from the literature review, and is visible in Table A.1, is that the relevance of SBOM is confirmed in almost every literary publication that cites the concept. The fact that supply chain attacks are growing rapidly (Xia et al., 2023) provides the basis for the added value and the need for a solution for SSC transparency. Consequently, this is the main objective of SBOM: to increase transparency and visibility of software and their supply chains (Eggers et al., 2022; Girdhar, 2022; Martin, 2020; Nadgowda, 2022; Okafor et al., 2022; Romanosky & Welburn, 2022; Xia et al., 2023).

Several important benefits follow from this main purpose of SBOM, which also contribute to the relevance of the concept. For example, the increased transparency enables organizations to better manage their cyber risk (Arora et al., 2022; Clancy et al., 2021; Moroz, 2022; Nissen et al., 2018; Romanosky & Welburn, 2022; Zajdel et al., 2022). Nissen et al. (2018) state, "*If done properly, an SBOM can estimate the overall risk of the ensemble of software elements based on the risk of the individual elements.*" When purchasing software products, customers can better determine their risks and make more informed decisions (Arora et al., 2022; Moroz, 2022; Zajdel et al., 2022). "*SBOMs can help organizations or people to avoid consumption of software that could harm them*" (Zajdel et al., 2022).

Mitigation of risks is also cited as a major advantage of SBOM by Xia et al. (2023), Clancy et al. (2021), Martínez and Durán (2021), Okafor et al. (2022), Moroz (2022), and Eggers et al. (2022). Thus, the associated impact of SSC attacks is dramatically reduced (Clancy et al., 2021). This is due to the fact that identifying security vulnerabilities is easier (Girdhar, 2022; Okafor et al., 2022) and can be shared much faster. That way, when a vulnerability is reported, an organization knows much sooner whether they are impacted by it or not (Xia et al., 2023). In the case of Log4j, Eggers et al. (2022) even

mention: *"a facility that had implemented an SBOM program could quickly search and find all instances of Log4j in their operational environment"*. In the event of an SSC attack, if an organization knows early on whether it is affected, it can take much more effective and reliable action (Eggers et al., 2022; Moroz, 2022; Okafor et al., 2022).

Furthermore, a number of other benefits are identified by Girdhar (2022) and Martin (2020). For example, SBOMs could help with decision making and create insights regarding licensing. This could directly ensure better enabling of regulatory compliance.

1.2.4. Adoption of SBOM

There is one important aspect to the success of SBOM that is cited several times: interoperability (Arora et al., 2022; Clancy et al., 2021; Eggers et al., 2022). The introduction explains the complexity of the dependency trees of software components. The key point is that there are numerous layers of dependencies, which implies that in order to generate a high-quality SBOM, you also need SBOM information from the dependencies implemented during the development process. This means that the stakeholders developing those components should also produce and make available SBOMs. The only way to accomplish this is through widespread adoption (Arora et al., 2022; Clancy et al., 2021; Eggers et al., 2022; Moroz, 2022). An additional crucial aspect of adoption is the uniform adoption of standardized SBOM formats across all stakeholders. Why this is all important for optimal SBOM functionality will be elaborated upon in Chapter 2. However, even though the concept has been around for years, literature reviews show that SBOM adoption is still lacking. This is most prominently addressed by Xia et al. (2023), Arora et al. (2022), and Moroz (2022). Interviews and surveys of the first research group indicate 83.1% agree that third-party software or components that are purchased are not equipped with SBOMs. The lack of adoption is also cited beyond the scientific literature. This is not included in the 'official' literature review, but is worth mentioning. For example, the same Allan Friedman as in Section 1.1 makes a lot of comments on the lack of current SBOM adoption in several interviews (Elias & Jones, 2022; Owen, 2022).

1.2.5. (Dis)incentives Concerning SBOM and Similar Matters

A misalignment of (dis)incentives regarding SBOM of the crucial stakeholders involved appears to be a main reason for the lack of the adoption of the concept, according to Xia et al. (2023) and Moroz (2022). Moroz (2022) specifically highlights this issue and argues that many organizations prioritize short-term interests over long-term goals. Meanwhile, Xia et al. (2023) argue that the lack of availability of SBOMs for software components is hindering software vendors from adopting SBOMs, and causing them to question whether SBOM adoption is an industry-wide consensus. The authors state that "*The (dis)incentives for generating SBOMs for OSS and proprietary software need to be propagated*" as the benefits of SBOM adoption are not yet clear enough for software vendors.

Non-scientific publications also provide interesting insights into the SBOM field. As mentioned, Allan Friedman is a prominent figure in this area and his opinions should be taken seriously. According to Elias and Jones (2022), Friedman argues that there is a "*chicken and egg*" problem in SBOM adoption. Few parties are requesting it, and as a result, few vendors are supplying it. Similarly, few vendors are offering it, and therefore, nobody is asking for it. This observation aligns with both the previously identified network externalities theory and the findings of Xia et al. (2023), who also noted a lack of clarity regarding the benefits of SBOMs for vendors. Koran et al. (2022) suggest that software customers should demand more SBOMs from vendors and developers. Currently, vendors do not seem to understand the potential return on investment from producing SBOMs (Crowdstrike, 2021), which is consistent with the findings of Xia et al. (2023). Given that vendors need to know what they stand to gain from investing significant resources, it is concerning that there is no clear and tangible value proposition for SBOM adoption (Koran et al., 2022).

Other scientific articles have also indicated issues with (dis)incentives between the major participants in related SSC systems in relation to other cyber security concepts as well, not just SBOM. Nygard and Katsikas (2022), Fouad (2022), Gordon and Loeb (2002), Viega and Michael (2021), and Wright et al. (2021) all give examples of problems in obtaining security due to friction between vendors and customers. Nygard and Katsikas (2022) echo the sentiments of Xia et al. (2023) and Koran et al. (2022), but in the context of software in SSCs in general. They suggest that customers should request vendor development security practices and that vendors should disclose their security practices. It is evident that vendors are not sufficiently incentivized to prioritize security as their main focus is on selling and earning profits from their products (Gordon & Loeb, 2002). Viega and Michael (2021) provide an example of assessments and argue that vendors are reluctant to spend time on them and instead focus solely on their business. Wright et al. (2021) and Fouad (2022) both note that vendors often have "*weak commercial incentives*" to invest in and prioritize cybersecurity in software development. They attribute this to a lack of consumer awareness that limits commercial incentives for vendors to compete on cybersecurity. Both authors suggest that regulatory intervention is necessary in such situations.

An important finding of this initial literature review is that, despite potential challenges and disincentives surrounding SBOM adoption, this does not imply that SBOM cannot obtain future success. An analogy is drawn to the implementation of nutrition labels on food products in the food industry, which also experienced a prolonged period of time and encountered

friction between governmental bodies, industries, and consumers. However, despite these challenges, the concept was ultimately fully implemented (Koran et al., 2022).

1.3. Knowledge Gap and Research Objectives

The current state of research confirms the potential of SBOM in promoting transparency within the SSC. However, despite the numerous benefits of SBOM, there is a pervasive lack of widespread adoption, which is evident both in the literature and in practice. This reluctance to adopt SBOM is largely attributed to a misalignment of (dis)incentives among the various SSC stakeholders, which poses a significant obstacle. The stakeholders involved in the SSC have varied objectives and priorities that could span from, e.g., delivering high-quality software, minimizing costs, complying with regulations, and protecting intellectual property. The misalignment in the set of (dis)incentives creates a substantial hurdle to the adoption of SBOM as it creates a conflict of interest between the different stakeholders.

Despite the recognized significance of the misalignment of (dis)incentives among stakeholders in the SSC, there is currently a lack of dedicated research that comprehensively examines how this phenomenon inhibits the adoption of SBOM. This represents the main knowledge gap in the current literature. Subsequently, the main research objective will be to gain insights into the inhabitant behaviour of the set of (dis)incentives, in order to try to contribute to the current knowledge gap. While some studies have explored the technical aspects of SBOM, few have investigated, e.g., the socio-economic factors that influence its adoption. To address this knowledge gap, the proposed thesis will adopt a holistic approach to investigate the various factors that affect the adoption of SBOM from all angles, including both OSS and commercial software suppliers, customers, regulators, and industry associations. The research will seek to identify the main set of impacting (dis)incentives, concerns and capabilities regarding SBOM adoption among the SSC stakeholders. The findings will then be utilized to formulate recommendations, strategies, and future research directions aimed at promoting the adoption of SBOM by aligning the (dis)incentives of different stakeholders within the SSC. Ultimately, the thesis will make a contribution to the field of software engineering by addressing a crucial knowledge gap and providing novel insights into a fresh and relevant subject.

1.4. Main Research Question

The thesis seeks to investigate the (dis)incentives related to SBOM adoption among stakeholders within the SSC, using empirical data to generate new insights in this area. The study aims to provide valuable recommendations and future research directions based on the findings. The main research question, which builds upon the preceding discussion, represents the thesis's core inquiry, and the study endeavors to provide the most robust answer possible.

Main Research Question:

What are the main (dis)incentives regarding SBOM among stakeholders in the SSC, and how do these impact its adoption?

1.5. Research Sub-questions

In order to provide a comprehensive and structured answer to the main research question, the research is divided into several sub-questions. Before attempting to fully understand the problem within this study, it is important to first establish a thorough understanding and the boundaries of the problem. Much of this context-setting is covered in Chapter 2. Another important aspect of the research of determining what stakeholders are most important and relevant to gather empirical data from (in the context of certain time constraints) will be addressed in Chapter 4. A detailed examination of the various stakeholder groups within the SSC, differences both between and within those groups, interdependencies between them, and all of their relationships with respect to SBOM, will provide an answer to the following sub-question.

Sub-question 1:
What are the most important SSC stakeholders involved with SBOM?

With this fundamental basis established for approaching the research, empirical data on SBOM incentives (as well as disincentives) can be gathered from the identified stakeholders. It is important to first define what the research considers as "(dis)incentives" and what it will assess its respondents on. The capabilities of various SSC stakeholders with respect to SBOM will also become clear from the results of the following sub-question. These results will be displayed in Chapter 5.

Sub-question 2:
What are the (dis)incentives and capabilities of SSC stakeholders regarding SBOM?

Subsequently, the gathered data can be subjected to analysis in order to identify patterns and relationships between stakeholders and their (dis)incentives. This will lead to new insights in an area where little research has been conducted thus far. These insights will be the result of sub-question 3, and showcased in Chapter 6.

Sub-question 3:
What factors can explain the lack of SBOM adoption?

Figure A.2 provides a clear overview of these sub-questions and what their corresponding research approach, data collection methods, and the associated deliverables are. Chapter 3 provides further detail on the research approach and methods.

1.6. Societal Relevance

As already evident from Section 1.2, almost all existing, relevant literary articles on SBOM indicate the relevance of the concept by stating its benefits. The main thrust there was about increased transparency, and consequently being able to better manage and mitigate risk. This already implies the relevance of the concept, but to really indicate societal relevance as well, this section touches on some additional relevant elements.

The SBOM has become increasingly relevant due to the growing threat of SSC attacks. An important fact, for example, is that those SSC attacks are growing tremendously fast. By 2021, the total was up 650% from the year before (Xia et al., 2023). SSC attacks involve the manipulation of code in third-party software components during the development process with the aim of compromising the downstream applications that are eventually utilized by the customers (Okafor et al., 2022). The attackers are able to subvert the integrity of the source code of a widely used software component, allowing them to insert backdoors or malicious code, such as malware, which provides them with access to organizations that are customers of the compromised software vendors. This type of attack is often referred to as a "supply chain" attack because the ultimate targets (organizations) are reached through the software vendors, rather than directly targeting them (Martínez & Durán, 2021; Wang, 2021).

The societal damage caused by SSC attacks is significant. A recent example of a SSC attack is the SolarWinds attack in the United States (Martínez & Durán, 2021). As SolarWinds' Orion software was so widely distributed, the damage caused by the attack was immense. Both private and public government agencies' data were compromised, and the economic damage is estimated to be over billions of dollars (Okafor et al., 2022). This illustrates the need for increased transparency in the SSC, which can be achieved through the use of SBOMs. Arora et al. (2022) argue that the SolarWinds attack (and at least the severity of it) could have been prevented if the use of SBOMs had already been widely adopted and used. This highlights the potential benefits of the widespread adoption of SBOMs, which can help to increase transparency and security in the SSC.

In fact, the relevance of SBOMs has been recognized by the United States government. A recent U.S. executive order on cybersecurity, EO 14028, highlights the potential of SBOMs in improving the security of the SSC (Arora et al., 2022). Vendors supplying to the U.S. government already are mandated to provide SBOMs with their software. The order calls for the maintenance of accurate and up-to-date data, including the origin of software code or components, which aligns with the SBOM concept. The lack of visibility into software components and their origins is recognized as a significant vulnerability in the SSC, and the order calls for the implementation of controls to address this issue.

1.7. Application to CoSEM

The research in question has been deemed appropriate within the guidelines set forth by CoSEM, as outlined in the graduation portal. It is focused on addressing a complex socio-technical problem that has the potential to yield new insights relevant to the design of future solutions. This problem involves a wide range of stakeholders with conflicting interests that must be carefully considered and balanced. To fully explore this issue, the research will approach it from multiple angles, taking into account technical, economic, and institutional factors. Additionally, the study will be informed by both public and private values, recognizing the important role that each plays in shaping the problem and potential solutions.

The research will also apply various methodologies and theories covered in the core courses of CoSEM. This section provides some examples. One such course is "*Institutional Economics for Designing in Socio-technical Systems*", which provides knowledge on how to diagnose problems (in market functioning) and how institutions at different levels can influence them, for example, through Williamson's four-layer model (2000). The course taught me to have a holistic overview of

the socio-technical system from macro to micro-level. It also provides illustrations of general frameworks that can guide whether or not to intervene in a market. Many of these elements can be useful for this thesis. For instance, the SSC is a socio-technical system, in which free market functioning currently fails to achieve a safe level of software transparency. Institutional considerations and questions will be addressed later in the research, so elements from this course will be revisited.

Another course that contained relevant material for this research is "*Managing Multi-Actor Decision-Making*." This course was mentioned as the follow-up course to "*diagnosing the complexity of systems and problems*" from previous courses and takes a step further towards "*realizing change*." It focuses specifically on all the different stakeholders in a socio-technical system and asks, "*How do they behave, individually and collectively?*" It turns out that this behavior often greatly complicates the designability of systems and the creation of intentional change. For this research, it is interesting to determine the different behaviors, (dis)incentives, and interrelationships between stakeholders. This can later inform the design of solutions. Furthermore, this course also provided valuable experience in conducting extensive literature research.

The course "*CoSEM Research Challenges*" also provides useful information. Given that I will conduct interviews and work with personal and other sensitive data for this research, it is important to consider the taught material regarding scientific integrity. Moreover, this course helped to raise "*academic curiosity*" and foster an "*academic attitude*."

1.8. Thesis Outline

The thesis outline is displayed in Figure A.2, which includes a visual representation of the research process via a research flow diagram. The diagram illustrates the principal phases of the research project, from introduction to conclusion.

2

Theoretical Background

Chapter 1 presented a concise outline of the problem domain, introducing the concept of SBOM and its potential benefits, while also highlighting the challenges regarding the (dis)incentives among important stakeholders in the SSC ecosystem, which hinders the adoption of the concept. The complex socio-technical nature of SSC systems, makes it difficult for those unfamiliar with the topic to fully comprehend the research presented in this thesis. Particularly, as it integrates the complex domain of SSC with a new concept like SBOM. It involves numerous actors with interdependent relationships, power and interests, technical challenges, and a dynamic institutional playing field. However, to appreciate the comprehensive findings of this thesis, a thorough understanding of various aspects related to SSCs and SBOM is essential. Thus, this chapter provides an overview of the important concepts for the research subject. Experts in the field may skip this chapter and proceed directly to Chapter 3. The chapter starts with a more extensive overview of the potential threat landscape and associated risks that can arise from the lack of software transparency in SSCs. This includes an explanation of how attacks on the SSC generally occur, thereby emphasizing the importance of SBOM for better vulnerability risk management and mitigation. Subsequently, the concept of the SBOM itself is completely broken into various important aspects that make it the promising concept it is (Section 2.2) This will mainly consist of technical details such as its core elements (both technical and metadata), and the important stages to facilitate the utility of SBOM. Then, the institutional context regarding SSCs and SBOMs is established (Section 2.3). This is important for socio-technical systems as it helps in understanding the organizational and societal factors that influence the system's development and implementation. This determination is significant as it supports the analysis of power distribution and decision-making processes amongst system stakeholders.

2.1. Software Supply Chain Attack

Organizations have very little insight and understanding of the composition of their software stack and its dependencies (see Chapter 1). Malicious actors employ this lack of understanding to their advantage by committing SSC attacks. From the 'Societal Relevance' (see Section 1.6), it is evident that attacks on SSCs have shown a significant increase in frequency over the last years and have the potential to cause substantial damage (Okafor et al., 2022; Xia et al., 2023). Additionally, a high-level description has been provided for how these attacks typically play out and how they can spread so extensively. However, a complete technical explanation of these SSC attacks and how they can have such a broad reach has not been explicitly detailed. Thus, this section serves to provide that level of detail.

In brief, attacks on SSCs are aimed at compromising *downstream* software components (meaning the progression of software from developer/supplier side to the demand/customer side of the SSC) and products by targeting the *upstream* levels of the SSC (Martínez & Durán, 2021; Wang, 2021). This is accomplished by manipulating third-party (OSS) code early in the software lifecycle. During the development process of software vendors, the modified code (e.g., with injected malware) is integrated into the final product, which is then distributed downstream. Section 2.1.1 provides further explanation and examples of these attacks. It has been found that attackers typically target widely used software components, particularly those belonging to OSS (Martínez & Durán, 2021). OSS is a software development model that provides access to the source code, making it easier for developers to customize and improve the software. However, despite its benefits, OSS has its own set of issues, with a prominent one being the lack of regulation (Zajdel et al., 2022). Most OSS projects are maintained by single developers or small teams of volunteer developers who contribute out of intrinsic motivations, but are constrained by limited time and resources to properly test and maintain their code. As a result, a lot of OSS contains bugs, vulnerabilities, and other issues that make it highly susceptible to exploitation (Zajdel et al., 2022). While the sheer number of open source contributors is argued to limit the number of bugs and vulnerabilities,

the reality is that there are almost an equal number of malicious actors who are also analyzing the code to discover ways to exploit and attack the software, which is easier to do given that the source code is open.

The proposition of SBOM should be able to contribute to mitigating the risks related to these attacks. Through increased SSC transparency, organizations that have adopted SBOM technology can identify and mitigate widely spread SSC attack vulnerabilities more rapidly (Roberts, 2021). Given the significance of SBOMs in the context of these attacks, it is relevant to have a clear understanding of how an SSC attack unfolds for the background of this thesis.

2.1.1. Lifecycle of a SSC Attack

Nowadays, threat actors often comprise of sizable and highly coordinated organizations. They intentionally seek for (open-source) software components that are (widely) used by various developers. Through analysis and downloading of the OSS code, they identify and exploit software bugs and vulnerabilities (Zajdel et al., 2022). Another method used by attackers is 'repository poisoning', where they develop imitative libraries that mimic authentic ones and insert malicious code into them. These libraries are then slightly modified and uploaded to the repository with names that closely resemble the legitimate versions. As a result, developers unknowingly download these contaminated libraries without verifying their names, leading to the inclusion of an exploitable library into their code base. One other method that goes even further consists of threat actors embedding their vulnerabilities within the original repositories alongside patches. This deceptive technique increases risk for developers, as they may unknowingly incorporate the compromised code into their projects while intending to apply necessary updates. The ultimate goal of these attacks is to distribute the contaminated software products and services downstream over the SSC as widely as possible. This makes it a "supply chain" attack where the target is not directly attacked, but rather organizations are compromised through indirect means. The average SSC attack, identified by Okafor et al. (2022) can be summarized in four steps, as shown in Figure (2.1) below.

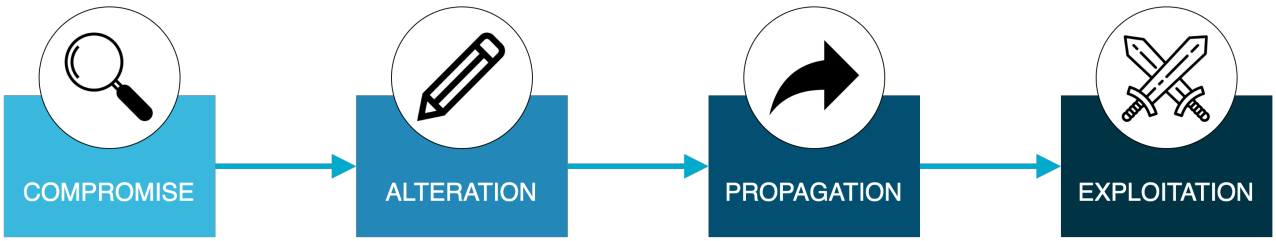


Figure 2.1: The four step software supply chain attack (Okafor et al., 2022)

The analysis and downloading of source code are essential elements preceding the first step of a SSC attack (Zajdel et al., 2022). This is done to determine the vulnerabilities present in the SSC that can be exploited. Additionally, through methods such as 'repository poisoning', the foundation for the attack can be established. According to Martínez and Durán (2021) and Okafor et al. (2022), the procedure begins when the threat actors infiltrate and *compromise* a software component. Step 2 of a SSC attack, called *Alteration*, is a crucial step where the threat actor leverages their initial access to the system to modify the SSC, compromising the integrity of the software. This involves subverting the software source code to insert backdoors and malware. Backdoors allow the attacker to bypass authentication mechanisms and gain unauthorized access to the system, while malware refers to any software designed to cause harm to the system. The third step of a SSC attack, called *Propagation*, involves the spread of the introduced malicious code to downstream components and links. Once the threat actor has successfully altered the software component, the malicious code is distributed to all associated entities, including customers, partners, and suppliers (Zajdel et al., 2022). This phase is concerning as it can lead to the widespread distribution of malware, compromising the security and integrity of numerous systems. It is important to note that the propagation phase can continue long after the initial attack as the compromised software can continue to be distributed to new customers and partners. The fourth and final step of a SSC attack involves *exploiting* the downstream links, allowing threat actors to gain access to the systems of organizations that have installed the compromised software. This access can potentially result in the theft of sensitive data, disruption of system operations, or other types of harm.

The SolarWinds supply chain attack is a notorious example of such a SSC attack (Martínez & Durán, 2021). It involved the use of a sophisticated technique in which the threat actors falsified the identity and authentication mechanisms of access accounts to infiltrate the network monitoring and management platform software known as Orion. Referring to Figure **??**, this corresponds to the Compromise step. Following that, step 2 was the Alteration. The threat actors implanted malicious code into a specific software library, called '*SolarWinds.Orion.Core.BusinessLayer.dll*', within the Orion Platform. To propagate the malware, step 3, SolarWinds unknowingly signed and distributed the infected library as part of its regular update processes (Martínez & Durán, 2021). The threat actors used this strategy to gain access to critical data and systems, enabling them to exfiltrate sensitive information and cause significant damage to targeted organizations, which relates

to step 4. The attack ultimately affected more than 18,000 customers and 40 public entities across different sectors and locations worldwide, including government entities, technology companies, insurance companies, financial companies, and retail companies.

The SolarWinds supply chain attack highlights the critical need for enhanced security measures and careful monitoring of SSCs. It also underlines the importance of implementing multi-layered security measures to protect against advanced and evolving threats that can infiltrate trusted software systems.

2.2. Technical Breakdown of SBOM

According to the literature, in addition to providing better insights into licensing, codebase quality, and compliance with regulations, a major advantage of the transparency realized by SBOM is the ability to manage and mitigate security risks more effectively. This increased transparency within the SSC and its dependencies enables faster identification of vulnerabilities.

To conduct in-depth interviews with participants from all stakeholder groups and obtain relevant and comprehensive results, it is important to have a thorough understanding of all technical aspects of SBOM. As a start, this includes gaining insight into the minimum core elements that must be included, as outlined in Section 2.2.1. Section 2.2.2 discusses the responsibilities regarding the production of SBOM and how it should be done. 2.2.3 proceeds to describe how an organization intending to utilize the SBOM should capture the value from it. Finally, 2.3 examines the institutional and regulatory context of the playing field regarding SBOM and its associated stakeholders. It mainly focuses on EU laws and regulations, but legislation from the U.S. will also be included as context.

2.2.1. Core Elements

According to most descriptions, an SBOM is a comprehensive list of all the components that constitute a certain software component, which can vary widely in nature. To ensure an adequate SBOM production, multiple authors and organizations, including the NTIA (2019), have developed standards outlining a minimum set of SBOM elements. However, it is important to note that the specific elements of the SBOM are not uniformly defined and can vary depending on individual perspectives. This variation may also depend on the organization or sector involved. The SBOM elements presented in Figure 2.2 is a aggregation of various scientific publications and government reports, which provide insights into the elements necessary for its comprehension. According to the NTIA (2019), an SBOM should be created for each software component, which is essentially a unit of software. Each piece of information about these components is referred to as an attribute. Together, the component and its attributes form an SBOM entry in an SBOM artifact. Ideally, the artifact would be a type of aggregated SBOM, where data from all individual SBOMs for an application, for example, can be consolidated to provide a comprehensive overview of the application.

Based on Girdhar (2022), there exist two distinct types of attributes associated with the SBOM. The first type of attribute is responsible for providing meta-information about the SBOM record itself. This meta-information may consist of details such as the license type, copyright information, and any security vulnerabilities that may be linked to a particular dependency of the software component (Moroz, 2022). Additionally, the SBOM can also provide instructions that are relevant to installing, configuring, or operating the software component. The additional technical attributes in the SBOM provide information on the dependencies of that specific software component. These dependencies include, e.g., libraries, frameworks, and other software modules that are integral to the functioning of the component. Also, details such as version numbers and supplier names of all those dependencies need to be included. Multiple sources, including Arora et al. (2022), Eggers et al. (2022), and Girdhar (2022), and the NTIA (2019), offer a clear overview of the baseline elements expected in a minimum SBOM. The synthesis of the literature has resulted in the following list of SBOM elements (Figure 2.2).

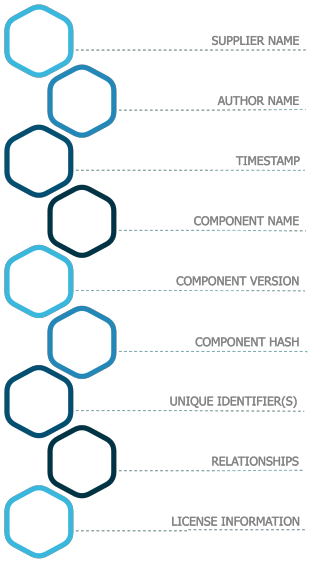


Figure 2.2: The baseline elements that make up a minimal SBOM (own illustration)

From top to bottom, the "supplier name" represents the name or entity of the component's supplier. The "author name" refers to the person who produces the SBOM, which may not necessarily be the same as the supplier. The "timestamp" provides meta-information about when the SBOM was created and/or last updated. An identifier assigned to the component forms the "component name," which is determined by the original supplier. The "component version" makes it easier to identify specific components and specify software changes. The "component hash" is a special code that allows to uniquely identify the software component. It's created by using certain techniques to generate a unique value based on the file's content. This code acts like a digital fingerprint, making sure the file hasn't been changed and allowing for easy comparisons with other files. On the other hand, a 'unique identifier' is a method used to uniquely identify a software component. Unlike being based on the file itself, it is generated using specific information unrelated to the component. For example, a Universally Unique Identifier (UUID) is a type of unique identifier. These identifiers are like labels or codes that make each software component stand out from the others. They provide a standard way to refer to and identify components, making it easier to keep track of them, manage them, and talk about them in the software world. Very important SBOM data is included in the "relationships", which describe the dependencies of the SBOM component and separate them into "includes" and "included in". The former determines which upstream components it is dependent on, while the latter defines which downstream components it is included in, though it is less common. Finally, "license information," while not mandatory, provides better insights by identifying licenses and their terms.

Balliu et al. (2023) present an illustrative example of an SBOM excerpt. For contextual purposes, it is instructive to gain insight into such an exemplar to form a more immediate comprehension of the literal content of the SBOM. The authors also note that the provided example represents a somewhat simplified version, as an actual SBOM would encompass more extensive data. The showcased example pertains to an SBOM excerpt specific to a Java component (async-http-client), aligning with the study's exploration of SBOM challenges within this ecosystem. This example is depicted in Figure 2.3 and is organized, from top to bottom, into metadata, components, and dependencies. The standardized SBOM format, CycloneDX, has been adhered to in this context. An elucidation of distinct formats will be expounded upon later in this chapter. In the example of Balliu et al. (2023), the metadata encompasses information pertaining to the production tool and the project in which the production was conducted. The components encapsulate a concise compilation of data concerning each dependency identified within the project. The "dependencies" element comprises a catalog that delineates the interconnectedness among all the dependencies previously listed. Notably, in the excerpt featured in Figure 2.3, jakarta.activation emerges as a direct dependency of the scrutinized project.

```
{ "bomFormat" : "CycloneDX",
  "specVersion" : "1.4",
  "metadata" : {
    "timestamp" : "2023-02-20T16:14:42Z",
    "tools" : [
      { "name" : "CycloneDX Maven plugin",
        "version" : "2.7.5" }
    ],
    "component" : {
      "group" : "org.asynchttpclient",
      "name" : "async-http-client-project",
      "version" : "2.12.3",
      "hashes" : [ { "alg" : "SHA-512",
          "content" : "e5435852...7b3e6173"}, ... ]
      "licenses" : [...],
      "externalReferences" : [ {
        "url" : "http://github.com/AsyncHttpClient/a
        ↪  sync-http-client"
        ↪  }
      ],
      "bom-ref" : "pkg:maven/org.asynchttpclient/asy
      ↪  nc-http-client-project@2.12.3?type=pom"
    }
  },
  "components" : [
    { "group" : "com.sun.activation",
      "name" : "jakarta.activation",
      "version" : "1.2.2",
      "bom-ref" : "pkg:maven/com.sun.activation/jaka
      ↪  rta.activation@1.2.2?type=jar"
    } ...
  ],
  "dependencies" : [ {
      "ref" : "pkg:maven/org.asynchttpclient/async-h
      ↪  ttp-client-project@2.12.3?type=pom",
      "dependsOn" : [
        "pkg:maven/com.sun.activation/jakarta.activa
        ↪  tion@1.2.2?type=jar"
        ....
      ]
    } ... ] }
```

Figure 2.3: An example of a (CycloneDX) SBOM exerpt (Balliu et al., 2023)

2.2.2. SBOM Generation

Simply put, generating an SBOM involves combining all the used software components and their corresponding component attributes (from Section 2.2.1). However, there are several underlying processes involved. It is important to understand which parties are responsible (and when) for the various steps involved. This will be useful later in the thesis when analyzing incentives. Additionally, this section covers the various tools and formats that are available. The number of these tools and formats is increasing as the SBOM tooling market appears to be exploding in recent years (Xia et al., 2023).

Any entity that develops and supplies software is a supplier, including individual (open source) developers, software vendors, and IT-SIs. These are the stakeholders responsible for generating SBOMs (NTIA, 2019). The ideal scenario is for the SBOM records to be automatically generated as an integral part of the development process. The software components utilized during development must be enumerated directly into a list, including those developed by the supplier and those directly included.

An essential first step in the SBOM generation process is to ensure that it provides a complete, accurate, and auditable record of each dependency built into the final software product (Nadgowda, 2022). SBOMs can be generated using two methods: *pre-build* and *post-build*. In pre-build, the record is created by scanning the source artifacts, resulting in a more comprehensive discovery of dependencies. In post-build, the artifacts are scanned, and an attempt is made to determine the list of dependencies after they have been built (Nadgowda, 2022). Generating post-build, however, often results in a less detailed, and thus less useful, SBOM. For SBOMs to contain detailed information about every layer of dependencies (including dependencies of dependencies, and so on), it would be ideal to initiate the production of SBOMs early in the SSC during OSS development. By including these components in the SBOMs of downstream components as they progress through the SSC, it can greatly enhance the quality of SBOMs.

Generation Tooling

However, it's important to note that the quality of SBOMs is influenced by various factors, and one of those factors is tooling. No matter when they are generated, suitable tooling is required (Xia et al., 2023). There are several open source and

commercial proprietary tools available (all relatively young) that scan directories, binaries, and container images to generate SBOMs (Eggers et al., 2022; Girdhar, 2022). These tools may provide additional functionalities like reporting security, licensing, and operational risks, which would be useful for the consumption of SBOMs (see Section 2.2.3 for details). Some examples of the well-known open source SBOM generating tools include Syft, Tern, Trivy, and Dependency-Track (Girdhar, 2022). These tools, and same goes for proprietary versions, differ in the programming language ecosystems they support and the formats in which they can output their results. Additionally, Github has recently introduced a feature to support the generation of SBOMs. This functionality tracks and updates dependencies in software projects by monitoring their repositories and analyzing the dependency graphs. As a result, individuals are now able to download the SBOM of a repository (GitHub, n.d.-b). The choice of different tools and formats strongly depends on the party, its needs, and its ecosystems. Based on the various roles an organization performs, it should select a tool that best meets its needs (Arora et al., 2022). Different levels of support may exist for specific software components. Moreover, organizations may have different requirements regarding how detailed their SBOMs should be and for what systems they would need it the most.

SBOM Formats

Apart from tooling and the various ecosystems they support, there are differences in the output formats of SBOM tools, which are also crucial for the success of SBOM. Standardized formats enable consistent interpretation and exchange of SBOM data across different organizations and systems. This ensures that the SBOM is understandable and usable by all parties involved in the SSC, from upstream developers and vendors to downstream B2B customers. Three widely accepted formats are SPDX, CycloneDX, and SWID (Phillips et al., 2023). However, considerably fewer SBOM tools appear to be using SWID compared to the other two formats (Eggers et al., 2022). Additionally, other literature seems to focus only on the first two formats (Nadgowda, 2022). Therefore, this thesis excludes SWID.

CycloneDX is a standard format for SBOM that is designed to streamline the process of component analysis in the context of application security and supply chain. It was originally developed within the Open Web Application Security Project (OWASP) community. The format supports widely-used component identity standards, making it suitable for use with both open-source and proprietary software.

SPDX, originating from the Linux Foundation, is an international open standard for SBOM security, license compliance, and supply chain artifacts that can link with similar identity standards as CycloneDX, enabling users to generate SBOMs with little effort. The choice of tool and format depends on the organization's requirements, such as the level of support for specific software components or the desired level of detail in the SBOM.

It is important to note that not all information may be available for SBOM generation, and in such cases, suppliers can provide "best effort" SBOMs. This will result in the 'author' for an included component not being the 'supplier' of the component in the SBOM record (NTIA, 2019). Also, current SBOM generation tools often rely on discovering dependencies managed through package managers, which may not provide a complete picture of all dependencies, as developers may bring in dependencies as pre-compiled binaries or raw code in their build process (Nadgowda, 2022).

SBOM Transformation

Given the variety of potential formats, it is crucial to have tools that enable seamless transformation between these formats without the loss of any critical information (Arora et al., 2022). When organizations use different formats, it is a missed opportunity if they cannot take advantage of certain tools due to formatting limitations. Moreover, with adoption in mind, stakeholders will more likely be reluctant to adopt SBOMs when formatting challenges arise, as it severely hinders the ease of use of the concept. Current transformation tools can translate SBOMs into different formats, files, or integrate them into, e.g., APIs (Eggers et al., 2022). Also, they should allow the combination of multiple SBOMs and other relevant data together for analysis and audit purposes (NTIA, 2021a). For instance, CycloneDX CLI is an example of such tools that enable conversion to other widely accepted formats like SPDX. Conversion from the latter to CycloneDX is also possible and is facilitated by tools like SPDX Golang or SPDX BT (Arora et al., 2022). Additionally, tools that are mentioned for the generation of SBOMs, such as Syft, can also achieve this conversion (Girdhar, 2022).

2.2.3. SBOM Consumption

The SBOMs produced by the stakeholders higher up in SSC are then consumed by B2B customers. The latter then go through the process of SBOM acquisition, for which they need to know that the SBOM exists, where to find it, and how to access it (NTIA, 2021b). Sometimes suppliers can provide the SBOM to customers prior to procurement, allowing customers to make more informed choices about their suppliers. It is then up to the B2B customers, who will be consuming the SBOM, to realize the utility of the concept. The real value only arises when it is used properly (Nadgowda, 2022). The main functions that it aims to fulfill are vulnerability scanning, license auditing, and generating insights into the quality of the codebase.

Consumption Tooling

Many experts agree that software tooling is essential for consuming SBOMs (Xia et al., 2023). Without it, organizations at the end of the chain would often not know how to process or analyze them. There are many different tools available to perform these functions, and they depend on various factors such as the format of the upstream parties and organizational preferences. Generally, the descriptions and functionalities of most tools are similar. Examples include Dependency-Track and Dependency-Check (Dependency-Track, n.d.; OWASP, n.d.-b), which were created by OWASP, the organization behind CycloneDX (OWASP, n.d.-a). These tools allow all software consumers to upload and analyze their SBOMs, particularly for vulnerabilities using suitable vulnerability intelligence. They also provide insights into operational quality, auditing and evaluating license policies, and helping with compliance (Lin, 2023; OWASP, n.d.-c). Another tool for analyzing and consuming generated SBOMs is SCANOSS, which aims to identify vulnerabilities in software components by linking them to the CVE database using the CPE identifier, similar to Dependency-Check (SCANOSS, n.d.). They offer it for free and ensure that organizations can use it safely and anonymously.

SBOM Consumption Challenges

So, consuming SBOMs is on the move, but according to Xia et al. (2023), there is still some difficulty in this area compared to the tooling for SBOM generation. There are also two other critical issues that have emerged from literature over the years. Firstly, there are concerns about the completeness of the dependencies in the SBOM due to the introduction of pre-compiled binaries, raw code, or copied code during the development process (Nadgowda, 2022). For instance, when a developer only copies a few lines of code from a library into his source code without 'formally' importing the library in his code, the SBOM will no longer identify this library as a dependency. This could potentially result in the SBOM overlooking major sets of components, causing there to be "unknown unknowns" (Phillips et al., 2023). However, it is important to note that even a partially complete SBOM is preferable to no SBOM at all (Phillips et al., 2023). While SBOMs significantly decrease the risk of compliance issues and known vulnerabilities, it may not eradicate them entirely.

A second issue identified with respect to the use of SBOM consumption tools is related to the Common Vulnerabilities and Exposures (CVEs) that can be derived from the vulnerability analysis of SBOMs. For example, in many cases, a CVE identified in an upstream component may not actually be exploitable in the software product as it was run by the end B2B customer (NTIA, 2021c). This may be due to the affected component not being loaded by the compiler, not being used at runtime, or the existence of inline protections elsewhere in the software. The fact that the detection of vulnerabilities through SBOM consumption does not necessarily indicate whether a vulnerability is actually exploitable would limit the functionality of SBOM. The problem has been recognized and the NTIA (2021c) has proposed an initiative, the Vulnerability-Exploitability eXchange (VEX), which should partially address the issue. VEX is an artifact that is used in conjunction with an SBOM to provide a standardized way of exchanging vulnerability information between different organizations. It enables organizations to assess the exploitability of identified vulnerabilities in advance and classify them as either affected, not affected, fixed, or under investigation (Eggers et al., 2022). The recommended action then differs depending on the status. The main benefit is that users can better prioritize which CVEs are most relevant to address immediately, reducing unnecessary efforts spent on CVEs that are not actually exploitable. By fixing the most critical vulnerabilities first, organizations can reduce their overall risk exposure and improve their security posture. A big limitation of the initiative, however, is that organizations are still fully responsible themselves to assess the risks for each CVE that is identified by the vulnerability analysis. To do this appropriately it still requires a lot of time and knowledge, despite the help of VEX.

Overall, the lifecycle of SBOM can be divided into two major phases: generation and consumption, each with different stakeholders responsible. The generation of SBOMs is the responsibility of developers, vendors, and IT-SIs within the SSC, while at the end of the chain, B2B customers must ensure that they can actually consume the SBOM. Note that within these two main phases, there are several other processes that are also important for the life cycle of SBOM, such as exchange, transformation, and updates of SBOM. The two phases and their inputs and outputs are explained in Figure 2.4. The responsibilities of each stakeholder throughout the process are visualized in Chapter 4.

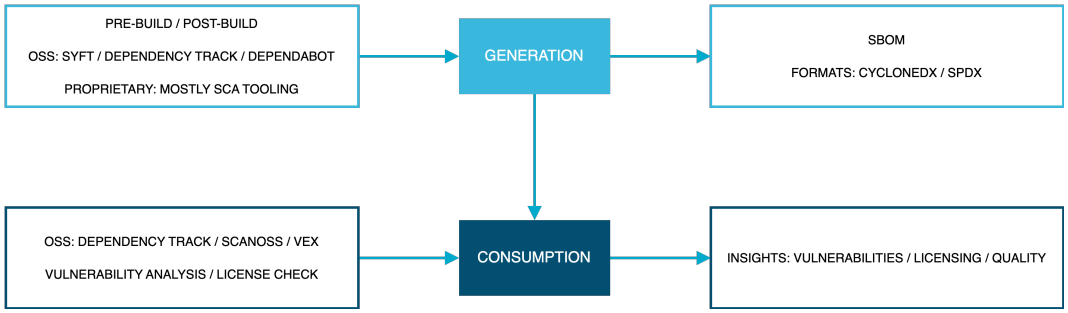


Figure 2.4: The two main phases in the lifecycle of SBOM (own illustration)

2.3. Regulatory Context

The regulatory context is important when it comes to the goal of this research. In order to gain insights into the adoption of SBOM in the software industry, it is important to map out the regulatory context and understand who the key players are, what their roles and (mandated) responsibilities are, and when they are expected to act. This includes all the indicated SSC stakeholders and government agencies. There are ongoing discussions and initiatives in the pipelines that could aim at regulating SBOM in the software industry. As a result, it is essential to monitor and evaluate any forthcoming laws or regulations that may impact the current playing field. This is where the importance of gathering empirical data comes to play. It is also relevant to investigate the perceptions of the different parties involved in the adoption of SBOM within the demarcation of the institutional context. This can help to understand the level of support for SBOM adoption and whether or not they believe it will contribute to the software industry's overall development. In light of this research, it is interesting to examine whether the proposed regulations could be effective or need further adjustments. This requires a critical analysis of the existing regulations and their potential impact on SSCs. The ultimate goal is to ensure that any regulations put in place are effective in promoting the adoption of SBOM and contribute to the overall development of the software industry.

As far as broad and comprehensive regulation regarding cybersecurity, there are currently three relevant EU legislative proposals that may impact the regulatory context of SBOM: the Network and Information Systems 2 (NIS2) directive, Cyber Resilience Act (CRA), and Digital Operational Resilience Act (DORA). In addition to the relevant Dutch/EU institutional context, the SBOM-related playing field in the U.S. will be briefed, too. That will primarily consist of the National Institute of Standards and Technology (NIST) and the EO 14028 (1.6). NIST provides guidelines and best practices for implementing and managing cybersecurity in the U.S., and their standards are often referenced by other countries and international organizations.

2.3.1. Network and Information Systems Directive 2

The current NIS Directive requires organizations deemed essential for the continuity of critical services and digital service providers to take appropriate technical and organizational measures to ensure the security of their network and information systems ("NIS 2 Directive", n.d.). This is intended to protect European citizens at the cyber level by ensuring that companies in critical sectors have good standards of cybersecurity (Dragomir, 2021). A set of standard measures and mechanisms are imposed on them to achieve this. Compared to the initial NIS Directive (2016), NIS 2 regulates ten sectors instead of the previous seven: energy, transport, financial-banking, financial market infrastructure, health, drinking water, wastewater, digital infrastructure, public administration, and space (Dragomir, 2021). Another major difference between the initial and revised directives is the addition of a focus on SSCs. It explicitly aims to strengthen the security requirements for businesses to address the security of their supply chains and supplier relationships, by requiring companies to address their supply chain cybersecurity risks. This also applies to the receiving parties of third-party software products. The proposal aims to enhance cybersecurity in the supply chain for critical information and communication technologies at the European level ("NIS 2 Directive", n.d.). To ensure compliance with obligations to address SSC security, the new directive enables Member States to require essential and important entities to certify specific ICT products, services, and processes under the EU Cybersecurity Act (EPRS, 2023). Compliance is also important for companies because fines can reach up to 5% of turnover (Dragomir, 2021).

SBOM could possibly be a good way to contribute to ensuring security and controlling supply chains. NIS 2 aims to control both technical factors (hardware- and software-related) and non-technical factors (suppliers not from an EU country or state-backed). The transparency that SBOM would bring could obtain both, as it contains both metadata and specific information on the software components used in their software stack.

2.3.2. Cyber Resilience Act

The CRA is a proposed regulation that aims to improve the cybersecurity requirements for products with digital elements (European Commission, 2022). With the increasing use of digital products, the CRA recognizes two problems that arise. Firstly, the lack of cybersecurity leads to widespread vulnerabilities that are not addressed. Secondly, the lack of transparency and understanding of information about products limits businesses and consumers from considering this information when making choices (European Commission, 2022).

CRA aims to establish, regulate, enforce, and harmonize the fundamental security requirements of developing and in-market software throughout their lifecycle (Nguyen, 2023). It has several objectives. Firstly, the security of digital products should improve by making manufacturers incorporate robust security measures by design and through the entire product lifecycle. Secondly, it seeks to establish a coherent cybersecurity framework that makes compliance easier for hardware and software producers. By providing clear guidelines and standards, the program helps ensure that all products meet a minimum level of security. Thirdly, the program aims to enhance the transparency of security properties for these products, which enables businesses and consumers to make informed decisions about the products they use. By providing clear information about security features and vulnerabilities, the program promotes accountability and encourages manufacturers to prioritize security in their product design. Finally, CRA seeks to enable businesses and consumers to also use digital products securely. The program aims to reduce the risk of cyber attacks and other security threats.

As the EU looks to various bodies to begin developing standards, one strategy relating to impending reporting obligations stands out: the importance of a SBOM in the CRA. According to a blogpost by Fox (2022), SBOM is cryptically defined in the CRA with the ability to recall, meaning that the entire supply chain must be better and more actively managed than before. This is what has been missing until now. Furthermore, when considering the objectives of the CRA, the third objective stands out in particular. The fact that the Act aims to enhance transparency of software products for customers aligns with the functionality and the primary benefit of SBOM, as described and identified throughout this research.

2.3.3. Digital Operational Resilience Act

DORA is the most relevant Act in the European Union (EU) concerning operational resilience (European Parliament, 2022). Although it is specifically aimed at the banking sector, it is still relevant to consider in an exploration of SBOM. The banking sector is a leading sector in terms of cybersecurity, as financial institutions are often targeted by cyber attacks due to their possession of highly sensitive data and assets (CSIS, n.d.). DORA addresses the need for managing ICT risks and sets rules on ICT risk management, incident reporting, operational resilience testing, and third-party risk monitoring. This last requirement presents an interesting opportunity for SBOM, as DORA emphasizes the importance of managing and monitoring third-party risks, requiring financial entities to define a holistic ICT view and identify all key dependencies of third-party suppliers (European Parliament, 2022).

The requirement for third-party risk monitoring within DORA suggests the adoption of SBOM as a best practice for managing third-party software risks. Rispens (2021) proposes that SBOM should be explicitly added to DORA, as general ideas on how to manage third-party risks need to be more concrete. By having a clear understanding of the software components used by third-party service providers, regulated entities can better manage their operational resilience and ensure that their critical systems are adequately protected against cyber threats. SBOM can also assist in compliance efforts by providing a clear and auditable record of the software components used in regulated entities' critical systems and those of their third-party service providers. As the banking sector is often at the forefront of regulatory developments, any requirements imposed through DORA are likely to be adopted more widely.

2.3.4. Regulatory Context for the U.S.

There have been notable developments outside of Europe that are worth considering in relation to SBOM, which may indicate the added relevance of this concept. For instance, the Biden Administration has signed an executive order aimed at enhancing the "Nation's Cybersecurity": Executive Order 14028 (Young, 2021). The National Institute of Standards and Technology (NIST), the leading agency for technology and cybersecurity standards in the U.S., is tasked with creating guidelines and recommendations for practices that improve the security and management of SSCs of organizations. In the meantime, this has evolved into the SBOM being actually mandated for suppliers who intend to provide software to government entities (CISA, n.d.; Riegelsville, 2023). According to NIST (2022), they see the provision of greater transparency into the components used in software products as a means by which organizations can better understand their risk exposure and take steps to mitigate those risks. This aligns with NIST's overarching goal of improving the cybersecurity standards in the U.S. Therefore, the mandate for SBOMs in the U.S. government's SSC can be seen as a significant step towards improving software security and supply chain management.

3

Research Methodology

The problem and its main theoretical, technical, and institutional context have been established in the previous chapters. Based on that, initial ideas have also been identified regarding potentially interesting aspects to research. This chapter presents the chosen research methodology for the thesis and formulates a concrete research plan. The chapter starts by explaining the research approach in Section 3.1. An exploratory research approach was selected to address the main research question. This choice was made because there is a lack of current research on the specific topic, and thus this approach can be used to develop new theories. The theory to be developed is the comprehensive understanding of how incentives or disincentives among key stakeholders of SSC impact their adoption behavior towards SBOM.

Next, Section 3.2 elaborates on the data collection and analysis methods used to achieve the objectives of the research approach. This includes conducting desk research and interviews to obtain empirical data, as well as applying a thematic analysis as a method for theory coding and building grounded theory. To give more weight to the identified themes, a frequency analysis is also applied to them. Considering the volume of the gathered findings, further aggregation and a SWOT analysis are also applied for each stakeholder group to present the most significant findings more comprehensively. To ensure sufficient interviews were conducted to draw meaningful conclusions from the data, a total of 16 interviews were carried out. The quantity of interviews is one specific data requirement, and further requirements will be addressed in section 3.3. This section will also establish additional requirements for the data analysis that will be applied in the research. Additionally, the limitations of each research method are also discussed in this section.

3.1. Research Approach

Given that this research aims to contribute to filling the current lack of scientific literature on the topic of the relationship between misaligned (dis)incentives within the SSC and the adoption of SBOM, using an exploratory research approach is appropriate. This is, for example, in line with Brown (2006) who states that exploratory research "*tends to tackle new problems on which little or no previous research has been done*". Elman et al. (2020) argue that by using the approach, new information and a deeper understanding about a topic can be generated by collecting and analyzing empirical data. This can provide a foundation for further research and possible solutions, which is exactly the aim of this study. Elman et al. (2020) even state that exploratory research is "*the soul of good research*". "*Without the ambition to say something new, research would come to a standstill*".

Like any other research approach, exploratory research has both advantages and disadvantages. Important advantages are: research costs are relatively small, the flexibility to change along the way, the fact that it can lay good groundwork for further research, and it can possibly save time if it assesses early on whether it is worth pursuing a topic (BRM, n.d.). Important disadvantages to take into account are, for example, that this form of research is subject to bias in the interpretation of qualitative data, there may be too low a sample size in data collection, and that you do not necessarily know that something novel will actually come out of it (BRM, n.d.; Elman et al., 2020).

In order to answer the main question for this thesis in constructive detail, a structured plan of action is needed. To achieve this, the research is divided into three phases, each with its own sub-question. These are identified in the introduction (see Section 1.5, and in this section a plan of action is attached to it on how to answer these specific questions. First, it will determine for each particular sub-question what the required data will be. Subsequently, in the next subsection, it determines which research methods and tools are then appropriate to obtain it.

SQ1: What are the most important SSC stakeholders involved with SBOM?
The identification of stakeholders within the general SSC and their interrelationships concerning SBOM has, as of yet, not been comprehensively addressed in literature on SBOM. For instance, the role of IT-SIs within the SBOM ecosystem remains relatively unclear. This research question aims to obtain this understanding. Based on the insights, a relevant selection of stakeholder groups are made for interviews, considering potential variations within stakeholder groups that should be either taken into account or disregarded.

SQ2: What are the (dis)incentives and capabilities of SSC stakeholders regarding SBOM?
This sub-question aims to exploratively research the (dis)incentives and capabilities of key stakeholders towards SBOM. The (dis)incentives that play a significant role within the SBOM ecosystem are currently not clear. Moreover, there has been a limited focus on the (technical) capabilities regarding SBOM, particularly concerning IT-SIs. Understanding these aspects directly from the stakeholders themselves, while trying to minimize potential bias, is crucial for obtaining accurate information. The approach involves soliciting information from stakeholders to gain insights into their motivations and abilities. To ensure an unbiased collection of data, the research will employ methods that promote open and transparent communication. By creating a neutral and non-judgmental environment, it aims to encourage stakeholders to provide honest and unbiased information regarding their (dis)incentives and capabilities.

SQ3: What factors can explain the lack of SBOM adoption?
Based on all the gathered data, this sub-question seeks to discover the most relevant information that can be derived from it. The data will be analyzed to gain insights and make the primary factors hindering the adoption of SBOM more apparent. During the analysis, patterns, trends, and recurring themes within the data will be identified. Special attention will be given to any significant variations or outliers that may provide valuable insights into the underlying factors that contribute to the resistance or reluctance towards SBOM implementation. The findings up to and including this third sub-question will also be presented in a session with a field expert. This will be done to determine if they agree with the various results, thereby increasing the validation of the findings. This should contribute to the scientific robustness and substantiation of the thesis.

3.2. Data Collection and Analysis Methods

The data sought by each sub-question is now defined. The approach and methods to obtain this data are elucidated in this section. Each sub-question is explained in detail, followed by a critical reflection on the methods in Section 3.2.1.

SQ1: What are the most important SSC stakeholders involved with SBOM?
The first research sub-question will be initiated by conducting extensive desk research, including literature reviews and document analysis of available and relevant publications. Since the amount of literature, particularly focused on specifically European-oriented SSCs, is limited, this step is crucial to gain clarity as an initial research step. Moreover, based on the findings, various choices and delineations will be made regarding the stakeholders. It is important for the further progress of the research to determine the stakeholder groups from which gathering data would yield the most insightful and relevant information, taking into account the time constraints involved. Given the constraints, the research will need to focus on the key players within the SSC regarding SBOM. These choices have been made based on the findings and in close consultation with supervisors from both TU Delft and Northwave.

SQ2: What are the (dis)incentives and capabilities of SSC stakeholders regarding SBOM?
An issue identified in the first chapters regarding the main problem is the fact that little has been published on why SBOM has not been widely adopted yet. This is where the exploratory research can be continued through interviews with open-ended questions, which is, after all, an appropriate tool to gather non-documented information (Alshenqeeti, 2014). Moreover, for this research approach, it is "*the most popular primary data collection method with exploratory studies*" according to BRM (n.d.). Interviews will be relevant for gathering insights into the experiences, behaviors and beliefs of these experts (Alshenqeeti, 2014).

Multiple steps were involved in developing the interviews. Initially, in collaboration with supervisors, the required information for addressing the formulated research questions was determined. This primarily encompassed the information needed to address the research questions. Based on this, appropriate questioning techniques were formulated, leading to various segments in the interviews. The interviews began with open-ended, semi-structured questions. This approach aimed to allow participants to express their own experiences, opinions, and perspectives, thereby minimizing potential researcher bias. These findings were considered of paramount value and deemed most significant, as participants provided responses to these questions independently, without the interviewer's influence. After the fully open-ended segment, the questions became more specific to (dis)incentives. To formulate these questions, a literature review was conducted in

Chapter 5, encompassing the available literature on SBOMs related to forms of (dis)incentives. This review also included literature that addressed the latter for similar security technologies. The themes and factors derived from this review were integrated into the more (dis)incentive-specific interview questions and validated with the participants. The final segment aimed to generate more quantitative results. Participants were asked to assess certain (dis)incentive-related statements regarding SBOM, indicating the extent to which they believed these hypothetical statements would facilitate or hinder SBOM adoption. These statements were also formulated based on the identified findings from the literature review.

While the questionnaire is largely the same for all stakeholder groups, some specific adjustments were made for each group using a bottom-up approach. This approach entails starting with specific details for each stakeholder and then aggregating the information to draw more general conclusions (Gibbons, 2022). A comprehensive explanation of the interview structure, including explanations of (question) choices, can be found in Section 5.2.

After the initial version was developed, it underwent rigorous testing to further enhance its quality. Test runs, including pilot interviews for the semi-structured, open-ended section, were conducted. Pilot interviews play a crucial role in qualitative research as they allow for testing and refining questions and provide practice prior to the actual interviews (Majid et al., 2017). For the section involving statements and ranking, cognitive interviews were conducted to ensure clarity and minimize ambiguity in question interpretation, which is often an issue for these methods (García, 2011). Both methods were performed with employees from Northwave representing various job functions, including both technical perspectives and management/strategic viewpoints on such matters. Based on the acquired knowledge, insights from these methods, and feedback received, the questionnaire was subsequently refined and adjusted.

Subsequently, the interview participants were approached. The guideline followed was to conduct interviews with stakeholder groups by going through the SSC starting from the end (downstream), consisting of the consumers of third-party software, being the B2B customers. Next, the IT-SIs and software vendors were approached, and the interviews concluded with gathering empirical data from developers. In addition to the order in which participants were approached, they were also asked to sign a consent form. The main message and persuasive factor for their cooperation, as stated in the form, is that all results will be anonymized when processed for the thesis. Additionally, the form also highlights the necessary measures taken regarding data processing.

SQ3: What factors can explain the lack of SBOM adoption?

To analyze and transform the collected dataset into relevant findings and build theory, appropriate data analysis methods must be chosen, which vary depending on the phase of data collection methods. Firstly, the collected outcomes from the semi-structured interview questions, which comprise the largest amount of data, are analyzed. A well-known method for analyzing qualitative data is thematic analysis (Caulfield, 2021), following a six-phase process: exploration, coding, theme identification, revision and refinement, defining and organizing, and presentation (Braun & Clarke, 2006). Thematic analysis is an effective method for identifying, analyzing, and reporting patterns (themes) within the data, providing insightful analysis that addresses specific research questions (Braun & Clarke, 2006). The details of each step in thematic analysis are further explained in Chapter 6. The purpose of this method is to develop grounded theory, for which it is particularly suitable (Heydarian, 2016). It serves as a means to introduce new concepts that emerge directly from the data without imposing preconceived notions (Makri & Neely, 2021). The grounded theory approach allows researchers to gain insights into how stakeholders perceive and interpret reality (Suddaby, 2006). In other words, researchers can "see" the research problem through the eyes of practical stakeholders, rather than solely relying on a literature analysis, leading to more practical and targeted solutions (Makri & Neely, 2021). This approach also aligns with the goals of the exploratory research methodology. In addition to the gathered findings from the thematic analysis, a frequency analysis is also applied to the identified themes. This addresses a significant limitation of solely relying on a thematic analysis, which lacks significance attribution to the themes (Getthematic, n.d.). For instance, if a particular theme is mentioned by only one participant while another theme is mentioned by 80% of the participants, there is a difference in the perceived importance of these factors for the overall SSC.

For analyzing quantitatively generated data from the ordinal preference ranking method, different data analysis methods are employed. An important aspect of analyzing ordinal preference ranking data is to examine the distribution of scores for each statement (Bhandari, 2022). Measures such as mode and median are calculated to determine the central tendency and assess the level of agreement or disagreement among participants. This analysis provides an understanding of whether people uniformly agree or disagree with certain statements and allows for comparisons across stakeholder groups to evaluate potential differences in perceptions and priorities. Rank order analysis is crucial for identifying statements that significantly contribute to or hinder the concept under study (Bhandari, 2022). By calculating the average ranks assigned to each statement, those consistently receiving high or low rankings can be identified. This analysis helps to identify the most impactful or challenging statements, providing insights into areas that require attention or improvement. Further details of these methods are elaborated in Chapter 6.

However, after executing the analysis methods for this third sub-question, it proved advantageous for the comprehensiveness of the thesis to iteratively include an additional SWOT analysis with a number of preparatory steps. Despite the

interesting and relevant novel findings that had been gathered up to that point, the volume of these findings and their presentation appeared extensive, lacking clarity on the primary incentives and disincentives for each stakeholder group regarding their adoption behavior towards SBOM. In order to address this, Section 6.4 is introduced. Within this section, the researchers aggregate all the accumulated themes, condensing them into a more manageable quantity. Furthermore, these iteratively aggregated themes are compared with the ex-ante identified (dis)incentives outlined in Section 5.1. As the final analysis in Chapter 6, the SWOT analysis is conducted. This method is frequently employed by establishments, often business enterprises, to explore their Strengths, Weaknesses, Opportunities, and Threats (Namugenyi et al., 2019). Its business-oriented focus aligns well with the scope of this research on the SSC and its stakeholder groups. Organizations often utilize the insights derived from SWOT analysis for strategic planning, quality control, and formulating policy and regulation. As a result, the concluding and future-oriented sections can directly engage with concrete points emanating from this analysis.

3.2.1. Reflection on Research Methods

Research methods and tools and its subsequent data are never quite perfect (Adèr & Mellenbergh, 2008). This is the first reason why it seemed appropriate for this research to use a mixed methods approach. In this way, all individual limitations of methods are tried to be mitigated and thus provide the most comprehensive perspective (Kipo, 2013). The reasons for the choice of research methods and tools have been mentioned in the previous section. However, the limitations and disadvantages of them have yet to be addressed. First of all, the research relies heavily on the extensive use of interviews for empirical data gathering. Despite the good qualitative information one can gather with these, they are known to be very time-consuming, the anonymity of respondents is sometimes compromised, they are very difficult to analyze and compare, and it actually requires a very skilled interviewer (Alshenqeeti, 2014). Representativity could also possibly be an issue due to the relatively small number of participants.

A literature or document review, while valuable in academic research, has some drawbacks worth considering, too. For example, the method can be time-consuming due to the extensive effort required to thoroughly review and analyze a substantial body of literature (Amoako, 2014). Additionally, one limitation is the possibility of limited or incomplete data, as not all sources may provide comprehensive or extensive information on the research topic.

Ordinal preference ranking as a method for gathering more quantitative data also has several limitations. Firstly, it exhibits limited granularity, as it enables participants to rank items based on preferences but fails to capture the magnitude or intensity of those preferences (Cook, 2006). Consequently, it provides information solely regarding the relative order of preferences without quantifying the extent of variation between ranked items. Secondly, ordinal preference ranking presents challenges when comparing the preferences of different groups or individuals. Relying solely on ordinal rankings makes it difficult to determine if the differences observed in rankings are statistically significant or meaningful, particularly in the absence of supplementary information or measures.

Moving on to the mentioned data analysis methods, first, thematic analysis on qualitative data. One issue that can arise is subjectivity (Nowell et al., 2017). The analysis involves a significant amount of interpretation, which means that different researchers could theoretically interpret the data differently. This subjectivity can introduce bias and compromise the reliability and consistency of the analysis. The lack of a predefined structure also adds complexity. Since the analysis can be flexibly approached and themes emerge organically, it becomes more susceptible to the same subjectivity and researcher bias. Lastly, there is the potential for oversimplification. Considering a large amount of data within a limited number of themes may oversimplify the information, potentially leading to the loss of other relevant acquired information.

3.3. Data Requirements

To ensure that the collected data is of sufficient quality to draw relevant and valid conclusions, it is important to establish specific data requirements in advance. These requirements pertain to aspects such as the execution of methods, data processing procedures, and more. It is also important to consider these requirements to mitigate the potential limitations or shortcomings of the research methods. All the various data requirements and measures to strive for compliance are presented in Table 3.1.

Table 3.1: Overview of Data Requirements and Fitting Measures

Data Collection Method	Data Requirements	Fitting Measures
Literature Research	• Relevant research papers and articles • Completeness and comprehensiveness of literature sources • Availability of recent and up-to-date information	• Consult mainly scientific research engines and use relevant search terms. • Avoid selecting sources only from authors without technical background. • Pay attention to recent and current sources.
Interview	• Effective questions that contribute to the research questions • Minimal bias in the questions • Sufficient number of interviews for meaningful findings	• Aim to interview participants from various organizations • Conduct test runs with individuals from different job functions to refine the questionnaire and address potential ambiguities • Target a minimum of 5 interviews per stakeholder group • Seek participants with diverse job descriptions to approach the research problem from different perspectives • Begin the interview with open-ended questions to avoid bias • Conduct the interviews in the participants' preferred language
Ordinal Preference Ranking	• Minimize ambiguities in the statements • Statements should be relevant to the research questions • Standardized scale for participants to assess the statements	• Categorize the statements into different incentives • Use a Likert scale • Seek participants with substantial experience • Include participants with diverse job descriptions to approach statement preferences from different perspectives

4

Stakeholder Analysis

Some of the key stakeholders involved in the SSC have already been identified (see Figure 1.1). However, a comprehensive understanding of all the parties involved in the SBOM lifecycle throughout the SSC has not yet been addressed, and that is the main focus of this chapter. From this point on, the report will start to address the research sub-questions. This chapter provides an answer to sub-question 1:

> **Sub-question 1:**
> What are the most important SSC stakeholders involved with SBOM?

To illustrate this, various diagrams will be used. For example, the Swimlane Diagram in Figure 4.1 aptly illustrates the progression of cross-functional SBOM processes throughout its lifecycle across different stakeholder groups in the SSC. Subsequently, the value streams are visualized in Figure 4.2. This thorough exploration of the value streams help us develop insightful questions that will provide the necessary information to answer the research questions. By understanding which parties are involved and determining their level of involvement, we can identify the most important stakeholder groups participating in the SBOM lifecycle. This directly informs the selection of stakeholders to approach for interviews. Furthermore, potential differences within these groups are examined, determining what should be included and excluded. A comprehensive reflection on these choices are provided, ex ante.

4.1. Identifying SBOM Stakeholders

Throughout the thesis, many of the important stakeholders have already been mentioned and included in process descriptions. For instance, in the general description of the SSC in Chapter 1, and subsequently in the lifecycle of third-party software and its associated SBOMs in Chapter 2. In the latter, various tasks and responsibilities have also been identified. However, not everything has been covered yet to have a holistic, comprehensive overview of the stakeholder landscape and the underlying responsibilities, influences, and relationships within it.

The introduction about the SSC has mapped out four distinct groups. The lifecycle of third-party software begins with developers who are responsible for (open source) repositories, libraries, APIs, and other components. These software components are included by developers of software vendors in their own commercial products. Depending on the products and the ultimate B2B customers (and their IT infrastructure), an IT-SI is also involved. The IT-SI is responsible for integrating and adapting the software products to the infrastructure of the B2B customer.

Then in Chapter 2, initial insights were provided into other stakeholders involved in the lifecycle of SBOM. In this context, relevant legislation and regulations, primarily at the EU level, were discussed. Various institutional parties such as the European Commission and the European Parliament are involved in the SSC and its security. Examples of this involvement include NIS 2, CRA, and DORA (Chapter 2.3). Through legislation and regulations, these parties can significantly influence the potential adoption of SBOM. The focus of legislation is increasingly shifting towards securing and assuming responsibility for the SSC.

In the technical context of SBOM, it also became apparent that different entities have been responsible for establishing initiatives related to SBOM formats and suitable tooling. Open-source organizations such as OWASP and the Linux Foundation have been involved in developing SBOM formats. As for the tooling, there are various parties involved in either generation tools, consumption tools, or both. Both commercial and open-source entities play a role in this domain,

but there is still no clear delineation of which parties are dominant. For this chapter, these parties involved in either tooling or standardization will be classified under the stakeholder group 'SBOM contributors'.

A stakeholder group that has not been addressed thus far are the external security companies. These companies are frequently contracted by organizations throughout the entire supply chain, irrespective of the stakeholder group. The responsibilities of external security companies encompass various tasks, such as performing vulnerability assessments and conducting penetration testing. They extensively evaluate software systems to identify vulnerabilities and weaknesses, simulating potential attacks through penetration testing. This enables them to assess the efficacy of existing security measures and offer recommendations for improvement. Additionally, security companies are actively involved in conducting security audits and ensuring compliance with industry standards and regulations. They help organizations in evaluating their security practices, identifying any gaps or areas of non-compliance, and providing guidance on how to enhance security measures. These audits play a critical role in maintaining a secure SSC and mitigating potential risks. It's worth noting that the extent to which organizations hire external security companies may vary depending on their size. According to a study conducted by the CBS in 2019, smaller companies with 2-10 employees outsourced approximately 31% of their security to external companies. On the other hand, larger companies with 250 or more employees outsourced around 67% of their security-related duties (CBS, 2022).

4.1.1. SBOM Lifecycle: Cross-Functional Processes

What all these different stakeholders and their process tasks throughout the lifecycle of SBOM look like are visualized in Figure 4.1, utilizing a Swimlane Diagram. Such diagrams are suitable for depicting inter-organizational relationships, each within their own distinct "swimlane" representing their sub-process within the overall process (Dussart et al., 2002). They provide a straightforward way to illustrate the involvement of all stakeholders, who, when, and what tasks they undertake.

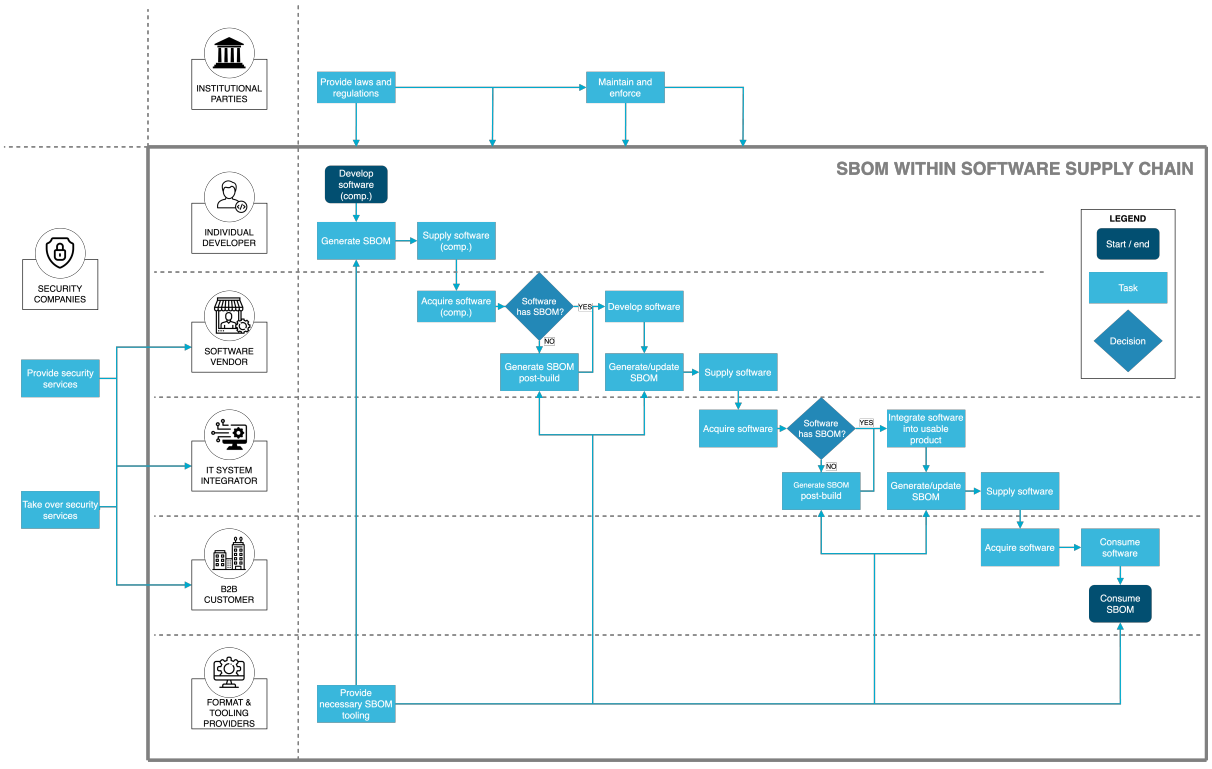


Figure 4.1: Swimlane Diagram for inter-organisational SBOM ecosystem (own illustration)

The above diagram is a normalized representation of how cross-functional processes unfold. An important element that is hard to show in the depiction is that within an SSC, there is rarely just one single developer involved. They themselves also typically use components built by other developers, which means that software components within that stakeholder group are formed by dependencies of dependencies, and so on. The software that reaches software vendors and integrators often consists of numerous layers of dependencies. It is crucial to keep this in mind when examining the diagram. In an ideal SBOM ecosystem, as mentioned in the technical background (see Section 2.2), all developers would generate SBOMs for

the components they build. This would mean that the corresponding SBOMs of professional software vendors would ultimately consist of a deep, comprehensive layer of all dependencies. However, the fact that numerous dependencies arise from interactions among developers makes this goal challenging to achieve. This lays the foundation for the "post-build" SBOM generation, which is why the conditional approach has been chosen to indicate whether the next sub-process begins with the next stakeholder: whether the SBOM has been produced and/or delivered. Subsequently, a post-build production task has been added. However, despite including it in the diagram, there are legitimate concerns about the quality of SBOMs that can be generated by post-build tooling. It is often impossible to precisely determine what a developer has done and which third-party components they have integrated into the codebase. Therefore, although efforts can be made for post-build SBOM production, it is possible that the final SBOM received by the B2B customer only contains detailed and accurate information from the stakeholder who started tracking SBOMs during the development process. Ultimately, the decision to include it in the diagram is also based on Phillips et al. (2023), who argue that at the end of the day, even a partially accurate SBOM is still better than no SBOM at all.

Government entities, in the context of the Swimlane Diagram, currently do not directly deal with SBOMs. At least in Europe, there is currently no legislation mandating SBOMs, whereas the U.S. has already introduced such regulations. As a result, the tasks assigned to government entities are described in a more generalized manner. One of their main focuses regarding cybersecurity revolves around laws concerning supply chain risk management.

On the other hand, the stakeholder group of the external security companies is also assigned tasks with a more generic scope. This is primarily due to the absence of a unified concept within the literature regarding their specific responsibilities in relation to SBOMs. Consequently, the tasks attributed to these entities remain aligned with their core business functions. However, there have been some initial proposals regarding SBOM-related activities. Within the service provision domain, these security companies could potentially assist clients in understanding SBOMs on a service-based basis. This assistance could include aiding in the integration of SBOMs for clients and facilitating the consumption of SBOMs. Additionally, they may contribute to assessing the quality of SBOMs to ensure their reliability. Regarding the takeover of services, these companies, for example, manage the Security Operations Centers (SOCs) of their clients. Through this arrangement, the latter entrusts their entire security monitoring operations to an external security company. In the context of monitoring, a security company could consume SBOMs to enhance their capabilities and provide comprehensive security monitoring services.

These proposed tasks illustrate potential areas where government entities and security companies could contribute to the SBOM ecosystem. As the understanding of SBOMs continues to evolve and consensus on specific tasks emerges in the literature, further refinement and specialization of their responsibilities can be expected. Although these stakeholder groups are not included in the empirical data collection, in a later phase, an examination will be conducted to determine whether relevant further recommendations can be formulated for both parties to potentially consider.

4.1.2. Stakeholder Values

The Swimlane Diagram provides clarity on how specific processes flow by illustrating the tasks, responsibilities, and handoffs among various participants. It is an effective tool for visualizing process workflows and identifying potential bottlenecks or inefficiencies. However, it is equally important to complement the Swimlane Diagram with a Value Stream Diagram to gain a comprehensive understanding of the overall value delivery processes and its significance for stakeholders involved. After all, the SBOM processes are interesting, but without the right value streams for every stakeholder group, they will probably not mean too much. Every entity expects to receive a value stream in return for their actions. The Value Stream Diagram maps out the end-to-end flow of value creation, which provides a holistic view of the entire value stream. Perhaps it can enhance the research, later on, by facilitating a more comprehensive interpretation of how specific interests are intertwined or impacted by particular value streams.

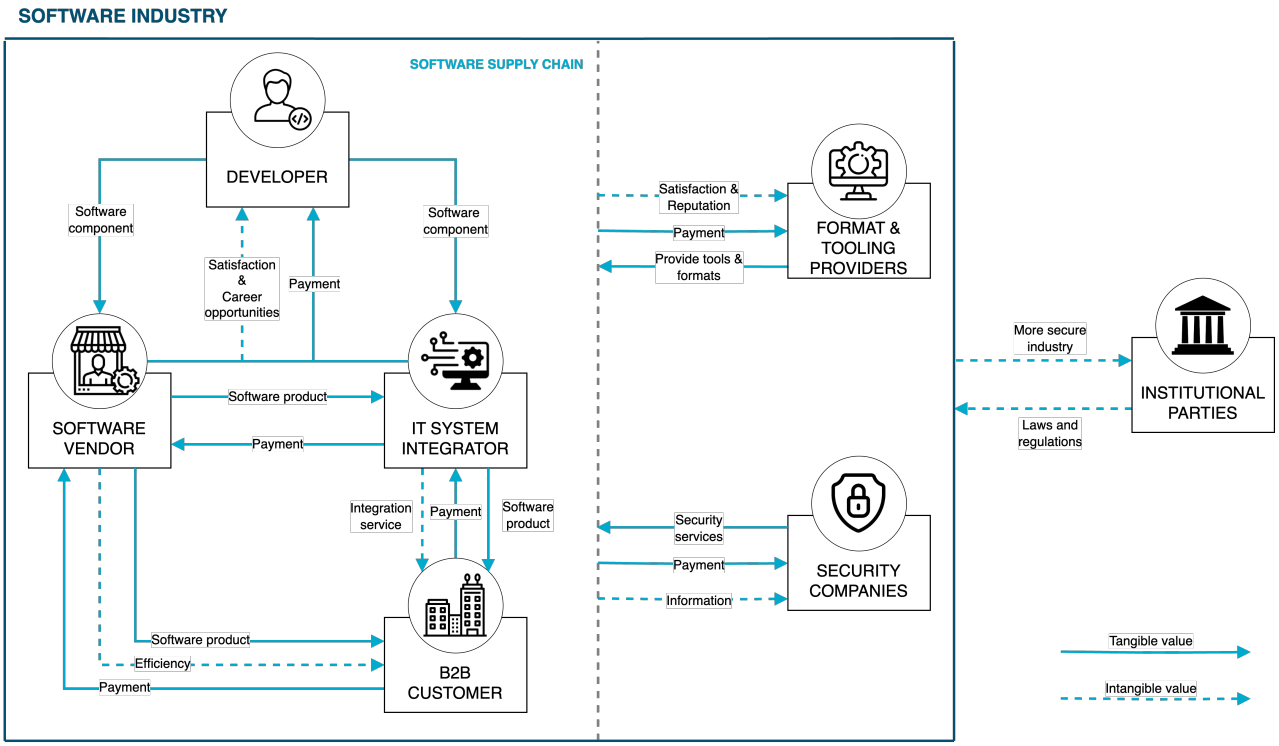


Figure 4.2: The Value Stream within the SSC (own illustration)

This value stream diagram presents a generalized representation of the software industry's workflow. Similarly, for these value streams, their characteristics depend on the software's architecture and how it progresses through the SSC. If it bypasses the IT-SI, for instance, the interrelationships between B2B customers and the IT-SI will not be applicable. In many cases, software vendors themselves take the responsibility for integration services. The payment structures can also vary between customers, IT-SIs and vendors. It depends on the agreement between the software vendor and the system integrator. In some cases, the system integrator pays the software vendor for the software and the customer pays the system integrator for their services. In other cases the B2B customers pay both. There are also instances where developers directly sell to B2B customers, although this occurrence is not customary. Hence, these streams have been omitted from this diagram. The research focus does not lie on those particular streams and transactions and, therefore, they have been scoped out of the analysis.

4.2. Determining Key SBOM Stakeholders

Throughout the thesis, and specifically within this stakeholder analysis, a total of seven stakeholder groups have been identified (see Table 4.1). As previously mentioned, not all of these groups will be included in the empirical data collection phase of this research. The researchers have made a well-founded decision to select the most significant stakeholders who have influence on the lifecycle of an SBOM. These are the stakeholders who will need to adopt the concept. By scoping the data collection to a smaller number of stakeholder groups, it becomes possible to conduct more interviews with experts within these groups compared to including all stakeholder groups. Consequently, this approach will yield considerably more valid results in the end.

Table 4.1: SBOM Stakeholders

All Stakholders Involved with SBOM
B2B Customers of third-party software
IT System Integrators
Software Vendors
Developers
Institutional Parties
SBOM Contributors
Security Companies

To make a selection from the aforementioned seven stakeholder groups, the focus will be on identifying the stakeholder groups considered to be the most directly involved with SBOM throughout its lifecycle. The parties consist of the four stakeholder groups identified within the SSC (Chapter 1). These groups represent the direct decision-makers, users, and producers within the SBOM ecosystem. With regard to SBOM, they are likely to have diverse and potentially conflicting incentives. Understanding these differences can provide insights into the challenges, trade-offs, and potential solutions associated with SBOM adoption. By prioritizing these groups, the research encompasses a broad range of perspectives while maintaining a manageable scope. Thus, Table 4.2 serves as the selected foundation for further investigation in this study.

Table 4.2: Key SBOM Stakeholders

Key Stakholders Involved with SBOM
B2B Customers of third-party software
IT System Integrators
Software Vendors
Developers

4.2.1. Excluded Stakeholder Groups

A deliberate decision has been made to exclude the contributors involved in standardized SBOM formats and SBOM tooling from the list of key SBOM stakeholders. While it is acknowledged that they play a crucial role in the entire SBOM ecosystem, their significance as influential stakeholders in the context of this study, which aims to explore potentially conflicting incentives, is considered relatively less pronounced. Regarding the format providers, their role revolves around the provision of clearly defined SBOM formats. These formats are typically developed by open-source parties with no significant commercial interests. Consequently, for the purpose of this research, they are excluded as pivotal stakeholders. Their main objective is simply to contribute to the overall success of SBOM by offering transparent and standardized formats. As for the tooling providers, the landscape is characterized by a lack of uniform guidelines regarding the best or most widely used tools. There exists a multitude of diverse tooling options available. While they may not be directly involved in the SBOM lifecycle, their involvement does intersect with it. Tooling providers have a degree of relevance due to their association with SBOM practices, albeit without a direct and definitive impact on its lifecycle.

Furthermore, the exclusion of institutional parties from the analysis is based on the assumption that their influence on SBOM adoption, as governed by existing legislation, may be relatively limited. However, it is worth noting that if institutional parties were to enforce SBOM adoption through regulatory measures, it would undoubtedly serve as a powerful incentive for all stakeholders to comply. Nevertheless, the research aims to shift its focus towards a more direct examination of the stakeholders involved in the SBOM ecosystem, exploring the underlying reasons for the limited widespread adoption of SBOM, particularly in the presence of other more 'organic' incentives.

In addition, the third and final stakeholder group excluded from the analysis comprises cybersecurity companies. These entities are also positioned outside the immediate lifecycle of SBOM. The specific role they would play within the SBOM framework remains largely unknown, despite preliminary considerations made in this thesis. Although their expertise and contributions in the realm of cybersecurity are highly valued, their precise role and responsibilities within the context of SBOM have yet to be fully defined and understood.

By narrowing the focus to the most influential stakeholders, specifically those directly impacting SBOM adoption, the research endeavors to capture a comprehensive range of perspectives while maintaining a manageable scope. Therefore, the aforementioned stakeholder groups have been excluded from the key stakeholder selection, as their roles and (dis)incentives

align differently compared to the primary stakeholders analyzed in this study. This approach allows for a more targeted exploration of the dynamics within the SSC and provides valuable insights into the factors influencing the broader acceptance of SBOM.

4.3. Stakeholder Group Distinctions

The previous section has provided an overview of all the stakeholders involved in the SBOM lifecycle. The selection of stakeholders to be included in the empirical data collection for this research has also been clarified. However, within certain identified stakeholder groups, significant variations are also to be expected. This section will address the levels of distinction within these groups, where relevant to the research. Subsequently, a systematic approach will be determined to address these distinctions. Distinctions between individuals, such as personal traits, will be disregarded. To ensure a diverse and comprehensive representation of perspectives and to gather results that are as broadly valid as possible, aligning with the established data requirements, the research aims to engage with individuals from a wide range of organizations. While some participants may work at the same organization (maximum of 2), the majority will be from different organizations, promoting a diverse participant pool. By incorporating participants from diverse backgrounds and organizations, the research seeks to obtain a comprehensive understanding of the dynamics within the SBOM ecosystem. This approach enhances the robustness and validity of the findings, providing valuable insights into the complexities surrounding SBOM adoption and its implications across various stakeholders.

4.3.1. Stakeholder Groups Without Distinctions

To begin with, let's focus on the stakeholder groups where differences are considered negligible: the developers and the IT-SIs. While there may be inherent variations within the demographics of these parties, the researchers have valid reasons to believe that these differences would not significantly impact their interests in SBOM. However, in order to completely eliminate any potential influence of demographics, an explicit delineation is provided regarding which parties will be included in the study.

Developers

Regarding the developers, they will be selected based on their contributions and/or interest in open-source repositories related to SBOM. This primarily includes various projects focusing on the tooling required for either producing or consuming SBOMs. The selective nature of this group necessitates that the research does not make further distinctions within it. The motivations for their contributions can stem from both value-based intrinsic factors aimed at making the software industry more efficient and of higher quality, as well as more tangible and commercial values (Taylor & Dantu, 2021). However, this distinction is disregarded for the purposes of this study. In these early stages of SBOM, the assumption is made that all OSS developers will strive to create optimal tooling that contributes to the adoption of SBOM. By focussing on this specific target group, the interview process will become easier due to the guaranteed knowledge on the subject.

It is important to note that one developer from a commercial IT-SI company was interviewed. However, considering that the responses provided insights for the entire company and not solely pertaining to (dis)incentives for developers, and taking into account the difficulty in finding participants from the IT-SI stakeholder group, the decision was made to categorize this developer within the IT-SI group rather than the developers' group.

IT System Integrators

The IT-SIs that will be approached within the Netherlands also exhibit broad similarities. First, the fact that they operate within the same country contributes to this. A second reason for the coherence between IT-SI views consists of the major tier 1 SIs are well-known names that have been operating in the field for a considerable period of time. B2B customers often choose these providers due to their years of experience and expertise they have accumulated (ArganoUV, 2020). This results in them largely sharing the same workforce. They can allocate a wide range of implementation resources to a project and boast various awards they have achieved thus far. In the report provided by ArganoUV (2020) it is stated that smaller SIs tend to specialize in specific industries or geographical regions. For this research, we are more interested in the extensive knowledge possessed by the larger players within this stakeholder group. Therefore, the focus will be on these entities.

4.3.2. Stakeholder Groups With (Potential) Distinctions

Within the context of examining the SSC and its implications for stakeholders, it is crucial to recognize the potential existence of differences among the key groups. Specifically, this section aims to shed light on two of those, namely software vendors and B2B customers, and the necessity to identify possible divergences between them. While it is not intended to segregate these groups, understanding and anticipating potential distinctions ex-ante can contribute to a more comprehensive

analysis of the SSC ecosystem. Therefore, this section aims to explore and outline some conceivable characteristics that may differentiate these stakeholder groups, serving as a reflection on possible limitations and considerations for the further progression of this thesis and future research. For now, it is not the intention to make significant distinctions between the stakeholder groups when reaching out to potential interview participants. However, these factors may be taken into account during the analysis and conclusion of the findings. They will also be incorporated into the questionnaires for the interviews. This approach allows for the inclusion of certain characteristic or demographic attributes at a later stage, if desired.

Software Vendors

Firstly, within the stakeholder group of software vendors, there are naturally differences in size, revenue, and so on. For this phenomenon, the research applies a similar strategy as for IT-SIs, focusing primarily on the major players. This is due to their extensive experience and expertise compared to the specific expertise of smaller vendors.

One of the main differences within this stakeholder group, identified during the pre-interview phase of the research, lies in whether the vendor delivers third-party software or Software-as-a-Service (SaaS) to their customers. This differentiation has notable implications for the relationship between the vendor and the B2B customer, affecting their respective responsibilities and opportunities across the supply chain regarding SBOM. When B2B customers utilize third-party software, they typically have a higher level of ownership and control over the software itself (Issa et al., 2021). They have the freedom to integrate, customize, and manage the software within their own IT infrastructure, granting them greater flexibility and influence. In this context, the presence of SBOMs for third-party software provides transparency and valuable insights into the software's components and dependencies. SBOMs enable B2B customers to effectively manage risks, assess vulnerabilities, and ensure compliance with industry regulations. Conversely, when B2B customers opt for SaaS solutions, they do not have direct ownership of the software. Instead, they access and utilize the software provided by the SaaS provider through a cloud-based subscription model (IBM, n.d.). The responsibility for managing and maintaining the software (thus, also its security) and its underlying components lies with the SaaS provider. Moreover, a vulnerability in this software could directly open a door to the B2B company resources. At the same time, SaaS solutions are managed by their vendors and have limited access to the B2B customer's infrastructure. The focus for B2B customers using SaaS primarily revolves around service-level agreements, data security, and overall performance, rather than the specific components and dependencies of the software itself. Although having SBOMs for SaaS can still offer value in terms of transparency and risk assessment, the level of control that customers have over the software is comparatively limited compared to the case of third-party software.

Lastly, the extent to which developers within these vendor organizations integrate OSS into their development processes may also have an influence. This significantly determines the number of dependencies in a software product, which, in turn, impacts the complexity of license management, maintenance, updates, and overall dependency management.

B2B Customers

For the stakeholder group at the end of the chain, we have the B2B customers (within the scope of this research). The main difference for this group lies in their willingness towards SBOM and their maturity level in terms of security. This can vary across organizations, but trends can also be identified based on different sectors and company sizes.

Starting with company size, it can be interpreted in terms of two factors: the number of employees or revenue size. Both factors are considered as indicating a "large" organization. The rule states that the larger the organization, the more software they bring in-house (Forbes, 2022). Consequently, the complexity of the software stack and its dependencies increases significantly. This can also impact the maturity of their security practices. Moreover, larger organizations often have more resources to allocate to security. As mentioned in the introduction of this chapter, it is also common for larger organizations to engage external security firms, which positively influences their security management.

A second factor that appears to have a reasonable impact on the overall security levels of companies is the sector in which they operate. For example, various critical sectors are known for being relatively advanced in their security practices. According to McKinsey & Company (2021), this includes sectors such as finance and healthcare. This can be attributed to the fact that these sectors are subject to a greater number of (EU) laws and regulations that they must comply with. The financial sector, for instance, is affected by stringent laws like DORA (Chapter 2), and other critical sectors are impacted by regulations such as NIS 2, which many already fall under the existing NIS framework. Companies operating in the financial sector in the Netherlands are actively supervised by De Nederlandsche Bank (DNB) (DNB, 2021), which significantly motivates the enhancement of their security measures.

4.3.3. Distinctions in Job Functions

To meet the established data requirements, it is important to have a diverse range of participants. Within an organization belonging to a specific stakeholder group, there are numerous different functions and roles that are filled. Additionally, the responsibilities encompassed within a similar role can also vary across organizations. For this research, specific job

descriptions within each organization will be identified to gather empirical data. It is expected that these individuals will be able to provide the most relevant data. No specific action is required for open-source developers as they are individual contributors. However, for the remaining three stakeholder groups included in this study (software vendors, IT-SIs, and B2B customers), a clear overview of the relevant job functions within each respective stakeholder group is obtained in Table 4.3. During the process of reaching out to potential interview participants it is used as guidance.

Table 4.3: Overview of Targeted Job Functions

Stakeholder Group	Job Function
Software Vendor	• Developers • Head of Development • Product Leads • Integration Engineers • CTO
IT System Integrator	• Developers • Head of Development • Product Leads • Integration Engineers • CTO
B2B Customers	• CTO • CISO • CIO • IT Manager

4.4. Conclusion of Chapter 4

In an effort to comprehensively define the stakeholder field within the SBOM context, this chapter delves into various aspects, including stakeholder dynamics, cross-functional processes, responsibilities, and value streams. The primary objective is to establish a clear understanding of the key stakeholders involved. Initially, the exploration identifies seven distinct stakeholder groups associated with SBOM in the SSC, providing a comprehensive landscape of those involved in the process.

However, the focus of this chapter is to determine the most important stakeholders within this diverse field. By analyzing the interplay of stakeholders and their contributions, the quest to identify the most significant players in the SBOM ecosystem is undertaken and research sub-question 1 "*What are the most important SSC stakeholders involved with SBOM?*" can be answered. As the investigation progresses, it becomes evident that certain stakeholders possess a higher degree of influence and impact on the overall SBOM landscape.

Drawing upon the insights gained, the analysis culminates in the identification of four essential stakeholders, as illustrated in Table 4.2. These key stakeholders hold crucial positions and play significant roles in the SBOM framework. Therefore, they become the prime targets for conducting in-depth interviews and gathering valuable perspectives and insights. In order to capture the full spectrum of viewpoints within these stakeholder groups, the interviews will specifically target the job functions and positions identified in Table 4.3. This targeted approach ensures that a diverse range of perspectives, experiences, and expertise is represented in the empirical data collection process.

5

Gathering Empirical Data

To determine which stakeholders are important to include in the interviews for collecting empirical data, Chapter 4 provides a clear categorization of suitable stakeholders. The four directly involved stakeholder groups in the SSC will be targeted: OSS developers, software vendors/suppliers, IT-SIs, and B2B customers (organizations). The open source parties of SPDX and CycloneDX (Linux and OWASP), the external security companies, and the governmental agencies are not included. Chapter 4 also clearly displays the value stream between all stakeholders involved. In a perfect world, there would be no transaction costs involved (Brousseau & Glachant, 2002). This would mean that if a customer derives value from having an SBOM, this value should equally flow back to the vendor, too. However, it seems that, given the aim of seeking incentive conflicts due to that lack of adoption, this is not currently the case. The goal of the interviewing method for the exploratory research approach is to gather new empirical information about the identified problem. The knowledge gap that it aims to fill is the lack of specific research that comprehensively examines how the phenomenon of misaligned (dis)incentives among SSC stakeholders inhibits the adoption of SBOM. For this chapter, this entails gathering new empirical data solely from the stakeholder groups concluded. In doing so, it answers sub-question 2.

> **Sub-question 2:**
> What are the (dis)incentives and capabilities of SSC stakeholders regarding SBOM?

As stated in Section 1.3, this research approaches the problem with a holistic approach. Section 3.2 highlighted that the interviews will consist of various segments. After conducting the complete open-ended, semi-structured segment, the researchers also aim to validate specific (dis)incentives mentioned in the literature with the participants. These will be addressed in the more (dis)incentive-specific segment. To formulate these (dis)incentives, Section 5.1 conducts a literature review and examines which factors are deemed most significant for SBOM and similar cybersecurity measures. The main objective of the literature review is to identify a set of relevant factors and help develop the more (dis)incentive-specific interview questions. These will be validated with participants, enabling a subsequent assessment of the extent to which stakeholder perceptions align with the current, albeit limited, literature. The actual structure and setup of the interviews are outlined in Section 5.2, including the strategy for the sequence of the interviews. Finally, the findings and collected empirical data are presented in the Appendices in Appendix B. Conclusions regarding the gathered dataset are drawn up in Section 5.3, in trying to provide an answer to research sub-question 2.

5.1. The Incentives To Research; Identified Ex Ante

In this section, the most probable (dis)incentives are identified, which may potentially play a role in influencing the adoption of SBOM. This is based on the existing literature published about SBOM and similar cybersecurity concepts, involving all the different parties within the SSC as well. It is important to note that these ex ante identified (dis)incentives will only be addressed in the interviews after the participant has extensively discussed the fully open-ended, semi-structured question set. During these initial questions, no mention will be made of the most important (dis)incentives identified in this section. Only after the participant has had the opportunity to freely express their views on SBOM and related interests without any researcher bias, will the theory from this section be lightly incorporated into the questioning. This is a crucial aspect of utilizing the interviewing method to generate empirical data for exploratory research. Furthermore, the questions based on the findings of this section will also remain broad and open-ended, allowing for unbiased insights and experiences. The

main purpose of this section is to help provide directions for the development of more (dis)incentive-specific interview questions. It is also relevant to validate the existing literature on SBOM (dis)incentives with the interviewees. Additionally, for the ordinal preference ranking method (see Section 5.2.3), this approach is also useful for creating the statements and assigning them to specific categories.

Not all factors can be included, so a selection of important factors is made here. This selection has been brainstormed with supervisors. An attempt has been made to consider the costs and benefits for different stakeholders and how they relate to each other. Some factors can be quantified to some extent, while others are less quantifiable. By relating these factors to each other, it becomes possible to gain better insight into potential areas of improvement (in Chapter 6). Throughout this section, the relationship between supplier and customer or vendor and customer is often discussed; in this context, the term "supplier" or "vendor" can also be used for the relationship between integrator and customer. The list of incentives to be further investigated is presented below (Table 5.1).

Table 5.1: Incentives to be Researched; Identified Ex Ante

Incentives
Economic
Time
Regulatory
Trust
Intellectual property
Awareness
Technical capabilities

5.1.1. Economic

The economic (dis)incentive is the most obvious motivation for stakeholders involved with SBOM, given the fact that we're living in a capitalistic world. Monetary value is a critical (dis)incentive for all stakeholder groups. Private organizations obviously seek profits, but also public entities require economic policies to maintain a healthy organization. In the context of cyber security, economic (dis)incentives often vary among stakeholders, creating issues. Weak commercial incentives can make it challenging for businesses to invest in cyber security (Wright et al., 2021). Vendors' primary focus can be on selling and earning from their products, which is contrary to the incentives of their B2B customers (Gordon & Loeb, 2002). Specific to SBOM, several authors recognize problems in the economic interests of stakeholders. SBOMs require additional efforts for their producers, but the producers are not the primary beneficiaries (Xia et al., 2023). B2B customers benefit from SBOM as it helps them manage and mitigate their risks. If vendors perceive that they will not receive any value in return for producing SBOM, such as a return on investment (ROI), they will not be motivated to adopt SBOM (Koran et al., 2022). Crowdstrike (2021) state that this ROI is often still not really clear to stakeholders involved with SBOM. The lack of an industrial consensus on SBOM causes vendors to hesitate in producing and incurring additional costs (Xia et al., 2023). Vendors might assume that if there is little customer demand for SBOM, they cannot pass on their costs to their products.

The impact of different monetary fines or penalties on various stakeholders is also an intriguing question raised in discussions with supervisors of the research. With more legislation emerging that holds boards accountable for managing their supply chain risks, fines of varying magnitudes may encourage stakeholders to start adopting SBOM. Customers need to be sufficiently aware of the risks they can manage and mitigate in economic aspects. Could paying a little more for products with SBOM save them significant economic damage or resources that they currently spend on finding vulnerabilities in their software stack? This awareness can be critical for the adoption of SBOM.

5.1.2. Time

The concept of time can often be linked to economic incentives up to a certain extent. The additional time and effort required for a task is often translated into extra "resources," which have economic significance. Therefore, gathering empirical information from interviews on time-related (dis)incentives among stakeholders involved with SBOM could also provide valuable insights into the economic implications of SBOM adoption. However, as far as developers, time itself could also be a crucial (dis)incentive. Time is perhaps easier to quantify for stakeholders in terms of how much time they spend producing an SBOM or how much time they currently spend on finding vulnerabilities in their software stack. For the software supplying stakeholder groups, time-related (dis)incentives are particularly significant since they are the ones who must make additional (timely) efforts to implement SBOMs (Xia et al., 2023). Various factors can influence this, including the complexity of the SBOM creation process, which can affect the time taken to complete it.

Viega and Michael (2021) provide another example of vendors who had to undertake assessments. They noted that *"vendors are reluctant to spend time on them and instead focus solely on their business."* Excessive time investment by vendors could indeed inhibit SBOM adoption. Therefore, investigating how they perceive this aspect is crucial. As a result, the study of time-related (dis)incentives among SBOM stakeholders, particularly vendors, can provide valuable insights into the potential economic benefits or drawbacks of SBOM adoption. Another well-known example that had a rather slow adoption is 2-factor authentication (2FA), which is also a concept aimed at enhancing the cybersecurity levels of a system (Petsas et al., 2015). It's a security process in which a user has to provide two forms of identification to access the online system; password and SMS code, for instance. This should make it harder for unauthorized parties to gain access to the system. However, the concept also requires users to make additional efforts and consume timely resources. This trade-off between user efforts and security has resulted in a slow adoption rate (Gunson et al., 2011).

5.1.3. Regulatory

Regulatory interventions or institutional policies can play an important role in incentivizing organizations to adopt best practices for managing SSC risks. While intrinsic incentives (those of the other sections) are important, external incentives such as relevant regulations can also be effective. Xia et al. (2023) highlight the importance of relevant regulations in improving SBOM awareness and managing supply chain risks. The European NIS2 directive explicitly states that organizations failing to manage their supply chain risks will be subject to penalties, and in the U.S., Executive Order 14028 shows a serious commitment to mandating SBOMs (Section 2.3).

Currently, unregulated aspects of SSCs pose significant risks, OSS being a prime example. Due to limited resources and time, developers often do not adequately test their software for security (Zajdel et al., 2022). Nevertheless, downstream organizations often use software components derived from OSS. The lack of transparency surrounding these components creates additional challenges for risk management. In Australia, soft law mechanisms have not been successful in addressing the market failure where private (dis)incentives and public benefit conflict (Wright et al., 2021). Commercial incentives are too weak for private parties to invest in adequate cybersecurity measures. Government intervention is necessary to ensure best practice cybersecurity measures are adopted. It is relevant to investigate how stakeholders involved in SBOM view the need for regulatory interventions and whether they consider them as serious incentives. For instance, if large vendors were required to provide transparent SSC information downstream, it could have a significant impact on the industry. If all vendors were mandated to do so, they would no longer have to compete against other vendors who do not produce SBOMs. A regulatory framework such as the NIS2 directive, which mandates SSC risk management, could also increase demand for SBOMs.

Another factor that could be of interest to research is the factor of compliance. This can apply to all different stakeholder groups, depending on the relevant legislation. If the law states that organizations purchasing third-party software can be held responsible for managing their supply chain risks, then compliance with that legislation may also be an important consideration for those organizations to demand SBOMs from their suppliers.

5.1.4. Trust

Trust is another value that can impact the adoption of SBOMs. Trust is a two-way street that can affect both the software vendors and their customers. Firstly, vendors have an incentive to generate trust among their customers and maintain it over time (Sharma et al., 2020). This incentive can lead to economic stimuli due to its contribution to loyalty, as customers are more likely to purchase products from vendors they trust. Therefore, it is important to explore how all stakeholders view trust in the context of SBOMs.

However, trust can only be taken seriously if the SBOMs produced are accurate and have integrity (Xia et al., 2023). Accuracy is crucial in ensuring that the SBOMs provide an up-to-date representation of the SSC. Integrity refers to the reliability and trustworthiness of the SBOMs, which determines whether customers can trust the information presented by higher-ups in the SSC. If vendors provide inaccurate or unreliable information, this can erode the trust that customers have in the SBOMs and the overall supply chain. Unfortunately, there have been cases where the integrity of vendors has been called into question. For instance, some vendors have been known to self-report their own security posture inaccurately (Viega & Michael, 2021). *"We've seen vendors, when asked to do a self-assessment, blatantly lie about having controls in place."* This undermines the trust that customers have in the SSC and highlights the importance of transparency and accountability in producing SBOMs.

5.1.5. Intellectual Property

Based on the preliminary research, the factor of intellectual property (IP) seems to have two different (possible) effects on (dis)incentives concerning SBOM. From the brainstorming, there is mainly a concern that software vendors may have disincentives to produce SBOMs for their products because they perceive this as infringing on their IP. This is also suggested by Remaley (2021), which states that within SBOMs *"dependencies share intellectual property (IP) relevant information*

and algorithms that can be too easily exposed by such declarations." They state that almost all SBOMs need to be maintained confidentially.

However, other studies suggest that the production of SBOMs need not be detrimental to IP. Laplante (2021) also talks about 'software labeling' for better SSC transparency in a similar way. They claim that this does not detract from the IP. They cite the commonly used comparison with a nutrition label on food packaging, which also does not reveal secret recipes. It only exposes important properties of the code that are conducive to safety, security, reliability, and so on. In fact, they state it could be a competitive advantage. Each software provider can advertise its own "*special blend*" of testing, test coverage, complexity, new and reused, open access, and so on. Then, the software component consumer can decide based on these qualities that the system is safe, reliable, trustworthy, and so on.

Other authors suggest that SBOM information can even assist IP applications (Arora et al., 2022; NTIA, 2019). Access to such data provides details of subcomponents used, licenses, and history of updates. This can improve those applications. It may also depend on how much customers want SBOMs provided with products and how much they would distrust vendors who do not provide SBOMs. For vendors, the consideration could be: how much money do I lose due to lost IP versus how much money do I lose due to customers leaving because of a lack of trust.

5.1.6. Awareness

While the listed (dis)incentives so far (could) play a vital role in driving the adoption of SBOM, there is another important factor that must be considered, namely 'awareness'. It refers to the level of knowledge and understanding among stakeholders regarding the importance of SBOMs in improving software security and reducing supply chain risks. Lack of awareness on either side of the vendor-customer relationship can lead to a "*chicken-and-egg*" problem (Jones et al., 2013), where vendors are hesitant to invest in SBOMs due to a lack of market demand, and customers do not demand SBOMs due to a lack of awareness of their benefits.

Several sources have identified the importance of awareness in driving the adoption of SBOMs. For example, both Xia et al. (2023) and Crowdstrike (2021) have highlighted the lack of market awareness and unclear ROI for vendors as barriers to adoption. On the other hand, B2B customers may not signal enough demand for SBOMs because they are not aware of the benefits that SBOMs can provide, or not even of SBOM at all (Owen, 2022). As a result, the lack of customer awareness of security "*limits commercial incentives for manufacturers to compete on cybersecurity*" (Wright et al., 2021). Another example from within the EdTech (Educational Technology) industry is given by (Fouad, 2022). There is too little evidence on the efficacy of the discussed EdTech tools, and thus little awareness, which ultimately hinders the adoption of these tools. Therefore, for this research it will be important to test the awareness of SBOM across the different stakeholder groups on the SSC.

5.1.7. Technical Capabilities

A last factor that can be crucial in the adoption of SBOM is the technical capabilities of the concept, its associated tooling and of the various stakeholders involved. Despite these factors not being a direct (dis)incentive, it can certainly contribute to other (dis)incentives to adopt SBOM. And the other way around, it could also be detrimental to the adoption. For example, regarding SBOM tooling, the stance of stakeholder groups can strongly depend on factors such as the actual necessity of the tooling, its ease of use, the required level of expertise, its quality, price, integration capabilities, and so on. The researchers aim to investigate the impact of these types of factors on the (dis)incentives of the participants. Additionally, other technical challenges or limitations (some of which were previously identified in Section 2.2.3) and their expected consequences will be brought to light.

One of the main challenges is stakeholders' ability to create accurate and complete SBOMs, due to the current lack of adoption. Software components developed by multiple parties make it difficult to trace origins and dependencies, since they don't get supplied with SBOMs. If an OSS developer creates a component later incorporated into a vendor's code without providing an SBOM, the vendor struggles to identify relevant data for a complete SBOM. This results in insufficient detailing for dependency layers.

Another challenge is the practice of developers copy-pasting lines of code instead of formally importing the library file from which the code originates (Donovan, 2020). This results in the omission of known vulnerabilities associated with the library during vulnerability analysis because the SBOM does not reveal the library as a dependency. Consequently, vulnerabilities can be overlooked. Similarly, concerns arise when B2B customers require avoiding components from specific countries, highlighting the need for developers to disclose code origin (Phillips et al., 2023). The current technical limitation lies in the near impossibility of recognizing copied and pasted lines of code from their initial source. Consequently, potentially relevant associated information remains undetected.

There are also concerns regarding CVEs in SBOMs (Remaley, 2021). Vulnerability databases only provide information about known vulnerabilities in specific components. This can lead to incomplete or misleading information when components are not vulnerable. It is possible for a vulnerability analysis to generate a long list of CVEs of which a lot are

not actually exploitable within a particular organization's software ecosystem. Consequently, customers may incorrectly pressure vendors to upgrade libraries that do not require upgrading, resulting in vendors expending valuable resources on low-priority issues by producing unnecessary patches.

Finally, there is a challenge related to the expectations of stakeholders regarding which software components require an SBOM. It may not be practical or feasible to create an SBOM for every software component, especially those developed using several programming language ecosystems. This challenge highlights the need for clear guidelines and standards around the creation and use of SBOMs to ensure that they are applied consistently and effectively.

Despite these technical challenges, the benefits of SBOMs cannot be overstated. Xia et al. (2023) state that even if SBOMs are less accurate than desired, they still provide more visibility and transparency than not having them at all. This is a critical first step in improving cybersecurity and supply chain risk management, and organizations should continue to work towards addressing these technical challenges to fully realize the benefits of SBOMs.

5.2. Interview Setup

As outlined in Chapter 3, the appropriate and most popular data collection method for addressing primarily sub-question 2 is conducting interviews with participants from all relevant stakeholder groups within the SSC who are directly involved or affected by SBOM. This method proves effective for exploratory research studies, particularly in the absence of extensive publications on the topic (Alshenqeeti, 2014; BRM, n.d.). Through interviews, we can easily generate insights into the experiences, behaviors, and beliefs of the participants.

The development of the interviews follows a series of steps outlined in a roadmap (Section 5.2.1). Additionally, the interview setup itself includes various phases, which will be explained in detail (Section 5.2.2). The selection process for participants in the interviews has already been extensively discussed in Chapters 3 and 4 and will not be addressed further in this section.

5.2.1. Generating the Interviews: The Roadmap

The first step in generating the interviews involved determining relevant interview structures for an empirical research approach. It is widely recognized that semi-structured interview questions are most suitable for eliciting new information from participants (Alshenqeeti, 2014; BRM, n.d.). This approach will be used as the starting point for the interviews, which is important for meeting the data requirement of minimizing researcher bias during the interviews. However, it was also found that more focused questions on the specific topic can be useful. To determine the direction of these questions, an extensive literature research was conducted, examining interests related to SBOM as well as similar cybersecurity concepts. The results are presented in Section 5.1. The translation of these results into concrete interview questions is shown in Section 5.2.2.

The second step involves consultation with involved researchers and supervisors. For this, a first meeting was scheduled with the responsible researcher of TU Delft to discuss and potentially refine the content of the interviews. A second meeting was scheduled with the main Northwave supervisor to do this, too. These meetings critically examined whether the questions would truly contribute to answering the research questions. It was during this step that the decision was made to include an ordinal preference ranking method, which allows for the collection of quantitative data in a quick manner. This method was also tested twice to ensure the relevance of the question formulations and to try to minimize potential ambiguities. The aim was to gain a more quantitative understanding of stakeholders' opinions on various SBOM interests and how they compare to one another.

Subsequently, the interview questionnaire, up to that point, was tested with actual potential participants in formal pilot interviews. These pilot interviews allowed for testing and refining the question set (Majid et al., 2017). They also helped minimize ambiguity in the statements for the ordinal preference ranking method, which is often a limitation of the method (García, 2011). Conducting pilot interviews is a good practice before conducting the actual interviews and was included as a planned measure in Chapter 3 to contribute to the data requirement of effective question formulation that addresses the research questions. The pilot participants had no prior knowledge of the research, allowing for an evaluation of question clarity. The pilot interviews were conducted with two different participants, intentionally selecting someone with a highly technical background and someone responsible for strategic technology policies within their organization. This approach provided insights from two different perspectives. It is important to note that the participants and the data generated from the pilot interviews are not included in the results. However, valuable lessons were learned from these initial pilots, and the feedback was incorporated before starting the actual interviews.

Following the interviews, all findings will be presented and discussed with a field expert, consisting of a major policy making and regulatory entity in the Netherlands. This is done purely for additional validation of the interview findings. In these sessions, possible next steps and potential solution directions will also be explored and discussed.

5.2.2. Generating the Interviews: The Content

In this section, we will provide a detailed explanation of the actual questions and statements used in the interviews. The questions for each segment of the interview will be presented, with necessary explanations where applicable. The first important data requirement, established at the end of Chapter 3, is the need for effective questions that contribute to the research questions. This requirement was kept in mind during the generation of the questionnaire. In the iterative feedback rounds with supervisors, questions were also removed if they did not meet this requirement. For some phases, the wording of the questions may vary for different stakeholder groups. This is due to the bottom-up approach applied, where the relevant details for each stakeholder group are included but aggregated as general information and conclusions during the data analysis (Gibbons, 2022). However, for the majority of the question set, the questions are the same across all stakeholders.

Before each interview began, the researcher and the participant engaged in a brief conversation about the research (purpose) and discussed SBOM in general to assess the participant's knowledge of the concept, if it was not already clear based on the selection and recruitment process.

Segment 0: Orientation

The purpose of this segment is to gather demographic information about the participant. This allows for the identification of correlations between different stakeholder groups or characteristic/demographic features during the analysis. The sector, role, and number of years of experience in the software field are particularly important for demographic purposes. Additionally, knowledge of and experience with SBOM are of interest. The orientation segment questions are the same for all stakeholder groups, with a slight variation for OSS developers. The questions are showcased in Table 5.2.

Table 5.2: Interview Questions: Segment 0

Segment 0
ORIENTATION
QUESTION:
Software Vendor | IT-SI | B2B Customer: What industry does your company operate in and what is your position within the company?
OS Dev: What are open source projects that you predominantly contribute to?
How many years have you been working/active in the software field?
Can you explain how you see the software supply chain, and possible risks?
Can you explain your understanding of SBOM?
Do you (and/or the company) have experience with SBOM?

Segment 1: Semi-structured

The semi-structured interviews conducted in this study aimed to gather rich and diverse data. For this segment only three open-ended questions are utilized. These questions were designed to allow participants to freely express their thoughts, experiences, and opinions without undue influence or biases imposed by the researcher. To minimize that bias it is important to note that the open questions were posed after a neutral introduction, without any prior discussion of the findings from Section 5.1. This approach ensures that participants' responses are not influenced by the researcher's interpretations or preconceived notions, thereby enhancing the reliability and validity of the data collected.

The first important aspect of these open questions is their ability to uncover participants' own (dis)incentives related to SBOM. By giving participants the opportunity to share their motivations, challenges, and perceived benefits, valuable insights can be gained regarding the factors that drive or hinder SBOM adoption. Understanding these (dis)incentives is crucial for assessing the feasibility and potential barriers to implementing SBOMs effectively. In addition, participants' expectations of SBOMs were also explored through these open questions. This aspect provides an opportunity to compare participants' initial expectations with the practical realities of SBOM implementation. By examining any discrepancies between expectations and actual experiences, researchers can gain a deeper understanding of the challenges and opportunities associated with SBOM adoption.

Furthermore, it is worth mentioning that the selection of these open questions was consistent across all participant groups. This standardization allows for comparative analysis between different stakeholder groups, facilitating the identification of common themes, as well as unique perspectives specific to each group. They are presented in Table 5.3.

Table 5.3: Interview Questions: Segment 1

Interview Questions: Segment 1
SEMI-STRUCTURED
QUESTION:
What are your expected benefits of SBOM for you or the software supply chain as a whole?
What could be drivers/interests or incentives for you to either do or do not adopt SBOM?
Do you have (technical) concerns about SBOM or its technical capabilities, and if so, which ones?

In addition to these three comprehensive questions, there were several other open semi-structured questions included in the interview. These questions were primarily derived from the identified (dis)incentives and factors mentioned in Section 5.1 during the questionnaire development phase. While these questions may have a slightly more guided approach compared to the previous three, they remained open-ended and semi-structured to minimize researcher bias. The exploration of these themes takes place throughout the interview, unless participants have already addressed them in response to the initial broad opening questions. In such cases, their answers are taken into account and the exact question may not be repeated.

Although certain questions may have slightly different formulations to accommodate the specific needs of different stakeholder groups, the overall content of the questions remains fairly consistent. This ensures that the interview captures a comprehensive perspective across various stakeholders while maintaining a focus on the research objectives.

The first segment concludes with an additional question that does not strictly fall under either the semi-structured segment or the Ordinal Preference Ranking segment. Nevertheless, it is included within Segment 1 to maintain coherence. The detailed overview of all the questions used in the interviews is in Table 5.4.

Table 5.4: Interview Questions: Segment 1

Segment 1
SEMI-STRUCTURED
QUESTION:
Do you think SBOMs are useful in managing and mitigating risks, and if so, what risks?
B2B Customer: Would you spend more on purchasing third-party software that comes with SBOM, and if so, what percentage/how much?
Software Vendor and IT-SI: Do you think you can pass on the cost of producing SBOMs to the customer?
OS Dev: Do you think any costs incurred by SBOM can be passed on down the supply chain?
B2B Customer: Is trust (e.g., reputation) an important factor in choosing a system integrator or software vendor to buy software, and why?
Software Vendor and IT-SI: Could customer trust (e.g. reputation) in you be an important factor in adopting a concept like SBOM?
OS Dev: Are there any specific reasons why you contribute to open source projects?
How many resources (financial/time) do you spend on finding vulnerabilities in your software?
Can you give your opinion/view on the current regulations regarding software supply chains?
Do you think legislative measures are needed to make SBOM widely adopted, and why?
Do you think customers should be able to view SBOMs prior to purchase, or only after purchase?
Could SBOM be a threat to the intellectual property of developers/vendors/integrators?
Do you have other (technical) concerns about SBOM or its technical capabilities, and if so, which ones?
OS Dev, Software vendor and IT-SI: Are there already "demand" signals from the customers?
B2B Customer: If you want it, does your company give off enough "demand" signals to suppliers?
PERCEPTION:
If you were to describe your sentiment regarding SBOM and its potential for success, choosing from *negative*, *skeptical*, *neutral*, *optimistic*, or *really positive*, what would you choose?

5.2.3. Ordinal Preference Ranking

At the end of the scheduled hour with all participants, the ordinal preference ranking method was introduced. Its purpose was to capture the participants' perception of certain (dis)incentive categories in a more quantitative manner through statements. To make the latter relevant to the research questions (data requirement, Section 3.3), these statements were formulated based on the identified (dis)incentive categories in Section 5.1. A second requirement that had to be considered was the use of a standardized ranking scale that would avoid confusion.

After researching suitable ordinal preference ranking methods, the Likert scale was chosen, as it is a commonly used method to measure participants' preferences or attitudes. According to the theory, participants evaluate the statement based on their level of agreement or disagreement, using a scale of numbers, often ranging from 1 to 5 (or any other number) (Yamashita & Millar, 2021). Although numerical values are assigned to the responses, the intervals between the different response categories are often considered unequal. In other words, the distance between "disagree" and "neutral" may not necessarily be the same as the distance between "neutral" and "agree". Therefore, the Likert scale is regarded as an ordinal scale.

For this research, the traditional scale is slightly adjusted. Participants will assess the statements using a Likert scale ranging from -5 to +5. This scale represents the range from "highly inhibiting for SBOM adoption" to "highly facilitating for SBOM adoption". The value of 0 represents "neutral", indicating that the participant believes the statement will have no significant impact on the adoption of SBOM. The tested statements are presented in Table 5.5. This set of statements remains the same for all stakeholder groups, as it aims to capture the perceptions of all participants regarding all relevant interests. For the following list of statements, it's important to note that after each statement, when read out to the participants, it was completed with the following sentence (filling in the dots): "*...to what extent will that impact SBOM adoption by the various stakeholders in the software supply chain?*"

Table 5.5: Ordinal Preference Ranking: Segment 2

No.	Category	Segment 2
S1	Economic	Suppose the implementation of SBOM dramatically reduces the financial risks arising from exploited vulnerabilities, ...
S2	Economic & Technology	Suppose in order to use SBOM, it is necessary to purchase additional software tooling. So this makes it more expensive. The tooling is good though, ...
S3	Time	Suppose SBOM saves half the time it currently takes in finding vulnerabilities in the software stack, ...
S4	Law and regulation	Suppose SBOM is not required by law, but is a good measure to be compliant with certain (EU) legislation, ...
S5	Economic & Law and regulation	Suppose if organizations fail to comply with supply chain management laws and regulations, they could be fined 1% of annual sales, ...
S6	Trust	Suppose providing SBOMs with software products creates a lot of additional trust from customers in the supplier, ...
S7	Awareness & demand	Suppose parties higher up the software supply chain (developers, vendors, integrators) assume that downstream customers are not yet aware of SBOM and are not asking for it, ...
S8	Intellectual property	Suppose SBOMs could threaten the intellectual property of the parties generating them, ...
S9	Technology	Suppose where there is already quite a lot of good tooling for SBOM generation, there is still little for SBOM consumption (use), ...
S10	Technology	Suppose SBOMs are really user friendly to use, ...
S11	Technology	Suppose SBOMs can only detect half of all vulnerabilities, for example, because developers copy-paste code from libraries without 'formally' importing it, ...
S12	Technology	Suppose most of the CVEs that SBOM finds are not really vulnerable, ...

5.3. Conclusion of Chapter 5

This chapter focuses on addressing sub-question 2: "*What are the (dis)incentives and capabilities of SSC stakeholders regarding SBOM?*". It accomplishes this by collecting empirical data through interviews and conducting preliminary research. The summaries of these interviews, which provide the data needed to answer this research sub-question, are included in Appendix B. The identified (dis)incentives in Section 5.1, along with the data from the interview summaries, together form the basis for answering this sub-question. It is evident that the main (dis)incentives largely align with the list identified through literature reviews, although there are variations in what participants have expressed. Some participants displayed a higher level of familiarity with SBOM than others, and their responses varied in terms of depth and extent. This variation in participant responses resulted in varying amounts of available data.

To make meaningful sense of the collected data, Chapter 6 follows, where a comprehensive analysis takes place. This analysis goes beyond a mere presentation of individual participant responses; it aims to uncover connections, relationships, and patterns within the data. By examining the data as a whole, common themes can be identified, and interrelationships between different (dis)incentives can be explored. This analytical approach allows for drawing meaningful conclusions and will significantly contribute to addressing the main research question.

6

Data Analysis and Findings

This chapter presents the analysis and findings derived from the empirical data collected during hour-long interview sessions with 16 different participants from the SSC. In order to answer the main research question, all the collected data needs to be analyzed and aggregated (given the use of a bottom-up approach) to extract relevant information and novel insights. It aims to identify the relationships, patterns, and other factors that may contribute to the main problem of SBOM adoption across the SSC. These findings contribute to the current scientific understanding of the (dis)incentives surrounding SBOM. Specifically, this chapter addresses sub-question 3:

> **Sub-question 3:**
> What factors can explain the lack of SBOM adoption?

To present the findings in a complete yet structured manner, this chapter follows a sequence of steps. It starts with thematic and frequency analysis. Chapter 3 outlines the analysis method broadly, while Section 6.1 elaborates on the exact theory behind the thematic analysis, its alignment with the research, and the steps taken to obtain the findings. These findings, derived from the thematic analysis in conjunction with the frequency analysis, are subsequently showcased in the ensuing Sections 6.1.2, 6.1.3, and 6.1.4. These sections highlight noteworthy outcomes from the examined interview responses, both at a macro-level (in a general context) and a meso-level (pertaining to distinctions between stakeholder groups). Moreover, Section 6.1.5 also identifies intriguing relationships and patterns on a micro-level (individual participant level). The latter are deduced from analyzing the dataset for this, which is available in Appendix C.

Section 6.2 delves into the data obtained through the ordinal preference ranking method, as described in Appendix B.2. Given the relatively small sample size of 16 respondents for a quantitative method, its data analysis primarily serves to validate the earlier findings presented in Section 6.1.

Furthermore, in Section 6.3, a validation session with a field expert is conducted to verify and refine the obtained results. The outcomes of this session are thoroughly examined and discussed in this section, further enhancing the reliability and validity of the research outcomes.

Up to Section 6.3, all noteworthy findings are presented. To a certain extent, this constitutes a substantial amount of information that might seem somewhat cluttered. It also encompasses various identified factors without delving specifically into their impact on stakeholder-specific incentives and disincentives. Given the volume of data and the research's emphasis on focusing on the (dis)incentive problem, ensuring the comprehensibility and coherence of the thesis requires a more structured arrangement of the result set. To obtain this, the researchers take several additional steps in Section 6.4. Within this context, Section 6.4.1 initially aggregates all identified themes and categorizes them into two categories: incentives and disincentives. These are subsequently matched up with the ex-ante identified (dis)incentives from Section 5.1 in Section 6.4.2, determining the extent of their alignment. Lastly, Section 6.4.3 provides a comprehensive SWOT analysis aimed at precisely delineating the complete (dis)incentive landscape for each stakeholder group. This analysis offers a clear overview of the most prominent incentives (strengths and opportunities) and disincentives (weaknesses and threats) for each considered stakeholder group, based on which strategies can proposed to promote the spread of the technology. The outcomes from this analysis can then serve as a more distinct foundation for building upon in the concluding and prospective chapters.

6.1. Thematic Analysis: Setup

As mentioned in Chapter 3, the thematic analysis, as described by Braun and Clarke (2006), consists of six different steps. Section 6.1.1 will elaborate on these steps and connect them to how the obtained dataset is approached within this research, on a per-step basis. Subsequently, all the results of the thematic analysis, as explained in the introduction of this chapter, including the findings from the empirical data collection method (interviews), will be presented.

6.1.1. Six Steps of a Thematic Analysis

Step 1: Exploration

The first step identified by Braun and Clarke (2006) is *exploration*. The main objective of this step is to become familiar with the obtained dataset, in order to create a holistic overview of the data. In this research, it was followed that before proceeding to any other step, all interview transcripts were consumed three times. This aids in the subsequent steps, as certain trends, codes, and themes can be observed more readily by the researcher.

Step 2: Coding

The next step involves systematically identifying interesting and relevant data. This can include specific phrases, sentences, or paragraphs that may add value to the analysis. These data units are then labeled by the researcher. In practice, during the screening session for this step, everything that stood out and seemed interesting was labeled for later reference.

Step 3 & 4: Theme Identification & Revision and Refinement

Step 3 required more time and closer attention. The identification of themes is based on patterns, connections, and frequently recurring concepts within the coded data. Based on this, different codes are grouped into overarching themes. These themes represent significant aspects or ideas emerging from the data. To ensure that the themes accurately represent the dataset, the entire dataset was screened again twice for step 4. After the first screening, initial themes were developed, and the second screening carefully examined whether all important data was encompassed. During this process, some theme names were refined, and certain themes were divided or merged as necessary.

Step 5 & 6: Defining and Organizing & Presentation

Both of the final steps will be addressed in the following subsections. In this fifth step, the aim is to provide clear definitions of the identified themes. This will be fully covered in the subsequent Sections. Additionally, a data analysis method, namely frequency analysis, will be added to the completed thematic analysis. According to Kuckartz (2019), the themes themselves are the main findings from the thematic analysis. However, as Getthematic (n.d.) also suggests, if only one interview participant addresses a particular theme and no one else does, it could indicate the significance of that theme not being too high and it may be given less consideration later on. The frequency analysis will therefore assist in the *presentation* step to give more weight to certain identified themes. Based on this, it enables researchers to uncover deeper relationships and patterns, potentially leading to more relevant and novel insights.

The presentation of the findings consists of various methods. For each important topic related to the interview questions, a clear bar chart is displayed. This chart clearly shows how many participants have addressed the importance of different themes (at a macro-level). To support the diagrams, detailed written explanations are provided. These explanations include numerous relevant quotes from the transcripts to provide more context to certain perceptions of the themes. This significantly enhances the reader's understanding of the findings in this thesis.

Another aspect that becomes apparent through the diagrams is the distribution of stakeholder groups per theme. The bars in the bar charts will consist of sub-bars representing the representation of a stakeholder group (the legend provides colors for each group). Based on this information, findings can be made at the meso-level, as mentioned at the beginning of this chapter. However, it is important to consider that the number of participants varies somewhat across stakeholder groups. Therefore, when identifying relationships and patterns at the meso-level, percentages within groups and similar factors will need to be taken into account.

Finally, it is important to mention that certain abbreviations are used for the diagrams in the legend. From top to bottom, 'B2B' refers to B2B customers, 'SV' denotes software vendors, 'SI' represents IT-SIs, and 'DEV' signifies developers. An overview of all the interviewed participants, identified with an ID P-number, their stakeholder group, work experience in the software industry, and their level of familiarity with SBOM, is presented in Table 6.1. Throughout this chapter, reference will be made to this table by mentioning the P-number and the group of the respective participant. This approach provides further insights into the representation of specific viewpoints from different groups.

Table 6.1: Overview of participant demographics

ID	Group	Work Experience	SBOM Expertise
P1	SI	4	low
P2	B2B	20	good
P3	B2B	27	good
P4	SV	20+	good
P5	B2B	29	medium
P6	SV	19	good
P7	SI	25	good
P8	SV	25	medium
P9	SI	20	expert
P10	DEV	15-20	expert
P11	B2B	17	good
P12	DEV	15	medium
P13	DEV	10	expert
P14	SV	19	expert
P15	DEV	8	low
P16	DEV	25	expert

6.1.2. Results of the Main 3 Questions

First, the results of the thematic analysis will be presented through the diagrams, based on which several aspects will be addressed. For each "findings" subsubsection, the process will follow the same step-by-step approach. In accordance with Step 5 as outlined by Braun and Clarke (2006), the different themes will first be explained and defined. Subsequently, interesting macro-level findings will be highlighted. Finally, relevant meso-level findings will be discussed, focusing on significant differences among stakeholder groups. In each of these steps, relevant or contextually enlightening quotes will be included where appropriate.

Findings: the Most Expected Benefits of SBOM

The initial open-ended, semi-structured question aimed solely to capture the participants' biggest anticipated benefits of SBOM. The obtained answers are unbiased since no further targeted (more incentive-specific) questions were asked at that point. This also applies to all three sub-subsections within Section 6.1.2.

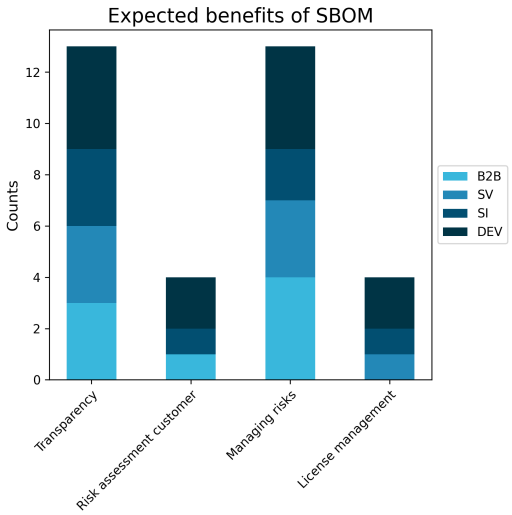


Figure 6.1: The expected benefits of SBOM

Transparency:	It is anticipated that one of the major advantages of SBOM is the enhancement of transparency and visibility of software within the SSC.
Risk assessment customer:	Based on comprehensive SBOMs provided by vendors, a better comparison of risk and security can be made between different suppliers.
Managing risks:	It is expected that through the use of SBOM, potential risks within the SSC can be better managed, and proactive measures can be taken, potentially leading to the mitigation of risks.
License management:	There are advantages of SBOM in terms of license management. Without visibility, it can be challenging to ensure compliance and avoid license violations. This lack of insight can have legal consequences. It is anticipated that SBOM mitigates those risks.

Macro-level Findings
The themes of transparency and risk management receive a high level of emphasis, with almost all participants acknowledging their importance (both 81.3%). This is consistent with the initial findings and aligns with the introductory section of this thesis and the early literature reviews conducted for this research. Furthermore, these two themes are interconnected. For instance, P5 (B2B) highlights that transparency enables better risk management and makes risks more controllable. It is encouraging that participants have accurate expectations of SBOM, making disincentives regarding this aspect unlikely.

On the other hand, the other two themes are mentioned less frequently. However, 4 participants (25%) is still a significant level of attention (relative to later themes in this section) and remains an interesting and relevant aspect that will be taken into consideration. Regarding the 'Risk assessment customer' P1 (SI) suggests that "*having better insights into software expectations would allow customers to make informed choices among suppliers, leading to more effective decision-making*". P6 (SV) emphasizes the importance of improved license management, citing instances from the previous year where licensing issues posed significant threats, requiring multiple interventions from their legal team.

Meso-level Findings
There are no prominent patterns observed at the meso-level for these themes. It is noticeable that B2B customers are particularly focused on making their risks manageable, as all of them raised this theme.

Additionally, it is evident that only parties involved in software development (developers, software vendors, and IT-SIs) mentioned license management as a benefit. This finding is logical since it directly affects their compliance with legal requirements. Nonetheless, it is an interesting observation.

Findings: the Most Impactful Incentives for SBOM
The second main open semi-structured question pertains to the (dis)incentives that participants consider most influential in the adoption of SBOM. The identified themes for the frequency analysis are based solely on the themes raised by the participants themselves in response to this question, without any bias from subsequent questions that focus on different (dis)incentives. The following are the results obtained from this analysis.

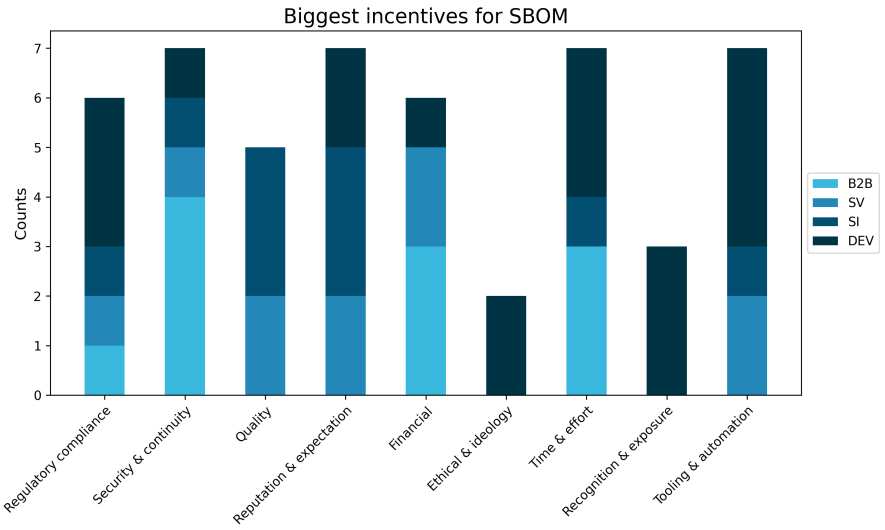


Figure 6.2: The most impactful incentives of SBOM

Regulatory compliance: Participants believe that a significant driver for organizations is the potential of SBOM to assist with regulatory compliance. They perceive that being able to comply with laws and regulations is a compelling incentive for adopting SBOM. Additionally, some participants view mandatory SBOM requirements as a means to promote its adoption across the industry.

Security & continuity: Participants consider the increased security that SBOM can (indirectly) provide as a significant motivator for adoption. They perceive that SBOM can contribute to enhancing security measures and mitigating the risk of being affected by cyber attacks. Furthermore, some participants emphasize the importance of ensuring business continuity by preventing disruptions caused by cyber attacks.

Quality: Participants believe that analyzing SBOM can contribute to improving the quality of the software (they deliver).

Reputation & expectation: It is believed that a driving force for adopting SBOM for many parties will be its status as an industry standard. This will generate more demand as it becomes an expectation, leading to increased demand automatically. Additionally, potential reputational damage is considered influential.

Financial: The financial incentives surrounding SBOM are considered significant. This includes both positive and negative financial incentives. Positive aspects include, for instance, the ability to mitigate potential damage caused by vulnerability exploits. Negative aspects encompass fines imposed by regulators, as well as the high costs associated with tools and implementation.

Ethical & ideology: They indicate operating based on ideology and because it feels ethically right.

Time & effort: Time and effort are considered important factors, both positively and negatively.

Recognition & exposure: They operate from a quest for recognition and exposure. This serves as a significant motivator for them.

Tooling & automation: They consider tooling and automation to be important factors within the SBOM ecosystem, regardless of the current status of the tooling.

Macro-level Findings

Almost all themes are broadly represented by the participants, resulting in minimal differentiation among them. Only 'Ethical & ideology' and 'Recognition & exposure' were mentioned less frequently by the participants. The meso-level provides clarity on these two aspects. The identification of these themes itself is already a noteworthy finding (Kuckartz, 2019). They largely align with the important (dis)incentives discovered in Section 5.1, which serves as a validation of those findings.

The theme of 'Security' is self-explanatory, but there are some important findings within this area. The high prominence of 'Regulatory compliance', 'Reputation & expectation', 'Financial', 'Time & effort', and 'Tooling & automation' is something to consider further in this research. The last two mentioned themes are closely related. Effective tooling and automation would reduce the time and effort stakeholders need to invest in SBOM. However, considering the importance of 'Financial', it raises the question of whether the costs outweigh the time saved, for example.

The concept of time is multi-interpretable. P3 (B2B) highlights the importance of the speed that OSS currently brings to all industries. "*We all want to develop faster and faster*." However, they emphasize the importance of security in this context. "*If that development (based on OSS) that is happening faster and faster can no longer be secure, or if you can no longer properly maintain it, then it can become a hindrance to innovation*." For others, time and effort are more of a short-term concept. For example, P15 (DEV) mentions that they would only be willing to adopt SBOM if it doesn't require too much time and effort.

The same multi-interpretability goes for 'Financial'. Where P6 (SV) emphasizes the financial damage that could evolve from reputational damage, P10 (DEV) mentions another perspective regarding the positive driver of 'Financial' incentives. For example, in the U.S., when parties are required to provide SBOMs to government agencies, the suppliers receive significant financial compensation for supplying those agencies. This financial incentive makes it worthwhile for suppliers to invest in producing and delivering SBOMs along with their software.

The significance of good tooling and automation is emphasized by P9 (SI). They mention that "*the moment you can automate these things from the start, so you just press a button and an SBOM with all the dependencies and everything you used comes out, that, in my opinion, is a whole different discussion than having to do it manually every time*."

Meso-level Findings

For the most impactful incentives regarding SBOM there are a few interesting points on the meso-level that will be addressed. Regarding 'Quality,' it will mostly be revisited later. It's notable that only software suppliers (vendors and integrators) have mentioned this theme. However, their perspective relates more to SBOM serving as a guarantor of their own delivered quality. They are also the ones who expressed the intention to use SBOMs more internally. Further elaboration on this will be provided in Section 6.1.4, where a dedicated part is devoted to it.

It can be observed that B2B customers highly prioritize security and business continuity. Most of them operate in critical sectors, which may contribute to the importance of maintaining their critical processes. Specifically, P3 (B2B) and P11 (B2B) both emphasize the significance of keeping their businesses running.

'Reputational damage' is a concern specifically expressed by the suppliers, as no B2B customers mentioned it. For instance, P6 (SV) is very clear about reputational damage, stating that "*if products become unreliable because we don't know what's in them and that becomes known... it directly leads to reputational damage, not to mention the financial damage it entails*."

'Expectation' is also highly important for the suppliers. P8 (SV) repeatedly emphasizes the necessity of an industry standard for software suppliers to adopt a concept like SBOM.

The importance of good 'Tooling & automation' is another aspect mentioned solely by the supplying stakeholders. The clearest statement comes from P1 (SI), who states that "*the success of SBOM is fully dependent on good tooling*." It's noteworthy that only the supplier side seems to directly consider this, while the significance of tooling could also be essential for B2B customers who would potentially consume SBOMs.

The two themes that score relatively lower ('Ethical & ideology' and 'Recognition & exposure') are only mentioned by developers. This can be explained by the fact that they typically engage in development without compensation. They also don't have to consider other financial interests of an organization, for instance. However, looking at the scores, it is worth contemplating the fact that 60% of developers indicate the importance of recognition and exposure. For example, P12 (DEV) mentions that contributing to certain repositories can even bring recognition to their employer.

Findings: the Biggest Concerns for SBOM

It is important to note that the count for themes in the main three questions during the interviews only increases when the participants themselves brought up the topic. For example, regarding IP and copy-pasting of code, if it was only mentioned by the participants after being specifically asked about it in later (the more specific) questions, it would not be included in the chart for these results.

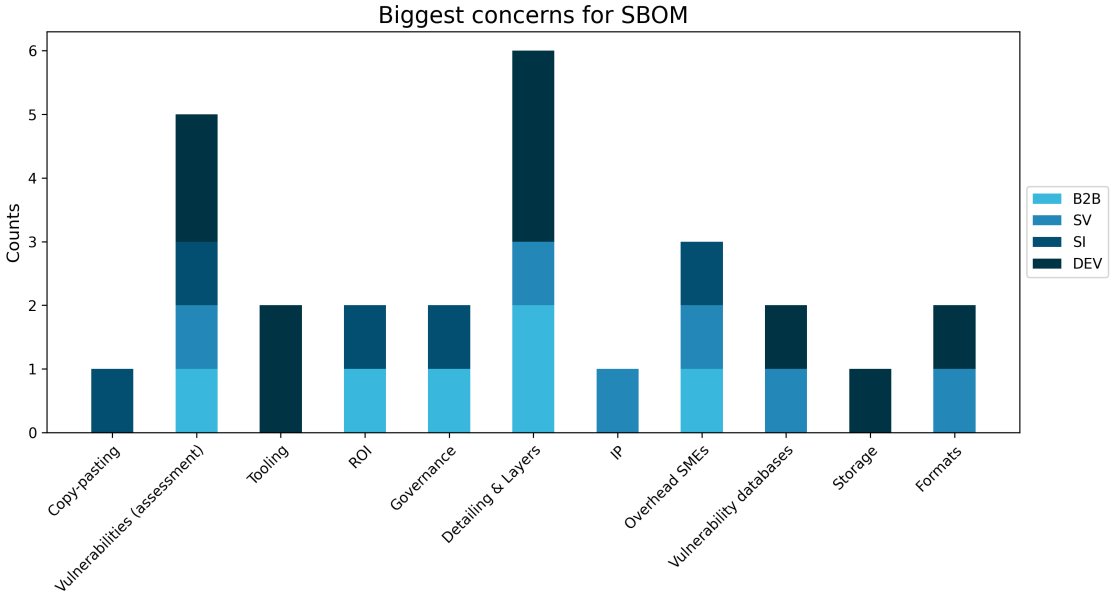


Figure 6.3: The biggest concerns for SBOM

Copy-pasting: They believe that when developers copy and paste lines of code from a library into their own code without formally importing the library, the SBOM does not identify that dependency. They find this concerning.

Vulnerabilities (assessment): They consider it a problem for SBOM that when vulnerability analysis is conducted, a lengthy list of vulnerabilities is identified, many of which may not actually be relevant or applicable to the respective organization. People also find the assessment of all vulnerabilities to determine their actual vulnerability status to be time-consuming and requiring sufficient expertise.

Tooling: They perceive the tooling not only as a significant (dis)incentive but also identify actual problems with the current state of available tooling.

ROI: ROI stands for Return On Investment. They are concerned that the incurred costs may not be recouped or they do not perceive the value it will bring to themselves in return.

Governance: Instead of technical issues, they perceive SBOM adoption more as a challenging governance issue involving various parties and responsibilities.

Detailing & layers: They have concerns about the level of detail in SBOMs and how deep the layering can be. They are convinced that virtually everyone in the SSC should be involved to have high-quality SBOMs.

IP: They are concerned that the content of SBOMs could pose a threat to the intellectual property of the parties generating them.

Overhead SMEs: They are concerned about the additional costs and effort that implementing something like SBOM may impose on SMEs (Small and Medium-sized Enterprises).

Vulnerability databases: They see problems in accessing the available vulnerability databases based on the analysis of their SBOM. Sometimes it is due to a lack of accuracy in the databases, while other times it is an issue of duplicate management that arises when multiple databases need to be consulted.

Storage: They do not see an SBOM as simply one SBOM, but rather the potential for multiple SBOMs per organization. They anticipate problems in managing and storing all those SBOMs effectively.

Formats: They fear problems and uncertainties arising from the acceptance of multiple standardized formats at the moment.

Macro-level Findings

The above chart highlights one theme that stands out: 'Detailing & layers'. With a count of 6 (37.5%), it is mentioned three times more often than most other themes. It is clear that something needs to be done to address these concerns. P13 (DEV) is one of those who mentions the level of detailing. They state that "*if SBOMs are generated at the supplier level based on open source libraries that don't have SBOM in themselves, what we'll lose is accuracy.*" Then they say, "*the later you are in the build process,*

the less accurate your SBOM will be. So if we want to have a complete benefit from SBOM, I guess it has to start all the way from the first open source developer." P10 (DEV) strongly agrees with this and also provides another example of why generating post-build SBOMs is not sufficient. For instance, when developers minify their JavaScript before shipping it around, "*the variable names that explain things that developers interact with, those are actually made into single character variable names, meaning there is no more one-to-one mapping.*" In short, they state, "*It just means that you need the SBOMs at every layer. You can't just retroactively go build them.*" This is a point that has already been mentioned in Chapter 2. The example of P10 (DEV) is one more confirmation of the issues regarding the detection of the exact libraries when generating SBOMs post-build.

Given the significant standout theme, the perspectives of multiple stakeholders are being examined. There is an interesting discovery among them. Some participants have a different stance on this issue. Considering the expert status of most of them and the significance of this concern, they will be addressed here in the macro-level findings. P16 (DEV) indicates that it largely depends on the software ecosystem being used. Most modern programming languages have a package manager that facilitates the management of third-party components. Package managers like NuGet, pip, Composer, and similar packages typically do not contain third-party components themselves. Instead, they provide a mechanism to resolve and download the required components during the build or installation process. Usually, in the dependency definition file the library versions to include are specified. Moreover, some project managers lock the exact versions of the libraries (with their hashes) in a seperate 'lock' file. P14 (SV) also believes that it doesn't make sense for developers to produce SBOMs for their components. For some of the same reasons as P16 (DEV), they state that SBOMs should be generated when software is compiled by professional vendors. The combination of all the different (OSS) components together provides the SBOM. CycloneDX also has close integration with various major build platforms such as Microsoft, Java, etc. They also see that the SBOM should be generated when the software is compiled in order to obtain the exact manifest. Only the compiler knows what it's doing and which packages it pulls in. P14 (SV) recognizes the different package managers and sees them as a good way to capture all packages in various ecosystems in different ways. However, there will never be standardization between them. That's what SBOM provides; the abstraction layer on top. P15 (DEV) fully agrees with this and sees SBOM as a kind of standardized format for representing the dependencies of various package managers in the same way. Additionally, they see the advantage that it should be easier to build tooling around it to understand all these separate package managers.

The concern could lead, or could have already led, to strong disincentives. The factor strongly influences the quality of SBOM, and since it was found to be essential for SVs and SIs, it could become a problem. However, an interesting finding is that only one SV participant mentioned this concern (25%), and no SI participants did. It suggests that, so far, this factor has not served as a disincentive. However, it could become one in the future, indicating a point of attention. Moreover, this factor could also impact developers' recognition and exposure incentives. 60% of developers express their concerns about this factor. If SBOMs at the SV level only consider primary dependencies, many components with deeper layers (and their developers) will not be acknowledged, which might undermine the incentive. Finally, it could also affect the expected benefits of B2B customers regarding security and continuity assurance. When a substantial amount of relevant data is missing, not all possible vulnerabilities, for instance, will be identified when an analysis is conducted on the SBOM.

In addition to "Detailing & layers," the concern of "Vulnerabilities (assessment)" is also widely shared (31.3%) among the stakeholder group participants regarding the functionality of SBOM. P3 (B2B) indicates that there are already many false positives encountered when scanning their networks. This is also confirmed by P12 (DEV), who often observes this in their work in the security business (for their employer). Both P14 (SV) and P9 (SI) express their concerns specifically about CVEs. They note that there is a significant difference between the number of CVEs identified through vulnerability analysis of SBOMs and the actual number of vulnerabilities within a particular organization. The reasons for this are consistent with what was previously identified in Chapter 2. P12 (DEV) further states that assessing all these risks actually takes too much time. P1 (SI) raises doubts about the expertise level of B2B customers and suggests that such tasks should be outsourced to cybersecurity experts. There appear to be efficiency-mitigating consequences and effectiveness-mitigating consequences from the vulnerability issue-related factor. For the B2B stakeholder group, the consumption of time and efforts will cause disincentives. For the SV stakeholder group, the effectiveness issues stemming from a significant number of false positives lead to disincentives. This adversely affects the quality of SBOM findings.

P6 (SV) expresses concerns about the overhead it may impose on SMEs, along with two other participants (P3 (B2B) and P9 (SI)). In the context of broad adoption, they believe that it could be challenging due to this overhead.

Apart from the prior two concerns, there are no other prominent issues that stand out. However, the participants have touched upon some interesting points in the context. Concerns related to tooling include the quality of SBOMs. P10 (DEV) is working on an evaluative SBOM project that assesses their quality. They observe that the current tooling is immature and often lacks version numbers or unique identifiers. P14 (SV) agreed on this and related it also with freshness risk, indicating the extent to which a component has not been updated over time.

Concerns regarding governance are mainly expressed by P3 (B2B). They suggest that in order to get the whole game running, it needs to be developed in a multidisciplinary manner with involvement from various stakeholders. It may require a comprehensive program involving stakeholders from different sectors, including suppliers, business, specific

developers, procurement, legal affairs, compliance, and software personnel. They believe that this is the only way to make progress and it should be done through a larger program.

Both participants who have elaborated on concerns regarding vulnerability databases are also worth mentioning as they have significant experience with their use and have encountered challenges in this regard. P13 (DEV) identifies two problems: once an SBOM is obtained, querying databases (open source or commercial) is necessary to retrieve CVE information. The NVD database is not always precise in its vulnerabilities, so multiple databases need to be used to obtain accurate data. This leads to the management of duplicates. P14 (SV) also mentions the difficulty of relating data on the developer side to data in databases such as the NVD, noting the lack of a unique identifier.

Lastly, briefly addressing the internal use of SBOMs by suppliers, which will be further explored in Section 6.1.4, P9 (SI) acknowledges that they see more challenges and complications in providing SBOMs to customers compared to using them solely for internal purposes.

Meso-level Findings

Regarding patterns and relationships among the stakeholder groups themselves, the distribution of concerns appears to be manageable. It seems that each stakeholder group primarily focuses on challenges within their own domain. The developer side primarily focuses on tooling, while businesses concentrate more on governance, ROI, and overhead costs for SMEs. This is not necessarily a problem unless the self-focused approach hinders adoption in general. This aspect will be kept in mind for future considerations. What became apparent, though, is that ROI is viewed from two perspectives, including within the businesses themselves. From a B2B standpoint, P2 (B2B) strongly questions what level of security they are actually getting for a certain price, including with SBOMs. Security is subjective, which makes it all quite tricky. On the other hand, P9 (SI) highlights the supplier's perspective. They state, "*The challenge you often see here, depending on the market segment you're in, is the quality you deliver in relation to the time you invest, so it's really about return on investment.*" The perspectives on the costs involved with SBOM and how the SSC stakeholders perceive them will also be further discussed in the next subsection, regarding the results from the more specific questions.

6.1.3. Results of the More Specific Questions

This Section shifts its focus to the more specific question set, which is still open-ended and semi-structured. However, most of these questions were related to the identified (dis)incentives in 5.1, which had a high probability of impacting SBOM adoption. In identifying patterns, we will also explore how certain findings may be connected to the findings from the previous subsection.

Findings: the Biggest Risks for the SSC

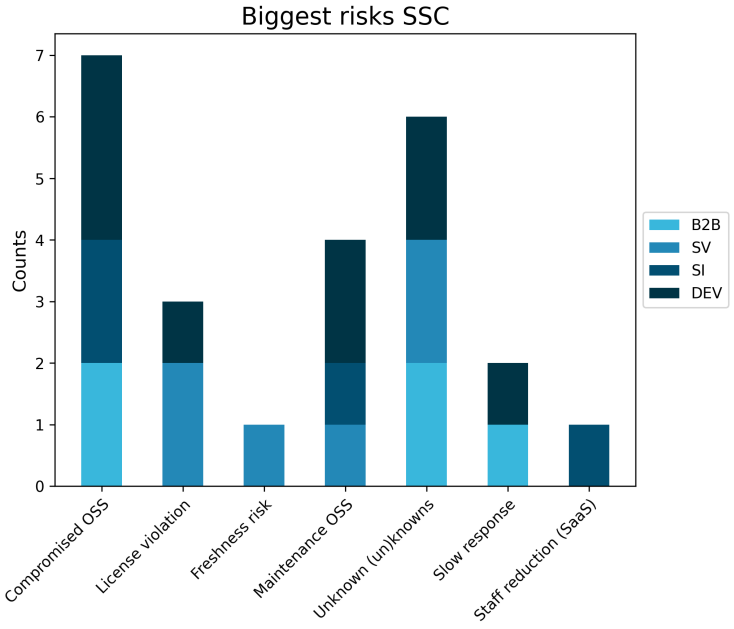


Figure 6.4: The biggest risks for the SSC

Compromised OSS: The stakeholders perceive the risks of compromised open-source components that subsequently flow throughout the SSC as significant.

License violation: The stakeholders identify risks related to license violations due to the extensive use of open-source components and the lack of transparency.

Freshness risk: Stakeholders perceive risks in the (lack of) updates for specific packages, as it can impact the security and functionality of the software.

Maintenance OSS: Stakeholders recognize risks in the fact that those who maintain open-source components are often a group of developers who do it on a voluntary basis as a hobby, rather than dedicated professionals. This raises concerns about the reliability, support, and timely updates of these components.

Unknown (un)knowns: Stakeholders express concerns about unknown vulnerabilities that may exist within their software but of which they are unaware. This fear stems from the potential risks associated with undiscovered vulnerabilities and the potential for exploitation by malicious actors.

Slow response: Stakeholders are concerned about the inability to respond promptly to "unknown knowns" when they lack visibility into the components and dependencies within their software. This fear arises from the challenge of addressing issues or vulnerabilities that are present but remain unidentified, potentially leaving the software exposed to risks without appropriate mitigation measures in place.

Staff reduction (SaaS): Stakeholders express concerns that as businesses increasingly adopt SaaS and cloud solutions, they are downsizing their internal security staff. This downsizing trend results in a reduction in expertise and manpower available within the organization when needed. Furthermore, the decreasing understanding of how software integrates with their own infrastructure among employees adds to the apprehension.

Macro-level Findings
Compromised OSS is seen as a significant problem (7 counts; 43.8%), which aligns reasonably well with the literature review conducted at the beginning of this research. However, it is important not to forget that even professional software vendors can be hacked, leading to supply chain attacks like the SolarWinds incident (Martínez & Durán, 2021).

The presence of unknown (un)knowns is also a concern in this context (6 counts; 37.5%). There is fear that vulnerabilities may go unnoticed and gradually infiltrate all organizations. This would inhibit organizations from responding to it, or not even responding at all, and not being able to mitigate harm.

Furthermore, within the associated dataset, several causes have been identified for the risks associated with OSS. Both P1 (SI) and P7 (SI) indicate that developers often lack sufficient time to thoroughly test the software components they incorporate. For instance, P1 (SI) states that there may be instances where pieces of OSS are integrated into products without sufficient investigation of any associated issues, mainly due to time constraints. P7 (SI) also confirms that their developers face similar problems due to time constraints. However, he emphasizes that if a client asks for an estimated development time, it is important to allocate an extra day if it ensures the secure delivery of the product. After all, security is an integral part of quality.

Another notable concern is the maintenance of OSS, which is frequently mentioned. For example, P12 (DEV) mentions that the "*maintenance of such projects often relies on a small group of people who do it for fun.*" If they lose interest or no longer have the time, they may discontinue their maintenance efforts.

Meso-level Findings
It is noteworthy that "Licensing violation" is once again only mentioned by stakeholders from the supplier side. This aligns well with the primary benefits highlighted by such stakeholders in the previous subsection. However, P9 (SI) offers a different perspective. Despite being an IT-SI, P9 (SI) suggests that if one encounters licensing problems, it simply means that they did not do their homework sufficiently. Nevertheless, it is not illogical for individual developers to occasionally fall short in doing that homework. As previously mentioned by P1 (SI) and P7 (SI), developers often face time constraints that prevent them from thoroughly documenting, testing, and ensuring compliance with licensing requirements. Furthermore, no distinct patterns emerge from the obtained results apart from the one mentioned.

Findings: the Financial Aspects of SBOM
As observed from the most significant incentives involved, financial incentives were also high on the list. The influence of financial (dis)incentives on adoption can be both positive and negative. For example, P5 (B2B) clearly states that their perception of SBOM adoption strongly depends on factors such as cost (compared to alternatives). The example of P2 (B2B) and their concerns regarding ROI have already been mentioned. This Section will delve into the empirical data obtained from participants' answers regarding the cost aspect of SBOM. It is important to note that these specific questions were not posed to OS developers, hence their absence in the following bar charts.

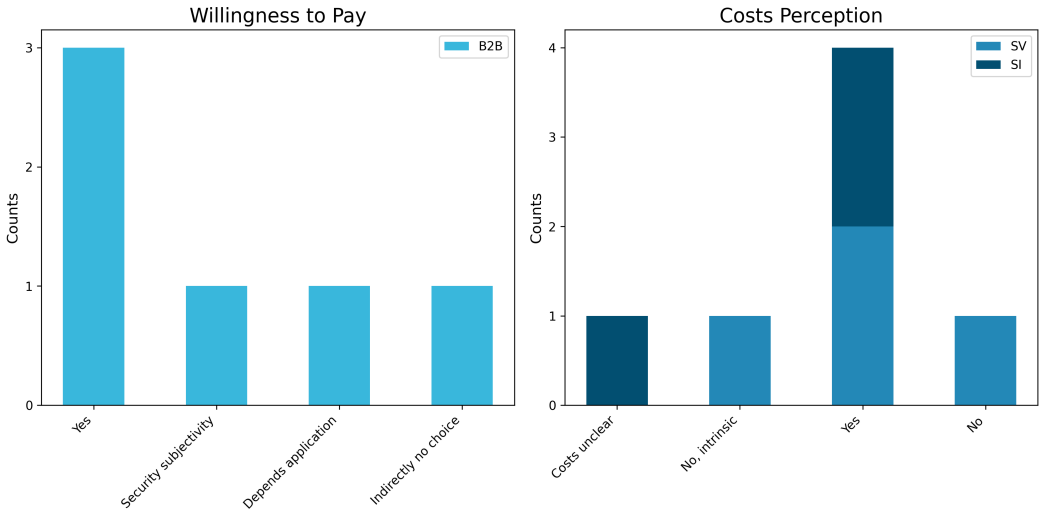


Figure 6.5: The financial aspects of SBOM

Yes (*left*):	On the B2B side of the SSC, there is a willingness to pay a higher price for software products that are provided with SBOMs.
Security subjectivity:	There is uncertainty from the B2B customer regarding what they will actually receive in return for an investment in security.
Depends application:	Whether a B2B customer is willing to pay extra for SBOMs also depends on the specific application for which it is intended.
Indirectly no choice:	It is believed that the only way SBOM adoption will occur is through legislation and regulations. If suppliers are required to provide SBOMs, the associated costs will undoubtedly be passed on to customers.
Costs unclear:	On the supplier side of the SSC, there is uncertainty regarding the costs associated with SBOM implementation. As a result, suppliers find it challenging to determine whether they can pass on those costs to customers.
No, intrinsic:	On the supplier side, there is no definite refusal, but rather a belief that providing products of quality should inherently include such practices. It is considered an intrinsic desire to incorporate these aspects.
Yes (*right*):	Suppliers are under the assumption that they can pass on the additional costs associated with SBOM to their downstream B2B customers.
No:	Suppliers are under the assumption that they cannot pass on the additional costs associated with SBOM to their downstream B2B customers.

Macro-level & Meso-level Findings

These findings are scaled under macro and meso levels. In the left chart, there is only a single stakeholder group, and even within the right chart, there is no significant difference between software vendors and IT-SIs. By visualizing the relationships from both perspectives regarding the cost aspect, a sort of meso-level analysis is already being applied.

What is apparent according to the findings, B2B customers within the SSC are quite willing (75% of paricipants) to pay more for software products that come with SBOMs. This indicates a recognition of the value and importance of SBOMs, given the high score of Financial for the impactful (dis)incentives. It suggests that B2B customers prioritize the inclusion of SBOMs in their software procurement process and are willing to invest financially in obtaining products that provide this additional level of information and assurance. There seems to be little friction between stakeholders regarding their willingness to pay from the B2B perspective and their belief in being able to pass on the costs from the SV and SI perspective. This should positively impact the adoption of SBOM within the financial incentive category.

Given the relatively low number of counts due to the involvement of only one stakeholder group, the remaining three findings regarding B2B customers are still noteworthy. The example of security subjectivity raised by P2 (B2B) has been mentioned multiple times. However, this same participant brings up another interesting issue: "*If you can obtain an SBOM by paying for it, can you also purchase products without an SBOM and receive a discount?*" This additional aspect is also a concern expressed by P9 (SI), as it would introduce more complexity and hassle.

P5 (B2B) provides an example of the software for which they would like to have SBOMs: "*I wouldn't be willing to spend money on an SBOM for a calculator, but I would be willing to spend a bit more for a customer database if it helps me manage my risks.*"

Lastly, P11 (B2B) emphasizes their belief in widespread SBOM adoption through regulation. They state that if software vendors are obligated to produce and provide SBOMs, B2B customers will have no choice but to comply and pay for them.

The other side of the cost aspect regarding SBOM pertains to the stakeholders who will have to incur the expenses, namely the suppliers. Within the scope of this research, this includes software vendors and IT-SIs. It is found that the majority (57%) of these stakeholders believe they can pass on additional costs to B2B customers. For instance, P6 (SV) mentions that nowadays, this is less common on an hourly billing basis but rather occurs in large project-based scenarios. At the beginning of such projects, it is stated, "*This product that we are going to deliver will save or generate a million for your business annually. And thus, it is justifiable that this project costs two and a half to three million. The specifics of the people involved, the tools used, or the frameworks employed become less relevant.*" In fact, P6 (SV) suggests that if all those details were discussed, people unfamiliar with SBOM, for example, would start debating whether it is necessary or not. Similarly, P14 (SV) views SBOM as part of a vulnerability management program, positioning it more as an operational expense rather than a capital expense. They state, "*These are recurring costs that need to be incorporated into your services. Eventually, you will pass them on to the customer.*" In principle, this is positive news for SBOM adoption: B2B customers are willing to pay, and the supply side generally believes they can pass on the costs. However, it should be noted that there are no specific figures indicating how much both parties think they can pay or pass on. This was also something that P1 (SI) struggled with during the interviews.

Furthermore, the percentage from the supplier side is considerably lower than that of the B2B customers. For example, P8 (SV) firmly believes they cannot pass on the costs, at least not until customers explicitly demand it, which they do not foresee happening at the moment.

Findings: Seeing SBOMs Preemptively

The idea of accessing SBOMs in advance before downstream stakeholders purchase software from a vendor is something that most stakeholders had not considered before. This was reflected in the results regarding the expected benefits of SBOMs. A few individuals seemed to think it would be a good idea to utilize SBOMs during procurement processes to enable better risk assessment. Here are the results following the more specific question about it.

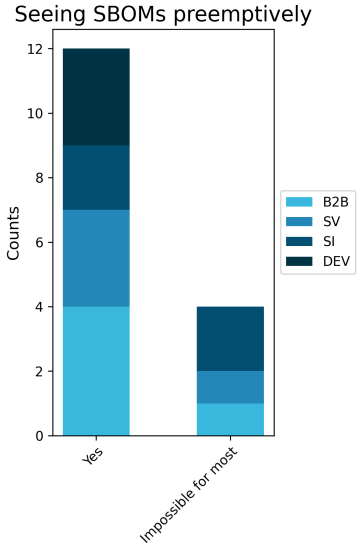


Figure 6.6: The perceptions on seeing SBOMs preemptively

Yes: The participant anticipates that having access to the SBOM during procurement processes would be a good idea and should be feasible.

Impossible for most: The participant notes that in many cases, during the procurement processes, it is not clear what will ultimately be delivered in terms of software. Many changes occur during the integration phase within the relevant ICT infrastructure.

Macro-level Findings

One initial interesting finding in analyzing the data was that none of the participants strongly opposed the idea. In fact, 75% of all participants indicated that they found it to be a good idea if it were feasible. However, there is a caveat. Multiple participants emphasized that in many cases, it is not possible to access SBOMs because the final product is not yet determined when software is purchased. During the development and integration processes, significant changes occur, making it impossible to obtain corresponding SBOMs in advance. The participants who support the idea would mainly rely on Commercial Off-The-Shelf (COTS) software products. This is confirmed by P14 (SV), who even mentions that they already see many large enterprises requesting such data from their suppliers in advance.

P8 (SV) and P12 (DEV) are both in favor of the idea but have doubts about its actual value. P8 (SV) mentions that "*customers would only ask if we have it but wouldn't do much with it*." The reasoning aligns with that of P12 (DEV), assuming that if customers are allowed to access SBOMs, they might not know how to effectively utilize the information and that evaluating the quality of the software would still be challenging.

Meso-level Findings

In terms of patterns and relationships, the frequencies of the different stakeholder groups mentioning the themes are fairly evenly distributed. There are no significant findings at the meso-level that need to be highlighted.

Findings: SBOM in the Context of Intellectual Property

Following the previous discussion on preemptively seeing SBOMs, initial questions arose regarding the potential threat of SBOMs to IP. As revealed in the initial questioning regarding the participants' major concerns about SBOMs, IP was not a significant concern (mentioned only once). Furthermore, regarding the access to SBOMs, it was found that as long as the SBOMs are not publicly accessible to everyone, the potential IP issue may not be a significant problem. Here are the results of the interview question regarding IP.

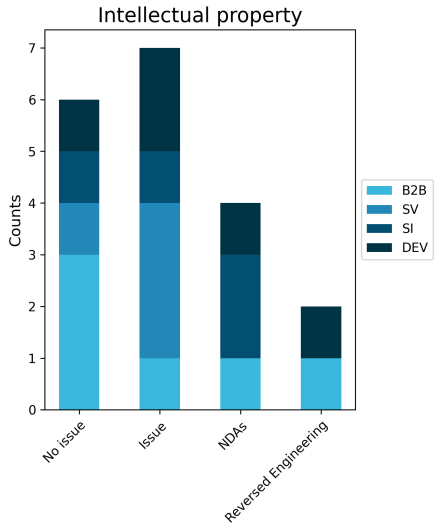


Figure 6.7: SBOMs in the context of intellectual property

No Issue:	Participants do not anticipate SBOMs to pose a threat to the parties developing software.
Issue:	Participants do foresee potential issues concerning the disclosure of (parts of) the intellectual property (IP) of the parties developing software.
NDAs:	Participants mentioned that NDAs could be a solution to prevent the leakage of IP, regardless of whether SBOMs are considered an issue or not.
Reversed engineering:	Participants are of the opinion that if others were very curious about the third-party components present in their software, they could still discover this information through reverse engineering.

Macro-level Findings

The issue of whether SBOMs pose a threat to stakeholders' IP is almost evenly divided. There is a difference of only one count between the number of participants who suggest it could be an issue and those who do not. This contrasting difference is significant and will require further exploration in the thesis. It is also possible that those who saw it as an issue considered it to be a minor one. When comparing the results with the concerns participants had about SBOMs and their adoption (from the main 3 questions), they do not align. There, only 6.3% of the participants identified IP as a major concern.

For example, P14 (SV) states, "*The unique composition of that open-source software says something about how you approach certain problems. If I were to make the bill of materials of our platform completely public, our competitors could see which software we use under the hood, and that could give them a competitive advantage.*" However, they add that it depends on whether the SBOM needs to be made available only to the customer or if it must be publicly accessible.

In addition to participants who believe SBOMs should not pose a threat to IP or do not see the connection, P3 (B2B) expresses a stronger stance. They argue that the transparency required in the supply chain should outweigh any potential IP risks for a software vendor.

P2 (B2B) takes a broader view of IP. They mention that transparency can only work if everyone is transparent. "*And in that sense, that is also the reason why the Western market is very afraid of the Chinese market. So on one hand, you want to be open, but if people can copy it within one or two days, and the other side may not be as open, then globally, you definitely have a problem.*"

Interestingly, P11 (B2B) highlights a different aspect of IP. They suggest that OS developers could receive more recognition for developing their components since the origins of the initial components would remain known for a longer

time in the SSC.

The theme of "NDAs" is also noteworthy, with four counts. The description of the theme under the bar chart generally captures the meaning conveyed by P1 (SI), P5 (B2B), P9 (SI), and P13 (DEV).

Meso-level Findings

The most notable observation is the significant imbalance between B2B participants who consider it a potential issue compared to those on the supply side, and vice versa for the "No issue" perspective. This raises the suspicion that B2B customers do not care, as it is not their IP but rather that of their suppliers. In any case, there are twice as many participants from the parties producing SBOMs who do not see it as a problem. On the other hand, there are three times as many B2B participants who consider it a problem. This is certainly worth further investigation and analysis in the later stages.

Findings: SBOM in the Context of Law and Regulation

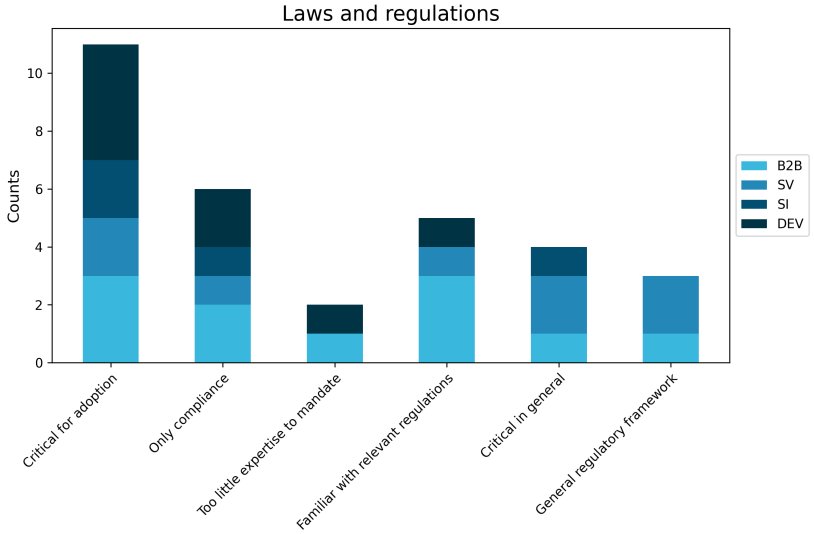


Figure 6.8: SBOMs in the context of law and regulation

Crucial for adoption:	Participants are under the assumption that regulations and legislation play a crucial role in achieving widespread adoption of SBOMs.
Only compliance:	Participants are concerned that if regulations and legislation strictly mandate SBOMs, it may become more of a compliance or checklist requirement for stakeholders rather than adding value.
Too little expertise to mandate:	Participants believe that if SBOMs were made mandatory, it would be ineffective because the involved stakeholders do not know how to effectively utilize them.
Familiar with relevant regulations:	The participant is familiar with the relevant laws and regulations related to SSC risk management, such as NIS 2, DORA, CRA, or EO14028 from the U.S.
Critical in general:	Participants are critical of legislation and regulations in general, regardless of their relevance to the topic at hand.
General regulatory framework:	Participants believe that legislation and regulations should primarily serve as a framework for what needs to be done, while the specific implementation and approach should be determined by the involved stakeholders themselves.

Macro-level Findings

It is evident from the findings that most participants (68.8%) believe that regulations and legislation are crucial for the widespread adoption of SBOM throughout the SSC. This theme stands out prominently among others and should be considered in the further recommendations. P11 (B2B), for example, strongly believes that SBOM's success relies on regulations and legislation, as they do not see it happening otherwise. The high score (37.5%) of "Regulatory compliance" for the most impactful incentives also confirms the significance of this theme.

However, adoption alone does not necessarily guarantee the achievement of the main objectives of SBOM. Not everyone who deems regulations necessary for adoption believes that they actually add value to the SSC. There are concerns regarding compliance aspects. Six participants express concerns about SBOM becoming more of a checklist requirement rather than a tool for improvement. P16 (DEV) mentions that government agencies now receive SBOMs according to EO14028 but do not do anything with them; it has become a mere formality. P8 (SV) also points out that many of the security and compliance measures they have to implement are merely checkmarks they need to meet.

P3 (B2B) emphasizes that although one can maintain an idealistic perspective, regulations will ultimately enforce SBOM adoption. It can create demand and awareness among users and also push suppliers to establish governance to ensure high data quality. Otherwise, the efforts may be futile.

P2 (B2B) raises the importance of enforcement and questions the effectiveness if regulatory authorities lack the knowledge or means to enforce compliance. They express doubts about whether the quality of SBOMs would be verified and whether organizations would effectively utilize them.

There were also participants who held a critical view. For instance, P6 (SV) and P9 (SI) expressed concerns that regulations in the IT field can be too late or formulated without sufficient knowledge or expertise from those directly involved. This aligns with the perspective that regulations should serve as a framework for compliance rather than explicitly dictating how to achieve it. P11 (B2B) highlights that the effectiveness can vary significantly across organizations, and overly explicit rules may miss the mark.

P14 (SV) provides nuanced criticism, mentioning the example of CRA where it was explicitly stated that no vulnerabilities should exist in software. They argue that this approach is futile as it is simply unattainable. It would be more effective to work towards reasonable goals.

Lastly, the "too little expertise" theme is interesting, despite having a relatively low count score. It will be further discussed in a broader context in Section 6.1.4.

Meso-level Findings

One noteworthy and relevant finding among the stakeholder groups is the lack of awareness and knowledge regarding regulations and legislation, particularly on the supplier side of the SSC (OS developers, software vendors, and IT-SIs). Surprisingly, the individuals I spoke with from these groups were largely unfamiliar with existing or upcoming laws related to supplier management, even though one would expect such regulations to be relevant for them as well. Directives like NIS 2 could have direct implications for suppliers regarding security measures and other aspects.

Even C-level executives within these stakeholder groups were not fully aware of the regulations, which is remarkable. There seems to be a lack of awareness and understanding regarding compliance requirements. Additionally, some individuals expressed the perception that compliance with regulations like NIS 2 would be challenging. For instance, P8 (SV) believes that customers taking responsibility for their own supply chain risk management is still a distant reality.

This finding highlights the need for increased awareness and education regarding relevant laws and regulations within the supplier community. It is crucial for suppliers to understand their obligations and actively engage in compliance efforts to meet the evolving regulatory landscape.

Findings: Vulnerability Analysis

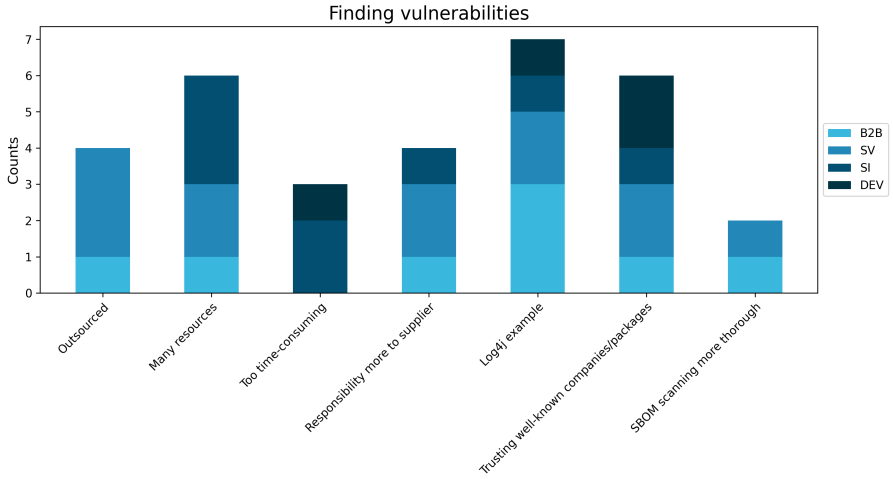


Figure 6.9: Vulnerability analysis

Outsourced:	Participants mention that they can save time by outsourcing vulnerability discovery to external security firms, thus reducing the need for them to dedicate their own resources to this task.
Many resources:	Participants indicate that the process of identifying vulnerabilities in the software stack requires significant resources in terms of time and/or money.
Too time-consuming:	Participants express that the process of identifying vulnerabilities is time-consuming and often deemed too burdensome to undertake.
Responsibility more to supplier:	Participants assert that the responsibility for identifying vulnerabilities lies primarily with the supplier side. They believe that suppliers should prioritize the security of their products and take proactive measures to keep them secure.
Log4j example:	Participants refer to the example of Log4j when discussing significant vulnerabilities within the SSC. They highlight this as a major use case for SBOM.
Trusting well-known companies/packages:	Participants express their trust in large, well-known software packages or reputable suppliers from whom they obtain software components, believing that these entities prioritize security measures.
SBOM scanning more thorough:	Participants believe that SBOMs should contribute to making current network scanning efforts more targeted and focused when searching for vulnerabilities.

Macro-level Findings

It is remarkable that the Log4j example has been mentioned the most by participants (43.8%). This indicates that the Log4j vulnerability and subsequent attack had a significant impact on the entire SSC, and a considerable number of organizations have become more alert as a result. P14 (SV) highlights the alarming aspect that the vulnerability (Log4Shell) could automatically exploit itself within organizations throughout the SSC, which is a frightening prospect. P11 (B2B) also notes that they have observed increased awareness and focus on supply chains and dependencies among surrounding companies since this attack.

P6 (SV) provides a clear use case for SBOM by stating, "*During the Log4j incident, the entire organization was in turmoil for a period of four days simply because we didn't have the SBOM.*" Not only the operations department but also all the involved architects were constantly questioned about the software components they had used. "*It easily cost us around 240 hours.*"

The second most mentioned theme is "Many resources." While somewhat self-explanatory, it is significant that participants acknowledge the need to allocate resources to address this issue. It indicates a level of awareness that software risks are business risks, as emphasized by P3 (B2B).

The theme of "Trusting well-known companies/packages" being mentioned six times (37.5%) by participants is noteworthy. It seems to deviate from what is prescribed in regulations and standards. However, it is closely related to the theme of "Responsibility more to supplier," which is also frequently mentioned.

The issue of "Too time-consuming" provides an explanation for why trust often lies with the suppliers. For example, P15 (DEV) states that it takes too much time to thoroughly check everything they use for their own development. Similarly, P3 (B2B) mentions that when procuring from large suppliers, it is expected that things should be in order.

According to P9 (SI), this expectation holds true for large suppliers who may have dedicated security teams with extensive expertise. However, individual companies may encounter problems if they have downsized their security staff, believing they were no longer necessary. When an incident occurs or action needs to be taken, there may be a lack of knowledge and expertise within the organization. This reliance on vendors aligns with the increasing adoption of SaaS solutions. In such cases, organizations have less control over the software and tend to assume that security is taken care of by the supplier. P2 (B2B) confirms this finding.

Meso-level Findings

The findings regarding vulnerability analysis also reveal several noteworthy aspects at the meso-level. Firstly, it is observed that relatively few developers mention the Log4j incident. This could be explained by the fact that they are not the primary target of the severe consequences of such an SSC attack. However, there must still be awareness among this stakeholder group, as malware can also be hidden in their software components, for example.

Contrarily, the lack of time is emphasized by the supplier side of the SSC (developers and software vendors). As mentioned earlier, SSC attacks originate by compromising a software component at an early stage and silently allowing it to propagate throughout the SSC. Therefore, the reported lack of time by this group is a significant finding.

These findings suggest the existence of a potential tension between the awareness of developers regarding the impact of vulnerabilities and their ability to dedicate sufficient time and resources to ensuring the security of their software components. Bridging this gap and ensuring that all stakeholders within the SSC are aware of the potential risks and take necessary measures to mitigate them is crucial.

Findings: Trust in the SSC and the impact on SBOM

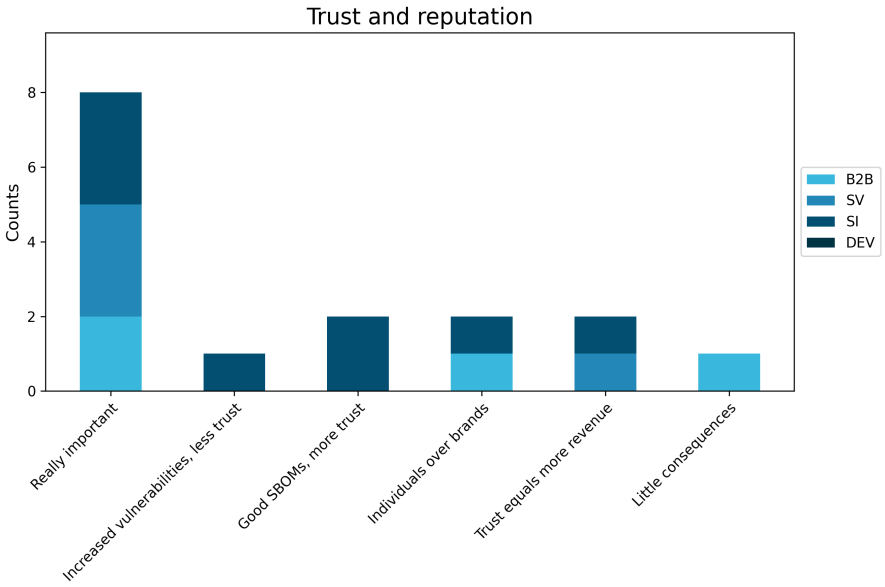


Figure 6.10: Trust in the SSC and the impact on SBOM

Really important:	It is assumed that trust and reputation are of utmost importance within the SSC.
Increased vulnerabilities, less trust:	There is concern that if the analysis of an SBOM reveals the presence of various vulnerabilities (whether they are vulnerable or not), it will undermine trust. They state that transparency isn't beneficial to all.
Good SBOMs, more trust:	Conversely, it is believed that if SBOMs indicate that the software has few or no vulnerabilities, it can enhance trust.
Individuals over brands:	It is argued that the composition of employees from a supplier assigned to a project is more important than the name of the company itself.

Trust equals more revenue:	It is suggested that higher levels of trust have a positive effect on revenue. Customers would be more likely to purchase and continue to engage with services, in this case.
Little consequences:	It is believed that despite temporary loss of trust due to reputational damage, trust is quickly restored.

Macro-level Findings
The findings from the bar chart confirm the significance of trust and reputation for stakeholders in the SSC (given 50% of them mention it), aligning with previous observations regarding the most impactful incentives. However, the significance of trust applies to all supplier-customer relationships. Notably, P1 (SI) expressed concern that SBOMs could potentially diminish trust in suppliers. The disclosure of numerous CVEs, regardless of their actual vulnerability status, may cast a negative perception. Conversely, a low number of CVEs might enhance trust.

Furthermore, P2 (B2B) and P1 (SI) emphasized the growing importance of the individuals involved in delivering services rather than relying solely on brand names. They state that within the same organization, the quality of developers can vary, prompting customers to pay more attention to individual expertise and performance.

P11 (B2B) also highlights one additional noteworthy point. They observe that although incidents can indeed result in reputational damage, this damage often proves to be temporary, with trust being restored relatively quickly. However, given that this observation was mentioned only once, it is prudent not to attach excessive significance to it.

Meso-level Findings
The only mild observation here is that it appears to be primarily suppliers who perceive trust as highly important. For them, selling their products is naturally their top priority, so they must maintain the necessary conditions for themselves as effectively as possible. They also have to contend with competition and similar factors. For instance, P9 (SI) indicates that if the trust from customers diminishes at some point, "*you might as well quit this business*."

Findings: SBOM Demand

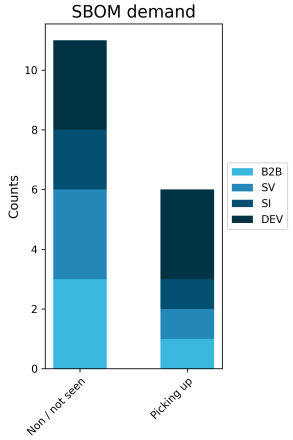


Figure 6.11: Demand for SBOMs

Non / not seen:	The participant has not yet heard or seen anything about SBOM from other stakeholders.
Picking up:	The participant observes that stakeholders around them are increasingly engaging with SBOM. They have noticed its presence at various conferences as well.

Macro-level Findings
From the above chart, not many significant findings can be drawn, except that the majority (68.8%) indicates that they have not yet seen or expressed demand signals for SBOM within the SSC. The initial participants (e.g., P13 (DEV)) have encountered SBOM at conferences and heard about it from industry stakeholders. P14 (SV) is slightly ahead and has noticed some large enterprises taking their first steps in SBOM implementation. Despite P4 (SV) and P6 (SV) being on the verge of starting to explore SBOM for their organizations, they have not seen any demand from customers as of yet.

P6 (SV) expresses surprise and draws a comparison with Germany. They note that in Germany, there seems to be a greater awareness of these issues, even though the market there may be lagging behind. They highlight that the Netherlands is more innovative, but there is less concern about vulnerabilities.

P7 (SI) indicates that there is still limited awareness among customers. They observe that certain obligations, such as those related to General Data Protection Regulation (GDPR), are seen as necessary evils, leading people to adopt a casual attitude. They describe a mindset of "put something on paper, sign it, and at least we have something. And if there are any changes over time, let's not bother updating the contract because I don't want to deal with it."

Meso-level Findings
At the meso-level, it appears that no significant patterns can be discerned from the bar chart. The distribution of responses is relatively balanced across the different categories, indicating a lack of clear trends or consensus among participants in that specific context.

Findings: SBOM Sentiment

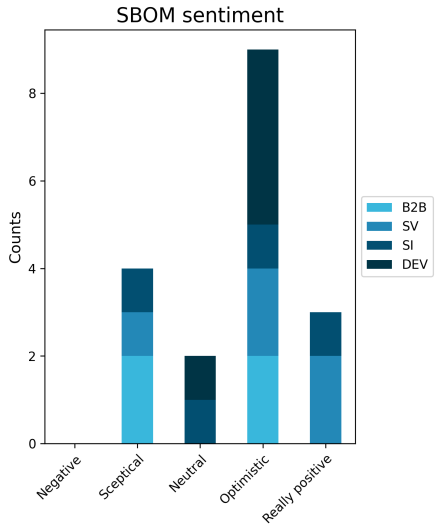


Figure 6.12: Sentiments regarding SBOM

Negative:	The participant describes its feelings towards SBOM as negative.
Sceptical:	The participant describes its feelings towards SBOM as sceptical.
Neutral:	The participant describes its feelings towards SBOM as neutral.
Optimistic:	The participant describes its feelings towards SBOM as optimistic.
Really positive:	The participant describes its feelings towards SBOM as really positive.

Macro-level Findings
The majority of participants (56.3%) express optimism, with a considerable number being very positive about SBOM. These are significant scores, indicating a belief in the potential of SBOM, especially when considering the associated benefits.

Participants overall display a high level of optimism regarding the SBOM concept itself. However, some participants express more skeptical feelings about the adoption of the concept. This goes for P1 (SI) and P6 (SV), for instance. These are also included in the bar chart, though.

Meso-level Findings
Indeed, a 50% skepticism rate among B2B customers is relatively high compared to the overall sentiment. While it could be a coincidence, it does stand out when considering the broader picture. Apart from this, there don't seem to be any significant deviations or outliers at the meso-level in terms of sentiment.

6.1.4. Interesting Results in General

In addition to the findings directly derived from the categorized interview questions (first the main three, then the more specific ones), several other interesting topics were touched upon and identified as themes. These themes emerged during various moments throughout the interviews and have not been specifically addressed in the results under a particular question. However, it would be a missed opportunity not to include this information in the findings of this research, as it still contributes as empirical data. The criterion used is that a theme must have been mentioned by at least two different participants to be included in these additional "generally interesting findings." Below is the horizontal bar chart displaying all the identified themes and their respective counts, categorized by stakeholder groups. It may also be relevant to examine the meso-level patterns and relationships for these findings. Furthermore, attention will be given to potentially relating certain findings to the previously discovered interesting points, where applicable. First, a brief explanation will be provided for each theme. Then, for each theme, starting from the most frequently mentioned to the least, the possible macro-level significance or impact of that theme will be discussed, along with any relevant meso-level findings within it. Here are the results:

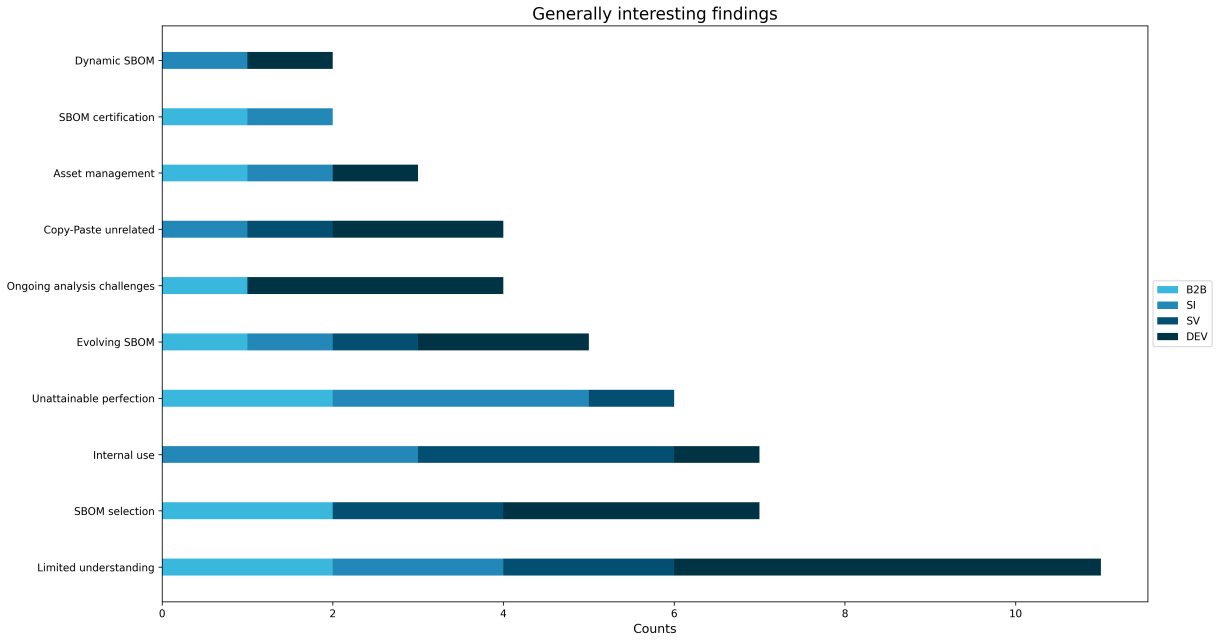


Figure 6.13: Generally interesting findings

Dynamic SBOM: The participant states that SBOM is not something you produce once and then never look at again. Instead, it needs to be continuously maintained and updated.

SBOM certification: The participant suggests that it could be a good idea to certify suppliers based on their SBOMs. This approach could ensure data quality.

Asset management: The participant argues that in addition to having SBOMs, having effective asset management is crucial (for the functionality of SBOMs).

Copy-Paste unrelated: The participant suggests that the highlighted issue of copy-pasting can no longer be categorized as an SBOM problem.

Ongoing analysis challenges: This theme specifically addresses current challenges related to vulnerability analysis. The participant indicates that, apart from SBOM, they are experiencing issues and challenges regarding the analysis itself, such as false positives and similar issues.

Evolving SBOM: Within this theme, the participant expresses the view that SBOM is still in its early stages. It is still a somewhat broad concept for which there is not yet a clear, uniform understanding of what should be included and who should be responsible for what aspects, among other things.

Unattainable perfection:	The participant suggests that striving for perfection in security is unnecessary. In fact, it is often not feasible to achieve perfection in security measures.
Internal use:	The participant acknowledges the use case for SBOM in internal utilization (as well). This particularly refers to suppliers who could better ensure their own quality by utilizing SBOM.
SBOM selection:	The participant highlights that there can be significant differences in the applications and/or systems for which the organization would or would not require an SBOM.
Limited understanding:	The participant indicates that a specific stakeholder group lacks the knowledge or expertise necessary to successfully implement SBOM adoption.

Findings: Limited understanding

One of the most prominent findings identified by the participants is the lack of knowledge and expertise, which was mentioned 11 times. This high count indicates a significant and serious concern regarding this theme. The distribution of counts across stakeholder groups is relatively even, suggesting that no specific meso-level finding can be made for this theme. However, it is worth noting the potential impact of this theme on other findings at the macro-level.

Within this theme, a further breakdown needs to be made as participants raise concerns about limited understanding within different stakeholder groups. The majority of concerns are expressed about the knowledge on the B2B side (mentioned by 8 out of 11 participants). For example, P2 (B2B) suggests that including SBOM in legislation could potentially help, but expresses serious doubts about whether B2B customers would know what to do with it. P15 (DEV) is more explicit, stating that if there are no adequate tools to translate the SBOM format into clear information, customers would have no use for it. People without a developer background may struggle to interpret the data presented in standardized formats.

Concerns about security expertise and knowledge of their own software are raised by a significant number of participants on the supplier side (mentioned by 6 out of 11). P3 (B2B) mentions the lack of awareness among suppliers during the Log4j incident, and how they themselves had no idea about the content and vulnerabilities in their software products. P8 (SV) echoes a similar sentiment.

Interestingly, P12 (DEV) even raises a concern about OS developers. They believe that when it becomes mandatory for OS developers, many inexperienced developers will have little to no knowledge of security practices and may not understand the expectations placed on them.

Overall, the lack of expertise or knowledge throughout the SSC is a significant concern that needs to be addressed, especially in the context of the previously identified findings. For example, it may align with the importance placed on having suitable tools. If people cannot extract information from the SBOM formats themselves, it becomes futile. Without proper understanding, the perceived benefits, such as risk assessment, may diminish. There is also a risk that SBOMs could become merely compliance tools if people are unsure how to utilize them. This has been indicated by P16 (DEV), among others, who mentioned that U.S. government agencies receive SBOMs but do not know what to do with them.

All of the above impacts (dis)incentives in a manner similar to the previously mentioned factors. For instance, the quality may suffer when there is a lack of expertise in producing SBOMs. Additionally, the benefits in terms of security and continuity are limited when B2B customers lack sufficient expertise to consume SBOMs effectively. Moreover, the effort required to implement and use SBOMs significantly increases when knowledge and expertise are lacking. These factors can all act as disincentives.

Findings: SBOM selection

The distinction between different applications or systems that may require SBOMs more than others is a relevant finding that has been frequently mentioned by the participants. This was an anticipated aspect prior to the research as well. Particularly in conjunction with financial considerations, participants, such as P5 (B2B), differentiate between the systems for which they would be willing to invest in SBOM and those for which they would not. P9 (SI) also highlights significant differences in systems that would warrant SBOMs. They mention that compromised front-end systems may not have catastrophic consequences, but for back-end systems, such as payment providers where every euro becomes 10 euros, the impact is fatal.

SBOM selection primarily impacts the financial (dis)incentives of B2B customers. The ability to potentially save financial resources by not requiring SBOMs for everything can be an incentive. However, this choice must be available to them. For instance, P6 (SV) mentions incorporating SBOMs as a standard part of their quality program. In such a case, customers will not have the option to obtain software without SBOMs and potentially pay less, addressing a question raised by P2 (B2B).

At the meso-level, it is noteworthy that all stakeholder groups have touched upon this topic except for IT-SIs. However, the researchers cannot establish any further correlations and suspect that this might have been a mere coincidence. Therefore, no specific findings are derived from this observation.

Consideration should also be given to regulatory frameworks in light of these distinctions. Currently, regulations such as NIS 2 and DORA primarily apply to entities operating in critical sectors. However, even within these organizations, there exists differentiation in the criticality of applications and systems that warrant SBOMs.

Findings: Internal use

The theme that emerged alongside the previous one, with a total of 7 counts, is "Internal use." In this case, the suppliers and developers within the SSC indicated that they primarily intended to use SBOMs internally within their organizations rather than necessarily providing them to B2B customers. This finding is considered highly interesting as it presents a significantly different use case for SBOMs than initially established in the theoretical background of this research (Chapter 2). Traditional literature on SBOMs suggests that the supplier side is responsible for generating SBOMs, while the customer side consumes them.

Given the substantial number of participants who raised this use case, it should be taken seriously. P16 (DEV) even states that "*if you have to say where's the most value for SBOMs, I would actually say for internal use*." This also relates back to the high ranking of quality among the most impactful incentives. P4 (SV) and P7 (SI) emphasize this when they express their intention to use SBOMs internally. P6 (SV) provides an example to support why they believe this use case for SBOMs is most suitable for them, comparing it to purchasing a car. They state, "*If a defective part is discovered three months later, I, as a consumer, won't keep track of that. I'll simply receive a letter from my garage stating that there's something wrong with the engine and that I need to come in. It's the same for our software products*."

At the meso-level, it is noteworthy that none of the B2B customers mentioned considering this use case. On one hand, this is understandable as they do not need to deliver a product for which they need to ensure quality. However, on the other hand, it could still be a useful use case for them. It would alleviate many concerns related to knowledge and expertise. Overall, it would still lead to transparency, provided that suppliers are open when customers would inquire. Furthermore, regarding regulations, simply verifying if suppliers maintain good SBOMs could help manage third-party supply chain risks.

Findings: Unattainable perfection

Sometimes, when you focus too much on specific challenges, the nuances can get overlooked. While there will always be challenges and problems that need to be addressed, it doesn't mean that a concept like SBOM becomes useless just because there are a few caveats. This is something that many participants have mentioned during the interviews. Striving for 100% security is a noble goal, but it's not always realistic. P14 (SV), for example, talks about the CRA regulation, which had a stringent security requirement regarding the avoidance of all vulnerabilities. Preventing everything simply isn't possible. It also aligns with the fact that during the literature review conducted prior to the interviews, it was acknowledged that even an imperfect SBOM still contributes to transparency. P11 (B2B) mentions that focusing too much on technical concerns, which may overlook a few vulnerabilities, can distract from the broader goal for which concepts like SBOM were originally designed. People shouldn't be discouraged from adopting SBOM because they think it doesn't add value.

At the meso-level, it is only noticeable that there were no OS developers who mentioned this. It could be inherent to the nature of technical developers to strive for complete precision and leave little room for error. This may explain why they wouldn't accept SBOMs that are not of the highest quality. However, this is an assumption, so it won't be further explored.

Findings: Evolving SBOM

As mentioned multiple times in the previous chapters, SBOM has been around for a few years, but adoption remains relatively low. However, different participants point out that SBOM is still very young. It is not yet universally clear what it is, what should be included, and who should be involved. We are still in the process of determining what to do. For example, P10 (DEV) highlights this situation in the United States. SBOMs are being provided to government agencies, but they are still unsure about how to utilize them. "*That is what the industry is trying to figure out*," as P10 (DEV) puts it. P14 (SV) expresses a similar sentiment in slightly different words. P16 (DEV) emphasizes that it is not a bad thing that this is the current state. Initially, SBOM may have only been seen as a compliance or checklist element, but over time, it can increasingly generate value. This theme also ties into the previous one. The fact that SBOM is still in its early stages means that there may be issues and challenges. However, this doesn't diminish its potential trajectory. As for the meso-level, there are no notable remarks to make.

Findings: Ongoing analysis challenges

These ongoing challenges are related to vulnerability analysis, as mentioned by the participants. The essence of their statements is that these problems are not specific to SBOM and would not suddenly arise upon adopting the concept. P3 (B2B) is the first to mention that regular network scans already yield a high false positive rate. P10 (DEV) also observes that "*folks are already dealing with that a lot*." P12 (DEV) shares their own experience with this issue. When it comes to their own OS projects, the number of vulnerabilities found is still manageable. However, when conducting analyses for their

employer's clients, they sometimes encounter hundreds of vulnerabilities, which presents a real challenge. Determining whether a vulnerability is exploitable varies from organization to organization, so "*you still have to interpret how much impact or risk it actually poses to your business. That assessment simply requires too much work.*" P14 (SV) also mentions that customers might be discouraged if they have never thoroughly scanned their software and then, for the first time, perform a vulnerability analysis on an SBOM, resulting in 300 vulnerabilities. They would have no idea how to proceed.

At the meso-level, it is evident that almost only OS developers raise these challenges. However, P12 (DEV) partly addresses them from their role within an organization rather than solely as an OS developer. Additionally, with a count of only 4, it becomes difficult to identify solid patterns that represent significant differences.

Findings: Copy-Paste unrelated

The copy-pasting problem identified in Chapter 2 is still recognized as an issue by the participants. However, the finding lies in the fact that they do not categorize it as an SBOM problem. P14 (SV) states that it is truly a "*problem in itself.*" For example, P9 (SI) strongly supports this view and describes a scenario to illustrate that the consequences may not even be significant. They mention that in the case of Log4j, if you wanted to determine if your organization was vulnerable, you could consult an SBOM to see if that particular library was present in your stack. To address the issue of unidentified libraries due to copy-pasting, you can run the vulnerable lines of code through a code checker or code scanner. This way, you should still be able to identify the problem.

At the meso-level, it is observed that only participants from the development and supply side of the SSC address this issue. This is logical since these individuals have a developer background and are more familiar with programming in general.

Findings: Asset management

Having proper asset management is considered the first step by the participants who mentioned it, in order to know what is in your software and on which third-party components it relies. If you don't even know what software you have running, you can't effectively utilize SBOM. P3 (B2B), for instance, raises concerns about shadow IT, highlighting the risk of unauthorized software installations by employees. In this regard, maintaining visibility and control over the software landscape is crucial. Furthermore, P16 (DEV) argues that asset management should be integrated as a core component of SBOM. Recognizing the significance of managing and documenting software assets enhances the effectiveness of SBOM implementation.

Findings: SBOM certification

Certifying suppliers on their SBOMs can provide several benefits to the overall supply chain ecosystem. It ensures that suppliers adhere to certain standards and practices, thereby promoting trust and confidence in the software components they provide. By verifying and certifying their SBOMs, suppliers can demonstrate their commitment to security and quality assurance. P3 (B2B) indicates that they are more interested in the fact that suppliers use good SBOMs than in what is actually included in the SBOM. Moreover, certification can serve as a valuable marketing tool. P7 (SI) mentions the use of certifications during sales pitches. Customers may be more inclined to choose suppliers with certified SBOMs, as it provides them with an added layer of assurance regarding the reliability and security of the software components they are acquiring. Additionally, certification can streamline the evaluation process for customers. Instead of scrutinizing every detail of an SBOM, they can rely on the certification as an indicator of a supplier's compliance with industry standards and best practices. This saves time and effort in assessing suppliers and allows customers to focus on other critical aspects of their procurement decisions.

Findings: Dynamic SBOM

This is the final finding among the other identified themes from the interview transcripts. Both P14 (SV) and P16 (DEV) highlight that SBOMs can be seen as dynamic processes rather than static entities. In today's fast-paced software landscape, where dependencies and vulnerabilities constantly change, SBOMs play a vital role in capturing the dynamic nature of the SSCs. They should provide real-time visibility into software components, their versions, vulnerabilities, and associated risks. By continuously monitoring and updating the SBOM, organizations could be able to proactively manage risks and respond swiftly to security and compliance issues.

6.1.5. Participant-specific Results: Micro-level

Analyzing the data at a micro-level and exploring potential relationships between specific participants' perspectives and opinions would indeed provide valuable insights beyond the thematic analysis and frequency analysis. By examining the responses of individual participants in relation to specific beliefs or viewpoints, it becomes possible to identify interesting connections. For example, if participants 1, 2, and 3 share the same opinion on belief X and belief Y, there might be a meaningful correlation worth identifying. Additionally, incorporating the demographic characteristics (segment 0) established at the beginning of each interview will further enrich the analysis. This subsection will focus solely on relevant relationships discovered in the research and will be organized into sub-subsections accordingly.

Finding: 'Experience with SBOM' & 'SBOM sentiment'
Based on the observations, it becomes evident that individuals who express skepticism towards SBOM have not had direct exposure to its implementation. On the contrary, those who have had hands-on experience with SBOM (such as P9 (SI), P10 (DEV), P13 (DEV), P14 (SV), P16 (DEV)) exhibit optimism or a strongly positive stance. It can be inferred that the level of positivity towards SBOM increases with greater familiarity and practical engagement with the concept. However, it is worth noting that P16 (DEV) remains neutral, suggesting that there may be a need to reevaluate our focus and address the right challenges associated with SBOM. "*Focus more on what the actual problem is than on SBOM as the technical solution.*"

Finding: 'SBOM demand' & 'SBOM sentiment'
The findings align closely with the previous discussion. Expert-level participants (P9 (SI), P10 (DEV), P13 (DEV), P14 (SV), P16 (DEV)) who have prior experience with SBOM also acknowledge an increased demand for it. Their exposure to the concept has provided them with valuable insights, a deeper understanding, and a sense of confidence of its potential benefits, leading to a more positive sentiment overall. As mentioned earlier, the significance of expectations is evident when considering the most impactful (dis)incentives for SBOM adoption. Consequently, it can be deduced that the level of demand plays a crucial role in shaping the perception and acceptance of SBOM.

Finding: 'Internal use' & 'SBOM sentiment'
It is noteworthy that there appears to be an interesting relationship between a participant's recognition of the use case of SBOM for internal purposes and their sentiment towards the concept itself. Participants who identify the internal use case include P1 (SI), P4 (SV), P6 (SV), P7 (SI), P9 (SI), P14 (SV), and P16 (DEV). All of them express optimism or a highly positive attitude towards SBOM, with only P7 (SI) and P16 (DEV) maintaining a neutral stance. Notably, P1 (SI) and P6 (SV) exhibit particularly strong optimism and positivity specifically regarding the internal use case, while expressing skepticism towards widespread adoption throughout the SSC. From these observations, we can deduce that participants who recognize the value of SBOM for internal use within their organization tend to have a more positive perception of the concept as a whole. Their optimism stems from experiencing the benefits of SBOM in enhancing transparency and quality control internally. This also confirms what has been discussed earlier in terms of the major benefits and most impactful (dis)incentives in this chapter.

Finding: 'Familiar with relevant regulations' & 'SBOM sentiment'
Another interesting finding relates to the relationship between participants' familiarity with supply chain management regulations (NIS 2, DORA, CRA, EO14028) and their sentiments towards the concept. It appears that participants who were aware of these regulations tended to have a more positive view of the SBOM concept. P2 (B2B), 3, 10, 11, and 14 all mentioned being well-informed about the relevant regulations. However, among this group, only P2 (B2B) expressed a neutral or less positive sentiment. Interestingly, P2 (B2B) was the only participant who was familiar with the upcoming regulations but did not have an optimistic or highly positive stance.

On the other hand, the remaining participants who held a less positive view were not familiar with these regulations and did not perceive their significance. P5 (B2B), despite being subject to the DORA regulation themselves, mentioned that they would wait for their legal team's thorough assessment before fully engaging with SBOM. Considering that SBOM is frequently mentioned online as a potential tool for compliance with these regulations, it is noteworthy that the participants who were familiar with both themes generally shared this perception.

Finding: 'Familiar with relevant regulations' & 'Critical for adoption'
It was also notable that every participant (all 5), regardless of their stakeholder group, who mentioned being well-informed about the relevant regulations (forthcoming ones), also emphasized the critical role of legislation and regulations in the adoption of SBOM. This observation is intriguing as it indirectly suggests that the respective laws are conducive to achieving widespread SBOM adoption. This finding underscores the notion that participants' attitudes towards SBOM adoption are positively influenced by their knowledge and awareness of the regulatory landscape. It further signifies that participants acknowledge the significance of adhering to legal requirements and regulations as catalysts for driving the adoption of SBOM practices.

Finding: 'Familiar with relevant regulations' & 'Responsibility more to supplier'
Another interesting theme emerged among participants who indicated their familiarity with supply chain management regulations. This time, it revealed a negative relationship with participants who expressed an increasing belief that the responsibility for security lies with the software vendor. Among the subgroup that addressed the latter theme (P2 (B2B), P6 (SV), P8 (SV), P9 (SI)), 75% were not familiar with the regulations. The trend of shifting responsibility onto vendors contradicts the ideas behind the new regulations, which aim to hold software consumers more accountable for ensuring their supply chain management.

Therefore, a tentative conclusion can be drawn that participants who are unaware of the regulations may be more inclined to place the burden of security on software vendors, potentially overlooking their own responsibilities in ensuring supply chain management compliance.

Finding: 'Limited understanding' & 'Only compliance'
There seems to be a clear relationship between the lack of knowledge, the most identified additional generally interesting finding, and the fear that if SBOM were to be mandated, it would be perceived solely as a compliance or check-list item. All participants who address the latter theme (P2 (B2B), 3, 7, 8, 10, 16) are also represented within the theme of 'Limited understanding'. This correlation can be explained as it intertwines. The concern stems from the belief that if people do not know what to do with SBOM, it will not provide added value and will become a mere checkbox exercise. The fear of SBOM being reduced to a superficial compliance requirement highlights the importance of knowledge and comprehension regarding its purpose and potential.

Finding: 'Unattainable perfection' & 'SBOM sentiment'
There appears to be a relationship between the sentiment regarding SBOM and another theme. Participants who express the nuance during the interview that achieving 100% security is not realistic (P3 (B2B), 4, 6, 9, 11, 14) are found to be optimistic and positive about SBOM. All of their sentiment scores are optimistic and higher. This could mean that these participants recognize the value of SBOM as an important tool within a broader security and risk management strategy. By embracing a realistic view that absolute security is unattainable, they understand that SBOM is a useful instrument to improve transparency and traceability of software components, rather than striving for absolute perfection. This perception of SBOM as a valuable addition to existing security measures and accepting a certain level of inevitable risks can contribute to their optimistic outlook on SBOM.

Finding: 'Job function' & 'Governance'
The participants who highlight that SBOM is a governance challenge (P3 (B2B) and P7 (SI)), possibly more so than a technical one, are also participants occupying executive roles within their organizations. One is in the top 3 management team positions, while the other is a founder. Both are primarily engaged in strategic and policy matters. The relationship can thus be attributed to the fact that these participants have a broader perspective on the implications of SBOM beyond technical implementation. As leaders responsible for governance and decision-making, they recognize the need for aligning SBOM with organizational strategies, policies, and compliance frameworks. Their emphasis on governance highlights the importance of integrating SBOM into overall business processes and decision structures.

Finding: 'Software vendors' & 'IT-SIs'
As a final finding for this sub-section, a notable meso-level finding has emerged. During the thematic and frequency analysis, it was observed that certain responses often aligned between the software vendor stakeholder group and the IT-SIs. This alignment was also evident in the demographic (segment 0) interview questions regarding their respective roles and responsibilities. Many participants from software vendor organizations also provided integration services, while IT-SIs were involved in development services. Furthermore, the analysis revealed that these stakeholder groups shared common (dis)incentives, including quality, reputation, expectations, and trust. Both groups also recognized the value of the internal use case for their own benefit. While this finding may not necessitate immediate action, it is noteworthy and worth mentioning.

The alignment of responses and shared (dis)incentives between software vendors and IT-SIs suggests a degree of convergence in their perspectives and priorities regarding SBOM. It implies that both stakeholder groups perceive similar benefits and motivations for implementing SBOM, reinforcing the notion that SBOM has relevance and value across different segments of the software industry. Understanding these similarities and common (dis)incentives can inform future collaboration and cooperation between software vendors and IT-SIs in adopting and leveraging SBOM effectively.

6.2. Ordinal Preference Ranking: Results

With the main analyses from the previous section, the key findings have now become apparent. The ordinal preference ranking method was added at the end of the interviews to capture quantitative data in a straightforward manner. The statements were linked to the (dis)incentives identified as relevant in Section 5.1. The thematic analysis revealed a significant overlap between the (dis)incentives identified by the researchers and those mentioned by the participants. The next step is to examine whether the results from the statements can confirm any of the findings from the analyses, thus contributing to the validation of those findings. It is also possible that certain results from this method may contradict earlier findings. However, it should be noted that the findings from this analysis will carry less weight than those from the previous section, given the disparity in empirical data available. Firstly, let's present the results obtained by averaging the scores for all statements across all participants. The statements corresponding to the Statement No. can be found in Table 5.5. The raw data obtained from this method is available in Appendix B.1. Lastly, it is important to reiterate that the statements used in the ordinal preference ranking method were hypothetical statements. They were designed solely to help determine (dis)incentives more effectively. Participants were asked to rank their preferences based on these hypothetical scenarios, providing insights into their perceptions and priorities.

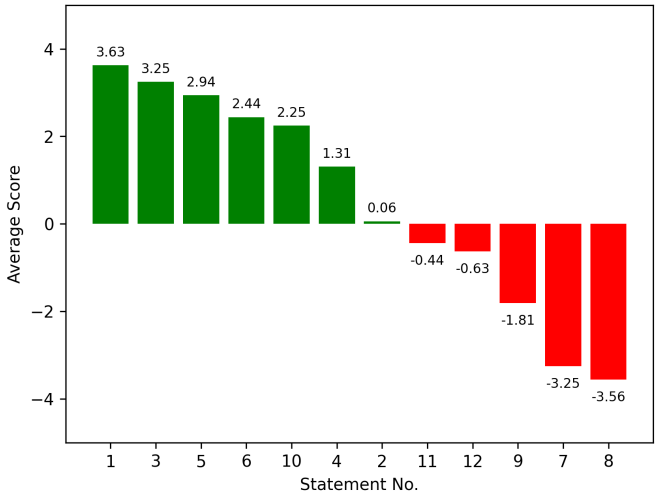


Figure 6.14: Average Ranking Scores of the OPR Statements

We will first discuss the two most significant outliers. S1 relates to a financial incentive, specifically the ability to reduce financial damages that may occur after, for example, SSC attacks. This financial incentive received the highest absolute score among participants. While economic factors were already mentioned as important, they did not rank as the highest among the most impactful (dis)incentives. This finding highlights the significance of considerations such as overhead for SMEs, ROI, and choices regarding which applications organizations are willing to pay more for. These are all economic aspects that gain greater importance in light of this result.

On the other end of the spectrum, S8 (SBOM could pose a threat to IP) scored the lowest and, hypothetically, would hinder the adoption of SBOM according to the participants. Fortunately, IP was only mentioned once in the segment on the most impactful (dis)incentives regarding SBOM in response to the main three questions. However, when specifically asked about it, seven participants indicated that it could potentially expose IP. This is something to consider further.

Next, the second most positive and the second most negative (S3 and S7) are addressed. S3 falls under the "time" category and examines how stakeholders perceive the value of SBOM if it could save half of the time required to detect vulnerabilities. The significance of time was already evident in the impactful (dis)incentives, as six participants also mentioned it. It was also mentioned as an important factor in vulnerability identification, CVE assessment, and so on. Therefore, the results of this statement confirm the findings from previous analyses. S7 pertains to the "demand" category and hypothesizes that there is no customer demand for SBOMs. The fact that this statement is identified as such a negative driver validates the findings regarding expectations and the perceived importance of industry standards, which were also highly regarded by the participants. This aspect proves to be crucial for SBOM adoption.

S4 and S5 are interesting to examine together as they both fall under the category of law and regulations. However, S5

also includes an economic factor. S4 hypothesizes that SBOM is an effective way to comply with laws and regulations related to managing supply chain risks. On its own, this factor is not considered highly influential for adoption. However, when a financial disincentive is added, as in S5 (financial penalty of 1% of annual sales is imposed if non-compliance occurs), its impact more than doubles. This intriguing finding highlights the significance of economic aspects in influencing adoption decisions.

The last two boosting statements are S6 and S10, which both scored relatively high. S6 addresses participants' perception of trust by examining the perceived value of increased trust through SBOMs. S10 focuses on perceived value of user-friendliness. Both are perceived as reasonably significant for the adoption of SBOM. This validates the findings regarding trust from the thematic and frequency analyses. User-friendliness, on the other hand, speaks to the quality of the required tools and automation associated with SBOMs.

S9 (on the lack of sufficient consumption tooling) also confirms the importance of tooling. The fact that there may be inadequate tooling for consuming SBOMs does not score as highly hindering. It does not necessarily refute the earlier findings regarding tooling, but it diminishes the significance to some extent.

Now, regarding the neutral scores, S2 (on SBOMs tooling adding costs, but being effective) suggests that good tooling and financial disincentives should be able to balance each other out. As long as the tooling works well, participants indicate their willingness to pay extra. This aligns with the willingness to pay identified in the thematic and frequency analyses.

Lastly, there are two technical concerns, formulated as statements, regarding CVE vulnerability analysis (S12) and its false positives, as well as the copying of code rules that may lead to certain dependencies not being detected by SBOM (S11). Both hypotheses are perceived as relatively neutral in terms of adoption. Participants do not believe they would have a significant impact. This confirms the previously identified generally interesting finding that vulnerabilities and copy-pasting are not specific issues related to SBOM.

Overall, this ordinal preference ranking method has been able to confirm and validate more of the previously identified findings than refute them. This is positive news and allows for stronger conclusions to be drawn. However, as mentioned in the introduction to this section, the amount of data gathered through this method is substantially lower than that from the interviews themselves. Therefore, these results should not be overemphasized. Nevertheless, since most of the results align with the existing findings, it can be seen as an additional confirmation.

6.3. Data Validation with Expert

To further validate the findings from the previous sections, the researchers had intended to schedule sessions with field experts in SBOM, who were not directly operative within the SSC, towards the end of the study. The initial approach was to conduct sessions with three different experts. At a certain point it had been lined out. However, due to unforeseen circumstances, this plan could not be executed as intended. Eventually, a session was scheduled with one field expert. However, due to their experience with SBOM, it is still relevant to include. The expert holds a position where they engage with people worldwide on the topic of SBOM and its societal implications. Since 2019, the expert has been conducting research on SBOM and working collaboratively with companies to explore its contributions and significance. SBOM is an integral part of their daily work, and they possess a comprehensive understanding of various aspects related to SBOM.

The validation process was approached in a structured manner, different to the interview sessions, to extract maximum value from the session. The conversation began intentionally with the main three questions, without presenting the findings of this research to the expert. This approach aimed to bypass any potential researcher bias, similar to the approach adopted during the participant interviews. The expert's answers, generated independently, were interpreted as carrying the most significance. The outcomes of the initial three questions were extensively discussed, and they were supplemented with some of this research' findings so far, aligning them with the expert's insights. This approach fostered a knowledge-sharing dynamic, enhancing the depth of the conversation. Furthermore, the expert was presented with the findings from this chapter that had not yet been discussed, allowing for additional validation. Although the validation emerging from this discussion may be considered slightly less significant, it is important to note that the expert's extensive knowledge on the subject matter led to valuable insights that should be taken seriously for the remainder of this research.

In the following sections, the validated findings and insights from this session will be presented and discussed, reinforcing the significance and relevance of the research outcomes. The full summary of the session is presented in Appendix D.

6.3.1. Validation of Findings from Main Three Questions

The answers to the following main 3 questions are solely those that the expert generated themselves, without prior discussion of the research' findings.

The biggest benefits of SBOM
Regarding the benefits, the expert indicates that they see the same advantages as those mentioned by the majority. Through improved transparency, vulnerability management, and consequently risk management, should be significantly enhanced. Additionally, they believe that it is indeed necessary at this point, given the current state of software in general.

The most impactful incentives regarding SBOM
According to the expert, there are several significant interests that they identify as being involved in the adoption of SBOM. For the most part, these align with the (dis)incentives identified through thematic analysis. One major interest they mention for organizations is compliance management (or the theme of 'Regulatory compliance' in this research). "*We need to do this, so let's just do it.*" Another important (dis)incentive within the supply chain is that the receiving parties need to demonstrate it to their suppliers (theme: 'Demand'). "*Make sure you challenge your suppliers to have SBOMs.*" The expert also notes that after the Log4j debacle, there was a significant push surrounding the SBOM hype. This same example was frequently mentioned by the participants when discussing vulnerability discovery and its combination with SBOM.

'Tooling & automation' are also deemed crucial elements by the expert. This is closely linked to the 'Time & effort' individuals need to invest, all of which are vital for adoption. It becomes a trade-off between "*Security, or simply good asset management, and maintaining quality versus costs versus time and resources.*"

Lastly, the expert also believes that software vendors being compliant and capable of producing SBOMs at a high quality level could instill a sense of trust in their customers. It would be a kind of "*stamp of maturity*" indicating that vendors can generate SBOMs effectively. This aligns somewhat with the notion of certification mentioned earlier during the findings.

The biggest concerns for SBOM
The very first issue raised by the expert during the session is: "*How far should you go? How deep should an SBOM go, how many dependencies should it encompass? That is still unclear.*" This strongly confirms the participants' major concern regarding the theme of 'Detailing & layers'. Additionally, it becomes even more challenging when trying to retroactively produce SBOMs for older systems after the build process. Obtaining accurate SBOMs for such systems remains a significant problem. For more modern applications, such as virtualization with Docker, extracting SBOMs should be relatively feasible. However, firmware poses greater difficulty, and generating SBOMs for binaries is also quite complex. "*So the principle is very simple, just a list of ingredients. But actually assembling that list is still quite complex.*"

One factor inhibiting adoption is the initial assumption that certain aspects would be straightforward, which turned out to be grossly underestimated. Creating the SBOM itself is difficult, and manual consumption is impractical. Tooling is essential for the process. In an experiment, they printed out the SBOMs and ended up with 30 pages of A4 paper for a relatively simple piece of software. In terms of 'time & effort', it simply becomes unmanageable. This results in people simply not being willing to engage with it. It's a lot of work, and organizations have to pay for the tooling. From their perspective, the expert considers that a valid point. "It would require a significant amount of additional work. I spoke with an organization, and they said they have about 60 people working on this. Not full-time, but it affects around 10 departments. That's how significant it becomes for your organization." It is all important, but companies are already struggling with their regular asset management. So, it is a problem.

Another major issue is the lack of standardization in the SBOM landscape, which aligns with the theme of 'Evolving SBOM'. The expert identifies two main sub-themes within this context. Firstly, there is a theme related to what two participants with 'expert-level' indicated regarding the existence of multiple SBOM formats. The need to choose among them and ensure interoperability hinders adoption. The second sub-theme confirms a problem that arose frequently in the results concerning vulnerability analysis and assessing the discovered vulnerabilities. For instance, the expert provides an example regarding CPE numbers: "*If you searched for a specific CPE number combination with open SSL, you would get a long list of vulnerabilities. And if you searched for a slightly different CPE number with the same open SSL library, perhaps one version earlier, you would get zero or two vulnerabilities.*" This leads to an abundance of false information. These issues with linking SBOM data (after analysis) to vulnerability databases confirm a finding that has been repeatedly observed. Assessing those vulnerabilities is also a problem, particularly in terms of being time-intensive. According to the expert, VEX is considered a valuable addition, but as observed, it still involves a significant amount of manual work and, therefore, consumes a lot of time.

6.3.2. Validation of the remaining findings

The results of the validation session follow, where certain relevant findings from the thematic and frequency analysis were presented. In a significant number of cases, the expert agreed with the findings, although there were a few instances where they were less aligned.

The two use cases

The various use cases identified during the research needed to be addressed. The expert confirmed the internal use case for software suppliers based on the Log4j scenario they simulated retrospectively. When they assumed the role of a software vendor, they quickly agreed that SBOMs are useful for identifying any Log4j-like vulnerabilities in their own products. This information can then be shared with customers. From the customer's perspective, it was slightly more challenging. There was a lot of debate about whether they wanted to have the SBOM themselves or just hear from the vendor about the potential vulnerabilities in the software. This use case seemed less uniformly clear than internal use. "*Some people said, well, I really want to have the SBOM myself because I want to be able to do the whole trust but verify thing. I want to check whether the vendor has actually looked into it. And there were others, and I was more on that side, who said, I don't want to know at all. The SBOM doesn't interest me. I have no desire to check all those dependencies myself. I just want a clear explanation from my vendor about the vulnerability in my system, and I want them to fix it. So whether they use an SBOM or not, it's fine. I just want an answer as quickly as possible.*" Therefore, according to the expert, this is the ongoing discussion within many organizations.

Law and regulations

Both of these use cases are also interesting in the context of upcoming legislation and regulations. For example, the CRA explicitly states that producers of information systems must create SBOMs. It also seems that they need to identify the vulnerabilities within them. This can be done in various ways, but using SBOMs through internal use is one option.

It is indeed important to closely examine the specifics of the legislation. Currently, there are minimum requirements in the U.S., but they are relatively minimal and don't go much further. The expert wonders if legislation should address and provide useful guidance on tooling as well. "*I would always lean towards ensuring that the SBOM requirements use state-of-the-art wording. It seems that tooling is evolving rapidly right now, with numerous small companies working to improve SBOMs as much as possible. I would say let that innovation continue for a while and keep the requirements broad, focusing on the need for an SBOM. This way, you won't get stuck in the changes that are currently happening. If you try to overly specify it, you might not reach a practical solution.*"

SBOM governance

The expert considers this to be something significant to take into account. Initially, they also thought it wouldn't require much effort. However, they now realize how much work it entails in terms of governance structure: processing the SBOMs, acquiring them, distributing them, and also engaging with legal and various stakeholders to properly manage it within the organization. It would require a full-time project team dedicated to this task. They believe it will indeed be quite challenging to implement this in an organization. It will consume a significant amount of time, even the process of requesting the SBOMs can become complicated. Therefore, both software suppliers and consumers may face challenges in this regard.

Overhead SMEs

The expert agrees with the issue regarding the potential overhead for SMEs when it is presented to them. They even state, they "*do not see any SMEs being able to handle this effectively in the coming year.*" Supplier management is very challenging because it requires a significant amount of time. They believe it is not a high priority for them and is complex to execute properly, considering the lack of adequate tooling and knowledge. From the perspective of software suppliers, it should be manageable. They think those parties should be able to handle it, including the developers. However, they do not see organizations on the consumer side being able to process it effectively themselves. Instead, they believe organizations should make good agreements with their suppliers, stating that they want SBOMs for the products they procure and timely and accurate information if any vulnerabilities are discovered. They can manage that aspect well. But processing the SBOMs themselves and conducting thorough checks is not feasible. They should be aware of SBOMs and acquire knowledge about them to engage in discussions with their suppliers. They believe that can be expected of them. However, handling the processing of SBOMs in bulk themselves is not realistic.

License management

License management is definitely a use case of SBOM that they have come across frequently, and there is certainly merit to it. However, they have decided to primarily focus on compliance and vulnerability management for now and set aside license management.

Intellectual property

Regarding the relationship between IP and SBOM, the expert does not see a significant problem. They can understand that companies might initially react to potential IP threats, but they believe that it will ultimately not be a major issue. They share the view that there is more IP involved in how software components are interwoven than in the individual components themselves. They also mention that in other sectors, it is common practice to disclose the components used during production. Additionally, they state that if one genuinely wants to know, reverse engineering should already provide significant insights.

6.4. Stakeholder-Specific (Dis)incentives Overview

The presented data thus far constitutes a substantial volume of information. While it contains intriguing findings, it is imperative to distill the most important and significant insights from the extensive array of results it currently comprises. The current state is too ambiguous to serve as a basis for concrete plans for readers or stakeholders to whom the thesis applies. Furthermore, a gap remains in linking some of the findings that lack clarity regarding how they influence stakeholder-specific (dis)incentives. Given that the thesis approaches the problem as an incentive issue among various stakeholder groups, this must be clearly comprehensible.

This section serves precisely this purpose. To enhance clarity, four additional steps are taken. Firstly, the identified themes and factors from Section 6.1 are further aggregated. Here, distinctions are made between factors falling under incentives and those generating disincentives. As the second step, it is also crucial to organize the results from the frequency analysis per theme in a coherent manner for each stakeholder group. While this information is included in Section 6.1, it is not presented cohesively, thus lacking insight into its significance. Then, in Section 6.4.2, the ultimately derived core set of incentives and disincentives is set against the ex-ante determined set from Section 5.1. Finally, in Section 6.4.3, all these elements converge within the SWOT analyses. These analyses comprehensively chart the primary incentives and disincentives for each stakeholder group, thereby providing concrete pillars for building conclusions and recommendations.

6.4.1. Aggregation and Frequency Overview

The first two steps can be presented together. The aggregated factors depicted in the tables below (Table 6.2 and Table 6.3) respectively serve as incentives (in Table 6.2) and disincentives (in Table 6.3). The description clarifies, where necessary, which themes from Section 6.1 fall under these new incentives and disincentives. However, in general, they correspond to the most significant (most frequently mentioned) identified themes. For each stakeholder group, the frequency with which they cited the incentives and disincentives is discernible. The total scores are also indicated and serve as the guiding thread for the order of the (dis)incentives.

Table 6.2: SBOM Adoption Incentives

Incentive	Description	Groups				All
		DEV	SV	SI	B2B	
Compliance	Mandatory or voluntary (but giving a competitive advantage) compliance with laws, regulations, or industry standards	0%	75%	100%	25%	44%
Enhanced Security of Consumed Software	SBOM (indirectly) contributes to higher transparency of the consumed software that can improve security measures and mitigate the risks of being affected by cyber attacks	20%	25%	33%	100%	44%
Improved Reputation or Trust	SBOM is adopted because it improves the reputation or trust of the software producers	40%	50%	100%	0%	44%
Time or Effort Savings	SBOM is adopted due to time or effort savings	0%	75%	33%	75%	44%
Improved Quality of Supplied Software	SBOM adoption may contribute to the improvement of the supplied software	0%	50%	100%	0%	31%
Ethical & Ideological	SBOM is adopted due to its alignment with ideological or ethical principles	40%	0%	0%	0%	13%

Table 6.3: SBOM Adoption Disincentives

Concern	Description	Groups				All
		DEV	SV	SI	B2B	
Lack of Knowledge or Expertise	Lack of knowledge or expertise may thwart successful SBOM implementation	100%	50%	67%	50%	69%
SBOM Usefulness	SBOMs could be generated for a) various software; b) on multiple levels; c) by different vendors. The usefulness of SBOM depends on the quality of all individual parts, that makes concerns for its adoption. This encompasses 'detailing & layers', 'SBOM selection' and 'only compliance'.	80%	25%	67%	100%	69%
Time or Effort Overheads	SBOM adoption may lead to additional time or effort overheads, e.g., due to SBOMs storage and maintenance, required proper assets management, and governance of the related processes	60%	50%	67%	25%	50%
Vulnerability Misclassification	Presence of False Positives (e.g., due to the vulnerable part of the code is not exploitable) and False Negatives (e.g., due to copy-pasting)	60%	25%	33%	25%	38%
Financial Losses	SBOM adoption may not cover all the incurred investments and operational costs. This also encompasses the overhead for SMEs	0%	0%	67%	25%	19%
Imperfect Tooling, Formats or Vulnerability DBs	Lack of or imperfect tools, incompatible SBOM formats and multiple vulnerability databases hinder SBOM adoption	40%	0%	33%	0%	19%
Threat to IP	Intellectual Property can be revealed to competitors/third parties through SBOM	0%	25%	0%	0%	6%

6.4.2. Matchup Against Ex-ante Identifiified (Dis)incentives

To introduce additional structure and coherence to the thesis, it is pertinent to match up the acquired incentives and disincentives with the ex-ante identified set in Section 5.1. This examination aims to ascertain which factors align with each other and whether such alignment pertains to incentives, disincentives, or both. An overview of this comparison is visually represented in Figure 6.15. In this illustration, the incentives (green) and disincentives (red) are depicted as arrows, corresponding to their arrangement in Section 5.1, with corresponding section numbers. These arrows point to the (dis)incentives as presented in Section 6.4.1. The explanations for these (dis)incentives are available in the tables within the latter section and are not expounded upon here. The accompanying percentages pertain to the overall scores (macro-level), which have been utilized to rank the (dis)incentives.

It emerges that nearly all (dis)incentives identified from the interviews align with and are encompassed by the pre-established set of (dis)incentives. This convergence underscores the validity of the set, demonstrating its ability to effectively encompass real-world sentiments and provide a comprehensive understanding of the (dis)incentive landscape. Moreover, it appears that the notion of the incentive issue for SBOM technology among involved stakeholders aligns with similar issues encountered in other security technologies, such as MFA (see Chapter 5). However, despite this relatively high convergence, not all incentives derived from the empirical segment of this research were initially represented in the ex-ante literature review. Enhanced security of the software consumed by B2B customers is an incentive that was not explicitly articulated initially. The same holds for the improved quality of supplied software for SVs and SIs. Lastly, the ethical and ideological incentives for DEVs were not distinctly evident in the literature review. Hence, these three incentives are absent from Figure X, yet they will be included in Section 6.4.3 due to their significance as indicated by the results in Section 6.4.1.

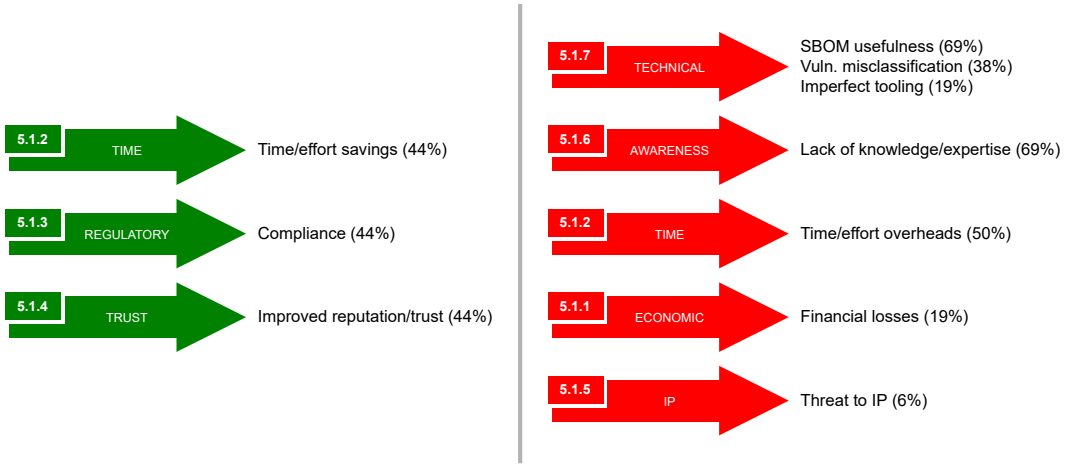
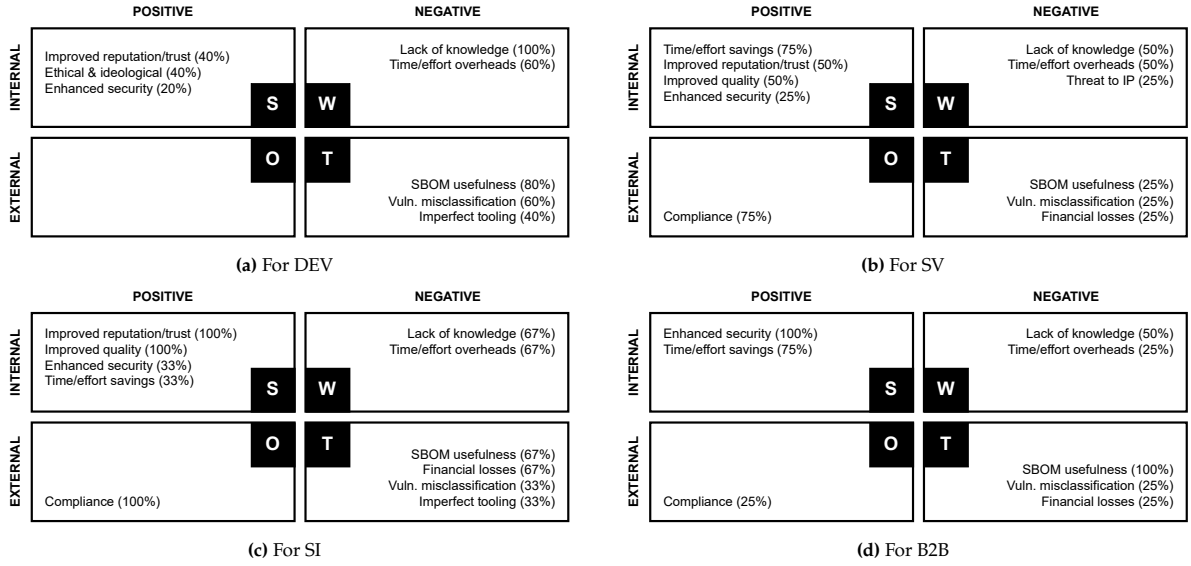


Figure 6.15: Matching up with Section 5.1

6.4.3. SWOT Analysis

In this section, a SWOT analysis (see Figure 6.16) is applied to each stakeholder group within the scope of the research, incorporating all accumulated results and findings. The SWOT analysis serves to illustrate the equilibrium between positive and negative factors concerning the (dis)incentive issue concerning SBOM. The findings have been organized based on their significance, as determined by their frequency within each stakeholder group. Notably, the incentives are allocated to the categories of strengths (S) and opportunities (O) within the figures, while the disincentives are distributed between weaknesses (W) and threats (T). The differentiation is predicated on whether the (dis)incentive functions as an internal or external factor within each stakeholder group.

By employing this SWOT analysis for each group, it facilitates the proposal of strategies on how to promote the spread of SBOM within each group. The strengths and opportunities reveal the areas where stakeholders are more inclined to be supportive or proactive in the adoption of SBOM. These aspects denote the factors that can be leveraged to encourage the uptake of SBOM, such as aligning with regulatory compliance or enhancing software quality. On the other hand, weaknesses and threats point to challenges and concerns that may hinder or impede the adoption of SBOM. These factors provide a comprehensive view of the potential obstacles and risks faced by each stakeholder group.



(a) For DEV

(b) For SV

(c) For SI

(d) For B2B

Figure 6.16: SWOT Matrices

Starting with the B2B group, a pivotal strength lies in the anticipation that the incorporation of SBOMs will yield **enhanced security** and **time or effort savings**. However, the current reality suggests that integrating SBOMs is likely to result in increased time and effort expenditures, with the associated benefits remaining somewhat uncertain. Over the past few years, there have been several highly publicized cyberattacks, such as Log4Shell, as previously discussed. These incidents could have potentially caused substantial damage, beyond what was already inflicted, and SBOMs could have played a crucial role in enhancing the detection of vulnerable components and reducing response times. Fortunately, due to extensive media coverage, organizations managed to timely patch their systems. Consequently, it is not surprising that the primary threat perceived by B2B stakeholders in adopting SBOMs is their (perceived) **limited usefulness**. The fact that a significant weakness identified by this group is a **lack of knowledge** regarding SBOMs could also play a role here. The analysis indicates that B2B stakeholders harbor reservations about the relevance of SBOMs to their operations and foresee substantial cognitive demands in integrating this technology. Therefore, it can be deduced that, at the present moment, this stakeholder group possesses limited internal motivation for SBOM adoption. Undoubtedly, the introduction of external stimuli in the form of regulatory **compliance** would alter this situation. However, currently, this factor holds relatively little significance for this group, as only one participant has mentioned it.

The pursuit of SBOM adoption is considerably stronger within both the SI and the SV group. They perceive **regulatory compliance** as a strong external motivator. However, under stringent compliance regulations, SBOMs may be seen as a mere procedural requirement. To relate it back to the analogy with nutrition labels, manufacturers must provide them, but consumers rarely read them. In addition to compliance, representatives from these groups recognize the value of SBOMs in **improving their reputation and trustworthiness**, as well as improving the **quality of the supplied software**. Nonetheless, they also acknowledge that the adoption of this technology may result in potential **financial losses** and additional **time or effort overheads**. It is noteworthy that the perceived impact of these challenges is less pronounced for the SV group. Concluding, the analysis posits that these two stakeholder groups could serve as the primary catalysts for the widespread adoption of SBOM technology.

Finally, let's consider the developers, who, much like the B2B group, appear to play a restraining role in the adoption of SBOM. The adoption of this technology is primarily driven by internal motivational factors, specifically **ethical and ideological** principles, as well as the desire to **improve their reputation and trustworthiness**. While these can be potent motivators for individual developers, sustaining the same level of internal motivation over the long term can be challenging without corresponding rewards. It's worth noting that financial contributions to even widely used software projects are relatively low, as indicated by participant P10 (DEV). Individual developers within our study have not mentioned financial incentives as motivating factors. This is not surprising since features like SBOM do not directly contribute to the core functionality of the software product for which people typically donate. Additionally, since many individual developers work on these projects in their spare time as a hobby, they are not compelled to adhere to certain requirements. Furthermore, as evident from their SWOT analysis, the implementation of SBOM would necessitate additional investments due to a **lack of knowledge** and increased **time and effort overheads**. The (perceived) **limited usefulness** of SBOM for developers also remains a concern. Taking all these factors into account, it can be concluded that the developer group currently exhibits very little interest in adopting SBOM.

6.5. Conclusion of Chapter 6

This chapter has presented a wealth of findings, drawing on a combination of thematic and frequency analyses, ordinal preference ranking analysis, and a validation session with a field expert. These findings have been systematically organized, first into two distinct tables and then into a SWOT analysis for each stakeholder group. In essence, these analyses address the research question SQ3: "What factors can explain the lack of SBOM adoption?" Given that the thesis frames the issue as an incentive problem, these factors have been categorized into incentives and disincentives (as detailed in Section 6.4.3).

After analyzing the findings, it becomes evident that the primary stakeholders involved in both producing and consuming SBOMs, namely the DEV and B2B groups respectively, currently exhibit the least incentives for SBOM adoption. On the other hand, the primary business stakeholders who have the potential to drive SBOM adoption are the SI and SV groups. Consequently, one plausible strategy to expedite the widespread adoption of SBOMs is to leverage the influence of these two driving groups. For instance, they could incentivize individual developers by compensating them for providing SBOMs as an additional feature or by becoming sponsors of their projects. This approach would get individual developers interested in investing their time and efforts into SBOM adoption. To stimulate SBOM adoption among B2B stakeholders, initial efforts may focus on compliance measures. However, the main thrust should be directed towards demonstrating the practical value of SBOMs and simplifying the usage of this technology to make it more accessible.

7

Discussion

In this chapter, the discussion of the research findings will be presented, providing a comprehensive analysis and interpretation of the empirical results. This chapter serves as a crucial step in the research process, allowing for an evaluation of the obtained empirical results and the existing literature. Starting with Section 7.1, the discussion will focus on the key findings that have emerged from the analysis of the data. This section aims to highlight and prioritize the most significant results obtained, emphasizing their relevance and implications for the research objectives. The section will also delve into the comparison between the empirical results and the current literature, providing insights into how the findings align with existing knowledge. The initial literature research conducted earlier in the study will also be reviewed and assessed in this section, ensuring that the research process remains consistent and coherent. This examination will contribute to the overall understanding of the research topic and shed light on any discrepancies or consistencies between the literature and the empirical findings. In Section 7.2, the feasibility of SBOM adoption will be explored based on the research results. This section will investigate whether there are any additional findings regarding the specific components that should be included in the SBOM, as well as the delineation of responsibilities and tasks related to its implementation. Understanding the feasibility of SBOM adoption is crucial for guiding future actions and decision-making processes in relation to software development and supply chain management. Furthermore, Section 7.3 will examine the potential involvement of stakeholders initially excluded from the scope in Chapter 4 within the SBOM ecosystem and adoption. This section will explore any relevant findings or implications regarding the participation and contributions of these stakeholders, shedding light on their potential roles and impact. The chapter will also assess the extent to which the research adhered to the data requirements outlined in Chapter 3. By reflecting on the data collection, analysis, and interpretation processes, this evaluation will ensure the reliability and validity of the research outcomes. Subsequently, the chapter will address the limitations of the research plan, its execution, and the extent of the findings' generalizability (7.4). These limitations will provide a comprehensive understanding of the constraints and boundaries within which the research was conducted. Finally, the chapter will conclude with the researcher's reflection on the entire research process. This personal reflection will encompass the researcher's experiences, insights gained, challenges encountered, and lessons learned throughout the research journey.

7.1. Discussing and Comparing the Empirical Results with Existing Literature

The obtained empirical results reveal several significant findings that warrant discussion in the context of existing literature on SBOM. The initial literature research conducted at the beginning of this study will also be revisited. By discussing these empirical findings and comparing them with existing literature, a more comprehensive understanding of the challenges and considerations surrounding SBOM adoption can be gained. It highlights areas where the research aligns with prior knowledge and identifies novel insights that contribute to the evolving understanding of SBOM.

Firstly, it was observed that there is a lack of knowledge and expertise among various stakeholders involved in SSC. B2B customers commonly exhibit a low maturity level in the realm of security. This is aggravated by the growing dependence on cloud services and the evolving trend of transferring security responsibility increasingly onto suppliers. Moreover, a recurring observation pertains to the software vendors themselves, who frequently lack visibility into the composition of their own development processes and products. This limited understanding was not prominently highlighted in the literature concerning SBOM, although it acknowledged the relatively low awareness and limited adoption of SBOM. Participants suspect that this limited understanding leads to the perception that SBOM serves merely as a compliance tool rather than adding significant value. This perception was noted among U.S. participants who are already required by

government agencies to receive SBOMs. They perceive that once they have received the SBOMs, their obligation has been fulfilled, without clear guidance on how to effectively utilize them. This concern was not addressed in the literature.

The young and evolving landscape of SBOM contributes to stakeholders' lack of clarity regarding its precise nature, making immediate adoption more challenging. The industry is still in the process of understanding and defining SBOM, including its use cases. The evolving nature of SBOM was evident from the varying descriptions found in the literature. The specific components to be included and the recommended tools for generating SBOMs are not uniformly defined. Additionally, the use case of internal use was not initially identified in the literature by the researchers.

The importance of having good tooling for SBOM was emphasized, as highlighted in the literature. This finding is further reinforced by the identified impactful (dis)incentives regarding quality and time-consuming factors. However, there seem to be some shortcomings in the current tooling available. Insufficient detailing and layering of SBOMs emerged as a concern, stemming from various reasons. One of these reasons is the existence of immature tooling that generates SBOMs. Another factor is that open-source developers often develop components within ecosystems without utilizing dependency managers.

Furthermore, it is worth noting that while IP-related concerns eventually emerged as an issue for certain participants during the interviews, the majority did not initially emphasize this aspect. Therefore, it seems that IP considerations do not hold the primary responsibility for impeding the adoption of SBOM.

Another contributing factor to the challenges faced in SBOM adoption is the lack of awareness regarding pertinent regulations and the overall demand for SBOM. The literature review revealed a limited discussion on the role of SBOM in complying with relevant laws and regulations, indicating a gap in understanding. This lack of awareness among stakeholders regarding the legal landscape and the imperative need for SBOM further complicates its effective implementation.

7.2. Feasibility of SBOM: Inclusions, Responsibilities, and Use Cases

In examining the feasibility of SBOM based on the empirical findings and insights gathered throughout the research, first, the requirements for creating robust SBOMs will be explored. One major concern highlighted is the need for proper detailing and layering of the components within an SBOM. The aggregated list of elements proposed in Chapter 2, derived from the literature, seems to be reasonably accurate in retrospect. However, achieving the desired layering seems to necessitate the involvement of developers in the process. Nevertheless, concerns were raised regarding their willingness to invest time and effort in something that may not directly benefit them. This underlines the importance of effective tooling, as emphasized by various developers. Additionally, it appears that the data provided by modern package and dependency managers should be sufficient for generating comprehensive SBOMs, provided that software vendors have access to this data. Consequently, the responsibility lies with developers to ensure that their components are equipped with suitable dependency managers.

Another concern raised by experts pertains to the challenge of smoothly linking SBOM data with vulnerability databases. Issues such as mismatched identifiers, inaccurate databases, and problems related to duplicate management when consulting multiple databases were identified. Introducing a unique identifier could potentially resolve many of these challenges. However, for this unique identifier to be effective, it would need to be widely accepted and standardized across the industry.

Next, the discussion turns to the two distinct use cases that were identified. Initially, the researcher perceived SBOMs solely as a concept to be generated by vendors and integrators during the development phase and subsequently delivered to B2B customers, who would derive value from consuming the SBOMs. However, participants revealed another use case that they found highly valuable: internal use of SBOMs by software vendors themselves. This includes managing services for customers as well as ensuring the quality and security of the software they deliver. Considering the findings, this additional use case appears to be reasonable. For instance, it addresses the lack of knowledge among B2B customers, as they would not need to engage extensively with SBOMs. In terms of payment, the research findings suggest that customers are willing to pay for increased transparency, and vendors, in general, can factor in the associated costs. Furthermore, when it comes to regulatory compliance, the inclusion of SBOM usage in the considerations of B2B customers during procurement could contribute to their obligations in effectively managing third-party supply chain risks. However, it is crucial to assess the data quality of the SBOMs in question, which might pose a challenge and potentially open doors for SBOM certification initiatives.

Additionally, this use case could potentially be mandated to enhance transparency within the SSC. Based on the expectations expressed by participants, there is a hopeful outlook that if software vendors are required to maintain SBOMs for their products, developers who aspire to have their components widely adopted by the professional industry would be motivated to provide the necessary data alongside their components. After all, they are seeking recognition and exposure.

7.3. The Role of Governmental Agencies and External Security Companies

After scoping in Chapter 4 resulting in solely focussing on the direct stakeholders involved in SBOM, there may still be certain considerations for stakeholders outside the immediate scope of the research. In this section, the potential role of governmental agencies and external security companies will be explored concerning the successful adoption of SBOM. This section aims to examine the possible contributions and value-additions these stakeholders could bring to the SBOM ecosystem.

Governmental agencies

The role of regulatory bodies in SBOM adoption can encompass various aspects, with a focus on establishing clear guidelines and promoting transparency and awareness within the SSC. It is not solely about imposing obligations but also about facilitating collaboration, awareness, and the development of effective frameworks that contribute to a resilient and reliable SBOM ecosystem. Some possible considerations are:

- Establishing Clear Guidelines: Instead of mandating SBOM for all organizations and all software, regulatory bodies can play a crucial role in defining clear frameworks. This involves determining specific requirements and standards related to risk management in the SSC. By clarifying how software consumers should comply with these frameworks, including the necessary data and measures, a more targeted and effective adoption of SBOM can take place.
- Increasing Awareness: Governmental agencies can concentrate on raising awareness and understanding among all stakeholders within the SSC. They can develop campaigns and educational initiatives to make organizations, software vendors, and consumers aware of the benefits and significance of SBOM. By providing guidelines, information, and resources, regulatory bodies can contribute to a broader understanding of SBOM and foster a culture of transparency and security.
- Requiring Transparency: Regulatory bodies can impose obligations on software vendors to be more transparent about the software components they provide. This may include providing detailed information about the utilized components, their dependencies, and any known vulnerabilities. By promoting transparency, regulatory bodies can enhance insights into the risks involved and enable software consumers to make informed decisions based on the available information.
- Collaboration and Certification: Governmental agencies can also facilitate collaboration among stakeholders and the development of certification programs. They can establish platforms where different parties collaborate to establish best practices and standards for SBOM. Furthermore, they can develop certification mechanisms to ensure the reliability and quality of SBOMs. This can help build trust and encourage widespread acceptance of SBOM within the SSC.

External security companies

These third-party companies can play a vital role in facilitating the adoption of SBOM by addressing various factors where organizations may lack knowledge or expertise. Some of the potential areas where these companies can contribute are as follows:

- Assisting Organizations in Developing SBOM Implementation Plans: External security companies can help businesses devise robust strategies and plans for the implementation of SBOM processes. They can leverage their expertise and experience to guide organizations through the complexities of adopting SBOM and ensure a smooth transition.
- Assessing SBOM Quality: With their expertise in security and vulnerability management, external security companies can assess the quality and completeness of SBOMs. They can conduct thorough evaluations to identify any potential gaps or vulnerabilities within the SBOM (of suppliers).
- Assisting Customers in Consuming SBOMs: External security companies can support customers in effectively consuming SBOMs. This includes educating customers about the importance of SBOMs, providing guidance on interpreting and leveraging the information contained in it, and assisting them in making informed decisions based on the SBOM data.
- Managing SBOMs and Security Operations Centers (SOC): External security companies can offer specialized services in managing SBOMs and establishing dedicated SOCs for organizations. They can assist in the continuous monitoring, analysis, and response to security incidents and vulnerabilities identified within the SBOM.

7.4. Limitations of the Research

Every research endeavor, including the present study, inevitably encounters limitations. Despite employing a mixed methods approach, there are several aspects that could have been improved. Time, financial resources, and specific constraints influenced the choices made throughout the research process, which might have been different if unlimited resources were available. Therefore, this section delves into a comprehensive examination of the potential limitations that

affect the entire study, including the research methodology, dataset, data processing, and other relevant factors. The aim is to adopt a critical perspective, cautiously considering the significance of the findings and exploring their applicability. By scrutinizing the limitations, it becomes possible to gain a clearer understanding of the research outcomes and identify areas that require further investigation. The following section examines these limitations in detail, providing valuable insights into the constraints faced and their potential impact on the study's conclusions.

Participant set

There are several limitations regarding the participant set from which empirical data was collected. The most notable limitation is the geographical context in which the research was conducted. While developers were interviewed from multiple continents, participants from other stakeholder groups were exclusively from the Netherlands, within organizations operating in the country. Stakeholders' perspectives on SBOM may vary across different countries, as highlighted by P6 (SV), who mentioned differences in vulnerability perception between Dutch and German stakeholders.

Additionally, the B2B side only included employees from organizations operating in relatively critical sectors, which generally have more mature cybersecurity standards. This may have influenced their perceptions and may not fully represent all B2B organizations. The software vendors and IT-SIs interviewed shared similarities in their work activities, and the findings may have been different if a simple SaaS provider offering a single off-the-shelf application had been included.

Another notable limitation of this study is the absence of Chief Financial Officers (CFOs) among the participants. CFOs play a crucial role in decision-making processes, particularly regarding financial matters and resource allocation within organizations. Their perspective on the financial implications of implementing SBOM practices could have provided valuable insights into the feasibility and cost-effectiveness of such initiatives.

Some participants had limited knowledge or experience with SBOM. This may have affected the validity of their answers and introduced potential researcher bias when explaining certain concepts.

The number of participants per stakeholder group was relatively small (e.g., N=5). A larger sample size would have enhanced the validity of the results. However, due to time constraints, collecting data from more participants could have compromised the quality of the analysis and theory formation.

Research Approach, Methods, and Analyses

Also, there have been limitations associated with the research approach, methods, and analyses employed in this study. One limitation in the analysis process pertains to not tracking the frequency with which each participant mentioned specific themes. This additional analysis could have provided even deeper insights into the participants' perspectives and the relative importance they assigned to various themes related to SBOM. By quantifying the frequency, a more comprehensive understanding of the participants' viewpoints could have been achieved, enabling a more robust interpretation of the data.

Another limitation arises from the varying levels of knowledge and understanding among the participants regarding SBOM. While most participants demonstrated a strong understanding, a few had limited or recently acquired knowledge on the subject. This discrepancy in knowledge could have influenced their answers and perceptions of SBOM and its significance. It is crucial to acknowledge this limitation, as it may introduce bias and affect the generalizability of the findings.

During the process of identifying themes, a limitation arises due to the researcher's subjective interpretation of the dataset. While efforts were made to ensure a rigorous and comprehensive analysis, the identification of themes inherently involved the researcher's judgment and potential bias. This limitation highlights the importance of transparency and potential subjectivity in the theme identification process.

A limitation concerning the literature review is the exclusion of recent publications that were released online during the course of the thesis. As these publications were not available at the time of the initial literature review, their insights and findings could not be incorporated into the analysis. This limitation suggests the need for ongoing literature monitoring and consideration of the most up-to-date research in the field.

The dataset used for the ordinal preference ranking method was relatively small, consisting of only 16 participants. While efforts were made to ensure diversity among the participants, the limited sample size may affect the generalizability of the findings. This limitation underlines the need for larger sample sizes in future studies to enhance the reliability and validity of ordinal preference rankings.

A further limitation pertains to the absence of meso-level findings in the ordinal preference ranking method. The focus of this analysis was on individual preferences, neglecting potential insights at the organizational or group level. By not capturing meso-level findings, an opportunity to explore collective perspectives and identify patterns across organizations was missed. Future studies could consider incorporating a broader range of participants to address this limitation.

7.5. Reflection

Overall, this research journey has provided various elements that I find interesting to reflect upon. It encompasses both positive aspects and areas for improvement or things I would approach differently if given the opportunity to redo it. Firstly, I am definitely satisfied with the end result. I am delighted that I initially chose such a novel and engaging topic to delve into, which quickly made me feel like an expert in a specific niche. This enthusiasm was evident from the participants, especially those familiar with SBOM, who don't often get approached for interviews on this subject. The collaboration between academia and industry at Northwave was also enjoyable. Coincidentally, during the thesis, their first customers started expressing their initial thoughts on SBOM and how to handle it. I was asked if I could come up with a solution, and it was exciting to see that the research could be directly applied.

Looking back, I am satisfied with the time allocation I dedicated to thorough desk research, literature studies, data collection, and analysis. Despite some interviews feeling a bit last minute, it was reassuring to enter them with confidence in my own knowledge of SBOM. This confidence ultimately helped me gather more relevant results.

If I had the opportunity to redo everything, there are a few aspects I would approach differently. In hindsight, I would have given more priority and allocated additional time to conduct a larger-scale validation of the results with experts. Although some efforts were made within the time constraints, a more comprehensive validation process would have significantly enhanced the research's validity. However, the idea of scheduling sessions with experts came to me later in the process. Fortunately, among the participants, there were certainly field experts on SBOM.

Lastly, I could have approached the process of seeking supervisors more effectively. Generally, the process began with the university, and then I connected with Northwave. At one point, things progressed quickly at the latter, while my committee had not yet been formed. In retrospect, I could have been more specific about what I wanted to do in terms of research. However, it was challenging because I wanted to come up with a relevant research topic that I found interesting myself.

8

Conclusion

The final chapter of this research study serves as a crucial stage where conclusions are drawn, encompassing the main findings and addressing the research objectives. It is essential to derive accurate and well-supported conclusions to provide valuable insights and contribute to the existing SBOM knowledge base. In Section 8.1, the sub-questions are revisited, offering a comprehensive overview of the findings associated with each one. This section serves to summarize and consolidate the key insights obtained throughout the research process. Building upon the individually identified components, the main research question will be answered, presenting a detailed and comprehensive synthesis of the entire study in Section 8.2. Section 8.3 highlights the scientific contributions of this research, shedding light on the novel insights and contributions made to the academic field. Additionally, Section 8.4 addresses the practical contributions, discussing the implications and potential applications of the findings in real-world contexts. Finally, based on all the accumulated results and insights, Section 8.5 presents recommendations for future research endeavors. These recommendations offer valuable directions for further exploration and suggest areas of focus that hold potential for advancements in the field.

8.1. Addressing Sub-Research Questions (1-3)

Now, a presentation of the findings for each sub-research question will be provided, offering a concise overview for each of their results. The subsequent section will then aggregate and synthesize all these results, providing a comprehensive analysis.

SQ 1: What are the most important SSC stakeholders involved with SBOM?
For the first sub-question, an extensive stakeholder analysis was conducted to identify the most relevant stakeholders involved with SBOM and its lifecycle. The identified stakeholders include:

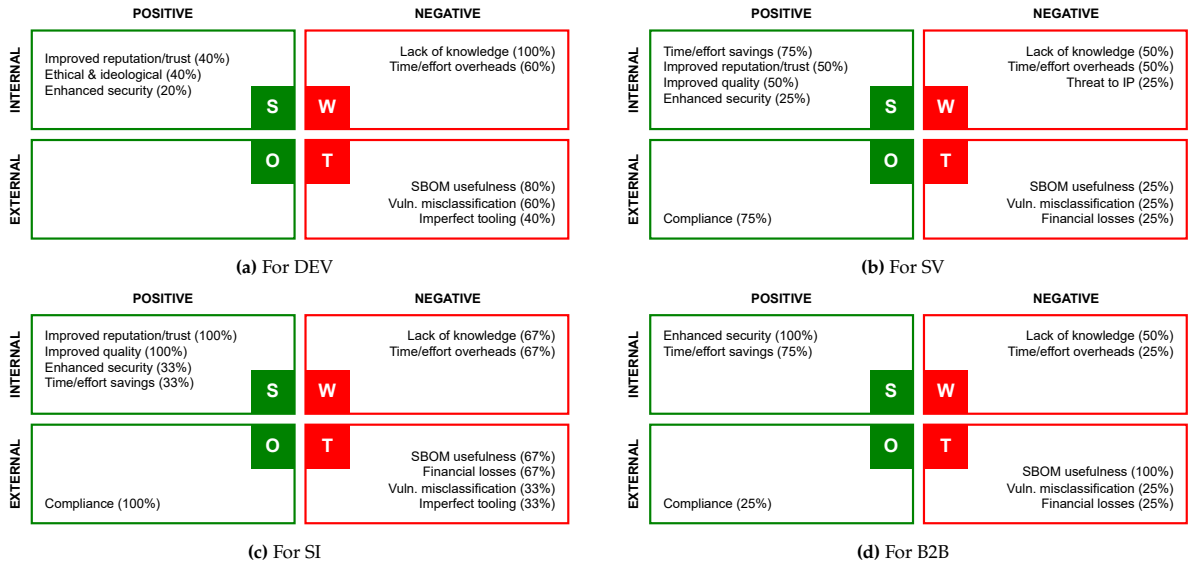
- B2B customers
- Software vendors
- IT system integrators
- Developers

SQ 2: What are the (dis)incentives and capabilities of SSC stakeholders regarding SBOM?
In addressing the second sub-question, Section 5.1 undertook an extensive literature review to compile an initial list of significant (dis)incentive categories relevant to both SBOM and other cybersecurity technologies. Based on this list, more specific interview questions were formulated. However, the responses obtained from participants during the fully open, semi-structured questions were predominantly deemed most significant in the outcomes. Through an iterative process, the thematic analysis, in conjunction with the frequency analysis, yielded findings that notably supplemented the answer to this second sub-question. Especially following the aggregation of the initially voluminous outcome findings, the primary incentives and disincentives per stakeholder group became evident (see Tables 6.2 and 6.3). These findings were matched up with the pre-established list, revealing that the latter comprehensively encompassed all empirically identified (dis)incentives. A few incentives not initially included in the list were appended based on their significance in the results. The collection of incentives and disincentives essentially constitutes the following two lists (see Table 8.1). This compilation includes the (technical) capabilities as well, predominantly addressing the technical concerns related to vulnerability misclassification and the disincentive associated with imperfect tooling, formats, and vulnerability databases.

Table 8.1: Overview of incentives & disincentives

Incentives	Disincentives
Compliance	Lack of knowledge or expertise
Enhanced security of consumed software	SBOM usefulness
Improved reputation or trust	Time or effort overheads
Time or effort savings	Vulnerability misclassification
Improved quality of supplied software	Financial losses
Ethical & ideological	Imperfect tooling, formats or vuln. DBs
-	Threat to IP

SQ 3: What factors can explain the lack of SBOM adoption?
To determine the most prominent factors among the identified incentives and disincentives that affect SBOM adoption within each stakeholder group, SWOT analyses were conducted (see Figure 8.1). These analyses served as the foundation for developing proposals or strategies aimed at fostering SBOM adoption within each respective group.



(a) For DEV

(b) For SV

(c) For SI

(d) For B2B

Figure 8.1: SWOT Matrices

For the B2B sector, a key strength is the expectation that incorporating SBOMs will result in **enhanced security** and **time or effort savings**. However, the current reality suggests that SBOM integration may lead to increased time and effort investments, with uncertain benefits. Recent high-profile cyberattacks like Log4Shell highlight the potential for significant damage, making SBOMs essential for vulnerability detection and response time reduction. B2B stakeholders perceive SBOMs as having **limited usefulness**, likely due to a **lack of knowledge**. This group is hesitant about SBOM relevance and anticipates cognitive challenges in implementation, resulting in low internal motivation.

The pursuit of SBOM adoption is notably stronger among the SI and SV groups, driven primarily by **regulatory compliance**. However, within stringent compliance regulations, SBOMs may be viewed as a procedural requirement. Additionally, these groups acknowledge SBOMs' value in **enhancing their reputation, trustworthiness, and the quality of supplied software**. Despite these benefits, they recognize the potential for **financial losses** and increased **time or effort overheads** associated with adoption. Consequently, these two stakeholder groups are poised to be the main drivers of widespread SBOM adoption, given their strong motivation and awareness of the technology's benefits.

Developers, similar to the B2B group, appear to be hesitant about adopting SBOM. Their motivation primarily stems from **ethical, ideological principles**, and the desire to **enhance their reputation and trustworthiness**. However, sustaining long-term internal motivation without corresponding rewards can be challenging. Financial contributions to widely used software projects are typically low, and developers in this study have not mentioned financial incentives. Additionally, since many developers work on projects as a hobby, they are not bound by certain requirements. Implementing SBOM

would require additional investments due to a **lack of knowledge** and increased **time and effort overheads**. The perceived **limited usefulness** of SBOM for developers is also a concern. Overall, developers currently show very little interest in adopting SBOM.

8.2. Addressing Main Research Question

The research aimed to gather new empirical insights into incentives and disincentives regarding SBOM from involved stakeholders in the SSC. Another goal was to examine how these factors influence adoption, to what extent, and which ones contribute to the current lack of adoption of the technology. To achieve this research objective, the following main research question was initially formulated:

What are the main (dis)incentives regarding SBOM among stakeholders in the SSC, and how do these impact its adoption?

This research has yielded a wealth of insights, which have been methodically structured in Table 8.1 and the SWOT analyses (see 8.1) for each stakeholder group. Upon examining these findings, it becomes apparent that the primary stakeholders engaged in both SBOM production and utilization, specifically the DEV and B2B groups, presently demonstrate the least incentives for SBOM adoption. Conversely, the key business stakeholders with the capacity to promote SBOM adoption are the SI and SV groups.

Furthermore, there are a few noteworthy points that deserve further discussion in the conclusion, because they stand out independently. These additional points should be taken into consideration to ensure a thorough conclusion.

SBOM selection

The selection of applications and systems for which an SBOM is needed was also identified as a potential additional complexity when considering ROI. This decision-making process varies for each application and system, adding difficulty due to the subjective nature of security. Determining the specific purpose and scope of SBOMs requires a risk assessment to assess the level of risk associated with each application or system. Moreover, the assessment itself incurs additional time and effort, further complicating the adoption process. It introduces an extra layer of choice and evaluation, making SBOM adoption less accessible for organizations. Especially for SMEs, it has been observed several times that they will struggle to allocate the necessary resources. This could potentially amplify the disincentives related to financial loss.

Suppliers emphasized that SBOMs should not be treated as add-ons but rather integrated into existing quality management programs. This perspective raises the potential issue of friction regarding payment and financial considerations. The integration of SBOMs seamlessly into quality management processes may require further negotiation and alignment between suppliers and customers.

Different use cases

Another significant finding from this study is how many individuals primarily viewed the use case where SBOMs are produced and consumed internally (within supplier companies) to ensure additional quality. At a micro-level, it was observed that participants who identified this use case had a more positive perception of SBOMs' success. The internal use case offers advantages in terms of the associated incentives. Particularly, it can result in time and effort savings, which are important considerations for the B2B sector. Furthermore, any concerns related to IP from the supply side may also be alleviated. It could also contribute significantly to ensuring quality, which proves to be a crucial incentive for SVs and SIs. However, the various use cases can also lead to confusion. Varied responsibilities and tasks can create ambiguity for SSC stakeholders, making it less clear what is expected of them. This ambiguity could potentially hinder adoption.

Law and regulation

Regarding the current regulatory context, there was also a significant lack of familiarity observed. Interestingly, those who were familiar with legislation such as NIS2, DORA, and CRA appeared to have a more positive sentiment towards SBOM. Another micro-level relationship seemed to exist between participants who acknowledged the lack of knowledge and expertise in the SSC and those who believed that if legislation were to mandate SBOM, it would become merely a compliance requirement without adding real value. The general consensus among participants was that legislation should serve as a framework, providing stakeholders with clarity on how to effectively manage their supply chain risks.

Unattainable perfection

This finding builds upon the previous observations regarding SBOM as a compliance tool, but in a positive light. Participants point out that starting with SBOM as a compliance measure is not necessarily a bad thing. Many suggest that it is important to start small and relatively simple, allowing it to gradually expand over time. This aligns with the notion of SBOM as an evolving process. The industry is still determining its trajectory. The mindset that it doesn't have to be (immediately) 100%

perfect and secure introduces a good nuance to the entire issue. Combined with the ongoing evolution of SBOM, this offers hope for adoption. At the micro-level, there was also a positive relationship between someone's level of experience with SBOM and their perception of the concept. As more individuals gradually become exposed to it, the SBOM culture may become more positive over time.

Governance

Lastly, the governance aspect of SBOM is important to consider, given the concerns raised by individuals, particularly those at the founder or high management level. Although the frequency count may not be extremely high, the fact that these individuals highlight it is something to take seriously. Their support and involvement are crucial in achieving adoption. Effective governance ensures that the necessary structures, policies, and decision-making processes are in place to drive SBOM implementation and utilization. It provides guidance, accountability, and strategic direction, fostering a supportive environment for adoption across stakeholders.

8.3. Scientific Contributions

Contributing to the scientific knowledge in a field, especially one as young as SBOM, can be really important. As evidenced, SBOM is still evolving, and any form of contribution at this stage can have a significant impact. In this regard, the research conducted in this study has made several scientific contributions that have filled important research gaps and shed light on various aspects of SBOM.

Firstly, this study has contributed to filling the research gap concerning the understanding of key incentives related to SBOM. By investigating the motivations and drivers behind SBOM adoption, the research provides valuable insights into the factors that influence organizations' decision-making processes. This contribution is essential in guiding policymakers, industry professionals, and researchers in developing strategies and frameworks that promote the adoption of SBOM.

Additionally, this study has addressed another research gap by exploring how these different interests, in combination with technical factors, may have hindered the adoption of the SBOM concept thus far. By examining the barriers and challenges faced by the identified key SSC stakeholders, the research highlights the complex dynamics involved in the adoption process. This understanding can inform future initiatives aimed at overcoming these barriers and promoting the widespread adoption of SBOM.

Furthermore, this study has provided new insights into the internal use case of SBOM, an area that has received limited attention in the existing literature. While previous research predominantly focused on the separation of production and consumption of SBOM, this study delves into the internal use of SBOM within organizations (primarily the suppliers of software). By exploring the benefits and challenges associated with internal utilization, the research uncovers the potential for improved operational efficiency and risk management. These findings contribute to a more comprehensive understanding of SBOM and expand the discourse surrounding its application.

The contributions made in this study not only advance the current state of knowledge but also pave the way for future research directions. By identifying research gaps, highlighting challenges, and proposing avenues for further investigation (which will be further elaborated on in the final Section of this Chapter, 8.5), this study establishes a foundation for future studies to build upon. It sets the stage for more in-depth examinations of specific aspects of SBOM, encourages the exploration of different contexts, and suggests potential areas for refinement and improvement.

8.4. Practical Contributions

The research has made practical contributions that can have an impact on various stakeholders within the software industry. One potential beneficiary is the regulatory bodies and policymakers who can benefit from understanding the areas they can influence. For instance, if these stakeholders would intend to promote SBOM among the SSC, they may find the research results valuable in complementing their efforts. The findings can provide insights and additional guidance for such initiatives.

Another practical contribution of the research is to Northwave, the industry partner involved in the study. As they are exposed to the first questions regarding SBOM coming in from their clients, the research outcomes can assist them in developing new services or solutions related to SBOM. The research findings can contribute to Northwave's ability to provide informed responses and solutions to their clients' needs.

Additionally, the research is relevant to the participants who were involved in the study. Some of the participants were actively involved in the development of proprietary or open source tooling related to SBOM. The research outcomes can potentially offer insights and guidance to these participants, enabling them to enhance their tooling and make it more effective and valuable.

By contributing to the overall improvement of the SBOM concept, the research aims to enhance the security of the entire software industry. As digitalization becomes prevalent across all sectors, one could say that the software industry plays a

crucial role in the economy. The concept of SBOM has the potential to benefit the entire industry, making it an exciting prospect. However, it is important to ensure that SBOM is a concept that genuinely adds value. The research findings indicate that the majority of people recognize a use case and hold an optimistic view of SBOM. Therefore, it is valuable to identify the pain points and barriers to mass adoption, as addressing and improving these areas can enhance the value and impact of SBOM. Ultimately, this can contribute to a more transparent and, hopefully, a safer society as a whole.

8.5. Recommendations for Further Research

To conclude the study, several recommendations are presented regarding stakeholder-specific factors within the SBOM domain that warrant further investigation, due to their potential to alleviate the current misaligned SBOM incentive issue. This final section initially focuses on identifying the most prominent concerns that create the most significant disincentives for the different stakeholder groups. Based on this, the section then examines which positive incentives could be strengthened and which negative disincentives could be mitigated. The aim is to restore a balance within the current (dis)incentive alignment and emphasize the importance of positive incentives. The overarching goal of these recommendations is to provide specific directions for the software industry and the scientific community to further investigate how widespread SBOM adoption throughout the SSC can be facilitated.

The SWOT analysis conducted is well-suited for this purpose. The conclusions drawn from it serve as the foundation for this subsequent section of further recommendations. The identified disincentives are thus the initial focus. Considering that the research presents a SWOT analysis for each distinct stakeholder group, the implications might potentially overlap. Moreover, the implications could vary based on the SBOM practitioners' intended actions derived from this study. Practitioners associated with particular groups would benefit the most by aligning their focus with the outcomes relevant to their specific group.

It is evident that the **lack of knowledge or expertise**, especially for the B2B stakeholder group, stands as the most significant weakness. Addressing this challenge entails various implications for them. To counter this deficiency, a potential avenue for improvement involves demonstrating them the **practical utility of the technology** and the **further refinement and development of tools** aimed at enhancing user-friendliness and comprehension. This proactive approach could potentially alleviate the severity of this disincentive by empowering stakeholders with varying levels of expertise to effectively harness the advantages offered by SBOM. Additionally, the concept of the **internal use case** could, at least for B2B customers, help alleviate the associated burdens. This is particularly relevant in light of the prevailing trend of shifting security responsibility towards the supply side. The increasing reliance on external expertise underlines the importance of mitigating knowledge-related challenges for B2B customers.

In the context of threats, **SBOM usefulness** emerges as the most prominent concern, once again irrespective of the stakeholder group. This aspect primarily encompasses issues surrounding detailing and layering, SBOM selection, and the notion of mere compliance. To enhance the usefulness of SBOM, focused interventions need to be researched and undertaken. Regarding **detailing and layering**, the early commencement of appropriate SBOM practices within the SSC is imperative, coupled with the accession of requisite dependency data through technologies such as dependency managers. Vital to this effort is the **timely incentivization of developers**, particularly those operating in the early layers of the SSC. Proactive involvement ensures the availability of necessary information pertaining to these layers in subsequent stages. This underlines the need to emphasize incentives for this stakeholder group (DEVs). There is a requirement for substantiating the fact that contributing to the improvement of detailing and layering is also beneficial to developers themselves. As per this research, such contributions should also **reinforce aspects like recognition and exposure** (encompassed by improved reputation and trust), acting as pivotal positive incentives for developers to adopt SBOM. Concerning **SBOM selection**, although feasibility might be constrained, especially for intricate integrated software systems, proactive efforts, particularly for COTS software, should be made. This initiative, in part, contributes to enhancing the usefulness of SBOM. Conversely, pertaining to the concept of **mere compliance**, if the assertion about the viability of initial compliance steps and the subsequent value extraction holds true, a transitional phase is likely to emerge, necessitating the establishment of quality requirements.

The weakness of **time and effort overheads** is prominently represented across all stakeholders, and especially a big inhibitor for the adoption behaviour of developers. To motivate them, compensating or sponsoring their projects could be a viable strategy. This approach would pique the interest of individual developers, encouraging them to invest their time and efforts in SBOM adoption. Notably, developers within organizations experience significant **time constraints**. While individual developers may not face such constraints, they perceive substantial **effort overheads** in implementing SBOM practices. Particularly, the **governance** associated with SBOM implementation can create substantial disincentives in this domain. The research reveals that the implementation of necessary processes can be time-intensive, exacerbated by the lack of clarity on a universally effective implementation approach. Addressing this challenge requires dedicated efforts. Collaborative endeavors and extensive engagement are pivotal for achieving successful SBOM implementation. To alleviate the burden of time and effort overheads, the processes related to SBOM must be streamlined. Research should

be conducted to define an effective **SBOM governance framework**. Issues such as **imperfect tooling and vulnerability databases** currently consume excessive time. Tooling remains inadequate, leading to labor-intensive manual work. The presence of inaccurate vulnerability databases often requires cross-referencing multiple databases to obtain comprehensive vulnerability insights. These aspects must also be considered for future focus and attention.

Among all participants, the aspect of **compliance** stands out as a widely recognized opportunity. It encompasses both **legal and regulatory** adherence as well as alignment with **industry standards**. Notably, strides have already been taken in the US with regards to direct initiatives, while Europe has forthcoming developments concerning the CRA, NIS2, and DORA. These advancements are encouraging. It remains to be seen what specific parameters will be established. An intriguing possibility lies in the potential obligatory implementation of the **internal use case for suppliers**. Additionally, a strategic assessment is required to effectively implement this legislation without conflicting with stakeholder value extraction, thus avoiding a mere compliance-oriented outcome. Regarding industry standards, the current landscape is relatively nascent, yet it holds promising prospects. Beyond legislative considerations, **substantial calls for SBOM from the B2B customer side** could prove instrumental. The amplification of customer demand is paramount, potentially instigating a ripple effect throughout the SSC. This, in turn, could catalyze heightened demand from commercial vendors, thereby extending the push to developers.

There seems to be a consensus among stakeholders that SBOM is an evolving concept. Starting with a focus on compliance is viewed as a reasonable strategy, allowing space for the concept's growth and evolution before drawing conclusive assessments. Nonetheless, it remains crucial to define explicit protocols for the creation of robust SBOMs, encompassing the identification of precise data components necessary. According to the findings of this study, the integration of dependency/package manager data could potentially enhance this objective. However, it is imperative to conduct further research to thoroughly develop these guidelines.

The strengths exhibit variations across distinct stakeholder groups. Notably, the attributes of **reputation and trust** hold significant importance for SVs, SIs, and developers. For this, ensuring that B2B customers possess a comprehensive understanding of SBOM is crucial, enabling them to factor these aspects into their evaluation and potential differentiation of suppliers. Possible **SBOM certifications** can also contribute to this endeavor, augmenting the overall reputation and trustworthiness of stakeholders. In the context of developers, addressing **detailing and layering issues** is paramount to fortify their incentives associated with **recognition and exposure**. This strategic alignment converges with the implications required to enhance **SBOM usefulness**, aligning with the multifaceted nature of promoting effective SBOM usefulness. Conversely, for B2B customers, the predominant incentive revolves around **security and business continuity**. The successful realization of SBOM value depends on addressing obstacles that have the potential to impede SBOM adoption. A strategic approach involves a comprehensive examination of the foremost threats and weaknesses, as expounded upon in the context of SBOM usefulness and the identified lack of knowledge.

All these potential implications and recommendations serve as starting points for the most significant findings identified in this study, to be further focused on if the industry or academia desires a more widely adopted SBOM. Hopefully, this research can contribute its small part to making SSCs and their stakeholders become more secure.

References

Adèr, H. J., & Mellenbergh, G. J. (2008). *Advising on Research Methods: A Consultant's Companion*. https://books.google.nl/books?hl=en&lr=&id=LCnOj4ZFyjkC&oi=fnd&pg=PA13&dq=Advising+on+research+methods:+A+consultant%27s+companion.&ots=L2x5p_WXlx&sig=shUs4swX4zU0YWmbUSOuLZxYj8w&redir_esc=y#v=onepage&q=Advising%20on%20research%20methods%3A%20A%20consultant's%20companion.&f=false

Alshenqeeti, H. (2014). Interviewing as a Data Collection Method: A Critical Review. *elr English Linguistics Research*, *3*(1). https://doi.org/10.5430/elr.v3n1p39

Amoako, R. (2014). Illicit drug use among Finnish children: Channels of acquisition.

ArganoUV(2020). The Pros and Cons of Working with Big vs Small System Integrators. https://weareuv.com/the-pros-and-cons-of-working-with-big-vs-small-system-integrators/.

Arora, A., Wright, V., & Garman, C. (2022). Strengthening the Security of Operational Technology: Understanding Contemporary Bill of Materials. *Journal of Critical Infrastructure Policy*, *3*, 117–135. https://doi.org/10.18278/jcip.3.1.8

Balliu, M., Baudry, B., Bobadilla, S., Ekstedt, M., Monperrus, M., Ron, J., Sharma, A., Skoglund, G., Soto-Valero, C., & Wittlinger, M. (2023). Challenges of Producing Software Bill Of Materials for Java. http://github.com/AsyncHttpClient/a

Bhandari, P.(2022). Ordinal Data | Definition, Examples, Data Collection & Analysis. https://www.scribbr.com/statistics/ordinal-data/.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706QP063OA

BRM(). Exploratory Research - Research-Methodology. https://research-methodology.net/research-methodology/research-design/exploratory-research/.

Brousseau, E., & Glachant, J.-M. (2002). *The Economics of Contracts: Theories and Applications* (Cambridge University Press, Ed.). https://books.google.nl/books?hl=en&lr=&id=fnnJ39z5UugC&oi=fnd&pg=PR8&dq=the+economics+of+contracts&ots=MrHLX1nx-8&sig=YlM8l04UosretkWByHEjVdtKUcY&redir_esc=y#v=onepage&q=the%20economics%20of%20contracts&f=false

Brown, R. B. (2006). Doing Your Dissertation in Business and Management : The Reality of Researching and Writing. *Doing Your Dissertation in Business and Management*, 43.

Caulfield, J.(2021). Een introductie tot thematische analyses | Met voorbeelden. https://www.scribbr.nl/onderzoeksmethoden/thematische-analyse/.

CBS(2022). 2. Cybersecuritymaatregelen. https://www.cbs.nl/nl-nl/longread/aanvullende-statistische-diensten/2022/cybersecuritymonitor-2020/2-cybersecuritymaatregelen.

CISA(). Executive Order on Improving the Nation's Cybersecurity | CISA. https://www.cisa.gov/topics/cybersecurity-best-practices/executive-order-improving-nations-cybersecurity.

Clancy, C., Ferraro, J., Martin, R., Pennington, A., Sledjeski, C., & Wiener, C. (2021). Deliver Uncompromised: Securing Critical Software Supply Chains. *MITRE*.

Cook, W. D. (2006). Distance-based and ad hoc consensus models in ordinal preference ranking. *European Journal of Operational Research*, *172*(2), 369–385. https://doi.org/10.1016/J.EJOR.2005.03.048

Crowdstrike. (2021). *Software Bill of Materials Elements and Considerations* (tech. rep.). https://www.crowdstrike.com/blog/what-the-new-cybersecurity-executive-order-means-for-public-sector/.

CSIS(). Financial Sector Cybersecurity. https://www.csis.org/programs/strategic-technologies-program/archives/cybersecurity-and-governance/financial-sector.

Dependency-Track(). Dependency-Track | Software Bill of Materials (SBOM) Analysis | OWASP. https://dependencytrack.org/.

DNB(2021). Resultaat jaarlijkse onderzoeken naar Cyber gepubliceerd in IB monitor 2021. https://www.dnb.nl/nieuws-voor-de-sector/resultaat-jaarlijkse-onderzoeken-naar-cyber-nu-gepubliceerd-in-ib-monitor-2021/.

Donovan, R.(2020). Good coders borrow, great coders steal. https://stackoverflow.blog/2020/05/20/good-coders-borrow-great-coders-steal/.

Dragomir, A.-V. (2021). WHAT'S NEW IN THE NIS 2 DIRECTIVE PROPOSAL COMPARED TO THE OLD NIS DIRECTIVE. https://seaopenresearch.eu/Journals/articles/SPAS_27_1.pdf

Dussart, A., Aubert, B. A., & Patry, M. (2002). An Evaluation of Inter-Organizational Workflow Modeling Formalisms.

Eggers, S., Simon, T., Morgan, B., Bauer, E., & Christensen, D. (2022). Towards Software Bill of Materials in the Nuclear Industry A primer on the current SBOM ecosystem and a recommended "crawl, walk, run" approach for seamlessly integrating an SBOM program in nuclear power plants. https://doi.org/10.2172/1901825

Elias & Jones(2022). Software bills of materials face long road to adoptionSoftware bills of material face long road to adoption. https://cyberscoop.com/dhs-sbom-adoption/.

Elman, C., Gerring, J., & Mahoney, J. (2020). *Exploratory Research: The Production of Knowledge: Enhancing Progress in Social Science - Google Books*. Cambridge University Press. https://books.google.nl/books?hl=en&lr=&id=vlTMDwAAQBAJ&oi=fnd&pg=PR13&dq=Elman,+C.,+Gerring,+J.,+%26+Mahoney,+J.+(2020).+Exploratory+Research:+The+Production+of+Knowledge:+Enhancing+Progress+in+Social+Science.+Cambridge+University+Press,+pp.+17-41&ots=lTuCmZUfXp&sig=NSgescGj7ZkVTznyWW3WFC11mXs&redir_esc=y#v=onepage&q&f=false

EPRS. (2023). The NIS2 Directive: A high common level of cybersecurity across the Union.

European Commission(2022). Cyber Resilience Act | Shaping Europe's digital future. Policy and legislation. https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act.

European Parliament(2022). EUR-Lex - 32022R2554 - EN - EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2554.
Forbes(2022). The Cautionary Tale Of The Third-Party SaaS Buyer. https://www.forbes.com/sites/forbestechcouncil/2022/09/01/the-cautionary-tale-of-the-third-party-saas-buyer/.
Fouad, N. S. (2022). The security economics of EdTech: vendors' responsibility and the cybersecurity challenge in the education sector. *Digital Policy, Regulation and Governance*, *24*(3), 259–273. https://doi.org/10.1108/DPRG-07-2021-0090/FULL/XML
Fox, B.(2022). EU Cyber Resilience Act: Good for Software Supply Chain Security, Bad for Open Source? https://blog.sonatype.com/eu-cyber-resilience-act-good-for-software-supply-chain-security-bad-for-open-source.
García, A. A. (2011). Cognitive interviews to test and refine questionnaires. *Public health nursing (Boston, Mass.)*, *28*(5), 444–450. https://doi.org/10.1111/J.1525-1446.2010.00938.X
Getthematic(). Thematic analysis: an overview. https://getthematic.com/insights/thematic-analysis-overview/.
Gibbons, S.(2022). Stakeholder Interviews 101. https://www.nngroup.com/articles/stakeholder-interviews/.
Girdhar, S. (2022). Identification of Software Bill of Materials in Container Images. https://doi.org/10.13140/RG.2.2.26124.80003
GitHub(). Exporting a software bill of materials for your repository. https://docs.github.com/en/code-security/supply-chain-security/understanding-your-software-supply-chain/exporting-a-software-bill-of-materials-for-your-repository.
GitHub(). Introducing self-service SBOMs | The GitHub Blog. https://github.blog/2023-03-28-introducing-self-service-sboms/.
Google Scholar(). Google Scholar. https://scholar.google.com/.
Gordon, L. A., & Loeb, M. P. (2002). The Economics of Information Security Investment. *ACM Transactions on Information and System Security*, *5*. https://doi.org/10.1145/581271.581274
Gunson, N., Marshall, D., Morton, H., & Jack, M. (2011). User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking. *Computers & Security*, *30*(4), 208–220. https://doi.org/10.1016/J.COSE.2010.12.001
Hertweck, D., & Bouché, D. (2006). Case study: How to implement collaborative software supply chains Lessons learned from the task initiative. *IFIP International Federation for Information Processing*, *224*, 627–634. https://doi.org/10.1007/978-0-387-38269-2{_}66/COVER
Heydarian, N. M. (2016). Developing Theory With the Grounded-Theory Approach and Thematic Analysis. https://doi.org/10.1080/09515071003776036
IBM(). IaaS vs. PaaS vs. SaaS. https://www.ibm.com/topics/iaas-paas-saas.
Issa, A. A., Bailey, T., Boehm, J., & Weinstein, D.(2021). Enterprise cybersecurity: Aligning third-party cyber risk. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/enterprise-cybersecurity-aligning-third-parties-and-supply-chains.
Jones, T. L., Baxter, M., & Khanduja, V. (2013). A quick guide to survey research. *Annals of the Royal College of Surgeons of England*, *95*(1), 5–7. https://doi.org/10.1308/003588413X13511609956372
Kipo, D. D. (2013). Mixed Research Methods: Reflections on Social Public Policy. *Asian Social Science*, *9*(17). https://doi.org/10.5539/ass.v9n17p259
Koran, A., Nather, W., Scott, S., & Brackett, S.(2022). The cases for using the SBOMs we build. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/the-cases-for-using-sboms/.
Kuckartz, U. (2019). Qualitative Text Analysis: A Systematic Approach, 181–197. https://doi.org/10.1007/978-3-030-15636-7{_}8
Laplante, P. (2021). Software Labels. *Computer*, *54*(11), 82–86. https://doi.org/10.1109/MC.2021.3102360
Lin, L. (2023). Generating Software Bill of Material for Vulnerability Management and License Compliance. https://aaltodoc.aalto.fi:443/handle/123456789/119386
Majid, M. A. A., Othman, M., Mohamad, S. F., Lim, S. A. H., & Yusof, A. (2017). Piloting for Interviews in Qualitative Research: Operationalization and Lessons Learnt. *International Journal of Academic Research in Business and Social Sciences*, *7*(4). https://doi.org/10.6007/IJARBSS/V7-I4/2916
Makri, C., & Neely, A. (2021). Grounded Theory: A Guide for Exploratory Studies in Management Research. *International Journal of Qualitative Methods*, *20*. https://doi.org/10.1177/16094069211013654/ASSET/IMAGES/LARGE/10.1177{_}16094069211013654-FIG3.JPEG
Martin, R. A. (2020). Visibility Control: Addressing Supply Chain Challenges to Trustworthy Software Enabled Things. *Systems Security Symposium, SSS 2020 - Conference Proceedings*. https://doi.org/10.1109/SSS47320.2020.9174365
Martínez, J., & Durán, J. (2021). Software supply chain attacks, a threat to global cybersecurity: SolarWinds' case study. *International Journal of Safety and Security Engineering*, *11*, 537–545. https://doi.org/10.18280/ijsse.110505
McKinsey & Company(2021). Organizational cyber maturity: A survey of industries | McKinsey. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/organizational-cyber-maturity-a-survey-of-industries.
Moroz, A. (2022). Towards secure software development at Neste: a case study. http://www.cs.helsinki.fi/handle/10138/350407
Nadgowda, S. (2022). Engram: The One Security Platform for modern Software Supply Chain Risks. *WoC 2022 - Proceedings of the 8th International Workshop on Container Technologies and Container Clouds, Part of Middleware 2022*, 7–12. https://doi.org/10.1145/3565384.3565889
Namugenyi, C., Nimmagadda, S. L., & Reiners, T. (2019). Design of a SWOT Analysis Model and its Evaluation in Diverse Digital Business Ecosystem Contexts. https://doi.org/10.1016/j.procs.2019.09.283
Nguyen, B. A.(2023). Why SBOMs are critical to complying with the EU Cyber Resilience Act. https://www.cybeats.com/blog/why-sboms-are-critical-to-complying-with-the-eu-cyber-resilience-act.
()NIS 2 Directive. https://www.nis-2-directive.com/.
Nissen, C., Gronager, J., Metzger, R., & Rishikof, H. (2018). Deliver Uncompromised: A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War. *Mitre*. https://apps.dtic.mil/sti/citations/AD1108046
NIST(2022). Software Security in Supply Chains: Software Bill of Materials (SBOM). https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/software-security-supply-chains-software-1.

Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic Analysis: Striving to Meet the Trustworthiness Criteria. *International Journal of Qualitative Methods*, *16*(1). https://doi.org/10.1177/1609406917733847/ASSET/IMAGES/LARGE/10.1177{_}1609406917733847-FIG4.JPEG

NTIA. (2019). Framing Software Component Transparency: Establishing a Common Software Bill of Material (SBOM) NTIA Multistakeholder Process on Software Component Transparency Framing Working Group. https://flic.kr/p/46dsiz

NTIA(2021). SBOM Tool Classification Taxonomy. https://www.ntia.gov/files/ntia/publications/ntia_sbom_tooling_taxonomy-2021mar30.pdf.

NTIA. (2021b). Software Consumers Playbook: SBOM Acquisition, Management, and Use.

NTIA(2021). Vulnerability-Exploitability eXchange (VEX) – An Overview. https://www.ntia.gov/files/ntia/publications/vex_one-page_summary.pdf.

Nygard, A. R., & Katsikas, S. (2022). SoK: Combating threats in the digital supply chain. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3538969.3544421

Okafor, C., Schorlemmer, T., Torres-Arias, S., & Davis, J. (2022). SoK: Analysis of Software Supply Chain Security by Establishing Secure Design Properties. *Department of Electrical and Computer Engineering Faculty Publications*. https://docs.lib.purdue.edu/ecepubs/160

OWASP(). OWASP CycloneDX | OWASP Foundation. https://owasp.org/www-project-cyclonedx/.

OWASP(). OWASP Dependency-Check | OWASP Foundation. https://owasp.org/www-project-dependency-check/.

OWASP(). OWASP Dependency-Track | OWASP Foundation. https://owasp.org/www-project-dependency-track/.

Owen, R.(2022). The SBOM Is Coming, with Allan Friedman. https://finitestate.io/blog/the-sbom-is-coming-with-allan-friedman.

Pashchenko, I., Scandariato, R., Sabetta, A., & Massacci, F. (2021). Secure Software Development in the Era of Fluid Multi-party Open Software and Services. *Proceedings - International Conference on Software Engineering*, 91–95. https://doi.org/10.1109/ICSE-NIER52604.2021.00027

Petsas, T., Tsirantonakis, G., Athanasopoulos, E., & Ioannidis, S. (2015). Two-factor Authentication: Is the World Ready? Quantifying 2FA Adoption. https://doi.org/10.1145/2751323.2751327

Phillips, A., Maple, C., Lukavsky, F., Pearson, I., Richardson, M., Hanson, N., Kearney, P., & Dobson R. (2023). Software Bills of Materials for IoT and OT devices.

Remaley, E. L. (2021). *Software Bill of Materials Elements and Considerations* (tech. rep.).

Riegelsville, P.(2023). The Government's Software Bill of Materials (SBOM) Mandate Is Part of a Bigger Cybersecurity Picture. https://www.prweb.com/releases/the_governments_software_bill_of_materials_sbom_mandate_is_part_of_a_bigger_cybersecurity_picture/prweb19219949.htm.

Rispens, S. I.(2021). Why the World Needs a Software Bill Of Materials Now. https://drrispens.medium.com/why-the-world-needs-a-software-bill-of-materials-now-5a565df65dff.

Roberts, P.(2021). Log4j is why you need a software bill of materials (SBOM). https://www.reversinglabs.com/blog/log4j-is-why-you-need-an-sbom.

Romanosky, S., & Welburn, J. W. (2022). Disclosure of Software Supply Chain Risks. *Disclosure of Software Supply Chain Risks*. https://doi.org/10.7249/PEA2072-1

Scacchi, W., & Alspaugh, T. A. (2019). Securing Software Ecosystem Architectures: Challenges and Opportunities. *IEEE Software*, *36*(3), 33–38. https://doi.org/10.1109/MS.2018.2874574

SCANOSS(). SCANOSS | Open Source Inventorying Engine. https://scanoss.com/.

Scopus(). Scopus preview - Scopus - Welcome to Scopus. https://www.scopus.com/home.uri.

Sharma, A., Gupta, J., Gera, L., Sati, M., & Sharma, S. (2020). Relationship Between Customer Satisfaction and Loyalty. *SSRN Electronic Journal*. https://doi.org/10.2139/SSRN.3913161

Suddaby, R. (2006). From the editors: What grounded theory is not. *Academy of Management Journal*, *49*(4), 633–642. https://doi.org/10.5465/AMJ.2006.22083020

Taylor, J., & Dantu, R. (2021). For Love or Money? Examining Reasons behind OSS Developers' Contributions. *https://doi.org/10.1080/10580530.2021.1879323*, *39*(2), 122–137. https://doi.org/10.1080/10580530.2021.1879323

Top, S., Dilek, S., & Çolakoğlu, N. (2011). Perceptions Of Network Effects: Positive Or Negative Externalities? *Procedia - Social and Behavioral Sciences*, *24*, 1574–1584. https://doi.org/10.1016/J.SBSPRO.2011.09.033

Viega, J., & Michael, J. (2021). Struggling With Supply Chain Security. *Computer*, *54*. https://doi.org/10.1109/MC.2021.3075412

Wang, X. (2021). On the Feasibility of Detecting Software Supply Chain Attacks. https://doi.org/10.1109/MILCOM52596.2021.9652901

Wright, E., Lindsay, D., Wilkinson, G., Fraser, H., & Collings, N. (2021). Strengthening Australia's cyber security regulations and incentives A call for views. https://www.pmc.gov.au/government/commonwealth-coat-arms.

Xia, B., Bi, T., Xing, Z., Lu, Q., & Zhu, L. (2023). An Empirical Study on Software Bill of Materials: Where We Stand and the Road Ahead. https://doi.org/10.48550/arXiv.2301.05362

Yamashita, T., & Millar, R. J. (2021). Likert Scale. *Encyclopedia of Gerontology and Population Aging*, 2938–2941. https://doi.org/10.1007/978-3-030-22009-9{_}559

Young, S. D. (2021). EXECUTIVE OFFICE OF THE PRESIDENT. https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/security-measures-eo-

Zajdel, S., Elias Costa, D., & Mili, H. (2022). Open Source Software: An Approach to Controlling Usage and Risk in Application Ecosystems. *SPLC '22: Proceedings of the 26th ACM International Systems and Software Product Line Conference*, *A*, 154–163. https://doi.org/10.1145/3546932.3547000

A

Appendix: Search and Selection

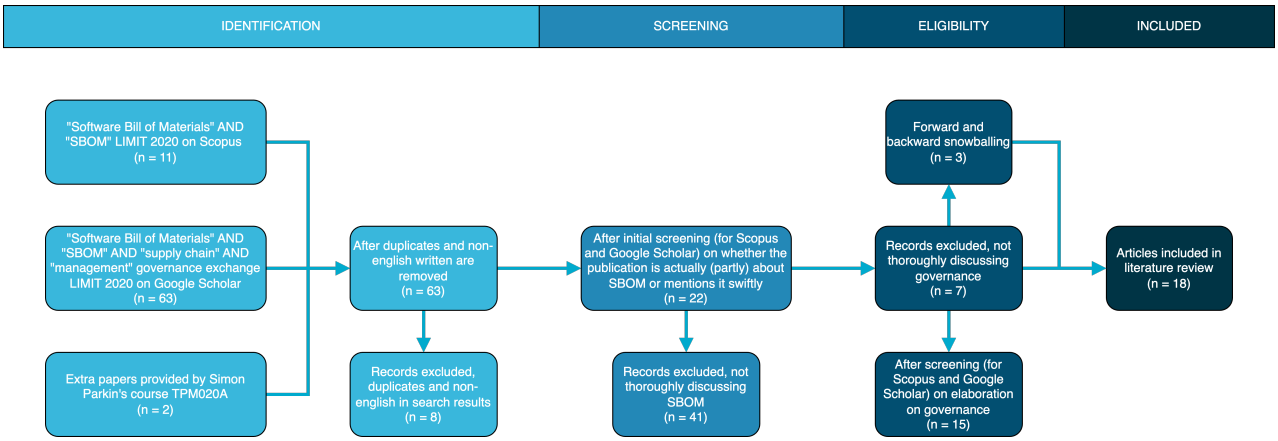


Figure A.1: Visualization of the search and selection process

Table A.1: Overview Selected Articles

Title of article	Author(s) & date	Benefits of SBOM	Lack of SBOM adoption	Misaligned incentives on SSC
An Empirical Study on Software Bill of Materials: Where We Stand and the Road Ahead	Xia et al. (2023)	x	x	x
Deliver Uncompromised: A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War	Nissen et al. (2018)	x		
Deliver Uncompromised: Securing critical software supply chains	Clancy et al. (2021)	x		
Disclosure of Software Supply Chain Risks	Romanosky and Welburn (2022)	x		
Engram: The One Security Platform for Modern Software Supply Chain Risks	Nadgowda (2022)	x		
Identification of Software Bill of Materials in Container Images	Girdhar (2022)	x		
Open source software: an approach to controlling usage and risk in application ecosystems	Zajdel et al. (2022)	x		
Software Supply Chain Attacks, a Threat to Global Cybersecurity: SolarWinds' Case Study	Martínez and Durán (2021)	x		
SoK: Analysis of Software Supply Chain Security by Establishing Secure Design Properties	Okafor et al. (2022)	x		
SoK: Combating threats in the digital supply chain	Nygard and Katsikas (2022)			x
Strengthening Australia's cyber security regulations and incentives	Wright et al. (2021)			x
Strengthening the Security of Operational Technology	Arora et al. (2022)	x	x	
Struggling With Supply-Chain Security	Viega and Michael (2021)			x
The economics of information security investment	Gordon and Loeb (2002)			x
The security economics of EdTech: vendors' responsibility and the cybersecurity challenge in the education sector	Fouad (2022)			x
Towards secure software development at Neste - a case study	Moroz (2022)	x	x	x
Towards Software Bill of Materials in the Nuclear Industry	Eggers et al. (2022)	x		
Visibility & Control: Addressing Supply Chain Challenges to Trustworthy Software-Enabled Things	Martin (2020)	x		

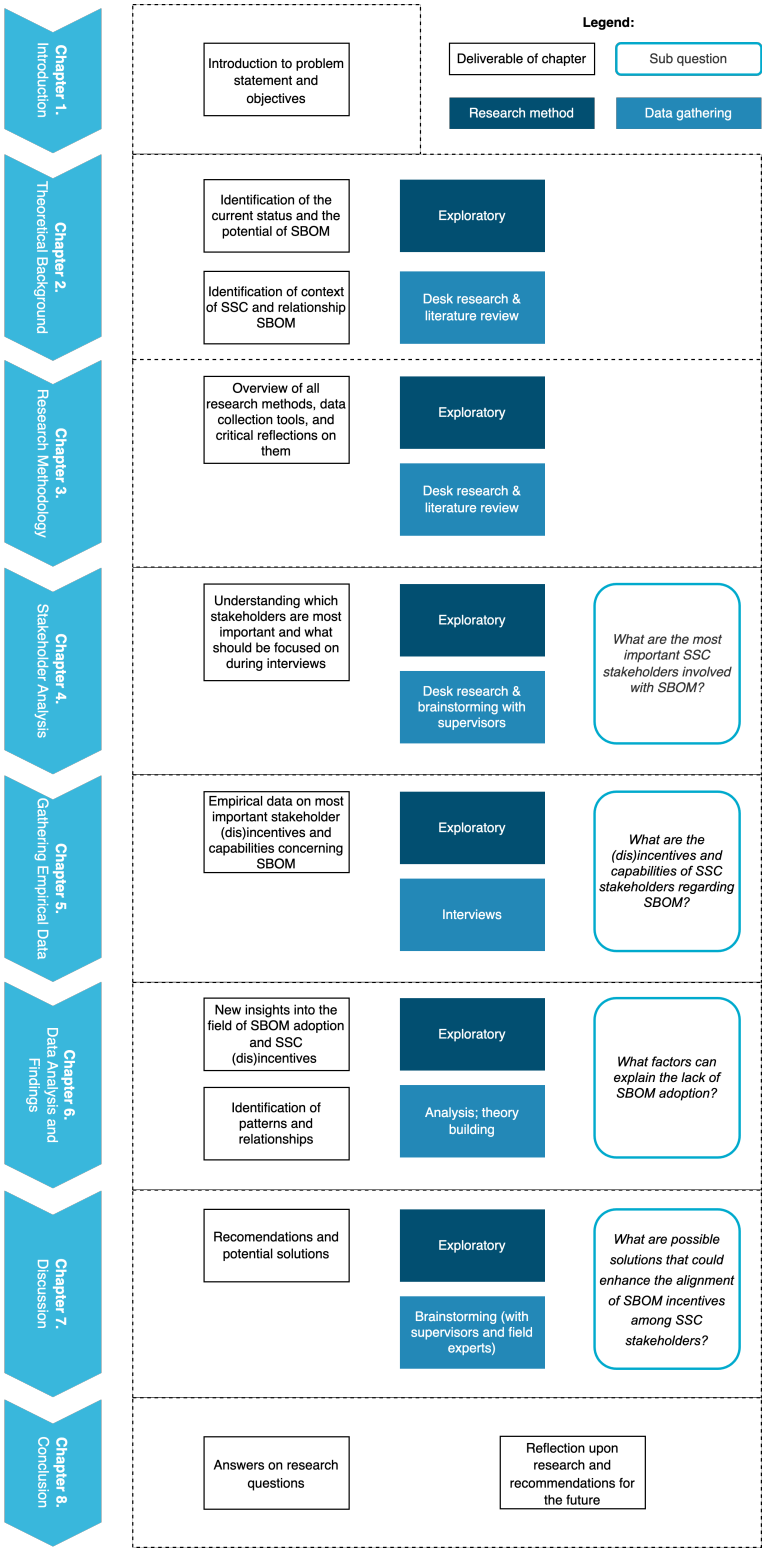


Figure A.2: Research Flow Diagram of the Thesis

B

Appendix: Results of Gathering Empirical Data

B.1. Summaries of Interviews

B.1.1. Summary 1

Demographic Characteristics	Response
Stakeholder Group	IT System Integrator
Years of experience in the software field	4
Company sector	IT Consultancy
Job function	Low-code Developer
Prior SBOM knowledge	Little
Prior SBOM experience	None

Software supplied to customers is not always clear to them. This may be because they have limited knowledge or because it lacks proper documentation from the developer's side. The interviewee also believes that developers should be given more time to document such things in order to increase transparency. However, they acknowledge that developers are not hired specifically for documentation but for development.

The risks involved include implementing out-of-the-box software components in the application provided to the customer, without fully exploring potential issues or bugs. While the software may pass initial testing and user acceptance phases, it may later reveal bugs due to the open-source software incorporated into the application.

The primary benefits are transparency and the potential prevention of security risks. Customers may have better insights into what they can expect from the software, enabling them to make informed choices among various software suppliers. However, this depends on whether other suppliers adopt similar practices.

A significant driving force is the responsibility for the software being offered. If the interviewee could consume the SBOM in a specific tool, identify vulnerabilities, and address them before offering the software to the customer, it would greatly alleviate issues. Therefore, the advantages of SBOM adoption extend beyond customer communication, as they can be applied even before engaging with the customer. The interviewee also mentions that alongside publicity, regulatory compliance is a major driving force for SBOM adoption.

Trust and reputation can work in two ways for a supplier towards the customer. If the customer receives an SBOM that reveals numerous vulnerabilities after consumption, it damages trust. Suppliers want to avoid this scenario, so they should consume the SBOM themselves before delivering it to the customer. Conversely, delivering high-quality SBOMs and software has a positive effect.

The interviewee believes that once one major player adopts SBOM, others will quickly follow suit. Given their prominent name, there is already some level of trust. However, the interviewee acknowledges that large companies employ many individuals, and the software they deliver often varies. If a major player falls short, it becomes big news, which is something they want to avoid. Big players rely heavily on their reputation. For small suppliers, it could be highly motivating to demonstrate that their software is secure and to differentiate themselves.

The interviewee suggests that NDAs should be in place for SBOMs, ensuring their privacy and prohibiting dissemination. This would address concerns about IP for suppliers.

The interviewee points out that when developers retrieve code from the internet, such as from Stack Overflow or ChatGPT, SBOMs might struggle to detect it. Good tooling is crucial; SBOMs depend on it. People don't have time to extensively document every version number they use. Similarly, customers also need to consume SBOMs, which often require hiring cybersecurity specialists to understand them.

In conclusion, regulation will be crucial. If regulations are implemented, the interviewee remains optimistic; otherwise, they are somewhat skeptical about adoption.

B.1.2. Summary 2

Demographic Characteristics	**Response**
Stakeholder Group	B2B Customer
Years of experience in the software field	20
Company sector	Financial
Job function	CISO
Prior SBOM knowledge	Good
Prior SBOM experience	None

Security by design or by default is still not widely implemented. We are primarily focused on responding to vulnerabilities that are discovered after the fact. As more software moves to the cloud and is offered as a service, there is less emphasis on the responsibility of the user. Even from our company's perspective, when we purchase software, we assume that the vendors have taken care of security.

The main advantage of SBOM is increased transparency. It provides a better understanding of the software we use. Software doesn't have to be 100% secure, but it's important to know its weaknesses and weigh them against the benefits in order to make an informed decision.

One significant conflict arises from the question of ownership. Who ultimately has control? Users often assume some level of responsibility when they purchase a product, but they may lack the knowledge to fully take on that responsibility. They expect the vendor to be accountable. The larger the gap between the vendor and the user, the more challenging this becomes.

SBOM can be a useful tool for managing and mitigating risks. However, there is a question of who possesses the necessary knowledge and expertise to effectively utilize it.

Paying more for software with an SBOM should be feasible. However, determining the value is subjective, depending on the benefits received in return.

When it comes to big-name suppliers, the most important factor is their ability to deliver results.

The consumption of Software as a Service (SaaS) is increasing. The responsibility for updates is shifting more towards the vendor. However, vendors face difficulties when customers integrate their product with other systems in their primary processes. Releasing a new patch may cause disruptions, leading to additional challenges.

Often, regulations are the only effective means to address these issues. However, enforcement plays a crucial role. If regulations are mandated but there is no clear way to monitor and penalize non-compliance, the effectiveness is compromised. Explicitly including SBOM in NIS 2 regulations would be helpful, but it remains uncertain whether people would understand and know how to comply.

It's important to recognize that software can be vulnerable. Vulnerability itself is a weakness. However, the level of vulnerability depends on the software's location and usage. For example, if it is used on-premises with multiple layers of security, a critical vulnerability may exist, but it is inaccessible. This poses challenges for penetration testers who identify critical code that doesn't contain sensitive data. The value of CVEs lies in their ability to identify vulnerabilities. However, if many vulnerabilities are not exploitable and require no action, their usefulness is questionable. Maybe the software is then just built really well.

Organizations face numerous challenges, and the question of what SBOM brings arises. Is it worth investing time and money, or should others handle it? Security remains a secondary concern compared to primary revenue-generating processes. While attention must be given to security, costs should not outweigh the benefits of these processes. SBOM is just one aspect to explore among the many considerations.

In conclusion, skepticism remains regarding the benefits of SBOM. The concept is understood theoretically, and optimism can exist in theory, but practical implementation presents significant challenges. At this point, widespread adoption of SBOM is not evident.

B.1.3. Summary 3

Demographic Characteristics	**Response**
Stakeholder Group	B2B Customer
Years of experience in the software field	27
Company sector	Water sector (critical)
Job function	Division manager, and also responsible for cybersecurity and IT
Prior SBOM knowledge	Good
Prior SBOM experience	None

Large risks within the supply chain arise from a lack of awareness regarding vulnerabilities. Organizations often remain unaware of their own vulnerabilities, making it difficult to identify and address potential threats. The lack of transparency hinders the ability to quickly locate and address vulnerabilities when updates are released. Shadow IT further complicates the situation by introducing unknown elements into the supply chain. Asset management systems may not effectively capture these elements.

The Log4j incident served as a catalyst for many companies to take significant steps towards improving their vulnerability management practices. While some organizations had existing lists, doubts arose regarding their completeness. It was also discovered that certain suppliers had limited knowledge of their vulnerabilities.

The main advantage of implementing an SBOM is achieving control and transparency within the supply chain, particularly in critical sectors such as water supply, where security is crucial. The ability to continuously deliver essential services and maintain operational and financial stability relies on robust security measures.

The biggest driving force is solely the ability to provide 24/7 delivery of drinking water and keep your operations and finances running. When you reach a point where you can no longer pay anyone, purchase chemicals, and face various other challenges, ultimately your production of drinking water will collapse.

The demand for faster software development is driving the need for speed and innovation. However, open-source solutions, while accelerating development, require additional security measures to ensure safety and maintainability. Striking the right balance between speed and security is essential to avoid hindering progress and creating future maintenance challenges.

European procurement processes allow organizations to score suppliers based on quality and safety, enabling the prioritization of secure vendors. However, striking a balance between stringent requirements and supplier availability, especially in a challenging labor market, is crucial.

While larger companies are generally expected to have robust security measures in place, effectively managing network scanning results can be challenging due to the prevalence of false positives. Contextual understanding is necessary to accurately assess risks and prioritize actions.

Legislation and regulations are expected to drive the implementation of SBOM, compelling both users and suppliers to be aware of and accountable for their supply chains. Ensuring data accuracy and quality within the SBOM requires meticulous data management and a robust governance framework. Successful implementation relies on collaboration among multiple stakeholders from different sectors.

Striving for 100% guarantee in terms of SBOM completeness may not be realistic or practical. It is important to identify and prioritize critical factors and set achievable goals. Certification of SBOM could play a role in ensuring quality and adherence to standards.

While optimistic about the necessity and potential of improving supply chain security through SBOM, it is acknowledged that the implementation process is complex and challenging. Skilled leadership, high-level support, and collaboration are vital to drive progress and overcome the associated obstacles.

In conclusion, implementing SBOM offers the promise of enhanced supply chain security, but it requires careful planning, coordination, and cooperation across various disciplines to achieve the desired outcomes.

B.1.4. Summary 4

Demographic Characteristics	Response
Stakeholder Group	Software Vendor
Years of experience in the software field	20+
Company sector	Digital agency
Job function	Process manager and security coordinator, responsible for delivery management and maintenance processes
Prior SBOM knowledge	Good
Prior SBOM experience	About to get started

The main benefit of SBOM for us would be having an overview of all software components in the solutions we provide to our customers. As a security coordinator, I can quickly determine the impact of a critical vulnerability on specific solutions, projects, and customers. This enables effective communication with the customer, informing them about the identified risk in our managed systems and the need for mitigation.

From a security perspective, the primary driving force behind SBOM is the ability to act swiftly when a critical vulnerability is reported. This proactive approach allows us to address security issues promptly and ensure the safety of our systems.

In my view, we should not pass on the costs of SBOM to our customers. Initially, it should be a tool aimed at enhancing the quality of our deliverables. Quality should be our intrinsic priority, alongside the production-first mindset. Our solutions should operate seamlessly without issues, and SBOM can assist us in achieving this goal. Additionally, it should prioritize security to prevent any potential hacking incidents that could compromise our customers' trust. Customers should only incur additional costs if they request additional services, such as monthly reports.

When customers trust us to deliver reliable products and be proactive in addressing security concerns, it increases the likelihood of them choosing us for future projects. Meeting expectations regarding well-regulated practices is crucial for established companies. While no company is perfect from the start, implementing SBOM is one of the necessary improvements we must undertake.

Regulations serve as a motivator, providing a fallback if companies don't take intrinsic initiative. However, businesses should be proactive in adopting SBOM even before it becomes a regulatory requirement. Once regulations enforce SBOM, it will undoubtedly be a significant step forward for software vendors.

IP might pose challenges depending on how SBOM is structured and what information it includes. It will depend on the specific details. As of now, I don't anticipate any issues regarding open-source components. If the focus is solely on identifying open-source elements, I understand the rationale behind making it a requirement, especially for the US government, which seeks to avoid unwanted backdoors.

The key concern is ensuring that generating an SBOM is as simple as possible, avoiding lengthy manual processes. A successful implementation requires a user-friendly tool that can generate the SBOM with a press of a button, in a desired format. This ease of use and searchability are crucial for the tool's success.

To date, I haven't encountered any questions or concerns about SBOM from our customers. However, I remain optimistic about its potential benefits and importance.

B.1.5. Summary 5

Demographic Characteristics	Response
Stakeholder Group	B2B Customer
Years of experience in the software field	29
Company sector	Insurance
Job function	Manager Product and Tech
Prior SBOM knowledge	Okay
Prior SBOM experience	None

We operate under the supervision of DNB and AFM, and rightfully so, they have security requirements in place. We have engaged Northwave for that purpose, but they also impose their own demands. Currently, SBOM is less relevant from a compliance perspective since DNB does not require it. However, this may change in the coming years.

The greatest advantage of SBOM is having a clear understanding of the software components we possess. It provides insight into the technology stack, allowing us to assess risks on our own. For example, when the log4j issue arose, we actively investigated it. With an SBOM, we can easily verify the presence of vulnerable components. SBOM aids in identification, but it does not provide a solution. Mitigation measures need to be implemented based on the information it provides.

Ultimately, security is our primary concern. As long as the solutions we use are stable, secure, and maintainable by vendors, the specific technologies they employ are of less importance.

Regarding DORA, our legal department reviews it before it is rolled out. Once I have a clear understanding, I form my own opinion. I don't actively pursue information about it at the moment. Generally, I have reservations about European regulations. Often, things were better regulated in the Netherlands before European involvement. Compromises are frequently made at the European level, and they are not always an improvement.

The adoption of SBOM depends on whether it becomes a means of complying with supply chain management legislation. What are the alternative compliance methods? If SBOM is the only option, adoption will be high. If it is the most expensive route, adoption will be low.

Personally, I don't believe SBOM should be implemented universally. It requires sensible considerations. Some situations may benefit from it, while others may not. Enforcing it through regulations may make it relevant everywhere, leading to unnecessary administrative burdens without added value in all cases. That would be a waste.

If SBOM is already present, then it should be used. For example, when issuing a tender and comparing multiple vendors, security and technology aspects should always be considered. In such cases, we would provide the SBOM.

As for IP, the risks should be manageable. The list of components used is provided, but the specific algorithms or proprietary arrangements implemented on top of those components remain undisclosed. That is still valuable IP. While reverse engineering is possible, revealing too much could jeopardize the confidentiality. When initiating projects and involving two or three parties, we typically start by signing a confidentiality agreement, protecting the information.

There is a concern about the level of detail in SBOM. It is crucial to specify the third-party components and their composition. Otherwise, there is a false sense of security. We might disclose 80%, but the black box, which we have acquired, constitutes the remaining 20%. In that case, the value of the disclosed 80% diminishes significantly without knowledge of the missing 20%. We don't have the complete picture. We know something, but not everything.

The future adoption of SBOM heavily depends on the actions of regulators like DNB and AFM. If they demand SBOM as a risk management measure, its adoption will accelerate. If such demands do not materialize, it's uncertain what will be the catalyst for widespread adoption. In the absence of regulatory pressure, I question whether SBOM will gain significant traction in the near term. It may eventually happen, but in the short to medium term, it remains uncertain.

B.1.6. Summary 6

Demographic Characteristics	**Response**
Stakeholder Group	Software Vendor
Years of experience in the software field	19
Company sector	Digital agency
Job function	Head of Technology
Prior SBOM knowledge	Good
Prior SBOM experience	About to get started

Open source software and frameworks play a crucial role in software development projects, providing time-saving solutions and enabling efficient application development. However, challenges arise when it comes to licensing and IP protection. Strict open source licenses may require disclosing and publishing solutions, which conflicts with preserving proprietary IP and satisfying client expectations. Nevertheless, SBOM has emerged as a standard for gaining transparency into software components used in applications, ensuring security, and facilitating effective risk management.

Last year was probably the most challenging year with all the security threats that came in, but also our legal department stepping forward and saying, "Hey guys, be careful". There are now some open-source matters with very strict licenses. That means we also need to disclose the solution and make that open-source. And for us, that's just a no-go. Customers paid for that. There's our own IP involved. We can't simply publish it like that. And there were also some mistakes made

by developers who, unconsciously, incompetently, or however you want to call it, published parts of the customer's IP as open-source.

A customer hires us because of our expertise in software development. That includes SBOM. It's just a standard to understand what your application consists of. It's the same as when you buy a car, and it often happens that you buy a car and then three months later, a defect is discovered, and the cars have to be recalled, and it needs to be fixed. I'm not going to keep track of that. As a customer of the car, I'm not going to keep track of it. I'll just get a note from my garage saying, "Hey, there's something wrong with your engine. You need to come back." And that's exactly the same thing.

SBOM offers numerous benefits across the software development and maintenance lifecycle. It aids in detecting and addressing security threats, privacy concerns, and overall vulnerabilities. By providing visibility into the technology stack, SBOM enables informed decision-making and proactive measures to mitigate risks. This becomes especially crucial in application maintenance scenarios where third-party software is involved, and organizations may not have complete knowledge of the underlying components. The potential reputational and financial damages resulting from undetected vulnerabilities emphasize the necessity of SBOM adoption.

While implementing SBOM comes with associated costs, including licensing fees for tools, it is essential to consider the value it brings to customers. Rather than focusing on technical details such as hours spent or specific frameworks used, the emphasis should be on delivering value and ensuring the reliability and security of the software solution. Trust and confidence in software vendors are critical, and failing to address vulnerabilities can lead to severe consequences for both the vendor and the client.

Legislation regarding SBOM should prioritize establishing guidelines and requirements rather than prescribing specific tools or methods. This approach allows for flexibility and innovation within the industry while ensuring customer protection. By mandating SBOM adoption, regulators can push software vendors to become more professional and accountable for the solutions they deliver.

Addressing concerns about IP protection, SBOM primarily focuses on providing transparency and insight into software components rather than exposing specific code or proprietary information. It enables understanding the composition of an application, which is essential for risk assessment, but does not inherently jeopardize IP.

One incident that stands out to me is the log4j incident. And solely due to not having the SBOM, I do think that for a period of three to four days, the entire organization was in a frenzy. And it wasn't just the management department, but also the involved architects who were bombarded with questions like, "Is this being used?" and so on. So, you can see that in a very short period of time, a lot of questions start to arise simply because we don't have this information management in order. I believe that we easily spent around 240 hours just dealing with that log4j incident. Yes, it's absurd because it essentially boiled down to SBOM functionality. Calling people, asking if they built this application, and if they know what's included in it. If they did, then we could proceed. Additionally, there were some administrators who were busy contacting all the customers to check if there were any references or indications that it was being used.

Although awareness of SBOM is more prevalent in some countries, such as Germany, it is yet to gain significant attention in others, including the Netherlands. While the Dutch market is known for embracing innovation, the urgency around vulnerabilities and the demand for SBOM have not been widespread. However, proactive clients and organizations responsible for application maintenance should actively inquire about SBOM and encourage its adoption to ensure software reliability.

While the universal adoption of SBOM remains uncertain, individual organizations can take the initiative to implement it within their processes and workflows. This proactive approach can improve transparency, enhance security, and strengthen relationships with clients. For the interviewed organization, SBOM adoption is deemed necessary and is currently being pursued.

In conclusion, SBOM serves as a valuable tool in the software development industry, providing transparency, risk management, and enhanced security. While challenges and skepticism exist, the adoption of SBOM can contribute to a more mature and accountable software industry, benefiting both vendors and customers alike.

B.1.7. Summary 7

Demographic Characteristics	Response
Stakeholder Group	System Integrator
Years of experience in the software field	25
Company sector	Digital development
Job function	Founder, responsible for strategy and security; developer-background
Prior SBOM knowledge	Good
Prior SBOM experience	None

The participant discusses various aspects related to software development and the potential risks and benefits associated with them. One of the main points raised is the reliance on open-source packages and the lack of awareness about their maintenance and security. Developers often use these packages based on trust and popularity without knowing much about the individuals behind them. This presents a risk in terms of potential vulnerabilities and the possibility of unknowingly including malicious code in projects.

Another concern is the SSC, which includes tools and services that require access to the project's code. While most of these tools are safe, there have been instances of supply chain attacks, such as the Codecov incident, where many companies worldwide were affected. The increasing complexity of the software ecosystem and the potential for hacking make such attacks a significant risk.

Implementing a SBOM is seen as a way to gain transparency and understanding of the application's components. It helps ensure that the software being used is trustworthy and allows for better risk assessment and management. Customers may also find it reassuring to know that the development company is making conscious choices about the technologies used and taking security seriously.

Preventing data breaches and ransomware attacks are key motivations for implementing security measures. While there may be discussions about balancing quality and budget constraints, it is crucial to prioritize security and allocate time and resources accordingly. Clear communication with clients about the importance of security measures and their impact on project timelines and budgets is essential.

The level of awareness and importance assigned to these issues can vary among IT managers and companies. Smaller businesses or individuals may be less concerned about implementing security measures, while larger companies that heavily rely on digital processes may have a greater appreciation for the value of such measures.

They also emphasizes the need for continuous improvement and the potential benefits of adopting security practices, such as having an SBOM. While some may view these measures as unnecessary or burdensome, they can provide assurance and trust to clients and may become industry standards in the future.

It is noted that the software development sector is open and accessible, attracting hobbyists and passionate individuals. However, when delivering professional software, certain obligations and considerations come into play. Striking a balance between protecting intellectual property and providing information about the software components used can be challenging.

Developers themselves generally prefer structured and organized work processes, although there can be concerns about who is responsible for implementing security measures and ensuring their completeness and effectiveness.

Overall, they suggest that professional software companies may have fewer risks related to software security, with the primary vulnerabilities lying in other areas such as individual workstations and human error. However, for critical systems and industries like banking, understanding the intricacies of the software components becomes crucial. The importance of software security measures increases with the significance of the software system and its potential impact.

B.1.8. Summary 8

Demographic Characteristics	Response
Stakeholder Group	Software Vendor
Years of experience in the software field	25
Company sector	HR and payroll software development
Job function	CTO
Prior SBOM knowledge	Okay
Prior SBOM experience	None

The movement we are currently undergoing is a shift towards fully embracing SaaS environments. Although we still have some legacy systems running, delivering a reliable SaaS solution to customers allows us to offer more value by eliminating much of the management burden. Customers now expect software providers to ensure rigorous security measures and conduct thorough testing, relieving them of those responsibilities.

While we offer customers the option to perform acceptance tests before updates, none of them actually take advantage of this opportunity. They rely on us to deliver a thoroughly tested application more effectively than they can.

The use of open source components presents a challenge since it's difficult to fully understand their contents. When undergoing application reviews or penetration tests, we have been cautioned about being up to date with all NuGet packages and open-source elements. However, the depth of these components makes it nearly impossible to have complete visibility, posing inherent risks.

The success of adoption relies heavily on the entire industry embracing the concept. Merely claiming that we have implemented it properly won't be sufficient if other vendors and open-source projects do not follow suit. The absence of an industry standard indicates the need for one to ensure the initiative's success.

The primary driving force would be the expectation from customers and environments that it becomes an industry standard. Just as serious companies are expected to have ISO 27001 certification, this expectation may not stem from intrinsic motivation. However, it is likely to be the determining factor.

Our pricing structure is based on specific contractual provisions, and we cannot pass on costs associated with regular maintenance unless we provide additional value that justifies additional charges.

Once it becomes an industry standard and customers bring their IT audits, compliance will be expected. This is a standard practice.

Even as a prominent company, we receive IT audit checklists from customers, asking if we perform specific tests and how we address follow-up actions. Despite our stature, these questions are raised.

The idea of customers taking responsibility for their own supply chain risk management is still distant. We rely on external security companies to guide us and recommend logical steps, leading us towards ISO 27001 compliance.

Legislative measures may not be necessary. ISO 27001, for example, is not a legal requirement. However, as adoption grows and people recognize its benefits, it becomes a common practice. The government does not mandate penetration testing.

While security and compliance practices are partly obligatory, they can be designed to provide tangible benefits. This has been my experience with these processes.

IP can indeed be a concern, and regulations may be required to govern its access. Similar to IC3402, where certain information is not disclosed to the client but only to the accountant for assurance purposes, third-party evaluation could work in this scenario.

An even greater challenge is that many companies lack a comprehensive list of their third-party components. Even with each subsequent acquisition, we struggle to compile such a list. Many software companies are unaware of the full extent of their usage. It becomes an issue of asset management. Additionally, the extensive use of NuGet packages by these third-party components makes it nearly impossible to have complete visibility, as there are thousands of packages involved.

Overall, considering our discussion, I cautiously remain optimistic. However, the success of this initiative heavily depends on adoption and its establishment as an industry standard.

B.1.9. Summary 9

Demographic Characteristics	Response
Stakeholder Group	System Integrator
Years of experience in the software field	20
Company sector	IT consultancy
Job function	Senior System Architect and Delivery Manager, responsible for software engineering, developers and testers
Prior SBOM knowledge	Expert
Prior SBOM experience	Implementing SBOMs for customers

The concept of the SSC can be viewed from different perspectives. On one end of the spectrum, there is open source software with its associated considerations such as free distribution. The challenges in this domain lie in the quality of the delivered product compared to the invested time, emphasizing return on investment. With the advent of cloud technology, outsourcing becomes more prevalent, eliminating the need to purchase hardware and providing ready-made tools and applications. This shift in the SSC also affects how IT departments are structured and managed.

When considering the cloud specifically, one advantage is the enhanced security it offers. Large cloud providers such as Google, Amazon, and Azure employ hundreds or thousands specialized security experts, making their products more secure compared to individual companies with limited security resources. However, it is crucial to have a proper understanding of cloud security within your own organization to avoid potential vulnerabilities and attacks. Therefore, there are advantages and disadvantages to both sides of the SSC equation.

One significant benefit of SBOM is its ability to define and specify what should and should not be delivered. It serves as a checklist to ensure compliance with requirements and contributes to overall maturity. The expertise and experience of the people involved in the process play a vital role in the quality and effectiveness of the SBOM implementation. While SBOMs are commonly used for B2B deliveries, they can also serve as internal documents to ensure quality and facilitate audits.

Standardized formats like CycloneDX are often utilized for SBOMs, similar to the OWASP framework, which acts as a checklist for security-related aspects. These standards provide clarity and allow for a systematic approach. However, it is essential to consider different perspectives and individual preferences when approaching these frameworks. The primary focus of SBOMs lies in ensuring quality, with comprehensive coverage of licensing, tooling, and other relevant aspects.

From a supply chain perspective, SBOMs can significantly contribute to managing and mitigating risks. They enable early identification of vulnerabilities and potential software supply chain attacks, reducing their impact. While customers may not directly pay for an SBOM, trust and reputation are crucial in B2B relationships. Trustworthiness, especially in sectors like finance and banking, plays a significant role in maintaining business relationships and securing long-term partnerships.

The dynamics of trust and reputation have evolved, and relying solely on reputation or name recognition is no longer sufficient. Any security issue, regardless of a company's size or reputation, can have severe consequences. The market now offers more options, allowing for rapid shifts between different providers. Thus, it becomes crucial to ensure the security and reliability of the back-end systems, as even small errors can have significant consequences.

Regarding regulations, there is a dual perspective. While legislation can help address security concerns, it often lags behind technological advancements. Implementing regulations can be challenging due to the varying interests and perspectives involved. It is preferred that industry standards and best practices guide the software supply chain rather than relying solely on legislation. Standards developed by industry professionals who understand the domain have the potential to be more effective and up-to-date than regulatory frameworks.

Considering procurement processes, it would be beneficial for customers to have access to SBOMs during the evaluation phase. Openness and transparency are valued, especially for standard products. However, for highly classified or sensitive software, specific rules and non-disclosure agreements may apply. Intellectual property plays a crucial role in software development, and revealing proprietary information without proper precautions could undermine a company's competitive advantage.

All in all, I am somewhere between neutral and optimistic. I think it is great to have it, but indeed, it also depends on how much effort you put into it. From what, what, how much time it takes to describe everything, how much can be automated. However, I am always very positive about these things when you can automate them right from the beginning. So, when you simply press a button and an SBOM comes out with all the dependencies, everything you have used, and so on, that, in my opinion, is a completely different discussion than having to do everything manually every time.

B.1.10. Summary 10

Demographic Characteristics	Response
Stakeholder Group	OSS Developer
Years of experience in the software field	15-20
Primary contributions	Well-known SBOM evaluation repository and feature flags repository
Prior SBOM knowledge	Expert
Prior SBOM experience	Working on the quality of SBOMs

The participant expresses their contributions to two main projects: a well-known SBOM repository and the open feature project focused on feature flags. They believe in the ethical value of working on open source projects and promoting the sharing of useful resources for the betterment of society.

Regarding SBOMs, they emphasize the importance of accurate and specific information about software components and their versions. They highlight the need for canonicalization and precision in SBOMs, as many currently lack specificity due to being generated by inadequate or immature tools.

The individual explains that multiple SBOMs may exist for a single project, particularly when components are bundled. Each bundling step may require its own SBOM, creating challenges in managing the data effectively.

They note that although the requirement for SBOMs is growing, some organizations generate low-quality SBOMs merely to fulfill contractual obligations without fully comprehending their value. There is a need to educate both developers and government entities about the significance and utilization of SBOMs.

The individual sees great potential in the data provided by SBOMs, particularly in assessing usage and the relative risk profile of applications. They consider SBOMs to be a valuable data source that is easier to capture and use in the present rather than generating it retrospectively. Additionally, having license information within SBOMs is seen as beneficial.

The misalignment of incentives between businesses, which benefit from SBOMs, and open source developers, who may not have strong incentives to produce them, is highlighted. This misalignment creates tension within the open source community, as developers face additional work without direct benefits. The reliance on open source and the commercial interests surrounding it present unsolved problems in the context of SBOMs.

The individual views the Executive Order in the US as a positive step, recognizing the need to control the software supply chain, particularly in defense applications. They believe the government's purchasing power can drive meaningful change in the industry.

The importance of tooling is emphasized, with ongoing efforts to address the quality of SBOMs and the fragmentation in the space due to various programming languages and deployment mechanisms. The lack of a compelling solution for SBOM storage is mentioned, presenting an opportunity for innovation in that area.

The individual suggests that SBOMs should be generated during the development process by open source developers themselves to ensure their usefulness. Retroactively trying to identify software components without SBOMs is challenging, especially with techniques like minification in JavaScript, which may obscure original variable names.

They mention other tools like Syft that can build dependency graphs of Docker containers, but acknowledge their imperfections and technical limitations.

Overall, the individual maintains an optimistic outlook on SBOMs, highlighting their potential in understanding software composition at scale, particularly in enterprise contexts. Monitoring the health of packages and gaining insights into their future trajectory is seen as a fascinating aspect of SBOMs.

B.1.11. Summary 11

Demographic Characteristics	Response
Stakeholder Group	B2B Customer
Years of experience in the software field	17
Company sector	Water sector (critical)
Job function	CISO and Enterprise Architect
Prior SBOM knowledge	Good
Prior SBOM experience	None

The interviewee discusses various aspects related to cybersecurity risks and the importance of implementing measures to mitigate these risks. They highlight the challenges faced when dealing with uncertain situations, such as a supplier refusing to provide necessary information. This lack of transparency forces organizations to find alternative solutions, which can be time-consuming and inefficient.

Understanding vulnerabilities and taking appropriate measures to address them is crucial. The interviewee emphasizes the significance of knowing where vulnerabilities exist and which actions should be taken to mitigate them. Without this knowledge, organizations remain blind to potential risks and are unable to implement effective security measures.

The primary motivation is security. They recognize the broad spectrum of cybersecurity risks, encompassing data integrity and availability, and emphasize the need to protect against such threats. However, they find it challenging to allocate more resources to software investments, suggesting that mandatory regulations might be necessary. By making security measures obligatory, organizations would be more inclined to allocate funds as vendors would charge for compliance. Although this would increase costs, the interviewee believes it would be a necessary step.

Reputation is identified as a significant concern, but the interviewee notes that past instances of data breaches and privacy law violations have had minimal long-term impact on a company's revenue. This observation indicates that reputation damage may not be a strong deterrent for some organizations, potentially underscoring the need for stricter regulations.

Regarding large suppliers, the interviewee mentions the influence they wield within the supply chain. They explain that major suppliers have the power to exert pressure, particularly when working with government entities. This concentration of power highlights the importance of addressing market dynamics and the need for fair practices.

They express caution regarding excessive reliance on legislation for cybersecurity. They argue against imposing specific measures without considering the knowledge and expertise of those involved. The interviewee believes that blanket regulations might not be suitable for all organizations and that different measures could be essential for different parties. Striking a balance between prescribing measures and allowing room for innovation is crucial.

The interviewee suggests that having a clear understanding of the supply chain is vital. By knowing who is involved and responsible for each component, organizations can track the usage of their software. This visibility can help demonstrate compliance and accountability.

They believe that technical concerns regarding SBOM adoption may be overstated. Although some may threaten to discontinue their work, most individuals are passionate about their projects and would likely continue despite the regulatory requirements. However, they acknowledge the challenge of accurately detailing an SBOM, especially starting with open-source components. Without comprehensive information on the origins and composition of open-source software, vulnerabilities may go unnoticed even when using larger vendors.

The participant highlights the need for a broader understanding of the software supply chain. While achieving complete control and security is unlikely, gaining a more comprehensive view of the components involved would already be beneficial. Recent incidents like Log4j and SolarWinds have underscored the importance of knowing the exact composition of software. Organizations are increasingly demanding transparency from suppliers to ensure a thorough understanding of the underlying technology.

In conclusion, the interviewee is optimistic about the potential of SBOM and similar initiatives to drive discussions and prompt action in the cybersecurity domain. They acknowledge that the exact form of SBOM implementation remains uncertain but believe that the discourse it generates will lead to some form of comparable solution. Regardless of the specific outcome, the interviewee believes that progress will be made in improving transparency and security in the SSC.

B.1.12. Summary 12

Demographic Characteristics	Response
Stakeholder Group	OSS Developer
Years of experience in the software field	15
Primary contributions	Primary dev of MFA App with 30000+ users
Prior SBOM knowledge	Okay
Prior SBOM experience	None

The person identifies two main risks associated with SBOM. The first risk relates to the use of open-source dependencies, which are often maintained by hobbyists or non-commercial entities. This reliance on unpaid individuals for maintenance can lead to unresolved bugs or issues that are difficult to fix since the code is not owned by the user. This becomes a concern when distributing software to a wider audience who relies on these dependencies. The second risk mentioned is related to security. The person highlights that security issues in open-source software or compromised dependencies have been observed in the past. Malicious code or hacking incidents can potentially compromise the entire chain of software using those dependencies.

The biggest benefit of SBOM, according to the person, is the ability to proactively address security concerns. By having a clear understanding of the software's dependencies and the components involved, organizations can quickly identify vulnerabilities or necessary updates. This information can help them take action and mitigate risks. Additionally, the person suggests that SBOM could potentially assist with copyright and IP concerns by clearly identifying the code's authors and copyright details, thus helping prevent infringement.

Regarding the significance of SBOM, the person believes that adopting it would be important for exposure purposes. By creating an SBOM for their software, other parties are more likely to reciprocate and include their software in their own SBOMs. This increased visibility can be beneficial. However, the person indicates that in terms of security, they already utilize dependency managers to monitor vulnerabilities, so SBOMs might not add substantial value in that regard. Nevertheless, the person considers SBOM implementation to be relatively easy and sees little reason not to adopt it.

One observation made by the person is that the SBOMs they encountered only include direct dependencies and not the dependencies of the dependencies. This limitation makes it inconvenient for users since they would have to acquire additional SBOMs to obtain a comprehensive view of the dependencies. However, if software users or open-source developers are proactive in addressing issues, having a recursive SBOM can provide them with valuable information, enabling them to take action without relying on all the suppliers in the chain.

The person suggests that if SBOMs become mandatory through laws or regulations, it could facilitate implementation and increase awareness among software developers. However, they express skepticism about universal compliance, as some open-source developers may not have the inclination or time to adhere to such requirements, even if mandated by law.

While the person does not believe that implementing SBOMs would cause significant hindrances, they acknowledge that understanding the implementation process and possessing the necessary knowledge could pose challenges, especially for less experienced software engineers or those unfamiliar with SBOMs. However, for individuals knowledgeable in implementation, they foresee minimal hindrance.

Regarding procurement processes, the person suggests that accessing SBOMs could aid in risk assessments for business-to-business interactions. However, they note that organizations must be experienced enough to evaluate SBOMs effectively. They also mention that for organizations seeking to exclusively use software from certain regions, SBOMs can assist in identifying the origin of the software, such as determining if software development involves individuals from specific countries.

The person highlights the difficulty of freely sharing comprehensive SBOMs, particularly for confidential software or cases where source code confidentiality is critical. There may be concerns about exposing unique software features to potential competitors or unauthorized use.

Lastly, the person shares their experience with CVEs and believes that even with SBOMs, challenges regarding interpretation and impact assessment remain. They express optimism about the potential benefits of SBOMs but acknowledge the complexity of universal adoption, suggesting that it could be the start of a solution that evolves into a less complex alternative in the future.

B.1.13. Summary 13

Demographic Characteristics	Response
Stakeholder Group	OSS Developer
Years of experience in the software field	10
Primary contributions	One of the main contributors to a very well-known tool that produces and consumes SBOMs
Prior SBOM knowledge	Expert
Prior SBOM experience	Contributing for well over a year

In their statement, the individual mentions their contributions to open source projects such as Dependency Track and Key Clock, as well as their involvement in developing tooling and libraries related to SBOM generation for language ecosystems. Their main interest lies in software security, and they have encountered limitations in existing SBOM tooling, which motivated them to contribute and fix issues in these sub-projects.

They highlight the risks associated with including open source libraries with vulnerabilities or incompatible licenses in software. The main benefit they see in using SBOM is transparency, as it provides developers and customers with a clear view of the open source components used in software. Security analysis is an important aspect derived from this transparency.

Regarding their incentives and motivations for contributing to open source, they mention a desire for recognition and the opportunity to contribute to the software industry. Initially, their motivation was driven by personal needs to fix bugs, but they also realized that contributing to open source projects could enhance their skills and provide recognition in their professional career.

They believe that transparency is essential for open source development to encourage adoption and usage of the software. They emphasize that waiting until the entire supply chain implements SBOM may lead to a loss of accuracy in the generated SBOMs. Starting from the first open source developer would ensure the completeness of the SBOMs. While they don't advocate for mandating SBOM production by open source developers, they suggest that providing SBOMs could be a professional proof for those who want their libraries to be used by government or major companies.

In terms of adoption, they acknowledge the need for some kind of regulation or incentive to drive widespread SBOM adoption. While they don't support mandatory SBOM production for all open source software, they believe that regulatory or compliance incentives, like the US executive order, can lead to significant adoption.

To address potential IP concerns, they propose private repositories where software suppliers can publish their SBOMs, accessible only to authorized individuals who have signed NDAs.

Technical challenges they identify include the reliability of vulnerability sources and the management of duplicate vulnerabilities, which can generate noise and hinder SBOM adoption. They also mention the variety of SBOM formats (such as Cyclone DX and SPDX) and the need for proper tooling to generate and assess the quality of SBOMs and perform vulnerability analysis.

Regarding the VEX, they explain that it is specific to each company and software. They mention that creating a VEX requires manual analysis and contextual understanding, as it is not an automatic tool.

They make a distinction between the copy-pasting of code and the use of SBOMs and code checkers or scanners. They emphasize the importance of relying on other tools, such as SBOMs and VEX, in managing vulnerabilities and assessing source code.

Lastly, they express optimism about the adoption of SBOMs, as they observe the emergence of new SBOM generation tools and increasing discussions about SBOMs in IT conferences. They believe that with time, SBOM adoption will become more widespread.

B.1.14. Summary 14

Software composition analysis (SCA) is a field that aims to create an inventory or "shopping list" of all the software artifacts used in a software system. This includes source code, packages, and binaries. The European Union's CRA highlights the importance of eliminating vulnerabilities in software, but achieving this goal is challenging. Not every vulnerability is exploitable in every context, so it is essential for software users to assess the risks within their specific context.

When evaluating open-source software, various risks need to be considered. One of the primary risks is the presence of known vulnerabilities that can be easily exploited, making large organizations potential targets. Additionally, there is a risk associated with licenses that may affect software usage, such as intellectual property rights. Many companies lack visibility into these license issues, which can lead to legal complications. Keeping the software up to date is also crucial, as outdated

Demographic Characteristics	Response
Stakeholder Group	Software Vendor
Years of experience in the software field	19
Company sector	Digital agency
Job function	Head of Technology
Prior SBOM knowledge	Expert
Prior SBOM experience	Developed an own produce and consume SBOM tool

packages are more prone to issues and updating them can be a time-consuming task. Another aspect to consider is the active involvement of the open-source community behind a package and whether it is officially managed or simply copied and pasted. These are the risks taken into account when evaluating open-source software.

Regarding the creation of a SBOM for open-source projects, it may not be practical because these projects already describe their dependencies in a manifest. The manifest can be used by upstream software to include those packages. However, when another software piece uses the same package, it can modify the build configuration, resulting in significant deviations from the original SBOM of the project. Therefore, an SBOM should be created at the product level, encompassing all the different open-source components considered together. It is not a matter of merging SBOMs from individual packages into one. Instead, it should be generated at the compilation level, as CycloneDX does by integrating with various build platforms. The compiler knows which packages it imports and can provide an accurate SBOM.

The main advantage of SBOMs is the visibility they provide, not only of the software components but also of the underlying risks. However, there is still much work to be done in terms of establishing industry standards and addressing data compatibility issues between different formats.

SBOMs are becoming a regulatory requirement in the United States and are expected to be adopted in the European Union and other regions. For companies, the cost of implementing SBOM practices should be considered as an operational expense rather than a one-time capital expense. SBOMs can save time, especially when automated through software composition analysis tools. While 40% of large enterprises already use such tools, broader adoption is still necessary. However, the adoption of software composition analysis tools does not necessarily mean embracing the concept of SBOMs. Both aspects should be seen as separate but complementary.

Ideally, the software industry should have embraced SBOM practices voluntarily, but now governments are intervening to address the industry's shortcomings by imposing regulations. This regulatory approach can contribute to the maturity of the software industry in terms of vulnerability management and overall transparency.

Challenges in implementing SBOMs include vulnerability management and data integration. Vulnerability data from sources like the National Vulnerability Database (NVD) does not always align with package data provided by developers, as there is no unique identifier that links the two. Software composition analysis tools address this problem differently. Additionally, many vulnerabilities reported in the NVD may not be exploitable, as certain code paths may not be triggered. Thus, distinguishing between critical vulnerabilities and those that can be accepted is crucial. This challenge highlights the need for clearer criteria to determine which vulnerabilities require action and which can be accepted based on the specific context.

Overall, SBOMs serve as a foundational step toward understanding software components, managing risks, and advancing the maturity of the software industry.

B.1.15. Summary 15

Demographic Characteristics	Response
Stakeholder Group	OSS Developer
Years of experience in the software field	8
Primary contributions	Bible app, games, text editor
Prior SBOM knowledge	Okay
Prior SBOM experience	None

The person expresses their enthusiasm for open-source apps, as it allows them to make changes if they feel something is not working well. They also mention that in their work, they use a lot of tooling, and when they fix something, they have the ideology of upstreaming it so that others can benefit. They believe that if they encounter an issue, it's likely that others will also face the same problem.

They point out the challenge of checking all the layers of code in projects for security issues. It's practically impossible to review every line of code for potential malicious code or backdoors, especially in popular projects. They emphasize the importance of ensuring software security but acknowledge the difficulty of achieving it.

Maintainability is another crucial aspect for them. They prefer using projects as close to the original source as possible and avoid using wrappers or outdated dependencies that may cause compatibility issues.

They view the biggest benefit as SBOM being a standardized format to represent dependencies from various package managers. The advantage of SBOM is that it enables the development of tooling that can understand and translate the format without needing to comprehend all package managers individually. This allows for fast scanning of dependencies for known vulnerabilities.

However, they mention that the decision to adopt SBOM depends on the time and effort it requires. They would be more inclined to use it if the process could be automated. Integration with widely used package managers is also essential for seamless adoption.

They believe that the usefulness of SBOM lies in the availability of user-friendly tooling that can check SBOMs for vulnerabilities quickly. However, they note that the SBOM format itself contains a vast amount of data that might not be easily understandable for non-developers, making its immediate usefulness questionable.

They discuss the responsibility of ensuring software security and suggest that if customers demand SBOMs before purchasing software, it would become the responsibility of suppliers to provide them. However, they also mention that there are other methods, such as penetration testing, to assess software security, and not all customers might automatically demand SBOMs.

The person suggests that customers could benefit from reviewing an SBOM before purchasing software to conduct better risk assessments and make informed decisions about suppliers. They also note that providing an SBOM does not necessarily mean disclosing the source code, but rather indicating the components and tools used in the application, providing insights into its structure and methods.

Finally, the person expresses optimism about the adoption of SBOM, especially if it becomes integrated into popular package managers. Once SBOM usage becomes widespread, they believe it will be more commonly utilized.

B.1.16. Summary 16

Demographic Characteristics	**Response**
Stakeholder Group	OSS Developer
Years of experience in the software field	25
Primary contributions	One of the Leads of well-known SBOM format
Prior SBOM knowledge	Expert
Prior SBOM experience	Actively working on SBOM related things

The interview participant initially started contributing to SBOM format out of personal necessity in their role leading a development team at a government organization in Australia. They faced the challenge of managing numerous projects that would enter maintenance mode once the project budget dried up, resulting in over 300 items requiring their attention. To gain visibility into the state of these projects, they started using SBOMs internally, without initially involving the security team, to assess the severity and location of potential vulnerabilities.

The interview participant emphasized the importance of SBOMs in sectors like smart cities, where physical devices are integrated into infrastructure with potential implications for public services, such as town water supply. However, these operational technology systems often overlook the cybersecurity risks associated with software components, focusing more on regular equipment maintenance.

One of the key benefits of SBOMs is providing organizations with a foundational understanding of their assets, addressing the challenge of not knowing what they have. This visibility enables different teams within an organization, such as the legal team for open-source software license compliance or the security team for known vulnerabilities, to utilize SBOMs effectively. Additionally, SBOMs can be used to verify the software components included in products purchased from external vendors.

The primary advantage of SBOMs lies in their ability to provide visibility. By generating SBOMs for all their assets, organizations can identify and address problems that were previously unknown. This visibility enables them to present concrete data to management, demonstrating the need for funding to tackle identified issues.

When considering the scope of SBOMs within an organization, it is unlikely to have a single SBOM covering the entire organization. Instead, it is more practical to have an SBOM for each product or system, with potential sub-SBOMs for specific components within those systems. Integration with existing Configuration Management Databases (CMDBs) can streamline asset management by incorporating SBOM data alongside other IT assets.

While over 100,000 organizations currently use SBOMs, this represents only a fraction of software-building entities worldwide, indicating that SBOM adoption is not yet widespread.

For open-source software developers, SBOMs may not be necessary in most cases. Distribution of packages typically does not include third-party components, rendering SBOMs mostly empty. The relevance of SBOMs arises when others use the software and additional dependencies are introduced during the build process.

The incentives for working with SBOMs include their ease of generation at build time, the ability to choose how to utilize the data, and the potential for gradual process enhancement as software development practices evolve.

Regarding suppliers providing software to other parties, the primary driver for SBOM adoption is often government requirements. Some industries, such as financial services, have stricter procurement standards, leading to higher expectations for SBOMs. However, in most cases, the incentive stems from federal government regulations or niche industry requirements.

The main challenge in SBOM adoption lies in the lack of historical data formats to support the associated use cases. Organizations may start generating SBOMs for their products but encounter issues when customers utilize the data. These issues arise due to the absence of a standardized data format to capture relevant information effectively.

The participant expresses their thoughts on SBOMs and raises several points throughout their discussion. They mention that there might be instances where reported vulnerabilities in SBOMs turn out to be false positives. This could be due to the issues already being fixed or not exploitable in the composed software. They believe that suppliers should still assess these vulnerabilities, even if they are false positives, as it helps shed light on the situation.

They suggests that copy-pasting issues are more of a process problem than an SBOM problem. They explain that while SBOMs can capture information about code snippets being copied, it is the process that needs improvement to accurately resolve packages. They compare the lifecycle of software development to the lifecycle of SBOMs, emphasizing the need to record information about copied code snippets.

In terms of risk assessment, the author mentions the importance of evaluating risks, especially in industries where software has a significant impact, such as medical devices or emergency response systems. They note that certain industries, including medical devices and critical infrastructure, are starting to require SBOMs. However, they point out that there isn't much liability-related activity associated with SBOMs in these areas yet.

The participant believes that initially, SBOM adoption may be more of a checkbox activity, with organizations needing time to figure out how to effectively use SBOMs and develop systems to consume them. They suggest that many organizations may not be ready for SBOM implementation at this stage.

When it comes to open-source software, the author argues against shifting the responsibility for secure software from suppliers to open-source developers. They highlight that open-source developers are often volunteers and shouldn't be burdened with additional responsibilities. They also mention that open-source developers take pride in their work and may voluntarily create SBOMs as a matter of professional pride. However, they note that not all supply chain issues in open-source software require shipping an SBOM with the component itself.

The participant addresses concerns about IP and visibility. They dismiss concerns about IP, stating that reverse engineering has existed for a long time, and knowing which libraries are used can already be determined easily. They highlight the importance of providing visibility into the usage of certain components and the need for context. They believe that if a federal government-level SBOM clearing house can provide such information, it would be beneficial. This visibility could help direct funding upstream to critical open-source projects.

In conclusion, the interviewee is neutral since they suggest that there is an overemphasis on SBOMs as the technical solution, rather than focusing on the underlying transparency problem. They believe that the real issue lies in the lack of transparency and advocate for addressing the actual problem rather than solely relying on SBOMs.

B.2. Ordinal Preference Ranking: Results

Table B.1: Ranking Scores of Statements

Participant	Ranking Scores of Statements											
	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	S11	S12
P1	3	-1	4	0	5	1	-3	-4	-4	5	-1	-3
P2	4	-3	4	1	2	4	-4	-2	-1	2	-2	-3
P3	4	0	0	5	5	4	-5	-4	-5	3	0	0
P4	4	3	4	2	5	2	-1	-4	-4	4	0	1
P5	4	-1	2	0	1	2	-4	-4	-2	2	1	0
P6	4	-2	5	-3	3	4	-5	-5	-3	3	0	-1
P7	3	2	4	2	5	4	-3	-3	-3	2	0	0
P8	4	-1	5	1	-1	2	-4	-4	-1	1	0	0
P9	4	-1	1	3	5	2	-1	-4	2	-1	-3	-1
P10	-1	0	4	0	5	1	-4	-3	-2	1	0	0
P11	4	1	3	-3	3	1	-5	-4	-2	3	1	1
P12	5	2	3	0	1	4	-4	-4	0	2	0	-1
P13	4	-1	4	2	5	3	0	-4	-3	3	0	0
P14	4	4	2	3	-2	0	-4	0	0	0	0	-3
P15	5	-1	4	3	0	5	-5	-5	1	3	-3	0
P16	3	0	3	5	5	0	0	-3	-2	3	0	0

C

Appendix: Data Analysis

C.1. Main 3: Thematic Analysis

Table C.1: Expected benefits of SBOM

Label	B2B	SV	SI	OS
Transparency	P2, P3, P5	P4, P6, P14	P1, P7, P9	P10, P12, P13, P16
Risk assessment customer	P5	–	P1	P10, P15
Managing risks	P2, P3, P5, P11	P4, P6, P14	P1, P7	P10, P12, P13, P16
License management	–	P6	P9	P12, P16

Table C.2: Biggest incentives for SBOM

Label	B2B	SV	SI	OS
Regulatory compliance	P5	P14	P1	P10, P12, P16
Security & continuity	P2, P3, P5, P11	P4	P7	P16
Quality	–	P4, P6	P1, P7, P9	–
Reputation & expectation	–	P6, P8	P1, P7, P9	P15, P16
Financial	P3	P6, P14	–	P10
Ethical & ideology	–	–	–	P10, P15
Time & effort	P3	–	P1, P7	P10, P12, P15
Recognition & exposure	–	–	–	P12, P13, P16
Tooling & automation	–	P4, P14	P1, P9	P10, P12, P13, P15

Table C.3: Biggest concerns for SBOM

Label	B2B	SV	SI	OS
Copy-pasting	–	–	P1	–
Vulnerabilities (assessment)	P2	P14	P9	P12, P16
Tooling	–	–	-	P10, P13
ROI	P2	–	P9	–
Governance	P3	–	P7	–
Detailing & layers	P5, P11	P8	–	P10, P12, P13
IP	–	P6	–	–
Overhead SMEs	P3	P6	P9	–
Vulnerability databases	–	P14	–	P13
Storage	–	–	–	P10
Formats	–	P14	–	P13

C.2. Specific Semi-structured Questions

Table C.4: Biggest risks in the SSC

Label	B2B	SV	SI	OS
Compromised OS	P2, P5	–	P1, P7	P12, P13, P15
License violation	–	P6	–	P16
Freshness risk	–	P14	–	–
Maintenance OS	–	P14	P7	P12, P15
Unknown (un)knowns	P3, P11	P8, P14	–	P15, P16
Slow response	P3	–	–	P16
Staff reduction (SaaS)	–	–	P9	–

Table C.5: Willingness to pay

Label	B2B	SV	SI	OS
Yes	P2, P3, P5	–	–	–
Security subjectivity	P2	–	–	–
Depends application	P5	–	–	–
Indirectly no choice	P11	–	–	–

Table C.6: Preemptive SBOMs

Label	B2B	SV	SI	OS
Yes	P2, P3, P5, P11	P4, P8, P14	P1, P9	P12, P13, P15
Impossible for most	P11	P6	P7, P9	–

Table C.7: Intellectual property

Label	B2B	SV	SI	OS
No issue	P3, P5, P11	P6	P9	P16
Issue	P2	P4, P8, P14	P9	P12, P13
NDAs	P5	–	P1, P9	P13
Reversed engineering	P5	–	–	P16

Table C.8: Laws and regulations

Label	B2B	SV	SI	OS
Critical for adoption	P2, P3, P11	P4, P14	P1, P7	P10, P12, P13, P16
Only compliance	P2, P3	P8	P7	P10, P16
Too little expertise to mandate	P2	–	–	P12
Familiar with relevant regulations	P2, P3, P11	P14	–	P10
Critical in general	P5	P6, P14	P9	–
General regulatory framework	P11	P6, P14	–	–

Table C.9: Finding vulnerabilities

Label	B2B	SV	SI	OS
Outsourced	P2, P5	P4, P6, P8	–	–
Many resources	P2, P3	P8, P14	P1, P7, P9	–
Too time-consuming	–	–	P1, P7	P15
Responsibility more to supplier	P2	P6, P8	P9	–
Log4j example	P3, P5, P11	P6, P14	P9	P12
Trusting well-known companies/packages	P3	P4, P8	P9	P12, P15
SBOM scanning more thorough	P2	P6	–	–

Table C.10: Trust and reputation

Label	B2B	SV	SI	OS
Really important	P3, P5	P4, P6, P8	P1, P7, P9	–
Increased vulnerabilities, less trust	–	–	P1	–
Good SBOMs, more trust	–	–	P1, P7	–
Individuals over brands	P2	–	P1	–
Trust equals more revenue	–	P4	P9	–
Little consequences	P11	–	–	–

Table C.11: Trust and reputation

Label	B2B	SV	SI	OS
Non / not seen	P2, P3, P5	P4, P6, P8	P1, P7	P12, P13, P15
Picking up	P11	P14	P9	P10, P13, P16

Table C.12: SBOM sentiment

Label	B2B	SV	SI	OS
Negative	–	–	–	–
Sceptical	P2, P5	P6	P1	–
Neutral	–	–	P7	P16
Optimistic	P3, P11	P6, P8	P9	P10, P12, P13, P15
Really positive	–	P4, P14	P1	–

C.3. Generally Interesting Findings from Thematic Analysis

Table C.13: SBOM sentiment

Label	B2B	SV	SI	OS
Limited understanding	P2, P3	P6, P8	P1, P7	P10, P12, P13, P15, P16
SBOM selection	P5, P11	–	P7, P9	P10, P12, P16
Internal use	–	P4, P6, P14	P1, P7, P9	P16
Unattainable perfection	P3, P11	P4, P6, P14	P9	–
Evolving SBOM	P11	P14	P9	P10, P16
Ongoing analysis challenges	P3	–	–	P10, P12, P13
Copy-Paste unrelated	–	P14	P9	P12, P16
Asset management	P3	P8	–	P16
SBOM certification	P3	P8	–	–
Dynamic SBOM	–	P14	–	P16

D

Appendix: Data Validation

D.1. Summary of Data Validation with Field Expert

From their perspective, the expert considers vulnerability management to be the most crucial use case of SBOM. Their understanding of software bill of materials is a straightforward one: it is simply a list of software components present in an application. However, the challenge lies in determining the extent to which an SBOM should go, including how many dependencies it should encompass. This remains unclear, although some guidelines have been established by the White House and the NTIA, outlining minimum requirements. Nevertheless, there are complexities, particularly when dealing with older embedded systems or OT systems. Extracting an accurate SBOM from such systems proves to be quite difficult. While modern applications, such as those utilizing virtualization and Docker, are relatively straightforward to generate an SBOM for, firmware and closed-source binaries pose greater challenges. The concept is simple, a list of ingredients, but the actual compilation of that list remains complex.

The expert highlights that compliance management is the most significant use case for organizations. Compliance is mandated by US government legislation, and similar legislation is on the horizon in Europe. Additionally, the recent log4j vulnerability brought heightened attention to SBOMs as a potential silver bullet for addressing such issues in the future. However, implementing SBOMs poses its own challenges. Many organizations already find asset management to be an overwhelming task, and the prospect of monitoring an SBOM that changes with every patch raises interesting questions.

The expert has encountered two perspectives on the matter of using SBOMs internally. In a workshop conducted, participants were given two SBOMs; one for a Docker container with a Flask web server and another for the same Docker container without the Flask web server. They were then asked to compare the two SBOMs. However, the task proved to be impractical when printed on paper, resulting in approximately 30 pages of A4-sized documents per SBOM. Even for such simple software, the number of dependencies to be compared made manual comparison infeasible. Thus, the use of tooling becomes necessary. In another workshop held earlier last year, the discussion revolved around simulating the log4j scenario. When playing the role of software vendors, there was a consensus that SBOMs were useful for identifying vulnerabilities such as log4j or library-related issues. Informing customers about these vulnerabilities was considered feasible. On the other hand, among software consumers, there was significant divergence of opinion. Some expressed a desire to obtain the SBOM themselves, emphasizing the principle of trust but verify to independently assess the vendor's examination. Others, including the expert, were less inclined to receive the SBOM and instead focused on receiving clear communication from the vendor about the existence of vulnerabilities and prompt remediation. Whether an SBOM was used in the process mattered less as long as swift and accurate information was provided. This ongoing debate is prevalent in many organizations, highlighting different perspectives on the matter. It ultimately comes down to individual preferences and priorities. The expert is interested to know if the research encountered similar viewpoints.

The expert believes that in the future, and even currently, having a compliance management system that includes SBOMs can serve as a seal of trust and maturity for software vendors who can produce high-quality SBOMs. Therefore, organizations should prioritize assessing their vendors' capability to produce SBOMs and the methods by which they provide them. The expert suggests making agreements with vendors, and if necessary, establishing sector-wide practices to ensure vendors are challenged to meet the SBOM requirement. This, the expert believes, is the crucial step for organizations. If there is a need, organizations should be able to request SBOMs from vendors and perform checks when vulnerabilities arise, ensuring the SBOMs are examined and relevant information is shared. This step is emphasized in the CRA, which states that vendors must possess SBOMs. However, a challenge encountered with SBOMs is the assumption that the landscape upon which SBOMs are based is standardized and clear, which is not the case. For instance, the Common

Platform Enumeration (CPE) is a significant problem as it can be interpreted differently by different parties, making it challenging for SBOMs to accurately extract vulnerabilities. An example was given involving OpenSSL, where searching for vulnerabilities using different combinations of CPE numbers resulted in varying numbers of vulnerabilities. This is due to the lack of standardization in filling out CPE numbers used by SBOMs, leading to potentially false information. Additionally, generating consistent hashes for signaling purposes, which are necessary for SBOMs, is also problematic and results in inconsistencies. These issues are specific to security and become even more complex when dealing with firmware, as identifying libraries within firmware can be exceptionally challenging. The process of obtaining accurate information for SBOMs is currently labor-intensive and involves multiple parties working towards achieving a more organized approach.

Regarding SBOMs as a compliance or check-box measure, the expert sees the inclusion of VEX as an interesting addition. VEX addresses a problem faced by SBOMs in vulnerability management. It allows for indicating whether a library includes potentially vulnerable functions or not. This standardized framework enables tracking of whether a library is affected, unaffected, or fixed. However, the challenge lies in the labor-intensive nature of implementing VEX. The expert spoke with individuals working on this in American startups who mentioned the need for full-time data analysts to integrate information from advisories, which often come in PDF or text formats. The analysts have to create parsers and convert the data into a suitable format for their database and subsequent use in generating SBOMs for clients. While this process may seem outdated, it currently remains the approach taken.

There are indeed benefits to be found in SBOMs for OT, as the landscape tends to change at a slower pace. The current challenge lies in generating SBOMs for older legacy devices, where it becomes difficult to identify the appropriate libraries. Although including firmware can be attempted, it often yields insufficient information. However, for future systems, SBOMs can be valuable since the OT landscape undergoes slower changes, with patches implemented over years rather than weeks. The expert sees potential value in SBOMs for OT in such scenarios.

The CRA explicitly mentions SBOMs as a requirement for organizations. It applies to producers of information systems, categorizing them based on criticality levels. Both critical and non-critical systems are mandated to have an SBOM. Whether it pertains to software, firmware, or hardware, a comprehensive SBOM must be created. Additionally, the CRA emphasizes the need to identify vulnerabilities within the SBOMs of these products.

One of the hindrances to adoption, in the expert's view, is simply people's lack of effort. It's a common occurrence with such matters; security, for instance, was often an afterthought. Implementing SBOMs is seen as additional work and acquiring the necessary tooling presents a valid argument against it. The workload should not be underestimated. In discussions with an organization, it was revealed that they had a team of 60 people involved, albeit not full-time. It affected around ten departments, with a project team of five individuals. For larger organizations, the scale becomes significant. It is understandable that people question whether it is truly necessary. However, given the state of software today, the need is indeed pressing. These conflicting interests arise between security, effective asset management, and maintaining quality on one hand, and the concerns of cost, time, and resources on the other.

The expert finds it intriguing that determining the specific contents of an SBOM remains challenging. While there are requirements in place, they are quite minimal. At the recent s4 conference, various tools were assessed in terms of what they generate and how they handle different applications. However, the expert doubts whether legislators can provide valuable insights on this matter. It is advisable to focus on using state-of-the-art terminology in SBOMs to avoid being tied down by the ongoing changes. Tooling is evolving rapidly, with numerous small companies striving to improve SBOM practices. Therefore, it is suggested to allow the current developments to unfold and keep the requirements broad, emphasizing the need for an SBOM. While some requirements can be specified, it is important to let parties drive the depth of implementation. Imposing rigid regulations may lead to impractical outcomes.

The expert believes that SMEs will struggle to implement SBOM effectively in the coming year. From the perspective of software vendors, it should be manageable, especially for open-source developers who are accustomed to such practices. However, on the consumer side, it is unlikely that organizations can handle SBOM processing internally. They can establish agreements with suppliers to provide SBOMs for the products they acquire and timely information regarding vulnerabilities. SMEs are generally ill-equipped to process SBOMs and perform thorough checks themselves. Supplier and supply chain management pose significant challenges, requiring considerable time and expertise. Given the complexity and lack of adequate tools and knowledge, managing SBOMs is not a high priority for most SMEs. The expert hopes for a system where suppliers have well-established practices and can provide timely information, relieving SMEs from the burden. While SMEs should be aware of SBOMs and engage in discussions with their suppliers, bulk processing of SBOMs is beyond their capabilities.

The expert acknowledges the significant effort required in establishing the governance structure for effective SBOM adoption. Processing SBOMs, including their acquisition and distribution, entails engaging with various stakeholders, including legal departments and other parties within the organization. The expert encountered a dedicated project team consisting of five individuals solely responsible for SBOM governance. Implementing such a structure within an organization is challenging and time-consuming. Even the process of requesting SBOMs can pose difficulties. Therefore, both vendors and consumers are likely to encounter challenges in navigating the complexities of SBOM governance.