Charting the Path to SBOM Adoption

A Business Stakeholder-Centric Approach

Kloeg, Berend; Ding, Aaron Yi; Pellegrom, Sjoerd; Zhauniarovich, Yury

DOI
10.1145/3634737.3637659

Publication date
2024

Document Version
Final published version

Published in
ASIA CCS '24

Charting the Path to SBOM Adoption: A Business Stakeholder-Centric Approach

Berend Kloeg*
Northwave Cyber Security
Utrecht, Netherlands

Aaron Yi Ding
TU Delft
Delft, Netherlands

Sjoerd Pellegrom
Northwave Cyber Security
Utrecht, Netherlands

Yury Zhauniarovich
TU Delft
Delft, Netherlands

ABSTRACT

Organizations are increasingly reliant on third-party software products to expedite their own development cycles, often incorporating numerous components into their end systems, resulting in a lack of transparency in software dependencies. Malicious actors exploit this, leading to Software Supply Chain (SSC) attacks with substantial economic and security damages. To mitigate this threat, the Software Bill of Materials (SBOM) concept was introduced. It details software components and their supply chain relationships, thus enhancing SSC transparency. Unfortunately, SBOM adoption still remains limited. While previous studies identified some reasons behind this, they overlooked the perspectives of different business stakeholder groups involved in SBOM's lifecycle.

In this work, we address this gap by studying business stakeholder groups directly involved in SBOM production and consumption. The main goal of this work is to identify which groups can drive or inhibit SBOM adoption and the rationale behind this behavior. By conducting interviews with the group representatives, we identified stakeholder-specific risks, benefits, concerns and incentives regarding SBOM adoption. Our analysis suggests that SBOM adoption potential is higher among System Integrators and Software Vendors. At the same time, B2B customers and Individual Developers have the least motivation, inhibiting the process of SBOM adoption. Given that these are the main SBOM consuming and supplying stakeholders correspondingly, we conclude that the overall adoption potential of this technology is currently limited and requires considerable external impulse.

CCS CONCEPTS

• **Software and its engineering** → **Software maintenance tools**; *Software configuration management and version control systems*; • **Security and privacy** → *Vulnerability management*; *Human and societal aspects of security and privacy*.

KEYWORDS

SBOM Adoption, Stakeholders, Incentives, Concerns

ACM Reference Format:
Berend Kloeg, Aaron Yi Ding, Sjoerd Pellegrom, and Yury Zhauniarovich. 2024. Charting the Path to SBOM Adoption: A Business Stakeholder-Centric Approach. In *ACM Asia Conference on Computer and Communications Security (ASIA CCS '24), July 1–5, 2024, Singapore, Singapore.* ACM, New York, NY, USA, 14 pages. https://doi.org/10.1145/3634737.3637659

1 INTRODUCTION

Organizations increasingly depend on software products and services [35]. Growing industry demand calls for faster software development cycles, leading developers to rely on third-party components implementing the required functionality [37]. Martínez and Durán [25] estimate that 85 to 97% of commercial software products comprise open-source software (OSS) components, and an even higher percentage may depend on proprietary packages, which often rely on other solutions [12].

An issue prevalent within complex Software Supply Chains (SSC) is that stakeholders involved in software development maintain inadequate records of the components they utilize. A lack of transparency regarding these dependencies leads to ambiguity concerning the software's composition [52]. As the software progresses through the SSC, even a transparent initial picture becomes completely matte. Consequently, software end-users (i.e., the consuming stakeholders) have a limited understanding of what software elements run on their infrastructure [46, 47]. Malicious actors milk this unawareness by committing *software supply chain attacks*, which exploit downstream software components to seize upstream solutions [25, 47]. The SolarWinds case is a prominent example [53] of such an attack resulting in economic damages surpassing billions of dollars [35]. More recent examples include MOVEit [43] and 3CX [15] attacks. In the former case [43], hackers found several zero-days in the MOVEit app used by organizations to transfer files between computers. Through this software, they compromised a major payroll service provider and got access to its customers, including BBC and British Airways [43]. Currently, the number of victims has already reached 400, and counting [20]. In the latter case [15], adversaries compromised 3CX Voice Over Internet Protocol (VoIP) desktop client and used it to infect companies' machines.

To mitigate the risks related to these attacks, *Software Bill of Materials (SBOM)*, a record that describes various components used in building software and their supply chain relationships [16], was proposed. SBOM should accompany supplied software, thus, increasing

*The work has been done in fulfillment of a Master's thesis at TU Delft pursued concurrently with an internship at Northwave Cyber Security.

ASIA CCS '24, July 1–5, 2024, Singapore, Singapore

ACM ISBN 979-8-4007-0482-6/24/07.
https://doi.org/10.1145/3634737.3637659

SSC transparency [16, 25, 35, 50], fostering a better understanding of its licensing, security, quality, and compliance with relevant laws and regulations aspects [44]. For instance, the infamous Log4Shell vulnerability [49] could be mitigated faster if organizations had utilized SBOMs [40]. Despite the promising potential, this concept has not yet received widespread adoption. For instance, Xia et al. [50] reveal that at least 83.1% of the surveyed organizations do not receive SBOMs along with third-party software or components. Other researchers [9, 27, 51] report the lack of SBOM adoption as well.

The reasons behind low SBOM adoption previously received little attention. The first academic works studying this topic [10, 21, 42, 50, 51] have appeared only recently. For instance, Linux Foundation surveyed 412 organizations regarding SBOM readiness and the main concerns of its usage [21]. Xia et al. [50] interviewed SBOM practitioners and found out that uncertainties regarding use cases, benefits of the usage, and concerns about production quality hinder SBOM adoption. Zahan et al. [51] performed the grey literature review and identified the benefits (facilitation of dependencies, vulnerabilities, risk, and licenses management; competitive advantage supply) and challenges (e.g., lack of tools, interoperability, and data about the effectiveness and value) of using SBOM. Bi et al. [10] analyzed the discussions within GitHub SBOM-related projects and identified the gaps in existing SBOM solutions.

While all these recent works study the reasons behind low SBOM adoption, they do this *without considering the interests of different business stakeholder groups involved in the SBOM lifecycle*. Therefore, it is unclear *which groups catalyze and which ones inhibit the adoption of this technology and what is the rationale behind this behavior*. In this work, we make the first step toward closing this gap. In particular, we identified the business stakeholder groups directly involved in SBOM production and consumption and interviewed their representatives to determine what factors incentivize or hinder SBOM adoption within them. In summary, the contributions of this work are the following:

- We identified four stakeholder groups directly involved in SBOM production/consumption processes. We recruited 16 interviewees representing these groups and conducted a qualitative study of their attitudes regarding SBOM using semi-structured interviews.
- We performed a thematic analysis of the data and obtained the stakeholder-group-specific lists of perceived SSC risks and expected SBOM benefits, as well as concerns and incentives regarding SBOM adoption. We estimated the importance of these factors to each group of stakeholders.
- We built SWOT matrices using the identified concerns and incentives, which allowed us to estimate SBOM adoption potential within each stakeholder group. The elimination of stakeholder-specific concerns and promotion of stakeholder-specific incentives may facilitate faster SBOM adoption within a group.

However, true acceptance of the technology as a whole can be achieved if the expectations of all parties are also aligned. Our study provides hints on how to reach this goal as well. Our results can empower regulatory agencies and compliance bodies to formulate more targeted regulations and standards. Industry associations and alliances can leverage these insights to foster collaborative initiatives, while policymakers can shape policies that actively promote SBOM adoption.

2 METHODOLOGY

In this research, we adopt an exploratory empirical study approach to gain new qualitative insights into the relevant concerns and incentives most important to business software supply chain (SSC) stakeholders, which may have restrained or promoted SBOM adoption thus far or have the potential to do so in the future. Figure 1 presents an overview of the applied methodology, consisting of three phases. In this section, we provide a detailed overview of these phases and the methods used in each of them.

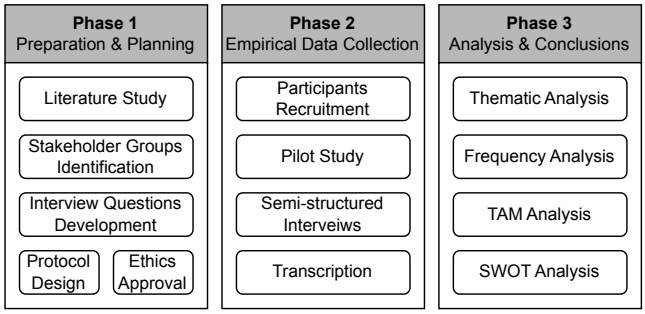

Figure 1: Overview of research methodology

2.1 Phase One: Preparation & Planning

The goal of this phase is to set up the research stage and prepare for the interviews ensuring their quality and relevance. It also aims to address certain limitations, particularly the need to avoid researcher bias. To ensure the originality of our idea and to obtain hints about potential questions and the involved stakeholder groups, we started this phase with careful examination of the relevant literature.

SBOM does not exist in a vacuum; it is a part of the software production business, which involves various stakeholder groups. For our study, we selected the ones who are directly involved in SBOM production/consumption: *B2B Customers (B2B)*, *System Integrators (SI)*, *Software Vendors (SV)* and *Developers (DEV)*. Therefore, stakeholder groups such as government bodies, SBOM format and tools providers, and external security companies are excluded from the scope of this research despite their potential interests in the SBOM field. To the best of our knowledge, we are the first who explore stakeholders' incentives and concerns regarding SBOM according to their position in the software production business chain rather than their involvement in the SBOM lifecycle (e.g., Linux Foundation study [21] splits split stakeholders into SBOM producers and consumers). This gives us a unique view of their SBOM adoption attitude from the business-needs perspective.

So as our research encompasses the study of different stakeholder groups, we stick to the semi-structured interview design. To ensure comprehensiveness, we developed a set of open-ended interview questions. These questions start with broad inquiries, deliberately avoiding any specific introduction to incentives and concerns or related topics. This approach is crucial for minimizing researcher bias and collecting valuable data for analysis. Then, we ask more specific questions based on the literature studies' [18, 27, 50, 51] findings. Contrary to the previous studies [21, 50], in this work, we rely on open-ended questions that contribute to a more nuanced

understanding of the research and uncovering missing data [39]. Since participants have the freedom to respond openly, they might provide insights and perspectives that the researcher hadn't anticipated. This can lead to the discovery of new angles and themes.

In collaboration with the research ethics department, we developed the research protocol for our study (see Appendix A). This protocol underwent two iterations to ensure comprehensive coverage of all potential risks. We obtained ethical approval from our Institutional Review Board to conduct this research. From all interview participants, we got explicit consent for the anonymized processing of the results.

2.2 Phase Two: Empirical Data Collection

Finding the right interviewees is paramount to obtaining valuable insights. For this study, we partnered with an international security software production and service provider company. We recruited our B2B representatives among their customers; SI and SV participants were employed among the software providers to their customers using connections and the good reputation of our partner. Finally, DEV-group interviewees were found among the developers working on SBOM-related projects on GitHub by contacting them through publicly available email addresses. As a result, we recruited 16 individuals for this study. Table 1 reports their demographic information.

Table 1: Overview of participant demographics

ID	Group	Work Experience (years)	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

The participants' knowledge levels were distinguished based on their direct experience with SBOM. Only two participants had limited familiarity with SBOM, while the majority displayed a good understanding of the concept. Work experience was another crucial factor considered among the participants, particularly their years in the software industry. This information added valuable context to the insights gained during the interviews.

To refine the questionnaire, we conducted two pilot interviews within the collaborating organization, incorporating perspectives from both technical and C-level individuals. The pilot study was vital in identifying potential ambiguities. Through an iterative process, we addressed these ambiguities and incorporated relevant concerns raised during the pilot study into the final questionnaire.

To maintain consistency, we followed a systematic approach in conducting the interviews. Starting from the B2B groups, the interviews progressed along the SSC hierarchy, ensuring a comprehensive understanding of perspectives and experiences. Care was taken to prevent earlier interview findings from unduly influencing subsequent interviews.

The interviews lasted approximately one hour. The interviews were audio-recorded and then transcribed with the help of a speech-to-text state-of-the-art tool running on a local machine [3]. The first author then additionally verified and edited the extracted text.

2.3 Phase Three: Analysis & Conclusions

To make conclusions and obtain actionable knowledge from our study, we scrutinized the empirically gathered data by applying three types of analysis.

First, we conducted a *thematic analysis* to identify the most interesting themes derived from the interviews following the six-step plan proposed by Braun and Clarke [11], which includes: 1) exploration; 2) coding; 3) theme identification; 4) revision & refinement; 5) defining & organizing; and 6) presentation. During the first step, we became familiar with the dataset and then carefully examined it three times. During the second step, we systematically identified relevant data units, such as specific phrases, sentences, or paragraphs, and labeled them for later reference, capturing anything that stood out and seemed interesting and insightful. The theme identification step required more time and closer attention. This step is based on patterns, connections, and frequently recurring concept recognition within the coded data. We grouped different codes into overarching themes representing significant aspects or ideas emerging from the data. To ensure the accuracy of the themes, the entire dataset was screened twice. We developed initial themes after the first screening, and the second screening helped us to verify whether all essential data was included and to refine some theme names. In Step 5, we provided clear definitions of the identified themes and selected the themes that fall into four categories relevant to this study: 1) SSC risks, 2) expected SBOM benefits, 3) concerns regarding, and 4) incentives for SBOM adoption. As a result of this analysis, we obtained themes grouped into categories and the corresponding semantic units.

According to Kuckartz [22], the themes themselves and the corresponding identified semantic units constitute the thematic analysis's main findings. At the same time, if a particular theme is only addressed by one participant and not by others, its significance may be relatively low and should be given less attention later on [26]. Therefore, secondly, we applied the *frequency analysis*. This type of analysis helps researchers to weigh the importance of identified themes, enabling them to uncover deeper relationships and patterns, potentially leading to more relevant and novel insights. In the context of our study, it allowed us to estimate the themes' importance for each stakeholder group.

Third, we employed the Technology Acceptance Model (TAM) [45]. According to this model, the adoption of technology by users depends on its *perceived usefulness* (users are more likely to accept and

use technology if they believe it will enhance their performance, productivity, or effectiveness in achieving their goals) and *perceived ease of use* (users are more likely to accept a technology if they perceive it as easy to learn, use, and integrate into their existing routines). We use TAM to ponder SBOM adoption within each stakeholder group.

Finally, we applied SWOT analysis [28, 48]. SWOT, which stands for Strengths, Weaknesses, Opportunities, and Threats, is a widely used framework for assessing the potential of new technology by evaluating internal and external factors. It helps to identify the technology's internal strengths and weaknesses, as well as external opportunities and threats, to understand its viability in the given context. It facilitates gaining a comprehensive understanding of the current situation, making more informed decisions and developing effective strategies. Based on the identified incentives and concerns and their importance, we drew SWOT matrices for each stakeholder group. This allowed us to make clear what factors can be used and how to strengthen SBOM adoption potential within each stakeholder group. Moreover, knowing the business relations between different groups, we are able to propose some strategies on how to promote the spread of this technology.

3 FINDINGS

In this section, we discuss the main findings of our study. We start our analysis by identifying the SSC risks perceived by stakeholders and their outlook on expected SBOM benefits (Section 3.1). By correlating these factors, we can assess whether SBOM is likely to address or mitigate the identified risks, thus concluding on the value of this technology in general. Then in Section 3.2, we extract the stakeholders' incentives and concerns regarding SBOM adoption, identifying the factors that accelerate or slow down the embracement of this technology. In Section 3.3, we split these factors according to SWOT categories and draw conclusions about the adoption potential of this technology in each stakeholder group. This helps us to figure out which groups and in what way should be targeted to promote SBOM adoption.

3.1 Perceived SSC Risks and Expected SBOM Benefits

To find out how to drive SBOM adoption, we need to figure out what are the most important SSC risks stakeholders perceive and what their anticipations are about the benefits provided by SBOM. The more risks the technology is expected to address or mitigate, the higher its value and the stronger the appetite of the corresponding group to adopt it. Table 2 lists the most significant SSC risks perceived by stakeholders, while Table 3 reports expected SBOM benefits. The percentages represent the fraction of participants within each stakeholder group mentioning the corresponding theme.

As we can see from Table 2, the fear of **Compromised Components** emerges as the most prominent risk, highlighted by 44% of all participants. It is clear that SBOM cannot fully address this risk, and the stakeholders do not expect that. However, the risk can be mitigated given **Transparency** and **Better Vulnerability Management** ensured by SBOM. Indeed, companies would be able to discover vulnerabilities in their software faster and would be able to install barriers to limit their exploitation until the patch is deployed. Moreover, they would be able to ask their software integrators for the patches, thus creating pressure along the SSC to develop updates faster. Not surprisingly, these are the most expected and valuable stakeholders' benefits: 81% of participants agreed that the main SBOM advantage is **Enhanced Transparency** and the same percentage mentioned **Better Vulnerability Management**. In this respect, expected SBOM benefits partially cover the SSC risk.

The risk of **Absent or Slow Response** follows as the second most cited theme, mentioned by 38% of all participants. For instance, P5[B2B] mentioned that they were *"actively reaching out to their suppliers to inquire about the use of components"* related to the Log4Shell vulnerability, as they lacked visibility about it themselves. The **Transparency** benefit, if facilitated by SBOM, can eliminate this risk. Indeed, consumers might not even need to contact the providers of the software if they have an accurate SBOM for it.

Another notable risk is **Maintenance and Support of Components** (25%). For example, P12[DEV] noted that *"maintenance of OSS 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. P14[SV] also mentioned this and related it also with *"freshness risk"*, indicating the extent to which a component has not been updated over time. The **Transparency** (identified by 81% of the interviewees) and **Educated Suppliers Selection** (mentioned by 25% of the respondents) benefits are called to mitigate this risk. Indeed, if those benefits come true, it would be easier for software consumers to select solutions that do not contain outdated or pure-maintained components [8]. Unfortunately, preemptive assessment of the software solutions and their SBOM is not always possible. While almost all participants (75%) agree with the idea of preemptive access for **Educated Suppliers Selection**, some, e.g., P9[SI], noted that it is often not feasible due to the uncertain nature of the final product at the time of software acquisition. Significant changes occur during the development and integration phases, making obtaining corresponding SBOMs in advance impossible. Participants who support this idea rely primarily on Commercial Off-The-Shelf (COTS) software products.

Regarding **License Violations** risk, P6[SV] is one of the three participants (19%) who mentioned complications related to stringent OSS licenses, leading to issues in the past year, primarily involving the legal department. This risk can be mitigated simply by having access to more accurate information. Nevertheless, this is something that *"often goes wrong now,"* as mentioned by P10[DEV]. In this respect, the expected **Better License Management** benefit, mentioned by 25% of all participants, would help to address this risk. At the same time, P9[SI] offers a different perspective, suggesting that if one encounters licensing problems, it simply means that *"they did not do their homework sufficiently."*

An interesting trend, although not frequently mentioned, is related to the risk of **Staff Reduction** by software-consuming organizations. Participant P9[SI] expressed the view that security staff cannot compete with the larger workforce employed by major cloud companies, leading to the perception that security staff is no longer necessary. However, this poses a challenge as it results in a significant reduction in in-house security expertise. This perspective aligns with the finding regarding the increasing shift in responsibility for seeking vulnerabilities and ensuring security,

Table 2: Perceived SSC Risks

Risk	Description	Groups				All
		B2B	SI	SV	DEV	
Compromised Components	The risks of compromised software components that subsequently flow throughout the SSC	50%	67%	0%	60%	44%
Absent or Slow Response	The risks related to untimely or absent mitigation response to vulnerabilities that may exist within the software but which stakeholders are not aware of	50%	0%	50%	40%	38%
Components Maintenance and Support	The risks related to an inadequate level of software components maintenance and support due to the limited developer resources that raise concerns about the reliability, support, and timely updates of these components	0%	33%	25%	40%	25%
License Violations	The risks related to license violations due to the lack of transparency of what software components are used	0%	0%	50%	20%	19%
Staff Reduction	The risks connected to the internal security staff downsizing due to the SaaS outsourcing that results in a reduction in expertise and manpower available within the organization when needed	0%	33%	0%	0%	6%

Table 3: Expected SBOM Benefits

Benefit	Description	Groups				All
		B2B	SI	SV	DEV	
Better Vulnerability Management	It will be easier to identify potential vulnerabilities within the SSC and take proactive measures to mitigate the risk of their exploitation	100%	67%	75%	80%	81%
Transparency	The enhancement of transparency and visibility of software within the SSC	75%	100%	75%	80%	81%
Educated Suppliers Selection	It will be easier to choose between different software suppliers using the comprehensive SBOMs they provide	25%	33%	0%	40%	25%
Better License Management	With SBOM, it will be easier to manage software licenses to ensure compliance and avoid license violations	0%	33%	25%	40%	25%

with 25% of total participants indicating a shift towards suppliers, including cloud providers. Unfortunately, from our point of view, SBOM cannot address or mitigate this risk.

3.2 SBOM Adoption Incentives and Concerns

3.2.1 SBOM Adoption Incentives. Various positive factors become evident during (the analysis of) the interviews that indicate their importance for certain stakeholder groups. We interpret these factors as incentives to adopt SBOM. Table 4 lists the most significant adoption incentives perceived by stakeholders.

Compliance is among the most popular SBOM incentives mentioned by 44% of all participants. This percentage encompasses both regulatory compliance and industry standard compliance. Notably, 60% of developers indicated that regulatory compliance is an important adoption incentive for the SSC in general, while they personally do not encounter this incentive. Hence, we did not include their replies in the table – with their answers included, the percentage would be even higher. Moreover, specific interview questions about laws and regulations revealed that 69% of participants consider compliance crucial for SBOM adoption. P3[B2B] emphasized that, despite idealistic perspectives, regulations would ultimately drive SBOM adoption: *"it can create demand and awareness among users and also push suppliers to establish governance to ensure high data quality."*

For SVs and SIs, **Compliance** appears to be one of the dominant adoption incentives: 75% of SVs and 100% of SIs mentioned this incentive. These numbers align closely with the ones (50% of SVs and 100% of SIs) related to **Improved Reputation or Trust** factor that these groups also consider highly important. Unfortunately, as emphasized by P8[SV] on multiple occasions, there is currently no established industry standard for SBOMs; therefore, nothing to comply with. To encourage adoption among SVs and SIs, the establishment of industry standards is crucial. Certifying suppliers on their SBOMs could play a role in this regard (P3[B2B], P8[SV]), ensuring adherence to specific standards and practices, thereby fostering trust and confidence in the software components provided. Certification would enable suppliers to demonstrate their commitment to security and quality assurance. As noted by P3[B2B], certification, and thus knowing that a supplier uses SBOMs, can be more crucial than the specific contents of SBOMs themselves. Moreover, it can be an effective marketing tool during sales pitches, as mentioned by P7[SI]. Additionally, certification streamlines the evaluation process for customers, allowing them to rely on the certification as an indicator of a supplier's compliance with industry

Table 4: SBOM Adoption Incentives

Incentive	Description	Groups				All
		B2B	SI	SV	DEV	
Compliance	Mandatory or voluntary (but giving a competitive advantage) compliance with laws, regulations, or industry standards	25%	100%	75%	0%	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	100%	33%	25%	20%	44%
Improved Reputation or Trust	SBOM is adopted because it improves the reputation or trust of the software producers	0%	100%	50%	40%	44%
Time or Effort Savings	SBOM is adopted due to time or effort savings	75%	33%	75%	0%	44%
Improved Quality of Supplied Software	SBOM adoption may contribute to the improvement of the supplied software	0%	100%	50%	0%	31%
Ethical and Ideological	SBOM is adopted due to its alignment with ideological or ethical principles	0%	0%	0%	40%	13%

standards and best practices rather than scrutinizing every detail of SBOM.

Enhanced Security for Consumed Software incentive, as perceived by the participants, aligns with the benefits they previously mentioned and can indeed facilitate the adoption. Particularly for the B2B stakeholder group, this incentive is of paramount importance, with 100% of them recognizing it. As they also acknowledged the advantages of SBOM in better vulnerability management and security assurance, this factor contributed to the adoption incentive for this stakeholder group.

Another important adoption incentive emerges from the potential for SBOMs to contribute to **Improved Reputation or Trust** of suppliers, as well as the recognition and exposure of developers. In general, many SVs (50%) and SIs (100%) indicate that reputation and trust are highly significant incentives for them. For instance, P1[SI] and P7[SI] explicitly mention the belief that SBOMs will enhance trust in them as suppliers. Overall, participants emphasize the importance of trust. If SBOMs can contribute to its improvement, this presents a strong incentive. This aligns with quality management programs in which P4[SV], P6[SV], P9[SI], and P14[SV] intend to incorporate SBOM. P6[SV] suggests that improving quality should lead to reduced reputational damage. B2B customers did not directly mention that SBOMs would generate more trust for them. However, P3[B2B] stated an interest solely in whether suppliers use SBOMs and not their specific contents because this fact elevates the expectations about the reliability of the supplied software. Additionally, preemptive access to COTS software, identified as an advantage for educated supplier selection, could also contribute to trust and reputation. It provides customers with an additional opportunity to verify the quality of what they are acquiring, although, as indicated by the experience of P8[SV], customers often do not avail themselves of this option.

Developers indicate that their **Improved Reputation or Trust** incentives lie more in the improved recognition and exposure achieved via SBOM. With the appropriate component metadata related to supplier names incorporated into SBOMs, P12[DEV] believes that *"if you produce SBOMs yourself, other parties are more likely to use the software and include it in their SBOM, which in turn helps with exposure."* Similarly, P13[DEV] expresses the importance of recognition for their development endeavors.

Time or Effort Savings is also cited by a high number of participants. Especially the B2B and SV stakeholder groups see this incentive, with 75% mentioning this in both groups. Two noteworthy aspects emerge in this context. First, it pertains to the value SBOM brings to identifying known vulnerabilities within a software stack. Log4j serves as an example, leaving an impression on 44% of participants. Additionally, 31% mention the potential usefulness of SBOM in similar scenarios, contributing to time and effort savings. P6[SV] highlights that it could have easily saved them 240 hours, stating, *"That's bizarre, given that it was essentially just SBOM functionality."* P3[B2B] shares this concern, evaluating that it took them a month before everything was sorted out: *"Suppliers also sometimes respond quite tough, or not at all, or they didn't know either."* P12[DEV] affirms the use case, framing it more as something that will aid SSC stakeholders in general rather than developers. The second aspect contributing to **Time or Effort Savings** involves stakeholders outsourcing (part of) their security operations to external organizations.

Improved Quality of Supplied Software is particularly important for SVs and SIs, as it is solely indicated by these stakeholders. In a sense, it closely aligns with the incentive of enhanced security for consumed software, but for these stakeholder groups, security falls under the umbrella of supplied software quality. An intriguing finding related to quality assurance emerges from the internal use case. By consuming SBOMs generated themselves, SIs and SVs can swiftly identify risks and vulnerabilities for their customers. This internal use case was mentioned by 31% of the participants, with 100% and 50% of SI and SV respondents correspondingly. This case aligns with our other findings. First, there is a discernible shift in responsibility regarding security, as highlighted by 25% of the

participants. The increase in Software-as-a-Service (SaaS) products has led to less involvement of B2B customers in the software supply appraisal, leading them to assume that vendors should take care of software security. Therefore, 38% of participants indicate that they indeed rely on established, large vendors and well-known software components. Second, by not having to consume SBOMs themselves, B2B customers could save a lot of time and effort.

4 out of 5 developers (80%), who participated in our study, mentioned their engagement in open-source development is due to **Ethical and Ideological** incentives. Half of them indicated that the same factor also incentivizes them to adopt SBOM for their open-source components. P16[DEV] perceives their SBOM contributions as the ability *"to have a net positive impact on security"*, which motivates their involvement in SBOM projects. P13[DEV] asserts, *"The whole purpose of open-source development is to be open and to allow everyone to use the thing that we develop. So in order to have that incentive for them to use our software, we need some transparency."*

Interestingly, while answering the main questions, nobody mentioned direct monetary value as an incentive, which was very surprising to us. However, after discussing the financial aspects of SBOM with the participants, we found out that SBOM is mainly considered as costs rather than gains. Indeed, the main groups that can charge for SBOMs are SIs, SVs and DEVs. However, they do not consider SBOM as an accompanying service that can be sold to their customers. Currently, SBOM provision is required if one supplies software to US government agencies (according to EO14028 [2]). For individual developers, according to P10[DEV], if they work for these agencies, there is already sufficient incentive to adopt SBOMs in order to continue to collaborate with them. Similarly, commercial suppliers receive substantial financial compensation for providing software to these agencies. These financial gains justify suppliers' investments in generating and delivering SBOMs alongside their software.

At the same time, 75% of B2B customers are willing to incur additional costs given the SBOM is useful for them. 57% of the SV and SI interviewees believe that they can effectively transfer these costs to their customers. One SV participant was an exception, indicating they could not pass on the costs. However, a question persists (raised by P2[B2B]) regarding the direct allocation of these costs and the potential for customers to choose: *"If you can obtain an SBOM by paying for it, can you also purchase products without an SBOM and receive a discount?"* It appears that introducing this additional aspect would introduce a heightened complexity and challenges. P6[SV] suggests that a thorough deliberation of all details could lead to debates among individuals unfamiliar with SBOM, potentially questioning its necessity. To circumvent this, a majority of SVs and SIs indicate their intention to integrate SBOM-related costs into their quality programs, thereby framing it as an operational expenditure rather than a capital one. For instance, P14[SV] asserts: *"These are recurring costs that need to be incorporated into your services. Eventually, you will pass them on to the customer."*

3.2.2 SBOM Adoption Concerns. Table 5 lists the most significant adoption concerns perceived by stakeholders.

A significant concern for SBOM adoption is the **Lack of Knowledge and Expertise** cited by 69% of participants at various levels within the SSC. 8 out of 11 participants who raised this concern specifically mentioned the B2B stakeholder group for whom it will be too complex to derive value from SBOMs, given the current tooling and formats. 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. This issue is critical as it can lead to potential misuse of SBOMs, as P16[DEV] noted. 6 out of 11 participants expressed concerns about this factor also regarding SVs and SIs within the SSC. They encounter challenges when producing SBOMs and face difficulties understanding how to proceed. Many software companies lack insight into the third-party components they use for software development, as P8[SV] stated. Interestingly, P12[DEV] even raises a concern for developers: if it becomes mandatory for all developers to generate SBOMs, many inexperienced ones, having little to no knowledge of security practices, may not understand the expectations placed on them and may produce incorrect or useless SBOMs.

SBOM Limited Usefulness is caused by three distinct concern flavors: detailing and layering, SBOM selection, and mere compliance. First, a considerable number of participants (38%) express concerns regarding the level of detail and the layering of SBOMs throughout the SSC. They fear that if SBOMs are only produced at the commercial SV level based on first-order dependencies, this will not be enough to get actionable information. P13[DEV] confirms this by stating: *"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."* Ideally, one would want to have information about the whole dependency graph built on every stage. P10[DEV] strongly agrees with this: *"It just means that you need the SBOMs at every layer. You can't just retroactively go build them."* At the same time, it is not always necessary to produce SBOM at every layer. P16[DEV] indicates that it largely depends on the software ecosystem being used. Most modern programming language ecosystems rely on dependency managers (e.g., Maven for Java, Cargo for Rust, etc.) that simplify control over third-party components by resolving and downloading dependencies based on a dependency file that lists required components and version constraints. Some also offer the option to lock exact component versions in a separate 'lock' file. Consequently, in these ecosystems, creating a separate SBOM is usually unnecessary as it can be derived from the 'lock' file later. Open-source developers relying on dependency files typically don't need to produce separate SBOMs for their components, as P14[SV] points out. However, commercial vendors should generate an SBOM when they compile software to encompass all third-party components in the final product, as P16[DEV] suggests. Indeed, at this stage, different dependency managers are used that frequently do not interoperate with each other. That is where SBOM becomes useful – as the abstraction layer on top of them. P15[DEV] fully agrees with this and sees SBOM as a kind of standardized format for representing the information about the dependencies provided by different ecosystems in the same way. Thus, it should be easier to build tooling around it and make use of the provided information.

Table 5: SBOM Adoption Concerns

Concern	Description	Groups				All
		B2B	SI	SV	DEV	
Lack of Knowledge or Expertise	Lack of knowledge or expertise may thwart successful SBOM implementation	50%	67%	50%	100%	69%
SBOM Limited Usefulness	SBOMs could be generated for a) various software, b) on multiple levels, c) by different vendors. The overall usefulness of SBOM is constrained by the quality it maintains across all these distinct aspects	100%	67%	25%	80%	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	25%	67%	50%	60%	50%
Vulnerability Missclassification	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)	25%	33%	25%	60%	38%
Financial Losses	SBOM adoption may not cover all the incurred investments and operational costs	25%	67%	0%	0%	19%
Imperfect Tooling, Formats or Vulnerability DBs	Lack of or imperfect tools, incompatible SBOM formats and multiple vulnerability databases hinder SBOM adoption	0%	33%	0%	40%	19%
Threat to IP	Intellectual Property can be revealed to competitors/third parties through SBOM	0%	0%	25%	0%	6%

Second, a relatively substantial proportion (44%) of participants emphasize the importance of the organization's ability to select the specific applications and systems for which SBOMs are deemed necessary. It is unrealistic to have SBOMs available for every piece of software [32]. There is also a significant variation per sector and organization regarding the most critical components. For instance, regarding the distinction in criticality, P9[SI] states: *"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."* At the same time, whether the selection is feasible remains to be seen. As previously mentioned, this is not always possible due to the uncertainty surrounding the final deliverable. Therefore, such selection could potentially be applicable solely to COTS software. Nevertheless, concerns exist even in this context, e.g., as prompted by P2[B2B] regarding potential discounts when customers forego SBOMs.

Finally, 38% of the participants share the belief that SBOM could potentially serve merely as a compliance requirement if mandated by law. For instance, P8[SV] pointed out that many of the security and compliance measures they must implement are merely checklists they must meet. Due to the inability to realize its value, SBOM becomes perceived as a mere formality. P10[DEV] and P16[DEV] both mentioned that this situation currently persists in the U.S. in the context of EO14028 [2]. Suppliers do produce SBOMs, and government agencies receive them, but the quality of the produced SBOMs and their consumption value remains low. At the same time, there are counterarguments to this view. P16[DEV] suggests that compliance as the starting incentive of SBOM adoption is not bad. The realization of its potential value can gradually follow. Similarly, P14[SV] sees it as a step-by-step maturity ladder: *"The first step is to have a bill of materials. The next step is to manage the risks that come from it."* For instance, P11[B2B] believes that immediate quality requirements in legislation might not be necessary. Moreover, the required standards could significantly vary across sectors, organizations, applications, and beyond. Nonetheless, P3[B2B] thinks there might eventually be a need for more thorough regulations to ensure quality.

Time or Effort Overheads concern is mentioned by 50% of the participants. These overheads can be caused by several factors. The most common ones pertain to the storage and maintenance of SBOMs, having proper asset management in place, and governance of SBOM-related processes. Both P14[SV] and P16[DEV] highlighted that SBOMs must be seen as dynamic processes rather than static entities. They should provide real-time visibility into software components, their versions, licenses, vulnerabilities, and associated risks. They state that SBOM is not something one produces once and never looks at again. Instead, it needs to be continuously maintained and updated. This necessitates substantial time and effort, and, furthermore, the determination of who is accountable for this task. A quarter of the participants (25%) already mentioned issues regarding the maintenance of open-source components, with P12[DEV] indicating that this responsibility often falls on small groups that may lose interest or no longer have the time to maintain them. This lack of time among developers is also highlighted by P1[SI] and P7[SI]. Both state that developers in their organizations often face time constraints, which can lead to insufficient time for thorough testing of the incorporated software components. However, in response to this, P3[B2B] emphasizes the importance of security in this context: *"We all want to develop faster and faster. However, 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 becomes a hindrance to innovation."*

Proper asset management is considered the foundational step before a party adopts SBOMs, which also requires additional time and effort. P16[DEV] asserts that asset management should be integrated as a core component of SBOM. Recognizing the importance of managing and documenting software assets enhances the overall

effectiveness of SBOM implementation. Without a clear understanding of the software ecosystem, effective utilization of SBOMs becomes challenging. This aligns with the point raised by P13[DEV] that organizations intending to engage with SBOMs should possess a certain level of security maturity. P3[B2B] expresses concerns about shadow IT, underscoring the risk of unauthorized software installations by employees. Maintaining visibility and control over the software landscape is critical in this context.

Lastly, organizing all necessary processes for a successful SBOM integration is more challenging than initially anticipated (P3[B2B], P7[SI]). Processing SBOMs, which includes acquiring and distributing them, requires engagement with various stakeholders, including legal departments and other parties within the organization. Establishing such a structure within an organization is challenging and time-consuming. Even the process of requesting SBOMs can be difficult. Furthermore, the dynamic nature of SBOMs adds more complexity. Both vendors and customers will likely encounter challenges in navigating the intricacies of SBOM governance.

One of the most important concerns mentioned by 50% of the participants is **Vulnerability Misclassification**. There are several aspects regarding this concern. The first relates to the fear of a high number of false positives resulting from a vulnerability analysis using an SBOM (mentioned by 31%). P9[SI] states that in many cases, Common Vulnerabilities and Exposures (CVEs) identified in an upstream component may not be exploitable in the final software product run by a B2B customer. This may happen due to the affected component being defined as a dependency but actually not being used during the compilation or at runtime or the vulnerable functionality being sandboxed or safeguarded. It is estimated [6] that more than 90% of all dependencies' vulnerabilities are not exploitable in the final product. 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. The process of assessing the exploitability of each vulnerability is too time-consuming. P12[DEV] noted that whether a vulnerability is exploitable may vary from one setup to another, 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 mentioned that customers might be discouraged if they have never thoroughly scanned their software and then, for the first time, by performing a vulnerability analysis on an SBOM, found 300 vulnerabilities. They would have no idea how to proceed. Although a recently proposed Vulnerability-Exploitability eXchange format [31], which allows software suppliers to clarify whether a specific vulnerability in the dependency actually affects the final product, may mitigate this concern, it cannot eliminate it completely [7]. The second aspect is related to the practice of developers copy-pasting lines of code instead of formally importing the component (e.g., a library) from which the code originates and calling its functionality. This results in omitting known vulnerabilities associated with the component during vulnerability analysis (false negatives) because the SBOM does not reveal it as a dependency. Similar concerns arise when stakeholders require avoiding components from specific countries, highlighting the need for developers to disclose the code origin. P1[SI] recognizes this concern as when *"someone uses a piece of code from Stack Overflow without any evidence of who originally created it."* The same sentiment is expressed regarding modern Large Language Model-based systems, such as ChatGPT. However, a number of participants (25% of the total) do not categorize copy-pasting as a specific SBOM problem. P9[SI] strongly supports this view and describes a scenario to illustrate that the consequences may be even not significant. For instance, in the case of Log4j, if an organization wants to check if it is vulnerable, it might run all potentially vulnerable code through a code checker or scanner and not rely on SBOM. This way, one could identify the problem even if it is present due to copy-pasted code.

Another concern raised by 19% participants pertains to **Financial Losses** or Return on Investments for adopting SBOMs. This concern can be viewed from software suppliers and consumers perspectives. Consumers, e.g., as pointed by P2[B2B], strongly question what level of security they are actually getting for a certain price, including with SBOMs. Security is subjective, which makes this assessment even more complex. Suppliers also emphasize the complexity of the trade-off between security and the costs of investments. This consideration is influenced by various external factors. For instance, P9[SI] states that *"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."*

There are still areas for improvement in the current state of SBOM. Various concerns revolve around **Imperfect Tooling, Formats, and Vulnerability Databases**. Regarding tooling and automation, 44% of all participants emphasize their significance, with P1[SI] stating that *"The success of SBOM is fully dependent on good tooling."* The developer stakeholder group represents the majority, with 80% mentioning this factor. In this group, 40% consider the existing SBOM tools to be immature. According to P14[SV], they are associated with quality issues such as accuracy and completeness, and too much manual work is still involved. P10[DEV] contributes to SBOM quality assurance tool projects and observes that the current tooling is immature and often lacks version numbers or unique identifiers, which is also acknowledged by the experts [4, 34]. This sentiment extends to the SBOMs provided to government agencies in the US when they acquire software. The premature state of tooling and automation increases time and effort overheads. The current reliance on manual processes may discourage SBOM consumption within the B2B stakeholder group and diminish the sought-after quality by SVs and SIs in their production. Lastly, P15[DEV] suggests that *"if tooling is well integrated with commonly used package managers, then you're already halfway there."*

Two participants highlighted the existence of various accepted and standardized SBOM formats, such as CycloneDX [36] and SPDX [23], as a concern for adoption. P13[DEV] suggests that it is not very clear which format should be used, and once that decision is made, appropriate tooling is required to generate SBOMs, perform vulnerability analysis and utilize SBOMs provided in other formats. *"That's all quite heavy to manage, and it requires maturity regarding software security, and not all companies have developers with that,"* adds P13[DEV]. Similar concerns are expressed by P14[SV], who particularly emphasizes the lack of proper alignment between different formats, resulting in a disconnect in SBOM data. This remains a significant issue.

The last factor contributing to this concern regards the vulnerability databases that are commonly used for vulnerability analyses: once an SBOM is obtained, querying databases (open source or commercial) is necessary to retrieve the information about the corresponding CVEs. However, as P13[DEV] noted, the National Vulnerability Database (NVD) [29] is not always precise in its vulnerabilities, so multiple databases need to be used to obtain accurate data, leading to the management of duplicates. An alternative is to create one but comprehensive database [5]. For instance, Google backs one such initiative for open source projects [1]. 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 unique identifiers.

Previous studies [32, 33, 51] identified that there could be significant concern regarding the **Threat to Intellectual Property (IP)** because of SBOMs, but our findings showed that it was not perceived as severe as expected. Only one participant (6%) mentioned IP as a concern and significant concern for adoption. When we explicitly discussed the topic, seven participants (44%) acknowledged that SBOMs could potentially threaten IP. However, many participants stated that SBOMs might reveal some but not a significant amount of information, and the most critical IP is typically found not in the dependencies. To draw an analogy with nutrition labels, one cannot recreate the entire food product solely from the ingredients. Additionally, as long as SBOMs are not made public, there is no major problem. Concerning the public availability of SBOMs, no participants were particularly enthusiastic. P2[B2B] mentioned that *"Transparency only works when everyone is transparent. In advance, you know not everyone will be."* Regarding the private availability of SBOMs, several factors were mentioned that mitigated concerns about IP. 25% of the participants suggested that Non-Disclosure Agreements (NDAs) could be a solution. Additionally, two participants mentioned that reverse engineering could potentially be more effective for inferring the IP rather than the product's dependencies.

3.3 Analysis of SBOM Adoption Potential

In this section, we aggregate the findings we made in this work and try to answer the question about the adoption potential of SBOM. To reach our goal, we employ the Technology Acceptance Model (TAM) [45] to estimate the potential of SBOM adoption within each stakeholder group, and the SWOT analysis framework [28, 48] to propose some strategies on how to promote the spread of this technology within a group. Then, by analyzing the relationships between these groups, we draw conclusions about the adoption potential of this technology in general.

Figure 2 shows the SWOT diagrams for each stakeholder group. To build these diagrams, we selected the incentives and concerns that we have identified in Section 3.2 for each stakeholder group, ordered them based on their importance (percentage of group participants who mentioned the corresponding item), and clustered within two dimensions: the first splits the factors based on their negative or positive influence on adoption, while the second divides them based on their relation to the group, i.e., whether the factors are more internally or externally influenced. Moreover, the diagrams in the upper and lower halves are related to more software-consuming software-producing groups correspondingly, while the horizontal distribution shows the degree of that relation, i.e., in the left half, the degree is stronger, in the right – weaker.

So as the demand creates the supply, we start our SWOT analysis from the B2B stakeholders group. As we can see from Figure 2a, the most significant strength is the expectation that the presence of SBOMs will bring the **Enhanced Security** and **Time or Effort Savings**. Unfortunately, at the present moment, SBOM integration most probably leads to additional time and effort expenditures, while the benefits are not yet clear. Indeed, in the last several years, there were several very high-profile attacks, e.g., Log4Shell [49] or PyTorch dependency confusion [41], which could have potentially led to huge damage, and where the use of SBOMs would probably improve the detection of the vulnerable components and reduce the reaction time. Luckily, due to the wide coverage of these vulnerabilities in the media, organizations managed to patch their systems in time. Moreover, in the case of Log4Shell [49], security experts quickly developed custom scanners which allowed one to detect the presence of the vulnerable dependency in a piece of software. Therefore, not surprisingly, **SBOM Limited Usefulness** is the main threat to SBOM adoption perceived by the B2B stakeholders, which all the participants from this group unanimously identify. Note that **Lack of Knowledge** is quite a strong weakness identified by this group. As we can see from our research, the B2B stakeholders have doubts about the usefulness of SBOMs for them, and moreover, they expect high cognitive demands to incorporate this technology. Thus, according to TAM, we can conclude that at the present moment, this stakeholder group has limited internal incentives for SBOM adoption. Definitely, the external stimulus in the form of **Compliance** would change the situation. However, currently, this factor is not yet that important for this group as only one participant has mentioned it.

SBOM adoption pursuit is much stronger for the SI group. Indeed, they perceive **Compliance** as a strong external stimulus. However, with strict compliance rules, they can start considering SBOM as a mere formality. If we continue the analogy with nutrition labels, food producers must provide them, but we, consumers, rarely read them. Moreover, the verification of these "SBOM nutrition labels" is challenging. It is also not clear who has to do this, how, and what are the consequences for providing incorrect data. Additionally, the SI group representatives see the value of SBOM in **Improved Reputation or Trust** and **Improved Quality of Supplied Software**. However, they also identify that the adoption of this technology may incur additional **Financial Losses** and may lead to additional **Time or Effort Overheads**. Similar factors are also important for the SV stakeholders group, but the influence of the threats is much weaker. Therefore, we assume that these two groups of stakeholders could be the main drivers behind the adoption of the technology.

SBOM adoption from the DEV stakeholders group is mainly driven by internal motivation factors: **Ethical and Ideological** principles and **Improved Reputation or Trust**, which was also confirmed in other studies [14]. While they can be strong motivators for an individual developer, in the long run, it is quite hard to maintain the same level of internal motivation if one is not rewarded. Still, the financial contributions are quite low to even popular software projects [24]. Although the situation has improved in the last several years, e.g., with the introduction of GitHub Sponsors [17] that allows individuals to support software development

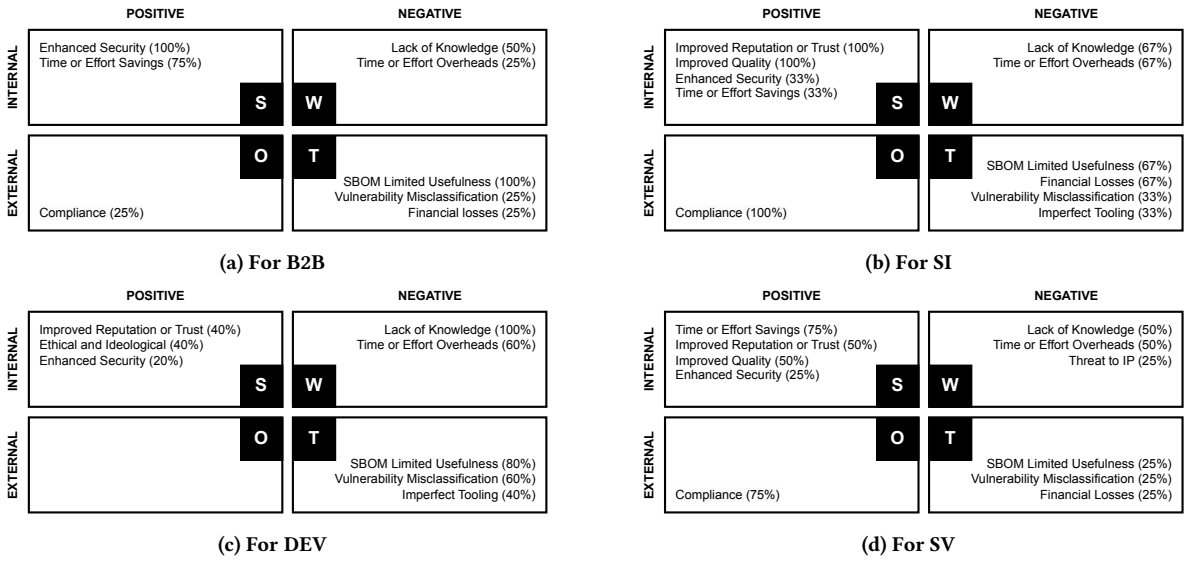

Figure 2: SWOT Diagrams

projects, the individual developers within our study still have not mentioned financial benefits among the incentives. This is not surprising because features like SBOM do not directly contribute to the core functionality of the software product to which people mostly donate. Moreover, developing the projects in their own time as a hobby, the individual developers also do not need to comply. At the same time, as we can see from Figure 2c, the implementation of SBOM would require additional investments due to **Lack of Knowledge** and **Time or Effort Overheads**, while the **SBOM Limited Usefulness** for the DEV stakeholders remains a concern. All these factors lead us to conclude that the DEV group is currently least interested in the SBOM adoption.

As we can see from our analysis, the main producing and consuming stakeholders, namely DEV and B2B groups correspondingly, are currently incentivized in SBOM adoption the least. The main business stakeholders who can drive SBOM adoption are SI and SV groups. Given that, one possible strategy to accelerate SBOM proliferation is to rely on these two driving groups. For instance, they can pay individual developers for an SBOM as for an additional feature or become sponsors of the projects. Thus, individual developers would be interested in investing their time and efforts into SBOM adoption. To accelerate SBOM adoption among the B2B stakeholders, in the initial stage, compliance might help. However, the main efforts should be aimed at showing the usefulness of SBOMs and making this technology usage much easier.

4 LIMITATIONS

One notable constraint of our study is the relatively small sample size of participants within each stakeholder group. A larger size would contribute to a better validity of our results and might even bring more insights (for instance, NTIA identifies more benefits for SBOM usage [30]). Nevertheless, since our study's objective is to comprehend the concerns and incentives surrounding SBOM adoption among stakeholders, even this sample size propels us toward our goal and introduces novel insights.

In addition to this evident limitation, another notable one is that, besides developers, there is a limited geographical distribution of the interviewees. Indeed, so as we start our search for participants among the customers of our partner and then go up across the stakeholder chains, this may affect the generalizability of findings, considering that perspectives on SBOM could vary across different countries, as pointed out by P6[SV], who highlights differences in vulnerability perception between Dutch and German stakeholders.

In our study, we specifically focused on open-source developers contributing to SBOM-related projects, but another important subgroup is the developers who work inside a company and need to produce an SBOM or operate with one from their supplier. Their perspectives could be different. The B2B participants solely comprised employees from organizations working in relatively critical sectors, characterized by more mature cybersecurity standards. This could have influenced their perceptions and may not fully encompass all B2B organizations. Additionally, the similarities in work activities among the interviewed SVs and SIs might have yielded different findings if we had included participants from other sectors.

Another limitation stems from the heterogeneity in participants' knowledge and understanding of SBOM. While the majority displayed a strong grasp of the subject, a few possessed limited or recently acquired knowledge. This discrepancy might have influenced their responses and perceptions, potentially impacting the generalizability of the findings. Acknowledging this limitation is imperative for a comprehensive interpretation of the study results.

The study also presents certain limitations concerning the methodology employed. Notably, the frequency analysis process lacked tracking the frequency of specific themes mentioned by each participant. Conducting this additional analysis could have provided deeper insights into the participants' perspectives and the relative significance they attributed to various SBOM-related themes.

A limitation emerges during the theme identification process, stemming from the main researcher's subjective interpretation of the dataset. Despite efforts to maintain rigor and comprehensiveness, theme identification inherently involves the main researcher's judgment and potential bias.

5 RELATED WORK

In this section, we analyze the contributions of our work and position our findings within the context of the related studies. We highlight novelties, which our study brought to the field, and known facts from the existing literature, which we confirmed in our work.

Our research and some of the findings align with those of other studies that also identified certain incentives and concerns regarding SBOM adoption. The closest to our work is that of Xia et al. [50], where the authors have analyzed the empirical data gathered by interviewing 17 participants and surveying 65 respondents. They establish a goal model that focuses on the quality of generation and the (un)clarity of consumption benefits, which is in line with our work. However, we delve into the differences between the concerns and incentives of the involved stakeholder groups. This allows us to understand the motivations and barriers attributed to particular stakeholder groups and how they promote or hinder SBOM adoption in general through network effects. Additionally, there is a difference in the method of conducting the interviews. While the authors [50] asked the interviewees to assess the provided factors using the Likert scale, we conducted our study in a semi-structured open-ended-questions manner, thus providing the participants more freedom to express their opinions.

The work of Zahan et al. [51] also closely relates to ours as they aim to promote widespread SBOM adoption by identifying challenges, presenting clear use cases, and providing guidelines. For their research, they employed a grey literature study approach. They found out that the main benefits of SBOM adoption include better dependencies, vulnerabilities, and risk management. Other researchers [13, 16, 25, 35] list them as major benefits. In our study, we draw similar conclusions, finding that the main benefits are transparency and better vulnerability management. Challenges identified by Zahan et al. [51], such as tool-related issues, value depreciation due to vulnerability issues, and the time-consuming nature of SBOM consumption, are also aligned with our findings.

In our work, the interviewees predominantly highlighted the risk posed by compromised software components, often attributable to deficient maintenance or support, with Log4j serving as a frequently cited exemplar. Moreover, a recurring risk encompassed the apprehension of absent or slow responsiveness to SSC attacks of this nature. These findings are in line with the research conducted by Xinyuan Wang [47] and Martínez and Durán [25]. Martínez and Durán [25] undertook an exploratory review of literature, governmental information, and reports pertinent to the SolarWinds case, culminating in a set of recommended best practices. The work of Wang [47] accentuates the severity of SSC attacks and dissects the prerequisites for their prevention, proposing an information flow-based detection paradigm for software customers.

Some other concerns identified in the related literature also resonate with our findings. Arora et al. [9] mention SBOM concerns related to a limited understanding of tools and IP. Phillips et al. [38] observe that the quality of SBOMs is challenging to ascertain, as they are often not detailed and complete. However, they also emphasize that even a partial SBOM is better than no SBOM. The work by Bi et al. [10] does not only consider governance a concern but even addresses the need for a governance phase for SBOM.

Stephen Hendrick from Linux Foundation [21] explored the state of SBOM adoption by surveying 412 companies. At the time of the study, 76% of the organizations identified that they already had some level of SBOM readiness, 88% would start using it in 2023. Interestingly, the results of our study, done at the beginning of 2023, show a different picture: 69% of our participants did not witness widespread adoption and perceived little demand from their customers or expressed demand to their suppliers for SBOM. Other researchers [9, 27, 50, 51] also confirm our findings that the SBOM adoption demand is low. It is not clear to us what the cause of such different results is.

In addition to SBOM, the research has also been conducted for other cybersecurity challenges, examining various costs and benefits per stakeholder and customer-supplier relationships. For instance, Gunson et al. [19] present valuable empirical evidence through a controlled experiment, illustrating the trade-off between security and usability. This study also investigates diverse costs and benefits from the perspectives of stakeholders as well as customer-supplier relationships. Furthermore, insights from the work of Viega and Michael [46] reveal that friction is not uncommon in supplier-customer relationships concerning security matters. For instance, some vendors have been known to self-report their own security posture inaccurately.

6 CONCLUSION

Modern software development heavily relies on external components, a trend illustrated by Martínez and Durán [25] who estimate that around 97% of commercial software products incorporate open-source components, and an even greater percentage might rely on proprietary software. These dependencies form a complex network that is often inadequately documented, thus creating blind spots in the security of the final software. To enhance software transparency, the industry proposed the Software Bill of Materials (SBOM) concept, providing developers with a facility to list the dependencies and describe their properties. Although SBOM offers significant potential, its adoption remains limited.

This study delves into reasons for low SBOM adoption among four business stakeholder groups. Through semi-structured interviews, we explored their incentives and concerns regarding SBOM adoption. Our analysis reveals that B2B customers and individual developers exhibit the least motivation, underscoring the responsibility of software vendors and integrators in driving the adoption. We conclude that the most crucial step in achieving this goal is to demonstrate the usefulness and simplify the use of SBOMs.

ACKNOWLEDGMENTS

We would like to thank Olga Gadyatskaya and Michel van Eeten for their feedback, which allowed us to improve the manuscript considerably. This work was partially supported by the Dutch Research Council (NWO) as part of the THESEUS project (NWA.1215.18.006).

REFERENCES

[1] [n. d.]. A distributed vulnerability database for Open Source. Retrieved 2023-08-14 from hhttps://osv.dev/

[2] 2021. Executive Order 14028: Improving the Nation's Cybersecurity. Retrieved 2023-08-18 from https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity

[3] 2023. Whisper: Robust Speech Recognition via Large-Scale Weak Supervision. Retrieved 2023-07-26 from https://github.com/openai/whisper

[4] Tom Alrich. 2022. The purl in your future. Retrieved 2023-07-30 from https://tomalrichblog.blogspot.com/2022/11/the-purl-in-your-future.html

[5] Tom Alrich. 2023. From the NVD to the IVD. Retrieved 2023-06-07 from https://tomalrichblog.blogspot.com/2023/05/from-nvd-to-ivd.html

[6] Tom Alrich. 2023. Is it time to abandon VEX? Retrieved 2023-08-14 from https://tomalrichblog.blogspot.com/2023/07/is-it-time-to-abandon-vex.html

[7] Tom Alrich. 2023. The problem with VEX documents. Retrieved 2023-07-12 from https://tomalrichblog.blogspot.com/2023/06/the-problem-with-vex-documents.html

[8] Tom Alrich. 2023. The Procurement use case for SBOMs. Retrieved 2023-08-01 from https://tomalrichblog.blogspot.com/2023/05/the-procurement-use-case-for-sboms.html

[9] Arushi Arora, Virginia L Wright, and Christina Garman. 2022. Strengthening the Security of Operational Technology: Understanding Contemporary Bill of Materials. *Journal of Critical Infrastructure Policy* 3, 1 (2022).

[10] Tingting Bi, Boming Xia, Zhenchang Xing, Qinghua Lu, and Liming Zhu. 2023. On the Way to SBOMs: Investigating Design Issues and Solutions in Practice. arXiv:2304.13261 [cs.SE]

[11] Virginia Braun and Victoria Clarke. 2006. Using Thematic Analysis in Psychology. *Qualitative Research in Psychology* 3, 2 (2006), 77–101.

[12] Alexandre Decan, Tom Mens, and Philippe Grosjean. 2019. An empirical comparison of dependency network evolution in seven software packaging ecosystems. *Empirical Software Engineering* 24, 1 (01 Feb 2019), 381–416.

[13] Shannon Leigh Eggers, Drew Christensen, Tori Brooke Simon, Baleigh Rae Morgan, and Ethan S Bauer. 2022. *Towards Software Bill of Materials in the Nuclear Industry.* Technical Report. Idaho National Laboratory (INL).

[14] Rishab A Ghosh, Ruediger Glott, Bernhard Krieger, and Gregorio Robles. 2002. Free/libre and open source software: Survey and Study. Part IV: Survey of developers. Retrieved 2023-08-14 from https://www.math.unipd.it/~bellio/FLOSS%20Final%20Report%20-%20Part%204%20-%20Survey%20of%20Developers.pdf

[15] Shmuel Gihon. 2023. What You Need to Know About the 3CX Supply Chain Attack. Retrieved 2023-07-26 from https://cyberint.com/blog/research/3cx-supply-chain-attack/

[16] Shubham Girdhar. 2022. *Identification of Software Bill of Materials in Container Images.* Master's thesis. Frankfurt University of Applied Sciences.

[17] GitHub. [n. d.]. GitHub Sponsors: Invest in the software that powers your world. Retrieved 2023-08-01 from https://github.com/sponsors

[18] Elias Groll and John Hewitt Jones. 2022. Software bills of material face long road to adoption. Retrieved 2023-08-18 from https://cyberscoop.com/dhs-sbom-adoption/

[19] Nancie Gunson, Diarmid Marshall, Hazel Morton, and Mervyn Jack. 2011. User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking. *Computers & Security* 30, 4 (2011), 208–220.

[20] Jessica Lyons Hardcastle. 2023. MOVEit Body Count Closes in on 400 Orgs, 20M+ Individuals. Retrieved 2023-07-26 from https://www.theregister.com/2023/07/20/moveit_victim_count/

[21] Stephen Hendrick. 2022. The State of Software Bill of Materials (SBOM) and Cybersecurity Readiness. Retrieved 2023-08-18 from https://www.linuxfoundation.org/research/the-state-of-software-bill-of-materials-sbom-and-cybersecurity-readiness

[22] Udo Kuckartz. 2019. *Qualitative Text Analysis: A Systematic Approach.* 181–197.

[23] Linux Foundation. [n. d.]. Software Package Data Exchange (SPDX). Retrieved 2023-08-14 from https://spdx.dev/

[24] Steve Marquess. 2014. Of Money, Responsibility, and Pride. Retrieved 2023-08-14 from http://veridicalsystems.com/blog/of-money-responsibility-and-pride/

[25] Jeferson Martínez and Javier M Durán. 2021. Software supply chain attacks, a threat to global cybersecurity: SolarWinds' case study. *International Journal of Safety and Security Engineering* 11, 5 (2021), 537–545.

[26] Caley McGillvary. 2022. Thematic Analysis: an Overview. Retrieved 2023-08-18 from https://getthematic.com/insights/thematic-analysis-overview/

[27] Anton Moroz. 2022. *Towards secure software development at Neste - a case study.* Master's thesis. University of Helsinki.

[28] Christine Namugenyi, Shastri L Nimmagadda, and Torsten Reiners. 2019. Design of a SWOT Analysis Model and its Evaluation in Diverse Digital Business Ecosystem Contexts. *Procedia Computer Science* 159 (2019), 1145–1154.

[29] National Institute of Standards and Technology. [n. d.]. National Vulnerability Database (NVD). Retrieved 2023-08-14 from https://nvd.nist.gov/

[30] National Telecommunications and Information Administration. 2019. Roles and Benefits for SBOM Across the Supply Chain. Retrieved 2023-07-20 from https://ntia.gov/sites/default/files/publications/ntia_sbom_use_cases_roles_benefits-nov2019_0.pdf

[31] National Telecommunications and Information Administration. 2021. Vulnerability-Exploitability eXchange (VEX) - An Overview. Retrieved 2023-08-14 from https://ntia.gov/sites/default/files/publications/vex_one-page_summary_0.pdf

[32] NTIA Formats and Tooling Working Group. 2021. Software Consumers Playbook: SBOM Acquisition, Management, and Use. Retrieved 2023-07-25 from https://ntia.gov/sites/default/files/publications/software_consumers_sbom_acquisition_management_and_use_-_final_0.pdf

[33] NTIA Formats and Tooling Working Group. 2021. Software Suppliers Playbook: SBOM Production and Provision. Retrieved 2023-07-25 from https://ntia.gov/sites/default/files/publications/software_suppliers_sbom_production_and_provision_-_final_0.pdf

[34] NTIA Multistakeholder Process on Software Component Transparency Framing Working Group. 2021. Software Identification Challenges and Guidance. Retrieved 2023-07-30 from https://ntia.gov/sites/default/files/publications/ntia_sbom_software_identity-2021mar30_0.pdf

[35] Chinenye Okafor, Taylor R. Schorlemmer, Santiago Torres-Arias, and James C. Davis. 2022. SoK: Analysis of Software Supply Chain Security by Establishing Secure Design Properties. In *ACM Workshop on Software Supply Chain Offensive Research and Ecosystem Defenses.* 15–24.

[36] OWASP. [n. d.]. OWASP CycloneDX Software Bill of Materials (SBOM) Standard. Retrieved 2023-08-14 from https://cyclonedx.org/

[37] Ivan Pashchenko, Henrik Plate, Serena Elisa Ponta, Antonino Sabetta, and Fabio Massacci. 2018. Vulnerable Open Source Dependencies: Counting Those That Matter. In *ACM/IEEE International Symposium on Empirical Software Engineering and Measurement.*

[38] Amas Phillips, Carsten Maple, Florian Lukavsky, Ian Pearson, Michael Richardson, Nigel Hanson, Paul Kearney, and Robert Dobson. 2023. Software Bills of Materials for IoT and OT devices. *IoT Security Foundation* (2023).

[39] Urša Reja, Katja Lozar Manfreda, Valentina Hlebec, and Vasja Vehovar. 2003. Open-ended vs. close-ended questions in web questionnaires. *Developments in applied statistics* 19, 1 (2003), 159–177.

[40] Paul Roberts. 2021. Log4j is why you need a software bill of materials (SBOM). Retrieved 2023-07-26 from https://www.reversinglabs.com/blog/log4j-is-why-you-need-an-sbom

[41] Ax Sharma. 2023. PyTorch discloses malicious dependency chain compromise over holidays. Retrieved 2023-08-01 from https://www.bleepingcomputer.com/news/security/pytorch-discloses-malicious-dependency-chain-compromise-over-holidays

[42] Trevor Stalnaker, Nathan Wintersgill, Oscar Chaparro, Massimiliano Di Penta, Daniel German, and Denys Poshyvanyk. 2024. BOMs Away! Inside the Minds of Stakeholders: A Comprehensive Study of Bills of Materials for Software Systems. In *IEEE/ACM 46th International Conference on Software Engineering.* 506–518.

[43] Danny Steed and Robert Black. 2023. MOVEit Hack: Attack on BBC and BA Offers Glimpse into the Future of Cybercrime. Retrieved 2023-07-26 from https://theconversation.com/moveit-hack-attack-on-bbc-and-ba-offers-glimpse-into-the-future-of-cybercrime-207670

[44] Eric Tooley and Courtney Claessens. 2023. Introducing self-service SBOMs. Retrieved 2023-08-11 from https://github.blog/2023-03-28-introducing-self-service-sboms/

[45] Viswanath Venkatesh. 2000. Determinants of perceived ease of use: Integrating control, intrinsic motivation, and emotion into the technology acceptance model. *Information systems research* 11, 4 (2000), 342–365.

[46] John Viega and James Bret Michael. 2021. Struggling With Supply-Chain Security. *Computer* 54, 7 (2021), 98–104.

[47] Xinyuan Wang. 2021. On the Feasibility of Detecting Software Supply Chain Attacks. In *IEEE Military Communications Conference.* 458–463.

[48] Heinz Weihrich. 1982. The TOWS matrix — A tool for situational analysis. *Long Range Planning* 15, 2 (1982), 54–66.

[49] Free Wortley, Chris Thompson, and Forrest Allison. 2021. Log4Shell: RCE 0-day exploit found in log4j, a popular Java logging package. Retrieved 2023-08-01 from https://www.lunasec.io/docs/blog/log4j-zero-day/

[50] Boming Xia, Tingting Bi, Zhenchang Xing, Qinghua Lu, and Liming Zhu. 2023. An Empirical Study on Software Bill of Materials: Where We Stand and the Road Ahead. In *IEEE/ACM International Conference on Software Engineering.* 2630–2642.

[51] Nusrat Zahan, Elizabeth Lin, Mahzabin Tamanna, William Enck, and Laurie Williams. 2023. Software Bills of Materials Are Required. Are We There Yet? *IEEE Security & Privacy* 21, 2 (2023), 82–88.

[52] Stan Zajdel, Diego Elias Costa, and Hafedh Mili. 2022. Open Source Software: An Approach to Controlling Usage and Risk in Application Ecosystems. In *ACM International Systems and Software Product Line Conference.* 154–163.

[53] Kim Zetter. 2023. The Untold Story of the Boldest Supply-Chain Hack Ever. Retrieved 2023-08-18 from https://www.wired.com/story/the-untold-story-of-solarwinds-the-boldest-supply-chain-hack-ever/

A RESEARCH PROTOCOL

A.1 Research Questions

Main Research Question

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

Research Sub-Questions

- SQ1: What are the stakeholder-specific incentives and concerns?
- SQ2: What factors impact the adoption of SBOM?

A.2 Collection of Empirical Data

Invitation and Explanation

The purpose of this research study is to gain insights into how the current set of incentives among the key stakeholders in the software supply chain inhibit the adoption of the Software Bill of Materials (SBOM). In this study, participants will be presented with open-ended questions that initially cover a broad range of topics and progressively focus on specific areas. The interview is estimated to take approximately 45-60 minutes to complete. Transcripts of the interviews will be anonymized. The data collected will be utilized for publication in academic repositories. The data will be stored for up to 2 years maximum. If data is published further, only anonymized summaries of interviews will be shared.

A.3 Interview Questions

Demographics

- **SV, SI & B2B**: What industry does your company operate in and what is your position within the company?
- **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?

Most Important Questions

- 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 concerns about SBOM or its technical capabilities, and if so, which ones?

More Specific Questions

- Do you think SBOMs are useful in managing and mitigating risks, and if so, what risks?
- **B2B**: Would you spend more on purchasing third-party software that comes with SBOM, and if so, what percentage/how much?
- **SV & SI**: Do you think you can pass on the cost of producing SBOMs to the customer?
- **B2B**: Is trust (e.g., reputation) an important factor in choosing a system integrator or software vendor to buy software, and why?
- **SV & SI**: Could customer trust (e.g., reputation) in you be an important factor in adopting a concept like SBOM?
- **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?
- **DEV, SV & SI**: Are there already "demand" signals from the customers?
- **B2B**: If you want it, does your company give off enough "demand" signals to suppliers?
- If you were to describe your sentiment regarding SBOM and its potential for success (negative, skeptical, neutral, optimistic or really positive), what would you choose?