

Software Bill of Materials (SBOM) and Cybersecurity Readiness

January 2022

Stephen Hendrick, *VP Research, The Linux Foundation*

With a foreword by Jim Zemlin, *Executive Director, The Linux Foundation*

In partnership with:



Contents

Foreword	4
Executive Summary	6
Introduction	8
Cybersecurity: A Worldwide Concern.....	8
Cybersecurity in the United States.....	9
SBOM Maturity.....	10
Demographics	11
SBOM Maturity by Geographic Region.....	11
SBOM Maturity by Enterprise Revenue.....	12
The Importance of Software Security	14
Relationship Between Open Source Maturity and SBOM Readiness	15
Are SBOM Innovators More Risk-prone in Their Use of Open Source Software?	15
Conditional Use of Open Source Software	16
Open Source Software Use Changes with SBOM Maturity	17
Key Concerns Regarding Software Security	18
Why Enterprises are Concerned about Software Security.....	19
The Impetus for Cybersecurity and SBOMs	20
U.S. Cybersecurity Executive Order Awareness and Actions.....	20
Cybersecurity and Software Supply Chain Priorities Emphasize SBOMs.....	21
SBOM Needs	24
Organizations Want SBOMs to Be Metadata Rich.....	24
Machine Readability Is a Key SBOM Requirement	25
SBOMs Should Identify Transitive Dependencies with Known Unknowns	25
SBOM Should Be Updated with Each Code Change	27
SBOM Metadata Should Be Bundled with the Component	27
SBOMs Should Reflect Vulnerabilities as They Are Found	27
SBOM Readiness and Segmentation by SBOM Maturity.....	28

Contents

- SBOM Production Perspectives.....30**
 - SBOM Production 30
 - SBOM Production Benefits.....31
 - SBOM Production Concerns..... 33

- SBOM Consumption Perspectives.....35**
 - SBOM Consumption..... 36
 - SBOM Consumption Benefits 36
 - SBOM Consumption Concerns..... 37

- Conclusions39**
 - How SBOMs Could Be Improved 39
 - The Importance of SBOMs.....41
 - The Future of SBOMs 42

- Methodology.....45**
 - Who We Surveyed and How We Analyzed the Data 45
 - Data Segmentation and Screening 45
 - Protecting Against Sample Bias 46
 - Respondent Ability to Answer SBOM Questions.....47

- Endnotes.....49**

- Appendix A: Demographics and Additional SBOM Readiness Information.....50**

- Disclaimer.....71**

Foreword

While open source communities continue to accelerate innovation in software, hardware, and standards, software cybersecurity concerns perennially capture our attention. Almost a year from the time of the disclosure of the SolarWinds Orion attack, 2021 would end with the fallout from another high-profile security crisis tied to Apache Log4j. However, open source has undeniably become a large attack vector and our communities and ecosystems need to work collectively on the standards, processes, education, and tooling to mitigate risks to global supply chains. While the year marked improvements in cybersecurity investment and compliance requirements, there remains much work to be done to harden the software supply chain, in terms of both prevention and response. It's not a problem exclusive to open source, but open source innovation has often led the way on solving collective problems, and this is not a problem any one organization can solve on its own.

To be clear, we are not where we were a year ago. Among the most important developments in the United States, with ripples felt by the global technology sector at large, was the Biden Administration's Executive Order on Improving the Nation's Cybersecurity. This bellwether indicator put Software Bills of Materials (SBOMs) at the forefront of software procurement practices. The United States was not alone, as other countries have discussed or are planning how to put in place similar requirements. Recognition of the importance of identifying software components to mitigate the damage created by software vulnerabilities has been an important milestone in global software security.

Fortunately, we already have the standards and tools to implement stronger software security practices throughout supply chains using SBOMs. SBOMs will play an essential role in building more trust and transparency in how all software is created, distributed, and consumed throughout supply chains. Last year we also saw the SPDX standard receive international recognition as ISO/IEC JTC1

5962:2021. Toolsets developed by SPDX and other communities are essential for adoption and industrialization of SBOMs. SPDX already plays an important role in software security and integrity across some of the world's largest commercial supply chains. Companies like Hitachi, Samsung, Microsoft, Intel, Cisco, Siemens, Google, and many more have already been producing and consuming SPDX SBOMs for years. We expect this to expand significantly in the coming years and hope to understand the challenges newcomers to the SBOM ecosystem face so that we can make it easier for them to adopt best practices.

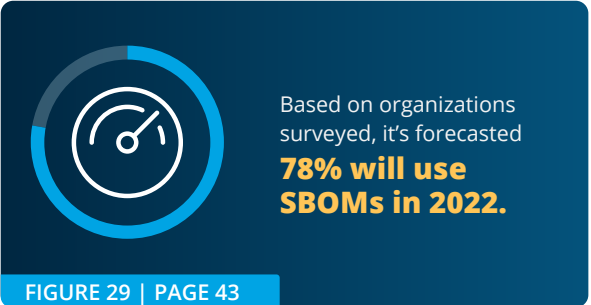
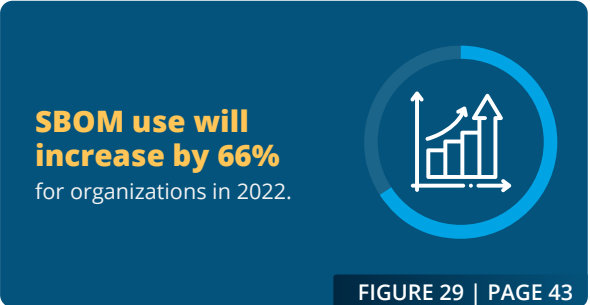
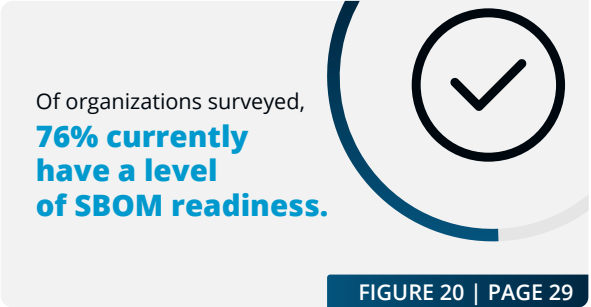
Beyond SBOMs, we've made investments in security-focused project communities. With the support of leading enterprises, we've expanded the Open Source Security Foundation (OpenSSF) to provide more tools, services, training, infrastructure, and resources to address cybersecurity vulnerabilities.

And, importantly, we've prioritized research to aid our collective understanding of the scope of cybersecurity challenges. The Linux Foundation launched the first in a series of core research projects to explore important issues related to implementing cybersecurity best practices and standards adoption, beginning with a survey of SBOM readiness. This report paints a clear picture of the current state of SBOM familiarity, adoption, and challenges as a means to inform and influence future collaboration efforts and implementation.

We hope that cybersecurity and IT professionals across the world will find the SBOM and Cybersecurity Readiness report informative. We encourage you to read it, share it with industry peers and supply chain partners, and make the necessary changes in your organizations to adopt SBOMs and other practices that prioritize cybersecurity.



Jim Zemlin Executive Director, *The Linux Foundation*



Executive Summary

A Software Bill of Materials (SBOM) is formal and machine-readable metadata that uniquely identifies a software component, its dependencies, and license data. SBOM data formats are evolving and are likely to soon provide information to verify component authenticity and provide a link to known vulnerabilities. SBOMs are designed to be shared across organizations and are particularly helpful at providing transparency of components delivered by participants in a software supply chain. Organizations concerned about software security are making SBOMs a cornerstone of their cybersecurity strategy.

Linux Foundation Research conducted worldwide empirical research into organizational SBOM readiness and adoption in the third quarter of 2021. A total of 412 organizations from around the world participated in a survey. The key results of that survey are presented throughout this report, with important findings from this study as follows:

1. 98% of organizations in this study are concerned about the security of their software and 72% are very or extremely concerned about software security. Concerns about software security are highest in Asia Pacific, where 35% of organizations are extremely concerned, compared to 21% of organizations in the Americas and 18% in EMEA (Europe, the Middle East, and Africa). **FIGURES: 1, A16.**
2. Security is the #1 priority that influences what software an organization will use. License compliance is the #2 priority. These priorities retain their respective positions each when second- and third-level priorities are considered. **FIGURE 5.**
3. The leading reasons why organizations are concerned about software security include financial risk (66%), reputational risk (61%), and legal risk (53%). These are potentially existential risks and explain the need for a coherent strategy to address software security. **FIGURE 10.**
4. The U.S. Executive Order on Improving the Nation's Cybersecurity is having a worldwide impact. Overall, more than 80% of organizations worldwide are aware of this White House executive order and 76% of organizations are considering changes as a consequence of this executive order. **FIGURES 11 AND 12.**
5. Key activities for securing the software supply chain emphasize SBOMs. Overall, 47% of organizations want scalable vulnerability reporting and 45% see SBOMs as a key method to secure the software supply chain. Additionally, 39% of organizations would like to see support for globally unique identifiers, and 34% back component verification through the use of reproducible builds. Component verification and vulnerability reporting are supported by some SBOM data formats today. Globally unique identifiers is a work in process supported by the leading data formats for package URLs (PURLs). Collectively, SBOMs today support a wide variety of activities for securing the software supply chain. **FIGURE 13.**
6. Across organizations in our sample, 90% of organizations have started their SBOM journey. Researchers found 10% of organizations have not begun any planning for SBOMs and 14% are in a planning or development phase. Survey participants revealed that 52% are addressing SBOMs in a few, some, or many areas of their business; 23% are addressing them across nearly all areas of their business or have standard practices that include the use of SBOMs. This means that overall, 76% of organizations have a degree of SBOM readiness. **FIGURE 20.**
7. SBOM production is most often associated with organizations who create commercial software, but our survey suggests they are being adopted far more widely. Across all organizations in our sample, only 7% have no plans to produce SBOMs. Another 40% are planning to produce

This landmark research, which surveyed IT vendors, service providers, and end users, provides an empirical view into software bill of materials (SBOM) readiness and adoption. This research shows that the use of open source software is widespread, and that software security is the #1 organizational priority. In the wake of worldwide efforts to address software security, SBOMs have emerged as a key enabler.

SBOM familiarity, readiness, and adoption is more extensive than anticipated. Familiarity with the SBOM term was 82%. SBOM readiness (actively engaged in addressing SBOM needs) was 76%. The production or consumption of SBOMs in at least a few segments of the business was 48% and 46%, respectively.

Based on organizational plans to produce or consume SBOMs, 47% of organizations are producing or consuming SBOMs in 2021. Growth of SBOM production or consumption is expected to accelerate by about 66% during 2022, leading to a SBOM production or consumption use by 78% or organizations. SBOM growth in 2023 is expected to trail off to 13%, with SBOM production or consumption use reaching 88% across organizations.

SBOMs in 6-24 months, 27% are producing them across a few, some, or many segments of their business. On the positive front, researchers found 21% are producing SBOMs across nearly all segments of their business or have standard practices that include their use. Overall, 48% of organizations are producing SBOMs to some extent today. **FIGURE 21.**

8. The top three benefits from producing SBOMs identified by our survey participants are: it is easier for developers to understand dependencies across components in an application (51%), it is easier to monitor components for vulnerabilities (49%), and it is easier to manage license compliance (44%). **FIGURE 22.**
9. Organizations remain concerned about how SBOM adoption and use will evolve. 40% are unclear about industry commitment to SBOMs, 39% question whether there is industry consensus around what an SBOM should contain, and 37% are unclear on the value that SBOMs provide to their customers. Herein lies a dichotomy in the SBOM market: There is significant operational involvement in SBOMs, but a lesser degree of commitment. **FIGURE 23.**

10. SBOM consumption mirrors SBOM production. Just 6% of organizations have no plans to consume SBOMs. 42% plan to consume SBOMs in the next 6-24 months, 28% are consuming SBOMs across a few, some, or many segments of their business, and 18% are consuming SBOMs across nearly all segments of their business or have standard practices that include the use of SBOMs. Overall, 46% of organizations are consuming SBOMs to some extent today. **FIGURE 24.**
11. SBOM consumption benefits are compelling. 53% of organizations report that SBOMs provide a better approach to addressing reporting and compliance requirements. 53% also say that SBOM information improves risk-based decision-making, and 49% said SBOM vulnerability reporting enables organizations to more immediately understand security exposures. These consumption benefits are well aligned with production benefits that echoed the same values: addressing compliance requirements ties back to managing license compliance, improving risk-based decision-making and security exposures tie back to clarity around dependencies and monitoring components for vulnerabilities. **FIGURE 25.**
12. Additional industry consensus will help improve SBOM adoption and implementation. 62% of organizations are looking for better industry consensus on how to integrate the production/consumption of SBOMs into their DevOps practice, 58% want consensus on integration SBOMs into their risk and compliance processes, and 53% want industry consensus on how SBOMs will evolve and improve. **FIGURE 27.**

SBOM readiness, production, and consumptions across industries and organizations is in the process of being operationalized. There are solutions emerging, but industry-wide practitioner consensus has yet to consolidate around a particular methodology, format, and tooling workflow. Highly visible support by the software and services vendor community would serve as a key accelerator of growth and validate the role of SBOMs in securing the software supply chain.

Introduction

Much of the digital transformation occurring is focused on enterprises positioning themselves to better address business process improvement, automation, and resource accounting, and to increase productivity. The opportunities presented by a digital economy include the ability to pursue new business models and access new customer segments and revenue streams. In many cases, industry leaders have transformed to “software-defined” models, enabled by cloud computing, edge computing, artificial intelligence software, and embedded systems. Along with this digital transformation opportunity comes increasing cybersecurity risk if software assets are not sourced and managed appropriately.

Cybersecurity: A Worldwide Concern

Cybersecurity is a worldwide concern. While the SolarWinds attack was against a U.S. company, its customers at the time numbered more than 300,000 across 190 countries, and 38% of its revenue originated from outside the United States. This makes the scope of the SolarWinds attack truly worldwide, and points to the increasing sophistication of the cybercriminal activities of nation-states and non-government actors. Cybersecurity attacks have a wide variety of goals. While most attacks can be classified as financial crimes, the more sophisticated attacks can have political, industrial, economic, or influence-oriented objectives.

Although the U.S. is responsible for 24% of the worldwide GDP, the share of GDP by region is more evenly distributed.¹ The share of GDP for the Americas is 32%, compared to 30% for Europe, the Middle East, and Africa (EMEA) and 38% for Asia Pacific. The distribution of worldwide GDP by region correlates well with the level of concern expressed regionally about software security. **FIGURE 1** shows the level of concern that organizations have about the security of the software they use. The Americas and EMEA show a distribution of concerns that peaks at 49% for the Americas and

55% for EMEA being “very concerned.” These distributions are roughly normally distributed, with about 20% of the Americas and EMEA being either “concerned” or “extremely concerned.”

The European Union (EU) has been increasing its cybersecurity footprint over the last decade. The General Data Protection Regulation (GDPR) was adopted by the EU back in 2014 and became an enforceable regulation in 2016. GDPR was designed to provide people with a high degree of control over their personal information (PI) and establish requirements for how PI could be processed. Building on this are the Directive on Security of Network and Information Systems (NIS Directive) and EU Cybersecurity Act in 2019. The NIS Directive requires digital service providers to proactively manage risk and increases national capabilities around addressing cybersecurity incidents. The EU Cybersecurity Act identifies regulations for certifying digital products, processes, and services.

The distribution for Asia Pacific in **FIGURE 1** is significantly different from that of the Americas or EMEA. Security concerns in Asia Pacific gradually ramp up, with 15% “slightly concerned,” 18% “concerned,” 31% “very concerned,” and 35% “extremely concerned.” There are nearly twice as many organizations in Asia Pacific that are “extremely concerned” compared to EMEA, and 67% more than in the Americas. The reason why the level of software security angst is higher in Asia Pacific is explained throughout this report; it appears due to Asia Pacific having invested less to date in security-related roles, functions, and activities.²

China has likewise been improving its posture on cybersecurity, beginning with 2017’s Cybersecurity Law, which regulated IT service providers and how they handled PI. This regulation was followed by the 2021 Data Security Law, which implemented tighter government-focused regulations of “national core data.”

As of November 2021, China enacted a new Personal Information Protection Law (PIPL) that provides the government with more leverage over technology companies while also incrementally improving PI requirements.

Taken together with the recent May 2021 U.S. executive order, there is clearly a worldwide sea change occurring in software security and cybersecurity. The protection of PI is clearly one dimension, but the protection of digital assets in the form of software products, processes, and services is clearly also of critical importance.

Cybersecurity in the United States

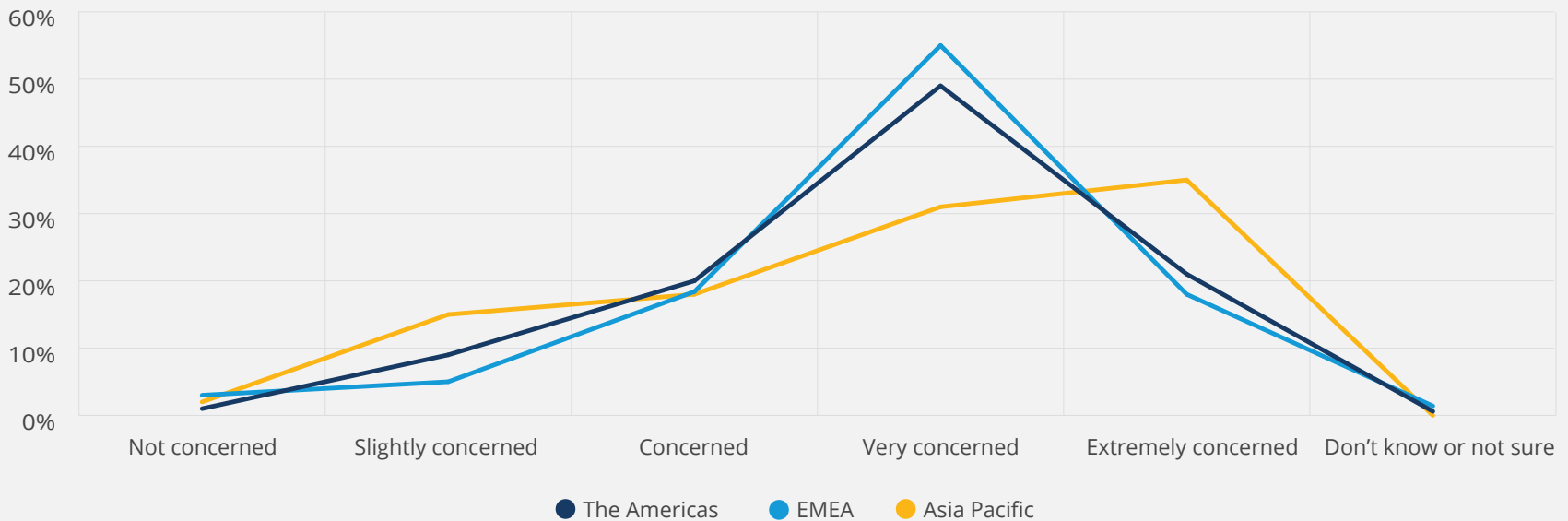
Cybersecurity issues have become so acute that in the United States, the White House issued an executive order (EO) on improving the nation's cybersecurity in May 2021.³ The rationale for this EO was the "increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy."⁴ The EO focuses on the following seven areas:

1. Removing barriers to sharing threat information
2. Modernizing the federal government's cybersecurity

FIGURE 1

How concerned is your organization about the security of the software that it uses?

Single Response | N = 341



3. Enhancing software supply chain transparency and security
4. Establishing a cyber safety review board
5. Standardizing how the federal government responds to cybersecurity vulnerabilities and incidents
6. Improving detection of cybersecurity vulnerabilities and incidents on federal government networks
7. Improving the federal government's investigative and remediation capabilities

This issue is not limited to the United States, nor is the United States the only country allocating resources to improve cybersecurity. Enhancing software supply chain transparency and security is of critical importance because the U.S. federal government as well as virtually every public-sector and private enterprise around the world relies on critical software to support business- and mission-critical activities. As defined by the EO, critical software is software that performs functions critical to trust, such as affording or requiring elevated system privileges or direct access to networking and computing resources. Addressing software supply chain security involves a host of activities, such as:

- Securing development environments
- Employing tools that check for known and potential vulnerabilities in included software components and remediate them
- Maintaining accurate and up-to-date data and provenance of code going into software products
- Providing purchasers with a software bill of materials (SBOM) for each software product

A software bill of materials is an effective way to address several of these needs, especially those focused on understanding vulnerabilities, license obligations, and provenance of software-based products. Producing and consuming SBOMs is therefore viewed as an effective way to address a variety of trust issues across all types of software products, including both open and closed source

components. The benefits of SBOMs, as identified by the National Telecommunications and Information Administration (NTIA), are as follows:

- Reduced cost
- Less security risk
- Reduced license risk
- Decreased compliance risk

SBOM use cases included improved software development, supply chain management, vulnerability management, asset management, procurement, and high assurance processes.⁵

Technology vendors, solution and service providers, and industry organizations are all taking this EO seriously. The central role of SBOMs in addressing software supply chain security was a key catalyst for this research. This research sought to answer the question, "How ready are organizations for SBOM requirements and the cybersecurity practices necessary to implement them?"

SBOM Maturity

This report talks extensively about SBOM readiness as well as the level of SBOM production and consumption. These questions were designed to identify where organizations are in their SBOM journey, ranging from no interest to planning to various stages of adoption. Because SBOM readiness was the best overall identification of SBOM adoption, we consolidated responses to this question into three categories: SBOM procrastinators, SBOM early adopters, and SBOM innovators. Respondents self-selected the category they were reported under. For details on how these categories mapped to SBOM readiness responses, see the Methodology section of this report.

Demographics

Selected survey demographics are shown in this section. The remaining demographics are found in Appendix A. The demographics discussed in this section help provide an understanding of who we surveyed, organizational size and revenue, roles, and industry. **FIGURE 2** summarizes this information.

FIGURE 2 shows that the SBOM readiness survey was worldwide, involved enterprises of all sizes and revenues, focused primarily on senior information technology (IT) roles, and cut across many vertical industries. There was strong representation across

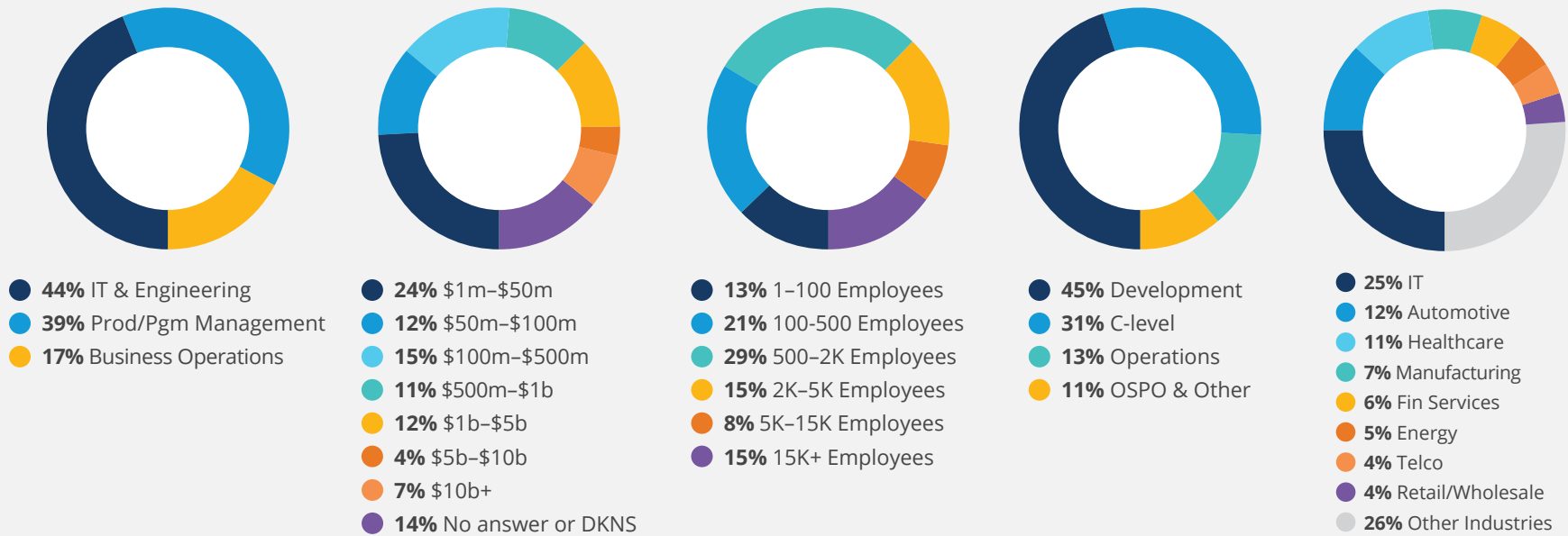
enterprises in information technology, automotive, healthcare and life sciences, manufacturing, financial services, and energy.

SBOM Maturity by Geographic Region

Each geographic region is uniquely profiled when it comes to SBOM maturity. **FIGURE 3** shows the three primary geographic regions segmented by SBOM maturity. SBOM innovators made a strong showing in the Americas and Asia Pacific. In the Americas, where 90% of the responses came from North America, the

FIGURE 2
Summary level demographics

N = 412



relative percent of SBOM innovators in North America was the same as the rest of the Americas (Mexico, Central, and South America).

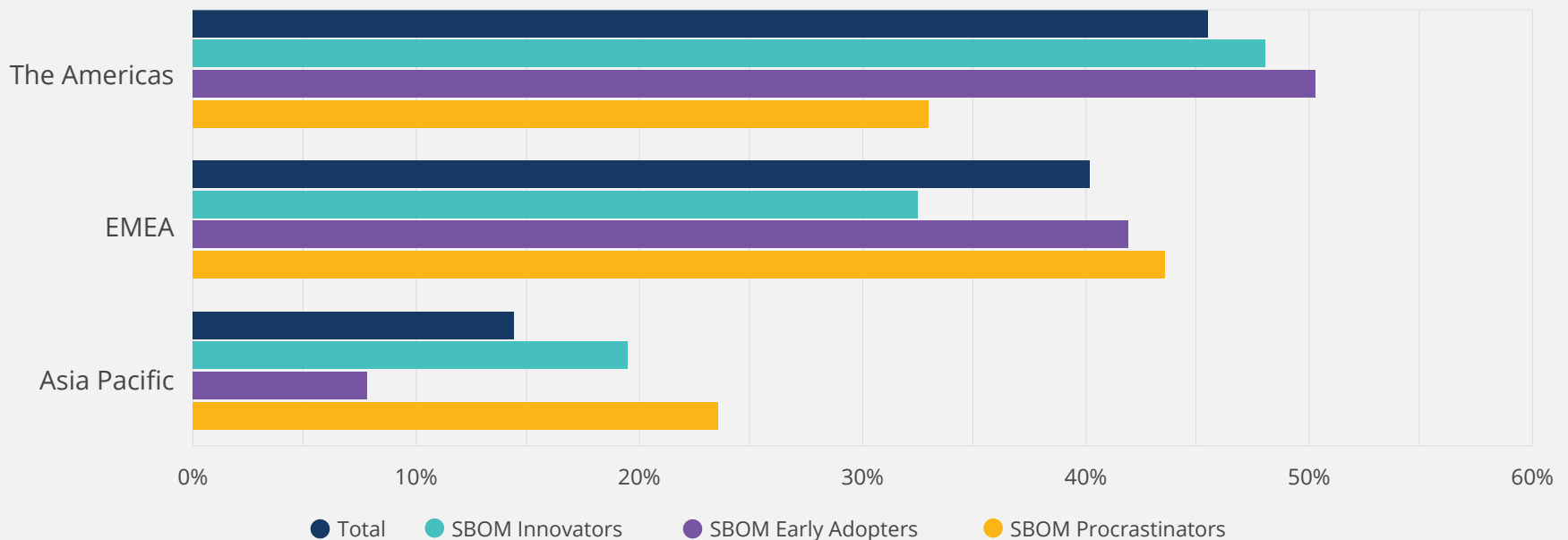
Asia Pacific saw the greatest number of SBOM innovators on a proportional basis, with strong showings by India and other Asia-Pacific countries, including Australia and Singapore. However, Asia Pacific is also characterized by a bimodal distribution where the majority of respondents were either SBOM innovators or procrastinators. This characteristic was especially true for China, Russia, and other Asia-Pacific countries.

EMEA proportionately has the fewest number of SBOM innovators, but matches the Americas in relative terms based on the size of its SBOM early adopters.

SBOM Maturity by Enterprise Revenue

The survey sample contains a large number of smaller enterprises, as well as a surprising number of very large enterprises. Overall, 51% of the sample had annual revenue of less than \$500 million, and 11% of the sample showed revenue greater than \$5 billion (14% of the sample were not sure of their corporate

FIGURE 3
What geographic region do you live in?
Single Response | Segmented by SBOM maturity | N = 341



revenues or preferred not to answer). Additionally, 63% of the sample involved enterprises with fewer than 2,000 employees and 15% of the sample included companies with 15,000 or more employees.

Given the wide variety of enterprises in the survey, we wanted to understand if enterprise size and revenue had a bearing on SBOM maturity. Our hypothesis was that as the size of the enterprise and revenue of the enterprise increased, so would their SBOM maturity. Larger companies will likely have more complex product portfolios, a larger investment in IT, and a greater need to improve software supply chain issues. **FIGURE 4** shows average annual revenue by SBOM maturity.

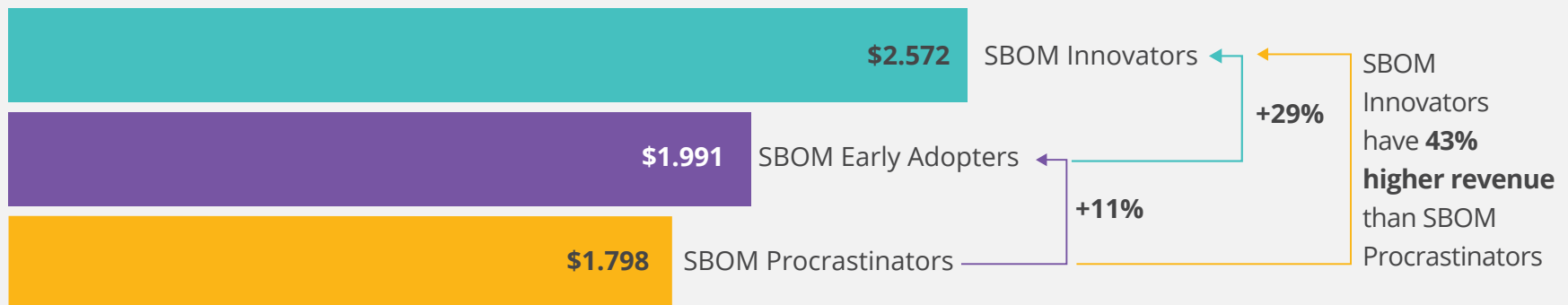
The findings supported our hypothesis, but not as dramatically as we expected. The reason for this is that there are three orders of magnitude built into the revenue classifications, so even a small percentage of respondents with revenue in the billions will dwarf the contribution of those respondents with revenues in the millions. While there clearly was a progression in the revenue

Larger enterprises have more to gain and more to lose than small or medium enterprises, whose scale and IT priorities make SBOM production/consumption nice to have, but something to be addressed later.

distributions by SBOM maturity, it was most apparent once revenues were over \$250 million.

What this does tell us is that large and very large enterprises are primarily driving the SBOM agenda. This makes sense, because larger enterprises have more to gain and more to lose than small or medium enterprises, whose scale and IT priorities make SBOM production/consumption nice to have, but something to be addressed later.

FIGURE 4
Average Annual Revenue (\$B)
Segmented by SBOM maturity | N = 341



The Importance of Software Security

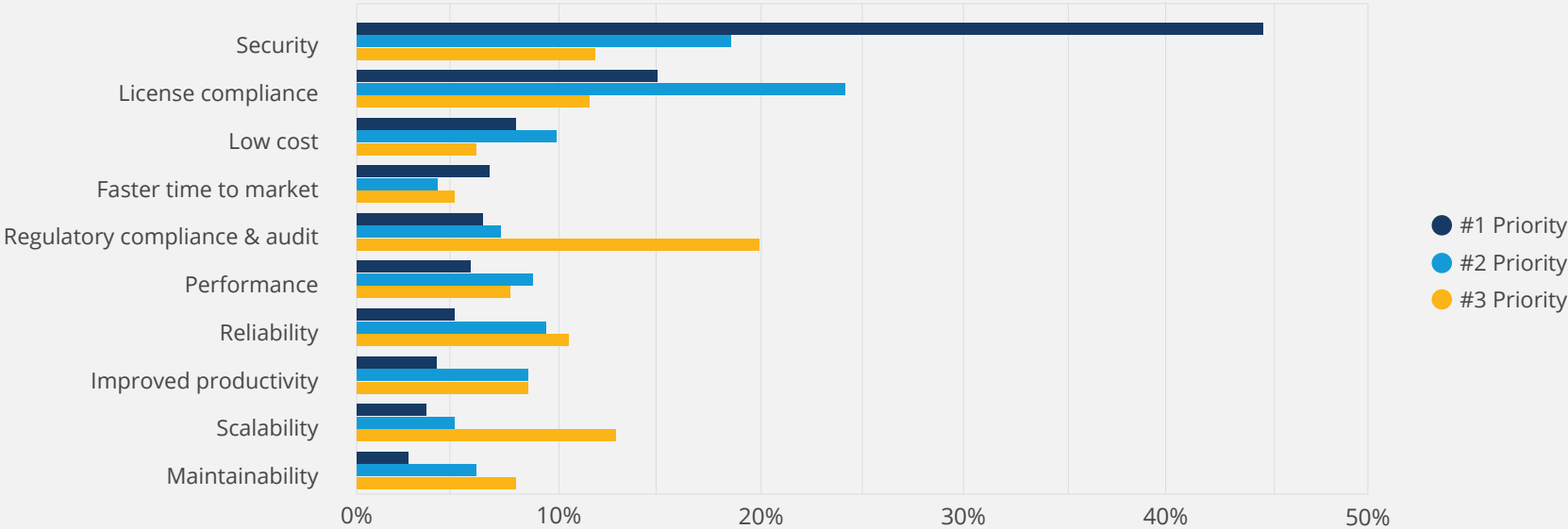
In order to establish where security ranked relative to a variety of enterprise priorities, we asked respondents to rank order 10 IT objectives. **FIGURE 5** shows the top three ranked results of this question sorted in descending order by the #1 ranked priority. Security was not only the #1 priority, at 45%, but it was also three times more important to organizations than second-ranked first choice, which was license compliance, at 15%.

Security's importance is clear, given that it remains the top-ranked IT objective based on the cumulative addition of incremental rankings. License compliance remains the second-ranked IT objective when first and second choices are considered, and its

strong second-choice status enables it to gain ground on security and pull away from the #3 ranked objective, which was low cost. Regulatory compliance, which was ranked fifth among first-ranked choices, improved its standing based on a very strong third choice showing, moving it up to the #3 priority overall.

The importance attached to security and compliance (license, regulatory, and audit) relative to a wide variety of IT objectives that traditionally perform well in comparisons like this means that security and the financial risks now associated with GRC (governance, risk and compliance) have grown significant enough to make these high-priority issues.

FIGURE 5
Rank order the priorities below that most often influence what software your organization chooses to use.



Relationship Between Open Source Maturity and SBOM Readiness

With open source being such a pervasive part of application development and operations, it is important to look at the relationship between SBOM maturity in the use of open source software. The following four questions and figures explore the similarities and differences in how enterprises approach SBOM maturity based on their use of open source software.

Are SBOM Innovators More Risk-prone in Their Use of Open Source Software?

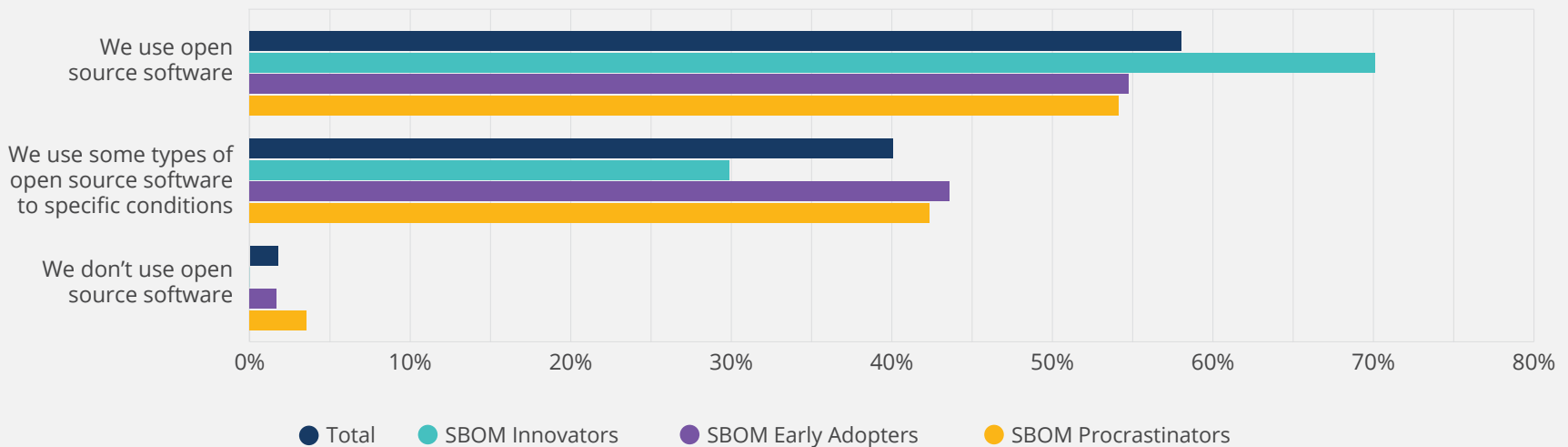
At first glance, **FIGURE 6** makes it clear that the use of open source software is pervasive. Overall, 98% of our sample uses open

source software. The difference in how enterprises use open source software is based on the conditions that they attach to its use. 58% of the overall sample use open source software much the way they would use closed source software, based on need, capabilities, and cost. However, 40% of the overall sample use open source software subject to specific conditions. Presumably, these conditions are in place to ensure that the software meets or exceeds internal requirements designed to mitigate risk.

With the exception of SBOM innovators, the segmentation view by SBOM maturity is nearly perfectly aligned with the characteristics of the overall sample—except that SBOM innovators have a

FIGURE 6
What is your organization's perspective on using open source software?

Single Response | Segmented by SBOM maturity | N = 341



higher propensity to use open source software without conditions. Because SBOM innovators are largely using SBOMs as part of their standard practices, we would presume that the automated use of SBOMs ensures that many key concerns regarding licensing and security are being addressed. SBOM innovators are not risk-prone; they simply have a more comprehensive and sophisticated culture around the use of open source software.

Conditional Use of Open Source Software

For those respondents that said they would use open source software subject to specific conditions, a multiple response follow-up question was asked to understand under what conditions their

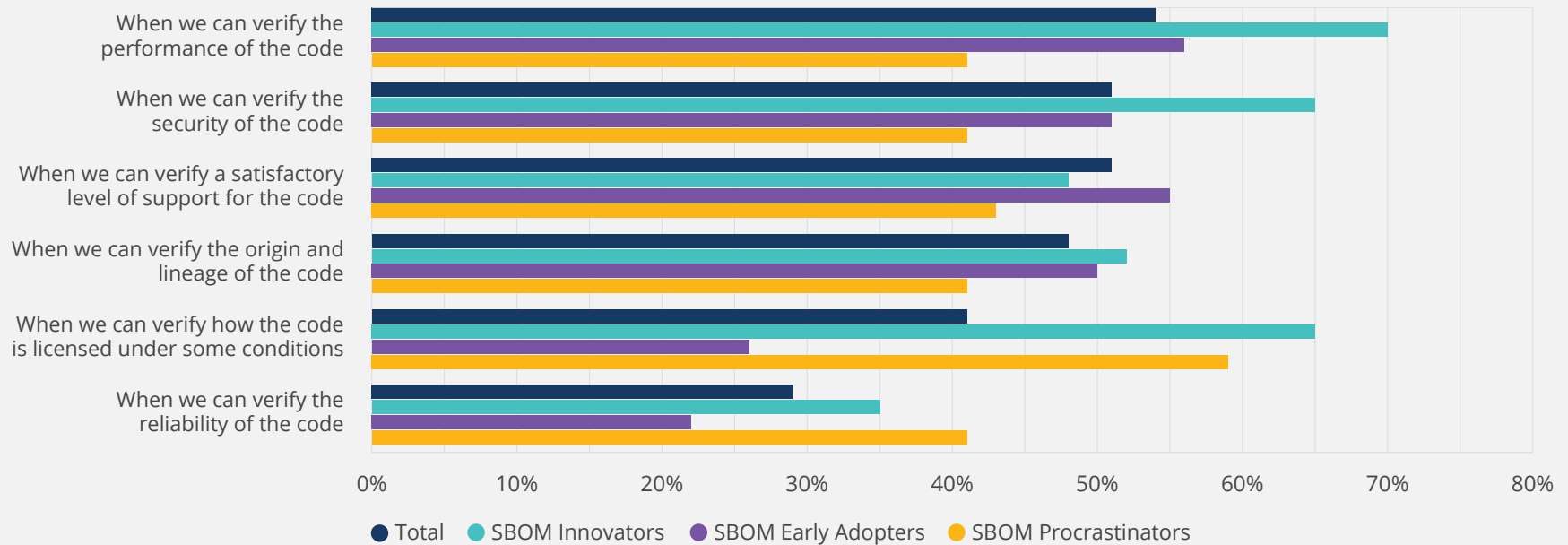
organization would use open source software. **FIGURE 7** shows that the overall findings included verifying code performance (54%), verifying code security (51%), verifying appropriate code support (51%), verifying code provenance (48%), and verifying code licensing (41%).

The overall finding in **FIGURE 7** is that organizations who use open source software subject to specific criteria are interested in vetting this software in all of the ways described. SBOMs are effective at addressing three of these criteria: security (vulnerabilities), provenance (origin and lineage), and licensing. The importance of validating performance, technical support, and reliability of open source code is also important, but requires the consuming organization to test components thoughtfully.

FIGURE 7

Under what conditions will your organization use open source software?

Select all that apply | Segmented by SBOM maturity | N = 138, Valid Cases = 138, Total Mentions = 381



Segmenting the data by SBOM maturity showed only a few differences from the overall findings. SBOM innovators showed a strong focus on verifying code performance (70%), verifying code security (65%), and verifying code licensing (65%). These three issues are clear priorities for SBOM innovators.

SBOM early adopters are largely in step with the overall totals for issues related to performance, security, support, and provenance. The only difference comes in code licensing, which only attracted 26% of SBOM early adopters, compared to 41% of the overall sample.

SBOM procrastinators are distinctive in their concern about everything. While licensing at 59% stands out, SBOM procrastinators appear to have a higher level of anxiety about using open source, which correlates with the lower level of investment they have made in developing open source policy.

Open Source Software Use Changes with SBOM Maturity

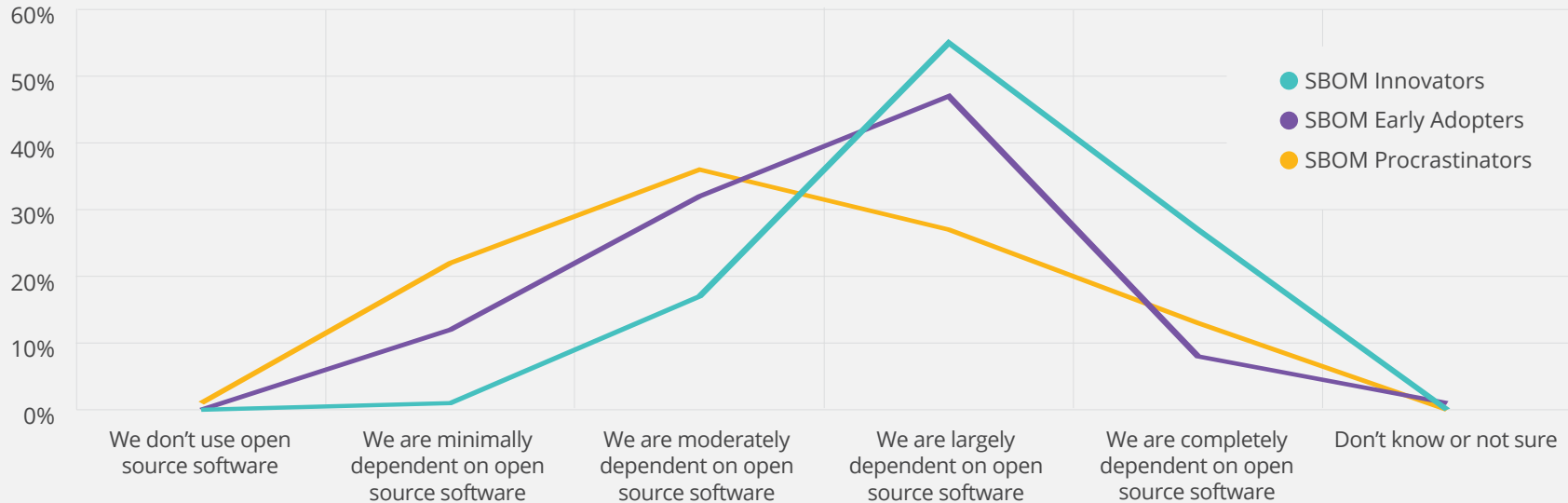
FIGURE 8 shows that open source software is used pervasively. But just how dependent are enterprises on open source software, and how does this dependency change based on SBOM maturity? FIGURE 8 provides insight into the degree to which enterprises are dependent on open source software segmented by SBOM maturity. The distributions in FIGURE 8 simply reflect a more continuous way to show the distribution of responses by SBOM maturity level and provide some additional visual insight into the shape of these distributions.

The distribution for SBOM procrastinators peaks at 36% with a moderate dependency on open source software. The distributions for SBOM early adopters (47%) and innovators (55%) have peaks showing a large dependency on open source software.

FIGURE 8

How dependent is your organization on open source software?

Single Response | Segmented by SBOM maturity | N = 341



SBOM innovators are the only segment with a material number of respondents who claim to be completely dependent on open source software, at 27%.

Key Concerns Regarding Software Security

Concerns about the security of the software that is being used were nearly unanimous across our sample. **FIGURE 9** shows that 91% of the overall sample was either concerned, very concerned, or extremely concerned about the security of software that their organization uses. Adding the 8% of enterprises that were slightly concerned brings the total to 99%.

FIGURE 9 is also segmented by SBOM maturity and while there are some differences in comparing distributions, the surprise was that

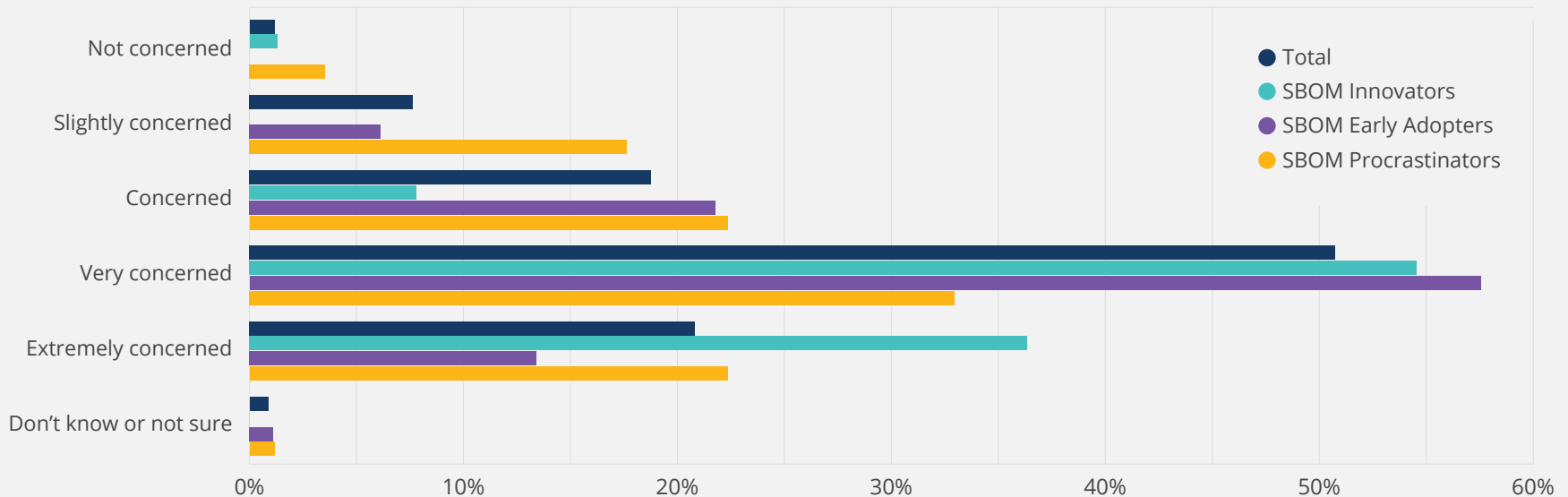
18% of SBOM procrastinators were slightly concerned about software security and 4% were not concerned. The 18% of SBOM procrastinators who were slightly concerned about software security is characterized by enterprises having between 1 to 99 employees and less than \$1 million in revenue. These enterprises were more focused on survival and growth and are not yet in a position to prioritize software security.

SBOM maturity is well correlated with concerns about software security. Comparing across segments, 99% of SBOM innovators were either extremely concerned, very concerned, or concerned about software security, which contrasts with 93% of SBOM early adopters, and just 77% of SBOM procrastinators. The net is that there is consensus that software security remains a significant problem.

FIGURE 9

How concerned is your organization about the security of the software that it uses?

Single Response | Segmented by SBOM maturity | N = 341



Why Enterprises are Concerned about Software Security

The natural follow-on to the prior question is why are organizations concerned about software security? FIGURE 10 shows overall that 66% of the sample is concerned about financial risk, 61% about reputational risk, 53% about legal risk, 40% about unauthorized access to customer systems, and 31% about unauthorized access to their own systems.

A segmentation by SBOM maturity as some additional color to these findings. While most segment responses performed very close to the overall sample, there are two notable exceptions.

The first is that SBOM innovators have a higher level of concern

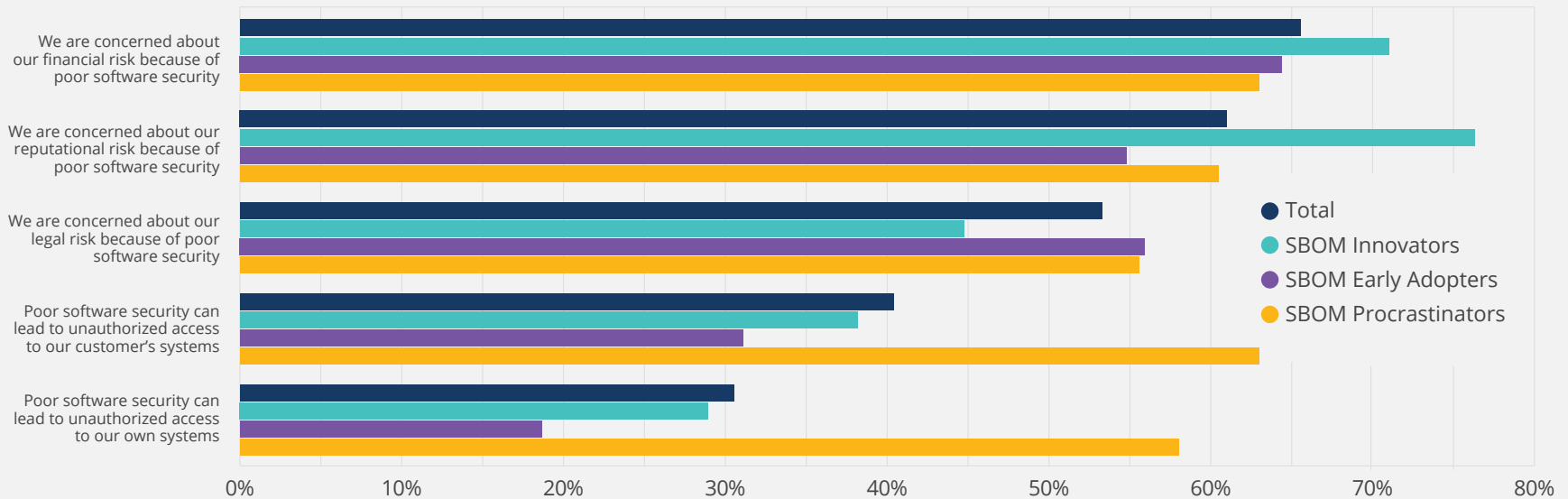
about financial risk (71%) and especially reputational risk (76%) than the overall sample, and slightly less concern about other issues. Our belief is that SBOM innovators, because of their longer tenure in software security, have largely addressed first-order issues such as unauthorized access and legal risk. However, financial risk and reputational risk are second-order security concerns that require more complex solutions.

The other exception is that SBOM procrastinators are tremendously concerned about unauthorized access, either to their customer's systems (63%) or their own systems (58%). These first-order security concerns do not generate nearly as much anxiety for SBOM innovators and the early adopters, presumably because these issues have already largely been addressed.

FIGURE 10

Why is your organization concerned about software security?

Select all that apply | Segmented by SBOM maturity | N = 334, Valid Cases = 334, Total Mentions = 840



The Impetus for Cybersecurity and SBOMs

The May 12, 2021, Executive Order on Improving the Nation's Cybersecurity by President Biden defined tight time frames for developing rules and guidance on cybersecurity requirements. A requirement of the executive order was for the National Telecommunications and Information Administration (NTIA) to publish minimum requirements for an SBOM. The Department of Commerce, in conjunction with NTIA, published the minimum requirements for SBOM in July 2021.⁶ A second draft of this report, titled "Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations," was published by the National Institute of Standards and Technology (NIST) in October 2021.⁷ These documents provide a window into how the U.S. government intends to improve software supply chain security.

The NTIA publication defines an SBOM as "a formal record containing the details and supply chain relationships of various components used in building software." This document further describes the value proposition of an SBOM as follows: "SBOM provides those who produce, purchase, and operate software with information that enhances their understanding of the supply chain, which enables multiple benefits, most notably the potential to track known and newly emerged vulnerabilities and risks. SBOMs will not solve all software security problems but will form a foundational data layer on which further security tools, practices, and assurances can be built." The NTIA document and appendix F of the NIST document are required reading for vendors and end-user enterprises who are or will be involved with SBOMs.

The cybersecurity executive order will be a catalyst for action in the SBOM market. Although the term *market* may be a bit premature, the level of familiarity and readiness with SBOMs, combined with ISO standards for formatting SBOMs, is creating a demand for SBOM tools.

The cybersecurity executive order will be a catalyst for action in the SBOM market. Although the term *market* may be a bit premature, the level of familiarity and readiness with SBOMs, combined with ISO standards for formatting SBOMs, is creating a demand for SBOM tools.

U.S. Cybersecurity Executive Order Awareness and Actions

The U.S. executive order was designed to increase cybersecurity awareness and accelerate the development and use of products, processes, and best practices to improve software security. To understand the impact of this executive order, we asked about organizational awareness and a follow-up question on changes as a result of this executive order. **FIGURE 11** shows that overall, 84% of the sample was aware of the executive order, 11% were not, and 5% were not sure. Awareness of the executive order did vary by geographic region (not shown). Awareness in the Americas was 86%, followed by EMEA at 79% and Asia Pacific at 64%.

FIGURE 11 also shows executive order awareness by SBOM maturity. Unsurprisingly, SBOM innovators show the highest awareness, at 97%, followed by SBOM early adopters, at 91%, and SBOM procrastinators at 56%.

Awareness is a prerequisite to making changes. **FIGURE 12** shows that overall, 77% of enterprises are considering making changes in response to the executive order, 13% are not, 6% prefer not to answer, and 4% are not sure. The segmentation by SBOM maturity

in **FIGURE 12** doesn't identify any significant differences among groups considering changes in response to the executive order.

However, the high level of awareness shown in **FIGURE 11** combined with the 77% who were considering changes in **FIGURE 12** suggest that the executive order is achieving its intended results, which is to drive improvement in cybersecurity across the public and private sectors.

Cybersecurity and Software Supply Chain Priorities Emphasize SBOMs

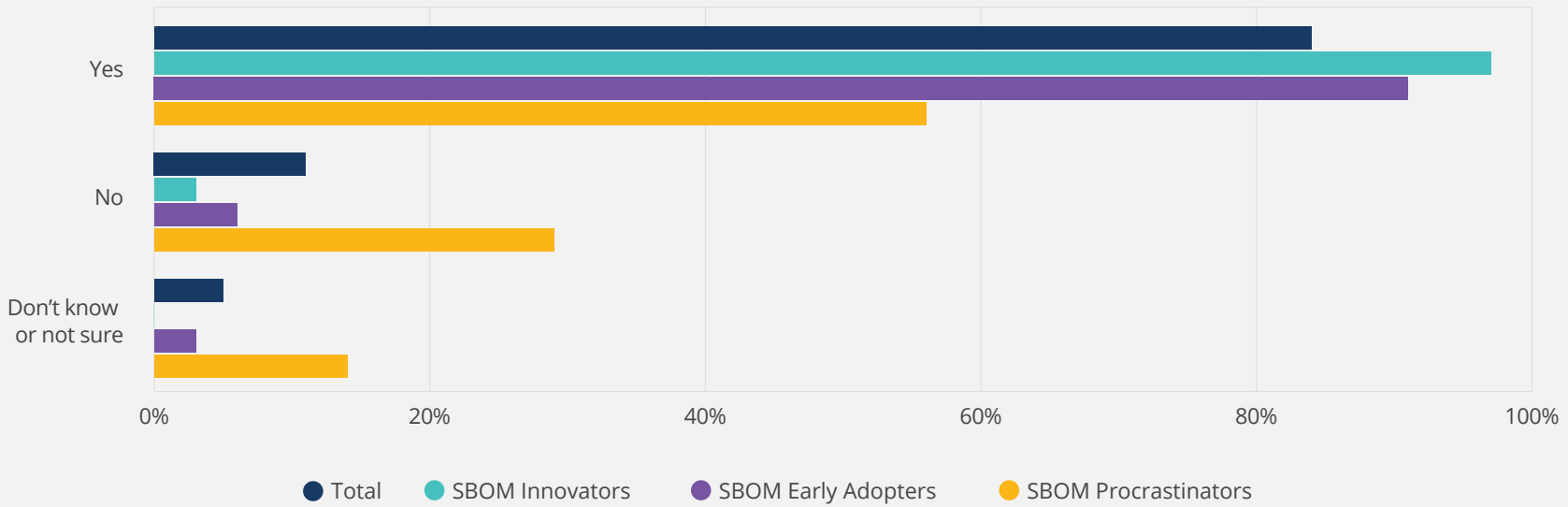
When asked to identify key activities for securing the software supply chain, SBOMs address a wide variety of needs. **FIGURE 13**

shows that overall, 47% of the sample identified vulnerability reporting systems as the leading activity for securing the supply chain. Currently SCA tools are the preferred choice for identifying vulnerabilities and license compliance in open source software. SBOMs have the ability to identify dependencies, and they could eventually include information on known vulnerabilities. However, the challenge with vulnerabilities is to understand which ones are exploitable and how to keep this information up-to-date. While SBOMs don't yet support the identification of vulnerabilities, it seems like a logical capability that should be shortlisted.

The overall finding in **FIGURE 13** is that SBOMs are perceived as an essential way to enable the security of the software supply chain.

FIGURE 11
Is your organization aware of the recent US Executive Order on Cybersecurity that mentions a software bill of materials?

Single Response | Segmented by SBOM maturity | N = 341



SBOM innovators communicated the importance of SBOM convincingly, and their experience in using SBOMs provides a trusted confirmation of SBOM value.

Use of SBOMs was the second-ranked activity for securing the software supply chain. On an overall basis, 45% of respondents identified SBOMs, and this included 65% of SBOM innovators, 39% of SBOM early adopters, and 37% of SBOM procrastinators. This is a strong endorsement of SBOMs and is being driven by the ability of SBOMs to define the component's provenance, licensing, and dependencies, and provide cryptographic information.

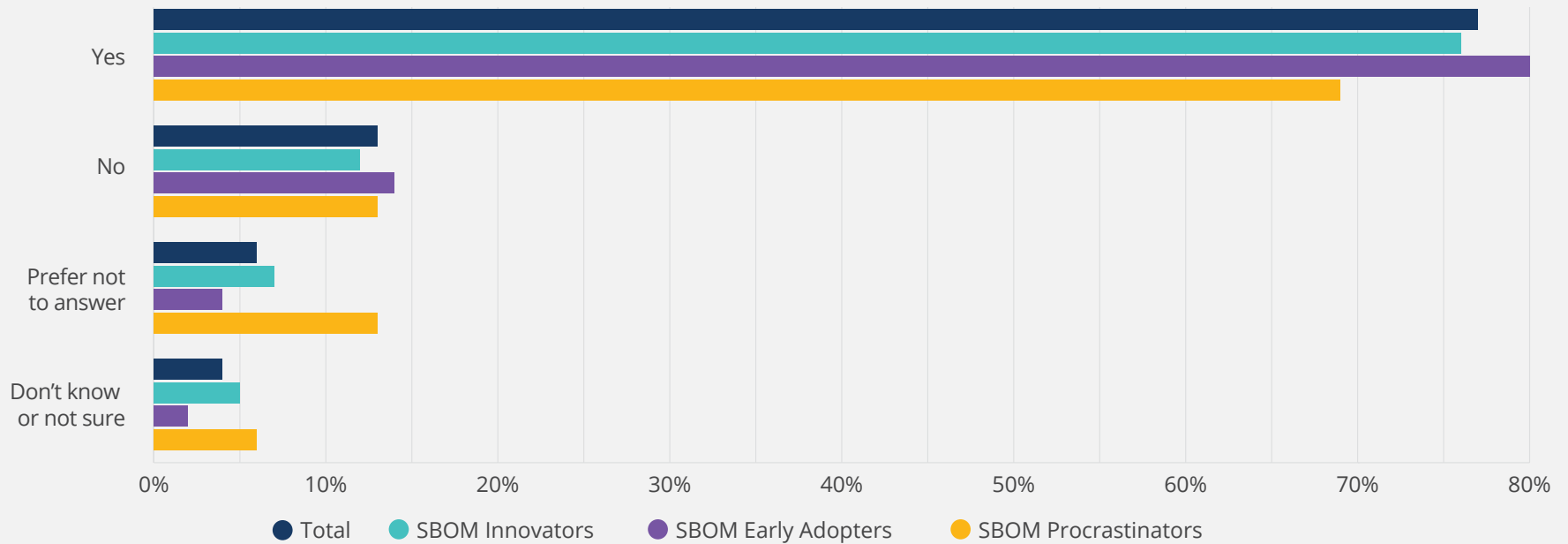
Two factor authentication (2FA) is the third-ranked activity in **FIGURE 13** and was identified by 42% of the sample. 2FA is a well-established technique for improving security, but a continuing number of highly visible security breaches means that 2FA is not always being followed. Because 2FA is a best practice and can be easily implemented, it's disappointing to hear of continued noncompliance.

The use of memory safe programming languages is a very important method of securing the software supply chain, as identified by 40% of the sample. Most newer languages, such as Rust, Go,

FIGURE 12

Is your organization considering any changes in response to the US Executive Order on cybersecurity?

Single Response | Segmented by SBOM maturity | N = 285

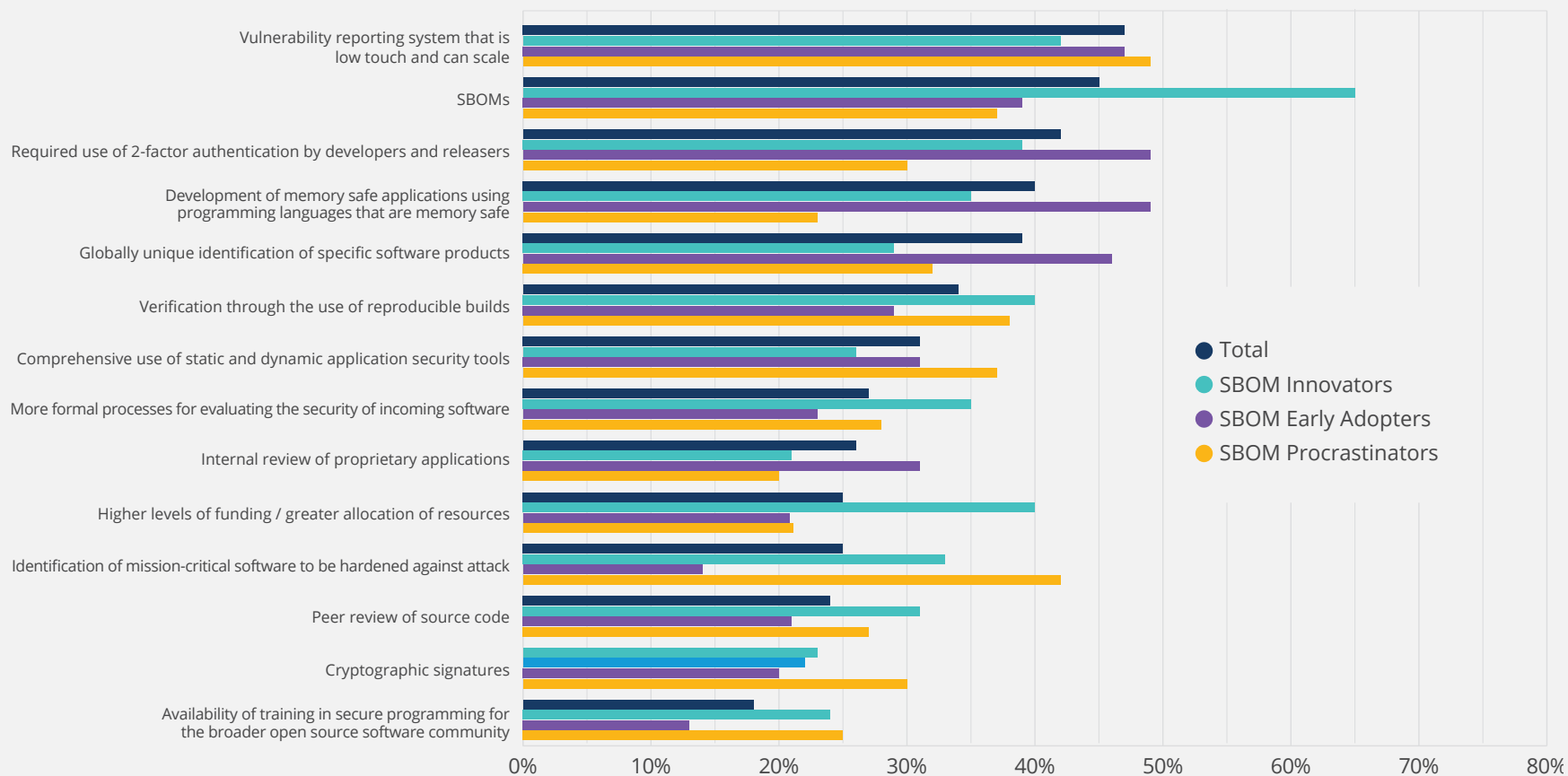


Java, C#, Swift, JavaScript, and Python, are memory safe. Noticeably absent from this list are C and C++. Vendors including Microsoft and Google have reported that the majority of the vulnerabilities they find are memory safety issues. These vulnerabilities are an easy pathway for attackers to exploit an application or operating system.

It should also be mentioned that globally unique identifiers (39%), verification through the use of reproducible builds (34%) and cryptographic signatures (23%) are capabilities that are all achievable when using SBOMs today. This wide array of features is what makes SBOMs so compelling.

FIGURE 13
What do you think are the key activities for securing the software supply chain?

Select all that apply | Segmented by SBOM maturity | N = 316, Valid Cases = 316, Total Mentions = 1,416



SBOM Needs

The framework for the following six figures (14 through 19) was sourced from the NTIA.⁸ These figures highlight six of the key dimensions and decision points that emerged from the NTIA multi-stakeholder process for SBOM.

The legend for each figure includes three dimensions:

- **Fallbacks** to accommodate industry adoption time and legacy processes/technologies
- **The initial consensus** for what is possible today with modern development processes
- **Enhancements** for emerging and high assurance use cases

The NTIA defines baseline component information as follows:

“The primary purpose of SBOMs is to uniquely and unambiguously identify components and their relationships to one another. In order to do so, some combination of baseline component information is required. Certain attributes provide greater uniqueness or unambiguity, as does having a greater number of baseline attributes in an SBOM entry.⁹”

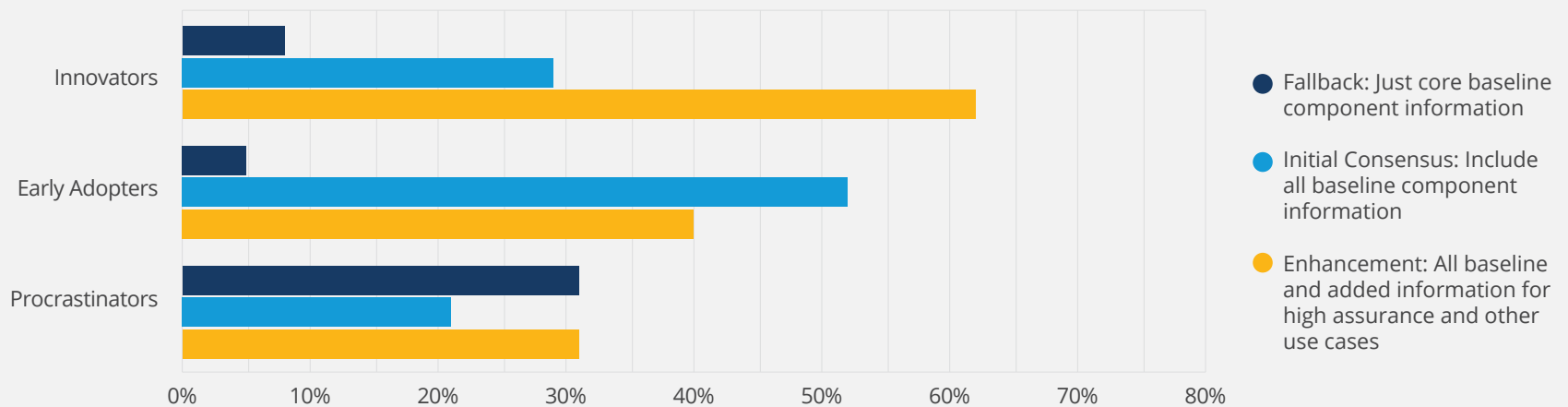
Organizations Want SBOMs to Be Metadata Rich

FIGURE 14 and each of the five figures that follow it describe an important dimension of an SBOM and provide feedback from users regarding what level of functionality is required: fallback, initial consensus, or enhancement. FIGURE 14 shows the preferred level of baseline component information segmented by SBOM maturity. SBOM procrastinators in FIGURE 14 are the least

FIGURE 14

What level of SBOM baseline component information do you currently need?

N = 356



opinionated segment given the relatively even distribution across fallback, consensus, and enhancement plans. SBOM early adopters coalesce around the initial consensus plan at 52%, although 40% are interested in the enhancement plan. SBOM innovators gravitate to the enhancement plan at 62%, which dwarfs the segment's remaining responses to other plans. We expect that this strong interest in enhanced baseline information is due to the immense value that cryptographic hash information (optional) and vulnerability information (in development) can provide.

Machine Readability Is a Key SBOM Requirement

FIGURE 15 defines what level of SBOM format and merge machine readability is required. SBOM procrastinators are once again relatively evenly distributed, although their preference for the initial consensus plan at 33% stands out because it aligns with the leading choice of SBOM early adopters (60%) and SBOM innovators (60%). The initial consensus plan, which requires baseline information to

be machine-readable in each of the leading SBOM formats, is clearly the most pragmatic of the plans. The fallback plan, which implies CSV is overly simplistic, and the enhancement plan create high levels of complexity that may not be needed or readily supportable, since standards in the SBOM space are changing rapidly and significantly.

SBOMs Should Identify Transitive Dependencies with Known Unknowns

FIGURE 16 evaluates what depth of component dependencies are needed by users. The initial consensus plan appears to be the leading candidate, based on a strong preference by 65% of SBOM procrastinators, 40% of SBOMs early adopters, and 49% of SBOM innovators. The appeal of the initial consensus plan is its support for transitive dependencies, which embed a layer of intelligence into how dependencies are identified. The enhancement plan is slightly favored by SBOM innovators, but challenges exist in determining how no unknowns can be declared.

FIGURE 15
What level of SBOM format and machine readability do you currently need?

N = 355

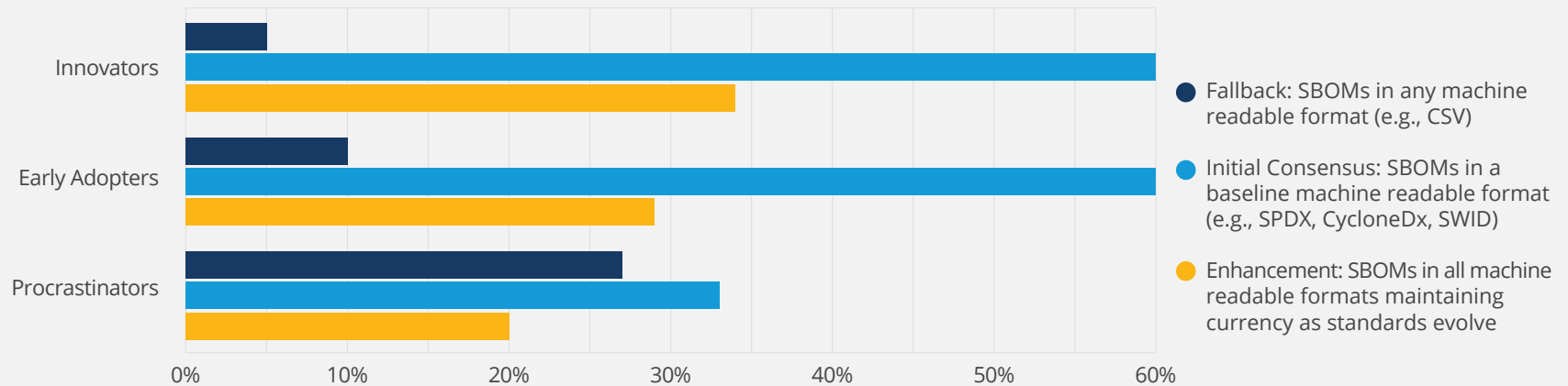


FIGURE 16

What level of SBOM depth of dependencies do you currently need?

N = 355

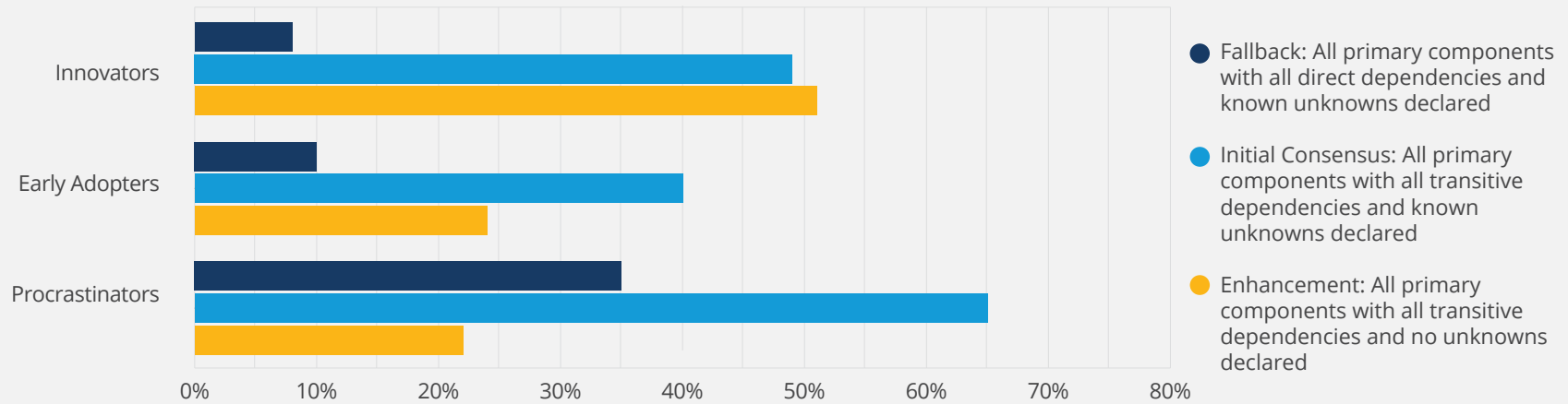
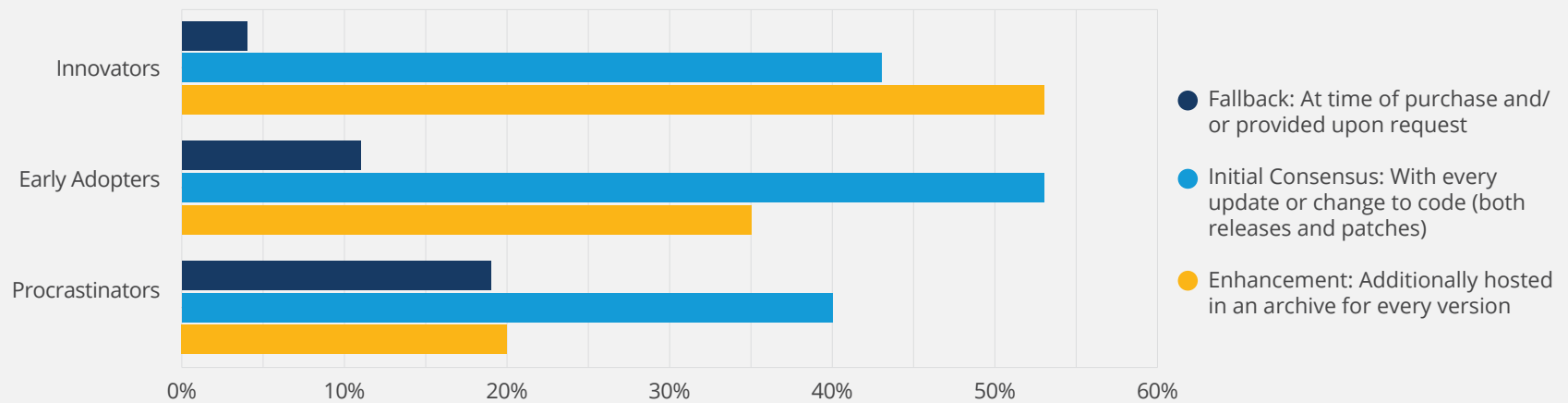


FIGURE 17

What level of SBOM generation frequency do you currently need?

N = 353



SBOM Should Be Updated with Each Code Change

FIGURE 17 determines what level of SBOM generation frequency is required. SBOM procrastinators, at 40%, and early adopters, at 53%, both strongly favor the initial consensus plan. SBOM innovators are divided on the choice of plans, with 43% preferring the initial consensus plan and 53% preferring the enhancement plan. The initial consensus plan is significantly more useful than the fallback plan because it generates an SBOM with every update or change to the component. However, the enhancement plan, by additionally providing support for archiving every version, improves access and provides a historical context that can be invaluable when researching anomalies.

SBOM Metadata Should Be Bundled with the Component

FIGURE 18 establishes what level of SBOM deliverability and interoperability users require. The initial consensus plan is

collectively preferred by the majority of users, which includes 45% of SBOM procrastinators, 51% of early adopters, and 42% of SBOM innovators. However, the enhancement plan received significant support from 43% of SBOMs early adopters and 42% of SBOM innovators. The differences between the consensus and enhancement plans are the support provided for automation, scalability, and interoperability. The enhancement plan provision for API access, and interoperability facilitated by M2M communication vastly accelerates and simplifies SBOM consumption and utilization. But because the consensus plan does support a level of automation, it can be viewed as a useful temporary stepping stone on the way to the enhancement plan.

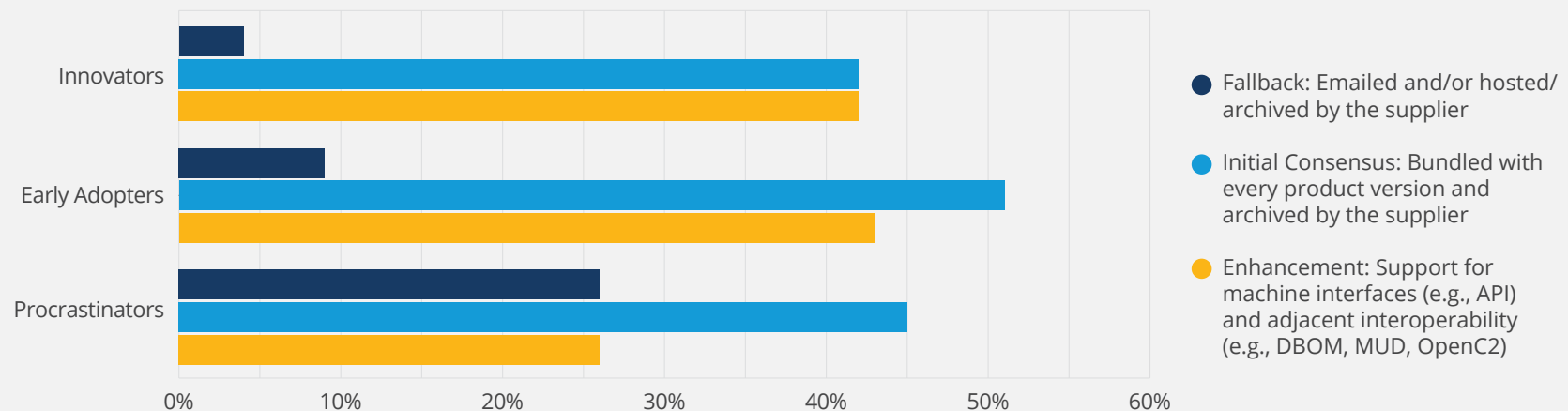
SBOMs Should Reflect Vulnerabilities as They Are Found

FIGURE 19 identifies what level of access and integration is necessary for leveraging vulnerability information. The initial

FIGURE 18

What level of SBOM deliverability and interoperability do you currently need?

N = 353



consensus plan and enhancement plan are both equally appealing to SBOMs users. This is encouraging, because both of these plans' suppliers push vulnerability data in real-time to consumers. The fallback plan does not have such a provision, and both expose the consumer to risk while delivering a highly inefficient process for understanding vulnerabilities.

SBOM Readiness and Segmentation by SBOM Maturity

An important segmentation of survey data was by SBOM readiness. The question asked was, "What is your group's current SBOM readiness?" This question was asked after providing a definition of what an SBOM is and was the first question in the survey to directly query the respondent on what SBOM actions were occurring in the group or business unit they work within. Unlike later questions specific to the status of SBOM production and consumption, this question's broader scope is valuable as a basis for segmenting the sample.

The question had eight responses, excluding don't know and not sure (DKNS). **FIGURE 20** shows that across organizations in our sample, 90% of organizations have started their SBOM journey. 10% of organizations have not begun any planning for SBOMs, 14% are in a planning or development phase, 52% are addressing SBOMs in a few, some, or many areas of their business, and 23% are addressing SBOMs across nearly all areas of their business or have standard practices that include the use of SBOMs. This means that overall, 76% of organizations have a tangible degree of SBOM readiness.

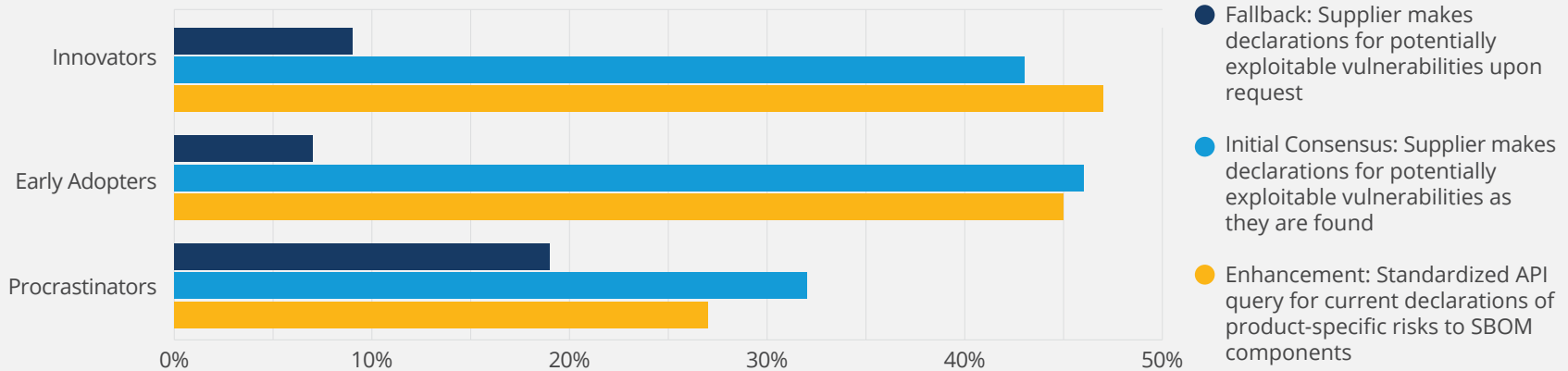
FIGURE 20 shows the overall responses (total) and how we mapped these responses to three categories: SBOM innovators, SBOM early adopters, and SBOM procrastinators.

The category SBOM procrastinators includes respondents who have not started to address SBOMs, are planning how to address SBOMs, or beginning to address SBOMs. SBOM procrastinators account for 24% of the total respondents, and 58% of SBOM procrastinators are planning to or are beginning to address

FIGURE 19

What level of SBOM-adjacent enhancement for vulnerability claims do you currently need?

N = 353



SBOMs support. 41% of SBOM procrastinators (10% of the overall sample) have not started their SBOM journey.

The category SBOM early adopters includes organizations and respondents who have addressed producing or consuming SBOMs across some portion of their business. 53% of the total sample fall into this category. Within SBOM early adopters, 29% are addressing SBOMs in a few segments of their business, 42% across some segments, and 28% are addressing SBOMs across many segments.

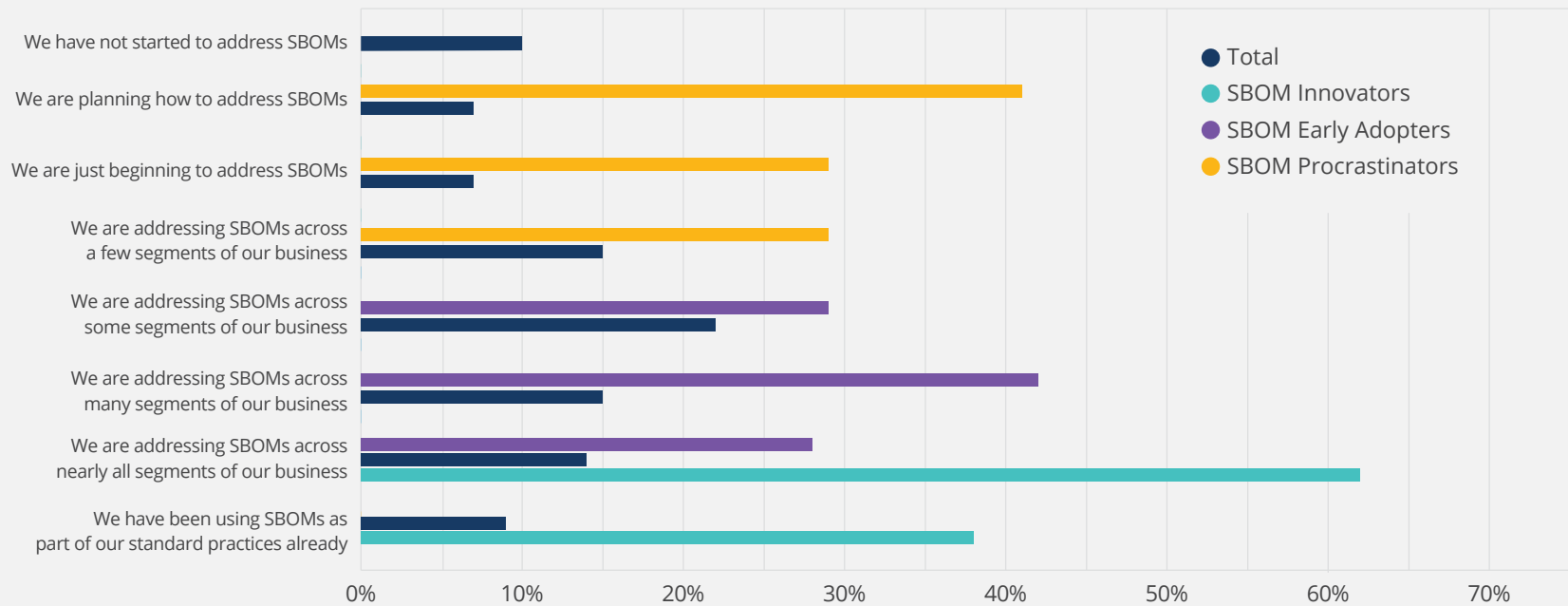
SBOM innovators is a category that is reserved for organizations that are highly committed and experienced in SBOM use. SBOM

innovators represent 23% of the total sample, and within SBOM innovators, 62% are addressing SBOMs across nearly all segments of their business and 38% have standard practices in place for using SBOMs.

The utility of constructing this view based on SBOM readiness is that when cross-tabbed with other variables in the survey, we can gain insight into the priorities and actions associated with each of these three segments: SBOM procrastinators, SBOM early adopters, and SBOM innovators. By examining how these priorities and actions change based on the level of SBOM maturity, we can also gain insight into how organizations adopt SBOMs.

FIGURE 20
What is your group's current SBOM readiness?

Single Response | Segmented by SBOM maturity | N = 341



SBOM Production Perspectives

Earlier in the survey we asked about SBOMs familiarity and then SBOM readiness. This was done primarily to get the respondent thinking about their organizations' use of SBOMs. In the second half of the SBOM survey we asked a variety of questions about organizational involvement in SBOM production and consumption. These questions required a more precise commitment to current or planned SBOM engagement.

SBOM production is most relevant to organizations producing commercial software, because regulators and customers will be demanding this information. But software intended for internal

use will also benefit from SBOMs to improve their security and maintainability.

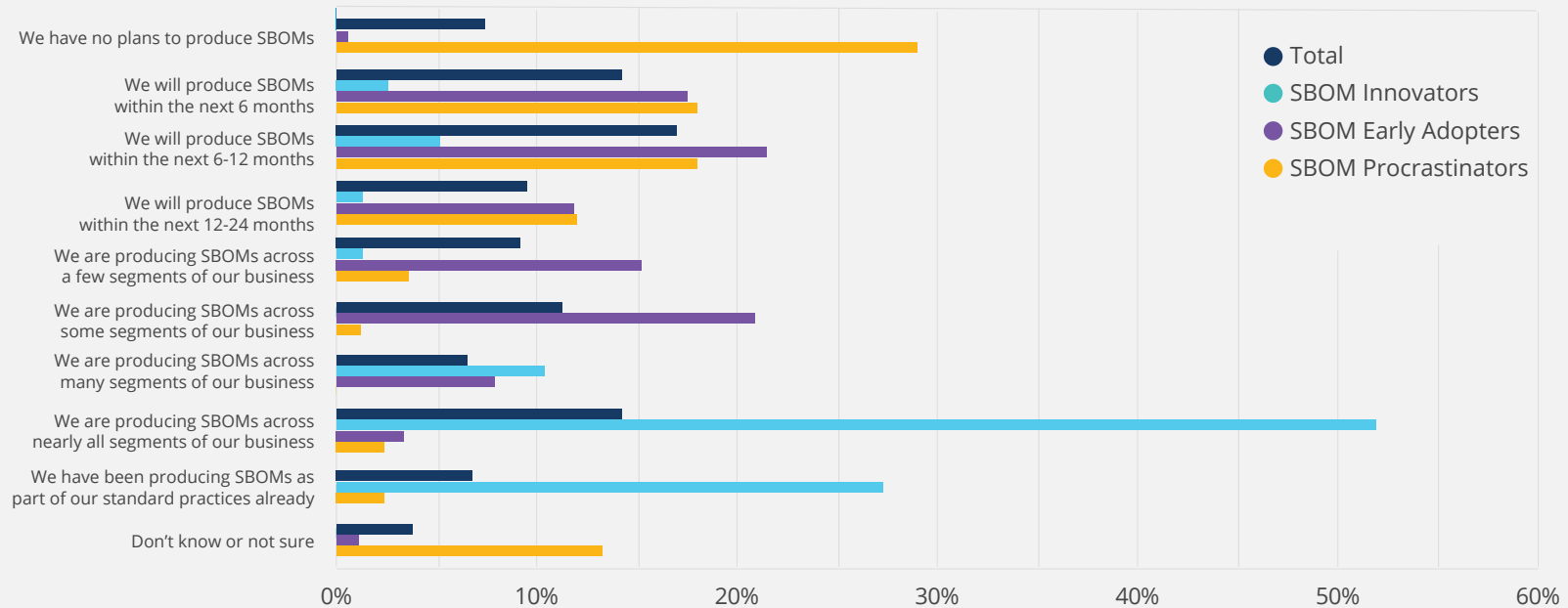
SBOM Production

Comparing the overall results of the SBOM readiness distribution (FIGURE 20) to organizational plans for producing SBOMs (FIGURE 21) shows that organizations aren't quite as far along as SBOM readiness suggests. FIGURE 21 shows that 40% of the overall sample is in the SBOM planning phase (will be producing SBOMs in the next 6–24 months). This is significantly more than the 14% that were in the SBOM readiness planning/beginning phase.

FIGURE 21

What are your organization's plans for producing SBOMs?

Single Response | Segmented by SBOM maturity | N = 337



Similarly, 20% of the overall sample said they are producing SBOMs in a few or some segments of their business, which is far less than the 38% who claimed they were addressing SBOMs in a few or some segments. The gap narrows a little, given the 21% of the overall sample producing SBOMs in many or nearly all segments of their business compared to the 29% from the SBOM readiness question.

The overall difference between SBOM readiness and SBOM production nets out to a 27% reduction (from 67% to 49%) in those organizations that are currently producing SBOMs and a

corresponding 66% increase (from 24% to 40%) in those organizations planning to deliver SBOMs. There is no material change in organizations that have either not started their SBOM journey or are not sure, or don't know how to answer the question.

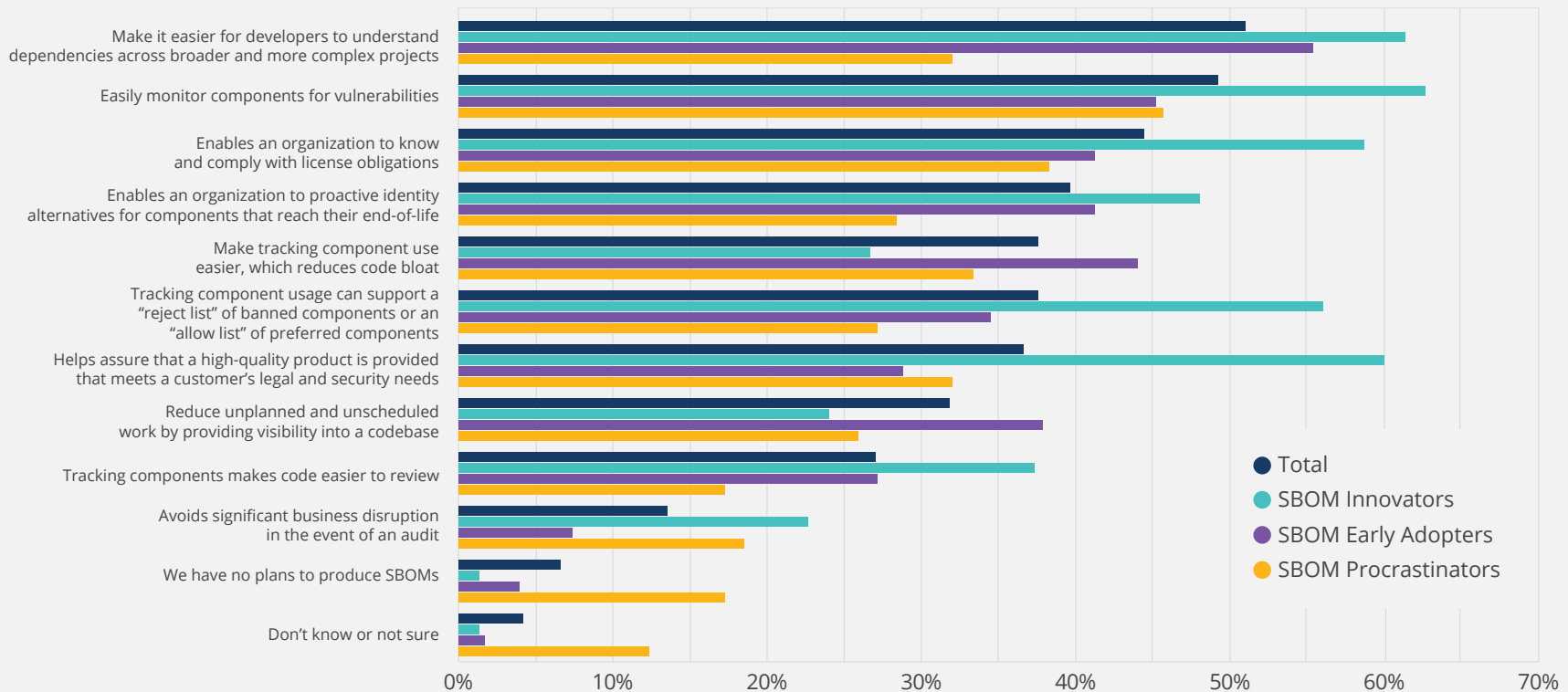
SBOM Production Benefits

Given 49% of organizations in our sample are already producing SBOMs and 40% are in the planning phase, these organizations see benefits from their SBOM involvement. **FIGURE 22** identifies

FIGURE 22

What benefits do you expect to realize by producing SBOMs?

Select all that apply | Segmented by SBOM maturity | N = 333, Valid Cases = 333, Total Mentions = 1,263



what benefits users expect to realize by producing SBOMs. Overall, 51% of organizations report that SBOMs make it easier for developers to understand dependencies across broader and more complex projects. In an era when micro services applications have many components, each component typically has some number of dependencies. SBOMs provide explicit identification of dependencies, which is increasingly useful as the complexity and number of components in an application grows. Identification of dependencies was especially important to SBOM innovators, at 61%, and SBOM early adopters, at 55%. Identification of dependencies was one of the two most important benefits highlighted.

FIGURE 22 also shows the overall importance of monitoring components for vulnerabilities. Overall, 49% of organizations identify this is a benefit, as did 63% of SBOM innovators. Monitoring for vulnerabilities is very much a work in progress, as discussed in our analysis of **FIGURE 28**. The challenge is that the list of vulnerabilities for each component is always changing, as new vulnerabilities are found and existing vulnerabilities are mitigated. How to communicate this information in a timely way to the consumers of a component is a work in progress. Since this was the leading benefit identified by SBOM innovators, an effective approach to vulnerability monitoring is an expected feature of SBOMs.

License compliance is an important requirement now that the use of open source software is pervasive. **FIGURE 22** shows that 44% of organizations see SBOMs as an effective way to identify and comply with license obligations. SBOM innovators, at 59%, were quick to reinforce the importance of license compliance as a benefit.

Taken together, the understanding of dependencies, vulnerabilities, and license compliance represent the most important benefits provided by SBOMs.

FIGURE 22 also provides a view into where SBOMs may be headed. 56% of SBOM innovators are interested in the concept of a component “reject and allow list” to help with access control. 60% of

“Our need for SBOM started with the fact that we have thousands of products and thousands of versions of those products. As third-party vulnerabilities are identified, we spend thousands of hours each year doing impact assessments to look for these vulnerabilities in our product. ... And what we found was that if you have an SBOM, then we had to bother the project teams less and it was taking less time to do the research.”

SBOM innovators are also interested in using SBOMs as a way to assure the delivery of a high-quality product that meets customer legal and security needs.

A leading global supplier of energy products discussed their SBOM journey with us:

“Our need for SBOM started with the fact that we have thousands of products and thousands of versions of those products. As third-party vulnerabilities are identified, we spend thousands of hours each year doing impact assessments to look for these vulnerabilities in our product. The only way that can be performed is by sending these impact assessments to the product teams. With thousands of products, some of these product teams don’t even exist anymore, so it’s quite a struggle. If you’ve got an existing project team that can examine what they’ve built, then it still takes them a lot of time to investigate. And what we found was that if you have an SBOM, then we had to bother the project teams less and it was taking less time to do the research.”

SBOM Production Concerns

The nascent status of the SBOM market is vividly reflected in the concerns organizations have about the use of SBOMs. **FIGURE 23** shows these concerns in decreasing order of importance and also segments the data by SBOM maturity. The top four concerns were voiced by between 40% to 33% of the overall sample.

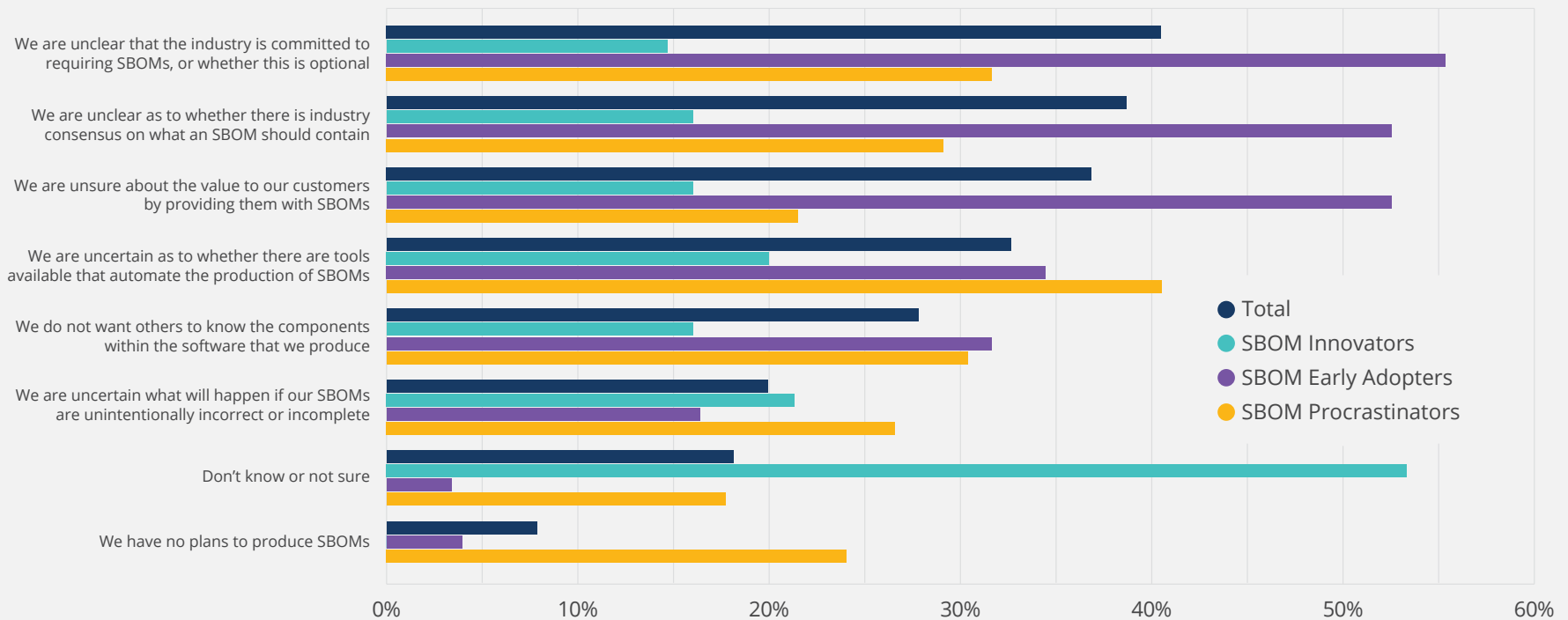
The leading concern, identified by 40% of the sample, was whether or not the industry is committed to requiring SBOMs. The U.S.

Food and Drug Administration (FDA) provided initial SBOM market guidance beginning in 2018, and in 2021 the FDA has prioritized delivery of its final SBOM market guidance. This guidance is expected to require medical device manufacturers to include SBOM information with their products. So, healthcare markets have fast-tracked SBOMs. Other markets, including automotive, manufacturing, and energy, each have domain-specific needs, but are looking to identify and adopt best practices from how SBOM compliance evolves in healthcare. While this indicates that the

FIGURE 23

What concerns do you have in producing SBOMs?

Select all that apply | Segmented by SBOM maturity | N = 331, Valid Cases = 331, Total Mentions = 736



SBOM market is gathering momentum, leading software vendor involvement has been spotty, causing leading vendors and end users to question how real the SBOM initiative is.

The second important concern, voiced by 39% of the overall sample, is whether there is industry consensus on what an SBOM should contain. The NTIA has delivered guidance on this in its July 2021 document: the minimum elements for a Software Bill of Materials. This document is useful in defining what an SBOM should contain, but largely leaves discussion around data formats, implementation, and process in the hands of vendors and industry organizations. While progress across the SBOM domain is accelerating, a distinct lack of visibility and messaging by leading IT vendors and organizations underlies all of these concerns.

Vendors and end users were also unsure about the value of providing SBOMs to their customers. This was voiced by 37% of the overall sample. Given the clear benefits in terms of identifying dependencies, vulnerabilities, and licensing that SBOMs provide, this concern is not apt to be long-lived.

Finally, 33% of the overall sample was uncertain about the availability of tools to automate the production of SBOMs. This is a valid concern, but needs to be addressed in the context of organizational policy and DevOps processes.

An effective approach for mitigating these concerns would be a significantly higher level of support of the IT vendor and service provider community, given the effectiveness and scale of its product development and product marketing capabilities.

The second important concern, voiced by 39% of the overall sample, is whether there is industry consensus on what an SBOM should contain. The NTIA has delivered guidance on this in its July 2021 document: the minimum elements for a Software Bill of Materials. This document is useful in defining what an SBOM should contain, but largely leaves discussion around data formats, implementation, and process in the hands of vendors and industry organizations.

FIGURE 23 also shows a unique characteristic, in that SBOM innovators are far less concerned about SBOM production issues (15% to 21%) than SBOM early adopters (16% to 55%) or SBOM procrastinators (22% to 41%). Additionally, SBOM innovator responses of don't know or not sure were 53%, indicating that innovators are largely committed to SBOMs and are mostly concerned with unknown unknowns.

SBOM Consumption Perspectives

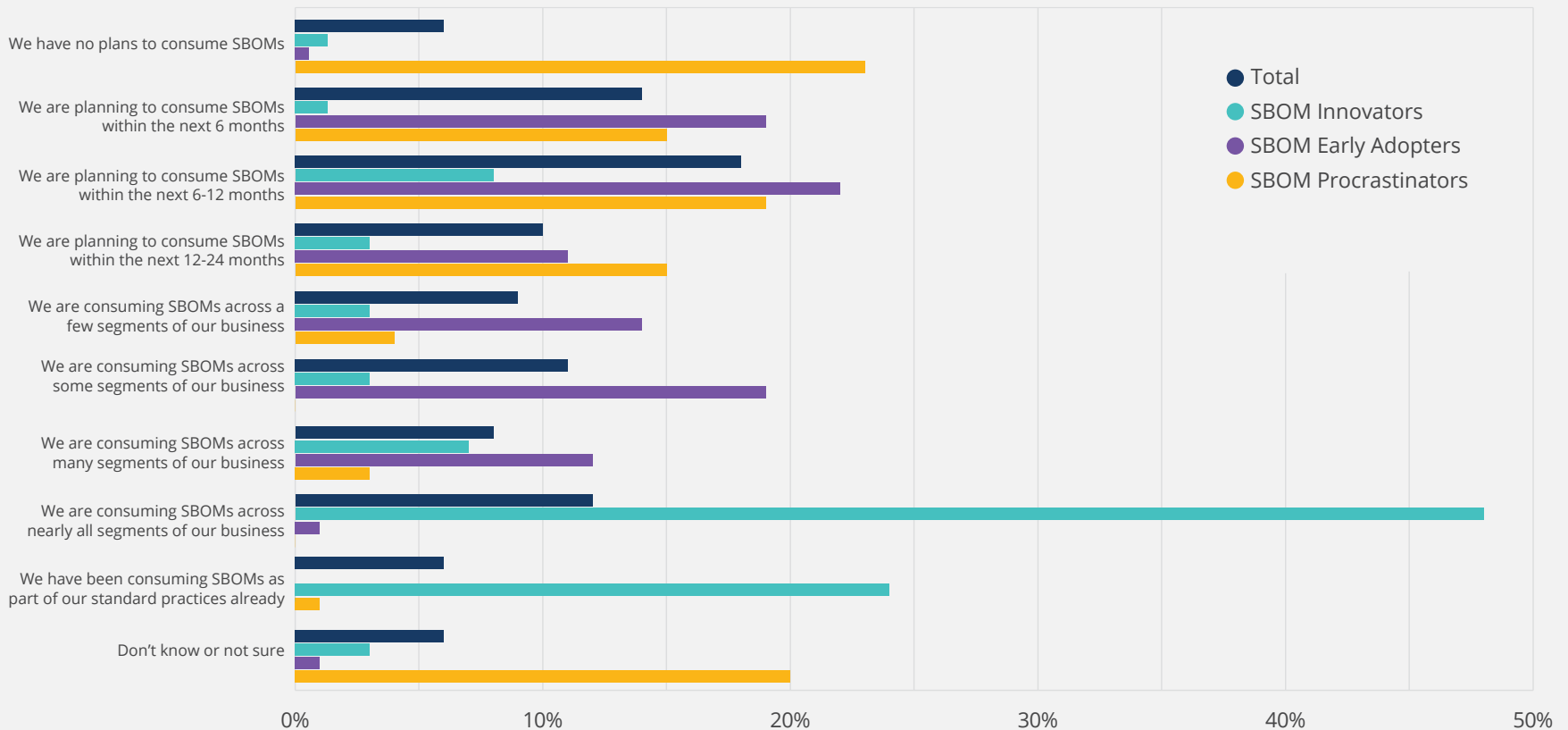
SBOM consumption patterns are well aligned with SBOM production patterns. A correlation of the data behind **FIGURE 21** (SBOM production) and **FIGURE 24** (SBOM consumption) yields a value of .70, which borders on a strong correlation.

What this means is that respondents generally answer these questions the same way. This intuitively makes sense, because vendors and end users concerned about SBOM production are also concerned about the upstream consumption of SBOMs.

FIGURE 24

What plans does your company have for consuming SBOMs?

Single Response | Segmented by SBOM maturity | N = 330



While end users may be more interested in the consumption of SBOMs, they also have an interest in SBOM production in support of the security and maintainability of the software they produce.

The global supplier of energy products that we spoke with summarized the value of SBOMs as follows:

“If I put myself in the role of an asset owner, would I not only want an SBOM, but I’d also want vulnerability information, how to validate authenticity and integrity of the component—so I need to have certificate information and I need to know the hashes that should be coming with it.”

A senior policy advisor for the U.S. Food and Drug Administration had the following to say about the utility and importance of SBOMs in the healthcare industry:

“SBOMs are multipurpose. We tend to start from the perspective of software transparency, because where the medical and healthcare sector is at is, we don’t even have this information. In rare cases, you have folks in hospitals with the skill set to be able to go out and find this information for themselves if they need it. But hospital procurement officers don’t know how to examine an SBOM, the package manager listings, or the open source licensing distribution lists to see if there is risky software that they should not be bringing into their environments. They don’t have the information or the expertise to make those kinds of decisions. There’s also an issue that nobody wants to disclose this information. The medical device manufacturers don’t necessarily want to admit that they’re using outdated pieces of software in some circumstances. So, they don’t necessarily want to tell anyone what’s in their product. So, for us, it starts with transparency. Because if you don’t have any of this information, you can’t make any decisions easily, you can’t make any assessments or evaluations easily as well. But once you have it, once you have an SBOM, the information is there for everyone to see, and you can start consuming SBOMs in formal ways to manage risk far more effectively.

“There is also a recognition that when cybersecurity vulnerabilities occur in other spaces, it’s annoying. Maybe you’re going to lose information or maybe there will be huge financial consequences, but it’s unlikely that people are going to get hurt. In healthcare, if there’s a cybersecurity vulnerability that gets exploited there is a very large possibility that somebody and a lot of somebodies are going to get hurt.

“Hospitals now have greater purchasing power, and they are essentially putting SBOM requirements in their contracts. When a hospital now wants to acquire a device, they’re essentially saying you will give us an SBOM, or we will not buy your product. So, it seems more of the market forces are now taking precedence.”

SBOM Consumption

FIGURE 24 shows that only 6% of organizations in our sample have no plans to consume SBOMs. Over the next six to 24 months, 42% of organizations in our sample are planning to begin consuming SBOMs. This leaves 40% of the sample consuming SBOMs in production, and 6% who have made SBOM consumption part of their standard practices. A segmentation by SBOM maturity confirms that SBOM innovators show heavy production use of SBOMs, and SBOM procrastinators either have no plans to consume SBOMs or are heavily involved in the SBOM planning phase.

SBOM Consumption Benefits

Vendors and end users were consistent in voicing expected benefits from consuming SBOMs. **FIGURE 25** shows that the top five benefits were identified by between 48% and 53% of the overall sample. The top two benefits included providing information about components that better support compliance and reporting requirements (53%) and providing information that enables more informed risk-based decision-making (53%). Addressing compliance, financial, and reputational risk are key objectives that organizations must consider when leveraging third-party software.

The next three benefits: the timely recognition of vulnerabilities (49%), the proactive identification of components that reach end of life (49%), and awareness of risky components (48%) were all possible because of the transparency provided by SBOMs.

These benefits help organizations improve security, reduce risk, and provide more reliable services to their customers and business partners.

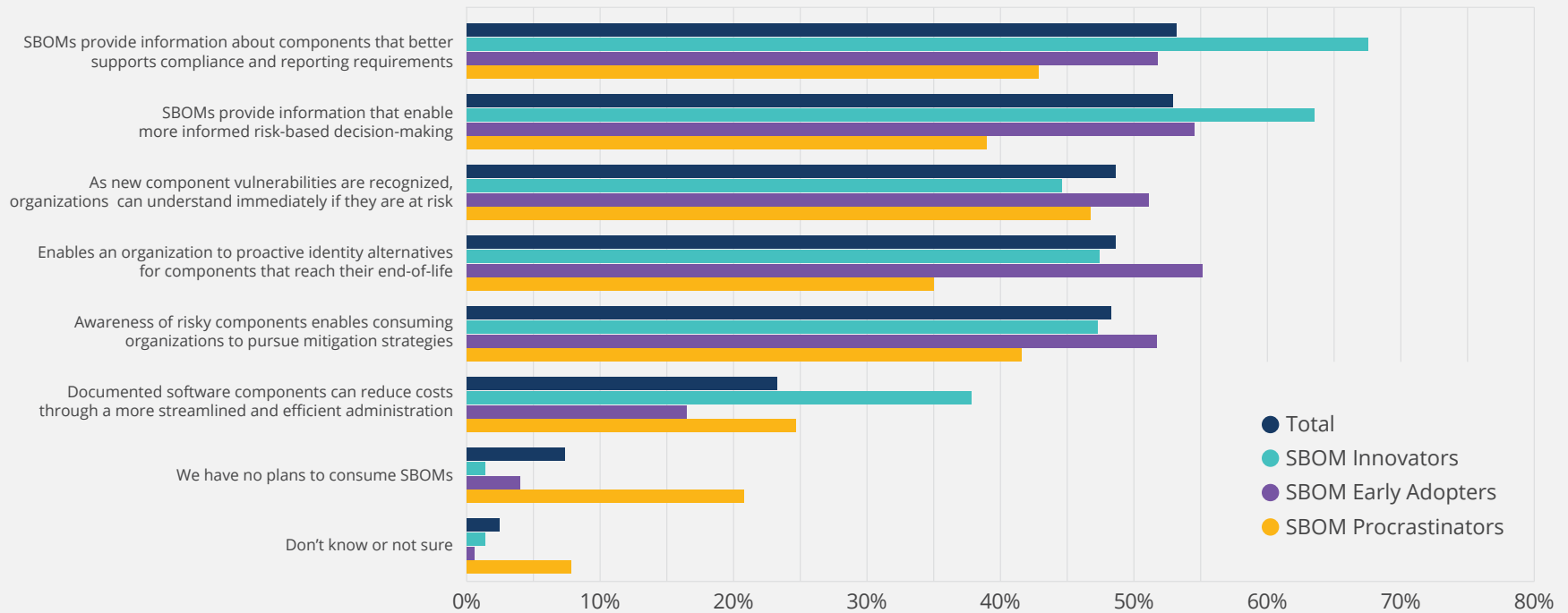
SBOM Consumption Concerns

Similar to SBOM production concern findings, SBOM consumption concerns were primarily voiced by SBOM early adopters and SBOM procrastinators. **FIGURE 26** shows that the overall leading SBOM consumption concerns included uncertainty around industry requirements for SBOMs (49%), the availability of tools to automate the consumption of SBOMs (48%), and industry consensus on what an SBOM should contain (44%).

FIGURE 25

What benefits do you expect to realize by consuming SBOMs?

Select all that apply | Segmented by SBOM maturity | N = 327, Valid Cases = 327, Total Mentions = 931



These are serious concerns. While it is encouraging that SBOM innovators were not overly concerned about these issues is a positive sign but does little to communicate the SBOM value proposition to SBOM early adopters and procrastinators who comprise 75% of our sample. In order to remove the uncertainty about industry-specific requirements for SBOMs requires a coordinated effort by government agencies, industry organizations (including industry-specific Information Sharing and Analysis Centers), and IT vendors and service providers to increase messaging around the SBOM value proposition, tools availability, integration capabilities, DevOps processes, and best practices.

The uncertainty that exists around the availability of SBOM tools

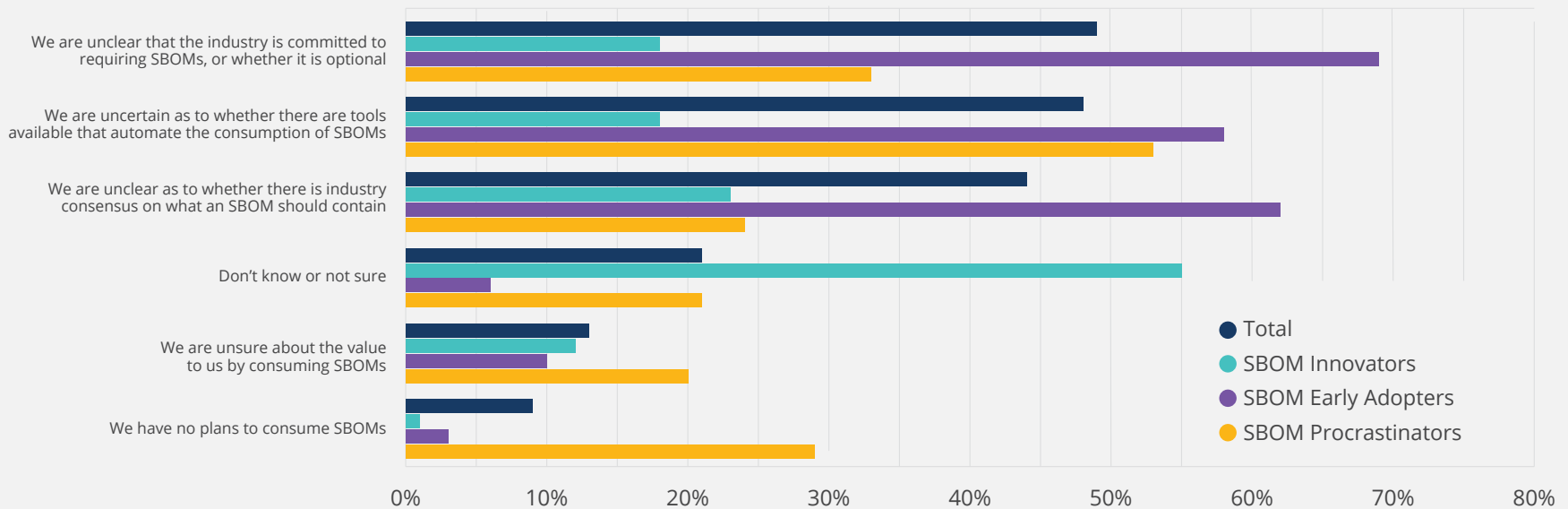
is a supply-side issue. Industry organizations and vendors need to ramp up their investment in and messaging around their SBOM tools portfolio, as well as its visibility. As we will see later in the report, the market for SBOM tools is likely to explode in 2022 and 2023. Vendors and service providers would be advised to fast-track products and services to take advantage of end-user demand.

The final concern, the lack of industry consensus around what an SBOM should contain, is far less of an Intellectual property issue and more a security issue. Advancements in vulnerability identification and reporting are currently a work in process. Because security has become such an important dimension of SBOMs, we would anticipate that this issue will achieve closure in 2022.

FIGURE 26

What concerns do you have in consuming SBOMs?

Select all that apply | Segmented by SBOM maturity | N = 324, Valid Cases = 324, Total Mentions = 593



Conclusions

This SBOM readiness survey showed SBOM familiarity, SBOM readiness, and SBOM production and consumption adoption greater than we anticipated. Much of the investment to date in SBOM has come from public and private companies such as Intel, Siemens, Sony, Toyota, and Wind River. U.S. federal government agencies (NTIA, FDA, NIST, and the Department of Commerce) are now involved in advocating and legislating (in some industries) SBOMs. IT industry organizations and vendors are increasingly messaging about the importance of SBOMs and supporting the evolution of data formats, best practices, and the definition of technology road maps. This represents a great start, but in order to cross the chasm, the SBOM market needs to evolve considerably.

The policy advisor we talked to at the U.S. Food and Drug Administration had this to say about the evolution of SBOMs.

“What is happening in healthcare is not like other industries where grassroot best practices were adopted over time and then eventually the regulators said we’re officially adopting this as a best practice. In healthcare it worked the other way around. Regulators announced that we were going to be pursuing SBOMs and that eventually there would be an expectation that SBOMs would be necessary to sell medical products in the United States—which is a multi-multi-billion-dollar industry. The recent executive order came out several years later, but it just represents more pressure being added from the regulatory government’s side of things on healthcare. I think all of the various parties involved have essentially said, we don’t have a choice. We’ve got to figure this out. So, I would expect to see an impact on every link in the supply chain. When a manufacturer in healthcare turns around to a supplier and says I’m not going to pay you anymore unless you provide SBOMs, it ends up being an N minus one forcing function of everybody turning around to their own suppliers and saying, because

I’m being forced to do this, you’re going to be forced to do this, and this is how it gets done.”

How SBOMs Could Be Improved

FIGURE 27 provides feedback on how SBOM activities can be improved. The most pressing issue, which was identified by 62% of the overall sample, was the need for industry consensus on best practices to integrate the production and consumption of SBOMs into software development. The production and consumption of SBOMs occur in DevOps. The challenge is that every organization has a unique DevOps tool chain, processes, and activities. There is also not yet consensus on where SBOM production or consumption should occur in DevOps. SBOM production is clearly a development-oriented activity, but SBOM consumption can occur either in dev or ops. Adding to this confusion of where SBOMs should be produced or consumed is the question of when SBOMs should be produced or consumed. Another dimension to SBOM production and consumption is that known dependencies and vulnerabilities are always changing and will impact where and when SBOMs were produced and consumed.

A large manufacturer of consumer electronics described some of the challenges involved in adopting SBOMs. A significant challenge was the complexity of figuring out how and where to start, given the complexity of some data formats. Another, related, issue was the lack of interoperability between various SBOM data formats. These issues point to the limited availability of SBOM tooling to facilitate SBOM production, consumption, integration, and interoperability.

The second-ranked industry need, voiced by 58% of the overall sample, is consensus on best practices to integrate the production and consumption of SBOMs into GRC (governance, risk, and compliance) processes. There are important policy and operational

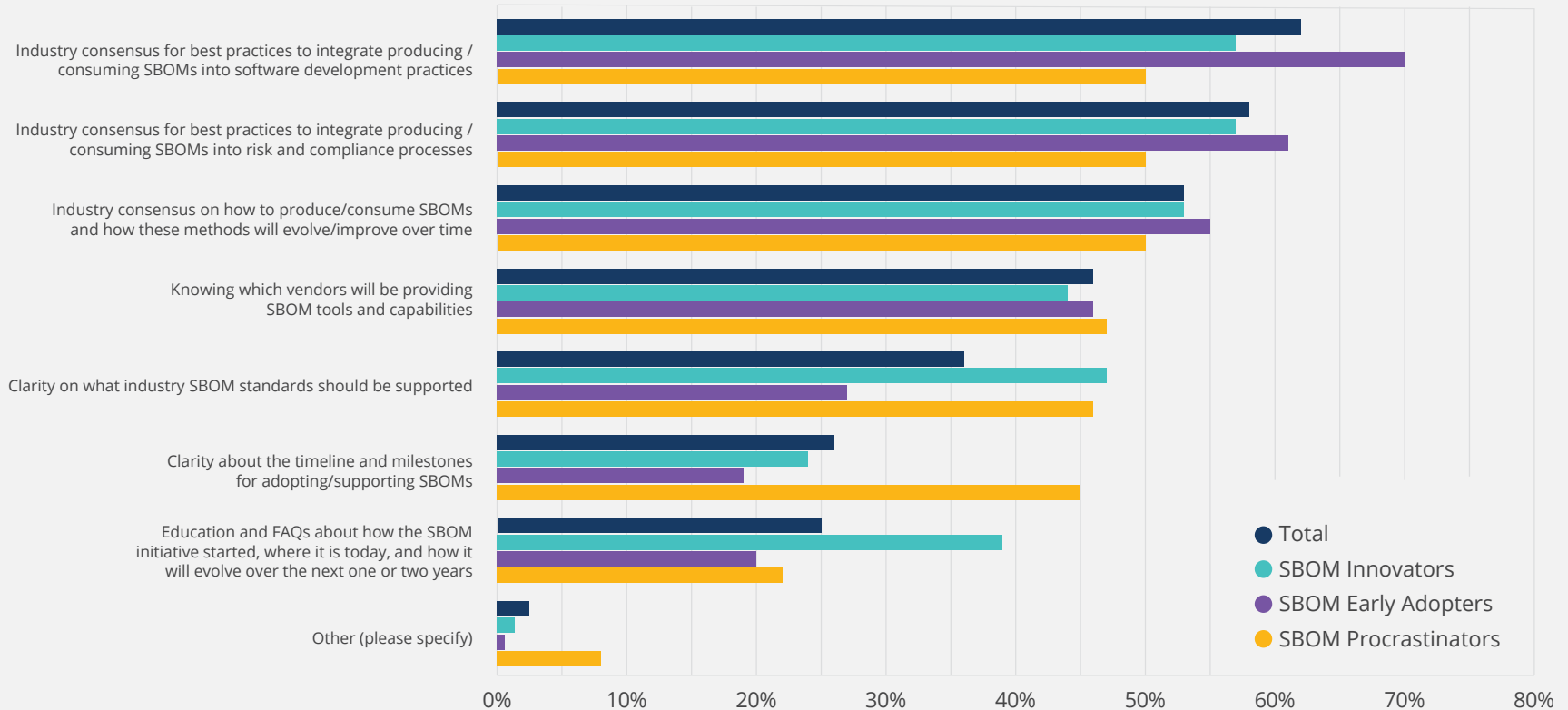
decisions that revolve around SBOMs. Organizations that have an OSPO (open source program office) and/or CISO (chief information security officer) are well positioned to address this need. However, this SBOM readiness survey showed that overall, about 20% of organizations did not have an OSPO or CISO. These numbers shrank to about 10% for SBOM innovators and early adopters, but increased to between 35% to 40% for SBOM procrastinators.

FIGURE 27 also shows that 53% of the overall sample is searching for industry consensus on how the methods for producing or consuming SBOMs will evolve over time. The NTIA has only recently published the minimal elements for a software bill of materials, and the data formats for SBOMs are also rapidly evolving. While this change is characteristic of nascent markets, it clearly makes the production and consumption of SBOMs far more

FIGURE 27

What would be useful to your organization to improve its ability to produce and/or consume SBOMs?

Select all that apply | Segmented by SBOM maturity | N = 319, Valid Cases = 319, Total Mentions = 983



challenging. At the same time, there are clearly significant market opportunities for the IT vendor community to help shape and accelerate the SBOM market, with **FIGURE 27** showing that 46% of the overall sample is struggling to understand which vendors will be providing SBOM tools and capabilities.

The Importance of SBOMs

Earlier in this report, **FIGURE 6** showed that 98% of organizations in our sample use open source software. It also follows that much of the proprietary software available in the market leverages open source software in some capacity. Given this context, **FIGURE 28** demonstrates how important SBOMs are for open source software compared to proprietary software.

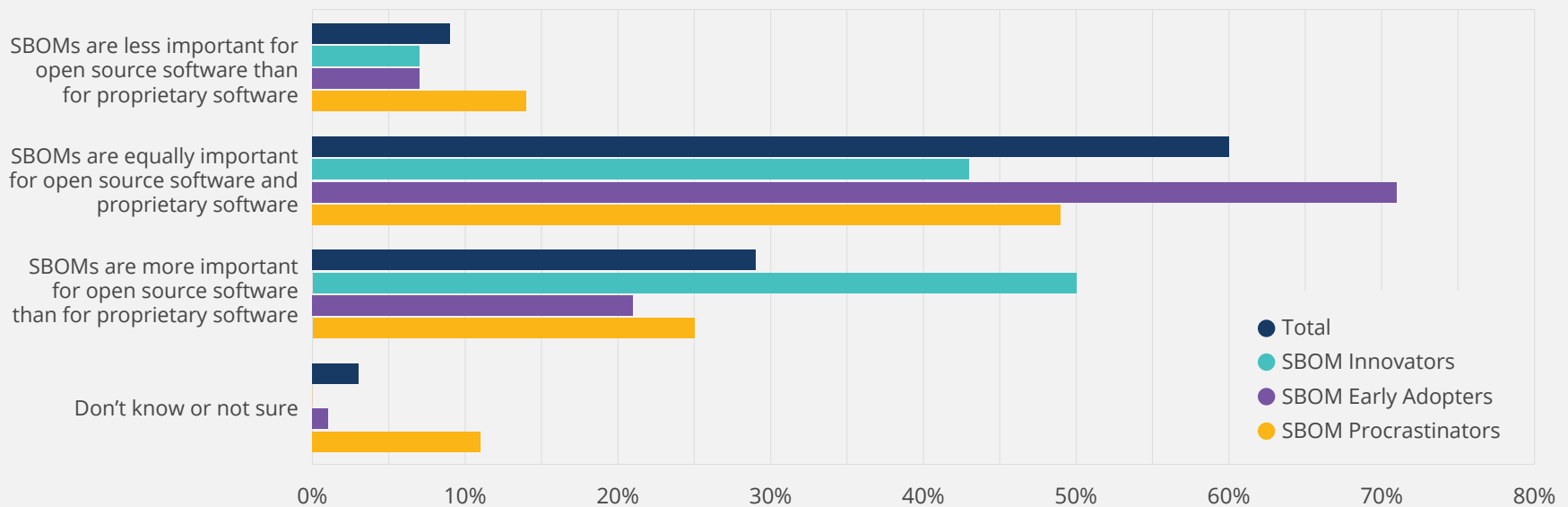
FIGURE 28 shows that 60% of organizations believe that SBOMs are equally important for open source software and proprietary software. Of the remaining organizations, 29% believe that SBOMs are more important for open source software and proprietary software and 9% feel that SBOMs are less important for open source software. There are several ways to interpret this data.

The fact that 60% of the sample believes that SBOMs are equally important for open source and proprietary software means that the majority of organizations are interested in seeing SBOMs for all software components. However, the 29% that believe SBOMs are more important for open source software can be interpreted as meaning that proprietary software vendors, despite potentially leveraging open source in their products, do a better job of vetting

FIGURE 28

How important are SBOMs for open source software compared to proprietary software?

Single Response | Segmented by SBOM maturity | N = 316



and testing their products. Complicating matters is that SBOM innovators are somewhat evenly split on this topic, with 43% seeing SBOMs as equally important and 50% stating that SBOMs are more important for open source software. Presumably, SBOM innovators are more experienced in working with SBOMs and see a greater need for open source SBOMs.

The answer to this dilemma is to legislate SBOMs for all software under the assumption that all software products are likely to include some open source code. This approach has been used successfully in the healthcare market, accepted by vendors, and applauded by end users. Other markets, including automotive, energy, and manufacturing, are evaluating the transition to SBOMs in the healthcare market.

Despite the relative incongruities of comparing SBOM needs in open source software to those in proprietary software, the importance of resolving cybersecurity issues is paramount across the software supply chain. The presidential executive order was not a wake-up call, but simply a confirmation that cybersecurity is an acute problem and efforts to address cybersecurity need to be accelerated. The good news is that SBOM policy, data formats, and tools have been in development for the past 4 to 5 years by the U.S. federal government, IT vendors, and IT industry organizations. It appears that initial SBOM teething problems are behind us and the biggest challenge looming in the near future is how to cross the chasm so that SBOMs are adopted by an early majority. The challenges are how to drive regulatory oversight, SBOM maturity, vendor participation, product development, and messaging in a coherent way that adds value effectively.

The Future of SBOMs

Based on organizational intent to produce (FIGURE 21) or consume (FIGURE 24) SBOMs, a forecast of SBOM use (penetration) and growth can be estimated. The overall profiles of SBOM production and consumption are similar, allowing us to aggregate these two measures, as shown in FIGURE 29. The forecast in FIGURE 29

Despite the relative incongruities of comparing SBOM needs in open source software to those in proprietary software, the importance of resolving cybersecurity issues is paramount across the software supply chain. The presidential executive order was not a wake-up call, but simply a confirmation that cybersecurity is an acute problem and efforts to address cybersecurity need to be accelerated.

is based on the incremental addition of organizations planning to produce or consume SBOM to those organizations already producing/consuming SBOMs. The 48% penetration rate in 2021 is the percent of organizations who are producing or consuming SBOMs across (a few/some/many/nearly all/as a standard practice) segments of their business (from FIGURES 21 and 24). The 2022 penetration rate adds those organizations planning to produce or consume SBOMs in the next 6 or a year. Likewise, 2023 incrementally adds those organizations planning to produce or consume SBOMs in 12-24 months.

FIGURE 29 shows that SBOM production/consumption growth for 2022 is expected to be high, at 66%, enabling SBOM penetration to reach 78%. Annual SBOM growth trails off in 2023, to 13%, but still drives SBOM penetration to 88%. This strikes us as a very aggressive growth scenario and is likely contingent upon the rapid development and growth of the tools market for SBOM production and consumption.

The United States government has taken a firm stand on requiring SBOMs when it purchases software. This is partially due to a legacy

of cyberattacks, culminating with SunBurst. But it is more a recognition that with the transition to a digital economy and the reliance on software, digital assets are mission-critical to virtually all organizations, and in some cases are life-critical, such as in the medical device industry. This research has shown a variety of benefits that stem from the production and consumption of SBOMs. SBOMs started out as being a way to identify and protect intellectual property. However, security is now a part of the SBOM agenda. A recent discussion with a senior policy advisor for the U.S. Department of Homeland Security amplified the role of SBOMs:

“SBOMs help us solve a couple of important issues, one of which is when there is a new vulnerability discovered, am I affected? if you have an SBOM, you can figure out where you might be affected. The more complete an SBOM is, the more likely it is that

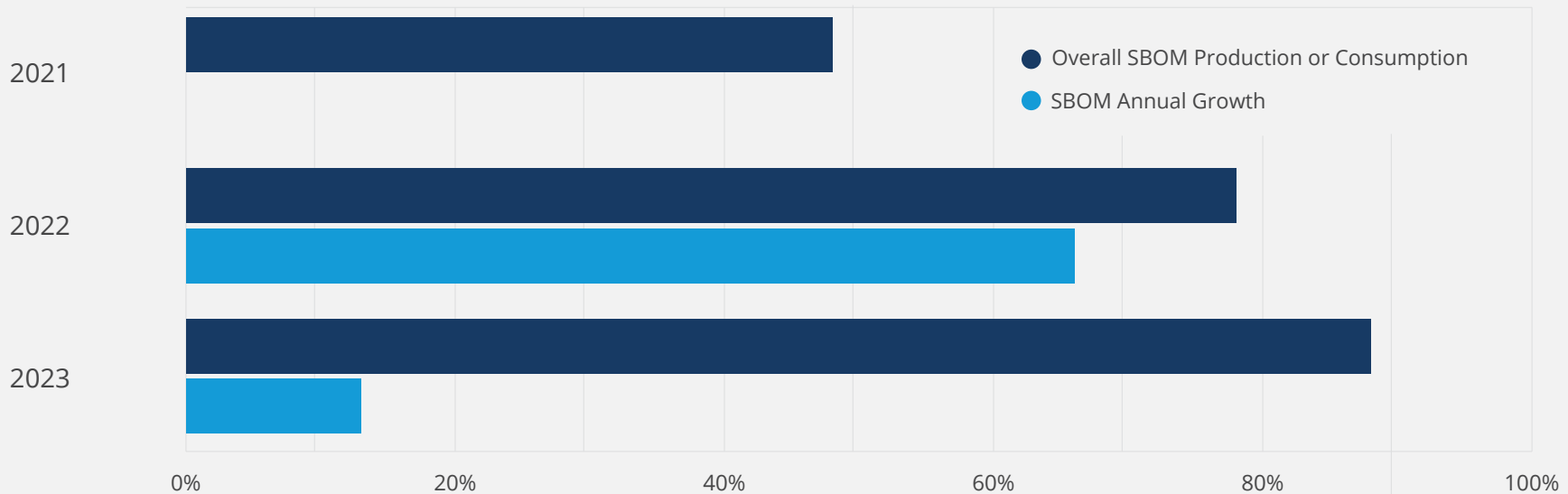
“We need visibility, we need incentives, and we need resiliency. An SBOM won’t give us those, but they enable all of those. In other words, we can’t move forward without SBOMs.”

you can prove a negative to show that you’re not affected. The bigger picture, however, is to get a handle on our supply chain for software. We need visibility, we need incentives, and we need resiliency. An SBOM won’t give us those, but they enable all of those. In other words, we can’t move forward without SBOMs. Widespread use of SBOMs will allow more organizations to pay attention to what open source products they’re using and what commercial

FIGURE 29

Forecast organizational production or consumption and growth of SBOMs 2021-2023

N = 330-337



products they're using in their supply chain. And just like we've seen with traditional supply chains and physical goods, awareness can drive better quality. Right now, the basic SBOM can't tell you if someone has injected a backdoor into a popular product. What an SBOM can do is to say, once we know that a backdoor has been injected, everyone can figure out whether or not they are affected. But once you have that visibility, then the next step can be to start layering on pedigree and provenance metadata and start integrating into our tooling—so we actually can detect malicious attackers. And so, an SBOM is necessary but not sufficient to make substantial progress for better software assurance and better software supply chains.”

The production (**FIGURE 21**) and consumption (**FIGURE 24**) data on SBOMs in this report shows that 49% of organizations are producing some number of SBOMs, and, likewise, 56% are consuming some number of SBOMs. While the SBOM subject and the SBOM market for tools do not attract much attention or generate visibility, many industries are engaged in building SBOM policy and best practices. The reason that SBOMs tend to fly under the radar right now is because industry activities are domain-specific. Information Sharing and Analysis Centers (ISACs) have been established in many leading industries.

The SBOM tools market has already attracted about twenty vendors. Some of these vendors come from adjacent markets like Software Composition Analysis (SCA), Artifact Registry and Repository Managers (ARRM), and software security. A variety of open source projects also exist—some focused on SBOM generation. We would assume that there will be a horizontal SBOM tools market with domain-specific plug-ins to tailor policy, data, and metadata by industry.

At this juncture, the U.S. federal government has put a stake in the ground to help stimulate the demand for SBOMs. Their approach will be to require SBOMs for software purchased by the government. This is a little different than in healthcare, where the federal government introduced regulations to require device manufacturers to provide SBOMs. The results, however, are similar—genuine end user demand or demand by proxy. Data formats for SBOMs exist supported by a variety of approaches, some of which are recognized as an ISO standard. As already mentioned, there are already SBOM supply side tool activities in process to help address what is expected to be a rapidly growing demand. The market for SBOMs is likely to evolve rapidly and has the potential to evolve even faster through support by the leading worldwide software vendors.

Methodology

This section explains our approach to sampling, data segmentation, and how we aggregated responses to SBOM readiness into a measure of SBOM maturity.

Who We Surveyed and How We Analyzed the Data

The objective of this research is to understand organizational readiness in the production and consumption of SBOMs. The techniques employed included quantitative survey-based and qualitative interview-based research. The quantitative aspect of this project included a worldwide survey of technology professionals that was fielded between June, 2021, and August, 2021. The survey was offered in six languages beyond English: Chinese (simplified), Japanese, Korean, French, German, and Russian. Respondents were sourced from two constituencies: Linux Foundation community members and technology professionals from a third-party panel. Target respondents were IT decision-makers and line of business leaders at end-user enterprises, technology vendors, solutions and service providers, and public sector organizations.

A total of 519 respondents began the survey, including 291 (56%) sourced by the Linux Foundation and 228 (44%) from the third-party market research services IT panel. Screening criteria were used to ensure that respondents would be able to answer questions throughout the survey. After screening, our sample included 412 completes of 222 (54%) organizations from the market research panel and 190 (46%) organizations randomly sourced by the Linux Foundation.

Data Segmentation and Screening

The survey data was segmented in multiple ways, providing a variety of methods to explore the data. Primary segmentation variables and definitions are as follows:

- **Data Collector, N=412.** Identifies the number of respondents (N) sourced by the Linux Foundation (46%) versus respondents sourced by a third-party panel provider (54%). Margin of error (MoE) = +/- 4.1% @ 90% confidence level (CL).
- **Industry Type, N=405.** Identifies respondents who work for a technology vendor or service provider (21%) versus respondents who work for an end-user enterprise (79%). MoE = +/- 4.1% @ 90% CL.
- **Primary Industry Group, N=405.** Aggregates worldwide respondents from 22 industries into six primary industries (and “other”): technology vendors, solutions, and service providers (25%), automotive (12%), healthcare and life sciences (11%), manufacturing (7%), financial services (6%), energy (5%), and other (34%). MoE = +/- 4.1% @ 90% CL.
- **Geographic Region, N=402.** Aggregates worldwide respondents from ten countries into the three primary geographic regions: the Americas (44%), Western Europe (39%), and Asia Pacific (17%). MoE = +/- 4.1% @ 90% CL.
- **SBOM Readiness, N=357.** An aggregation of self-selected responses based on the respondent’s belief as to their organization’s SBOM readiness: innovators (21%), early adopters (51%), procrastinators (24%), and don’t know or not sure (4%). MoE = +/- 4.3% @ 90%.
- **SBOM Qualified Respondents, N=341.** Based on a self-assessment question that asks if a respondent felt qualified to answer questions about software bills of materials: respondents who felt qualified to answer SBOM questions (83%), respondents who felt unqualified to answer SBOM questions (11%), and respondents who didn’t know or were not sure (5%). MoE = +/- 4.5% @ 90%.

All figures in this survey include results that are rounded to the nearest whole integer percent value. Therefore, totals for segmentation data may not always add to 100%.

This was a long survey, with an average time to complete of 20+ minutes, and the completion rate for the survey was 64%. This explains why there is some variation in the sample size for the above segmentation variables.

Comprehensive screening criteria was used to ensure respondents would have a high probability of being able to answer all survey questions. Screening criteria included familiarity with specific IT

issues, IT domain experience, a senior role in IT or a similar line of business, and employment in an established industry.

The qualitative dimension of this project included in-depth interviews with selected individuals across industries and in federal cybersecurity policy development.

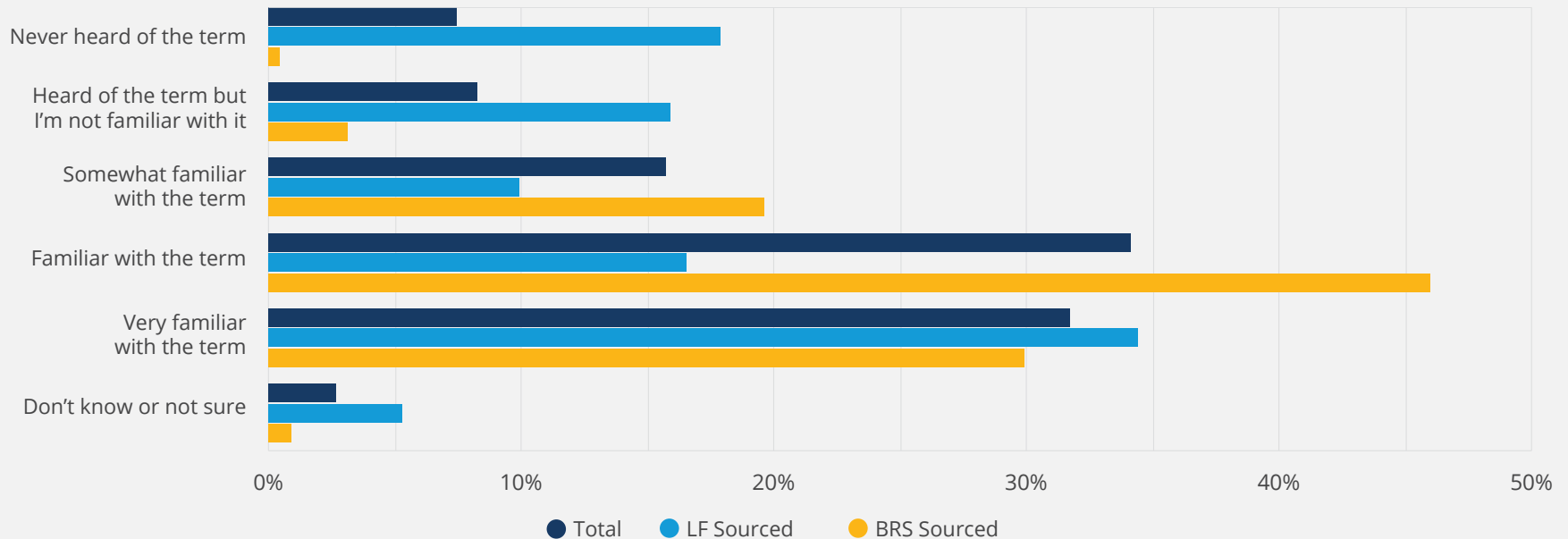
Protecting Against Sample Bias

Survey respondents were initially sourced from Linux Foundation (LF) community members. From a research standpoint, this had the potential to invite bias into the sample. For this reason,

FIGURE 30

What is your organization's familiarity with a software bill of materials (SBOM)?

Single Response | Segmented by data collector | N = 375



respondents were also sourced from a third-party market research panel provider. In order to determine if there is a relationship between the two samples, significance testing was employed. A significant difference was found between the two samples for most variables in the data set. **FIGURE 30** shows SBOM familiarity segmented by data collector, which is indicative of the differences we found.

The LF data shows a bimodal distribution showing a significant group (34%) who had never heard of SBOMs or were not familiar with SBOMs, and another group (51%) who was familiar or very familiar with SBOMs. This is consistent with participants in the LF community, which contains a group of young IT professionals, early in their career, who come to the LF for training and certifications as a way to improve their skill sets and increase employment opportunities. It is not surprising that this segment is unfamiliar with SBOMs. There also exists another group within the LF that includes highly experienced IT professionals who have important roles in IT decision-making and policy. This group is likely to have a high familiarity with SBOMs.

The research panel sourced data shows very different characteristics, with data somewhat normally distributed across the responses. Just 4% of the research panel sample had either not heard of the SBOM term or was not familiar with the term, which contrasts with the majority of the research panel sample (76%) that is either familiar or very familiar with SBOM terminology.

This comparison is simply one of many that show that the LF and research panel samples are significantly different. The fact that these two samples are different, with the research panel sample having a high familiarity with SBOMs, and the LF sample having a much lower familiarity, enables us to provide a conservative view of SBOM readiness.

Respondent Ability to Answer SBOM Questions

After providing respondents with an SBOM definition, the survey asked if the respondent felt qualified to answer questions about how their organization uses or intends to use SBOMs. The purpose of this question was another method to understand SBOM familiarity, as well as provide the ability to segment out those respondents without SBOM knowledge. **FIGURE 31** shows if respondents felt qualified to answer questions about SBOMs segmented by SBOM maturity.

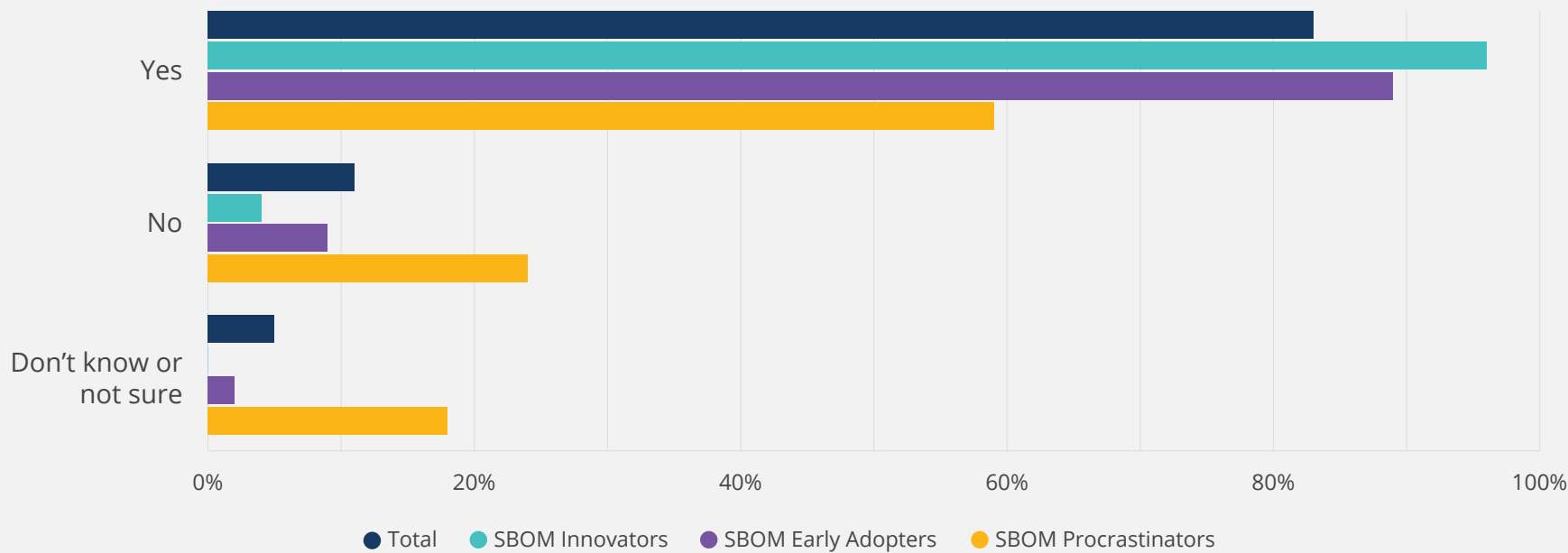
Overall, most respondents (83%) felt qualified to answer questions about SBOM usage, 11% did not feel qualified to talk about SBOM use, and 5% didn't know or were not sure. SBOM qualified responses were highly correlated with SBOM maturity. Higher levels of SBOM maturity were correlated with higher levels of SBOM qualified respondents and lower levels of unqualified respondents. **FIGURE 31** shows that 96% of SBOM innovators felt qualified to answer SBOM questions, compared to 89% of SBOM early adopters and just 59% of SBOM procrastinators. The highest proportion of respondents who did not feel qualified to answer SBOM questions (24%) or answered DKNS (18%) were SBOM procrastinators.

In the survey, respondents were asked to continue answering all SBOM questions, regardless of how qualified they felt. For the purpose of the SBOM analysis in this report, we have elected to use data from all respondents who completed the survey. This does not actually pose a problem, because unqualified respondents nearly always responded DKNS to follow-on SBOM questions.

FIGURE 31

Do you feel qualified to answer a questions about how your company uses/intends to use SBOMs?

Single Response | Segmented by SBOM maturity | N = 341



Endnotes

- 1 International Monetary Fund, World Economic Outlook Database, 2019 data.
- 2 For geographical region segmentations, see the following figures in this report: Figure 3, A9, A10, A11, A14-A17
- 3 “Executive Order on Improving the Nation’s Cybersecurity,” May 2021, available at <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity>
- 4 Id. at Section 1.
- 5 “SBOM at a Glance,” National Telecommunications and Information Administration, April 27, 2021, available at https://www.ntia.gov/files/ntia/publications/sbom_at_a_glance_apr2021.pdf.
- 6 The Minimum Elements for a Software Bill of Materials (SBOM), US Department of Commerce, July 12, 2021
- 7 Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations, National Institute of Standards and Technology, SP.800-161r1-draft2, October 2021
- 8 SBOM Options and Decision Points, National Telecommunications and Information Administration, April 27, 2021
- 9 SBOM at a Glance, National Telecommunications and Information Administration, April 27, 2021

Appendix A: Demographics and Additional SBOM Readiness Information

Appendix includes graphics to further describe sample demographic, current IT environments, and SBOM readiness. The following charts are included:

- A1** Total company employees
- A2** Primary role
- A3** Primary areas of responsibility
- A4** Organization's primary industry
- A5** For IT industry organizations, type of IT organization
- A6** Are you a Linux Foundation member company?
- A7** Respondents by geographic region
- A8** Organization annual revenues
- A9** Organizational familiarity with SBOMs by geographic region
- A10** Presence of OSPO in the organization by geographic region
- A11** Does OSPO share its inventory of projects with the security team by geographic region?
- A12** Presence of Chief Security Officer/security team in the organization by geographic region
- A13** Where in the software lifecycle are organizations producing SBOMs by SBOM maturity?
- A14** Where in the software lifecycle are organizations consuming SBOMs by SBOM maturity?
- A15** SBOM readiness by geographic region
- A16** Organizational concern about software security by geographic region
- A17** Organizational awareness of U.S. Executive Order on Cybersecurity by geographic region
- A18** Changes in response to U.S. Executive Order on Cybersecurity by geographic region
- A19** Organizational plans for producing SBOMs by primary industry
- A20** Organizational plans for consuming SBOMs by primary industry

FIGURE A1

Please estimate how many total employees your company has worldwide?

Single Response | N = 412

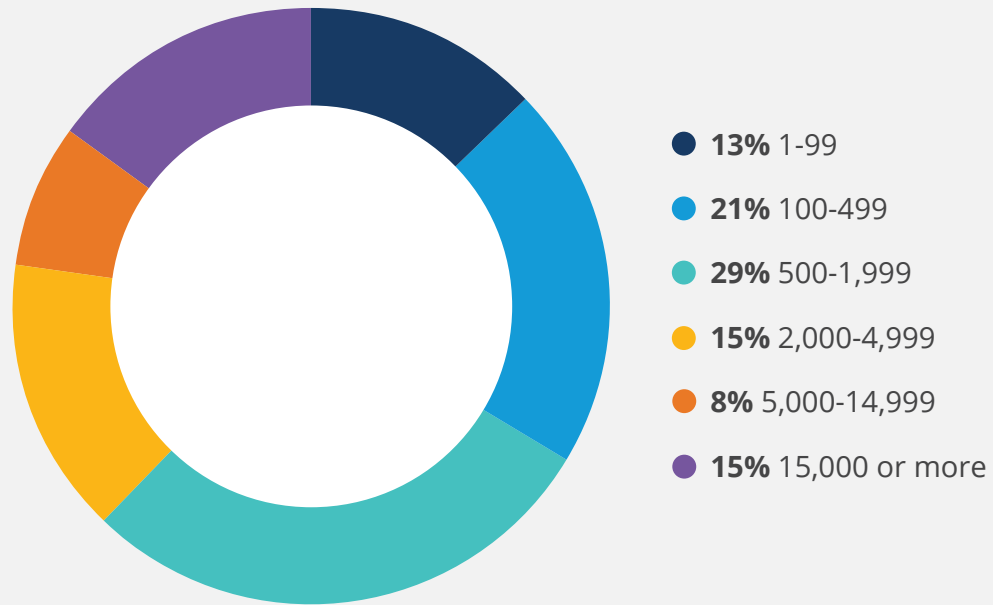


FIGURE A2

Which of the following best or most closely describes your primary job role or title within your organization or as a contractor?

Single Response | N = 412

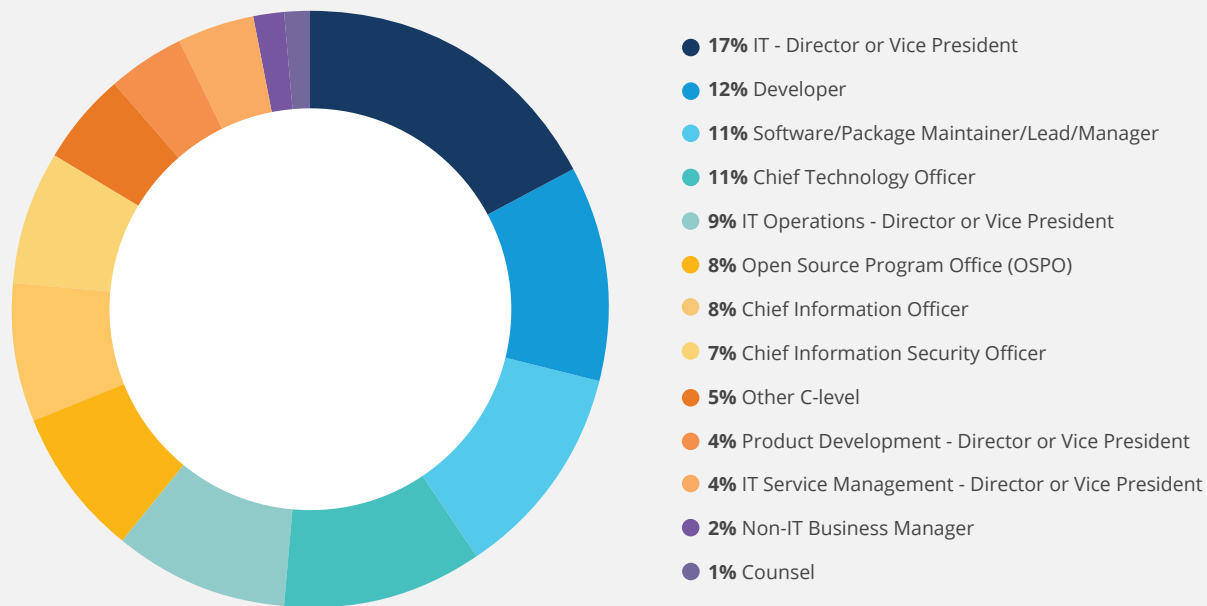


FIGURE A3

What are your primary areas of responsibility?

Select all that apply | N = 407, Valid Cases = 407, Total Mentions = 1,227

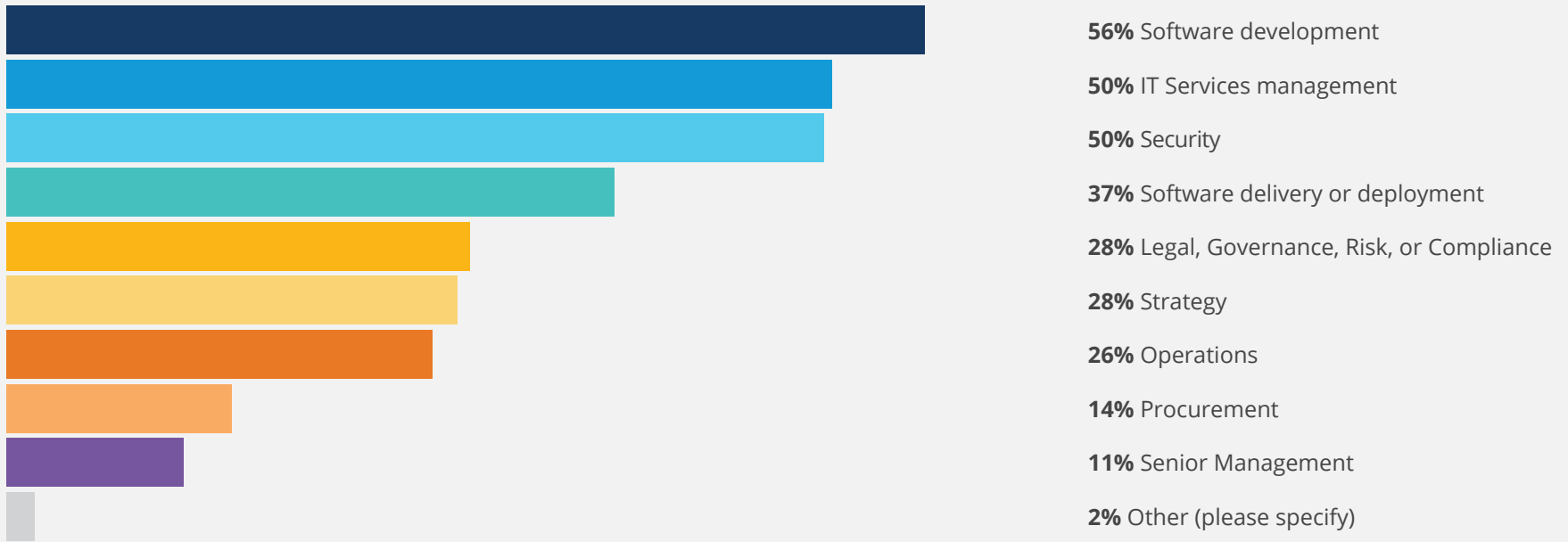


FIGURE A4

What is your organization's primary industry?

Single Response | N = 405

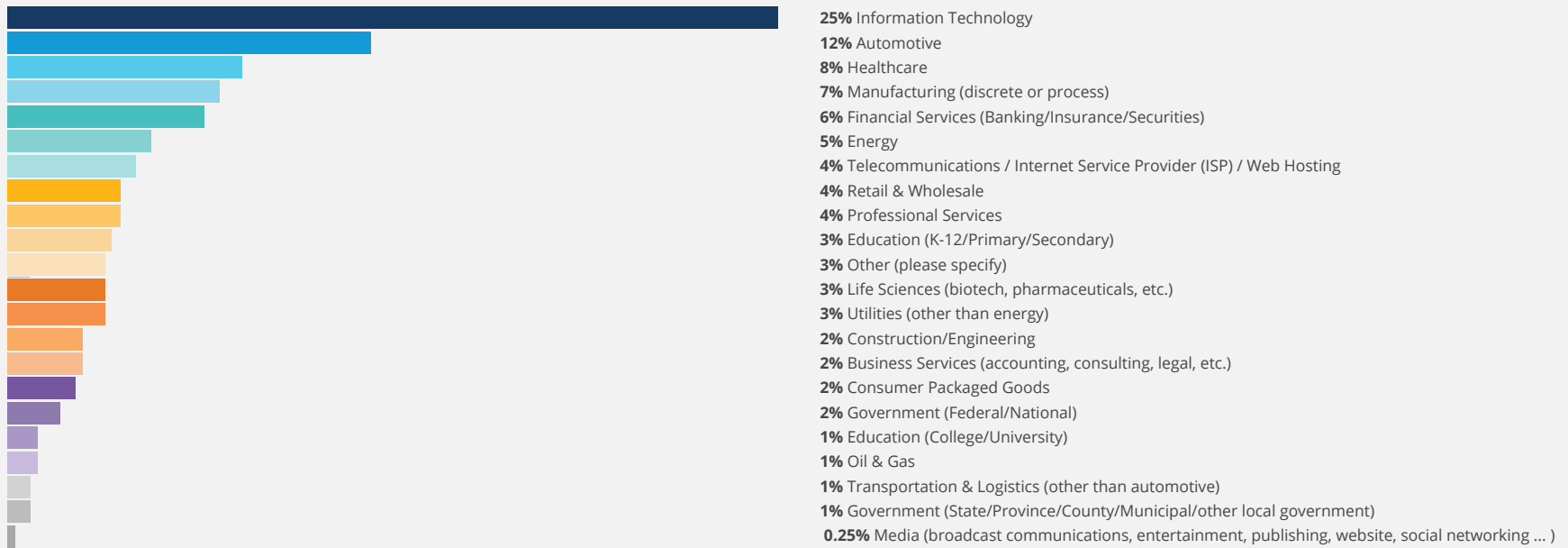


FIGURE A5

What type of information technology organization do you work for?

Select all that apply | N = 101, Valid Cases = 101, Total Mentions = 220

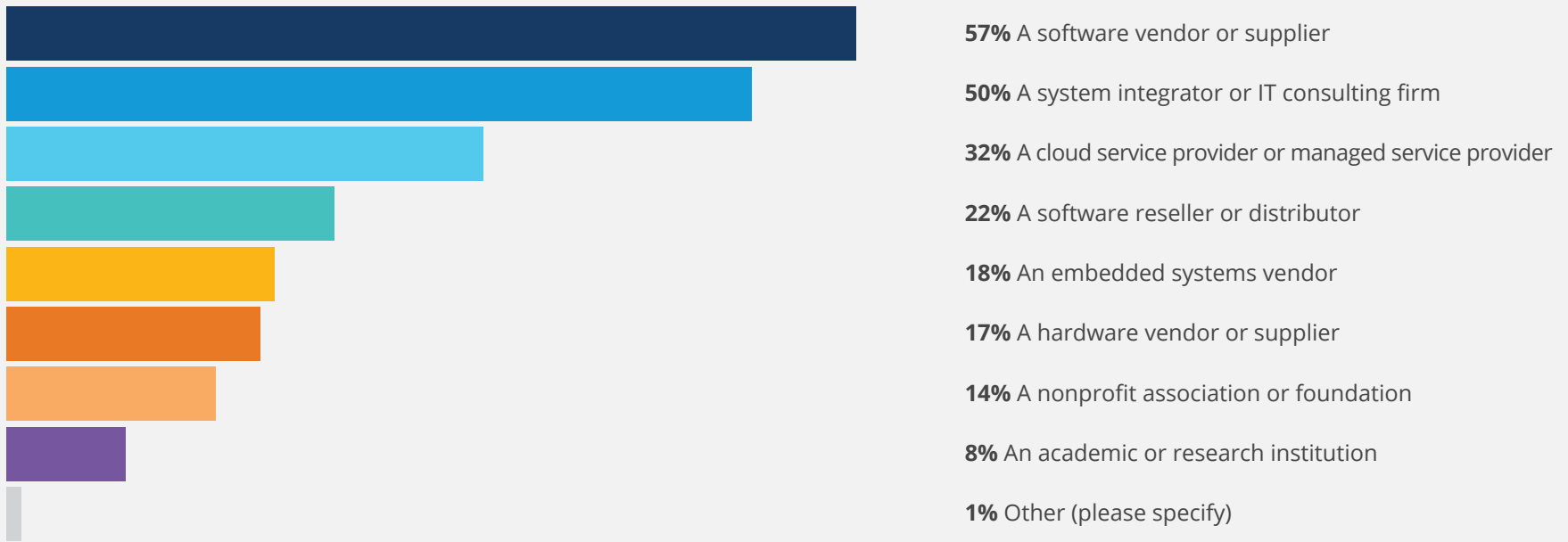


FIGURE A6

Do you work for a Linux Foundation member company?

Single Response | N = 404

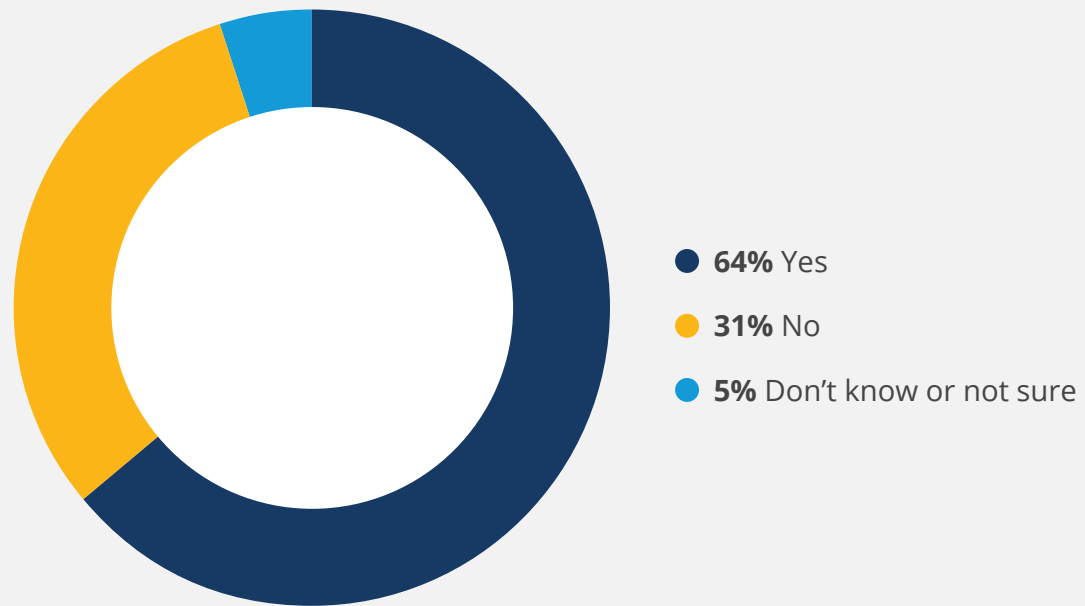


FIGURE A7

What geographic region do you live in?

Single Response | N = 402

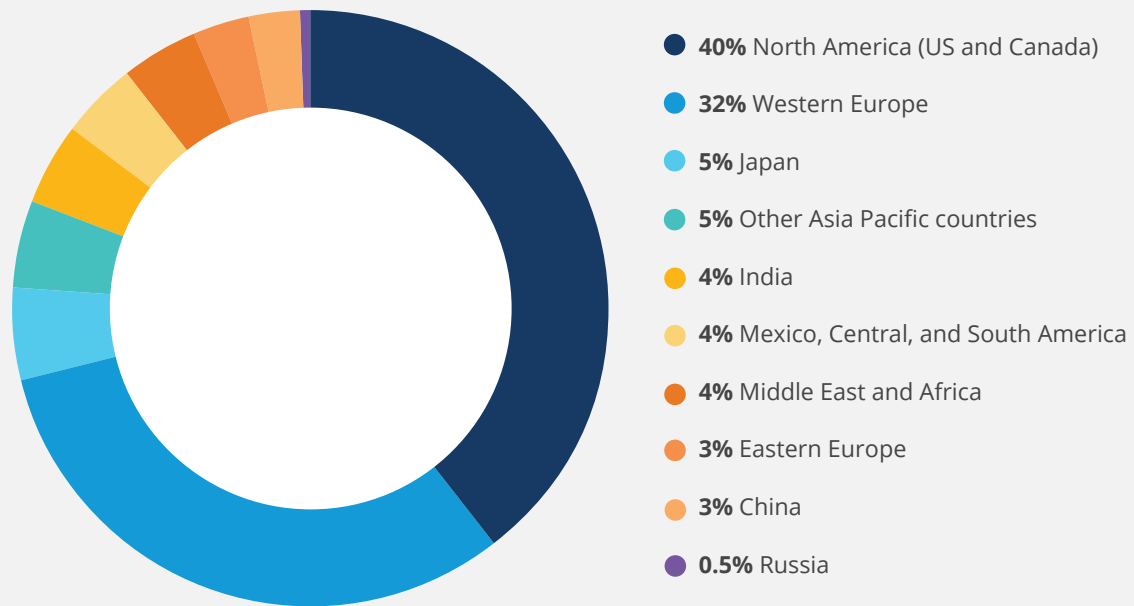


FIGURE A8

About what was your organization's annual revenue in 2020?

Single Response | N = 402

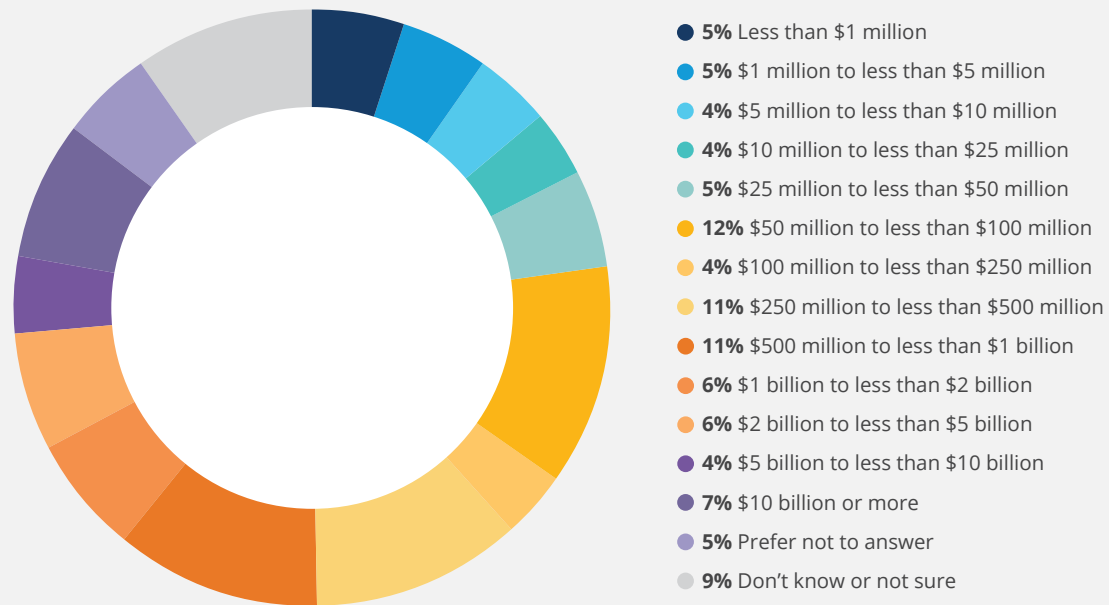


FIGURE A9

What is your organization's familiarity with a software bill of materials (SBOM)?

Single Response | By geographic region | N = 361

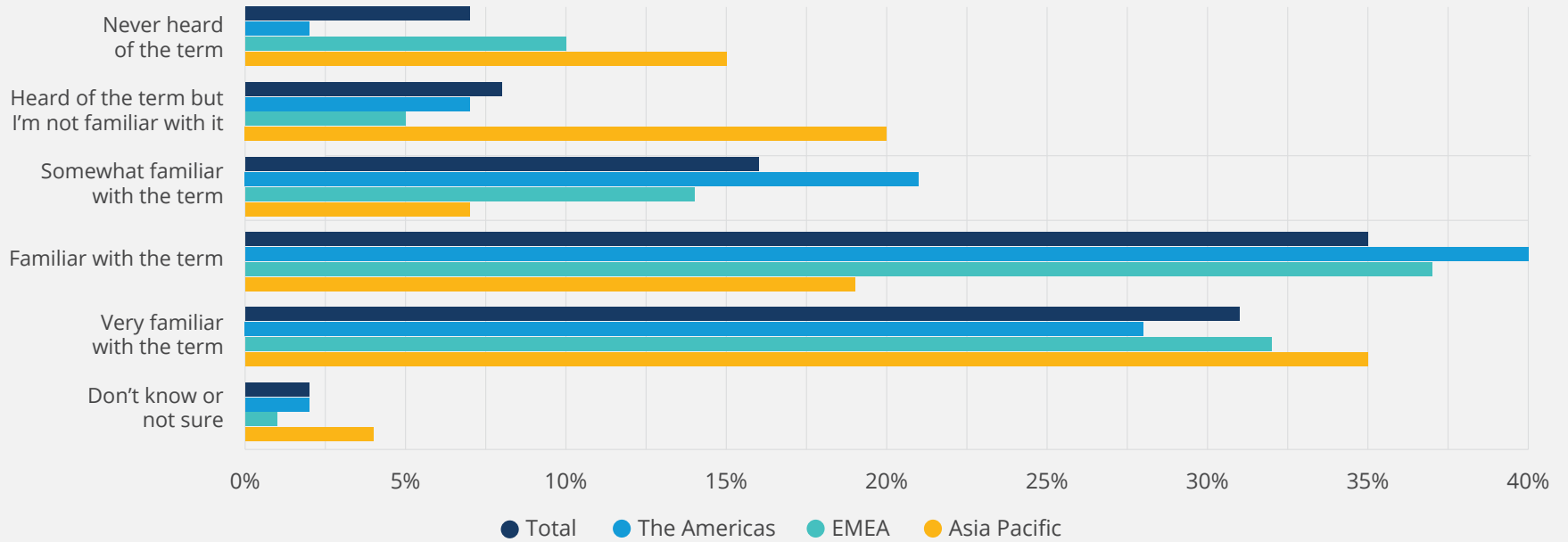


FIGURE A10

Does your organization have an Open Source Program Office (OSPO) to provide oversight on open source software use?

Single Response | By geographic region | N = 390

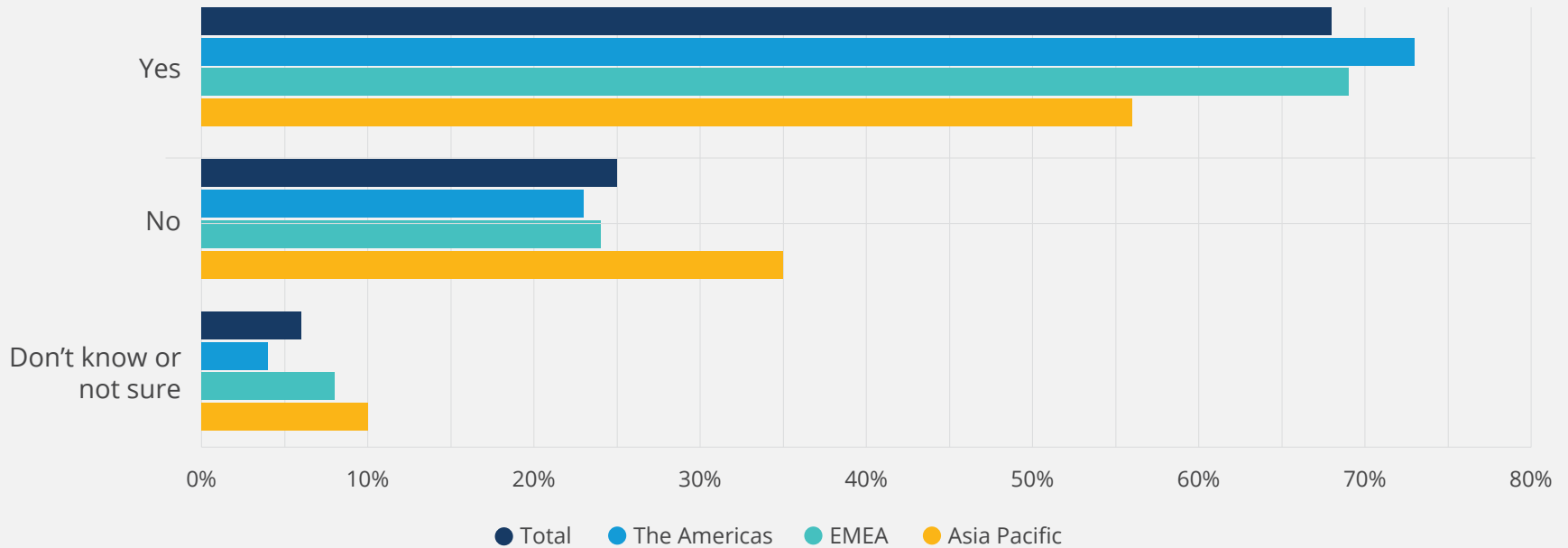


FIGURE A11

Does your Open Source Program Office share a common inventory of open source projects being tracked with your security team(s)?

Single Response | By geographic region | N = 384

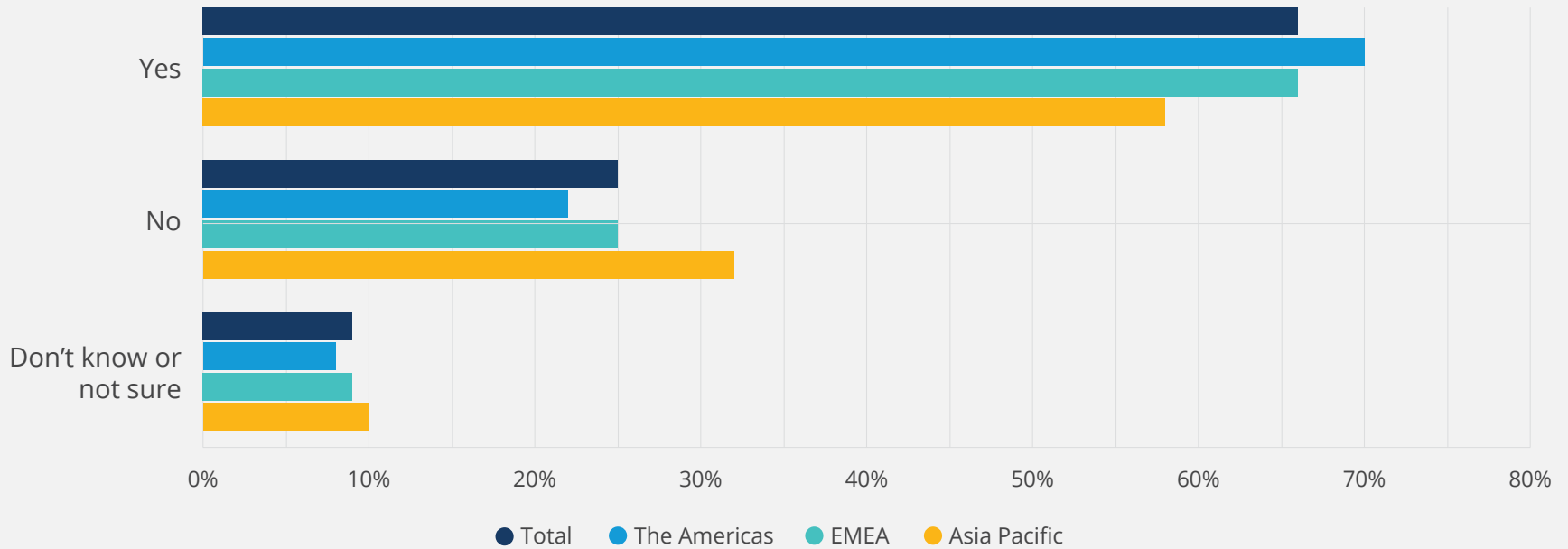


FIGURE A12

Does your organization have a Chief Information Security Officer (CISO)/security team that monitors upstream open source projects for vulnerabilities?

Single Response | By geographic region | N = 388

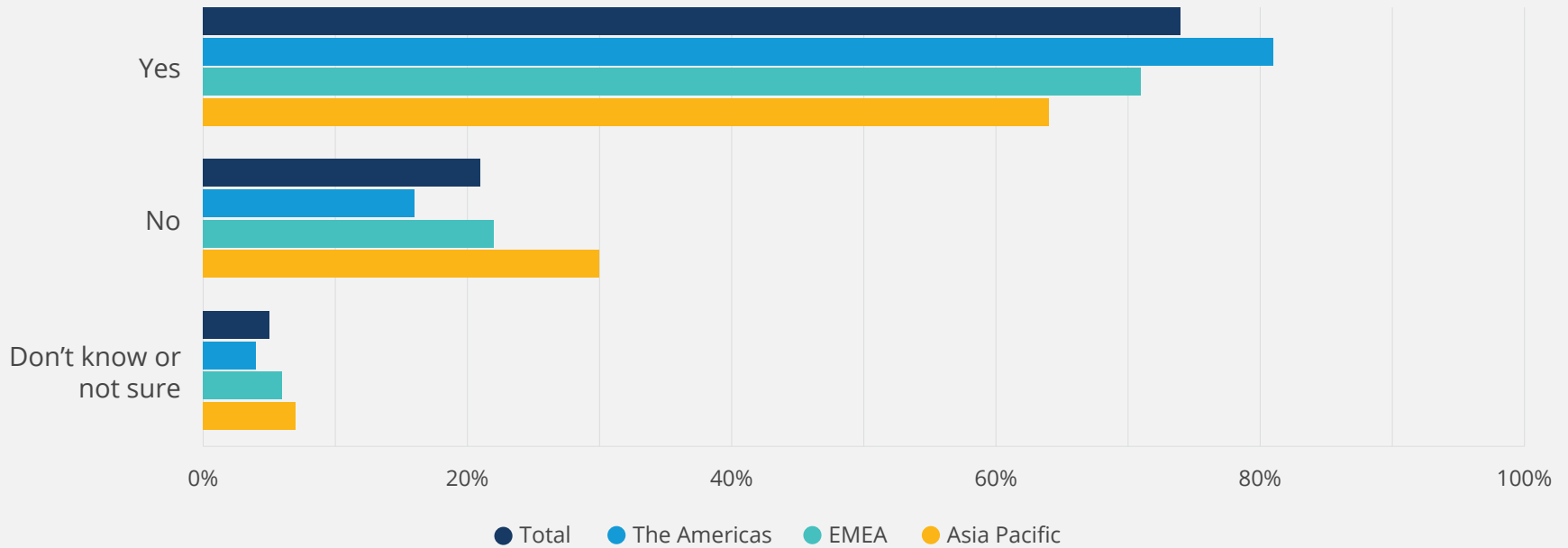


FIGURE A13

Where in the software development lifecycle is/will your organization be producing SBOMs?

Select all that apply | By SBOM maturity | N = 335, Valid Cases = 335, Total Mentions = 849

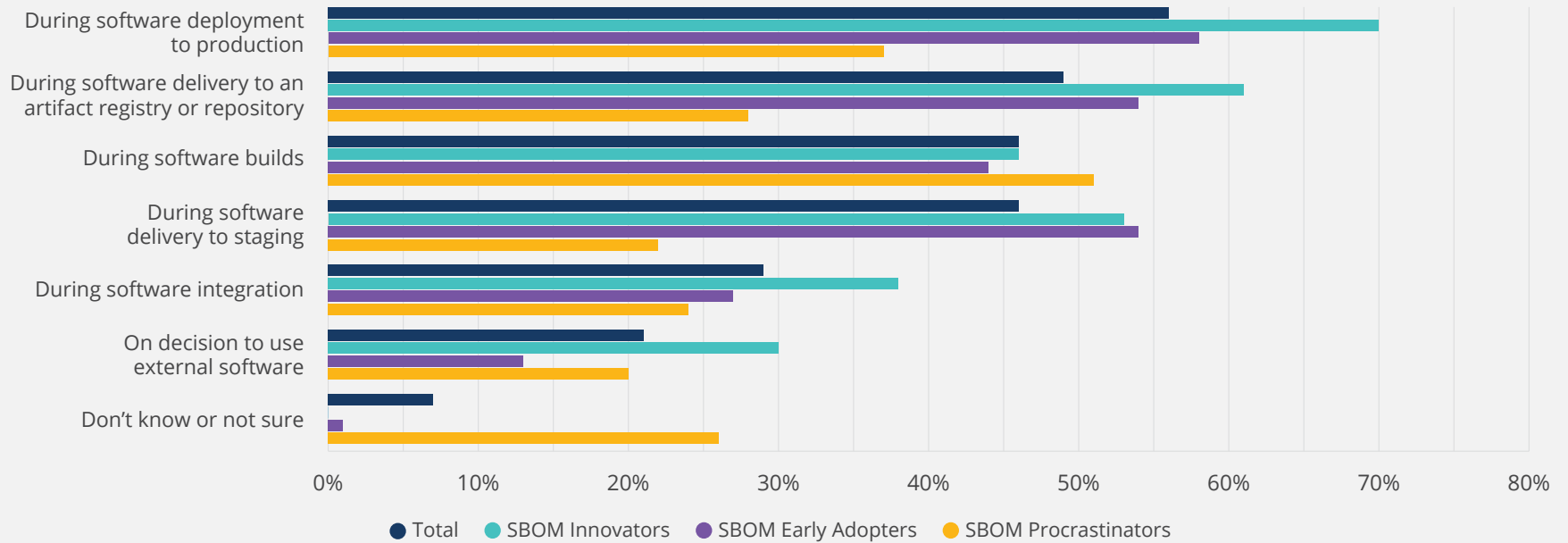


FIGURE A14

Where in the software development lifecycle is/will your organization be consuming SBOMs?

Select all that apply | By SBOM maturity | N = 325, Valid Cases = 325, Total Mentions = 896

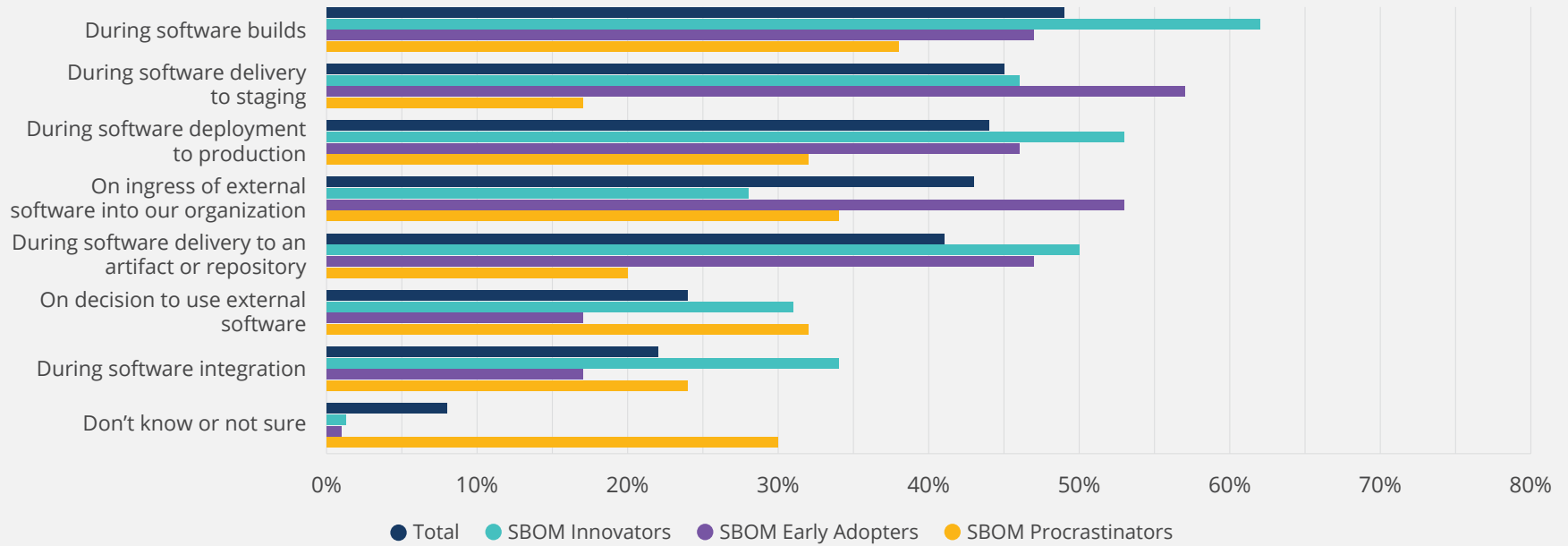


FIGURE A15

What is your group's current SBOM readiness?

Single Response | By geographic region | N = 357

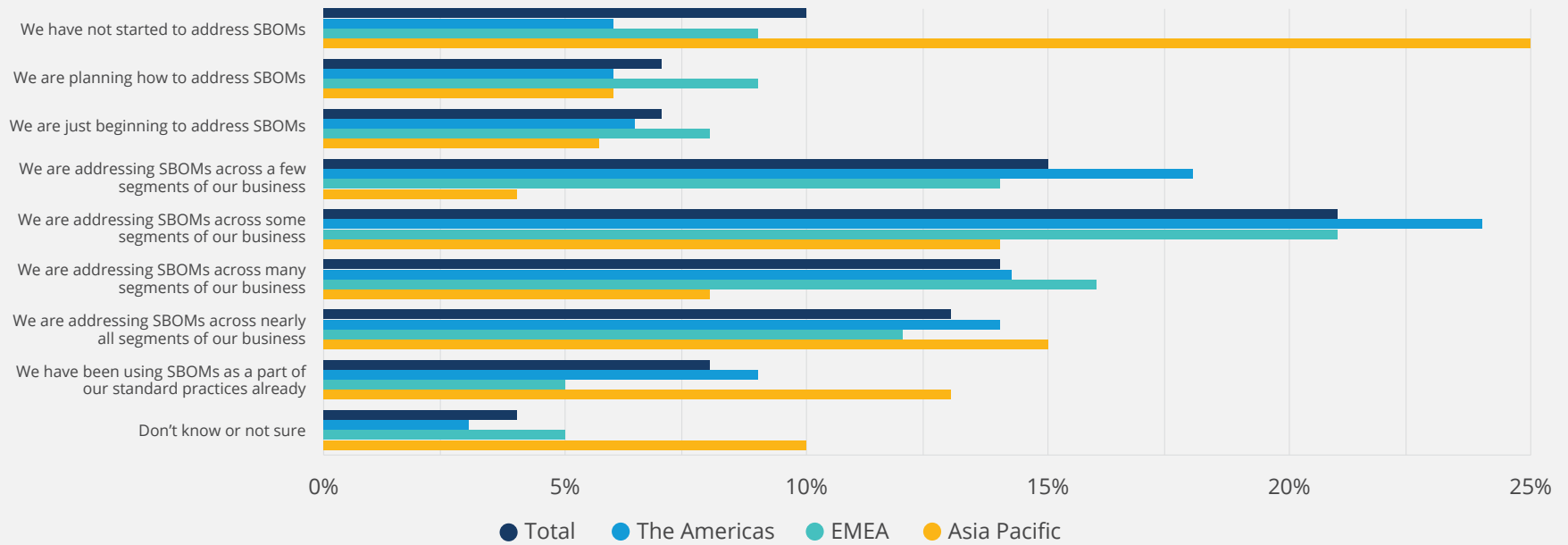


FIGURE A16

How concerned is your organization about the security of the software that it uses?

Single Response | By geographic region | N = 363

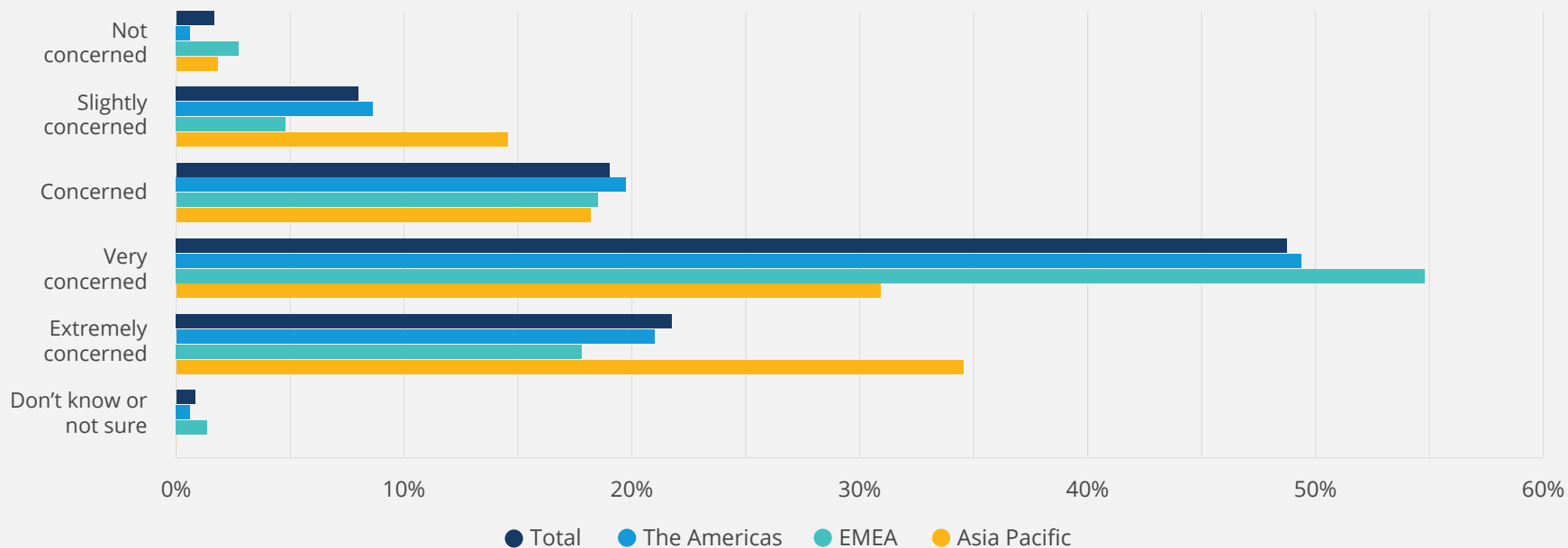


FIGURE A17

Is your organization aware of the recent US Executive Order on Cybersecurity that mentions a software bill of materials?

Single Response | By geographic region | N = 362

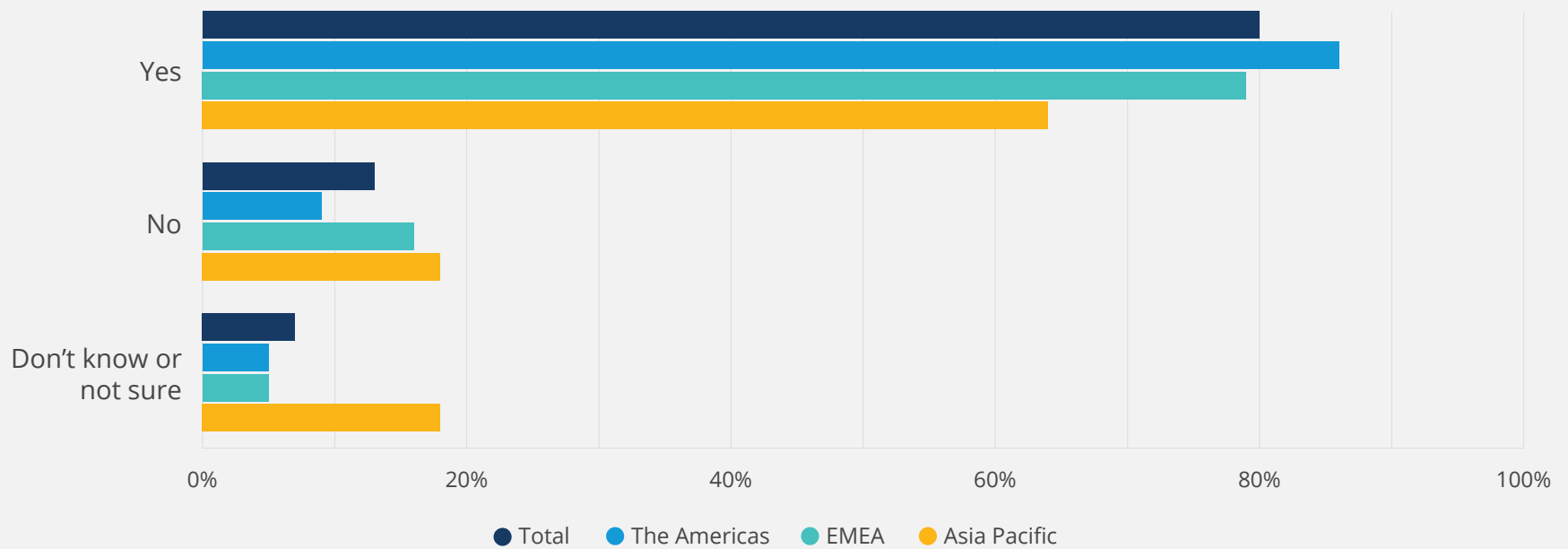


FIGURE A18

Is your organization considering any changes in response to the US Executive Order on Cybersecurity?

Single Response | By geographic region | N = 290

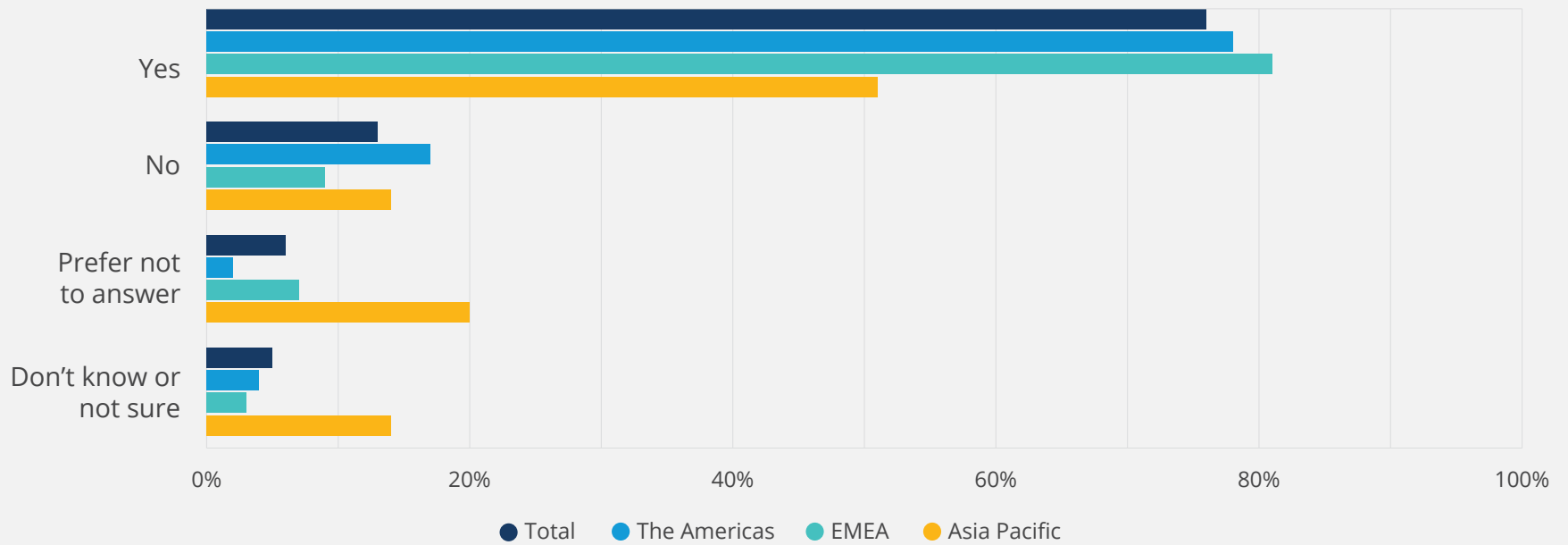


FIGURE A19

What are your organization's plans for producing SBOMs?

Single Response | By primary industry | N = 352

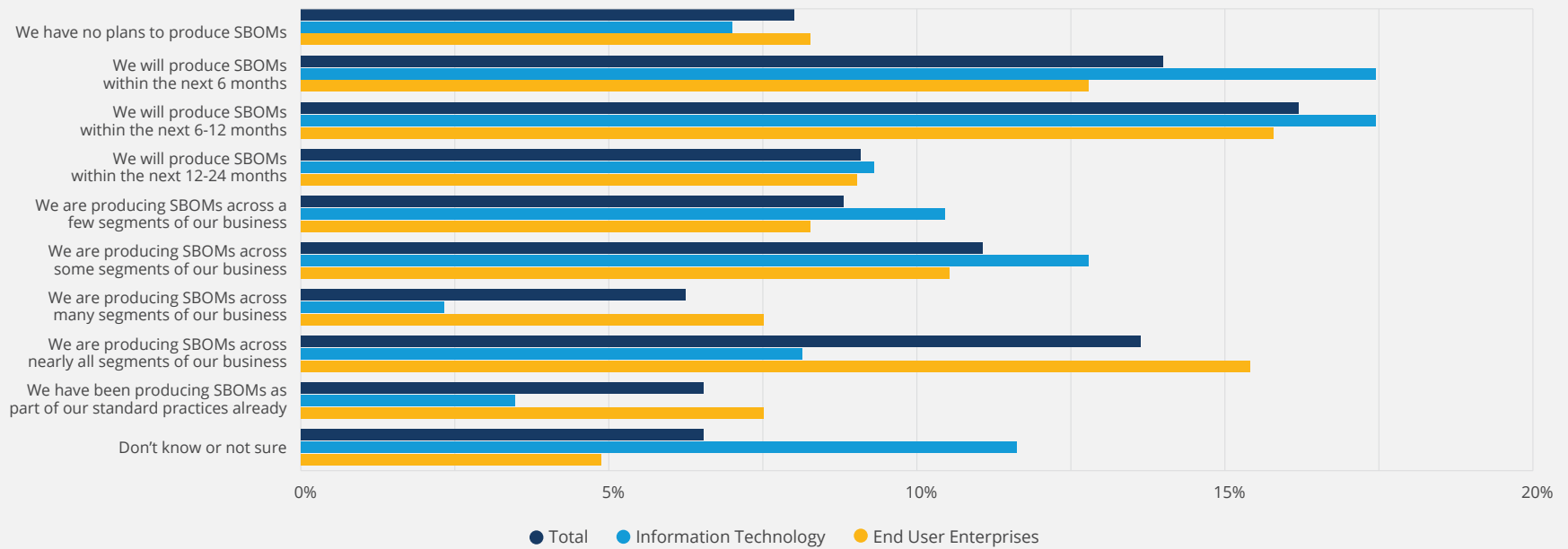
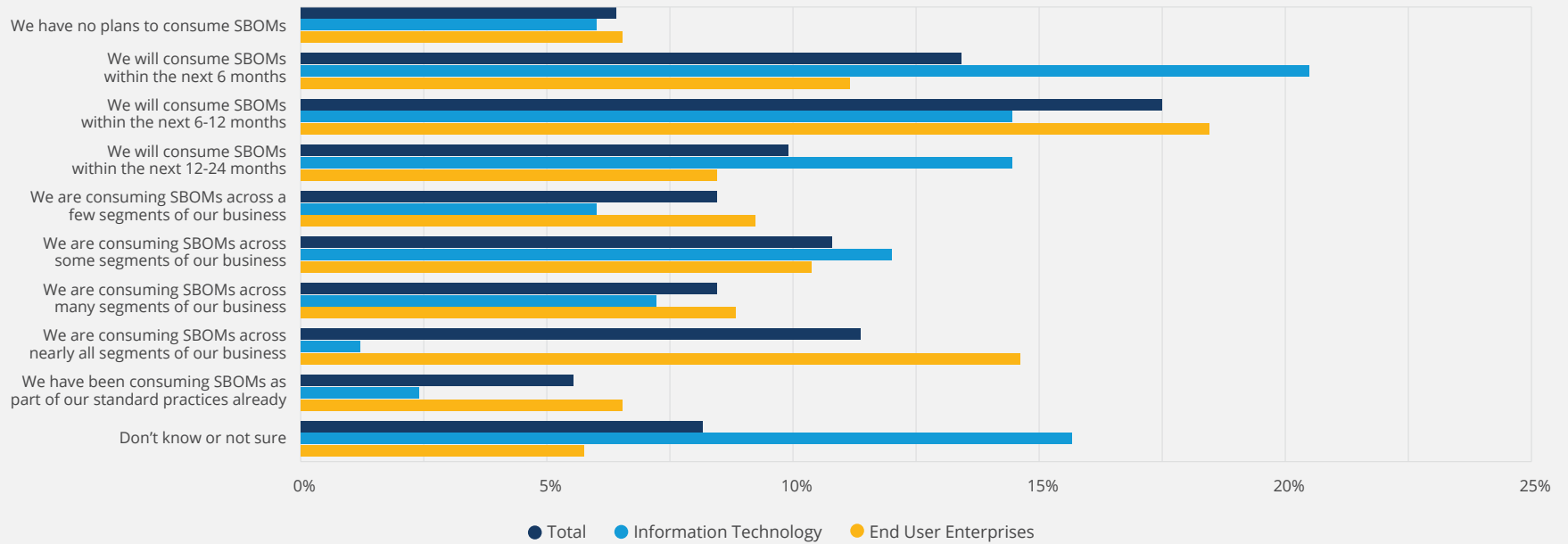


FIGURE A20


What plans does your company have for consuming SBOMs?


Single Response | By primary industry | N = 343





Disclaimer

This report is provided “as is.” The Linux Foundation and its authors, contributors, and sponsors expressly disclaim any warranties (express, implied, or otherwise), including implied warranties of merchantability, non-infringement, fitness for a particular purpose, or title, related to this report. In no event will the Linux Foundation and its authors, contributors, and sponsors be liable to any other party for lost profits or any form of indirect, special, incidental, or consequential damages of any character from any causes of action of any kind with respect to this report, whether based on breach of contract, tort (including negligence), or otherwise, and whether or not they have been advised of the possibility of such damage. Sponsorship of the creation of this report does not constitute an endorsement of its findings by any of its sponsors.

 twitter.com/linuxfoundation

 facebook.com/TheLinuxFoundation

 linkedin.com/company/the-linux-foundation

 youtube.com/user/TheLinuxFoundation

In partnership with:



Linux Foundation Research explores the growing scale of open source collaboration, providing insight into emerging technology trends, best practices, and the global impact of open source projects.



Copyright © 2022 [The Linux Foundation](https://www.linuxfoundation.org/)

This report is licensed under the [Creative Commons Attribution-NoDerivatives 4.0 International Public License](https://creativecommons.org/licenses/by-nc-nd/4.0/).

To reference the work, please cite as follows: Stephen Hendrick, "Software Bill of Materials (SBOM) and Cybersecurity Readiness," foreword by Jim Zemlin, The Linux Foundation, January, 2022.