

软件材料清单 (SBOM) 与网络安全准备度

2022年1月

Stephen Hendrick, Linux基金会研究院副总裁

前言: Jim Zemlin, Linux基金会执行董事

与合作伙伴关系:



目录

- 前言 4
- 摘要 6
- 导言 8
 - 网络安全: 全球关注的问题..... 8
 - 美国的网络安全 8
 - SBOM成熟度.....10
- 受访对象统计11
 - 按地理区域划分的SBOM成熟度11
- 软件安全的重要性14
- 开源成熟度和 SBOM 准备程度之间的关系 15
 - SBOM 创新者在使用开源软件时是否更容易出现风险?.....15
 - 有条件使用开源16
 - 开源软件的使用随SBOM的成熟度的变化17
 - 软件安全的核心关注18
 - 企业为何关注软件安全19
- 网络安全和SBOM 的推进20
 - 美国网络安全行政令-认识与行动20
 - 网络安全和软件供应链的优先事项强调SBOM21
- 对SBOM的要求.....24
 - 机构希望SBOM具有丰富的元数据24
 - 机器可读性是SBOM的关键指标25
 - SBOM应当识别已知和未知的依赖传递.....25
 - SBOM应该随着每次代码变更而更新25
 - SBOM元信息应该与模块绑定.....27
 - SBOM应在发现漏洞时及时反馈28
 - SBOM的准备情况和按SBOM成熟度划分28

目录

- SBOM生产观点..... 30
 - SBOM生产30
 - 生产SBOM的益处31
 - 生产SBOM的担忧33
- SBOM消费观点..... 35
 - SBOM消费36
 - 消费SBOM带来的收益.....36
 - 消费SBOM的担忧36
- 结论 38
 - 如何改进SBOM39
 - SBOM的重要性41
 - SBOM的未来.....42
- 调研方法 44
 - 我们调查了谁，如何分析数据..... 44
 - 数据分类和筛选 44
 - 防止样本偏差45
 - 受访者回答SBOM问题的能力.....46
- 尾注47
- 附录 A: 人口统计资料和附带的SBOM就绪水平信息 48
- 免责声明69

前言

虽然开源社区持续加速软件、硬件和标准的创新，但软件网络安全问题一直吸引着我们的注意。2021年网络安全攻击可谓是一波未平，一波又起。在SolarWinds Orion网络攻击事件曝光不到一年的时间，2021年底，与ApacheLog4j有关的另一场安全危机又掀起波浪。然而，不可否认的是，开源已经成为一个巨大的攻击载体，我们的社区和生态系统需要在标准、流程、教育和工具等方面共同努力，以减轻全球供应链的风险。尽管这一年网络安全方面的投入和合规遵从度上都有显著提升，但软件供应链方面，无论是主动预防还是被动防御上，仍有很多的工作要做。这不是开源独有的问题，但开源创新常常引领解决群体问题的道路，这不是任何一个组织可以单独解决的问题。

很明显，跟一年前相比我们已经有了很大的进步。美国最重要的进展之一是，拜登政府发布了《关于改善国家网络安全的行政命令》，全球科技行业都感受到了这一影响。这一风向标将软件物料清单（SBOM）置于软件采购实践的前沿。美国并不是唯一这样做的国家，其他国家已经讨论或正在计划如何实施类似的要求。意识到软件成分分析是降低软件漏洞风险的重要环节，已成为全球软件安全的一个重要里程碑。

幸运的是，我们已经有了SBOM应用标准和相应工程工具，以便在整个供应链中加强软件安全相关的活动和实践。SBOM将在软件供应链的供（软件构建和分发），需（软件使用）两侧，在端到端构建信任和透明度方面承担不可或缺的角色。去年我们也看到SPDX标准获得了ISO/IEC JTC15962:2021国际认可。SPDX和其他社区开发的工具集对于SBOM的采用和产业化应用至关重要。SPDX已经在一些世界上最大的商业供应链的软件安全和完整性方面发挥了重要作用。日立、三星、微软、英特尔、思科、西门子、谷歌等公司在SPDX的SBOM格式的采用和消费上已经有了多年的实践。我们预计在未来的几年里，这一领域会有显著发展，我们希望能够洞悉到SBOM生态系统的新进入者所面临的痛点和挑战，制定对策，从而可以让他们更容易地借鉴和应用SBOM的业界最佳实践。

除SBOM之外，我们还在以安全为重点的项目社区做了投入。在领导型/前瞻型企业的支持下，我们加大了对开源安全基金会（OpenSSF）的投入，提供更多工具、服务、培训、基础设施和资源来解决网络安全漏洞。

而且，重要的是，我们加强了调查研究，以使得我们能在更大领域内就网络安全范围挑战达成共识。Linux基金会启动了一系列以探索与实施网络安全最佳实践和标准采用为核心项目的调查研究，其中首要的就是对SBOM能力准备度的调查。本报告清晰地描绘了SBOM在业界的状态，包括熟悉度、采用度及面临的挑战，以此为基础来开展未来在业界对SBOM的实施的协同工作。

我们希望，世界各地的网络安全和IT专业人士能够获悉这份高信息量的SBOM和网络安全准备度报告；我们鼓励你阅读本文，与业内同行和供应链合作伙伴分享，并在您的组织中进行必要的调整，以SBOM和其他安全实践来提升组织的网络安全的管理效率。



Jim Zemlin

Linux基金会执行董事

根据调查显示，
98% 的受访组织使用开源软件。



图 6 | 第 15 页



根据调查显示，
95% 的受访组织担心软件安全。

图 9 | 第 18 页

根据调查显示
目前, 76% 的受访组织对于 SBOM 有一定的认知。



图 20 | 第 29 页



根据调查显示，
如今, 47% 的受访组织正在使用 SBOM。

图 21 & 24 | 第 30 页

SBOM 的使用将增加 66%。
f2022 年各组织对于



图 29 | 第 43 页



根据受访组织的调查显示，
2022 年使用 SBOM 的组织将会达到 78%。

图 29 | 第 43 页

根据受访组织的调查显示，
2023 年使用 SBOM 的组织将会达到 88%。

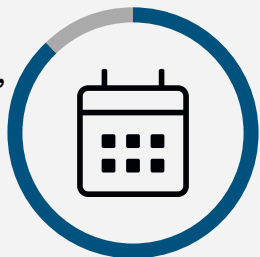


图 29 | 第 43 页



如今使用 SBOM 的组织，
74% 的组织同时生产和消费 SBOM。

图 21 & 24 | 第 30 页

#1 行动：
获取漏洞报告系统
为了更好的保障您的软件供应链安全。



图 13 | 第 23 页

#2 行动：
使用 SBOM 来保障您的软件供应链安全。



图 13 | 第 23 页

当生产 SBOM 时.....
#1 收益：
D 能让开发者更好的理解依赖。



图 22 | 第 31 页

当消费 SBOM 时.....
#1 收益：
更好的支持合规与报告。



图 25 | 第 37 页

摘要

软件物料清单 (SBOM) 是一种正式的且机器可读的元数据,可唯一标识软件组件、其依赖项和许可证信息。SBOM数据格式正在不断衍化,也许很快就可以提供信息来验证组件的真实性,并提供已知漏洞的链接。SBOM旨在跨组织共享,特别有助于提高软件组件的透明度,尤其是当这些组件是由供应链中的参与者交付提供的。有些企业非常关注软件安全,他们正将SBOM作为网络安全战略的基石。

2021年第三季度, Linux Foundation Research在全球范围内, 对企业SBOM的准备和采用情况进行了实证研究。来自世界各地的412家组织参与了这项调查。该调查的主要结果在本报告中给出, 本研究的重要发现如下:

1. 研究中98%的企业关注其软件的安全性, 72%的企业非常或极度关注软件安全性。亚太地区对软件安全的担忧最高, 有35%的企业极度关注, 相比之下, 美洲为21%, EMEA (欧洲、中东和非洲) 仅为18%, 如图1及图A16所示。
2. 安全性是影响企业选择软件的第一考虑因素, 许可证合规性是第二考虑因素, 即使考虑第二梯队和第三梯队各因素的优先级, 安全性和许可证合规性仍是最重要的考虑因素, 如图5。
3. 企业关注软件安全的主要原因包括财务风险 (66%)、声誉风(61%)和法律风险 (53%)。这些都是潜在的存在性风险, 它们解释了一个必要性问题, 即要强调软件安全问题的策略连贯性, 如图 10。
4. 美国《关于改善国家网络安全的行政命令》正在影响全球。总体而言, 全球超过80%的企业知晓这项白宫行政命令, 76%的企业考虑根据这项命令进行整改, 如图11和12所示。
5. 确保软件供应链安全的关键活动都强调了SBOM的有效性。总体而言, 47%的组织需要可持续更新的漏洞报告, 45%的组织将SBOM视为确保软件供应链安全的关键方法。此外, 39%的组织希望看到对全球唯一标识符的支持, 34%的组织希望通过使用可复制的构建方式来支持组件的验证。目前, 一些SBOM数据格式已经支持了组件验证和漏洞报告。全球唯一标识符也在进行中, 采用主流的数据格式URL (PURL)。总的来说, 如今的SBOM支持各式各样的活动, 以确保软件供应链的安全, 如图 13 所示。

6. 的企业已经在其少数、部分或一些业务领域中强调使用SBOM; 23%的企业将SBOM贯穿到业务的所有领域, 甚至拥有一套使用SBOM的标准做法。这意味着, 总体而言, 76%的组织在一定程度上已经做好了使用SBOM的准备, 如图20所示。
7. SBOM的生产通常与构建商业软件的企业紧密相连, 我们的调查表明SBOM正在被更广泛地采用。在我们调查的所有企业中, 只有7% 没有生产SBOM的计划, 另外有40% 的企业计划在 6-24 个月内生产 SBOM, 27% 的企业将在其业务的一些部门或多个部门内生产 SBOM。一个正面的现象是, 研究人员发现 21% 的企业几乎在其所有业务领域都在生产 SBOM, 或者有自行使用的标准做法。总体而言, 今天有 48% 的组织在某种程度上参与了SBOM的生产制作, 如图 21 所示。
8. 参与调查的人员明确了生产SBOM 的三大好处: 开发人员更容易理解应用程序组件之间的依赖关系 (51%), 更容易监控组件的漏洞 (49%), 以及更容易确认许可证的合规性 (44%), 如图 22。
9. 各个企业仍然关注SBOM的采用和使用将会如何演变。40%的企业不清楚行业对SBOM的承诺, 39% 的企业质疑行业是否就SBOM应包含的内容达成了共识, 37% 的企业不清楚SBOM为其客户提供的价值。所以在SBOM市场中存在一个二分法: 大量的企业运营参与了 SBOM, 但承诺程度比较低, 如图 23。
10. SBOM的消费反映了SBOM的生产。只有6%的企业没有使用SBOM的计划。42%的企业计划在未来 6-24个月内使用SBOM, 28%的企业在其少数几个、部分或一些业务部门使用SBOM, 几乎所有业务部门都在使用SBOM的企业占比18%, 它们有内部使用SBOM的标准做法。总而言之, 今天有46%的企业在某种程度上使用了SBOM, 如图24。
11. 使用SBOM收到的效益令人信服。53%的企业报告称, SBOM提供了一种更好的方法来满足报告和合规要求。53%的企业还表示SBOM提供的信息改进了之前基于风险的决策方式, 49%的企业表示SBOM漏洞报告, 使组织能够更快速、更直接地了解安全风险。使用SBOM的收益与生产SBOM的效益完全一致, 体现了相同的价

这项具有里程碑意义的研究，调查对象包括 IT 供应商、服务提供商和最终用户，为软件材料清单 (SBOM) 的准备和采用提供了实证观点。这项研究表明，开源软件的使用非常普遍，软件安全是组织的首要任务。随着全球范围内致力于解决软件的安全问题，SBOM 已然成为一个关键的推动者。

SBOM 的熟悉度、准备情况和采用范围比我们的预期要广泛的多。企业对 SBOM 术语的熟悉度为82%，SBOM准备就绪（积极参与解决SBOM需求）的企业占比76%。至少在一些业务部门中，SBOM的生产或消费的占比分别为48%和46%。

根据生产或消费 SBOM 的组织计划，2021 年有47%的企业正在生产或消费SBOM。在2022 年，预计SBOM生产或消费的增长将加快约66%，会促使78%的组织生产或消费 SBOM。预计 2023年SBOM增长率将放缓至 13%，各企业SBOM生产或消费的使用率将达到88%。

值观：解决合规性要求与管理许可证合规性密切相关，改进基于风险的决策和安全风险的暴露与组件依赖关系的清晰度和组件漏洞的监管程度密切相关，如图 25。

12. 额外的行业共识将有助于改进SBOM的采用和实施。62%的企业正在寻求更好的行业共识，考虑如何将SBOM的生产/消费集成到他们的DevOps实践中，58%的企业希望与其它行业达成共识，将SBOM整合到其风险和合规流程中，53%的企业希望与其它行业一起，共同探讨SBOM的改进和提升，如图27。

跨行业 and 组织的SBOM准备、生产和消费正在实施中。出现了一些解决方案，但行业范围内的从业者共识尚未围绕特定的方法、格式和工具工作流程巩固。软件和服务供应商社区的高度可见支持将成为增长的关键加速器，并验证SBOM在保护软件供应链方面的作用。

导言

大部分的数字化转型都集中在一些积极的企业内部，以便更好地应对业务流程改进、自动化和资源核算，以提高生产力。数字经济所带来的机会包括追求新的商业模式和获得新的客户群和收入来源的能力。在许多情况下，行业领导者已经转变为“软件定义”的模式，采用云计算、边缘计算、人工智能软件和嵌入式系统为企业赋能。伴随着这种数字化转型的机会，如果软件资产来源不明和管理不当，网络安全风险也会越来越大。

网络安全：全球关注的问题

网络安全是一个全球性的问题。虽然SolarWinds的攻击对象是一家美国公司，但在当时，其客户遍布全球190个国家、数量超过30万，而且其38%的收入来自美国以外其它国家。这使得SolarWinds的攻击范围确实是全球性的，并表明针对国家和非政府行为者的网络犯罪活动越来越复杂。网络安全攻击有各种各样的目标。虽然大多数攻击可以被归类为金融犯罪，但更复杂的攻击可能具有政治、工业、经济或影响导向的目标。

尽管美国GDP占全球的24%，但各地区的GDP份额分布较为均匀¹。美洲的GDP份额为32%，而欧洲、中东和非洲（EMEA）为30%，亚太地区为38%。全球GDP在各地区的分布情况与各地区对软件安全的关注程度密切相关。图1显示了企业对其使用的软件安全的关注程度。美洲和EMEA的关注分布情况显示，美洲和EMEA地区最高时分别有49%和55%的人表示“非常关注”。这些分布大致呈正态分布，美洲和EMEA约有20%的人表示“担心”或“非常担心”。

欧盟（EU）在过去十年中一直在加强其网络安全的规范。欧盟早在2014年就通过了《通用数据保护条例》（GDPR），并在2016年成为一项可执行的法规。GDPR旨在为人们提供对其个人信息（PI）的高度控制，并制定规则如何处理PI的要求。在此基础上，2019年出台了《网络和信息系统安全指令》（NIS指令）和《欧盟网络安全法》。NIS指令要求数字服务提供商积极主动地管理风险，并提高国家应对网络安全事件的能力。《欧盟网络安全法》确定了认证数字产品、流程和服务的法规。

图1中亚太地区的分布与美洲和EMEA分布明显不同。亚太地区的安全问题逐渐增加，有15%的人“略为关注”，18%的人表示“关注”，31%的人“非常关注”，35%的人“极其关注”。亚太地区“极为关注”的企业数量是EMEA的两倍，比美洲地区多出67%。本报告解释了亚太地区软件安全焦虑水平较高的原因——这似乎是由于亚太地区迄今为止在安全相关的角色、功能和活动方面投资较少。²

中国同样一直在改善其在网络安全方面的姿态，从2017年的《网络安全法》开始，该法对IT服务提供商以及他们如何处理PI提出了规范要求。紧随其后的是2021年的《数据安全法》，该法对“国家核心数据”实施了以政府主导的更严格监管。截至2021年11月，中国颁布了新的《个人信息保护法》（PIPL），提高了政府对技术公司的监管力度，同时也逐步提高了PI要求。

再加上最近2021年5月的美国行政命令，软件安全和网络安全显然正在发生全球性的巨变。保护PI固然是一个方面，但保护软件产品、流程和服务形式的数字资产显然也是至关重要的。

美国的网络安全

网络安全问题已经变得非常尖锐，在美国，白宫于2021年5月发布了《关于改善国家网络安全的行政命令》（EO）。³该行政命令的理由是“日益复杂的恶意网络活动威胁着公共部门、私营企业，并最终威胁着美国人民的安全和隐私。”⁴该行政命令侧重于以下七个方面。

1. 消除共享安全漏洞信息的障碍
2. 促使联邦政府的网络安全现代化
3. 提高软件供应链的透明度和安全性
4. 建立一个网络安全审查委员会
5. 规范联邦政府对网络安全漏洞和事件的响应
6. 改进对联邦政府网络中的网络安全漏洞和事件的检测方法
7. 提高联邦政府的调查和补救能力

这个问题并不局限于美国，美国也不是唯一可以分配资源以改善网络安全的国家。提高软件供应链的透明度和安全性是至关重要的，因为美国联邦政府，以及全世界几乎所有的公共部门和私营企业，都依赖关键软件来支撑业务和关键活动。根据该行政命令的定义，关键软件是指执行对信任至关重要的功能软件，如提供赋予权限、或要求提高系统权限、或直接访问网络和计算资源的软件。解决软件供应链的安全问题涉及一系列的活动，如：

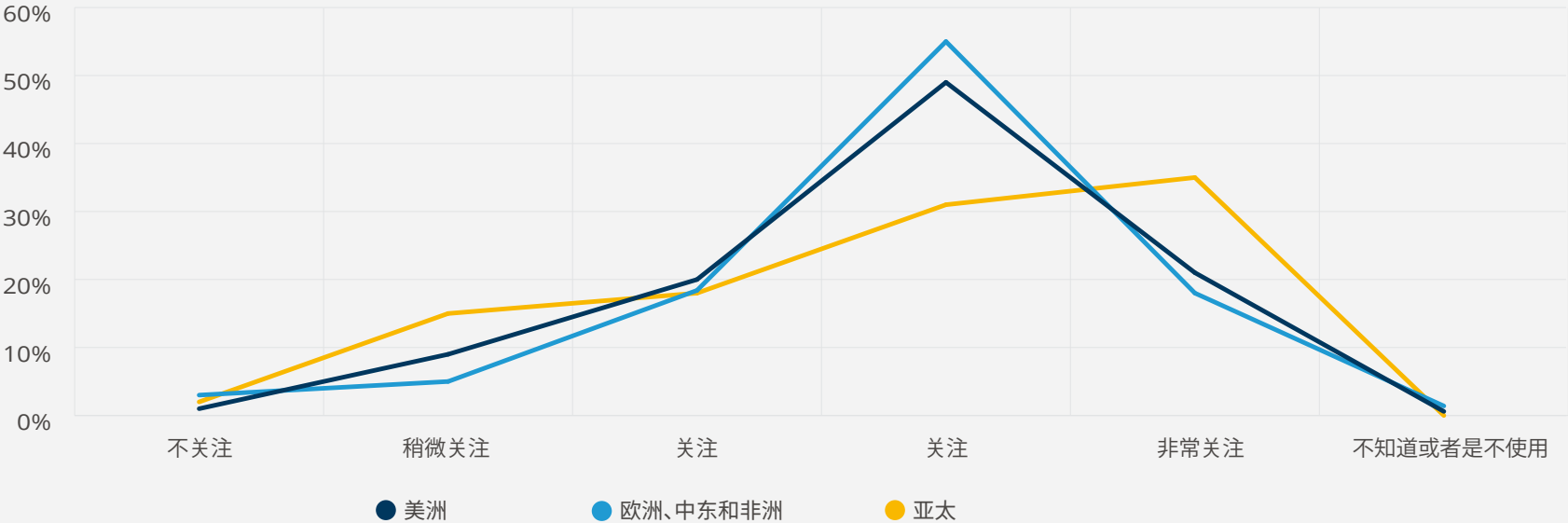
- 确保开发环境的安全
- 采用工具来检查软件组件中已知的和潜在的漏洞，并对其进行修复
- 维护准确和最新的数据，明确软件产品的代码的来源
- 为购买者提供每个软件产品的软件材料清单 (SBOM)

软件材料清单是解决其中一些需求的有效方式，特别是那些专注于了解软件产品的漏洞、许可证合规义务和代码来源的需求。因此，生产和消费 SBOM 被认为是解决所有类型的软件产品（包括开源和闭源组件）的各种信任问题的有效途径。美国国家电信和信息管理局 (NTIA) 指出，SBOMs 的好处如下：

- 降低成本
- 减少安全风险
- 减少许可证风险
- 降低合规性风险

图1
你的组织对所使用的软件的安全性有多关注？

单选 | 样本个数=341



SBOM的使用案例包括改进软件开发、供应链管理、漏洞管理、资产管理、采购和高保障流程。⁵

技术供应商、解决方案和服务提供商以及行业组织都在认真对待这个行政命令。SBOM在解决软件供应链安全的核心作用是本研究的一个关键催化剂。这项研究试图回答这样一个问题：“组织对SBOM的要求，和实施这些要求所需的网络安全实践准备得如何？”

SBOM成熟度

这份报告详细地讨论了SBOM的准备情况，以及SBOM的生产和消费水平。这些问题的设计是为了确定组织在其SBOM旅程中的位置，从不感兴趣，到有一定计划，再到实际采用的各个阶段。因为SBOM的准备程度是对SBOM采用情况的最好的整体识别。我们把对这个问题的回答归为三类：SBOM保守者、SBOM试用者和SBOM创新者。受访者自行选择，确定它们属于报告中的哪一类。关于这些类别如何映射到SBOM准备情况的详细信息，请参阅本报告的调查方法部分。

受访对象统计

本章节显示了部分所选的调查对象统计数据。其它的统计数据详见附录A。本章节讨论的统计数据有助于了解我们调查的对象、公司规模、收入、角色和行业。图2给出了这些信息的总结。

从图2可以看出，SBOM 的调查准备是针对全球范围的，包括各种规模和收入的企业，主要集中在高级信息技术（IT）岗位，并跨越许多垂直行业领域。在信息技术、汽车、医疗保障和生命科学、制造、金融服务和能源领域的企业中，具有很强的代表性。

按地理区域划分的SBOM成熟度

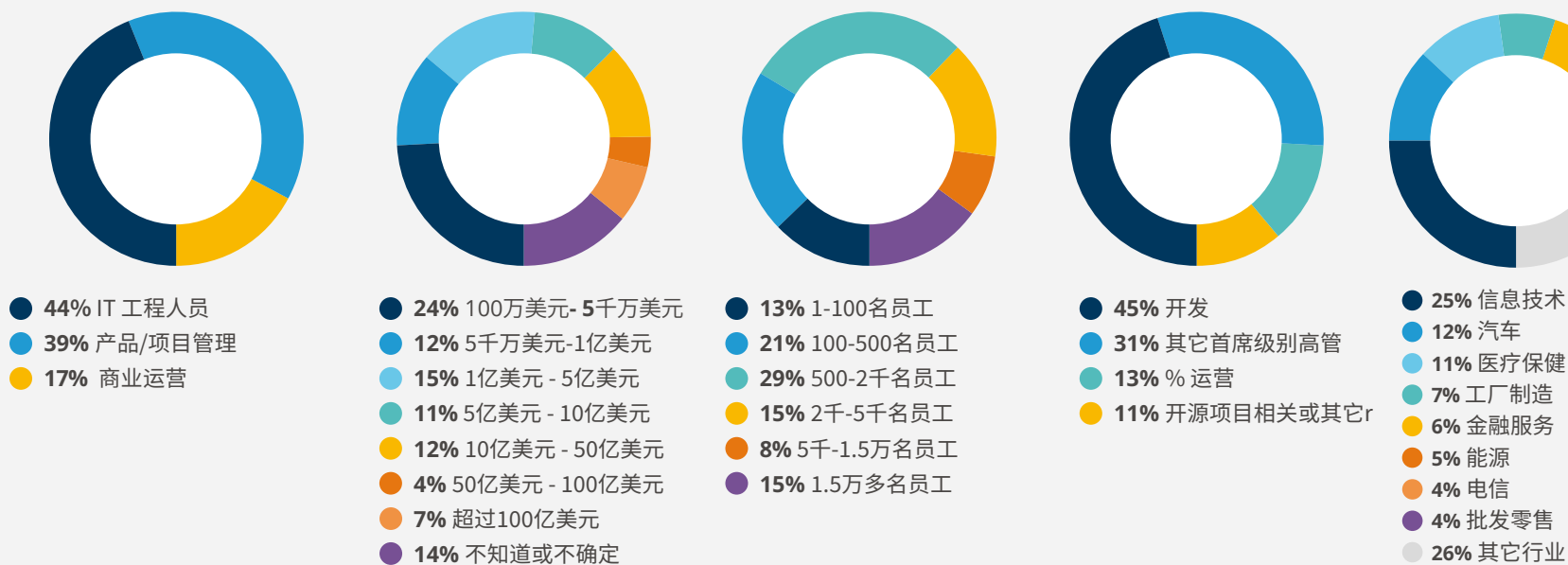
每个地理区域在SBOM成熟度方面，都有其独特性。图3显示了按照SBOM成熟度划分的三个主要地理区域。SBOM创新者在美洲和亚太地区的表现较为出色。在美洲，90%的回复来自北美，北美SBOM创新者的相对比率与美洲其他地区（如墨西哥、中美洲和南美洲）相同。

按照比例计算，亚太地区的SBOM创新者比例最大，印度和其他亚太国家，包括澳大利亚和新加坡的表现较为强劲。然而，亚太地区的特点是双驼峰分布，其中大多数受访者要么是SBOM创新者，要么是SBOM保守者。

图2

受访对象总览

样本个数=412



中国、俄罗斯和其他亚太国家尤其如此。EMEA 按比例拥有最少的SBOM 创新者, 但与美洲的 SBOM 试用者在数量上是一致的。

按企业收入划分的 SBOM 成熟度

调查样本包含大量的小型企业, 也包含数量众多的超大型企业。总体而言, 样本中51%的企业年收入低于5亿美元, 11%的企业年收入超过50亿美元 (14%的企业不确定他们的公司收入, 或者不愿意回答)。其中63%的被调查企业员工数量少于2000人, 而15%的企业员工人数超过15,000人。

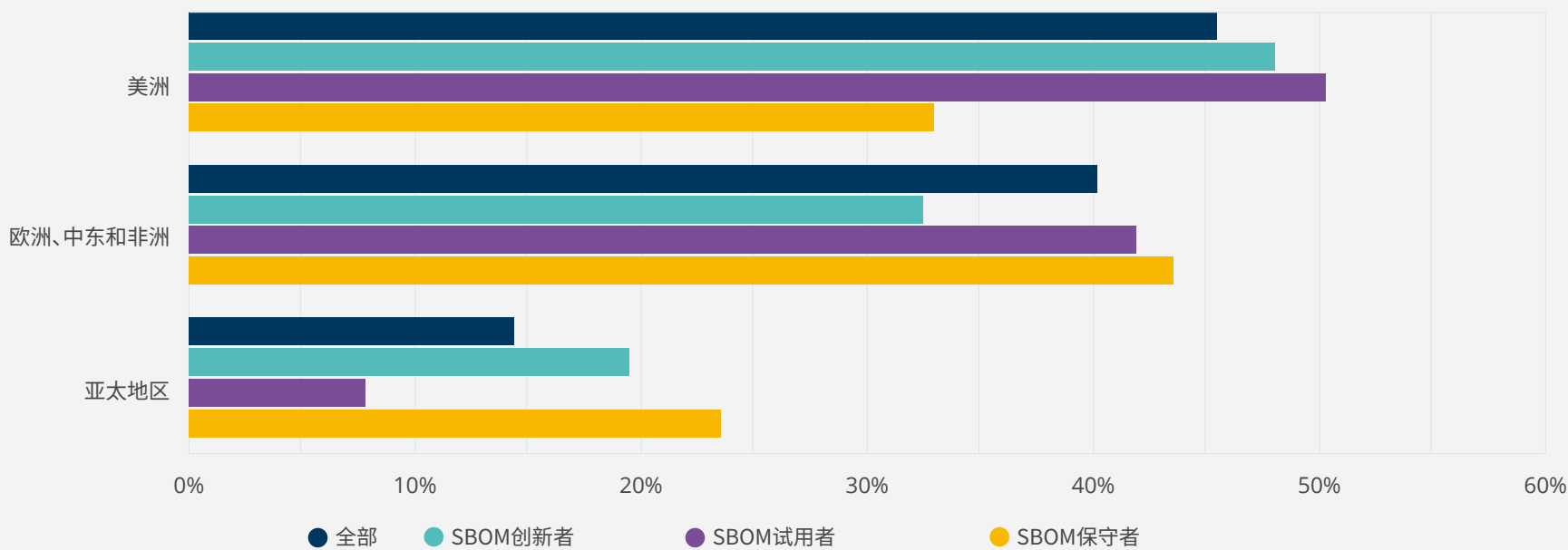
鉴于调查中的企业种类繁多, 我们想进一步了解企业的规模大小和年收入高低是否与 SBOM成熟度有关。我们的假设是, 随着企业规模和年收入的增加, 它们的成熟度也会增加。规模较大的企业, 可能会拥有更复杂的产品组合、更大的IT投资, 更需要改善软件供应链问题。图4显示了按照SBOM成熟度划分的企业平均年收入。

这些发现与我们的假设一致, 但并没有我们预期的那么显著。原因是年收入的分类有三个数量等级, 即使是年收入为数十亿的受访者中的一小部分, 也会使年收入为数百万的贡献者相形见绌。很显然, 企业的年收入随着SBOM的成熟度明显有所增长, 尤其是当年收入超过2.5亿美元时最为明显。

图3

你在哪里?

单选 | 根据 SBOM 成熟度区分 | 样本个数=3411



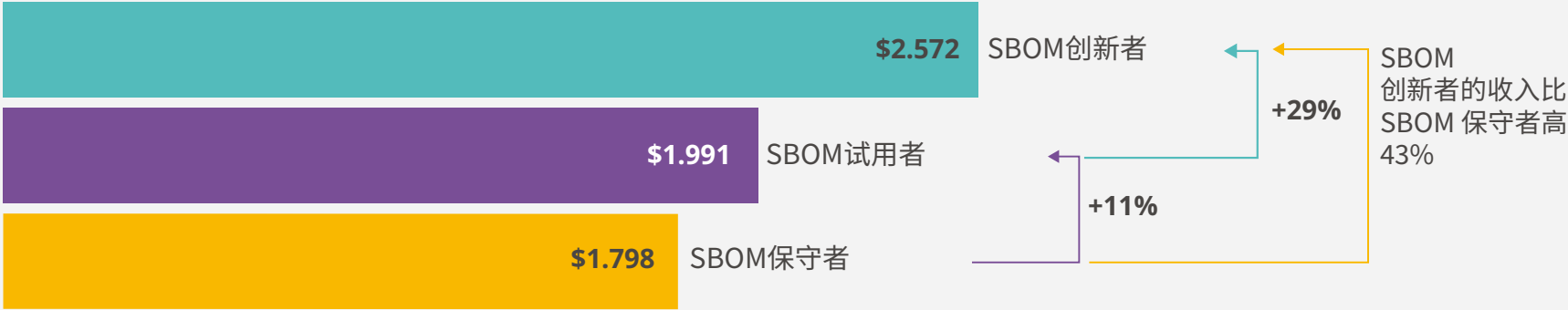
事实告诉我们，SBOM 议程主要由大型和超大型企业推动。这是有道理的，因为大型企业相比于中小企业有更多的收益和更大的损失，它们的规模和 IT 优先级更容易促进SBOM的生产和消费，但仍有问题亟待解决。

相比于中小企业，大型企业有更多的收益，也有更大的损失。中小企业的规模和 IT 优先级使得 SBOM 生产、消费很好，但仍有问题亟待解决。

图4

平均年收入(单位: 十亿美元)

根据SBOM成熟度区分 | 样本个数 = 341



软件安全的重要性

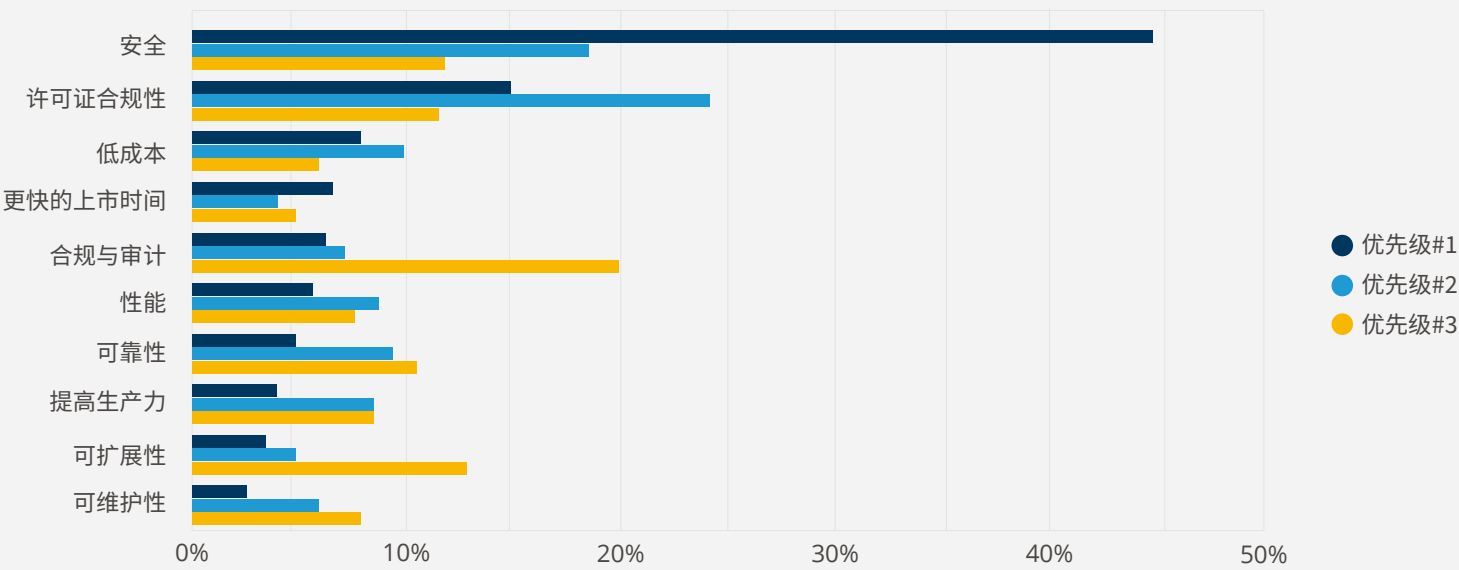
为了确定安全性相对于各种企业的优先级的排名，我们要求受访者对10个IT目标进行排序。图5显示了该问题的前三个排名结果，按排名第一的优先级的选项降序排列。对于企业来说，安全性是第一优先级，占45%，它的重要性也是第二梯队的首选项（即许可证合规性，仅占15%）的三倍。

安全的重要性是显而易见的，基于递增排名的累积增加，它仍然是顶级IT目标。在考虑第一和第二选项时，许可证合规性仍然是排名第二的IT目标，其强大的第二选项地位，使其能在安全性上站稳脚跟，并远远甩开排

名第三的选项（低成本目标）。监管合规性，在第一梯队的选择中排名第五，基于其强大的第三选项，使其整体上升到第三优先级。

相对于传统在类似比较中表现突出的各种IT目标而言，安全性和合规性（许可、监管和审计）受到重视，这意味着现在与GRC（治理、风险和合规性）相关的安全性和财务风险已经变得足够重要，足以使这些问题成为高度优先的问题。

图5
对以下最常影响你的组织选择使用软件的优先级顺序进行排序。



开源成熟度和 SBOM 准备程度之间的关系

由于开源已经成为应用程序开发运营中非常普遍的一部分，所以在使用开源软件时，研究它与SBOM成熟度之间的关系是很重要的。以下四个问题和图示探讨了企业如何基于其使用的开源软件实现SBOM成熟度的异同。

SBOM 创新者在使用开源软件时是否更容易出现风险？

首先，图6清楚地表明，开源软件的使用非常普遍。总体上，我们的样本中有98%都使用了开源软件。企业使用开源软件的不同之处在于，它们在选用开源软件时的标准。整体样本中，58%的人使用开源软件的方式与他们使用闭源软件的条件或标准相差无几——都是基于需求、功能和成本。

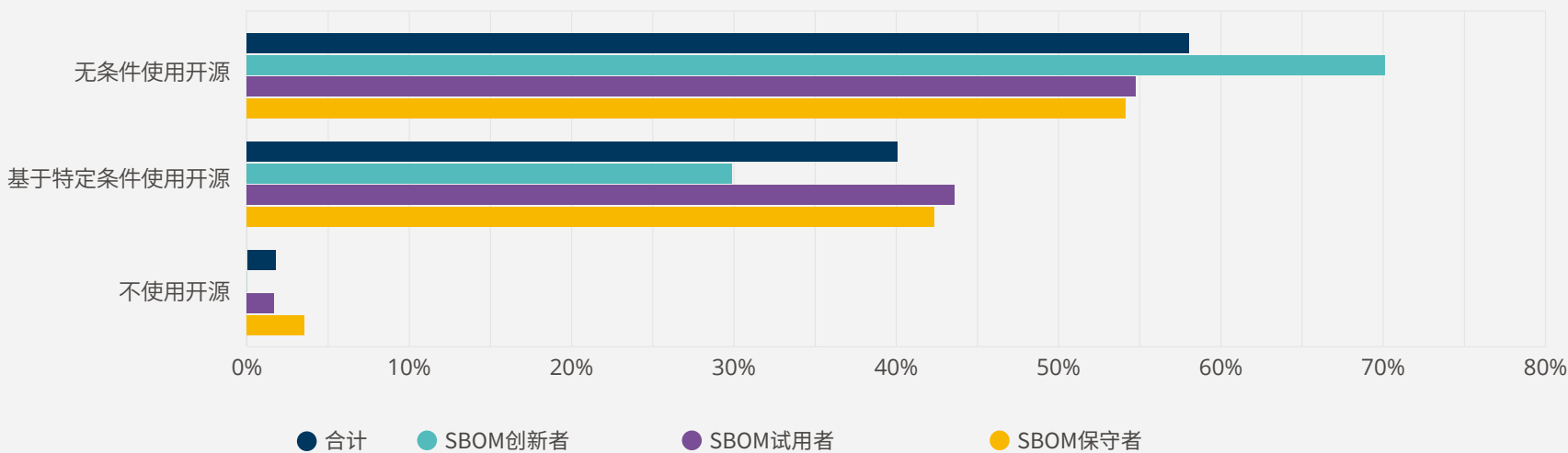
然而，有另外40%的企业使用开源软件是基于其他特定的条件。据推测，这些条件的存在是为了确保软件满足或超过旨在降低风险的内部需求。

除了SBOM创新者之外，SBOM成熟度的细分视图几乎与整个样本的特征完全一致——除了SBOM创新者更倾向于无条件地使用开源软件。因为在很大程度上，SBOM的创新者使用SBOM是作为他们标准实践的一部分，因此我们可以假定SBOM的自动化使用可以解决有关软件许可和安全的许多关键问题。SBOM创新者不是风险倾向者；他们只是在使用开源软件方面拥有更中庸温和的文化素养。

图表6

你的组织在使用开源软件时关注的维度/条件？

单选 | SBOM成熟度分类 | 样本个数=341



有条件使用开源

对于那些表示会在特定条件下使用开源软件的受访者，我们设定了一系列的多选问题以了解在什么条件下他们的组织会使用开源软件。

图7显示了总体结果，包括“当可以确保代码性能条件下” (54%)、“当可以确保代码安全性的条件下” (51%)、“当可以确保适当的代码支持下” (51%)、“当可以确定代码来源可信的情况下” (48%)和“代码许可证可靠的情况下” (41%)。

验证开源代码的性能、技术支持和可靠性的确很重要，但这需要使用企业投入验证成本，仔细测试组件。

从 SBOM 成熟度细分数据看，差异不大；总体上，SBOM创新者表现出了对代码性能验证 (70%)、代码安全性验证 (65%) 和代码许可验证 (65%) 的强烈关注。这三个问题显然是SBOM创新者的优先事项。

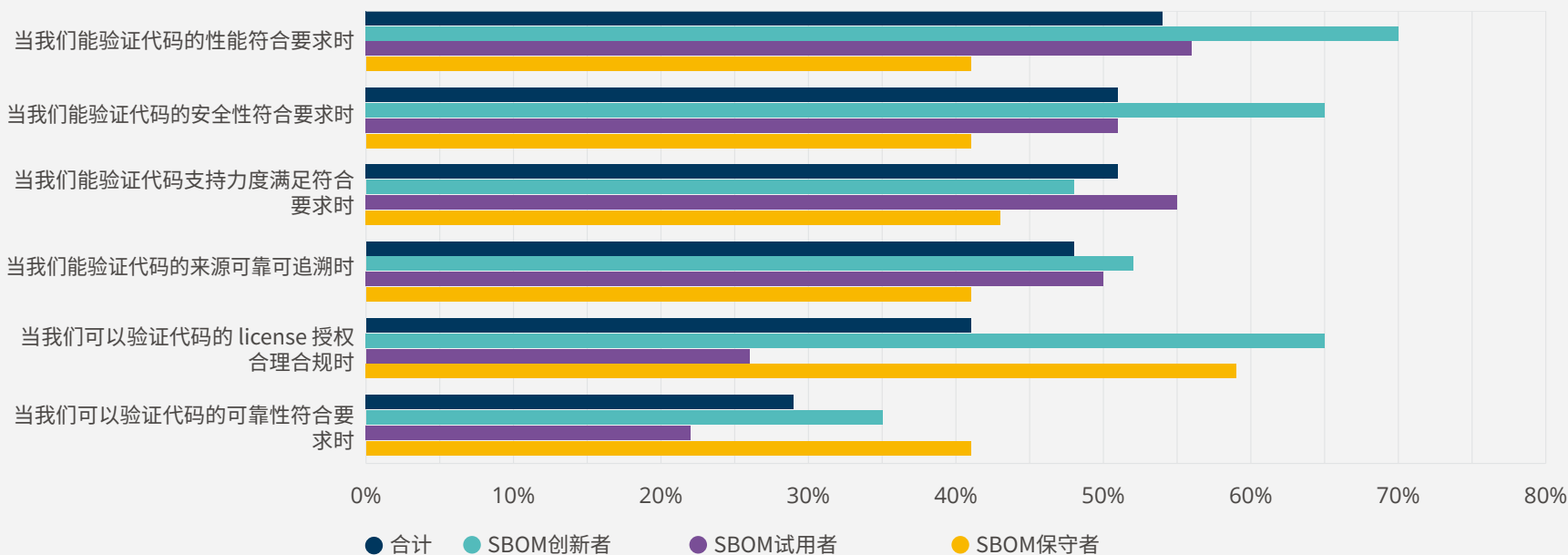
SBOM 的试用者在性能、安全性、支持和来源相关的问题保持一致的较高关注度。唯一的差异在于代码许可，它只吸引了26%的SBOM试用者的关注，与整体样本中41%有较大差距。

SBOM 保守者的特点是他们对所有维度都很关心。尽管有59%的人对开源软件的许可证很关注，但SBOM保守者似乎开源有更大程度的使用焦虑，这与他们在开发开源策略的投入较少有关。

图表7

你的组织在什么情况下会考虑使用开源软件？

多选 | 按SBOM成熟度分类 | 样本个数=138, 有效样本个数=138, 总样本个数=381



开源软件的使用随SBOM的成熟度的变化

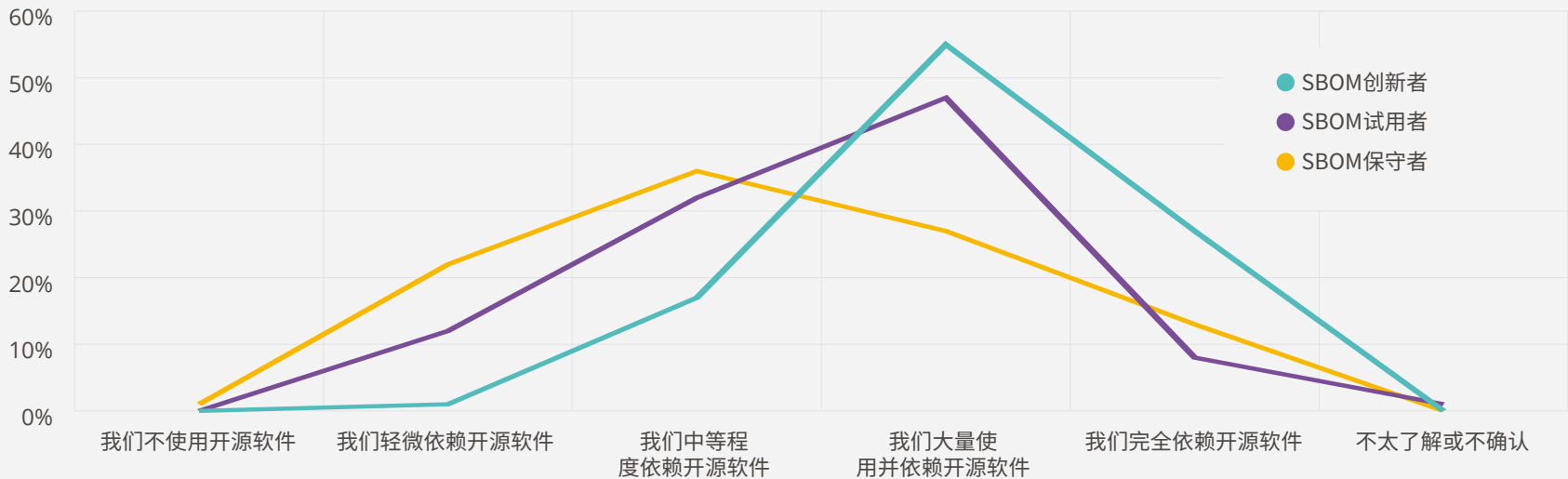
图8显示了开源软件使用很广泛。但是企业对开源软件的依赖程度到底有多高？这种依赖如何根据SBOM的成熟度而变化？图8揭示了企业对按照SBOM成熟度划分的开源软件的依赖程度。图8中的分布只是反映了一种连续的方式，以按SBOM成熟度级别显示依赖程度的分布，并基于这些分布形状提供了一些额外的可视化洞察。

BOM保守者的分布峰值是36%，他们对开源软件有中等程度的依赖。SBOM试用者（47%）和创新者（55%）的分布峰值显示了对开源软件的巨大依赖。SBOM创新者是唯一声称自己完全依赖于开源软件的细分群体，占27%。

图表8

你的组织对开源软件的依赖度如何？

单选 | 按 SBOM 成熟度分类 | 样本个数=341



软件安全的核心关注

对于正在使用的软件的安全性的担忧，在我们的样本中几乎是一致的。图9显示91%的样本要么是非常关注，要么是极端关注他们组织使用的软件的安全性。加上稍有关关注的8%，对于软件安全性关注的这一比例高达99%。

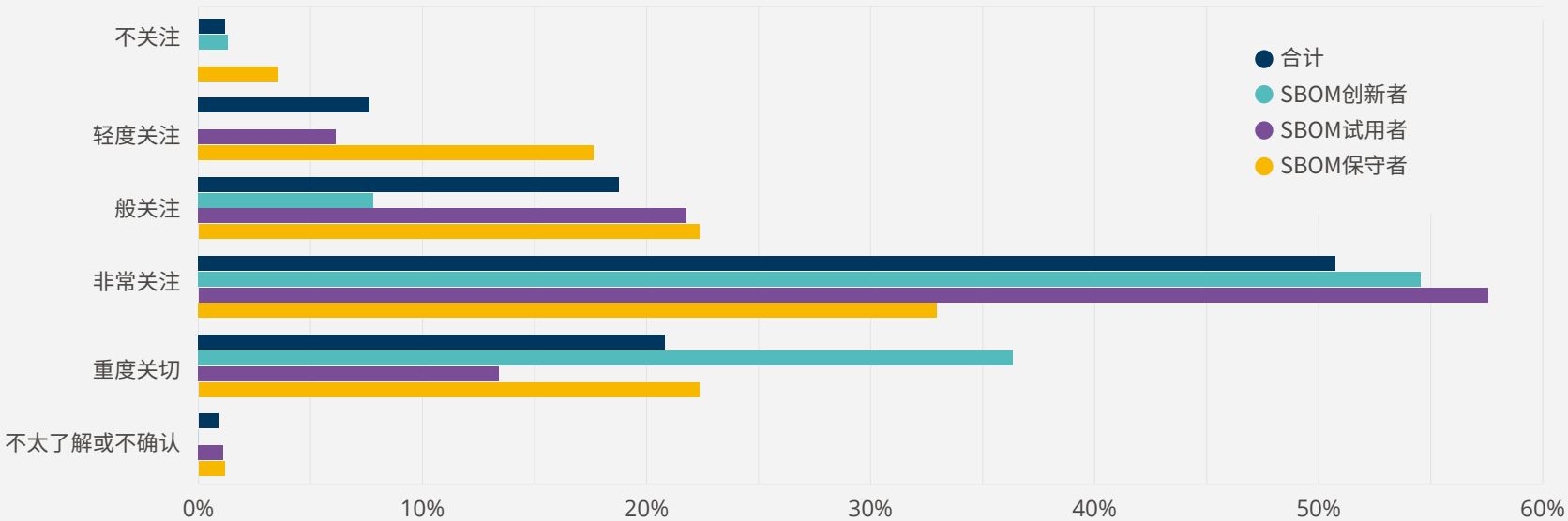
图9还按SBOM的成熟度进行了细分，虽然在比较分布时存在一些差异，但令人惊讶的是 18%的SBOM保守者略微担心软件安全性，4%不担心。而在这18%的SBOM保守者中，他们所在的企业，一般员工规模在1到99人之间，收入低于100万美元。这些企业更关注生存和增长，还没有处于优先考虑软件安全的位置。

SBOM的成熟度与软件安全性密切相关。在成熟度细分领域的比较中，99%的SBOM创新者要么非常关心，要么极度关注软件安全，这与93%的SBOM试用者和77%的 SBOM 保守者对安全的关注度形成了鲜明对比。整体共识是，软件安全仍然是一个重大问题。

图表9

你的组织对软件安全的关注程度如何？

单选| 按 SBOM 成熟度分类| 样本个数=341



企业为何关注软件安全

后续问题自然是为什么组织关心软件安全? 图10显示, 整体上66%的样本关注财务风险, 61%关注声誉风险, 53%关注法律风险, 40%关注未经授权访问客户系统, 31%关注未经授权访问自己组织的系统。

SBOM 成熟度的细分作可以补充解释这些额外的发现。虽然大多数问卷的回答表现得非常接近整体样本, 但有两个显著的例外。一个是 SBOM 创新者担忧安全导致财务风险 (71%) 和声誉风险 (76%) 的比率要高于整体样本, 而因安全导致其他方面的担忧较少。我们相信SBOM的革新

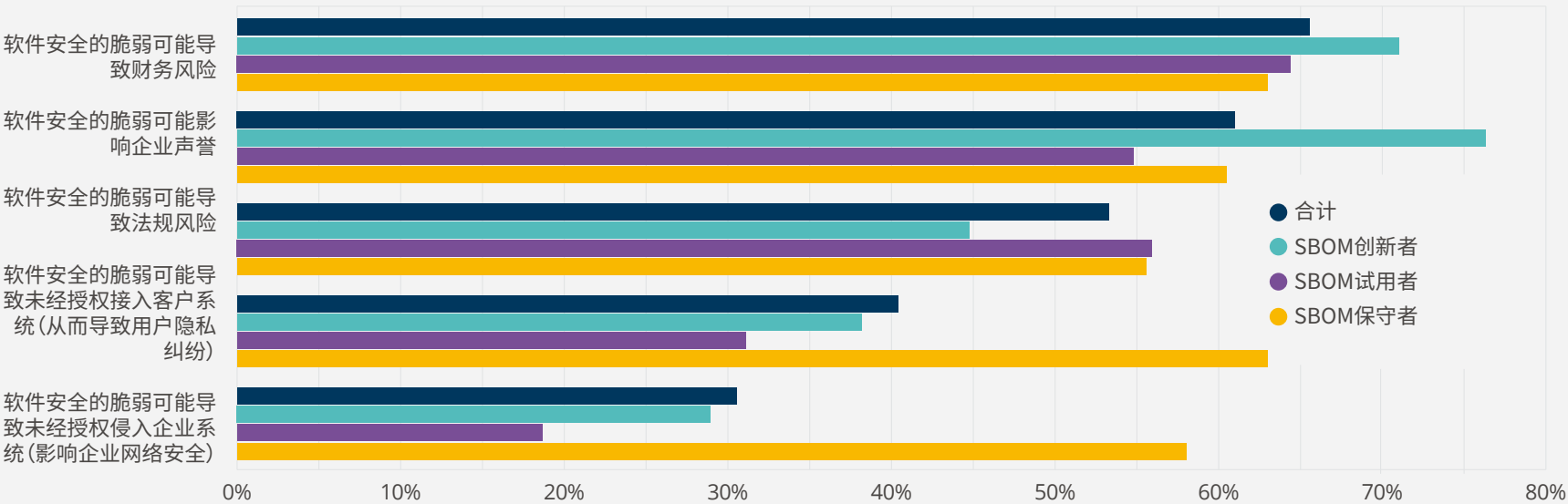
者, 由于他们在软件安全方面的长期投入, 在很大程度上, 已经解决了首要问题, 如未经授权的访问和法律风险。但财务风险和声誉风险是二阶安全问题, 需要更复杂的解决方案。

另一个例外是 SBOM 保守者非常担心未经授权的访问, 要么是客户的系统(63%), 要么是他们的系统(58%)。对于 SBOM 创新者和试用者来说, 这些首要的安全问题几乎不会产生太多的焦虑, 大概是因为这些问题在很大程度上已经被解决了。

图表10

你的组织为何关注软件安全?

多选 | 按 SBOM 成熟度分类 | 样本个数=334, 有效样本个数=334, 总样本个数=840



网络安全和SBOM 的推进

2021年5月12日, 美国总统拜登签署了一项行政令, 致力于改善国家网络安全, 行政令中针对制定网络安全要求的规则和指导一事, 明确了紧凑的时间框架。行政令其中一项是要求国家电信与信息管理局 (National Telecommunications and Information Administration , NTIA) 发布有关 SBOMs 的最低要求。2021年7月, 商务部与NTIA共同发布了SBOM的最低要求。⁶ 之后, 这份报告的第二版, 名为《系统与组织中的网络安全风险管理实践》, 于2021年10月由国家标准技术研究所 (NIST) 发布。⁷ 这些文件能够让我们对美国政府改善软件供应链安全的目标有所了解。

在NTIA发布的文件中, 将SBOM定义为“一个用于构建软件各模块详情与相互之间关系的正式记录”。该文件也进一步描述了一个针对SBOM的有价值的倡议, 表述如下: “SBOM为那些生产、购买和操作软件的人提供信息, 提高他们对供应链的理解, 这将带来许多好处, 尤其是提供了追踪已知和新暴露的漏洞及风险的潜在能力。SBOM并不会解决所有的软件安全问题, 但是它构成了一个基础的数据层, 在这之上可以进一步构建安全工具、实践和保证。” 正在或将要参与SBOM的供应商和最终用户企业都被要求阅读NTIA的文件以及NIST的附录F。

这份网络安全行政命令将会成为SBOM市场行动的催化剂。虽然采用术语市场还为时过早, 但是对SBOM的熟悉和准备程度以及格式化SBOM的ISO标准, 都迫切需求SBOM工具。

这份网络安全行政命令将会成为SBOM市场行动的催化剂。虽然采用术语市场还为时过早, 但是对SBOMs的熟悉和准备程度以及格式化SBOMs的ISO标准, 都迫切需求 SBOM 工具。

美国网络安全行政令-认识与行动

美国行政令的目的是提高网络安全意识, 并加速产品、流程、最佳实践的发展和使用, 以改善网络安全。为了理解行政令带来的影响, 我们询问了一些有关组织认知的问题, 并就行政令带来的变化提出了一些后续问题。图11显示总体上84%的样本对该行政令有所认知, 11%并没有, 8%尚不确定。对行政令的认知也因地域差异而不同 (图中并未显示)。美国有84%的人注意到了行政令, 欧洲中东及非洲地区比例达到79%, 而亚太地区为64%。

图11中也依据SBOM成熟度展示了对行政令的认识。毫不意外，SBOM创新者们的认识度最高，达97%，随后是SBOM的试用者，达91%，而对SBOM持保守态度的人只有56%。

认识是做出改变的先决条件。图12显示，总体而言，77%的企业正在考虑做出改变以响应行政命令，13%不考虑，6%不愿回答，4%不确定。图12中按SBOM成熟度进行的细分，并未发现因响应行政命令而发生变化的群体之间存在的任何显著差异。然而，图11所示的高程度认知，结合图12中77%的人正在考虑改变的情况，表明该行政命令正在实现其预期结果，即推动公共部门和私营企业网络安全的改善。

网络安全和软件供应链的优先事项强调SBOM

当被要求确定确保软件供应链安全的关键活动时，SBOM可以满足各种各样的需求。图13显示，总体而言，47%的样本认为漏洞报告系统是确保供应链安全的主要工作。目前，SCA工具是识别开源软件中的漏洞和许可证合规性的首选工具。SBOM具有识别依赖关系的能力，它们最终可能包含有关已知漏洞的信息。然而，漏洞的挑战在于了解哪些漏洞是可利用的，以及如何使这些信息保持最新。虽然SBOM尚不支持识别漏洞，但这种能力逻辑上合理，应该被列入候选名单。

图11
你所在的组织是否注意到最近的美国关于网络安全的提及软件物料清单的行政命令？
单选 | 根据SBOM成熟度划分 | 样本个数=341

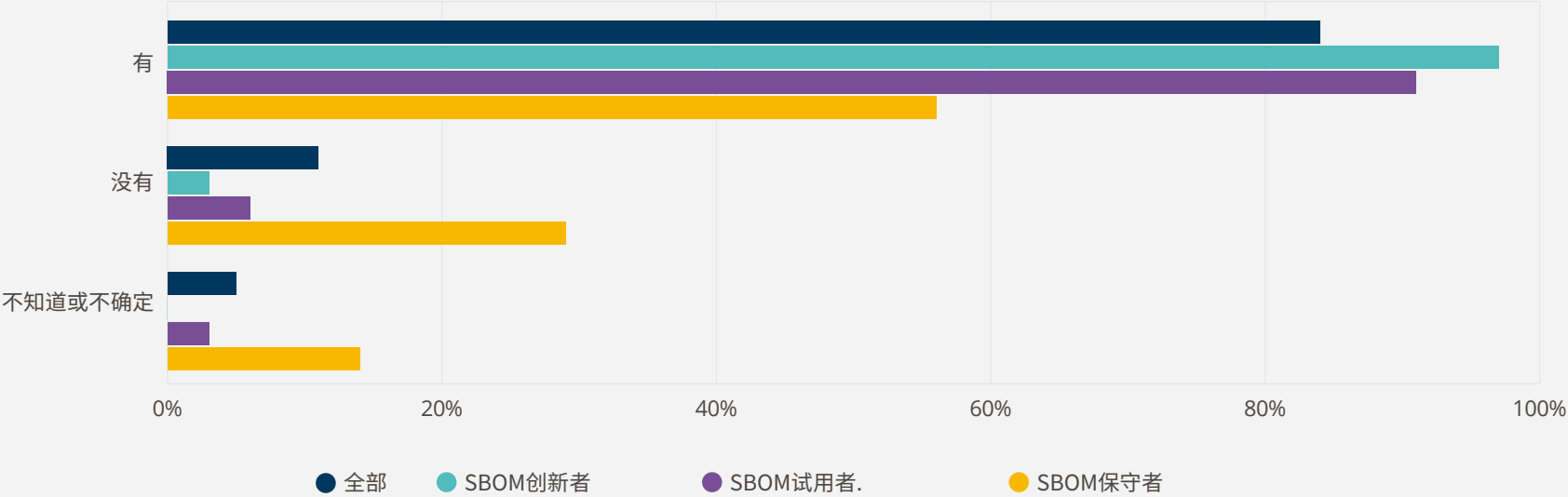


图12

你所在的组织是否正在考虑做出改变以响应美国关于网络安全的行政令？

单选 | 根据SBOM成熟度划分 | 样本个数=285

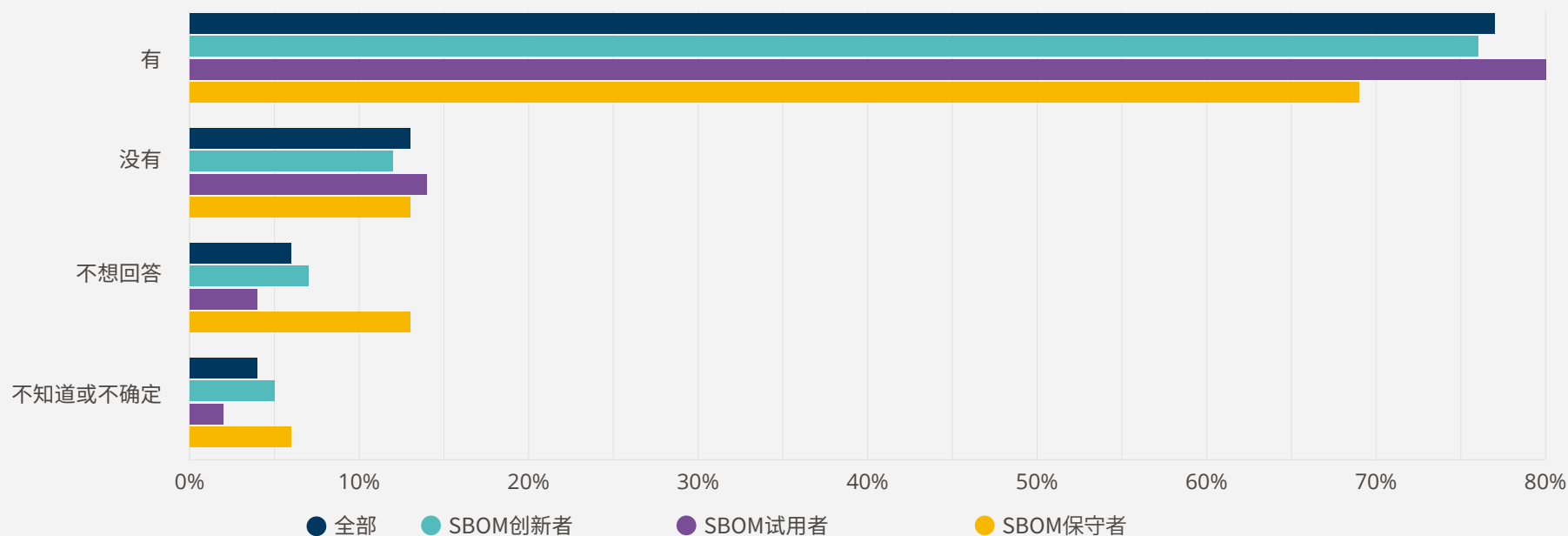


图 13 中的总体发现是，SBOM被视为实现软件供应链安全的重要方式。SBOM创新者令人信服地传达了SBOM的重要性，他们使用 SBOM 的经验确认了SBOM可以提供值得信赖的价值信息。

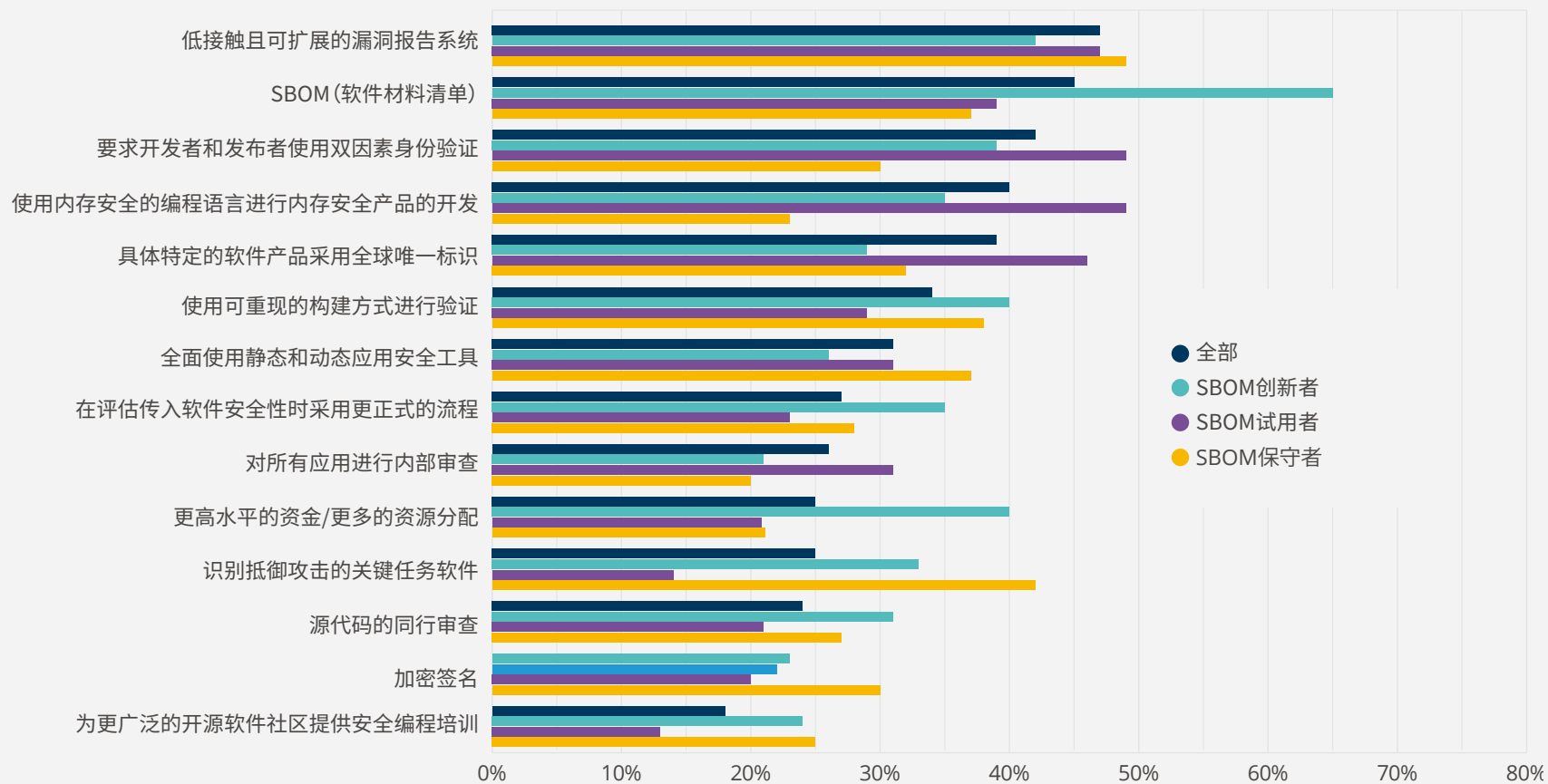
SBOM 的使用是确保软件供应链安全的第二项重要的工作。总体而言，45% 的受访者确定了SBOM的作用，其中包括 65% 的SBOM创新者、39%的SBOM试用者和37%的SBOM保守者。这是对SBOM的强烈认可，也来源于SBOM可以定义组件的出处、许可和依赖关系以及提供加密信息的能力。双因素身份认证（2FA）在图 13 中排名第三，样本中认同率达到42%。2FA 是一种完善的提高安全性的技术，但持续出现的高度可见的安全缺陷意味着 2FA 并不总是被遵循。因为 2FA 是一种最佳实践，并且可以轻松实施，听到这些持续不合规的消息是令人失望的。

样本中 40% 也认为，使用内存安全的编程语言也是保护软件供应链的一种非常重要的方法。大多数较新的语言，例如 Rust、Go、Java、C、Swift、JavaScript 和 Python，都是内存安全的。很明显，C 和 C++并不在此列表中。包括微软和谷歌在内的供应商报告说，他们发现的大多数漏洞都是内存安全问题。这些漏洞是攻击者利用应用程序或操作系统的简便途径。还应该提到的是，全球唯一标识符（39%）、通过使用可重复构建（34%）和加密签名（23%）进行的验证是当今使用SBOM时都可以实现的功能。这么多广泛的功能使得SBOM如此引人注目。

图13

你认为确保软件供应链安全的关键工作是什么？

多选 | 根据SBOM成熟度划分 | 样本个数=316, 有效样本量=316, 总提及个数=1416



对SBOM的要求

以下六张图 (14到19) 是根据NITA的框架设计的。这些图突出了NTIA⁸多 利益相关方在SBOM 流程中出现的六个关键维度和决策点。

每个图的图例包括三个维度：

- 备选：为适应行业采用基于时间和版本信息的流程/技术
- 初始共识：关于当今现代开发流程的可能性
- 增强：为了新兴和高保证的用例

NTIA 对基准组件信息的定义如下：

“SBOM的主要目的是唯一且明确地识别组件及其彼此之间的关系。为了做到这一点，需要一些基础组件信息的组合。一些确定的属性可以提供更大的唯一性或明确性，同样，在SBOM 条目中具有更多的基准属性。”⁹”

机构希望SBOM具有丰富的元数据

图14和其后的5个图中的每一个都描述了SBOM的一个重要维度，并提供了用户关于所需功能等级的反馈：备选方案、初始共识或功能增强。图14显示了按SBOM成熟度划分的基准组件信息的首选等级。图14中的

SBOM保守者是最不固执己见的一个群体，因为它们在备选、共识和增强计划中的分布相对均匀。SBOM的试用者合并了围绕起始共识的意见，该部分达到了52% 的比例，另外 40% 的人对增强计划感兴趣。SBOM创新者以62%的比例倾向于功能增强，这使该部门对其他计划的剩余反应相形见绌。我们预计，对增强基准信息的这种强烈兴趣是由于加密哈希信息（可选）和漏洞信息（开发中）可以提供的巨大价值。

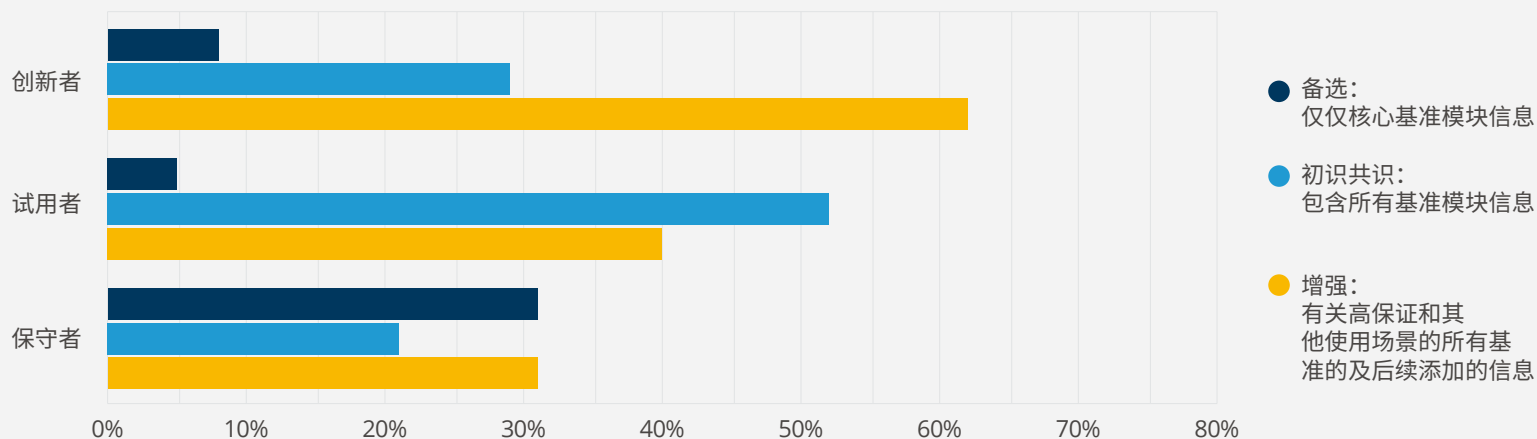
机器可读性是SBOM的关键指标

图15定义了需要什么级别的SBOM格式，和满足哪种程度的机器可读性。可以看到，SBOM保守者再次分布得很均匀，尽管共识的格式仅占33%，但依然鹤立鸡群，这与SBOM试用者（60%）以及SBOM创新者（60%）对共识方式的选择是一致的。初始共识要求基线信息在每种主要的 SBOM 格式中都是机器可读的，这显然是最务实的计划。备选计划意味着 CSV 过于简单化，而增强计划产生了可能不需要或不容易支持的高度复杂性，与此同时SBOM 领域的标准正在迅速而显著地变化。

图14

你当前需要什么级别的SBOM基准模块信息？

样本个数=356



SBOM应当识别已知和未知的依赖传递

图 16 表现了用户需要的组件依赖的深度。基于 65% 的SBOM保守者、40% 的SBOM试用者和 49% 的SBOM创新者的强烈偏好, 初始共识计划似乎是领先的候选者。初始共识计划的吸引力在于它支持传递依赖, 它将一层智能嵌入到如何识别依赖中。SBOM创新者略微偏爱增强计划, 但挑战在于如何确认不存在未知项。

SBOM应该随着每次代码变更而更新

图17显示了所需的SBOM更新频率级别。SBOM保守者 (40%) 和试用者 (53%) 都强烈支持初始共识计划。SBOM创新者在计划的选择上存在分歧, 43% 的人更喜欢初始共识计划, 53% 的人更喜欢增强计划。初始共识计划比后备计划更有用, 因为它会在每次更新或更改组件时生成一个 SBOM。但是, 增强计划通过额外提供对每个版本的存档支持, 改进了访问, 并提供了历史溯源数据, 这些数据在研究异常时可能非常宝贵。

图15

你当前需要什么等级的SBOM格式和机器可读性?

样本数量=355

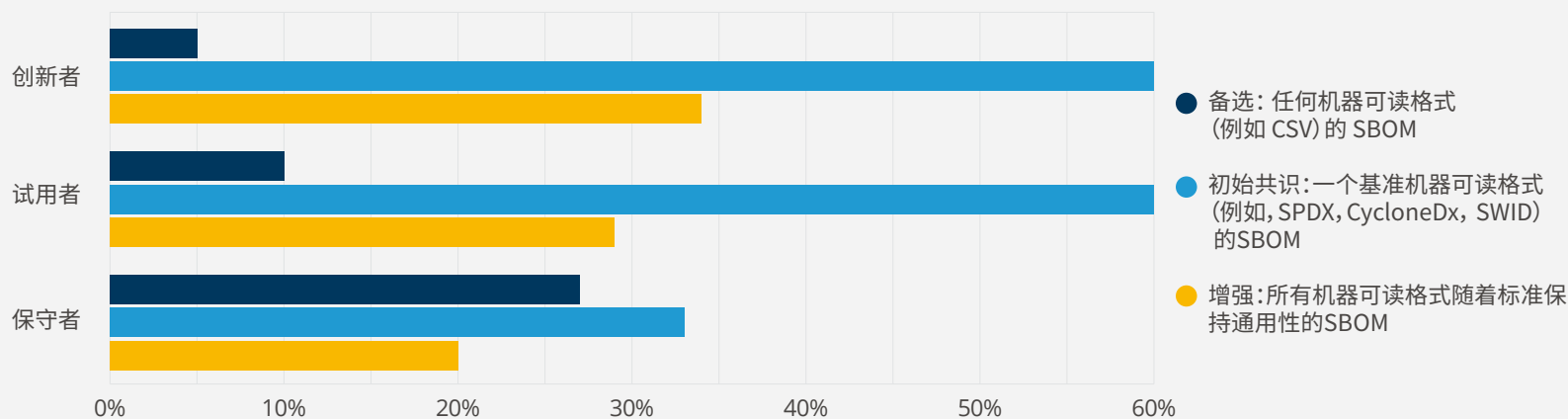


图16

你当前需要什么等级的SBOM依赖的深度?

样本个数=355

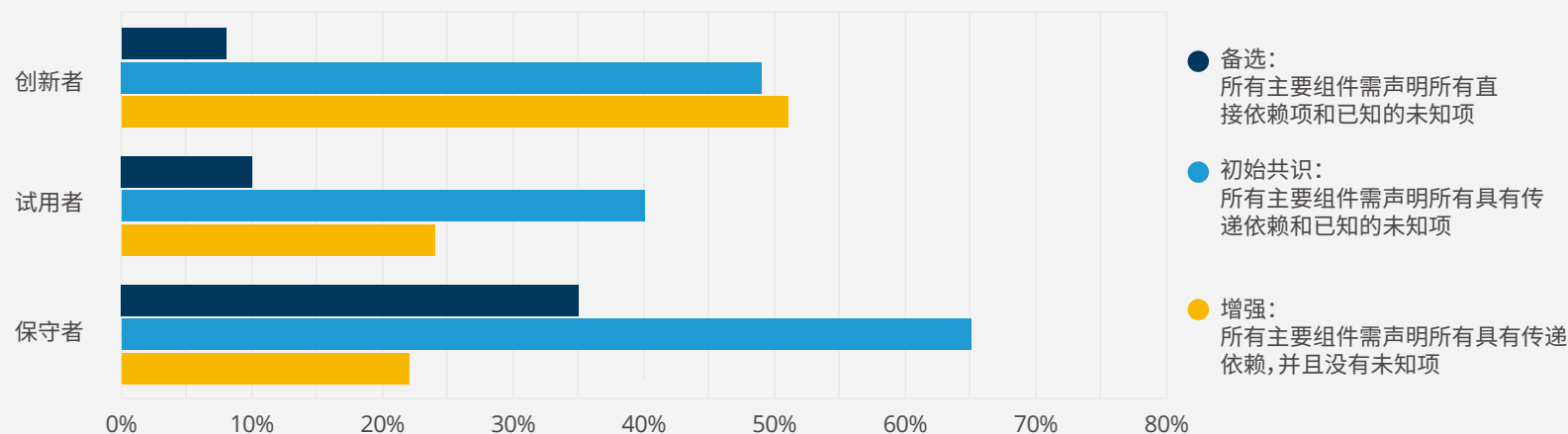
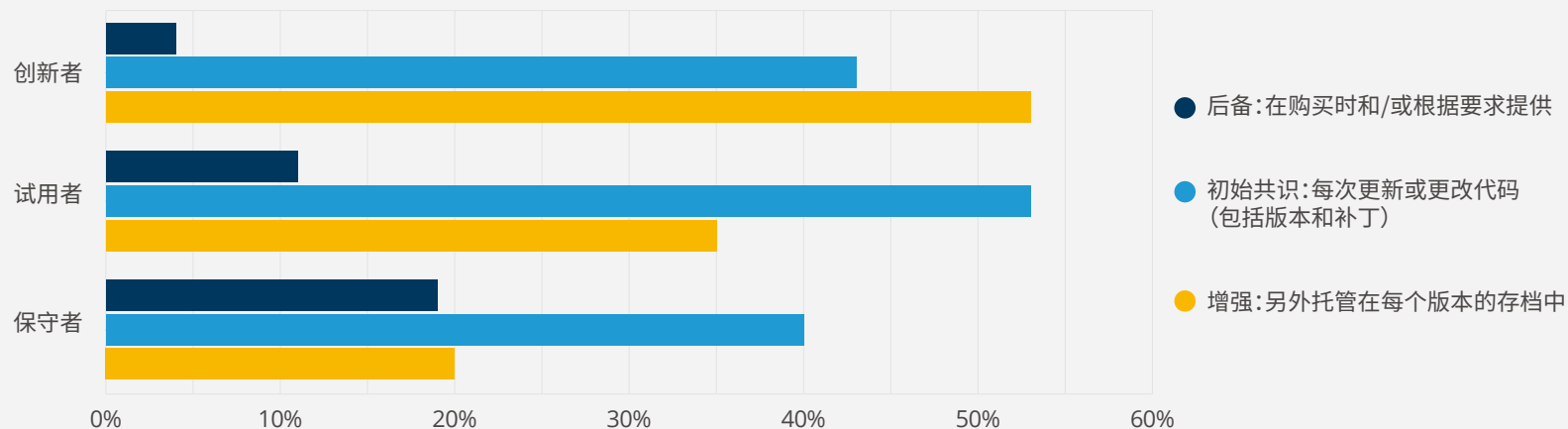


图17

你当前需要什么等级的SBOM更新频率?

样本个数=353



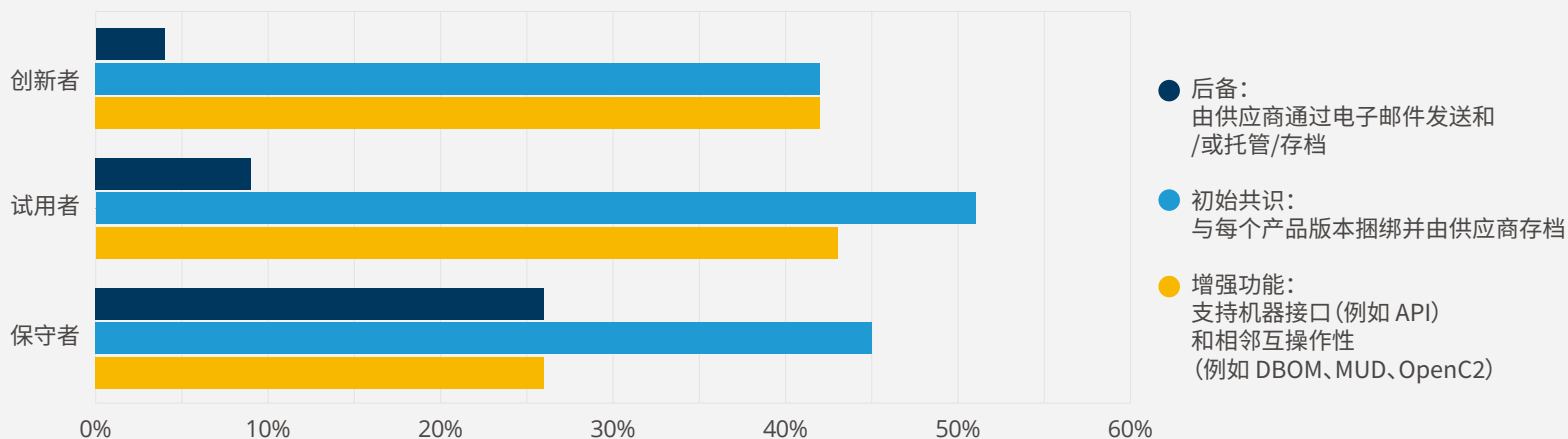
SBOM元信息应该与模块绑定

图18呈现了用户对SBOM可交付性和互操作性所需要的等级。初步共识方案受到广大用户的集体青睐，其中包括45%的SBOM保守者、51%的试用者和42%的SBOM创新者。然而，增强计划得到了43%的SBOM试用者和42%的SBOM创新者的大力支持。共识和增强计划之间的区别在于为自动化、可扩展性和互操作性提供的支持。增强计划有关API访问的条款，可以在M2M通信中加强互操作性，这极大地加速和简化了SBOM的消费和利用。但是由于共识计划确实支持一定程度的自动化，因此可以将其视为通往增强计划的有用临时垫脚石。

图18

你当前需要什么等级的SBOM可交付性和互操作性？

样本个数=353



SBOM应在发现漏洞时及时反馈

图 19 显示了利用漏洞信息所需的访问和集成级别。初始共识计划和增强计划对SBOM用户同样具有吸引力。这是令人鼓舞的，因为这两个计划的供应商都将漏洞数据实时推送给消费者。后备计划没有这样的规定，它一方面使消费者面临风险，另一方面还缺少高效的理解漏洞的过程。

SBOM的准备情况和按SBOM成熟度划分

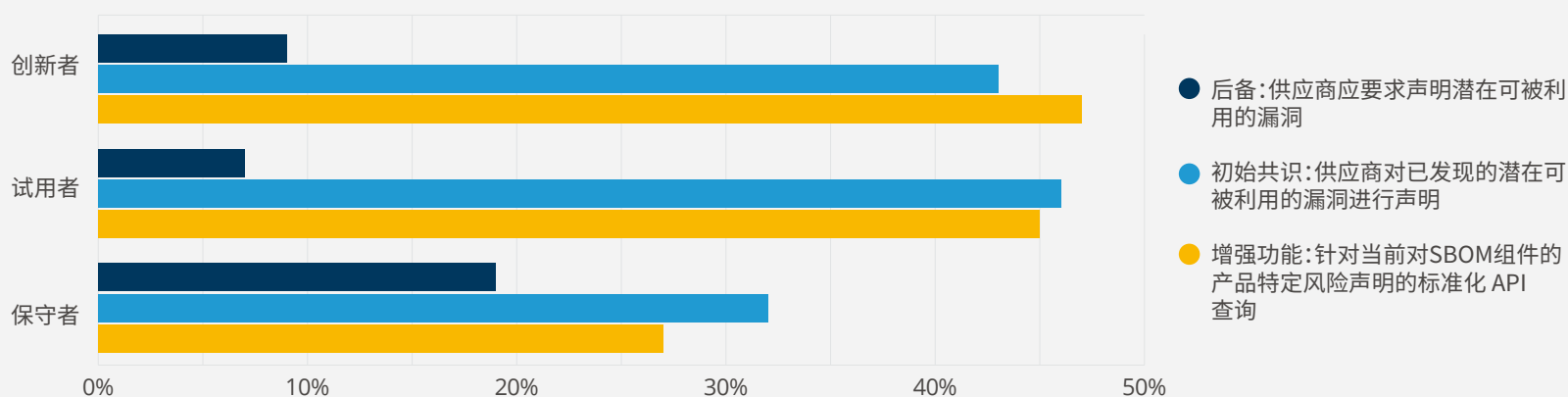
调查数据的一个重要划分依据是SBOM的准备程度。调研的问题是，“你们团队目前的SBOM 准备情况如何？”这个问题是在提供了SBOM的定义后提出的，并且是调查中的第一个问题，直接询问受访者，在他们工作的团队或业务部门中发生了哪些SBOM行动。与后面针对SBOM生产和消费状况的问题不同，这个问题的范围更广，作为分割样本的基础是有价值的。

该问题有8个回答，不包括不知道和不确定（DKNS）。图 20 显示，在我们样本中的各个组织中，90% 的组织已经开始了他们的SBOM之旅。10% 的组织尚未开始任何SBOM规划，14% 处于规划或开发阶段，52% 正在其少数、部分或许多业务领域采用SBOM，23% 正在所有业务中应用SBOM，并在有相应的实践标准。总体而言，76% 的组织对SBOM的应用做好了充足准备。图 20 展示了SBOM创新者、SBOM试用者和SBOM保守者在以上问题的不同反馈情况。

图19

你当前需要什么等级的SBOM交付能力和互操作性？

样本个数=353



SBOM保守者类别包括尚未开始处理 SBOM、正在计划如何处理SBOM或开始处理SBOM的受访者。SBOM保守者占受访者总数的 24%，58% 的SBOM保守者正在计划或开始解决SBOM支持问题。41%的SBOM保守者（占总样本的 10%）尚未开始采用SBOM。

SBOM试用者类别包括在其部分业务中生产或消费SBOM的组织和受访者。总样本的 53% 属于这一类。在SBOM的试用者中，29% 的人在其业务的几个部门中采用 SBOM，42% 的人在某些部门中采用，28% 的人在许多部门中采用 SBOM。

SBOM创新者是专为在SBOM使用方面高度投入和经验丰富的组织保留的类别。SBOM创新者占总样本的 23%，在SBOM创新者中，62% 的人在其几乎所有业务领域都在使用 SBOM，38%的人制定了使用SBOM的标准做法。

基于SBOM准备情况构建此视图的效用在于，当与调查中的其他变量交叉时，我们可以深入了解一些优先事项和行动，涉及这三个相关角色：SBOM保守者、SBOM试用者和SBOM创新者。通过研究这些优先事项和行动如何根据SBOM成熟度水平发生变化，我们还可以深入了解组织如何使用SBOM。

SBOM生产观点

在调查的开始，我们询问了他们对SBOM的熟悉程度和SBOM的准备情况。这样做主要是为了让受访者思考他们的组织对SBOM的使用。在SBOM调查的后半部分，我们询问了关于组织参与SBOM生产和消费的各种问题。这些问题要求对当前或计划中的SBOM参与情况进行更清晰的投入。

SBOM的产生对于有组织性地生产商业软件是最合适的，因为监管机构和客户要求提供这些信息。但是，拟用于内部使用的软件也将受益于SBOM，可以提高其安全性和可维护性。

SBOM生产

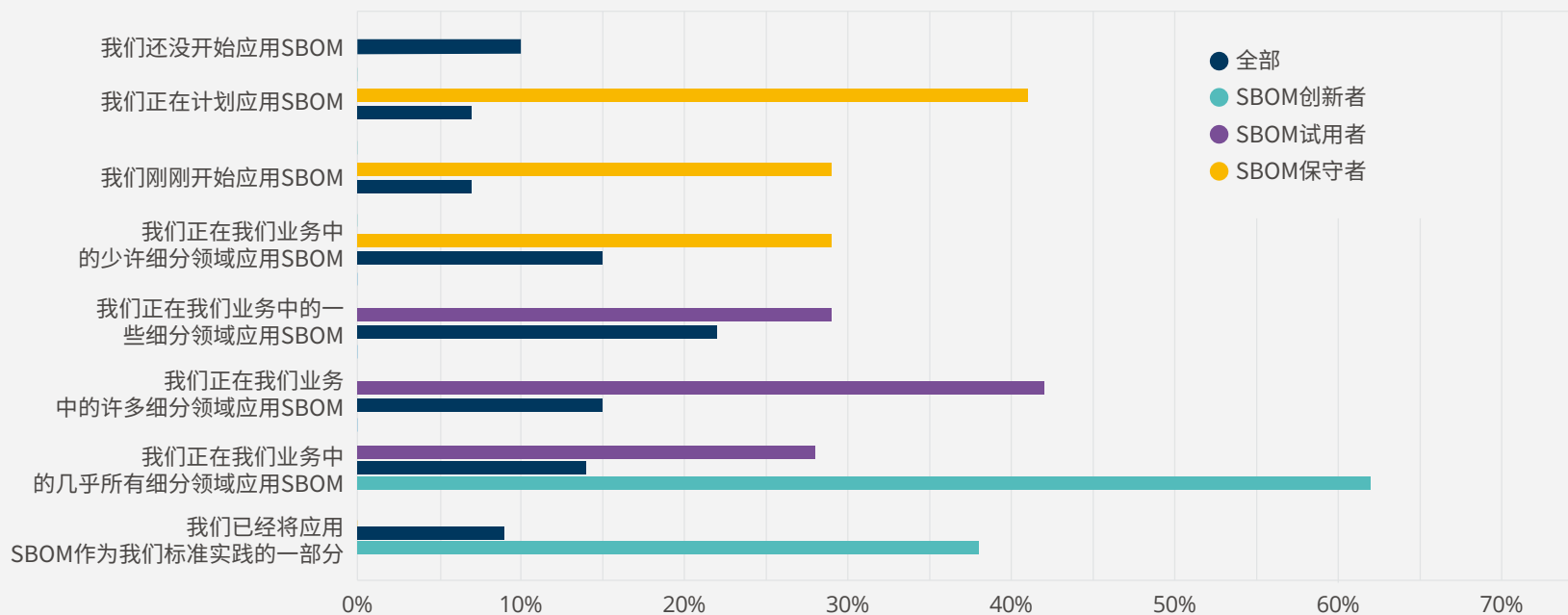
将SBOM就绪分布的总体结果（图20）与生产SBOM的组织计划（图21）进行比较，可以看出组织并没有达到SBOM的准备程度。图21显示，40%的整体样本处于SBOM规划阶段（将在未来6-24个月内生产SBOM）。这大大超过了SBOM准备规划/开始阶段的14%。

同样，整个样本中有20%的人说他们在少数或部分业务中生产SBOM，这远远低于38%声称他们在少数或部分业务中生产SBOM的人。

图20

你的群体当前的SBOM准备情况如何？

单选 | 根据SBOM成熟度划分 | 样本个数=341



考虑到21%的样本在许多或几乎所有业务部门生产SBOM，而在SBOM准备问题中只有29%的样本生产SBOM，这个差距缩小了一点。

在目前生产SBOM的组织中，SBOM准备和SBOM生产之间的总体差异导致了27%的减少(从67%到49%)，而在计划交付SBOM的组织中相应增加了66% (从24%到40%)。如果组织还没有开始他们的SBOM之旅，或者不确定，或者不知道如何回答这个问题，那么就没有实质性的改变。

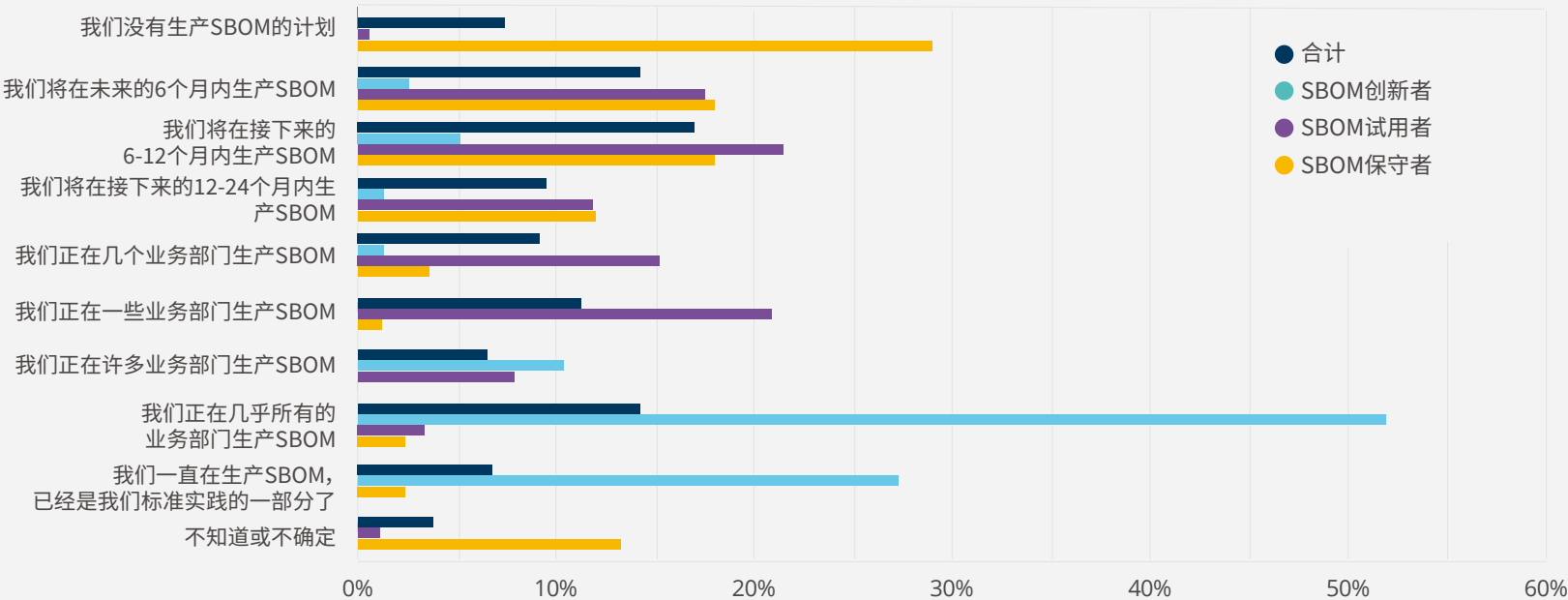
生产SBOM的益处

考虑到我们的样本中49%的组织已经在生产SBOM，40%正在计划生产SBOM，这些组织已经从他们采用SBOM的经验中看到了好处。图22指出了用户期望通过生产SBOM获得的益处。总的来说，51%的组织报告

说SBOM使开发人员更容易理解广泛且复杂的项目中的依赖关系。在微服务应用程序具有许多组件的时代，每个组件通常具有一定数量的依赖关系。SBOM显式地标识依赖关系，随着应用程序中组件的复杂性和数量的增加，这一点越来越有用。对61%的SBOM创新者和55%的SBOM试用者来说，依赖关系的识别尤其重要。识别依赖关系是两个最重要的优点之一。

图22还显示了从全局来看，SBOM对监控组件的漏洞有重要作用。总体而言，49%的组织认为这是一种好处，63%的SBOM创新者也是如此。正如我们在图28的分析中所讨论的那样，对漏洞的监控是一项正在进行的工作。挑战在于，每个组件的漏洞列表总是在变化，因为会不断发现新的漏洞，现有的漏洞也会被修复。如何及时地将这些信息传达给组件的使用者，这是一项正在开展中的工作。由于这是SBOM创新者确定的主要好处，因此一种有效的漏洞监控方法是SBOM的预期特性。

图21
你的组织生产SBOM的计划是什么？
单选|根据SBOM成熟度划分|N=337



随着开源软件的广泛使用，许可证遵从性是一项重要的要求。图22显示，44%的组织认为SBOM是识别和遵守许可义务的有效方法。59%的SBOM的创新者立马强调了许可证合规的重要性。

总之，对依赖关系、漏洞和许可证合规性的理解代表了SBOM所能提供的最重要的好处。

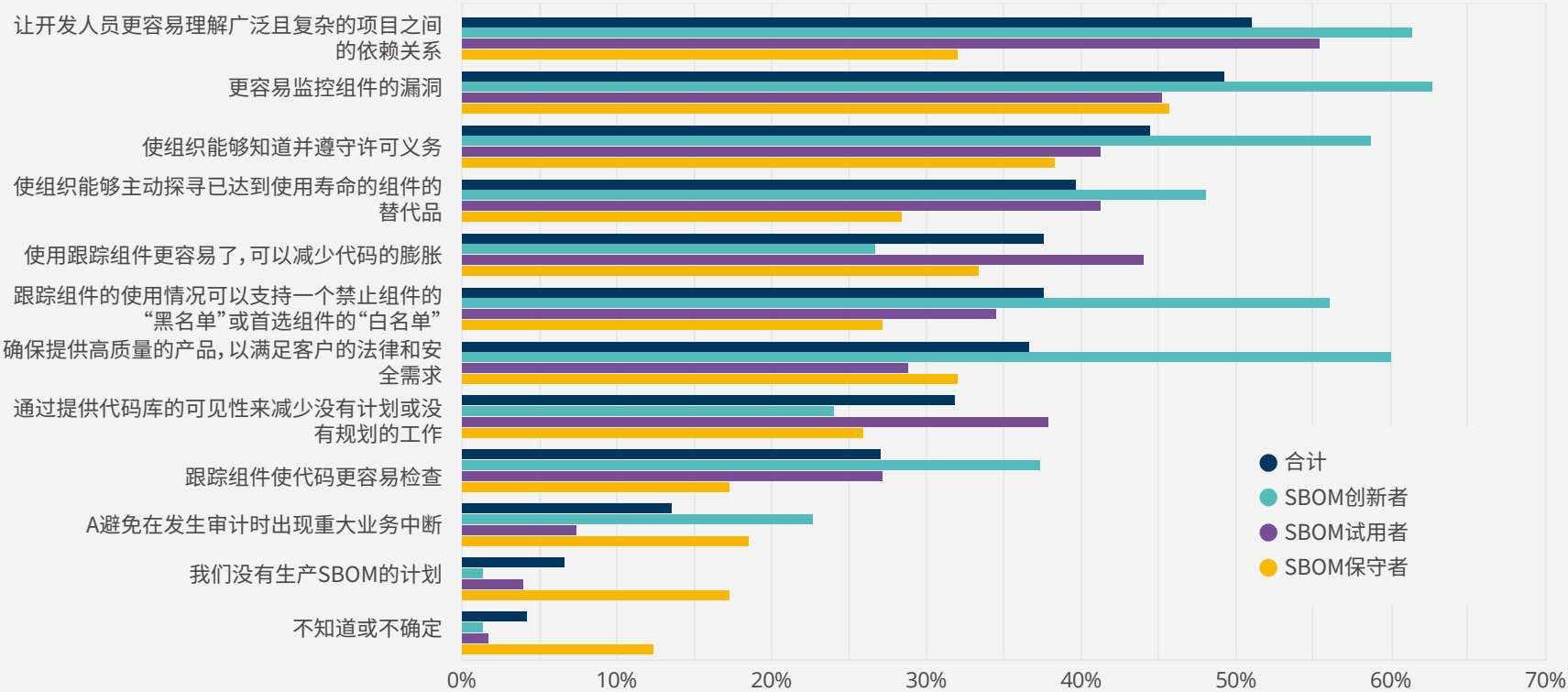
56%的SBOM创新者对组件“白名单和黑名单”的概念感兴趣，可以帮助设置访问权限控制。60%的SBOM创新者还对使用SBOM来确保交付满足客户法律和安全需求的高质量产品感兴趣。

“我们对SBOM的需求始于这样一个事实，即我们有数以千计的产品和数以千计的产品版本。随着第三方漏洞的识别，我们每年花费数千小时进行影响评估，以寻找我们产品中的这些漏洞.....我们发现，如果你有一个SBOM，那么我们就不必那么麻烦项目团队，而且进行研究所需的时间也更少。”

图22

您期望通过生产SBOM来实现什么好处？

多选|根据SBOM成熟度划分|N=333, 有效样本=333, 总样本=1,263



家全球领先的能源产品供应商与我们讨论了他们的SBOM之旅：

“我们对SBOM的需求始于这样一个事实，即我们有数千种产品和数千个产品版本。随着第三方漏洞的发现，我们每年花费数千个小时进行影响评估，以寻找我们产品中的这些漏洞。唯一可以执行的方法是将这些影响评估发送给产品团队。有了数千种产品，其中一些产品团队甚至已经不存在了，这是相当困难的。如果你有一个现有的项目团队可以检查他们已经构建的东西，那么他们仍然需要很多时间来调查。我们发现，如果你有一个SBOM，那么我们就无需那么麻烦项目团队，而且进行研究所需的时间也更少。”

生产SBOM的担忧

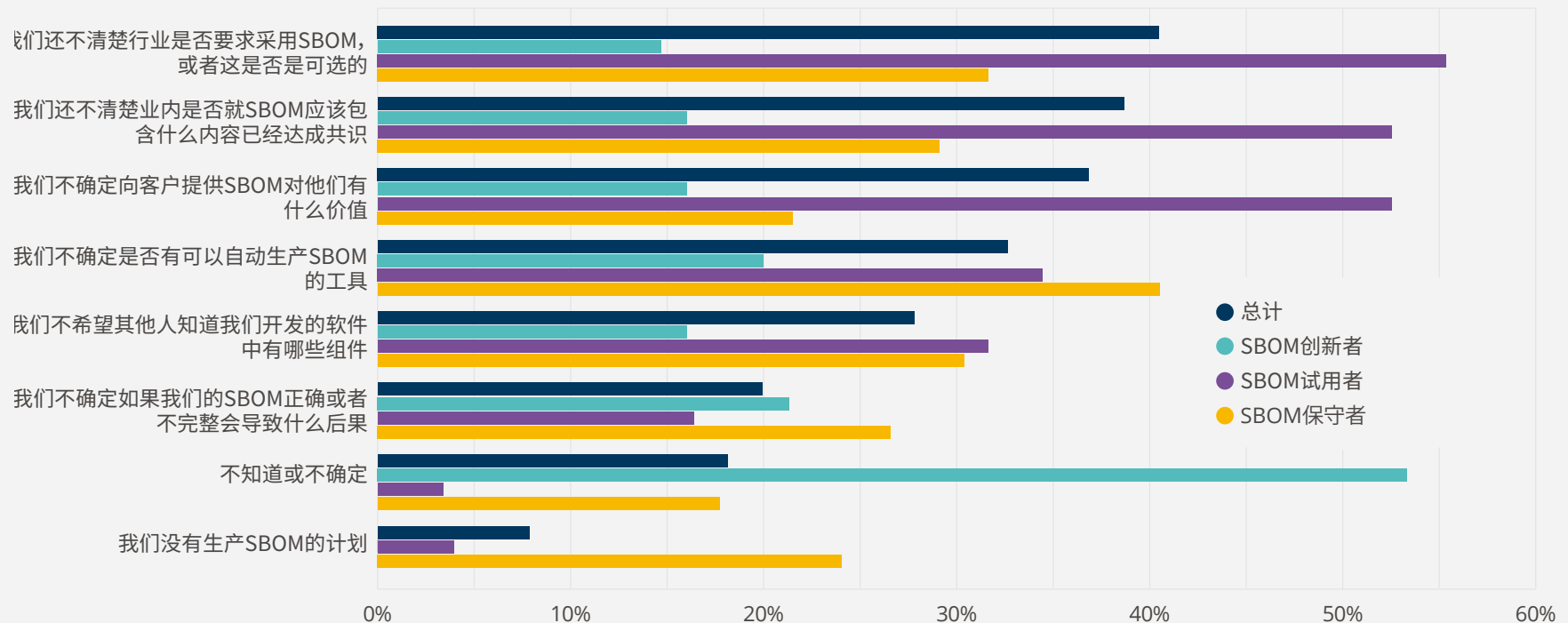
SBOM市场的新生状态生动地反映在各组织对SBOM使用的担忧中。图23按重要性递减顺序显示了这些担忧，并按SBOM成熟度对数据进行了细分。总样本的40%至33%的人表达了前4项担忧。

40%的样本确定的主要担忧是该行业是否致力于要求采用SBOM。美国食品药品监督管理局（FDA）从2018年开始提供初步的SBOM市场指南，并在2021年优先提供最终的SBOM市场指导。预计该指南将要求医疗器械制造商在其产品中包含SBOM信息。因此，医疗保健市场拥有快速跟踪

图23

你对生产使用SBOM有什么担忧？

多选 |按SBOM成熟度划分|N=331，样本个数=331，总样本个数=736



的SBOM。其它市场，包括汽车、制造和能源，每个领域都有特定的需求，但都希望从医疗保健SBOM合规性的演变中识别最佳实践，并采用之。虽然这表明SBOM市场正在蓄势待发，但领先的软件供应商的参与却参差不齐，导致领先的供应商和最终用户质疑SBOM计划的真实性。

第二个重要担忧是，39%的样本表示，行业是否已经就SBOM应该包含的内容达成了共识。NTIA在其2021年7月的文件中就此提供了指导：软件材料清单的最低要素。该文件有助于定义SBOM应该包含什么，但在很大程度上，它将关于数据格式、实施和流程的讨论留给了供应商和行业组织。虽然SBOM领域的进展正在加速，但领先的IT供应商和组织明显缺乏可见性和信息传递，这是所有这些问题的根源。

供应商和最终用户也不确定向客户提供SBOM的价值所在。37%的整体样本表达了这一观点。鉴于SBOM在识别依赖关系、漏洞监测和许可方面的明显好处，这种担忧不太可能长期存在。

最后，总样本的33%不确定是否有自动化生产SBOM的工具。这是一个合理的问题，但需要在组织政策和运营模式流程的背景下解决。

考虑到IT 供应商和服务提供商社区的产品开发和产品营销能力的有效性和规模，缓解这些担忧的有效方法是显著提高其支持水平。

图23还显示了一个独特的特征，即SBOM创新者对SBOM生产问题的关注度（15%到21%）远低于SBOM试用者（16%到55%），或SBOM保守者（22%到41%）。此外，SBOM创新者对不知道或不确定的回答为53%，这表明创新者主要致力于SBOM，并且主要关注未知的未知因素。

“第二个重要担忧是，39%的样本表示，行业是否已经就SBOM应该包含的内容达成了共识。NTIA在其2021年7月的文件中就此提供了指导：软件材料清单的最低要素。该文件有助于定义SBOM应该包含什么，但在很大程度上，它将关于数据格式、实施和流程的讨论留给了供应商和行业组织。”

SBOM消费观点

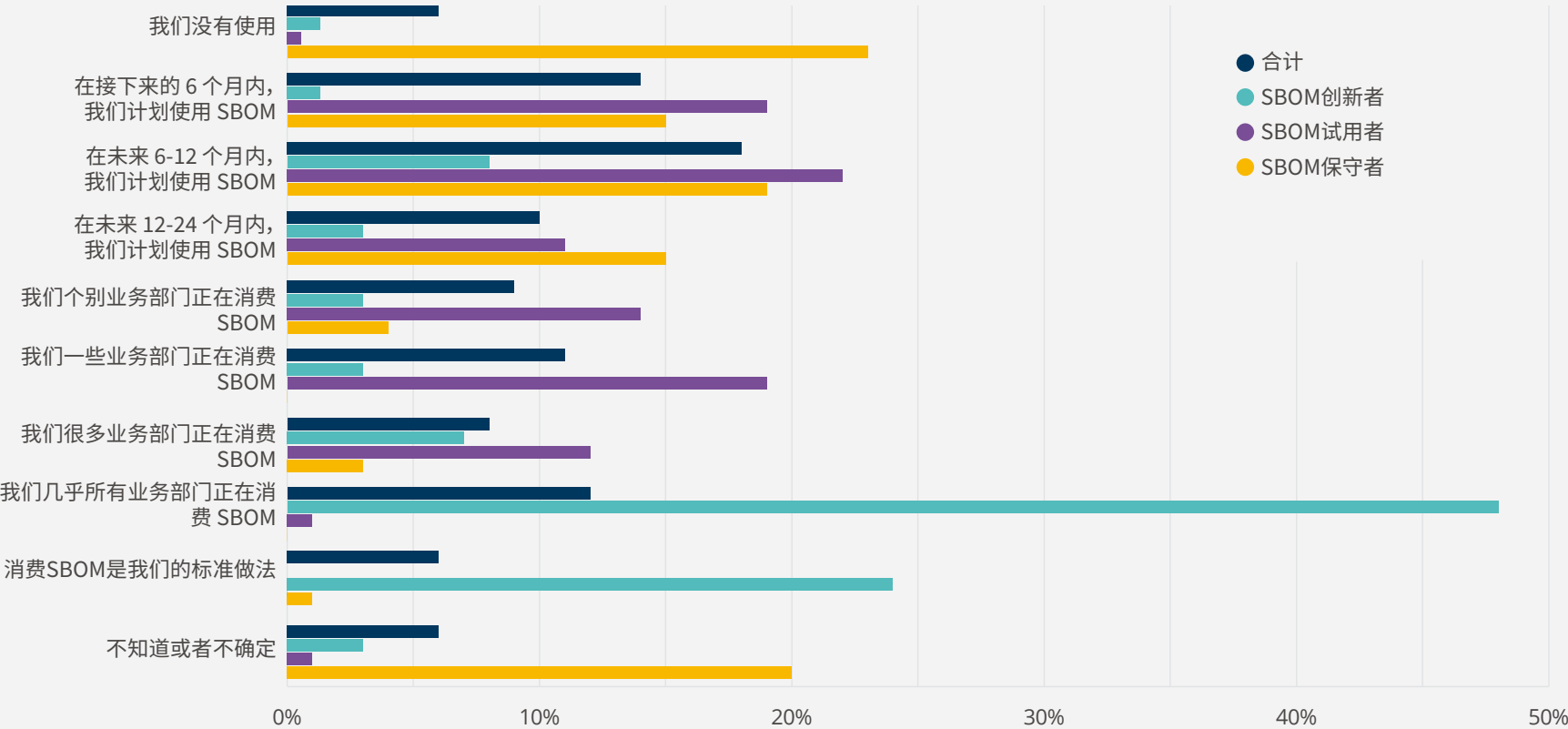
SBOM消费模式与SBOM生产模式完全一致。图21 (SBOM生产) 和图24 (SBOM消费) 背后的数据相关性的值为0.70, 接近强相关性。这意味着受访者通常以同样的方式回答这些问题。这在直觉上是有道理的, 因为

关注SBOM生产的供应商和最终用户也关注SBOM的上游消费。

图24

你们公司有什么样的消费SBOM计划?

单选|按SBOM成熟度划分 样本个数=330



随着最终用户可能在消费上对SBOM更感兴趣，他们也有兴趣生产SBOM以支持他们所生产软件的安全性和可维护性。

我们与全球能源产品供应商就关于SBOM的价值进行了讨论，总结如下：

“如果我是资产所有者，我不仅想要SBOM，而且还想要漏洞信息，及如何验证组件的真实性和完整性，因此我不但需要证书信息，我还需要知道它们对应的散列值。”

一位美国食品和药物管理局的高级政策顾问就SBOM在医疗行业的作用和重要性发表如下看法：

SBOM的用途是多样的。我们倾向于从软件的透明度的角度出发，因为医疗和保健部门目前的状况是，我们甚至没有这方面的信息。个别情况下，如果有需要的话，医院里的人都有能力找到这些信息。但是医院采购人员不知道如何利用SBOM检查软件包管理器列表，以及开源软件的许可分发列表里是否存在不应该引入的风险软件。他们没有这些信息或者是缺少做出这些决定的专业知识。另外一个问题是，没有人愿意披露这些信息。医疗器械制造商未必愿意承认他们在某些情况下使用过时的软件。所以，他们不一定想告诉其他人他们的产品中包含什么。因此，对于我们来说，这始于透明度问题。因为如果你没有这些信息，你不能轻易做任何决定，也无法轻易地进行任何评估或评价。但一旦你有了它——一旦你有了SBOM，每个人都可以看到这些信息，你就可以正式开始使用SBOM，从而有效地管理风险。

“还有一种认识是，当其它领域发生网络安全漏洞时，会令人恼火。你也许会丢失信息或者可能遭受巨大的财产损失，但人们不太可能会受到身体伤害。但在医疗保健中，如果软件安全漏洞被利用，有人甚至很多人的健康可能因此会受到伤害。

“现在医院有更大的采购能力，它们将SBOM纳入合同的必要条款中。医院现在想购买一个设备时，他们会说‘你必须给我提供SBOM，否则我不会购买你的产品。’所以呢，现在似乎更多的市场力量占据了主导地位。”

SBOM消费

图24显示，在我们样本中，只有6%的组织没有计划使用SBOM。在接下来的6到24个月内，42%的组织有计划开始使用SBOM。另外40%的组织正在生产中使用SBOM，以及6%的组织以及将使用SBOM作为他们的标准实践。按SBOM成熟度划分结果表明，SBOM创新者大量使用SBOM，而SBOM保守者要么没有计划使用SBOM，要么还没有规划SBOM。

消费SBOM带来的收益

供应商和最终用户一致表示使用SBOM有好处。图25显示了总体样本48%到53%受访者认为的前5大好处。前两大好处包括，能够提供更好地符合合规性与报告要求的组件信息（53%），以及能够提供有利于风险决策的信息（53%）。当使用第三方软件时，解决合规性、财务和声誉风险是组织必须考虑的关键目标。

接下来的三大好处：由SBOM提供的软件透明度使得及时发现漏洞（49%）、主动识别已达到生命周期终点的组件（49%）和及时察觉风险组件（48%）成为可能。这些好处有助于组织提高安全性，减少风险并为其客户和商业伙伴提供更可靠的服务。

消费SBOM的担忧

与SBOM生产担忧类似，SBOM消费担忧主要来自于SBOM试用者和SBOM保守者。图26显示了首要的SBOM消费方面的担忧，包括行业对SBOM需求的不确定性（49%）、SBOM消费的自动化工具（48%），以及业内对SBOM应包含内容的共识（44%）。

这些都是严重的问题。虽然令人鼓舞的是SBOM创新者并没有过度关注这些问题，这是一个积极的信号。向SBOM试用者和保守者——占我们样本的75%——传达SBOM的价值主张，几乎没有什么作用。为了消除SBOM行业特定要求的不确定性，需要政府机构、行业组织（包括特定行业的信息共享和分析中心）以及IT供应商和服务提供商，以增加围绕SBOM价值主张、工具可用性、集成能力、DevOps流程和最佳实践的消息传递。

围绕SBOM工具的可用性存在的不确定性，是供应方面的问题。行业组

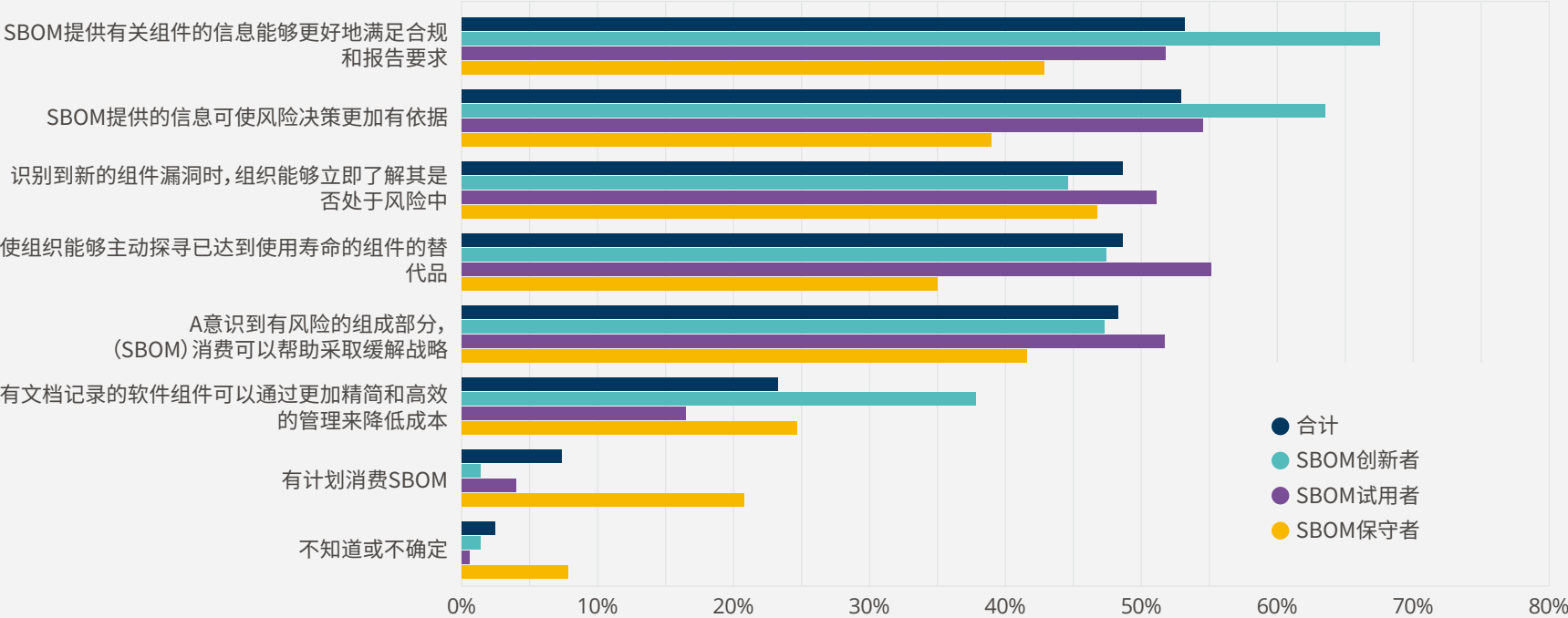
组织和供应商需要加大对SBOM工具组合及其可见性的投资力度和宣传力度。正如我们将在后面看到的报告显示，SBOM 工具市场可能会在 2022 年和 2023 年爆发式增长。建议供应商和服务提供商快速跟踪产品和服务，以满足最终用户的需求。

最后一个是业界对SBOM应包含的内容缺乏共识，这与其说是知识产权问题，不如说是安全问题。漏洞识别和报告方面的进展目前正在进行中。由于安全性已成为SBOM的重要维度，我们预计该问题将在 2022 年得到解决。

图25

你希望通过使用SBOM实现哪些好处？

多选|按SBOM成熟度划分|样本个数=327,有效样本个数=327,全部样本个数=931



结论

本SBOM就绪水平的调查，显示SBOM熟悉度、SBOM就绪程度以及其在生产和消费环节的采用程度均超出我们的预期。迄今为止，SBOM的大多数投资来自公共和私营企业，如英特尔、西门子、索尼、丰田和风河。美国联邦政府部门（NTIA, FDA, NIST和商务部）现在都在倡导SBOM，并在为某些行业制定相关法令。IT行业相关组织和厂商在不断宣传SBOM的重要性，并支持数据格式、最佳实践和技术路线图定义的演变。这是一个良好的开端，但为了跨越鸿沟，SBOM的市场还需要大力发展。

T我们与美国食品和药品管理局的政策顾问谈及SBOM的发展时，他这样

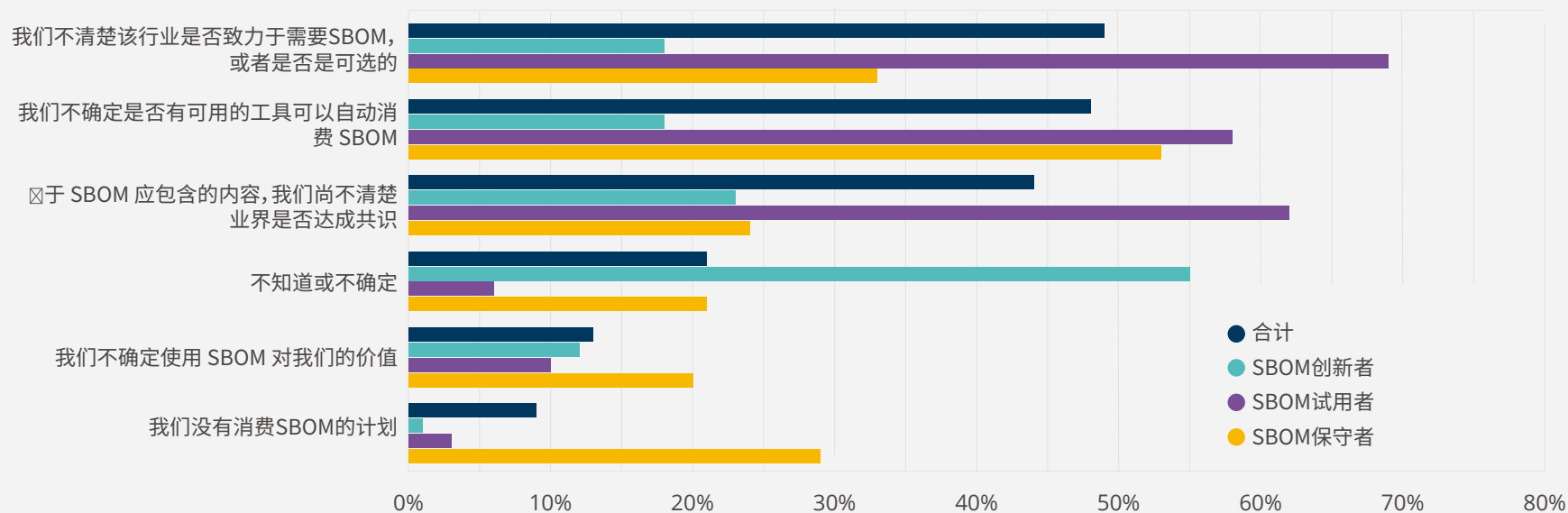
说：

“医疗保健领域正在发生的事情与其他行业不同。在其他行业中，随着基层最佳实践逐渐被采用，最终监管机构便宣布正式采用了这种最佳实践。医疗保健行业的情况恰恰相反。监管机构宣布将执行SBOM，并且期望SBOM最终会成为在美国销售医疗产品的必要条件——这是一个价值数十亿美元的行业。最近的行政命令是在几年后发布的，但它正好代表政府监管部门在医疗保健方面增加的压力。相关各方基本上都说，我们没有选择。我们必须想办法解决这个问题。因此，我希望看到对供应链中的每

图26

你在消费SBOM方面有哪些顾虑？

多选|按SBOM成熟度划分|样本个数=324,有效样本个数=324,全部样本个数=593



个环节都产生影响,做出改变。当医疗保健领域的制造商转身对供应商说,除非你提供SBOM,否则我不会再付钱给你了。这最终会成为一个N减1的强迫效应:每个人都转身对自己的供应商说,因为我被强迫这样做,你也会被强迫这样做。最终,大家都处于被强迫的状态。”

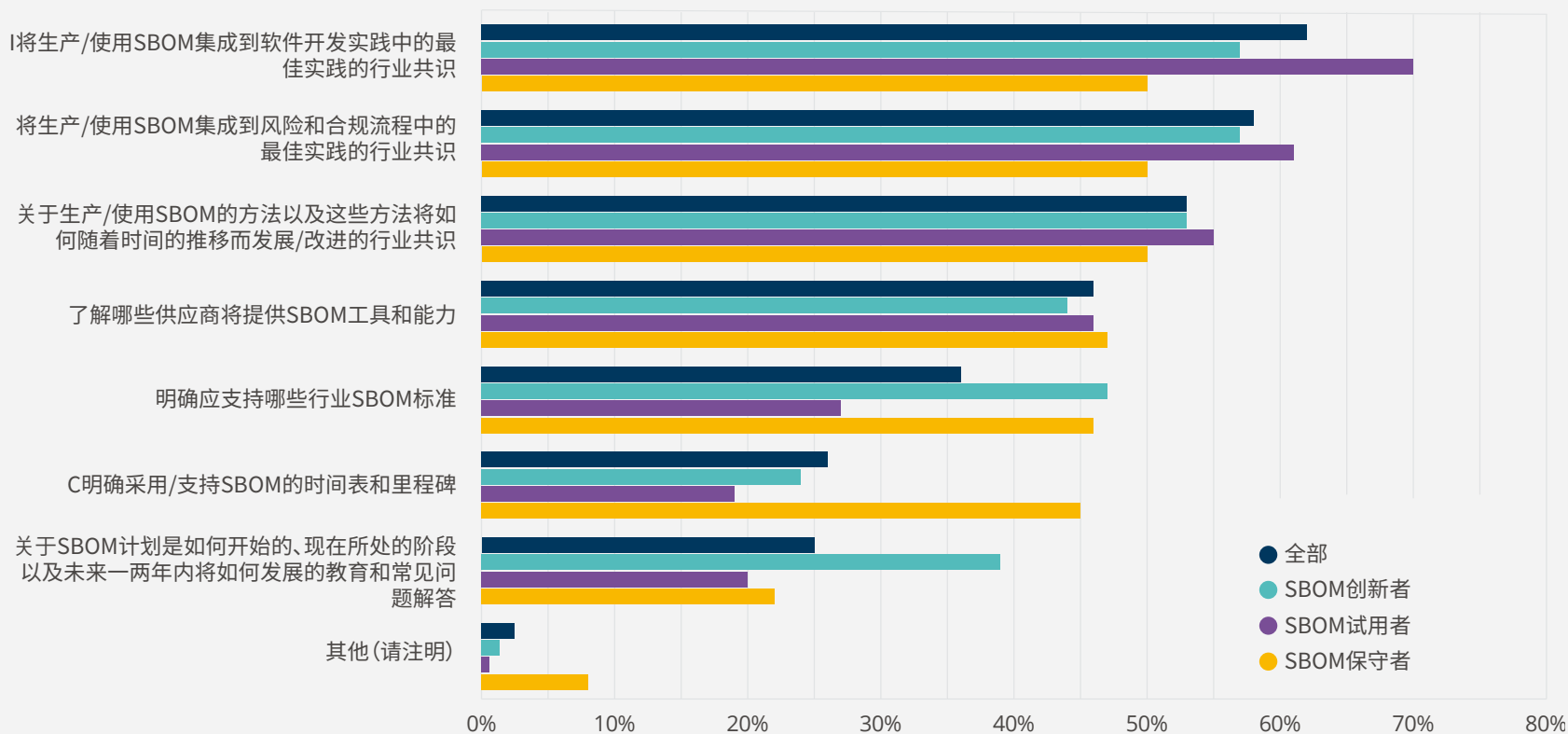
如何改进SBOM

图27提供了关于如何改进SBOM活动的反馈。62%的受访者认为,最紧迫的问题是需要就最佳实践达成行业共识,以便将SBOM的生产和使用整合到软件开发中。SBOM的生产和使用发生在开发运维中。挑战在于,每个组织都有独特的开发运维工具链、流程和活动。关于SBOM的生产或使用应该发生在开发运维中的哪个环节,目前尚未达成共识。SBOM的生产

图27

什么有助于您的组织提高其生产和/或使用SBOM的能力?

多选|样本个数=319,有效样本=319,总样本=985



显然是一种面向开发的活动，但SBOM的使用既可以发生在开发中，也可以发生在运维中。而何时应该生产或使用SBOM的问题又加重了此困惑。另一方面，已知依赖关系和漏洞的不断变化，也影响了关于应该在何处、何时生产和使用SBOM的决策。

一家大型消费电子产品制造商描述了在采用SBOM过程中的一些难题。其中一个重大难题是：鉴于某些数据格式的复杂性，要弄清楚如何和从哪里开始是非常复杂的。另一个相关的问题是：各种SBOM数据格式之间缺乏互操作性。这些问题表明用于促进SBOM生产、使用、整合和互操作性的SBOM工具的可用性有限。

排名第二的行业需求（占总样本的58%）是关于将SBOM的生产和使用纳入GRC（治理、风险和合规）流程的最佳实践的共识。有一些重要的政策和运营决策是围绕着SBOM进行的。拥有OSPO（开源项目办公室）和（

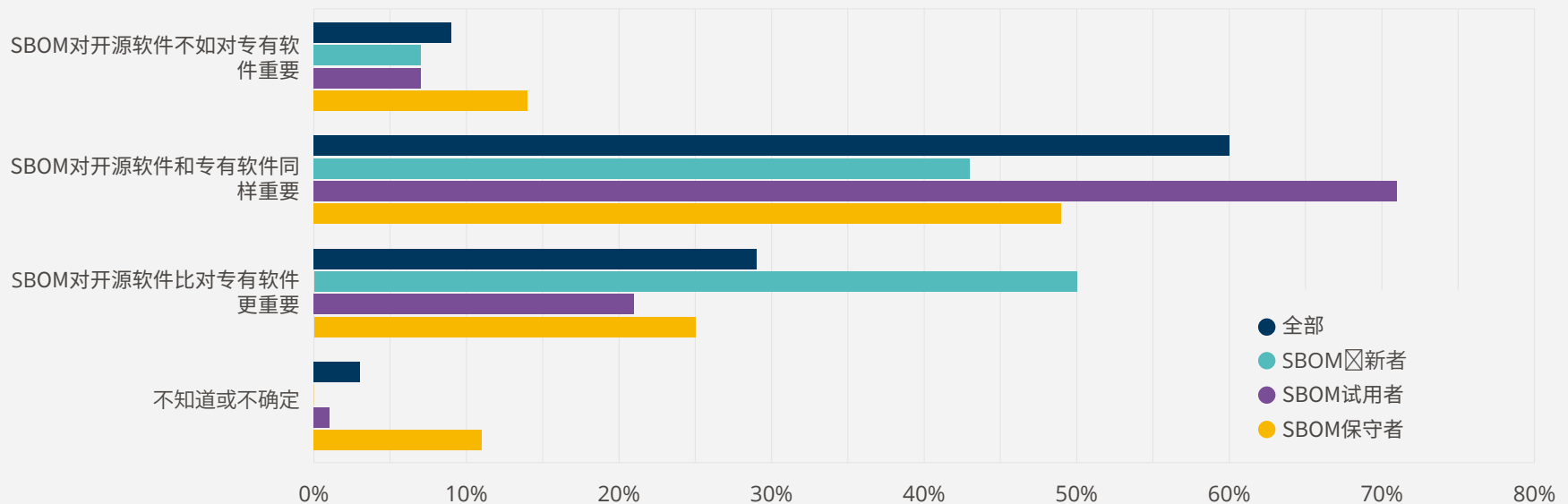
或）CISO（首席信息安全官）的组织能够很好地满足这一需求。然而，这项SBOM就绪水平调查显示，大约有20%的组织没有OSPO或CISO。这一数字在SBOM创新者和试用者中缩减到10%左右，但在SBOM保守者的组织中增加到35%至40%。

图27还显示，53%的受访者正在寻求，关于生产或使用SBOM的方法，将如何与时俱进的行业共识。NTIA最近才公布了软件材料清单的最低要素，SBOM的数据格式也在迅速发展。虽然这种变化是新兴市场的特点，但它显然使SBOM的生产和使用更具挑战性。同时，IT供应商群体显然有很大的市场机会来帮助塑造和加速SBOM市场。图27显示，占总样本46%的受访者正在努力了解哪些供应商将提供SBOM工具和能力。

图28

与专有软件相比，SBOM对于开源软件有多重要？

单选 | 按SBOM成熟度划分 | 样本个数 = 316



SBOM的重要性

本报告前面的图6显示，我们的样本中有98%的组织使用开源软件。由此可见，市场上的大部分专有软件都以某种方式利用了开源软件。在这种情况下，图28显示了SBOM对于开源软件和专有软件的重要性。

图28显示，60%的组织认为SBOM对开源软件和专有软件同等重要。在其余的组织中，有29%认为SBOM对开源软件更重要，而9%的组织认为SBOM对开源软件不太重要。可以从以下几种角度解释这个数据。

60%的样本认为SBOM对开源软件和专有软件同样重要，这意味着大多数组织希望看到所有软件组件的SBOM。然而，29%的被调查者认为SBOM对开源软件更重要，这可以解释为：尽管专有软件供应商可能在其产品中利用开源，但他们却在审查和测试其产品方面做得更好。更复杂的是，SBOM创新者在这个问题上的分歧不太大：43%的受访者认为SBOM对开源软件和专有软件同等重要，同时有50%的被调查者说SBOM对开源软件更重要。据推测，SBOM创新者在使用SBOM方面更有经验，且对开源SBOM的需求更大。

摆脱这一困境的办法是，在假设所有软件产品都可能包括一些开源代码的前提下，通过立法让所有软件包含SBOM。这种方法已经成功地应用于医疗市场，被供应商所接受，并受到终端用户的欢迎。其他市场，包括汽车、能源和制造业，正在观察医疗市场的SBOM转型。

尽管开源软件与专有软件对SBOM需求不太一致，但在整个软件供应链中解决网络安全问题是至关重要的。总统的行政命令不是一次警钟，而只是明确网络安全是一个突出问题，需要加快解决网络安全的步伐。好消息是，在过去的4到5年里，美国联邦政府、IT供应商和IT行业组织一直在制定、开发SBOM政策、数据格式和工具。看来，最初的SBOM磨合问题已经过去了。在不久的将来，最大的挑战是如何跨越鸿沟，使SBOM被早期的大多数人采用。面临的挑战是如何推动监管、SBOM成熟度、供应商参与、产品开发和持续传递有效增加价值的信息。

SBOM的未来

根据组织生产（图21）或使用（图24）SBOM的意图，可以对SBOM的使用（渗透率）和增长进行预测。SBOM生产和消费的总体情况是相似的。因此，正如图29所示，我们可以将这两种措施结合起来。图29中的预测，是根据计划生产或使用SBOM的组织，与已经生产或使用SBOM的组织之间比值的增量得来的。2021年，48%的渗透率是已经在其业务中（少数/部分/许多/几乎所有/作为标准做法）生产或使用SBOM的组织的百分比（来自图21和24）。2022年的渗透率增加了那些计划在未来6个月或一年内生产或使用SBOM的组织。同样，2023年的渗透率也增加了那些计划在12-24个月内生产或使用SBOM的组织。

图29显示，2022年的SBOM生产或使用增长预计会很高，将达到66%，使SBOM的渗透率达到78%。2023年，SBOM的年增长率将下降到13%，但仍将推动SBOM的渗透率达到88%。这让我们觉得这是一

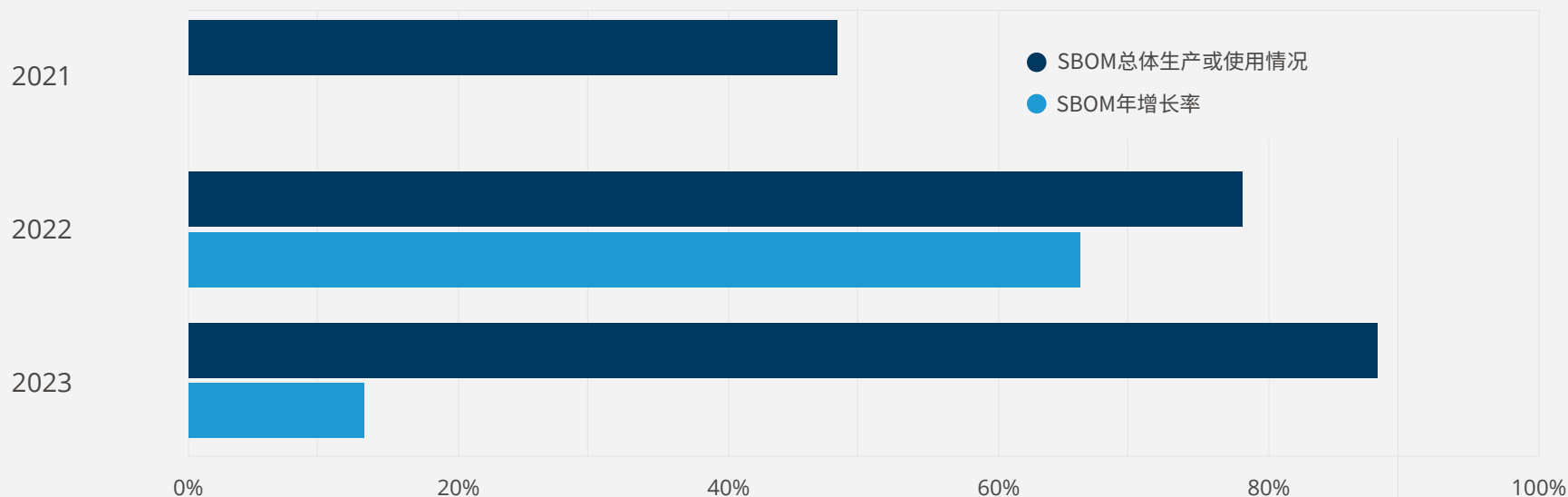
“尽管开源软件与专有软件对SBOM需求不太一致，但在整个软件供应链中解决网络安全问题是至关重要的。总统的行政命令不是一次警钟，而只是明确网络安全是一个突出问题，需要加快解决网络安全的步伐。好消息是，在过去的4到5年里，美国联邦政府、IT供应商和IT行业组织一直在制定、开发SBOM政策、数据格式和工具。”

个非常积极的增长情景，可能取决于SBOM生产和消费工具市场的快速发展和增长。

图29

预测2021-2023年组织对SBOM的生产或使用及增长

样本个数=330-337



美国政府在购买软件时坚决要求提供SBOM，部分原因是网络攻击的影响，这个影响最终导致了SunBurst的出现。但我们也更清楚地认识到，随着向数字经济转型和对软件的依赖，数字资产对几乎所有的组织都是至关重要的，在某些情况下是生命攸关的，如在医疗设备行业。这项研究表明，SBOM的生产和使用给我们带来了各种好处。SBOM最初只是被当作一种识别和保护知识产权的方式。然而，安全现在也是SBOM议题的一部分。最近与美国国土安全部的一位高级政策顾问的讨论放大了SBOM的作用：

“SBOM帮助我们解决了几个重要的问题。其中之一是：当有新的漏洞被发现时，我是否受到影响？如果你有一个SBOM，你就可以弄清楚你可能受到影响的地方。一个SBOM越是完整，你就越有可能证明你没有受到影响。然而，更重要的是要掌握我们的软件供应链。我们需要关注度，我们需要激励，我们需要弹性。SBOM不会给我们这些，但它们使所有这些成为可能。换句话说，没有SBOM，我们就无法前进。广泛使用SBOM，将使更多的组织关注他们正在使用的开源产品，和他们在供应链中使用的商业产品。就像我们在传统供应链和实体商品上看到的那样，意识可以驱动更好的质量。现在，基本的SBOM不能告诉你，是否有人在一个流行产品中植入了后门。SBOM能做的是：一旦我们知道被植入了后门，每个人都可以弄清楚他们是否受到影响。但是一旦你有了这种认识，下一步就可以开始对谱系和元数据溯源进行分层，并开始集成到我们的工具中——这样，我们实际上就可以检测到恶意攻击者。因此，SBOM是必要的，但不足以帮助在更好的软件保证和更好的软件供应链方面取得实质性进展。

本报告中关于SBOM的生产（图21）和使用（图24）数据显示，49%的组织正在生产一定数量的SBOM；同样，56%的组织正在消费一定数量的

“我们需要关注度，我们需要激励，我们需要弹性。SBOM不会给我们这些，但它们能使所有这些成为可能。换句话说，没有SBOM，我们就无法前进。”

SBOM。虽然SBOM主题和SBOM工具市场并没有引起很多关注或产生名气，但许多行业都在参与建立SBOM政策和最佳实践。现在，SBOM倾向于低调进行的原因是：行业活动是特定领域的。许多领先行业已经建立了信息共享和分析中心（ISACs）。

SBOM工具市场已经吸引了大约20家供应商。其中一些供应商来自邻近的市场，如软件组合分析（SCA）、工件注册和存储库管理（ARRM）以及软件安全。也存在各种开源项目——有些专注于SBOM的生成。我们认为会有一个横向的SBOM工具市场，其中有特定领域的插件进行政策、数据和元数据的行业定制。

在这个节骨眼上，美国联邦政府已经投入了资金，以刺激对SBOM的需求。他们的做法是要求政府购买的软件必须有SBOM。这与医疗保健领域有些不同。在医疗保健领域，联邦政府出台了法规，要求设备制造商提供SBOM。然而，结果是相似的——真正的终端用户需求或代理需求。SBOM的数据格式有多种方法支持，其中一些被认为是ISO标准。如前所述，已经有SBOM的供应方在准备工具，以帮助应对预计将迅速增长的需求。SBOM的市场可能会迅速发展，并且有可能通过全球领先的软件供应商的支持发展得更快。

调研方法

本节解释了我们的抽样、数据分割的方法，以及我们如何将各组织对SBOM准备就绪的调查情况整理为SBOM成熟度的衡量标准。

我们调查了谁，如何分析数据

该研究的目的是了解组织在生产和消费SBOM方面的准备情况。采用的技术包括基于定量调查和定性访谈的研究。该项目的定量方面包括在2021年6月至2021年8月之间对全球专业技术人员进行的调研。调查除英语外，还提供了六种语言：简体中文、日语、韩语、法语、德语和俄语。受访者来自两个机构：Linux基金会社区成员和来自第三方小组的技术专业人员。目标受访者是最终用户企业、技术供应商、解决方案和服务提供商，以及公共部门机构的IT决策者和业务线领导。

共有519名受访者接受了调查，其中291名(56%)来自Linux基金会和228个(44%)来自第三方市场调查服务IT小组。筛选标准是用于确保受访者能够在整个调查过程中回答问题。经过筛选，我们的样本共有412个完整样本，其中222个样本(占比54%)来自市场研究机构，190个样本(占比46%)来自Linux基金会的随机抽样。

数据分类和筛选

调查数据以多种方式分类，提供探索数据的各种方法。初级细分变量和定义如下：

- **数据搜集器，样本个数=412。**确定被调查者的数量(N)由Linux基金会(46%)与来自第三方市场研究机构的受访者(54%)。误差范围(MoE) = +/- 4.1% @ 90%置信水平(CL)。
- **行业类型，样本个数=405。**区分为技术供应商或服务提供商工作的受访者(21%)，与为最终用户企业工作的受访者(79%)。MoE = +/- 4.1% @ 90% CL。

- **主要行业组织，样本个数=405。**聚集全球来自22个行业的受访者，分6个主要行业（和“其他”）：技术供应商、解决方案和服务供应商(25%)、汽车(12%)、卫生保健和生命科学(11%)、制造业(7%)、金融服务(6%)、能源(5%)和其他(34%)。MoE = +/- 4.1% @ 90% CL。
- **地理区域，样本个数=402。**聚集全球十个国家受访者，区分为三个主要的地理区域：美洲(44%)、西欧(39%)、亚太地区(17%)。MoE = +/- 4.1% @ 90% CL。
- **SBOM准备，样本个数=357。**基于受访者对其机构的SBOM准备情况的回答进行汇总：创新者(21%)，试用者(51%)、保守者(24%)和不知道或不确定(4%)。MoE = +/- 4.3% @ 90%。
- **SBOM合格的受访者，样本个数=341。**基于一个自我评估问题，询问被调查者是否觉得有资格解答材料软件账单相关问题：认为有资格回答SBOM问题的受访者(83%)，认为没有资格回答SBOM问题的受访者(11%)，以及不知道或不确定的受访者(5%)。MoE = +/- 4.5% @ 90%。

本次调查的所有数据均采取了四舍五入的方式，设为最接近的整数百分比。因此，百分比的总和不一定总是达到100%。

这是一个很长的调查，平均完成时间要20多分钟，完成率为64%。这解释了为什么在上述分隔变量的样本大小上有一些差异。

采用全面的筛选标准，来确保受访者能大概率回答所有的调查的问题。筛选标准包括对特定IT问题的熟悉程度、IT领域经验、在IT或类似行业较高职位和在一个成熟的行业工作。

该项目的定性维度包括对跨行业和联邦网络安全政策制定中选定的个人进行深入访谈。

防止样本偏差

调查对象最初来自Linux基金会 (LF) 社区成员。从研究的角度来看, 这有可能导致样本出现偏差。为此, 受访者也来自第三方市场研究小组提供者。为了确定两个样本之间是否有关系, 使用显著性检验。对于数据集的大多数变量, 两者之间的样本存在显著的差异。如图30所示, 显示了按数据收集方式划分的SBOM熟悉程度, 就表明了我们发现的差异。

LF数据出现双峰分布, 显示出一个重要的群体 (34%), 他们从没听过或不熟悉 SBOM, 另外的群体 (51%) 是熟悉或非常熟悉的SBOM。这和LF社区的参与者是吻合的。社区包含一些年轻的 IT 专业人员, 他们在职业生涯早期就来 LF 接受培训和认证, 以提高他们的技能和增加就业的机

会。这部分人不熟悉SBOM并不奇怪。在LF中还存在其他一些群体, 包括经验丰富的IT专业人员, 他们在 IT 决策和政策方面发挥着重要作用, 该群体很可能很熟悉SBOM。

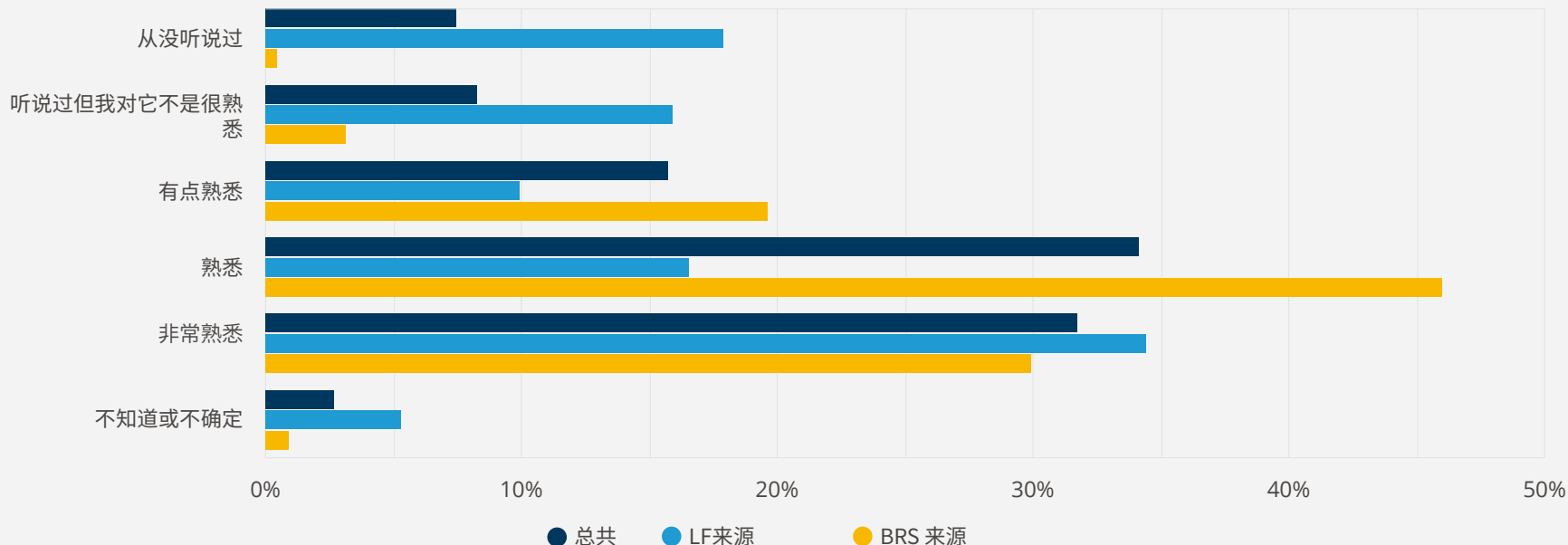
研究小组的数据显示非常不同的特征, 数据在某种程度上呈正态分布。只有4%的研究小组样本没有听说过或不熟悉SBOM这个术语, 与大多数研究小组样本熟悉或非常熟悉SBOM术语(76%)形成对比。

这个对比仅仅是众多表明LF和研究小组样本有显著差异中的一个。研究小组的样本是非常熟悉 SBOM, LF 样本没那么熟悉, 这两个样本不同的这一事实, 给我们提供了一个SBOM准备的保守观点。

图 30

您的组织对软件物料清单(SBOM)的熟悉程度如何?

单选 | 根据数据收集的方式分段 | 样本个数 = 375



受访者回答SBOM问题的能力

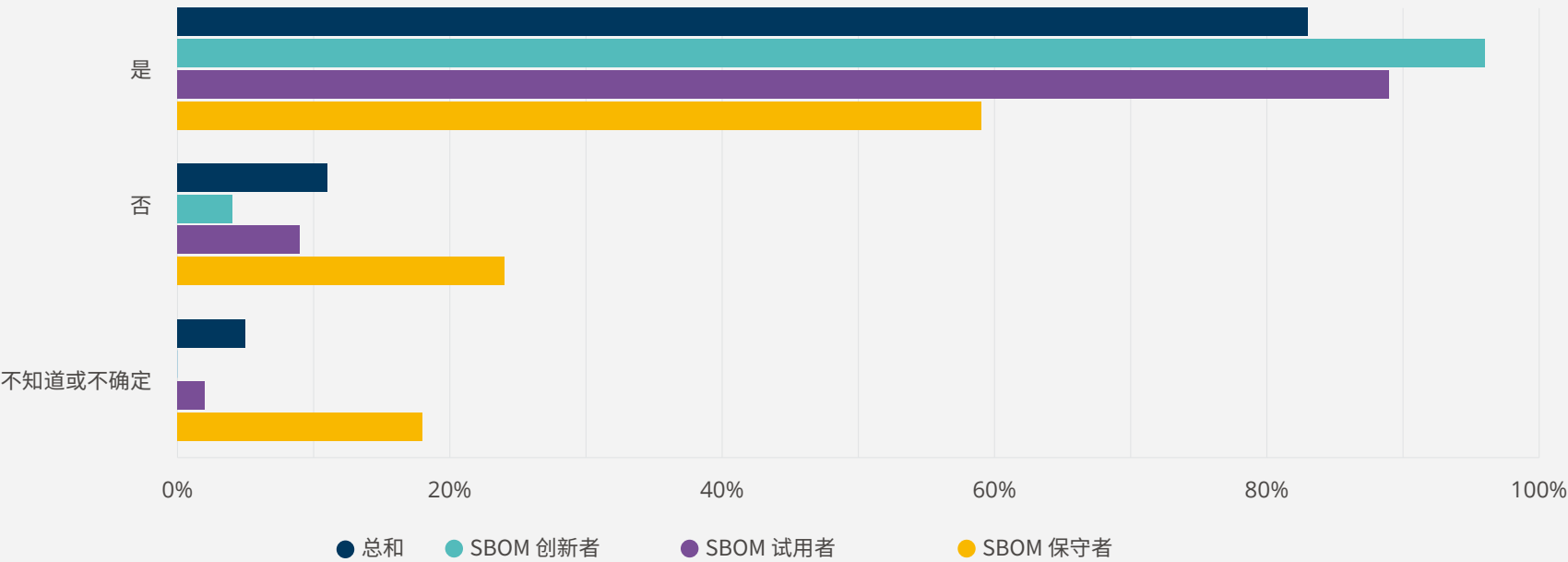
在向受访者提供SBOM定义后，调查询问受访者是否觉得有资格回答关于他们的组织如何使用或打算使用SBOM。这个问题的目的是另一种理解SBOM熟悉度的方法，以及提供细分那些没有SBOM知识的受访者的能力。图31显示了按SBOM成熟度细分的受访者感觉是否有资格回答SBOM的问题。

总体而言，大多数受访者(83%)认为有资格回答关于SBOM使用的问题，11%认为没有资格谈论SBOMSBOM的使用，5%不知道或不肯定。SBOM合格的答复与SBOM成熟度高度相关。更高的SBOM成熟度水平是和较高水平的SBOM合格的受访者、较低级别的不合格者受访者相关的。图31显示了96%的SBOM创新者认为能够回答SBOM问题，相比

之下，只有 89% 的试用者和 59% 的保守者能够回答该问题。认为没有资格回答SBOM问题 (24%) 或回答 DKNS (18%) 的受访者比例最高的是SBOM保守者。

在调查中，受访者被要求继续回答所有问题SBOM问题，不管他们觉得自己有多合格。为了这份报告中SBOM分析的目的，我们已经选出使用所有完成调查的受访者的数据。这实际上并不构成问题，因为不合格受访者几乎总是对后续的SBOM问题做出DKNS的回应。

图 31
您是否觉得有资格回答有关贵公司如何使用/打算使用 SBOM 的问题？
单选 | 按 SBOM 成熟度细分 | N = 341



尾注

1. 国际货币基金组织, 世界经济展望数据库, 2019 年数据。
2. F关于地理区域划分, 请参见本报告中的以下图表: 图3、A9、A10、A11、A14-A17。
3. 关于提升国家网络安全的行政命令”, 2021年5月, 可在<https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity>获取。
4. 出处在第一部分。
5. SBOM概览”, 国家电信和信息管理局, 2021年4月27日, 可在https://www.ntia.gov/files/ntia/publications/sbom_at_a_glance_apr2021.pdf 中查看。The Minimum Elements for a Software Bill of Materials (SBOM), US Department of Commerce, July 12, 2021
6. 软件物料清单 (SBOM) 的最少要素, 美国商务部, 2021年7月12日
7. 系统和组织的网络安全供应链风险管理实践, 美国国家标准与技术研究院, SP.800-161r1-draft2, 2021年10月。
8. SBOM选项和决策点, 国家电信和信息管理局, 2021年4月27日
9. SBOM概览, 国家电信和信息管理局, 2021年4月27日

附录 A: 人口统计资料和附带的SBOM就绪水平信息

附录包括进一步描述样本统计数据、当前IT环境和SBOM就绪水平的图表。

包括以下图表:

A1 公司员工总数

A2 主要角色

A3 主要职责领域

A4 组织的主要产业

A5 IT 组织的类型 (IT 行业组织)

A6 您是 Linux 基金会成员公司吗?

A7 按地理区域划分的受访者

A8 组织年收入

A9 按地理区域划分的组织对SBOM的熟悉程度

A10 按地理区域划分的组织中OSPO的存在情况

A11 OSPO 是否按地理区域与安全团队共享其项目清单?

A12 按地理区域划分的组织中首席安全官/安全团队的存在情况

A13 根据SBOM成熟度情况, 组织在软件生命周期的哪个阶段生产SBOM?

A14 根据SBOM成熟度情况, 组织在软件生命周期的哪个阶段使用SBOM?

A15 按地理区域划分的SBOM就绪水平

A16 按地理区域划分的组织对软件安全的关注度

A17 按地理区域划分的美国网络安全行政命令的组织认知度

A18 按地理区域划分的对美国网络安全行政命令做出调整的程度

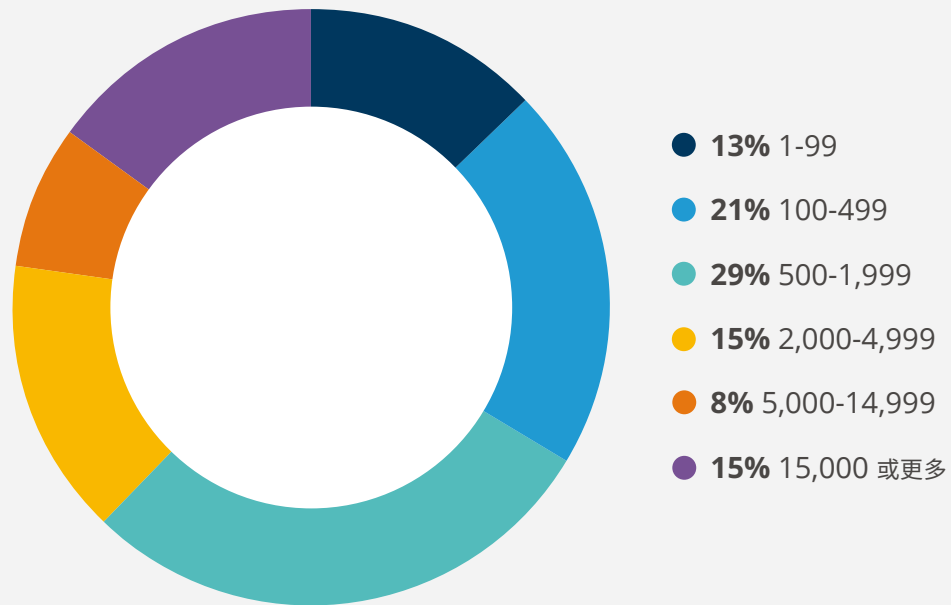
A19 按主要产业划分的组织制作SBOM的计划

A20 按主要产业划分的组织使用SBOM的计划

图A1

请估算贵公司在全球范围内共有多少员工？

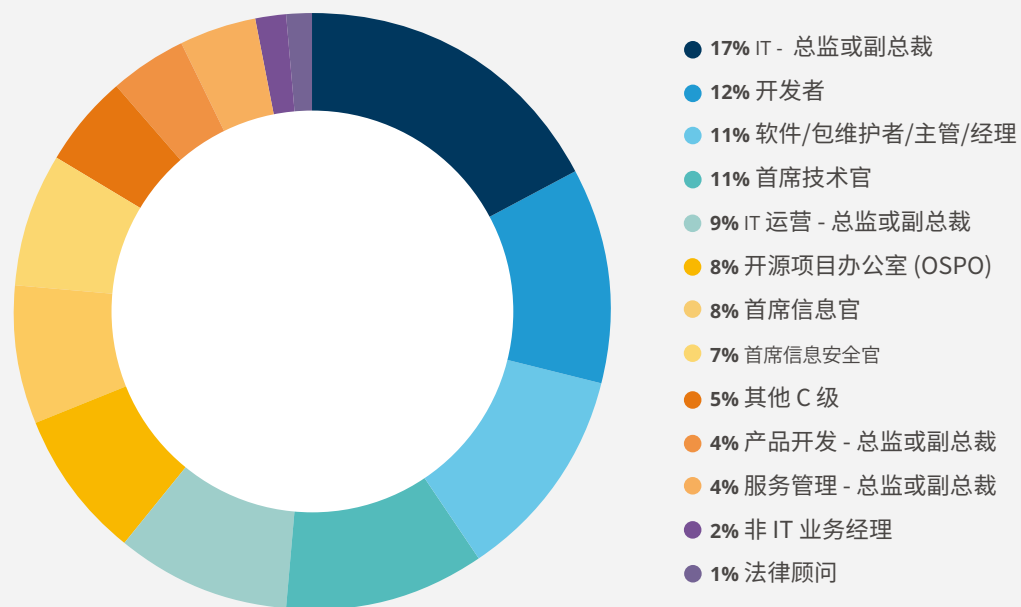
单选 | 样本个数=412



图A2

以下哪一项最能或最准确地描述你在组织中或作为承包商的主要工作角色或头衔?

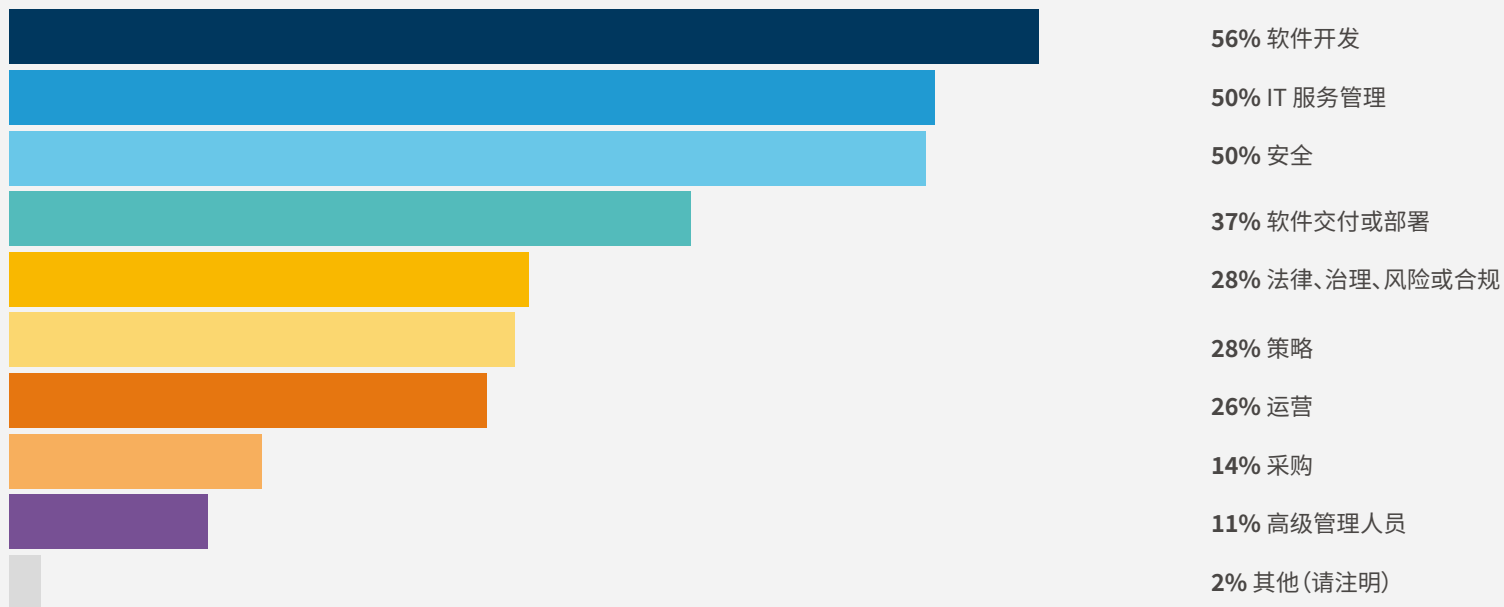
单选 | 样本个数=412



图A3

您的主要职责领域是什么？

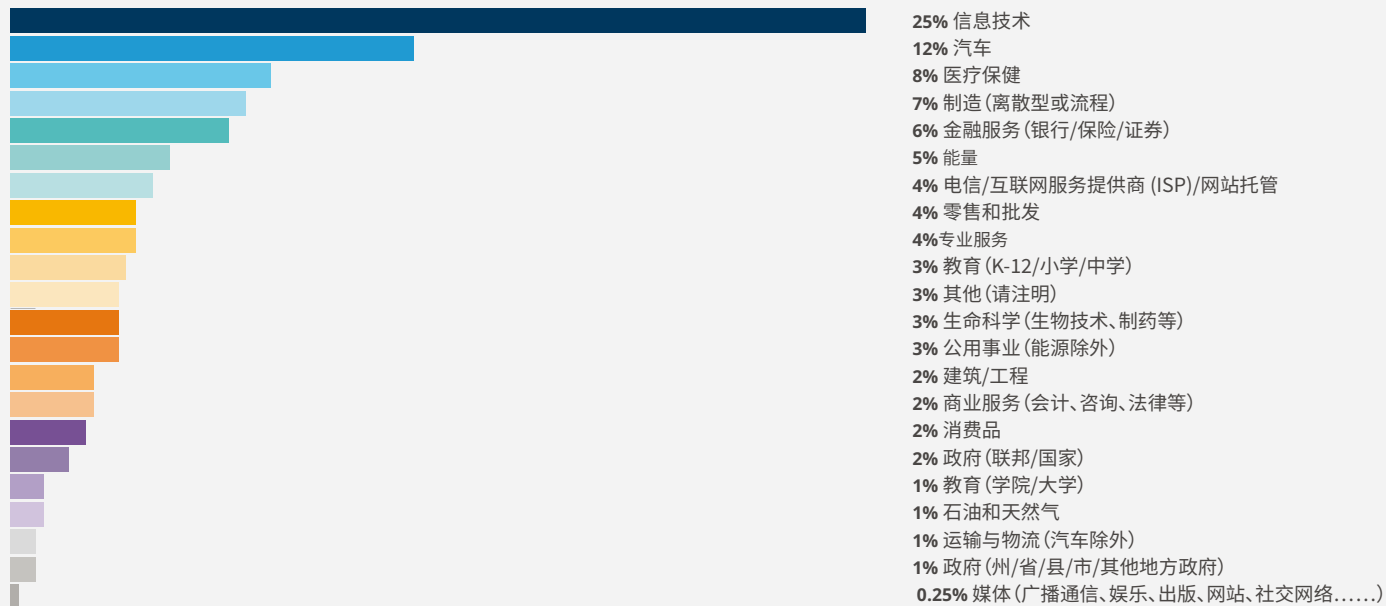
多选 | N = 407, 有效案例 = 407, 总提及次数 = 1227



图A4

贵组织的主要产业是什么？

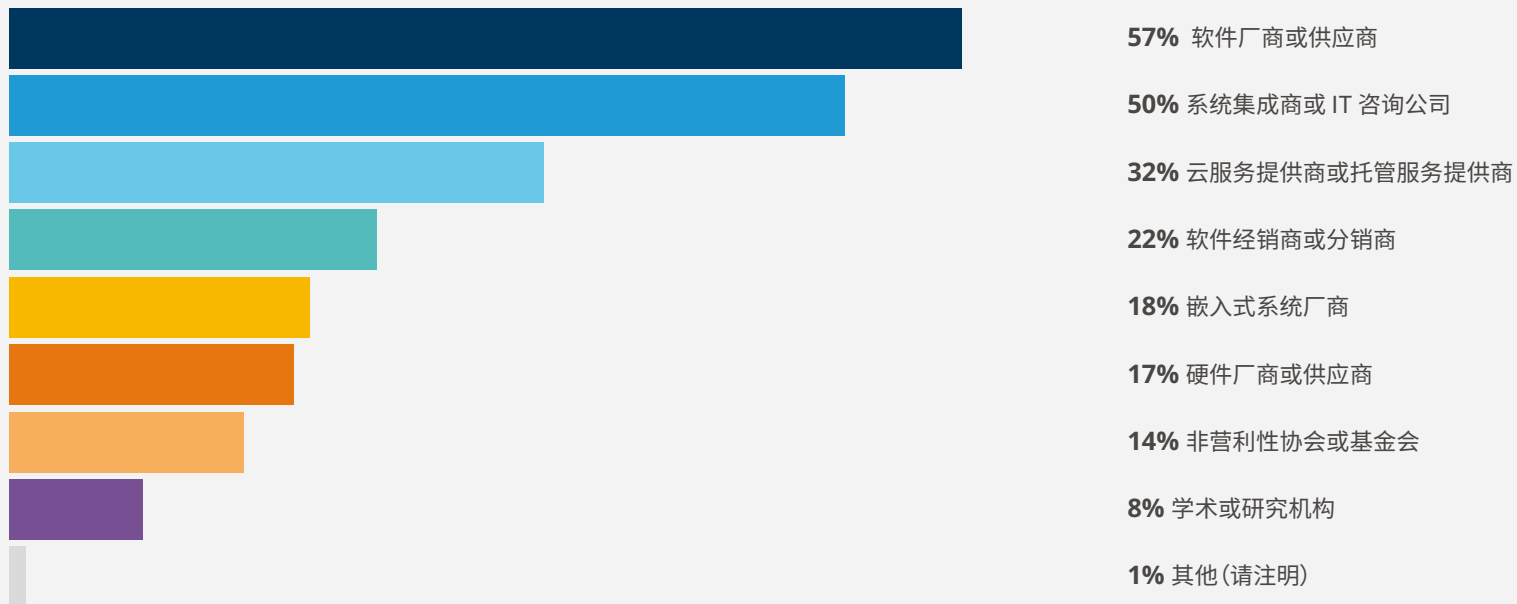
单选 | 样本个数 = 405



图A5

您为哪种类型的信息技术组织工作？

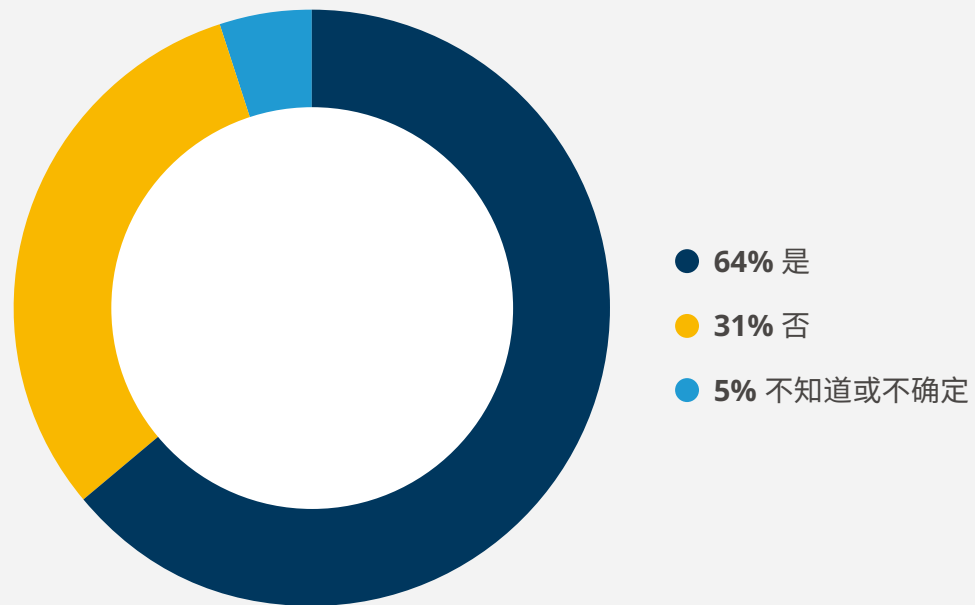
多选 | 样本个数 = 101, 有效案例 = 101, 总提及次数 = 220



图A6

您在 Linux 基金会成员公司工作吗?

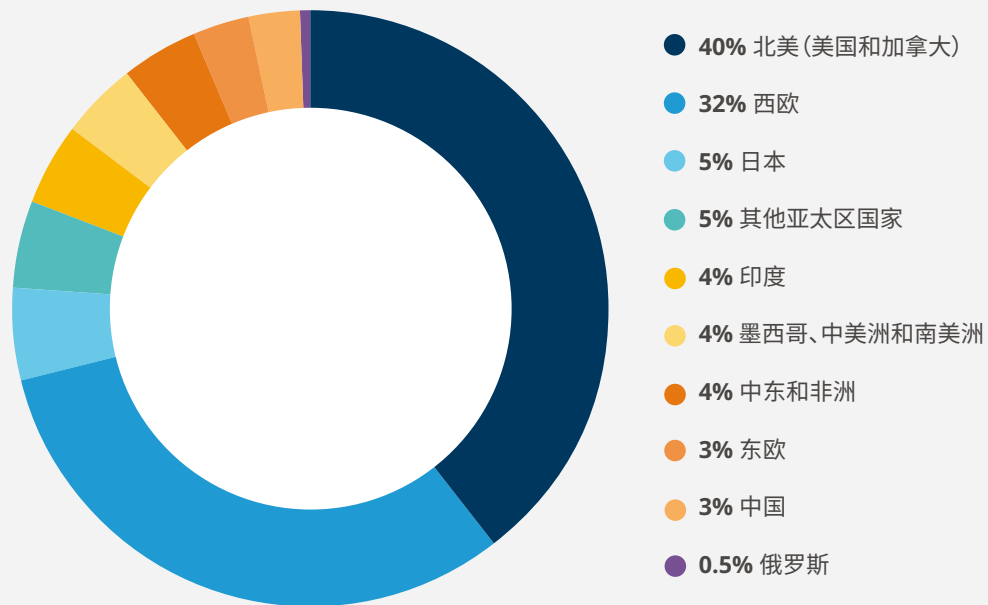
单选 | 样本个数 = 404



图A7

您住在哪个地理区域？

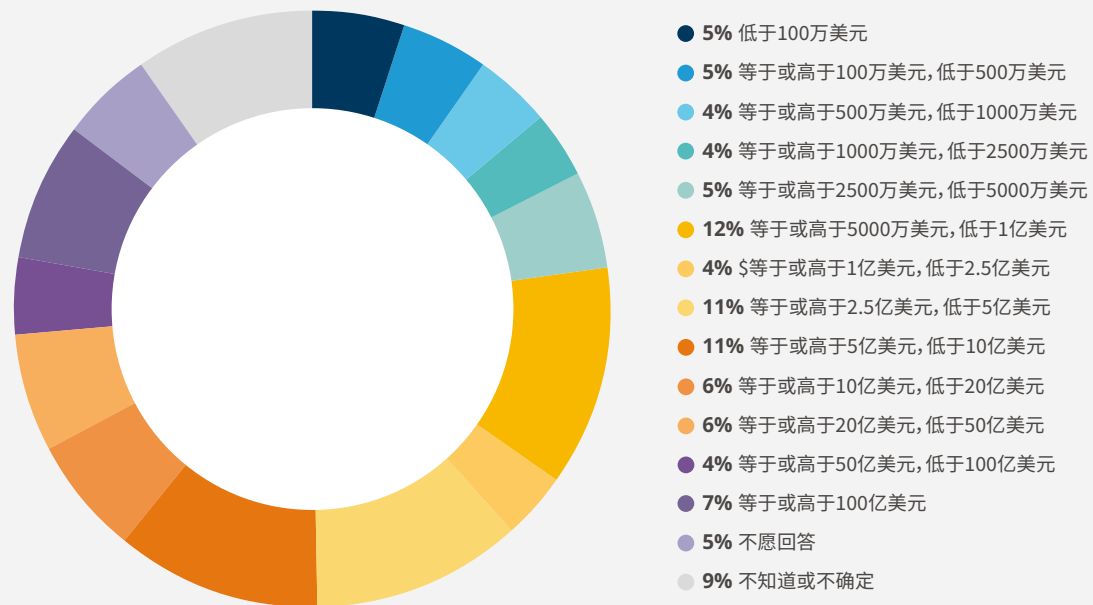
单选 | 样本个数 = 402



图A8

贵组织 2020 年的年收入大约是多少？

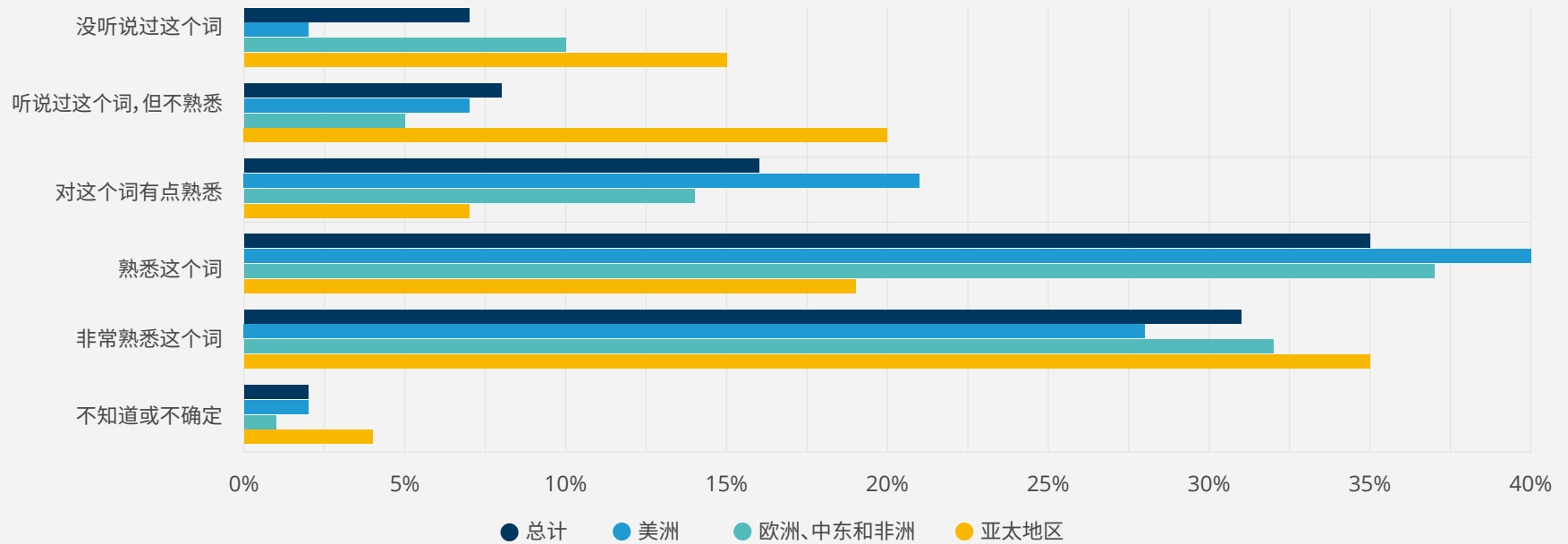
单选 | 样本个数 = 402



图A9

您的组织对软件物料清单 (SBOM) 的熟悉程度如何?

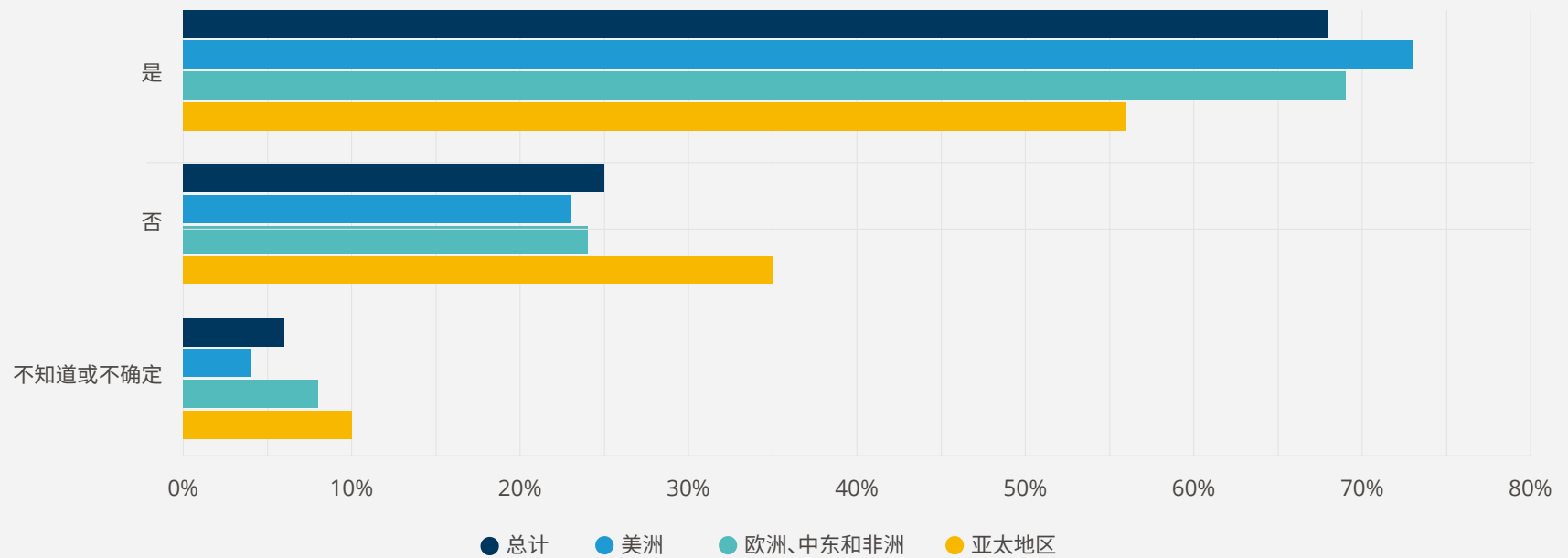
单选 | 按地理区域 | 样本个数 = 361



图A10

您的组织是否有一个开源项目办公室 (OSPO) 来监督开源软件的使用?

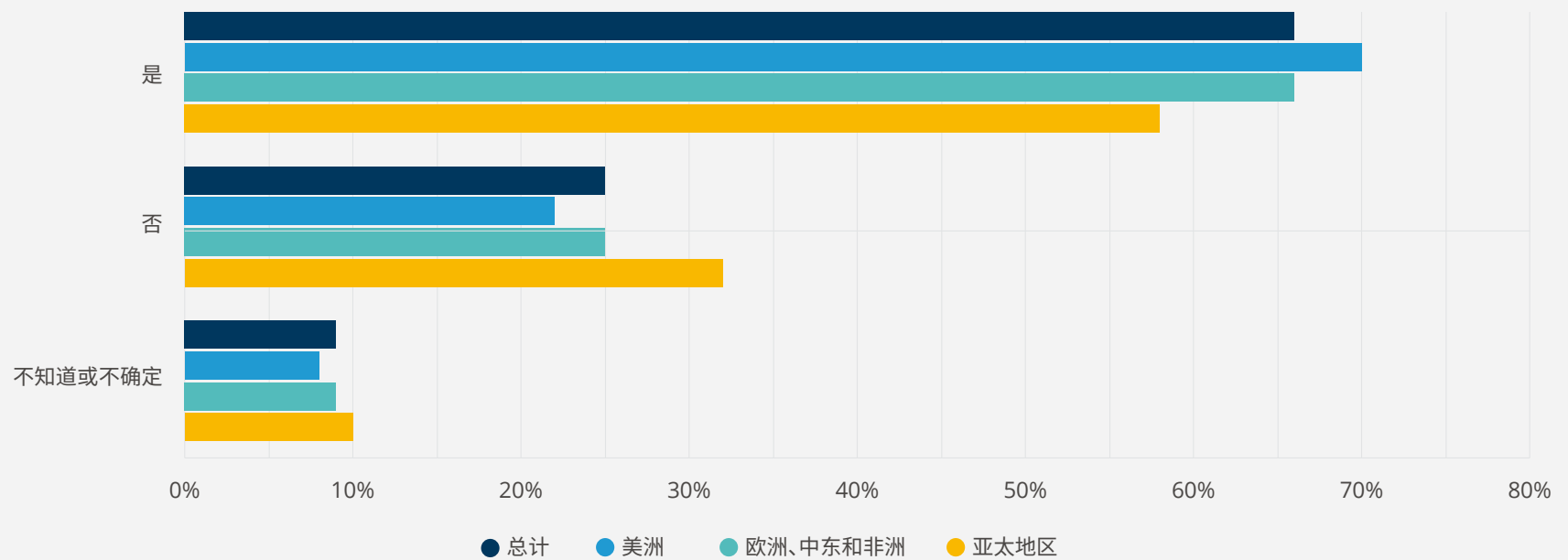
单选 | 按地理区域 | 样本个数 = 390



图A11

您的开源项目办公室是否与您的安全团队共享开源项目清单？

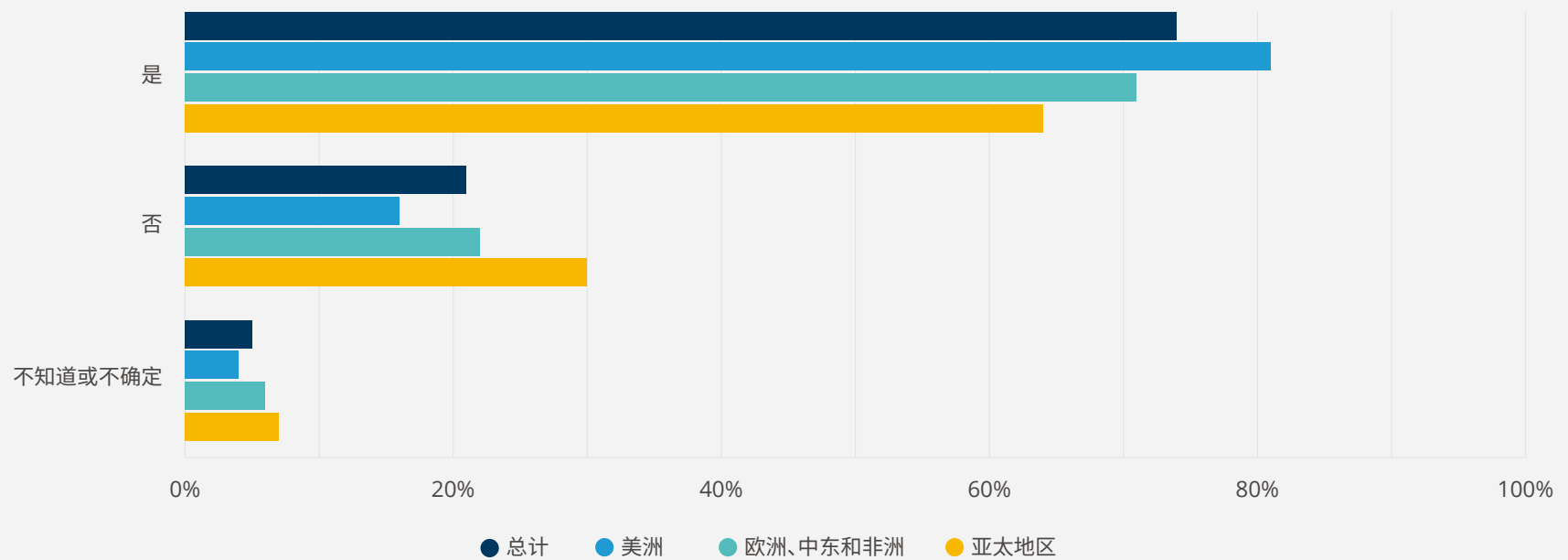
单选 | 按地理区域 | 样本个数 = 384



图A12

您的组织是否有一个首席信息安全官 (CISO)/安全团队来监控上游开源项目的漏洞?

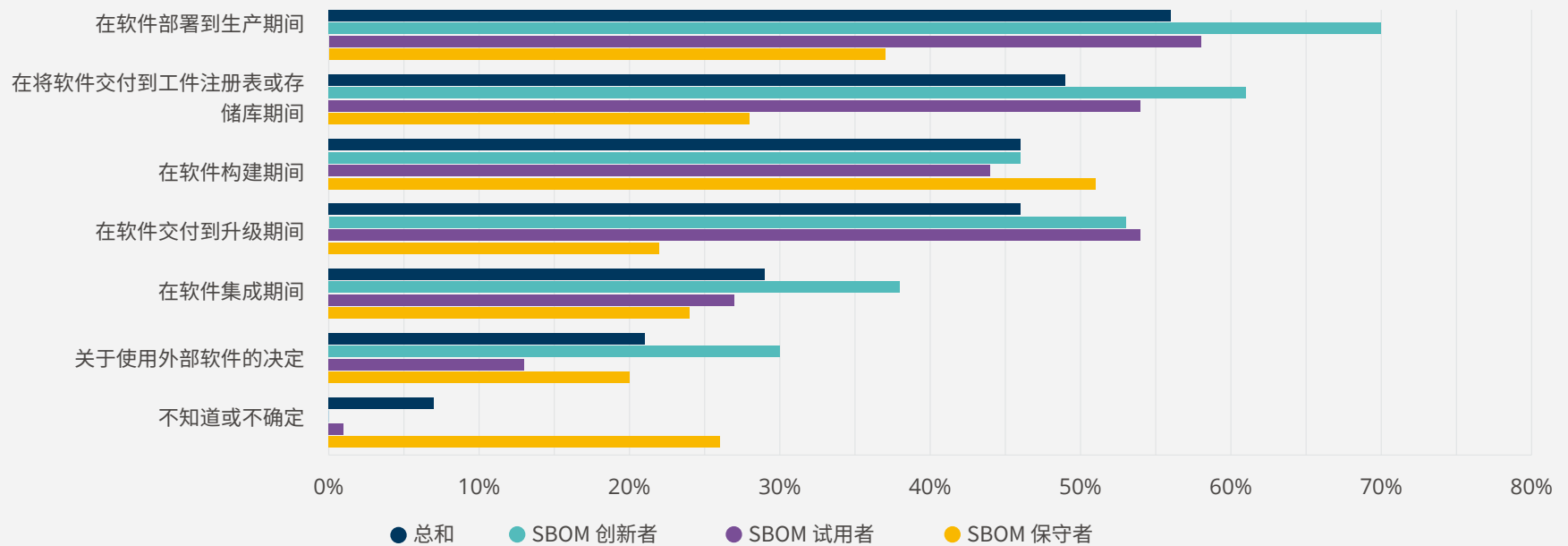
单选 | 按地理区域 | 样本个数 = 388



图A13

您的组织在或将在软件开发生命周期的哪个阶段制作SBOM?

多选 | 按SBOM成熟度 | 样本个数 = 335, 有效案例 = 335, 总提及次数 = 849



图A14

您的组织在或将在软件开发生命周期的哪个阶段使用 SBOM?

多选 | 按SBOM成熟度 | 样本个数 = 325, 有效案例 = 325, 总提及次数 = 896

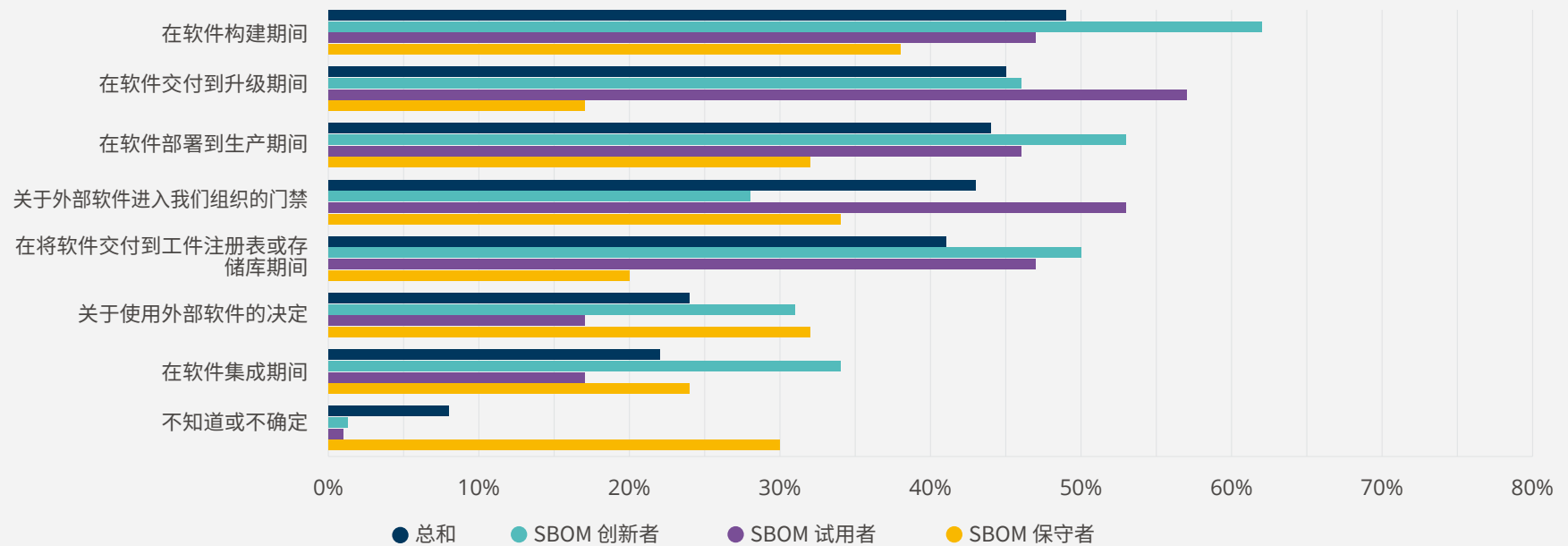
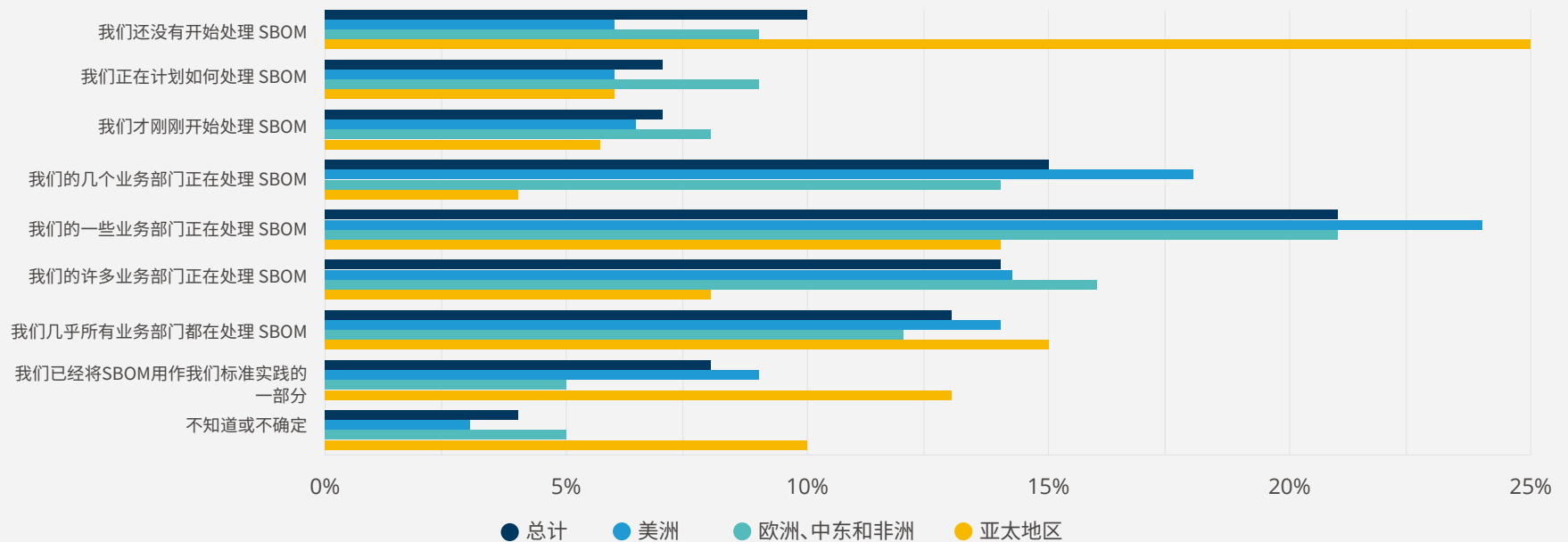


图15

您团队目前的SBOM就绪水平如何？

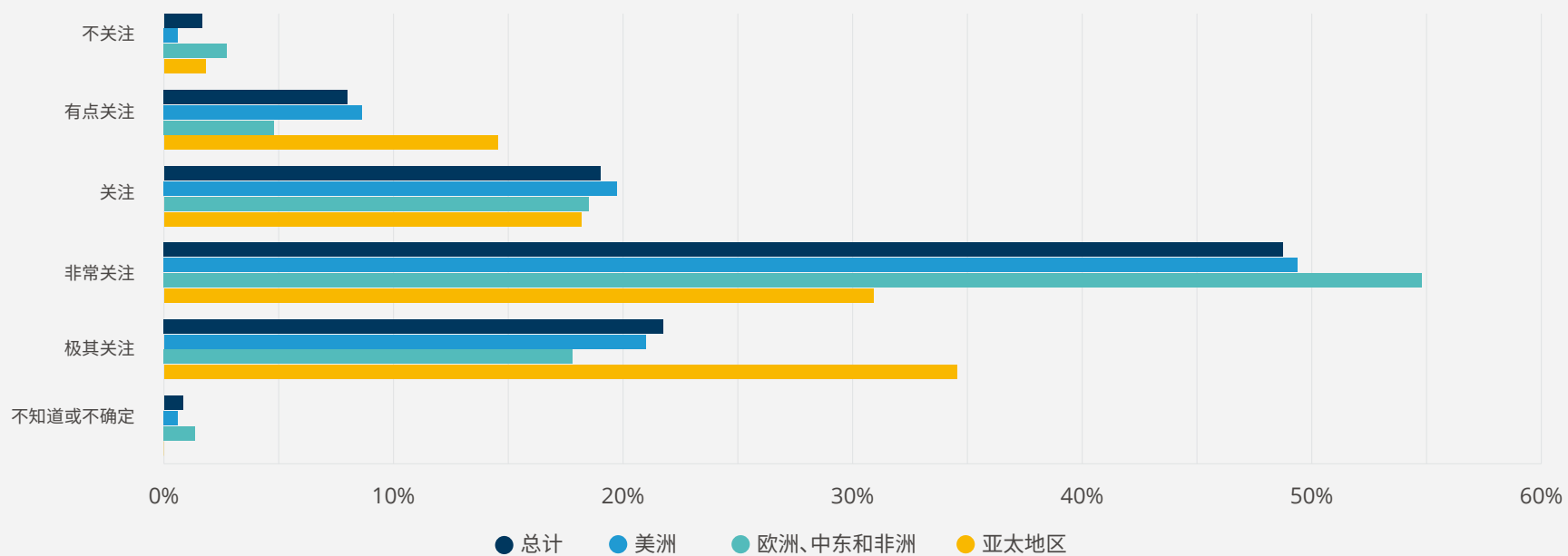
单选 | 按地理区域 | 样本个数 = 357



图A16

对所使用软件的安全性，您组织的关注程度如何？

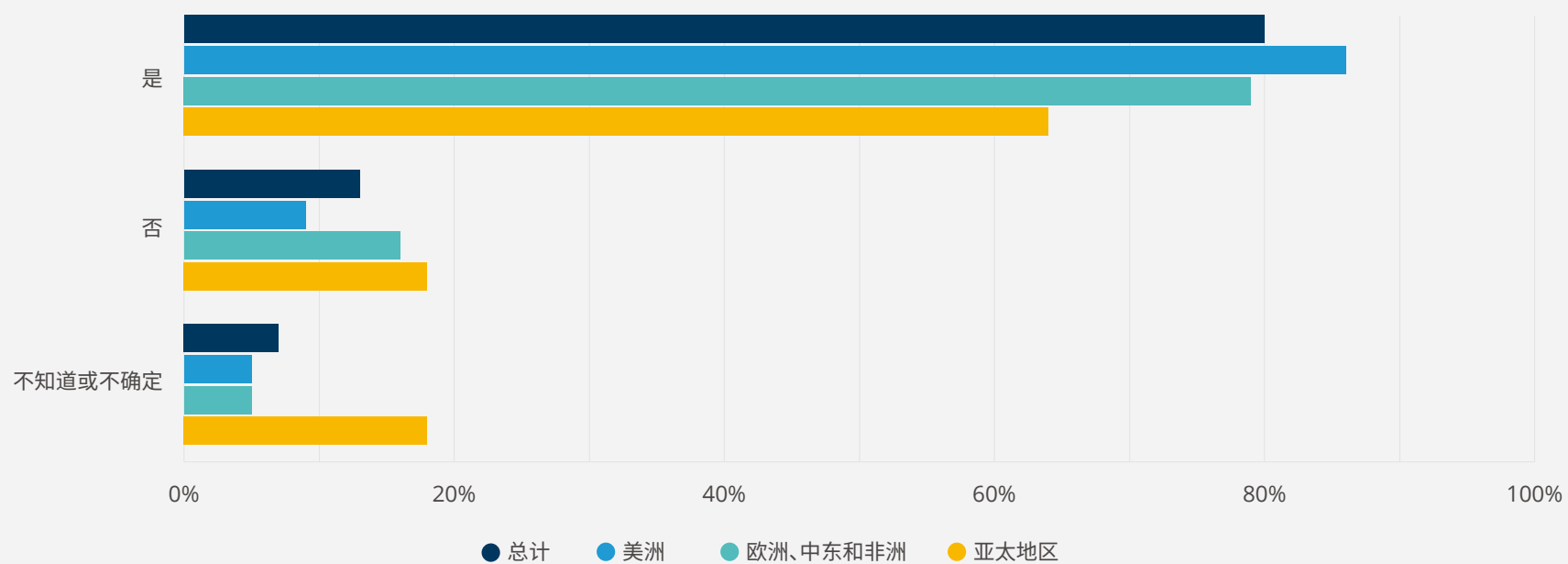
单选 | 按地理区域 | 样本个数 = 363



图A17

您的组织是否知道最近美国关于网络安全的行政命令提到了软件物料清单？

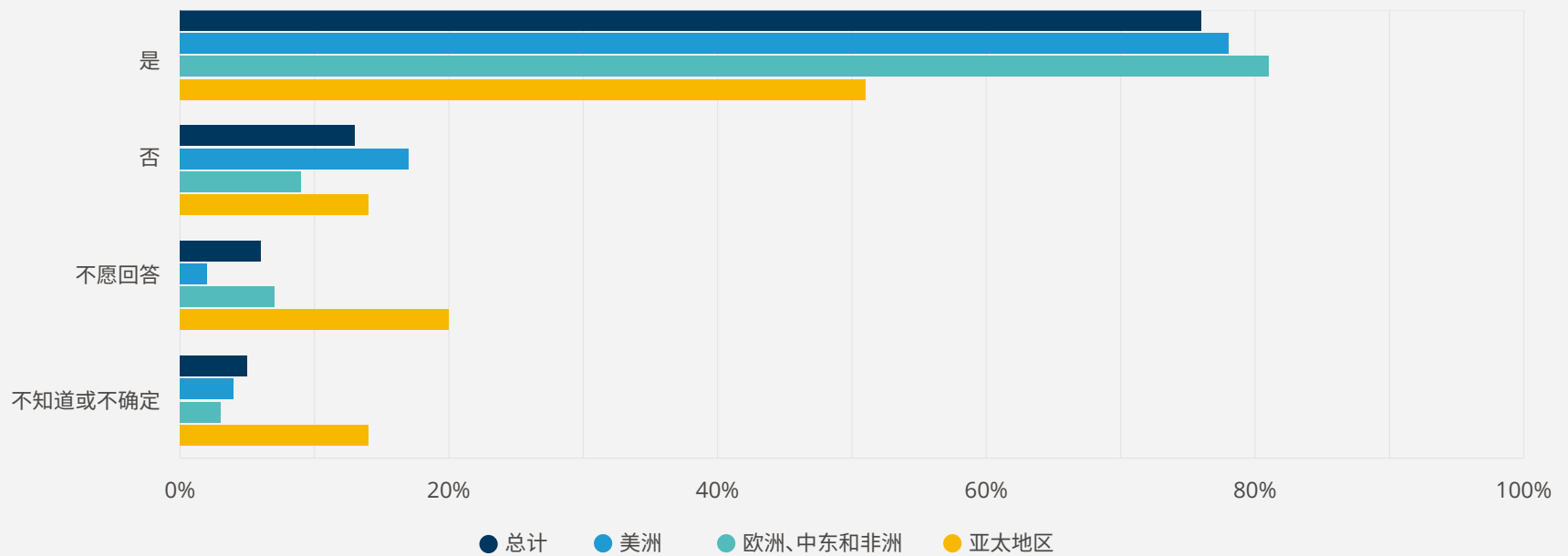
单选 | 按地理区域 | 样本个数 = 362



图A18

贵组织会否响应美国政府提出的网络安全行政命令

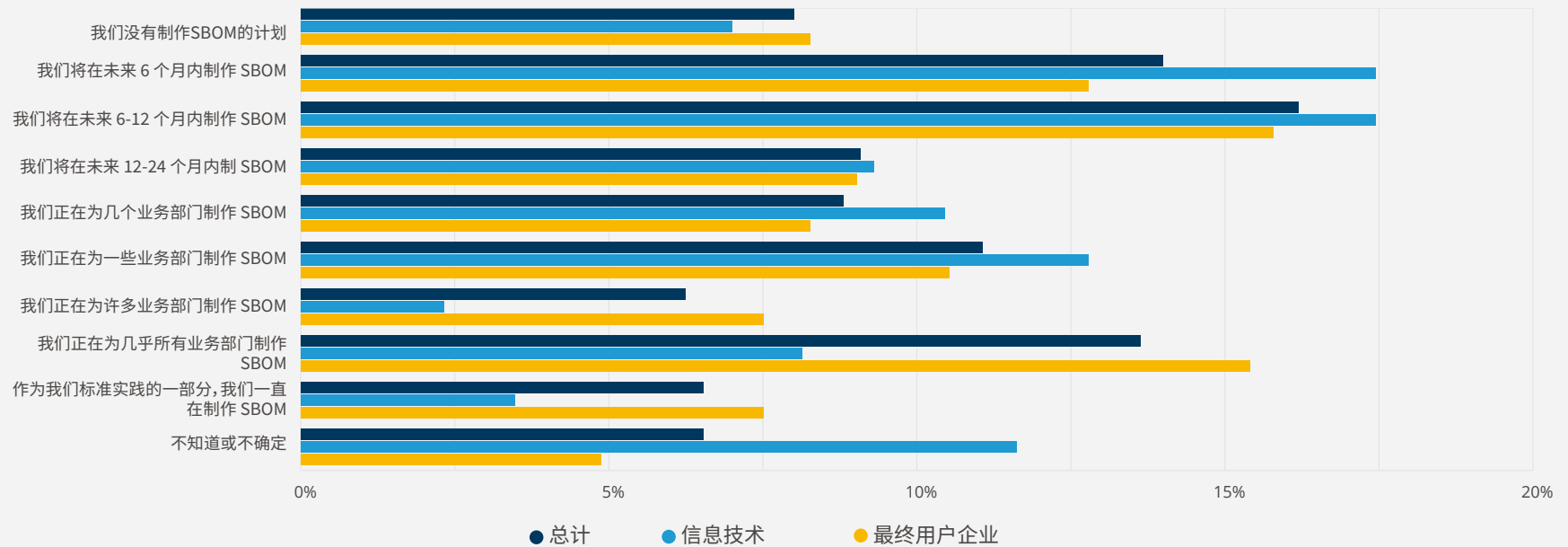
单选 | 按地理区域 | 样本个数 = 290



图A19

贵组织制作SBOM的计划是什么？

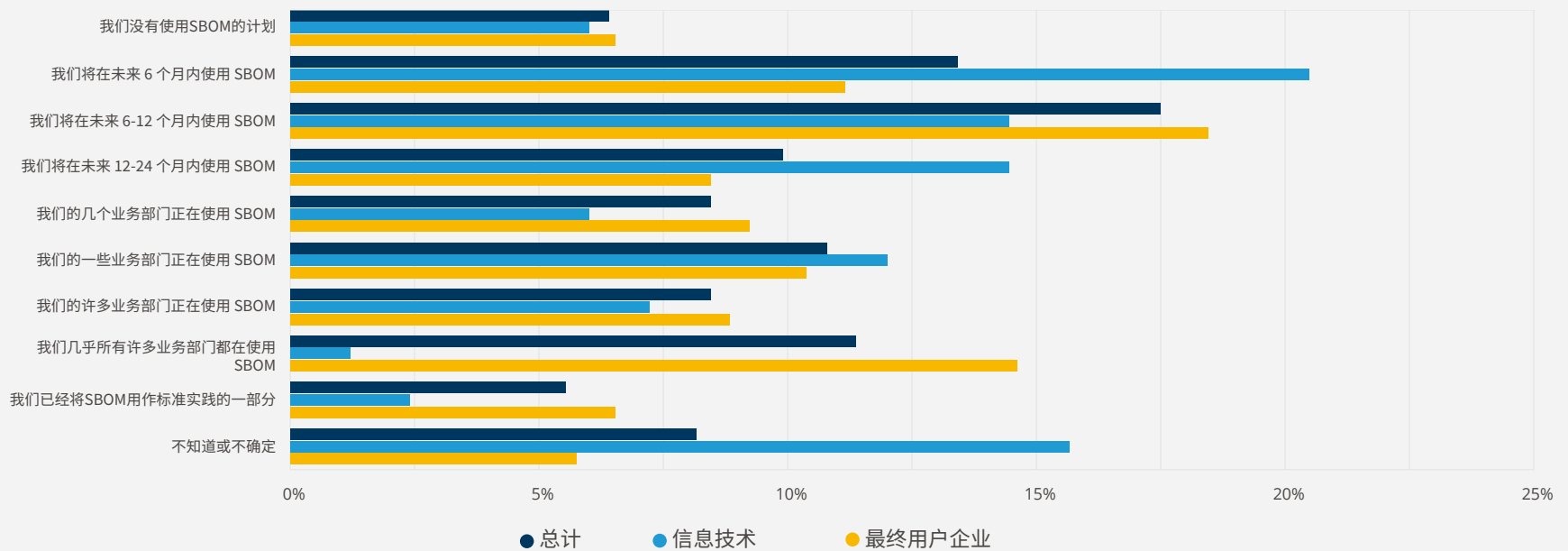
单选 | 按主要产业 | 样本个数 = 352



图A20

贵公司对使用SBOM有什么计划？

单选 | 按主要产业 | 样本个数 = 343





免责声明


本报告是“按原样”提供的。Linux 基金会及其作者、贡献者和赞助者明确表示不提供任何明示、暗示或其它保证，包括与本报告有关的适销性、非侵权性、特定目的适用性或所有权的暗示保证。在任何情况下，Linux 基金会及其作者、贡献者和赞助者都不对任何其他方的利润损失或任何形式的间接、特殊、偶然或后果性的损害负责，这些损害来自与本报告有关的任何类型的诉讼原因，无论是否基于违约、侵权（包括过失）或其他原因，也无论他们是否被告知这种损害的可能性。对本报告创作的赞助并不构成任何赞助商对其结论的认可。


**感谢以下Linux 基金会 APAC 开源布道者翻译 SIG 的成员，
为本软件材料清单（SBOM）与网络安全准备度翻译成简体中文作出了贡献。该团队成员包括：**

- | | |
|--------------------|--|
| 1. 赵振华 | 9. 全继安 |
| 2. 皮冰锋 | 10. 滕召智 |
| 3. 阎书利 | 11. 王伟超 |
| 4. 周冉 | 12. Donald Liu, Linux Foundation APAC |
| 5. 徐斌 | 13. Maggie Cheung, Linux Foundation APAC |
| 6. 马景贺, 极狐(GitLab) | 14. Hin Yang, Linux Foundation APAC |
| 7. 王玉茂, 华为 | 15. Dorothy Cheng, Linux Foundation APAC |
| 8. 王永雷 | |

 twitter.com/linuxfoundation

 facebook.com/TheLinuxFoundation

 linkedin.com/company/the-linux-foundation

 youtube.com/user/TheLinuxFoundation

In partnership with:



成立于 2021 年，Linux 基金会研究院探索规模不断增长的开源协作，提供对新兴技术趋势、最佳实践和开源项目的全球影响的洞察力。



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

[本报告采用知识共享署名-禁止衍生产品 4.0 国际公共许可协议给予许可。](https://creativecommons.org/licenses/by-nd/4.0/)

如需引用该作品，请按以下方式引用：Stephen Hendrick，“软件材料清单（SBOM）与网络安全准备度”，Jim Zemlin作序，2022 年 1 月。