全维度供应链数字化

软件定义未来的网络安全

IBM Microsoft

关于微软与 IBM 的合作伙伴关系

微软和 IBM 建立了战略合作伙伴关系，旨在帮助组织实现全面的企业级威胁管理。我们提供相互协同的安全解决方案，让组织满怀信心地在微软云上加速迁移、现代化和业务转型。

IBM 提供全面的云安全产品组合，包括用于协同和优化安全资源的战略与风险咨询、保护和实现数字信任的解决方案、威胁管理功能的实施和运营，以及利用现有资源推动安全转型的开放式多云解决方案。如需了解更多信息，请访问：https://ibm.biz/msftsecurity

IBM 如何提供帮助

IBM Security® 是值得信赖的合作伙伴，可为您提供融合 AI 的技术和服务，满足不断发展的业务需求。我们的现代化安全战略方法让您能够充分利用数字创新，并在充满不确定性和网络威胁的环境中蓬勃发展。如需了解更多信息，请访问：https://ibm.com/security

摘要

网络风险和供应链风险日趋融合。

- 安全的数字供应链对于保障物理供应链安全至关重要。

  物理操作日益依赖于数字控制。

- 在选择供应商时，高管往往更注重成本，而忽视高成本的风险因素。

  直接和间接供应商通常未将常规的网络风险管理实施到位。

- AI 可以更好地整合网络和供应链运营，从而增强运营韧性。

  组织可以利用先进技术来改善协作并降低供应商风险。

驾驭新风险时代

过去，供应链主要是指物理供应链。而如今，随着数字技术在供应链中的核心作用日益增强，不仅大幅提升了效率，也引入了新的、经常被低估的风险。尽管企业纷纷开始着力增强供应链韧性，但仍有许多企业的供应链网络暴露在网络风险中。

随着暗网网络犯罪市场日趋成熟，网络攻击者在蓬勃发展的“网络犯罪即服务”生态系统中共享资源，这使得恶意人员更容易针对供应链中的薄弱环节发起攻击。[1] 他们通常会针对资源较少、漏洞较多的细分供应商进行攻击。[2] 换句话说，大型供应链网络中的大多数公司都可能成为攻击目标。[3]

数以百计甚至数以千计的第三方直接或间接互联，提供了通向关键系统的无数路径。一项研究表明，在过去两年中，98% 的受访组织至少有一家供应商遭遇过数据泄露。[4] 另一项研究表明，来自业务合作伙伴的数据泄露成本要比其他类型的数据泄露高出近 12%。[5]

为了深入理解网络安全因素如何影响价值链、供应链和生态系统的发展，IBM 商业价值研究院 (IBM IBV) 与微软合作，针对全球各行业的 2,000 名安全和运营主管开展了一项调研（请参阅第 26 页的“研究和分析方法”）。调研结果表明，高管对供应商风险和网络漏洞的认识令人担忧。尽管 74% 的受访者表示供应链韧性对于其组织的成功至关重要，但只有 40% 的受访者认为生态系统正在扩大网络攻击面。而且，只有不到三分之一的受访组织正在通过优先的投资计划来建立安全、互联的供应链运营生态系统。

一部分组织认为网络风险与供应链风险的管理是相互依存的，这部分组织遭遇的供应链中断明显减少。

根据 IBM 商业价值研究院的调研，一部分组织认为网络风险与供应链风险的管理是相互依存的，而这部分组织遭遇的供应链中断明显较少。然而，由于分散的决策和薄弱的网络安全实践加剧了负面因素，许多组织都难以洞悉潜在威胁及其对运营的影响。

本报告探讨了在调研中发现的三项关键网络风险管理挑战。针对每一项挑战，我们提出了相应的机遇，即如何通过克服挑战来增强供应链韧性。每个部分还附有简明的行动方案，企业高管可以采取这些具体步骤，更有效地在其组织和生态系统中整合网络风险和供应链风险管理。

观点

首要问题：什么是“供应链”？[6]

供应链是指产品开发和销售流程中的相关个人、组织、资源、活动和技术 /IT 系统组成的网络。供应链涵盖从供应商向制造商供应原材料到产品最终交付给最终用户的整个过程。

软件供应链则涵盖软件开发生命周期中接触代码的所有要素和所有人员，包括组件相关信息（如基础架构、硬件、操作系统、云服务）、代码编写人员以及代码的来源，如注册表、GitHub 存储库、代码库或其他开源项目。其中还包括可能对软件安全产生负面影响的任何漏洞。

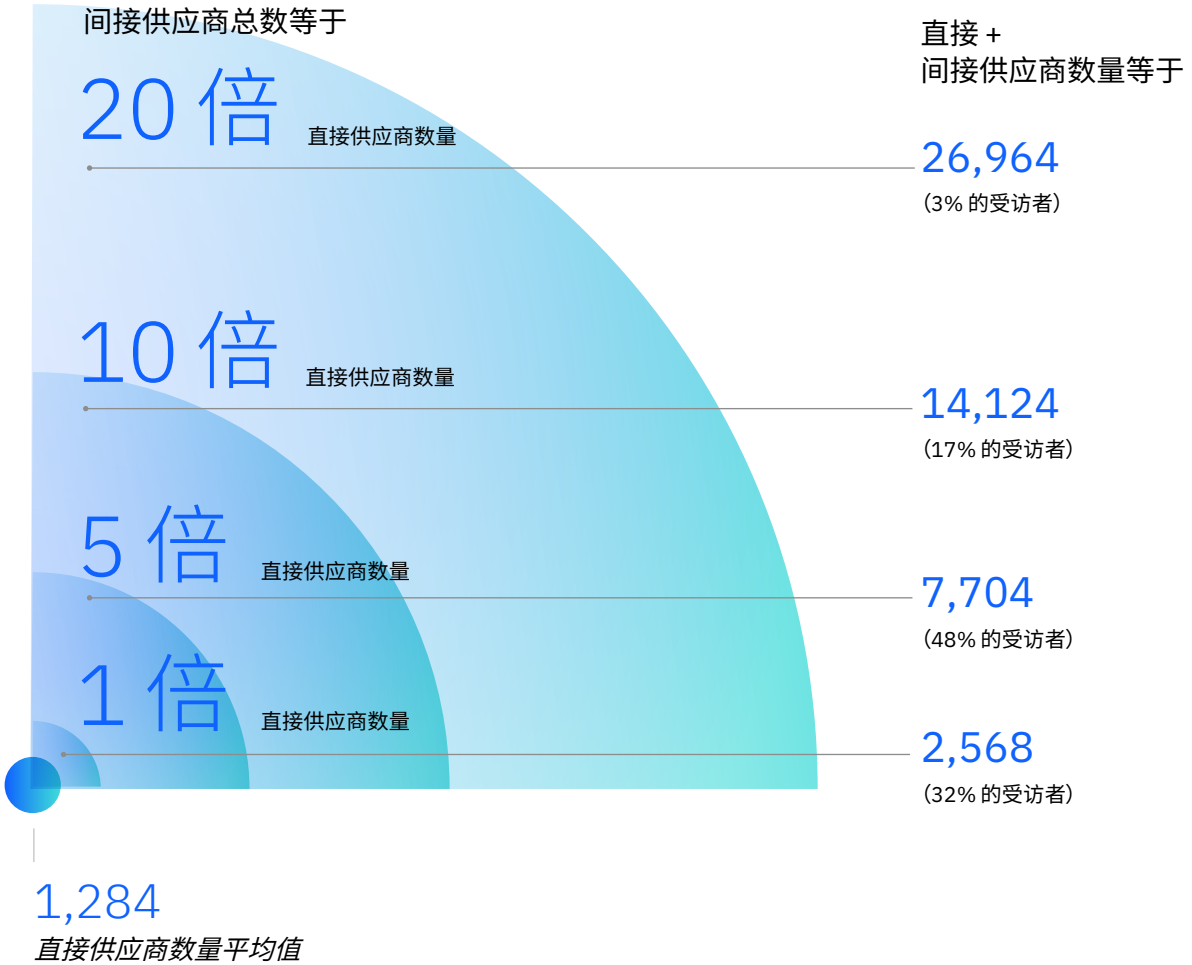
挑战一：
规模庞大

数字供应链运营和风险迅速激增

供应商网络正在迅速扩展。本调研表明，受访组织拥有庞大的直接和间接供应商网络。根据所有行业受访高管的数据，每家组织平均拥有 1,284 家直接供应商。而如果计入间接供应商，则第三方供应商数量会大幅增加（见图 1）。近一半 (48%) 的受访者估计，间接供应商数量是直接供应商数量的五倍，即 6,420 家。这些直接和间接供应商共同构成了一个庞大的攻击面 — 相当于至少有 7,700 个潜在威胁向量可能进入组织。

图 1

不断扩大的供应商网络带来了庞大的攻击面，为入侵关键基础架构和运营提供了许多切入点。



问：有多少直接供应商为贵组织的关键供应链提供支持？
问：估计有多少间接（第 n 方）供应商为贵组织的直接供应商提供支持？

供应商网络如此庞大，使得组织预测潜在中断变得非常困难，甚至不可能，更不用说协同有效的应对措施了。这将对运营产生巨大的影响。与供应商数量最少的组织相比，供应商数量最多的组织遇到的严重运营影响事件要多出17%。这项分析考虑了多项因素的影响，包括网络事件、人才和原材料短缺以及极端天气事件（参见第20页的分析）。

事实上，在高度互联的供应链环境中，网络事件往往会成为引发严重中断的导火索。尽管本调研表明，受访者并未遭受过通过供应商发起的大规模网络攻击，但30%的受访者表示在过去三年中因第三方漏洞而遭受过攻击。最近的一份报告表明，这一问题正变得日益普遍：41%的受访组织表示遭受过由第三方导致的重大网络事件。[7]

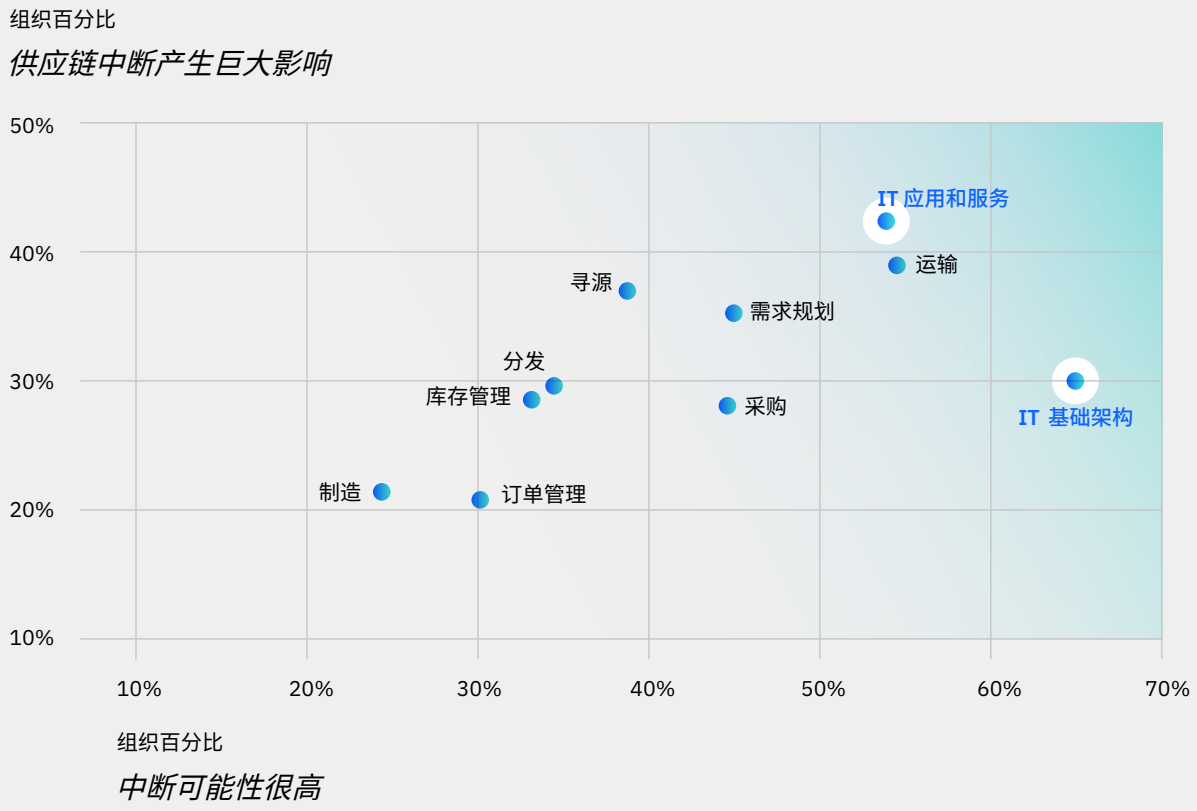
这一现状给供应链应用和服务的安全性带来了巨大的压力。在过去三年中，针对各行业受访者调研的主要发现包括：

- 近40%的受访者表示其组织遭遇过需要采取非常措施来应对的网络安全事件，或对运营产生持久而实质性影响的网络安全事件。
- 超过一半(52%)的受访者表示其组织的供应链IT应用和服务曾遭遇重大或严重中断。
- 与其他职能领域相比，IT应用和服务中断对运营产生的影响更为显著。

展望未来，65%的受访者认为供应链中断可能发生在组织的IT基础架构中，另有53%的受访者认为供应链中断可能发生在组织的IT应用和服务中（见图2）。

图2

IT相关职能是供应链中断最有可能发生且受影响最严重的领域。



问：供应链中断最有可能发生在哪里？回答“可能”和“极有可能”的受访者百分比。

问：哪些职能领域最容易受到供应链中断的影响？回答“影响中等”和“影响重大”的受访者百分比。

机遇：利用“安全设计”方法增强网络和供应链韧性。

鉴于广泛的业务合作伙伴关系，组织需要采用一种新方法来保障供应链安全，即认识到内部和外部 IT 平台与服务之间的共同功能。许多供应链输入和输出都是使用通用基础架构来实现和交付的，这为组织带来了优势。如果将网络风险和供应链风险管理视为相互关联的关系，则这两个维度的能力都会变得更加强大。

这就像是一种 DNA 双螺旋结构，网络韧性和供应链韧性会相互增强。两者凝聚为一股合力，可改善效率、协同和价值创造；但同时也代表了两种相互依赖且并行发展的能力。提高可视性和治理能力对于组织内部，乃至整个供应链和合作伙伴生态系统都至关重要。

从更实际的层面来说，这种程度的整合是什么样的？这是一种贯穿整个供应链的文化，从初始设计、采购材料、供应商、分销到产品生命周期结束，网络风险管理、安全和韧性均处于重要地位。作为第一步，供应链和风险管理领导者可以效仿软件和硬件开发社区的做法，采用“安全设计”原则，也称为“左移”。

这种方法将安全置于决策的最前沿，而不是事后再“亡羊补牢”。[8] 通过将“安全设计”应用于供应链的每一个阶段，可推动运营各方优先加强网络风险管理和协同治理实践。这有助于促进各职能部门以及整个合作伙伴生态系统的协作。这带来了诸多优势，例如能够尽早发现潜在漏洞、分享最佳实践，以及有助于协同应对威胁（参见第 8 页的案例研究：“汽车制造商采用全新的安全优先思维”）。

网络风险管理

供应链风险管理

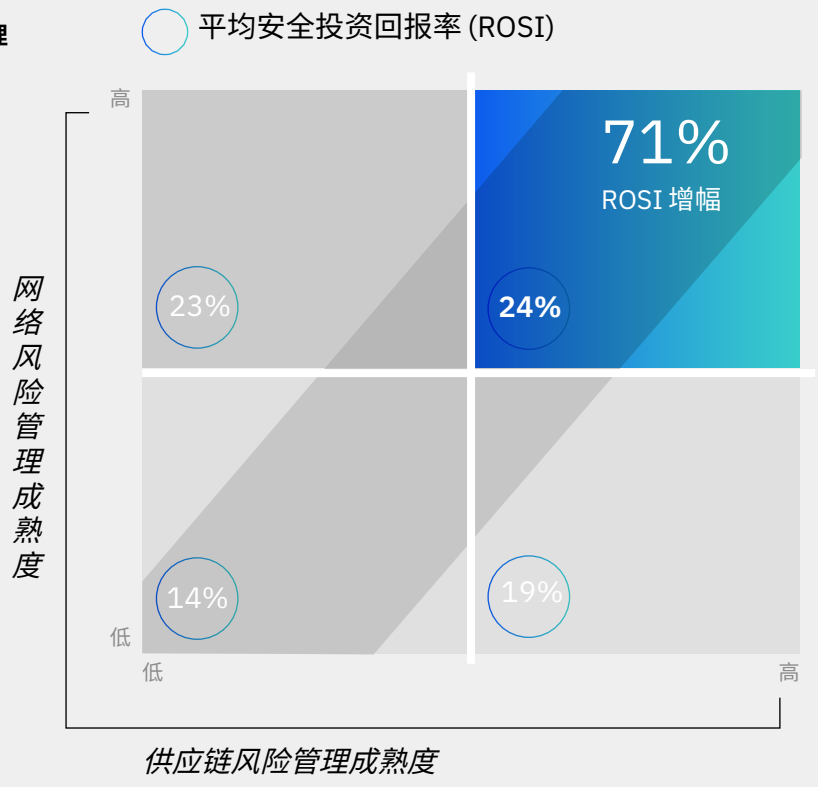
这种方法有助于改善运营和业务成效。根据 IBM 商业价值研究院的分析，在网络风险和供应链风险管理领域具有更高成熟度的组织实现了更出众的安全投资回报率（见图 3）。这两个维度的成熟度相互强化。与表示受到类似网络安全事件严重影响的其他组织相比，此类组织在过去三年中遭遇的网络事件要少 89%。

行动：采用“安全设计”方法优先增强供应链运营的安全性。

1. 组建一个跨职能的供应链风险管理团队，包括 IT、OT 和产品安全专家，负责审查当前的供应链流程和系统。
2. 编写一份供应商名单，并按关键性和风险暴露进行细分。安排团队识别所有潜在的薄弱环节，涵盖从供应商采购、物流到软件分销渠道的整个周期。
3. 然后，让团队合作设计和整合安全控制措施，以缓解已识别的风险。

图 3

更成功地整合网络风险和供应链风险管理的组织实现了更高的安全投资回报率。



基于 IBM IBV 分析。

案例研究

汽车制造商采用全新的安全优先思维[9]

随着汽车日益依赖于软件，网络安全对于保障汽车安全至关重要。现代汽车包含超过 1.5 亿行代码，自然也就增加了网络攻击的几率。为了应对这些威胁，各种新的法规不断出台，包括联合国欧洲经济委员会 (UNECE) 发布的 WP.29 法规和 ISO/SAE 21434 标准，旨在管理整个产品生命周期中的软件网络安全风险。[10]

一家全球汽车制造商意识到，要实现全面电动化和拓展智能互联汽车用户群的宏大目标，网络安全将发挥至关重要的作用。该公司还发现加速提高网络安全成熟度已势在必行——针对关键 IT 资产样本的风险量化评估表明，预计年损失超过 10 亿美元，这一惊人的金额可能会威胁到未来的运营和品牌形象。

基于对 Microsoft Azure 基础架构和服务的长期投资，该公司与 IBM 合作开启了重塑网络安全性旅程——从手动、被动的安全态势转变为主动预测可能发生的事件。

该流程采用一种全面的“安全设计”方法，在整个运营流程中嵌入安全功能并整合安全控制，从制造 /OT 和企业 /IT，到合理化互联产品供应商，再到企业的招聘和培训实践。对于这家 OEM 来说，这相当于一种全新的思维方式。该公司不是在安全漏洞出现后才去修补，而是将安全作为连接车队与后端服务、供应商生态系统与工厂车间的基本要素，包括为其代码库做出贡献的软件供应商。[11]转型路线图预计会在未来三年内将风险减少一半。

全面的“安全设计”方法在整个运营流程中嵌入安全功能和控制——从制造 /OT 和企业 /IT，到合理化互联产品供应商，再到员工招聘和培训实践。

挑战二：
管理分散

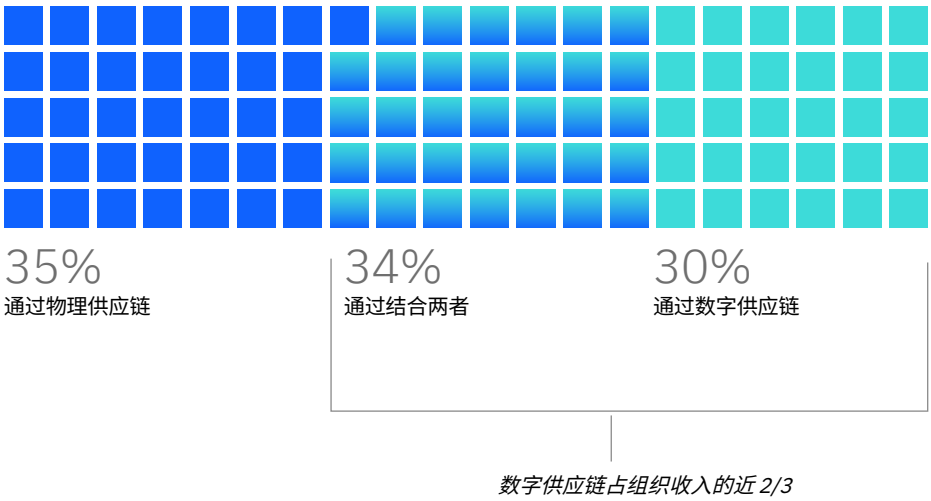
分散管理网络风险和供应链风险的后果

大多数组织的风险管理都处于一种各自为战的分散状态。不过，重大风险通常具有跨职能的性质，因此不会遵循组织边界，尤其是管理物理和数字供应链的组织边界。尽管物理供应链和数字供应链都对收入有巨大的贡献（见图 4），但组织缺乏将两者风险责任联系在一起的整体视图。70% 的受访高管表示，物理风险和网络风险由组织的不同部门管理，因此可能会忽视或低估物理和数字威胁向量的共同风险。

图 4

供应链大部分已经实现数字化。

组织收入百分比



问：估计贵组织的收入通过以下方式实现和达成的比例：通过物理供应链、通过数字供应链以及通过两者的组合。2023 年。由于四舍五入，百分比总数不等于 100%。

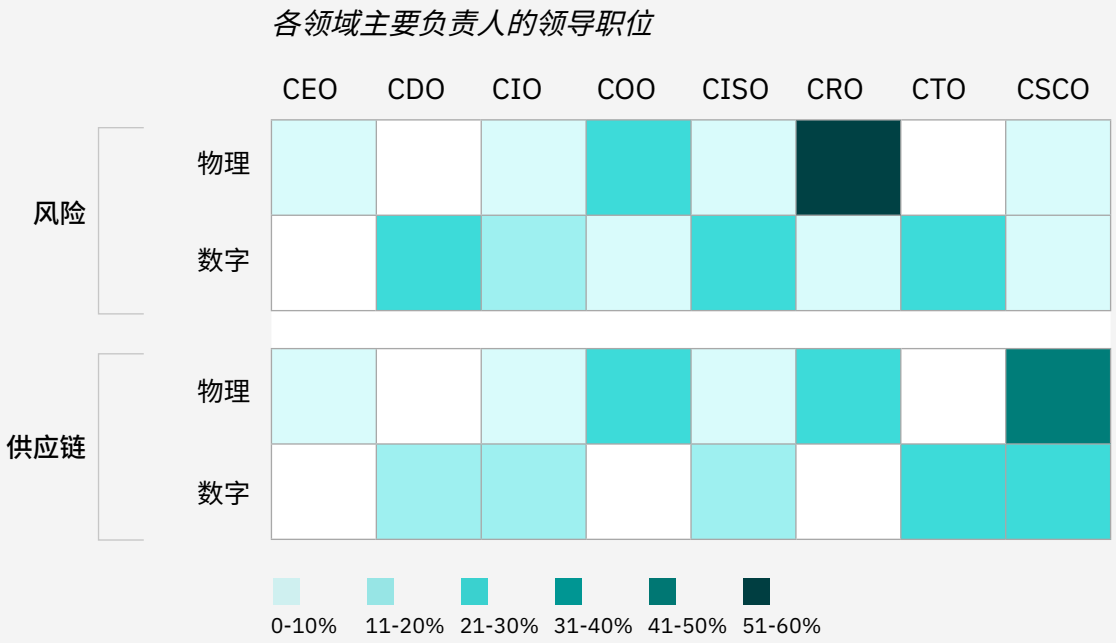
从更具体的层面来看，物理和数字风险以及整个物理和数字供应链的负责人员是谁？根据 IBM 商业价值研究院的调研，这些职责分散在高管团队中（见图 5）。并没有一位高管能够全面掌控所有潜在风险。职位名称可能因公司规模和组织结构而异，但如果风险管理和供应链运营由传统职能部门来组织，则整个企业的协同就会很困难。对于难以与生态合作伙伴保持同步的组织来说，这是一项更为严峻的挑战。对于许多组织来说，不同部门之间往往缺乏沟通 — 这为安全和供应链领导者带来了一项重大挑战。

机遇：利用 AI 和自动化改善内部可视性和协同能力，从而推动外部成效。

通过适当的治理，数字价值链可以提高可见性并推动有效协同，从而超越组织内的职能边界并增强整个供应商体系的能力。依托于云服务、物联网和 AI 等技术，互联互通的供应商体系可促进实时通信、协作、治理和数据共享。这些关键能力将推动整个供应链和生态系统合作伙伴进行有效协同，从而大幅提升生产效率和规模。

图 5

风险和供应链职责分散在高管团队中，因此难以建立涵盖物理和数字领域的整体视图。

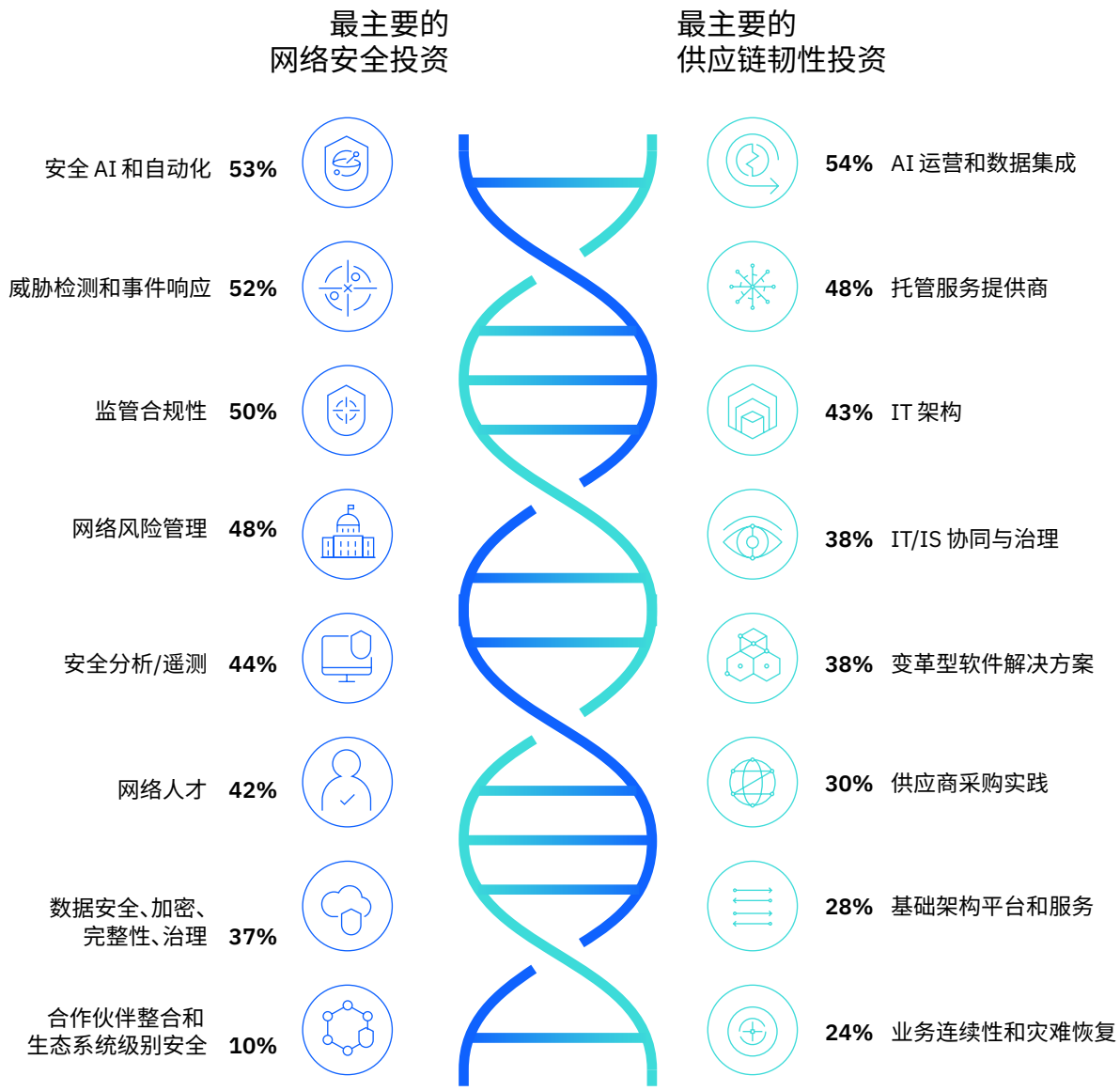


问：请指出负责物理风险、数字风险、物理供应链、数字供应链的最高级管理人员。

大多数 (84%) 受访组织表示在构建安全互联生态系统方面进行了中等程度到重大程度的投资；事实上，这些组织侧重于利用先进技术来改善供应链和网络防御能力（见图 6）。在增强供应链韧性的安全和运营投资中，AI 位于优先级列表的榜首（请参阅第 15 页的“观点：生成式 AI 助力保障生态系统安全”）。

图 6

企业高管正在优先采用先进技术来增强运营韧性，从而改善协作。



问：贵组织在增强供应链韧性方面最优先的网络投资是什么？

问：贵组织在增强供应链韧性方面最优先的投资是什么？

超过一半 (54%) 的受访组织表示正在运营中利用 AI 和数据集成，从而提高整个供应链的效率、可预测性和响应能力。受访高管还表示正在专注于构建更加现代化、可扩展且可靠的 IT 基础架构，相关的投资包括托管服务提供商 (48%) 和 IT 架构 (43%)。云平台构建于标准设计模式和通用治理框架之上，因此有助于增强洞察、协作和自动化。

在网络安全投资方面，安全 AI 和自动化 (53%) 位居第一，其次是威胁检测和事件响应 (52%)。借助 AI 赋能的自动化，组织可以建立更具预防性和主动性的安全态势，同时改善洞察力、生产力和规模经济。[12] 而 AI 赋能的运营则有助于推动建设安全运营中心 (SOC)，并借助合作伙伴逐渐实现虚拟安全运营中心。

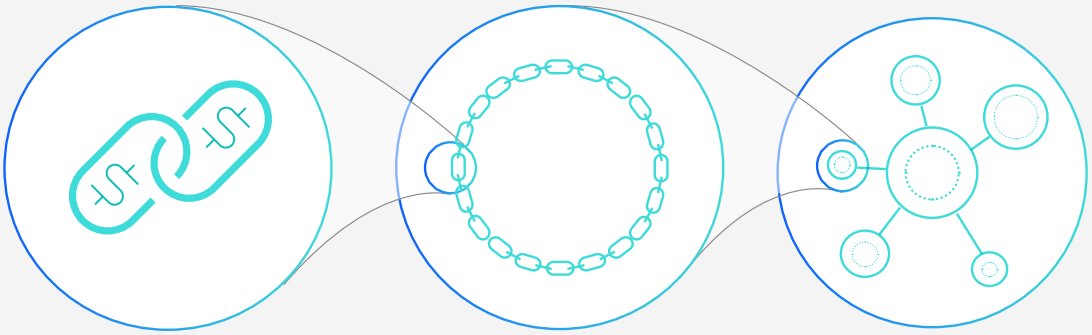
现代运营模式的真正考验在于如何无缝扩展能力，以覆盖整个供应商体系并延伸到生态系统环境中。

但组织需要更多地关注更新其运营治理和支持实践，而不仅仅是投资新技术。现代运营模式的真正考验在于如何无缝扩展能力，以覆盖整个供应商体系并延伸到生态系统环境中。[13] 运用责任共担模式来管理供应链安全有助于每个供应链参与者为维护整体安全态势的完整性和安全性做出贡献——从价值链、供应链到合作伙伴生态系统（见图 7）。这样一来，供应商体系就成为了更强韧性的来源，而不是更大的风险。

企业领导者正朝着这个方向砥砺前行：58% 的受访高管认为价值链、供应链和生态系统是相互关联的。受访者还认识到让合作伙伴参与风险管理的重要性：70% 的受访高管表示，通过将合作伙伴整合到自身的风险和治理模型中，其组织增强了供应链韧性。

图 7

价值链、供应链和生态系统正在并行发展。



	价值链	+ 供应链	+ 生态系统
规模	x1	x10	x100
重点	价值创造和效率	协同和履行	扩展能力和编排
输入 / 输出	已知且通常不变	高容量、专用、定制	动态；可按需扩展
直接	线性；通过有序组织来最大化增值活动	单向；供应商向客户提供产品或服务	多向；标准化模式和治理意味着中间方可以增加价值
设计	独立但模块化	单边；一方对一方，通常通过中间方	多边；针对复杂的供应商关系进行优化
方向	速度、消除摩擦和浪费	容量和韧性	通过标准和治理来改进效率和态势管理
风险	遏制和缓解风险以防止破坏价值	转移风险；供应商承担不确定性，但买方承担影响	风险共担；尽可能分散不确定性和影响

行动：加强组织内部以及与供应商共同承担供应链安全责任的模式。

1. 召集高管团队共同明确期望，并分配资源来支持改进跨职能协作，从而增强供应链韧性。定义标准并设定协同、沟通和治理的期望。
2. 组建团队并指定流程负责人来调查在组织内和重要供应商中如何处理安全责任。定义标准、政策和相关控制措施来维持强大的安全态势，详细明确利益相关者、流程负责人、供应商和合作伙伴的期望。确定应如何管理这些职责，以及如何将疏忽转变为改进的来源。
3. 创建所有直接供应商的清单，并列出对内部和外部系统、服务和数据存储的访问权限。要求重要供应商为其直接供应商（您的第 n 方供应商）创建类似的依赖关系图。
4. 当部署新的供应商平台时，利用投标和采购流程来改进整个供应商体系的可见性、可追溯性和网络治理实践。

通过应用责任共担模式来管理供应链安全，供应商就成为了更强韧性的来源，而不是更大的风险。

观点

生成式 AI 助力保障生态系统安全

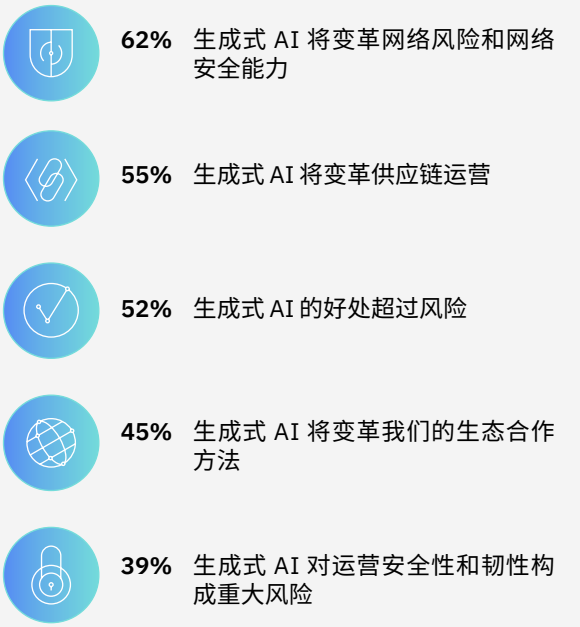
根据 IBM 商业价值研究院近期的一项调研，96% 的受访美国高管表示，采用生成式 AI 可能会在未来三年内导致其组织出现安全漏洞。[14] 而这次最新调研的受访者则表现得更乐观。只有 39% 的受访者预计生成式 AI 会对其运营安全性和韧性构成重大风险，而 52% 的受访者认为生成式 AI 的好处将超过任何潜在风险（见图）。这项技术为网络犯罪分子提供了新的工具，同时也能为防御者提供更高级的功能来检测和应对攻击。[15]

作为整体安全战略的一部分，生成式 AI 可以在增强供应链韧性方面发挥重要作用，包括加快供应商评估和管理实践、支持协同事件响应的模拟和规划、自动执行日常任务以减轻人为错误的影响，以及为供应链系统提供实时监控，以便及时发出安全问题警报。随着能力日趋成熟，生成式 AI 将变得更加以行动为导向 — 编写和修正代码、检查代码库，以及帮助定义和监控安全策略与控制措施。一项研究表明，生成式 AI 将编写代码的完成时间缩短了 35% 至 45%。[16]

超过一半的受访者 (55%) 看到了生成式 AI 在变革供应链运营方面的潜力。在当前或未来 12 个月内，企业投资部署生成式 AI 的主要供应链用例包括提高运营效率，例如资源分配、风险管理（包括网络安全），以及增强可视性以改进预测和决策能力。更长期的目标则包括合规管理和物流，例如机器人、无人机和自动驾驶汽车。

共同推动网络安全和供应链运营转型

高管们对生成式 AI 持乐观状态，但预期略为保守。



问：考虑贵公司未来三年的战略，您在多大程度上同意以下关于生成式 AI 的陈述？

挑战三：
最薄弱的环节

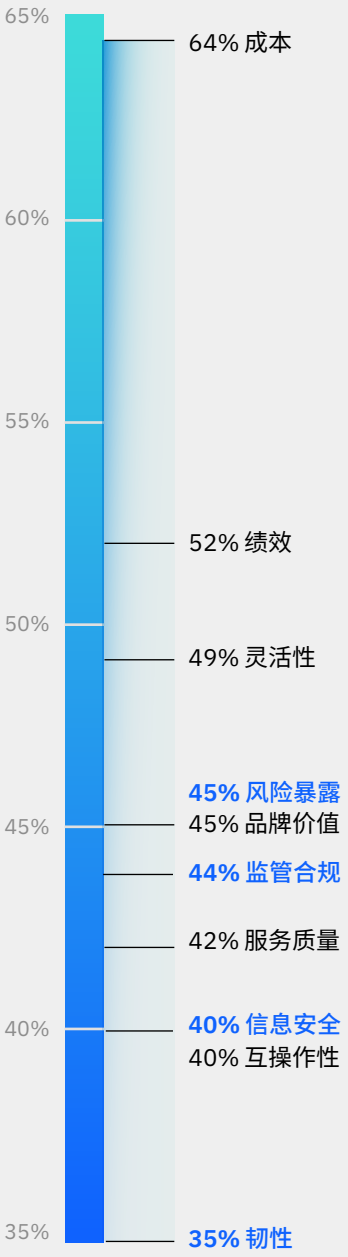
许多供应链合作伙伴的安全实践较差

如果供应链的安全性取决于其最薄弱的环节，那么不遵守组织安全准则的合作伙伴就会使整个供应链变得脆弱。然而，对于受访高管来说，安全实践并不是选择供应商的主要考虑因素。事实上，成本才是其首要决定因素，其重要性要比风险暴露、信息安全、监管合规和韧性等因素高出 23%（见图 8）。

不过，采购成本上的任何财务节省可能是短暂的，因为从长远来看，忽视供应商的安全实践可能会导致更高的延迟成本。随着时间的推移，较低的风险和韧性可视性可能会推高运营支持成本，而在风险和韧性方面的投资则有助于降低这些成本（请参阅第 20 页的“观点：累积风险如何将组织置于险境”）。

图 8

从长远来看，在选择供应商时优先考虑成本而不是风险和韧性因素可能会产生更高的成本。

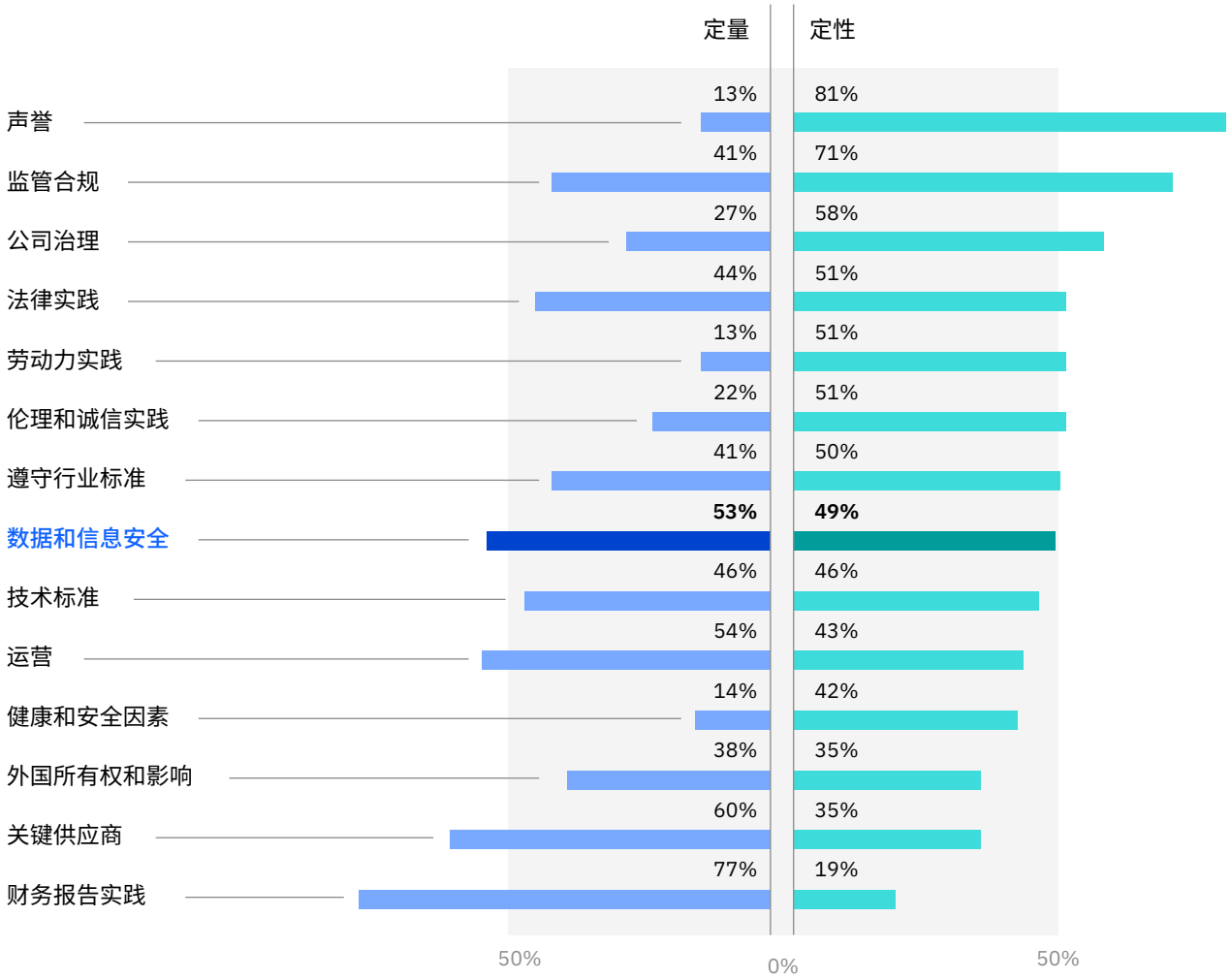


问：选择供应商时最重要的因素是什么？

即使在评估供应商风险时，只有约一半的受访者会将数据和信息安全纳入采购流程。这远低于品牌声誉和财务报告这两项主要因素，而这两者都无法提供真实可见的风险管理实践（见图 9）。

图 9

在评估供应商风险时，只有一半的受访者会考虑数据和信息安全。



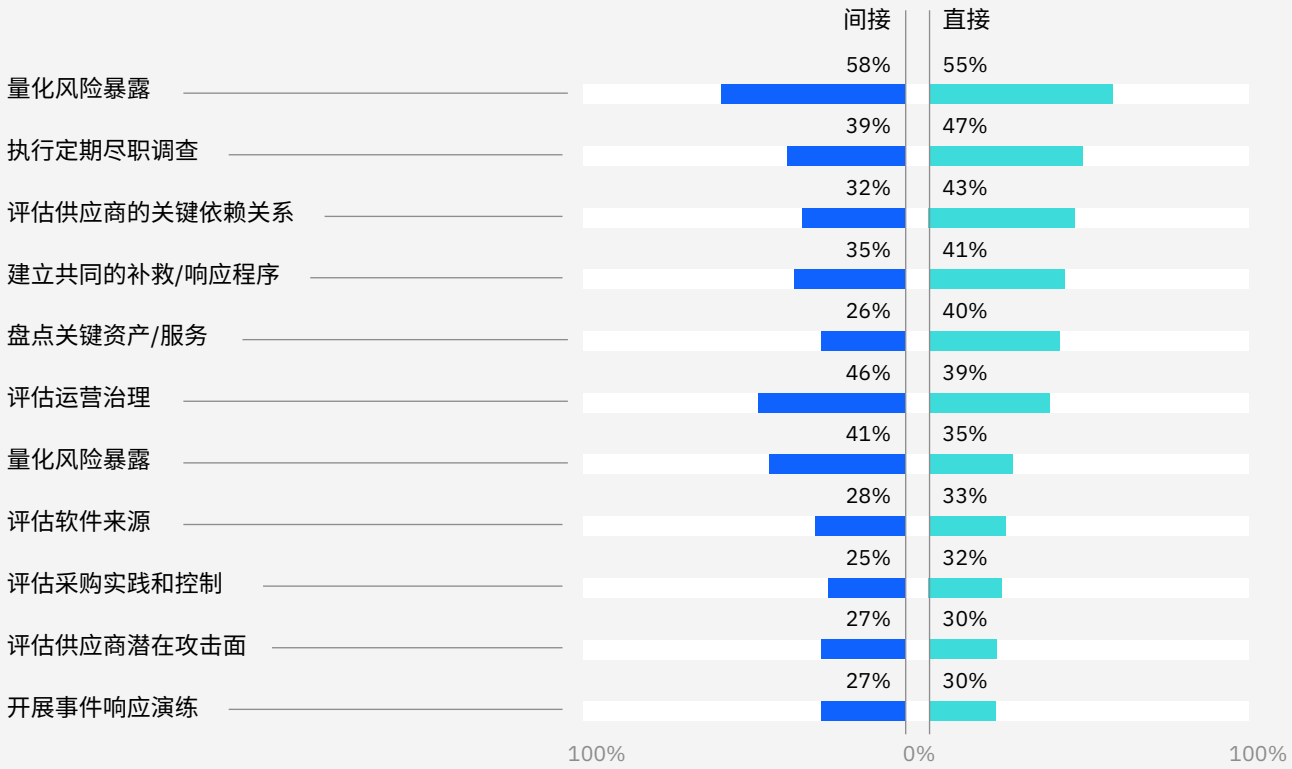
问：贵组织如何评估潜在供应商的风险（定量）？

问：贵组织如何评估潜在供应商的风险（定性）？

最令人担忧的是，受访组织表示其供应商对网络风险管理推荐实践的采用率较低（见图10）。例如，只有略高于一半的受访组织表示会对其直接和间接供应商进行风险态势评估。尽管这是一项最常见的实践，它不过是改善组织整体风险态势的最低标准。在供应商引导方面，只有不到一半的受访者使用了所有其他评估实践。

图 10

理解供应商风险暴露：不成熟的网络风险评估实践会导致更大的下游漏洞。



问：在您的直接供应商中，日常运营中采用了哪些领先实践？

问：在您的间接供应商中，日常运营中采用了哪些领先实践？

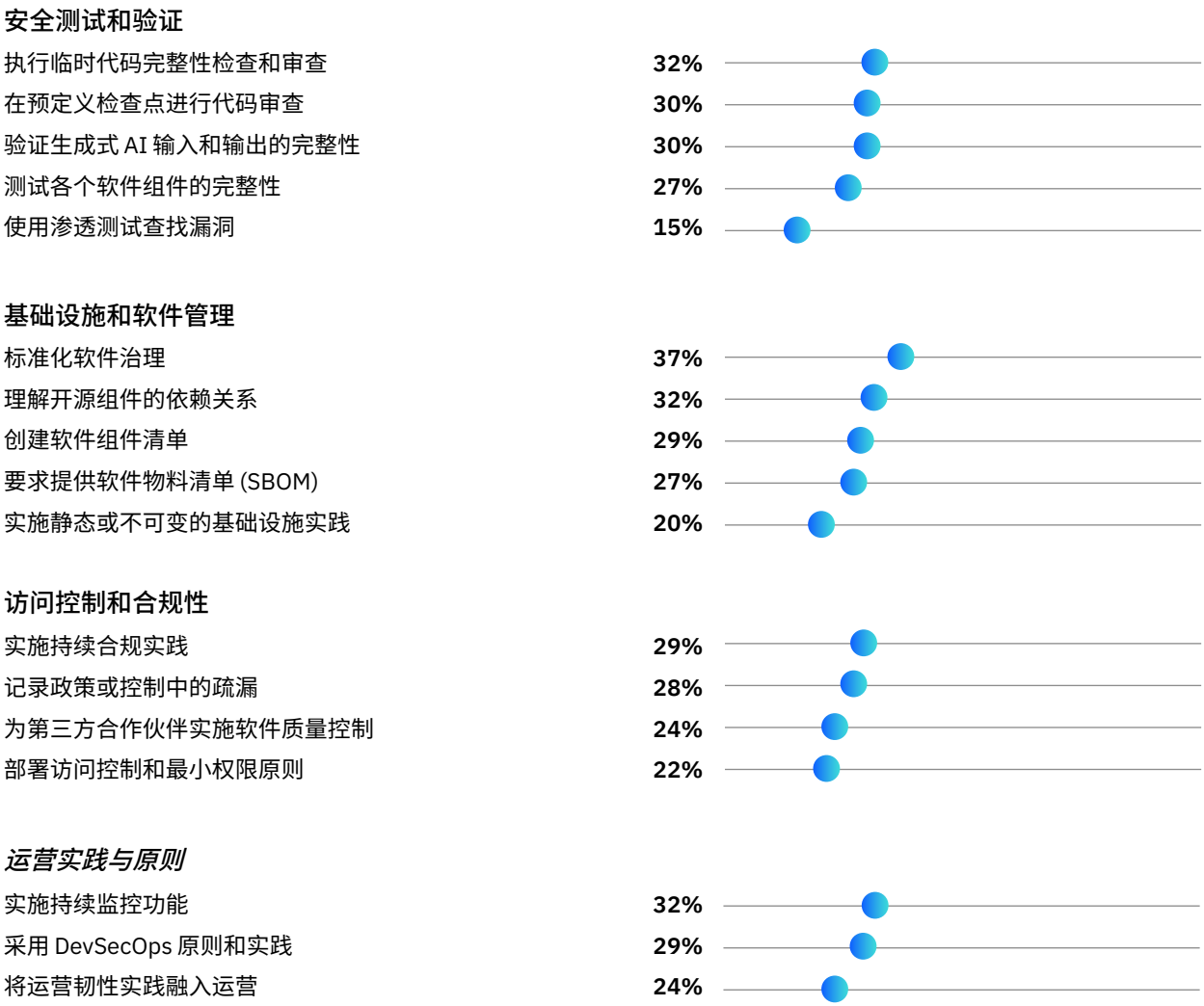
我们调研的受访者在其软件供应链管理实践方面也反映出类似的不成熟水平。尽管采用了一些领先实践，但受访者仅处于其采用的早期阶段（见图 11）。

我们以访问控制和合规措施为例。只有 22% 的受访者表示其组织部署了访问控制和最小权限原则来保护软件供应链。

IBM X-Force 威胁情报团队指出，这导致各种层出不穷的攻击方法都将软件供应链作为目标。最近的一项调研表明，使用有效凭证的攻击量同比大幅增长 (+71%)，这些凭证通过暗网销售，让攻击者从*黑客攻击*转向*登录攻击*。[17] 如果没有强大的风险文化来主动识别和管理供应商和软件漏洞，供应链韧性仍将无从谈起。

图 11

受访者仍处于采用软件供应链安全最佳实践的早期阶段。



问：您在组织中采取了哪些措施来保障软件供应链安全？

观点

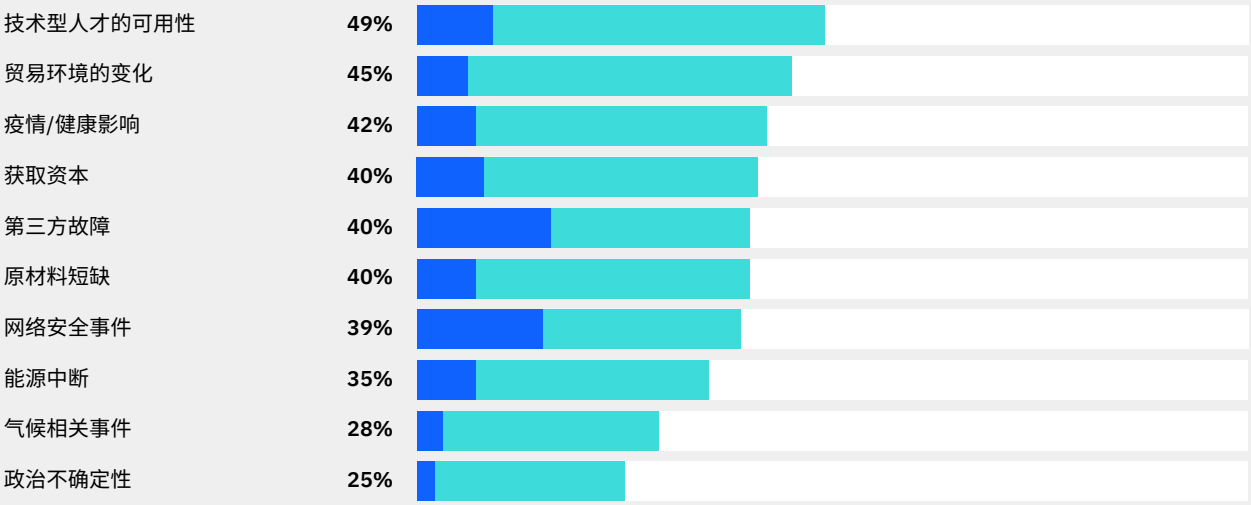
累积风险如何将组织置于险境

韧性不能止于保持警惕。运营中断通常是由各种复杂、连续的风险所导致的，这些风险难以通过标准风险模型进行预测。过去五年的经验明确表明，风险是逐渐出现的，然后由于无法预见的多项因素而突然爆发，从而引发连锁反应，对整个供应链上下游造成严重破坏。[18] 比如，想象一下勒索软件攻击加上人才短缺，再加上灾难性的天气事件，然后一条航运路线堵塞，需要绕行很长一段距离。

随着对数字服务的依赖日益增加，风险迅速扩展到 IT/IS 领域以外，从而扰乱核心运营和创收（见图）。大约三分之一的受访者表示曾受到多项风险因素的显著影响，这意味着需要采取非常措施来应对相应风险。还有一小部分但为数不少的受访者表示遭遇了更为严重和持久的中断。

随着风险因素的增加，累积风险成为一个日益严重的问题。

2021 年至 2023 年期间影响运营的因素



问：2021 年至 2023 年期间，以下因素对运营产生了什么样的影响？
表示产生“显著”或“严重”影响的受访者比例。

未来十年，随着新型贸易关系的出现，供应链运营可能会发生巨变。即使组织从复杂的供应链转向安全、具有韧性的生态系统，也会出现各种新的不确定性因素，也需要更加关注各种新的风险。[19] 尤其令人担忧的是，我们怀疑运营受到显著影响的组织中有较高比例可能已经达到管理多重风险的能力极限。只要外加一点冲击，就可能令这些组织落入“严重运营影响”的类别，从而导致收入受到巨大影响。

根据我们的分析，风险因素的增加可能会意外地迅速演变成一场毁灭性的大规模中断，在最严重的情况下会危及超过 75% 的收入。基于受访者对上述每个风险因素对收入影响的估计，我们的分析表明，那些受到多重严重风险困扰的组织必须要面对令人担忧的收入风险：小型组织每年有 1.605 亿美元的收入面临风险，大型组织每年有超过 220 亿美元的收入面临风险。

对于一些组织来说，当前的形势已经再糟糕不过了 — 高风险环境叠加经济不确定性带来了极其严峻的挑战。受访者表示，过去三年（2021 年至 2023 年期间），其组织的平均收入增长率下降了 55%，利润下降了 49%。

多重严重风险危及大量收入

	因严重影响因素而面临的预计收入风险					
组织规模	**低** +1 风险因素	**平均** +1 风险因素	**高** +1 风险因素	**低** +4 风险因素	**平均** +4 风险因素	**高** +4 风险因素
平均年收入 **1.2 亿至 8.38 亿美元**	3,700 万美元	7,100 万美元	1.256 亿美元	1.605 亿美元	2.746 亿美元	4.133 亿美元
平均年收入 **8.38 亿至 52 亿美元**	1.517 亿美元	2.91 亿美元	5.158 亿美元	4.729 亿美元	8.093 亿美元	12.2 亿美元
平均年收入 **52 亿至 161 亿美元**	6.486 亿美元	12.4 亿美元	22 亿美元	29.9 亿美元	51.1 亿美元	76.9 亿美元
平均年收入 **161 亿至 2,025 亿美元**	23.4 亿美元	44.9 亿美元	79.6 亿美元	85.9 亿美元	147 亿美元	221.2 亿美元

数字为四舍五入

注：“低”、“平均”和“高”基于受访者对特定事件影响运营的一系列问题的回答：对于被归类为“严重”的冲击，贵组织有多少百分比的收入面临风险？

机遇：为直接和间接供应商营造强大、共同的安全文化，增强整个供应商体系的韧性。

未来，组织需要将安全意识作为文化基石，在整个运营环境中加强网络风险管理、安全和韧性。这意味着采取整体方法来管理供应链、网络安全生命周期和 IT/IS 支持生态系统。为了遏制风险和漏洞，组织应当在内部和供应商网络中采用零信任原则。这正是“安全设计”方法的实际应用。

由于各种新的威胁向量可能会在运营生命周期的不同阶段出现，因此组织应当着重采用端到端的网络风险和网络安全方法，涵盖从初始设计、材料采购、供应商选择、分销到最终用户运营支持的整个周期。我们的分析表明，这种转变始于加强组织自身对软件供应链管理最佳实践的采用，包括遵守最新法规，例如汽车行业采用的法规。[20]

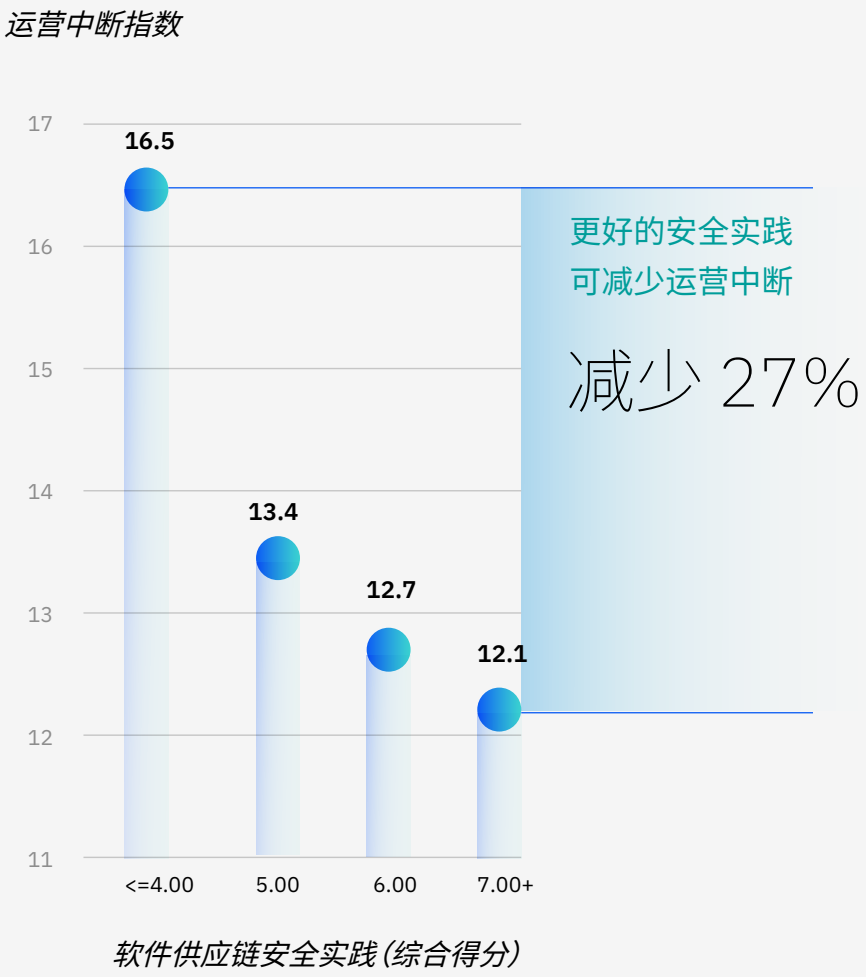
那些更有效采用这些实践的受访者正从强大的软件安全实践中获益。这些组织在其供应商体系中遇到运营中断的几率明显较低（见图 12）。

其次，出于自身利益考虑，企业高管必须通过适当的投资，支持业务合作伙增强风险管理和应对能力。更广泛地采用供应商评估、选择和采购流程时，应纳入对安全漏洞控制以及风险相关绩效指标的评估，最好是侧重于严重性和潜在风险收入的指标。这可能还要采用新的软件质量和验证标准。[21]

为了遏制风险和漏洞，组织应当在内部和供应商网络中采用零信任原则。

图 12

对于软件安全实践更好的组织，其运营中断减少了 27%。

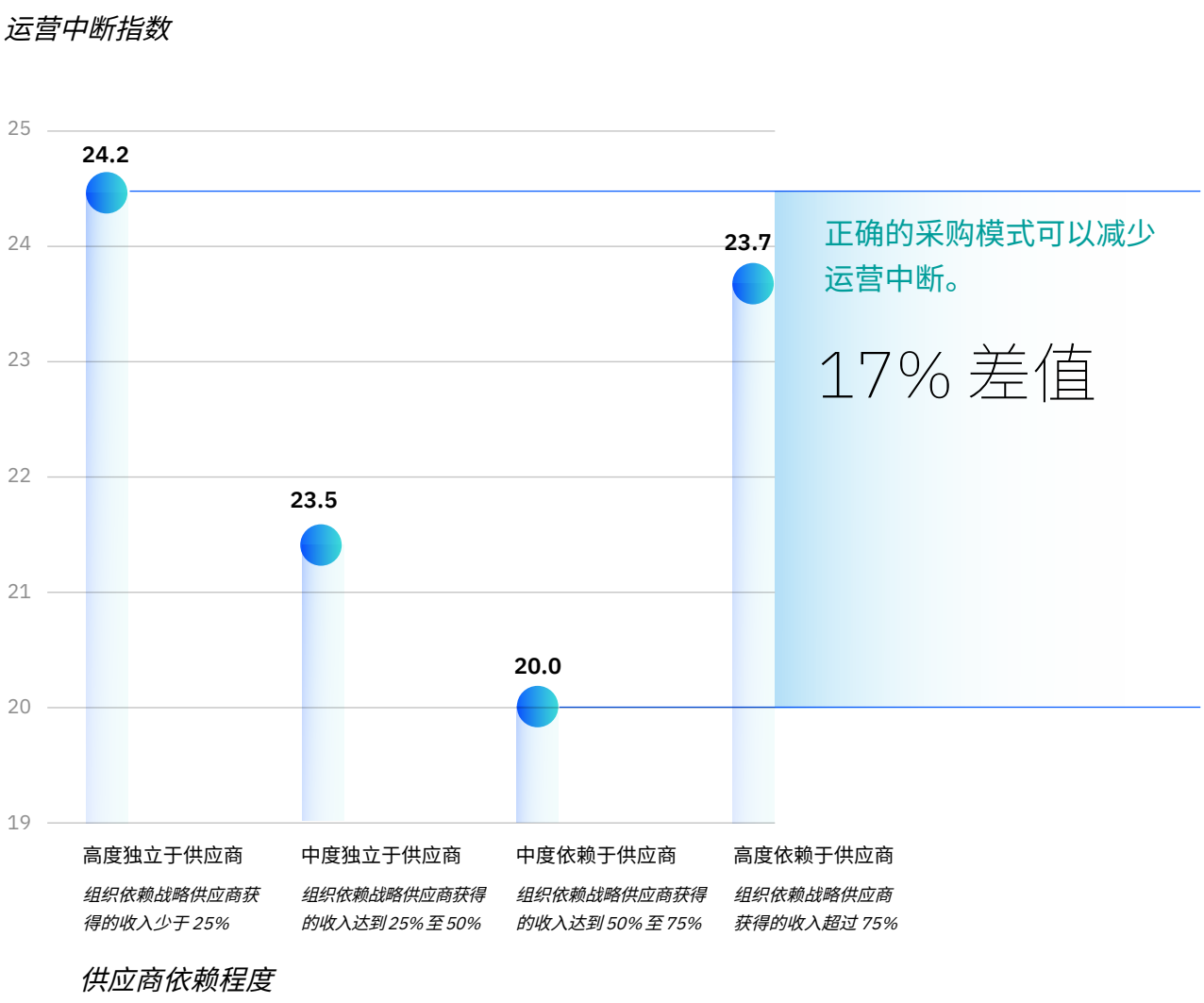


基于 IBM IBV 分析。运营中断指数（y 轴）是根据一系列常见风险因素来衡量组织中断倾向的综合指标。x 轴代表软件供应链安全实践采用情况的综合得分。分数越高则表示软件供应链领先实践的采用程度越高。这对应于更低的运营中断发生率。

IBM 商业价值研究院的分析还表明，采购模式可能在运营韧性中发挥着重要作用。我们发现，对于中度依赖供应商的组织（即战略供应商关系占收入的 50%-75%），其运营中断发生率降低了 17%（见图 13）。

图 13

一些组织在其供应商采购模式中找到了最佳平衡点，可将运营中断减少 17%。



基于 IBM IBV 对“您如何描述贵组织的供应链采购模式？”这一问题的分析。运营中断指数（y 轴）是根据一系列常见风险因素来衡量组织中断倾向的综合指标。

战略供应商的定义是“提供对于您的业务成功至关重要的商品或服务的公司”。

我们怀疑这是因为中度依赖供应商的采购模式是一种富有吸引力的折衷方案。组织可以通过密切的合作伙伴关系获得规模经济、标准化和治理，同时保留一定的灵活性，以避免供应商锁定或与极少供应商相关的风险集中。这种中度供应商依赖、共同投资和共担责任的完美平衡，构成了一个安全、互联的生态系统，也就不足为奇了。对于许多组织来说，这或许是增强供应链韧性的最便捷途径。

中度依赖供应商的组织正在有效分担责任——他们是安全、互联生态系统中的重要合作伙伴。

行动：将营造强大的安全文化列为第一优先要务。

1. 安排一场研讨会，为 IT/IS 员工和合作伙伴启动一项安全意识、行为和文化倡议。
2. 审查并更新现有政策，在其中纳入软件供应链最佳实践。制定并传达新的采购标准，并为各种领先实践实施安全控制措施，例如供应商安全评估、SBOM 治理、软件测试和代码质量审查等。
3. 查看美国国家标准与技术研究院 (US NIST) 关于网络安全供应链风险管理的框架，了解您的组织可以采用哪些领先实践。[22]
4. 优先选择具有安全意识的供应商。首先，选择三家关键供应商并评估其核心安全实践（包括是否采用零信任架构）以及相关的绩效和服务水平。评估合同条款是否包含遵守安全标准或绩效阈值方面的内容。根据定期安全审计来持续监控合规情况。

作者

Kaivan Karimi
移动合作伙伴关系以及制造与移动 OT 安全
Microsoft
kaivankarimi@microsoft.com
linkedin.com/in/kaivankarimi/

Fabio Campos
全球网络战略与风险执行合伙人
网络安全服务，IBM Consulting
camposf@us.ibm.com
linkedin.com/in/fabiolcampos/

Brett Drummond
网络安全服务合伙人
IBM Consulting
Brett.Drummond@ibm.com
linkedin.com/in/brettdrummond/

Gerald Parham
全球安全研究负责人兼 CIO
IBM 商业价值研究院
gparham@us.ibm.com
linkedin.com/in/gerryparham/

致谢
许多人为本研究的设计和材料开发做出了贡献。本报告中的内容体现了许多才华横溢的个人在研究设计、数据分析、编辑和叙述发展、图形设计、主题专业知识和赞助等方面的聪明才智和创造力。

作者谨此特别感谢以下个人做出的杰出贡献：Joanna Wilkins、Lily Patel、Kristin Biron、Sara Aboulhosn、Nagi Punyamurthula、Richard Hogan、Teresa Suarez、Allie Powell、Evelyn Anderson、Charles Chang、Liam Cleaver 和 Dimple Ahluwalia。

IBM 商业价值研究院

IBM 商业价值研究院 (IBM IBV) 成立二十年来，凭借 IBM 在商业、技术和社会交叉领域的独特地位，每年都会针对成千上万高管、消费者和专家展开调研、访谈和互动，将他们的观点综合成可信赖的、振奋人心和切实可行的洞察。

需要 IBV 最新研究成果，请在 ibm.com/ibv 上注册以接收 IBV 的电子邮件通讯。您可以在 Twitter 上关注 @IBMIBV，或通过 https://ibm.co/ibv-linkedin 在 LinkedIn 上联系我们。

访问 IBM 商业价值研究院中国官网，免费下载研究报告：https://www.ibm.com/ibv/cn

相关报告

CEO 生成式 AI 行动指南：网络安全

CEO 生成式 AI 行动指南：网络安全
IBM 商业价值研究院，2023 年 11 月
https://www.ibm.com/downloads/cas/2RMEW1QL

人工智能和自动化助力网络安全

人工智能和自动化助力网络安全：领导者如何统筹技术和人才以取得成功
IBM 商业价值研究院，2022 年 8 月
https://www.ibm.com/downloads/cas/GNWDN5GD

网络经济时代的发展繁荣之道

网络经济时代的发展繁荣之道：重新思考业务转型的网络风险
IBM 商业价值研究院，2023 年 2 月
https://www.ibm.com/downloads/cas/4MXMDOKA

调研和研究方法

为了解组织如何投资于安全功能以增强运营韧性，IBM 商业价值研究院与牛津经济研究院合作，对 2,000 名负责供应商管理、供应商采购和生态系统合作伙伴关系的高管开展了一项调研。调研采用双盲方式，受访者并不知道是哪些组织正在开展这项调研，IBM 或微软也不知道各个受访者的身份。

调研对象包括以下角色的高管（或其等同职位）：主要负责生态系统战略的高级管理人员（CEO、总裁、首席战略官、首席运营官、总经理）、CISO、CIO、CTO、首席供应链官、首席风险官、首席采购官，以及信息安全职能部门、信息技术职能部门和供应链职能部门的高级管理人员（副总裁或以上）。

受访者来自 31 个国家的 16 个行业：银行业、公共部门、汽车业（OEM 和供应商）、化工和石油业（包括石油和天然气）、电子产品、工业产品、消费品、能源和公用事业、金融市场、医疗保健（服务提供者和支付方）、保险业、生命科学 / 制药、电信、零售业、交通运输业和旅游业。

受访者的筛选标准如下：来自“正在很大程度上”实施安全供应链功能的组织，并且对其组织的供应链采购和方法“极其熟悉”。

对结果进行分析以确定安全实践与积极业务成效（例如增强运营韧性）之间的重要关系。某些情况下，回复结果会与类似项组合成一个综合指数，然后一起进行分析，以理解更复杂的现象，如组织的运营中断倾向或软件供应链实践的综合影响。

在估算组织面临的收入风险时，计算依据是归类为“严重”的各个风险因素的相对财务影响。组织因多个风险因素而面临的财务风险暴露是通过以下计算方法得出的：将各个风险因素相加，然后根据组织的总收入估算财务影响。“平均”估算值基于属于指定收入四分位数分布范围的组织的平均值。“低”估算值是具有最小财务影响的各个风险因素的组合。“高”估算值是具有最大财务影响的各个风险因素的组合。

备注和参考资料

1 Overby, Stephanie. “Cybercrime-as-a-Service: Commoditization Fuels Threat Surge.” *Mimecast*. April 18, 2022. https://www.mimecast.com/blog/cybercrime-as-a-service-commoditization-fuels-threat-surge/

2 “Widening Disparities and Growing Threats Cloud Global Cybersecurity Outlook for 2024.” World Economic Forum news release. January 11, 2024. https://www.weforum.org/press/2024/01/wef24-global-cybersecurity-outlook-2024/

3 Mills, Karen G., Elisabeth B. Reynolds, and Morgane Herculano. “Small Businesses Play a Big Role in Supply-Chain Resilience.” *Harvard Business Review*. December 6, 2022. https://hbr.org/2022/12/small-businesses-play-a-big-role-in-supply-chain-resilience

4 *Close Encounters of the Third (and Fourth) Party Kind.* Security Scorecard and Cyentia Institute. February 2023. https://securityscorecard.com/wp-content/uploads/2024/01/Research-Close-Encounters-Of-The-Third-And-Fourth-Party-Kind.pdf

5 *Cost of a Data Breach Report 2023.* IBM Security and the Ponemon Institute. July 2023. https://www.ibm.com/reports/data-breach

6 “What is a supply chain?” TechTarget. Accessed May 6, 2024. https://www.techtarget.com/whatis/definition/supply-chain; “What is software supply chain security?” Red Hat. Accessed May 6, 2024. https://www.redhat.com/en/topics/security/what-is-software-supply-chain-security

7 “Widening Disparities and Growing Threats Cloud Global Cybersecurity Outlook for 2024.” World Economic Forum news release. January 11, 2024. https://www.weforum.org/press/2024/01/wef24-global-cybersecurity-outlook-2024/

8 “Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default.” Cybersecurity and Infrastructure Security Agency. April 13, 2023. https://www.cisa.gov/sites/default/files/2023-04/principles_approaches_for_security-by-design-default_508_0.pdf

9 IBM internal case study.

10 Karimi, Kaivan. “The security cultural transformation of the automotive industry.” Microsoft blog. October 31, 2023. https://www.microsoft.com/en-us/industry/blog/manufacturing-and-mobility/automotive/2023/10/31/the-security-cultural-transformation-of-the-automotive-industry/; *Coding the Car | Volume 1.* MotorTrend + BlackBerry. 2023. https://www.motortrendgroup.com/coding-the-car-leaders-of-the-software-defined-vehicle/; “WP.29 – Introduction.” UNECE Sustainable Development Goals website. https://unece.org/wp29-introduction; ISO/SAE 21434:2021. Road vehicles: *Cybersecurity engineering.* ISO. August 2021. https://www.iso.org/standard/70918.html

11 “Vehicle Manufacturers Need to Know What’s Inside Their Supplier’s Code.” Argus. February 27, 2022. https://argus-sec.com/blog/cyber-security-blog/vehicle-manufacturers-need-to-know-whats-inside-their-suppliers-code/

12 Fisher, Lisa and Gerald Parham. *AI and automation for cybersecurity: How leaders succeed by uniting technology and talent.* IBM Institute for Business Value. May 2022. https://ibm.co/ai-cybersecurity

13 Rajasekharan, Mahesh. “Need A Strategy For Driving Supply Chain Convergence? Think Ecosystem-First.” Forbes. August 29, 2023. https://www.forbes.com/sites/forbestechcouncil/2023/08/29/need-a-strategy-for-driving-supply-chain-convergence-think-ecosystem-first/?sh=6f1aa4075407

14 *CEO’s guide to generative AI: Cybersecurity.* IBM Institute for Business Value. October 2023. https://ibm.co/ceo-generative-ai-cybersecurity

15 Warren, Tom. “Microsoft and OpenAI say hackers are using ChatGPT to improve cyberattacks.” The Verge. February 14, 2024. https://www.theverge.com/2024/2/14/24072706/microsoft-openai-cyberattack-tools-ai-chatgpt

16 “A coding boost from AI.” McKinsey. July 21, 2023. https://www.mckinsey.com/featured-insights/sustainable-inclusive-growth/chart-of-the-day/a-coding-boost-from-ai

17 *X-Force Threat Intelligence Index 2024.* IBM Security. February 2024. https://www.ibm.com/reports/threat-intelligence

18 *RiskN: The Era of Exponential Risk.* Moody’s. 2023. https://www.moodys.com/web/en/us/insights/exponential-risk.html

19 Ibid.

20 Karimi, Kaivan. “The security cultural transformation of the automotive industry.” Microsoft blog. October 31, 2023. https://www.microsoft.com/en-us/industry/blog/manufacturing-and-mobility/automotive/2023/10/31/the-security-cultural-transformation-of-the-automotive-industry/

21 “What is ASPICE?” APTIV. August 11, 2022. https://www.aptiv.com/en/insights/article/what-is-aspice; “GM Secures Supplier Ecosystem with Coding Standards.” *EPSNews*. September 7, 2018. https://epsnews.com/2018/09/07/gm-secures-supplier-ecosystem-with-coding-standards/

22 “Improving the Nation’s Cybersecurity: NIST’s Responsibilities Under the May 2021 Executive Order.” NIST. 2021. https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity; “Software Cybersecurity for Producers and Purchasers.” NIST. 2022. https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/software-cybersecurity-producers-and

关于研究洞察

研究洞察致力于为业务主管就公共和私营领域的关键问题提供基于事实的战略洞察。洞察根据对自身主要研究调查的分析结果得出。要了解更多信息，请联系 IBM 商业价值研究院：iibv@us.ibm.com

选对合作伙伴，驾驭多变的世界

在 IBM，我们积极与客户协作，运用业务洞察和先进的研究方法与技术，帮助他们在瞬息万变的商业环境中保持独特的竞争优势。

国际商业机器（中国）有限公司
北京市朝阳区金和东路 20 号院 3 号楼
正大中心南塔 12 层
邮编：100020

美国出品 | 2024 年 7 月

PNKRGA15-ZHCN-03

扫码关注 IBM 商业价值研究院

官网

微博

微信公众号

IBM