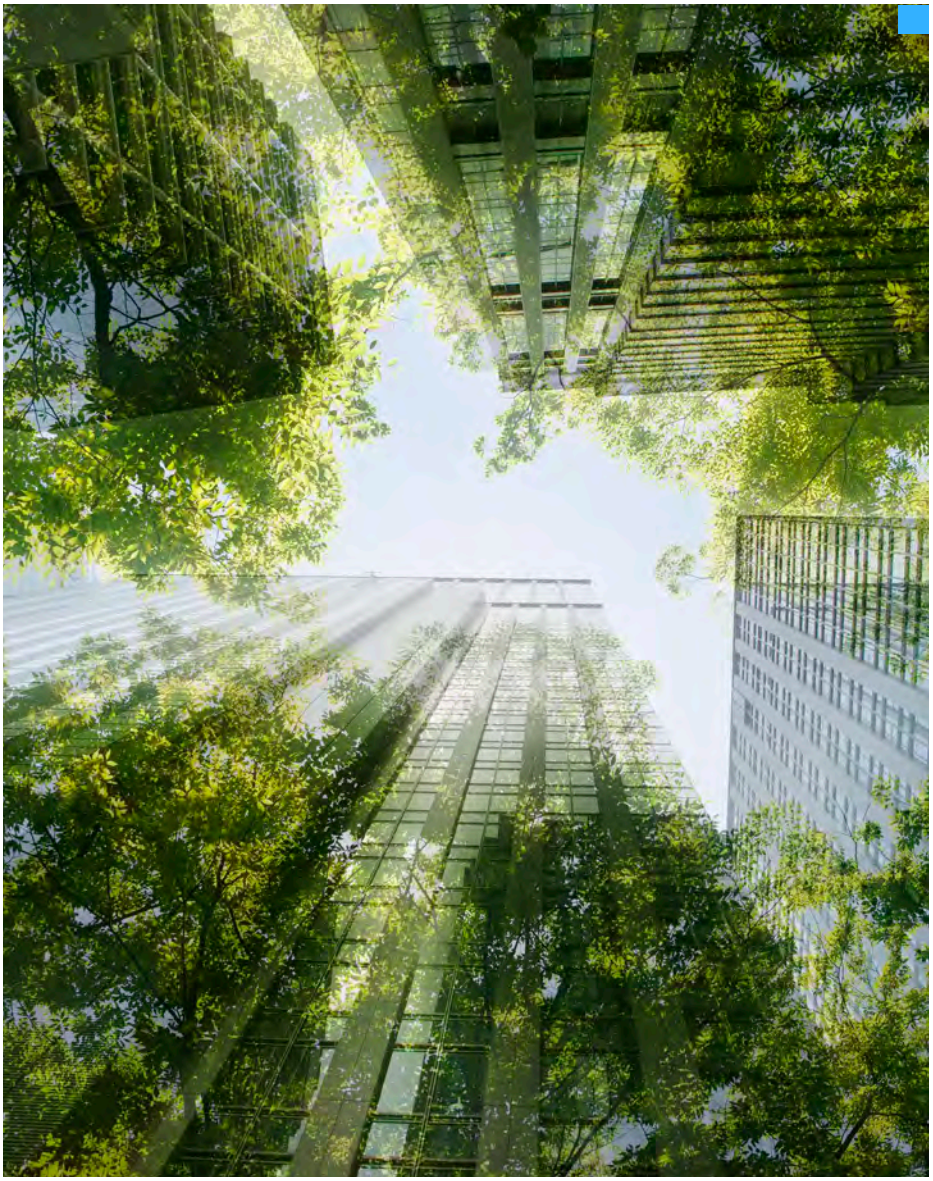


网络经济时代的发展繁荣之道

重新思考业务转型的网络风险

IBM

IBM 如何提供帮助

IBM Security® 致力于与您携手合作，帮助您管理网络风险以及加速推动业务转型。通过确保您的安全战略与业务相一致，我们可以帮助您将安全性转变为收入引擎。如需了解更多信息，请访问：https://ibm.com/security

摘要

“如今，网络经济关乎国家经济命脉。网络受到破坏将严重损害国家安全。”[1]

前美国国家安全顾问
Condoleezza Rice

66% 的受访高管将网络安全投资视为收入引擎。

转变思维方式，将安全投资视为价值而非预算，这有助于企业实现变革性增长。

与网络安全成熟度最低的组织相比，成熟度最高的组织在过去五年内的收入增长率要高出 43%。

采用高级安全功能的组织正在将安全投资转化为更瞩目的业务成效。

43% 的组织表示将其安全计划治理和运营外包给合作伙伴。

责任共担模式正在安全运营中发挥日益重要的作用，57% 的受访者正在携手安全合作伙伴，共同推动安全架构实现标准化。

运营领导者需要逆转网络犯罪等式 — 即转变自己的网络安全思维方式，而不再是寻求金钱损失与支出增加两者的平衡。

采取行动势在必行

在未来四年中，全球网络犯罪造成的损失（到 2025 年将达到每年 10.5 万亿美元）预计将达到全球网络安全支出（到 2026 年将达到每年 2673 亿美元）*40 倍以上*。[2] 两者可谓是相去天渊。

随着组织整体攻击面的不断扩大以及社会对互联服务的依赖带来更多的漏洞，威胁行为体正在网络经济中强势崛起。运营领导者需要逆转网络犯罪等式 — 不再是寻求金钱损失与投入增加两者的平衡。而是要转变自己的网络安全思维方式。

企业领导者需要将安全性视为将业务与技术战略联系在一起的重要纽带，而不是常年生活在防御状态，投入大量精力应对威胁，在夹缝中求生。技术驱动的业务转型不再仅限于通过投资于各个领域来发展成熟的功能，而是需要结合技术与能力来释放更大的价值，协同运营以提高效率，以及通过更有效的协作来改善业务成效。[3]

为了将安全性转变为成功转型和增长的关键动力，许多组织正在纷纷将其侧重点从风险敞口转移至网络弹性（参见图 1）。这样一来，组织将降低对固定边界的依赖程度，更加密切地与合作伙伴整合在一起，并针对当今运营环境中的未知因素保持更高的弹性。这种更成熟的新兴安全态势将在特定行业中以及每个组织的转型旅程中以不同方式表现出来。

有效的网络安全措施与其说是应对不良事件，不如说是预防、缓解和规避不良事件。

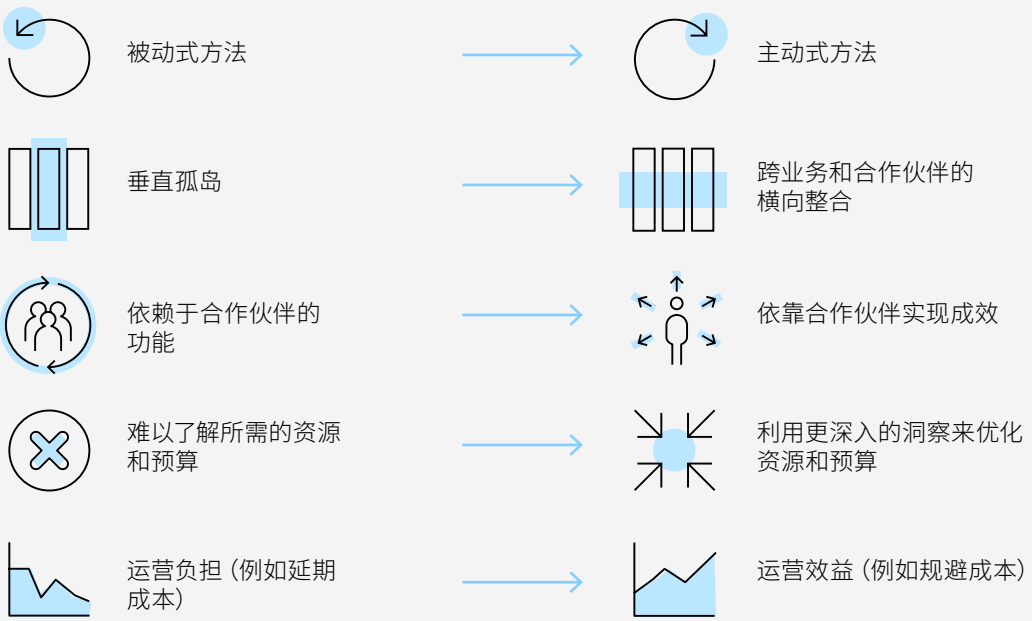
为了更深入地理解企业对网络风险和网络安全的看法，IBM 商业价值研究院 (IBV) 联合牛津经济研究院，针对 25 个国家/地区的 18 个行业的 2,300 多位业务、运营、技术、网络风险和网络安全高管开展了一项调研（参见第 28 页的“研究和分析方法”）。

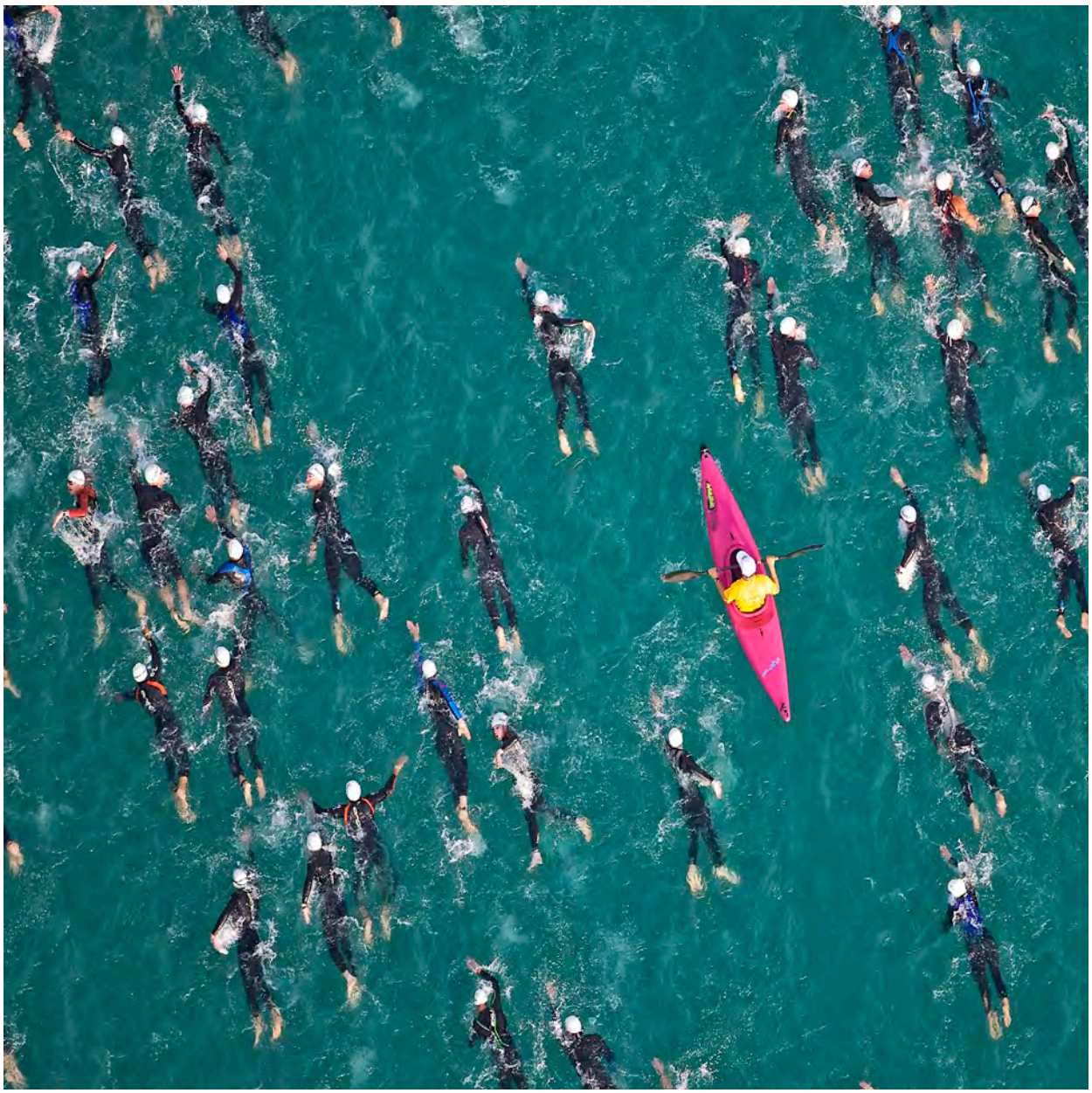
这项研究从迄今为止最全面的视角，深入分析了负责推动企业 IT 和信息安全 (IS) 转型议程的高管的独到见解。这些研究结果描绘了一幅令人信服的画面 — 网络安全正在成为一种核心战略能力，可帮助企业降低财务风险、提高运营效率以及发掘新的价值来源。

图 1

网络安全战略演变

将侧重点从风险转移到弹性上，建立更成熟的安全态势，从而推动业务转型并创造更大的价值。





“网络安全是新时代十年的重大问题。”[4]

IBM 首席执行官 **Arvind Krishna**

网络安全的新经济学

尽管网络安全已然跃升为企业最高管理层的优先任务，但运营成熟度和投资价值仍在不断演化。例如，根据 2022 年的 IBM 商业价值研究院 CEO 调研，网络安全被列为未来两到三年内的第三大业务挑战，45% 的 CEO 将网络风险视为 2022 年的主要业务挑战之一，这一比例相比 2021 年增长 15%。[5]

同时，IBM 商业价值研究院的研究还表明，安全支出在企业 IT 支出中所占的比重呈持续增长之势，预计将从目前的 9% 增长至 2024 年的 10% 以上。

而要将愿望转化为行动也是一项严峻的挑战。86% 的受访高管表示其组织已经采取了安全战略，但只有 35% 的组织已经将该战略落实到行动中。而且，只有大约 50% 的受访高管表示其组织会确保安全战略与业务战略相一致。

同时，这项调研的受访高管还表示，仅在过去一年，其组织就平均发生了 349 起网络安全事件和 9 起数据泄露事件。根据 IBM 和 Ponemon Institute 发布的《2022 年数据泄露成本报告》，企业数据泄露的平均成本为 435 万美元。[6] 为什么遏制网络威胁如此困难？

一个原因是：从经济角度来说，这根本就不是一场公平的战斗。多年以来，网络犯罪分子一直采取富有耐心、有条不紊的机会主义方法，只需极低的成本和风险就能实现超高的回报。他们通常很少或根本不会为自己的行为承担后果。而且，他们只需成功一次就能够获得丰厚的回报。

对于网络防御者来说，经济学问题显然要复杂得多。组织将直接承担相关成本。这包括与威胁缓解和恢复相关的直接成本，（甚至还包括更重要的）与声誉、知识产权、品牌声望、客户和竞争优势损失相关的间接成本，以及运营中断、保险费率增加和监管罚款。在安全事件发生后的数年内，所有这些成本都将持续累积。[7]

在这个经济学等式中，人才差异也是不可或缺的一部分。威胁行为体可以雇佣技能和工资相对较低的合同工或者采用自动化机器人来探测漏洞，而网络防御者则需要支付高价聘请高技能的稀缺性人才。事实上，对技术能力和高技能专业化的需求正在推动网络人才市场的变革：受访高管表示，其组织通过外包方式聘请的安全人员比例现已达到 58%。

网络防御者面临的挑战并不仅限于经济问题。复杂的运营流程也构成了重大障碍。

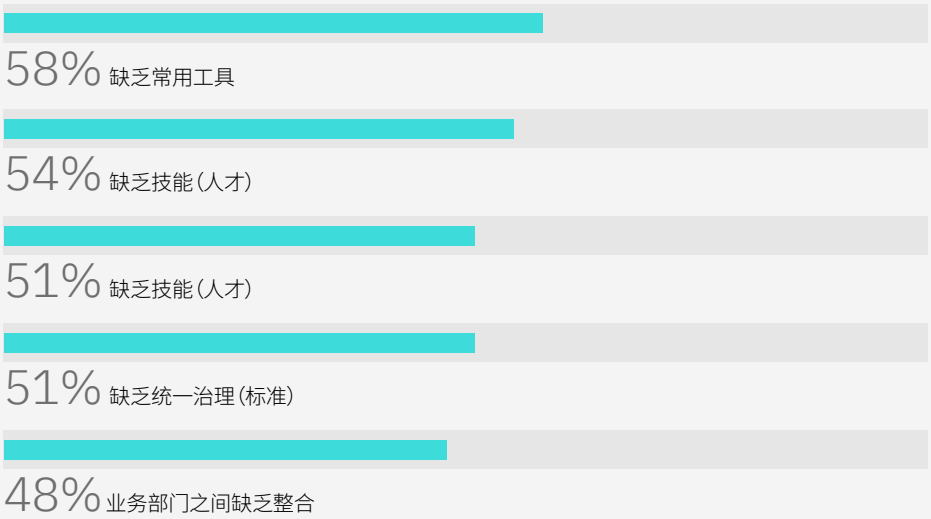
组织需要对不断扩大的广阔攻击面保持警惕，有效应对内部和外部威胁，还要管理与利益相关者、客户、员工、合作伙伴、竞争对手、政策制定者以及监管机构之间的关系。只要失误一次，组织就将承担重大的潜在责任，尤其是当各种风险以不可预测的方式相互叠加，抑或是未能及时识别难以察觉的系统漏洞。网络防御者必须做到万无一失。然而，即使是能力最出众的团队也会受到时间、注意力、技能、能力和工具的限制。犯错几乎是不可避免的。

我们的研究表明，组织整体网络弹性的最大障碍主要包括协同问题以及能力和技能欠缺（参见图 2）。

图 2

运营障碍

在整个企业中整合必要的工具和人才对于网络弹性至关重要，但实现难度较大。



问：贵组织在网络弹性上面临的最大障碍是什么？

此外，企业最高管理层内部在安全领域缺乏战略协同也构成了另一项挑战。CIO (36%)、CTO (35%) 和 CEO (35%) 之间似乎在网络战略制定方面存在分歧。而如果 CIO 关注运营目标，CTO 关注技术目标，而 CEO 注重战略可见性，则组织可能无法通过业务、IT 与信息安全团队之间的有效协同来创造更大的价值。

安全组合的演变意味着 IT 和信息安全问题日益相互依赖。74% 的受访高管表示其网络安全预算只是整体 IT 预算及其审批流程的一部分，只有 26% 的受访高管表示其组织保持独立的信息安全预算。如今，安全运营模式涉及不同职能领域之间的重要协作 — CIO、CISO 或 CTO 将（按此顺序）负责领导安全产品组合的大部分工作。

最后，在当今变幻莫测的商业环境中，许多未知因素都是不可忽视的。例如，第三方服务为企业提供日益广泛的支持，从而加剧了安全运营的复杂性。而如果未采取适当的战略性措施，则这一问题将尤为突出。这会加剧系统性和传递性风险（与第三方的相互联系产生的关系所驱动的风险）。这两种风险都难以理解、预测或建模。

如今，安全运营模式涉及不同职能领域之间的重要协作 — CIO、CISO 或 CTO 将（按此顺序）负责安全产品组合的大部分工作。

管理多学科网络安全计划的复杂性促使 43% 的受访组织将整体安全计划治理和运营外包给合作伙伴。

组织越发依赖共享基础设施、互联服务以及数量激增的设备和机器，这意味着他们所面临的风险要高出其自我认知。然而，我们的调研表明，受访高管估计不同类型的风险都会产生大致相同的业务影响，这反映企业高管可能并不了解不同的风险向量会产生哪些相对应的影响范围和财务后果。这些运营盲点本身就是一项重大风险。

因此，企业高管往往无法清楚了解其所面临的网络风险，尤其是对下游运营和财务的影响。对于许多网络安全高管而言，缺乏相关资源和决策能力是一项重大挑战。企业高管们要忙于协同运营与资源限制，处理相互竞争的优先任务，而且无法深入认识到哪些信息安全投资对业务成果有最大的贡献。

这些不确定性必然会增加运营复杂性，这通常会导致网络安全支出分配效率低下，而且难以为运营环境提供充分支持。事实上，管理多学科网络安全计划的潜在复杂性促使 43% 的受访组织将整体安全计划治理和运营外包给供应商。

网络风险管理将安全投资从预算项目转变为价值引擎

组织正在设法理解如何确定其安全投资的领域和优先级。一种理想的方案是使用风险量化和相关指标，例如使用证券投资回报率 (ROSI) 作为传统 ROI 指标的补充，进一步纳入通过规避或缓解风险创造的财务收益。理解风险价值指标对于支持跨网络风险和网络安全生命周期的决策至关重要。

这是因为安全的价值基础一直在不断发生变化。过去，网络安全一直被视为一项必不可少的支出。而现在，网络安全已经可以在引领战略转型计划方面发挥关键作用。最近，企业在云安全和零信任功能领域中的投资就是一项佐证。[8]（参见案例研究“美国航空公司降低网络风险并加速推动转型。”）

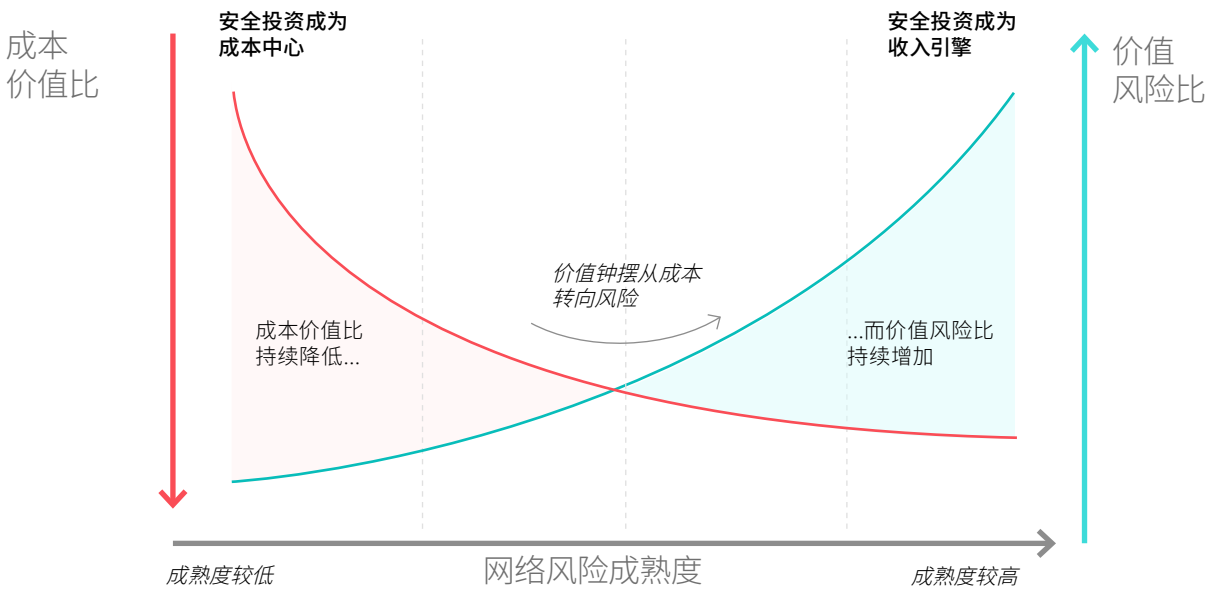
大多数企业最高管理层都支持这一观点。66% 的受访高管将网络安全视为收入引擎，而只有 34% 的受访高管将网络安全视为成本中心。根据情绪因素进行调整后，五分之四的受访高管表示他们将安全投资视为一项价值引擎，这凸显了安全投资在业务和 IT/信息安全转型计划中的重要作用。

精明的领导者会敏锐地发现其中的商机：在改善运营和财务绩效方面，网络风险是一个容易被忽视的环节。通过提高效率、缓解财务影响以及规避收入损失，组织可以大幅提升盈利水平。此外，抗风险能力更强的组织更有弹性，也不易受到阻碍其长期战略执行的干扰因素的影响。这有助于推动业务和收入增长（参见图 3）。

图 3

风险意识带来可观回报

更深入地理解和规避安全风险有助于改善绩效。



案例研究

美国航空公司降低网络风险并加速推动转型[9]

面对全然不同的威胁环境，美国某航空公司实施了广泛的数字化转型计划，包括将其应用迁移至云端。该公司需要积极改善网络弹性态势，设定降低网络风险的目标，并制定与其转型旅程相一致的零信任战略。

该航空公司的云和安全领导团队选择采用了一种云安全架构，旨在建立敏捷性以及形成更成熟的安全态势。最初，该航空公司的团队专注于采用涵盖其整个 IT 环境的微分段 (micro-segmentation) 和零信任方法。这种方法旨在防止入侵者访问敏感数据以及规避勒索软件风险。成功部署这一企业级解决方案之后，该航空公司增强了对网络风险的可见性，并且能够快速实时隔离威胁和高风险系统。

随后，该团队开始专注于开发 DevSecOps 模式，从而推动其应用开发流程转型。这有助于增强开发人员意识，实现更主动的安全方法。

在正式上线一年后，该企业级安全解决方案帮助这家航空公司降低了新应用和新云环境中的残留风险，从而加速了数字化转型进程。通过将安全投资作为转型的核心，该航空公司可以满怀信心地将运营迁移至云端，并提供更加个性化的客户体验，实现更高效、更具成本效益的运营，从而超越竞争对手。

跨 IT 和信息安全职能的治理、风险与合规性 (GRC) 计划的兴起有力佐证了网络风险管理的战略优势。[10] 作为对传统安全运营的补充，这种方法侧重于保护和预防活动，从被动威胁管理转变为主动风险缓解与风险规避。

许多组织似乎都在朝着这个方向迈进。受访高管表示，网络风险与网络安全职责主要由企业高管共同承担，主要包括 CIO、CISO 和 CTO。从本质上说，网络风险实践涉及多个学科，因此这是消除运营孤岛最为直接的方式之一。（请参见案例研究“保险公司协同安全与业务战略以推动转型。”）

从本质上说，网络风险实践涉及多个学科，因此这是消除运营孤岛最为直接的方式之一。

61% 的受访高管表示提高网络弹性是网络安全投资的一项重要业务驱动因素，而只有 25% 的受访高管实施了网络风险量化功能。

然而，大多数企业并未将开发更成熟网络风险功能的愿景落实到实施中。例如，61% 的受访高管表示提高网络弹性是其网络安全投资最重要的业务驱动因素之一，但 54% 的受访高管表示其组织并未建立与其风险态势相一致的安全控制措施，或仅在一定程度上保持一致。或许最能说明问题的一项数据 — 只有 25% 的受访高管表示正在实施、运营或优化网络风险量化功能。

在快速改善组织整体安全态势方面，开发高级网络风险功能是最具前景的领域之一。正如下一节所述，借助卓越的网络风险管理能力以及更具前瞻性的生态系统协同能力，一些组织正在实现更高水平的财务与运营效率、绩效及弹性。

案例研究

保险公司协同安全与业务战略以推动转型[11]

为了实现长期增长议程，一家财产和意外伤害保险公司需要通过整合前瞻性网络弹性功能来完善其网络安全战略。这需要全面评估行业趋势和新兴技术将如何影响其业务、技术和安全能力。最终，这家保险公司以网络弹性、创新、人员和客户为基础，成功明确了一条全新的发展路径。

通过联合各级跨职能团队举办一系列以能力为中心的研讨会来定义“可能性的艺术”，该公司开发了一个零信任参考架构来指导最小权限访问策略的设计和部署。借助这一运营优势，该公司做出了在网络环境中建立受限分段访问模式的技术决策。

几个月后，该公司的领导者得出结论，这一解决方案已经在安全和技术组合中实现了所需的战略业务一致性。这增强了整个公司的信心 — 在可预见的未来，该公司的安全战略将继续为其数字化转型旅程提供强有力的支持。此外，该公司还增强了应对紧急威胁的能力，从而提升整体网络弹性。不仅如此，该公司还可以利用从转型项目中获取的洞察，为未来的网络安全投资创建更强有力的商业论证。

“安全支出与我们客户的愿景密切相关，包括迁移上云、推动与其客户建立更直接的关系、实现 IT 基础架构现代化以及在适应新工作方式的同时提高效率。” [12]

Palo Alto Networks 首席执行官 **Nikesh Arora**

协同安全功能以实现价值

我们的研究结果表明，安全转型方法并不是一成不变的。为了更深入地理解不同组织所采取的安全发展路径，我们研究了安全功能对业务成效的影响。

首先，我们从五个领域评估了受访组织的安全成熟度。要在一个领域实现较高的成熟度，组织需要采取特定的行动，建立特定的能力，并结合运用这些相互依存的因素来创造更多价值（参见图 4）。

图 4

从价值的角度重新思考安全投资

现代安全功能相互依存，共同实现更广泛的企业和生态系统级价值主张。

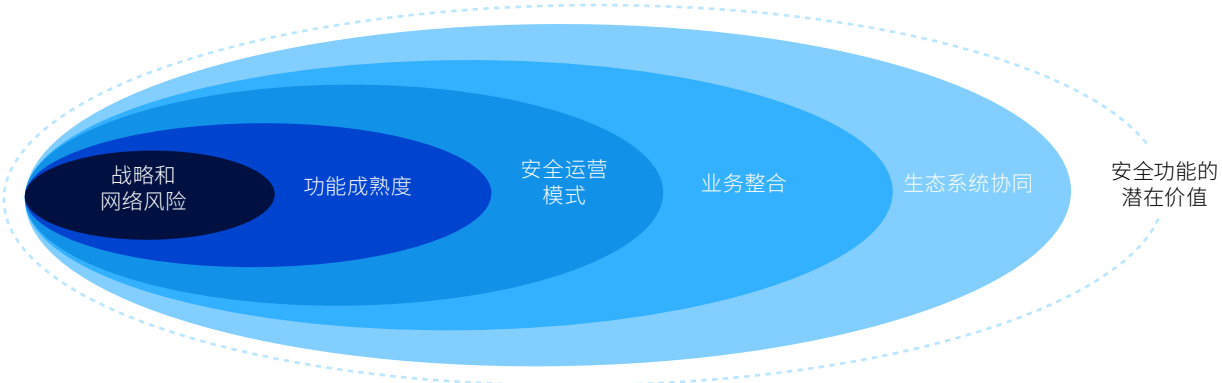
1
战略和网络风险
执行安全战略并确保建立与风险态势相一致的控制措施

2
功能成熟度
在云安全、DevSecOps 和安全架构等领域，建立现代化核心安全功能并实现协同交付

3
安全运营模式
跨安全职能设计、构建和编排技术、流程、技能与治理

4
业务整合
跨核心业务职能，从战略层面扩展安全功能

5
生态系统协同
广泛引入生态系统合作伙伴，共同设计和交付安全功能与新价值主张



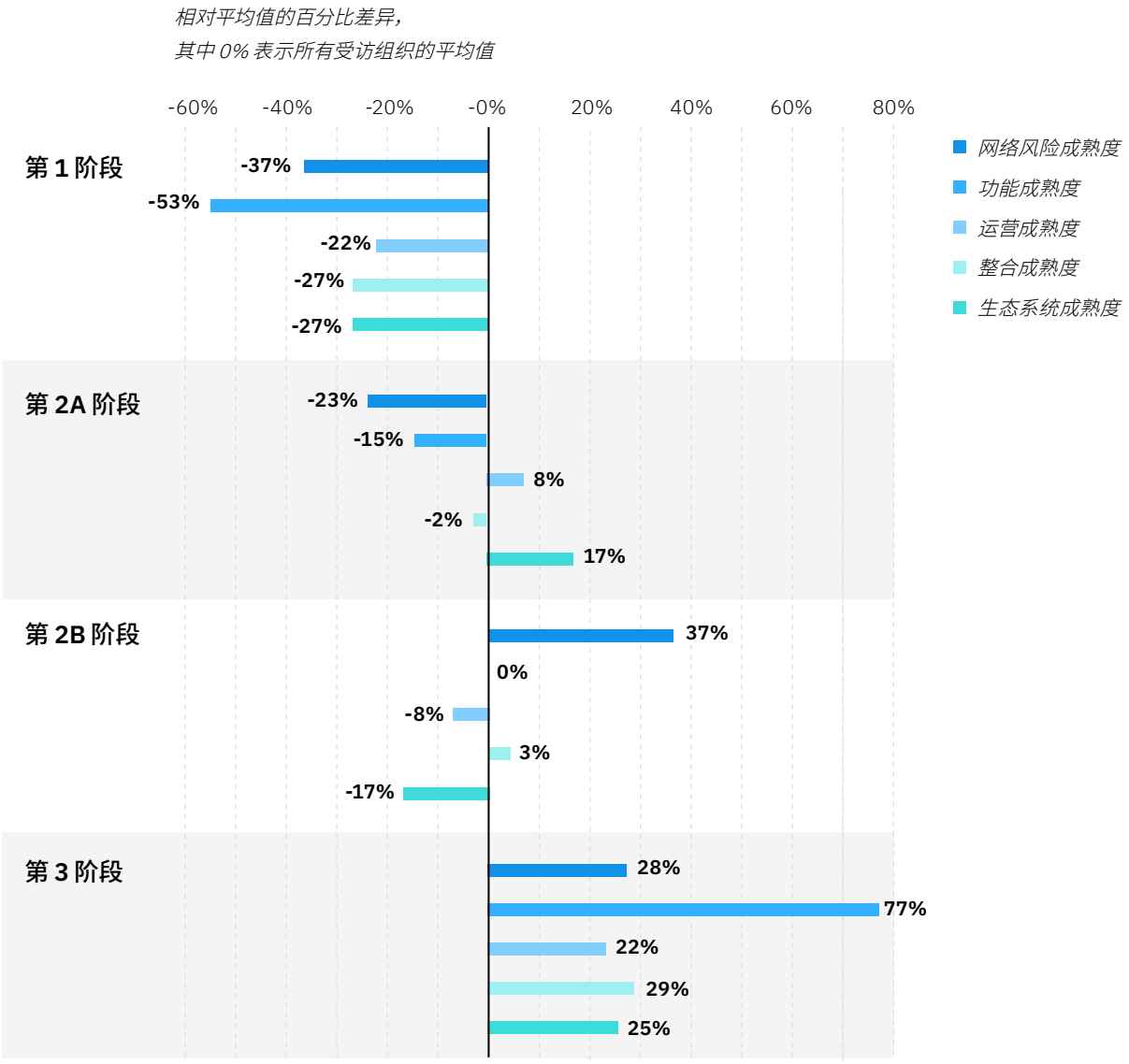
我们的分析表明，组织处于安全成熟度的不同阶段，从最低成熟度（第 1 阶段）到中等成熟度（第 2A 和 2B 阶段），再到更高的成熟度（第 3 阶段；参见图 5）。通过比较，第 1 阶段的组织与第 3 阶段的组织存在非常明显的差异：

– 第 1 阶段的组织通常规模较小（基于收入指标），环境不太复杂，在技术与运营方面成熟度较低，而且在实施新安全功能方面取得的进展最少。

图 5

安全成熟度的不同阶段

根据在这些领域的具体进展，受访组织处于不同的阶段。



基于 IBV 分析。

– 第 3 阶段组织的规模较大，采用了云和 AI 等新兴技术，并将安全性嵌入到整个企业及其生态系统中。
– 在成熟度较低的组织中，只有三分之一将其安全职能视为收入引擎，而在成熟度较高的组织中，这一比例则高达 90%。
– 在第 1 阶段组织中，只有 22% 的高管表示网络安全正在为其生态系统整合做出积极贡献，而在第 3 阶段组织中，这一比例为 52%。

我们还发现，不同组织从较低安全成熟度发展至较高安全成熟度的路径各不相同。正如第 2A 阶段和第 2B 阶段的组织所示，组织在某些领域对各项功能的优先级排序将决定其通往高成熟度的路径（参见图 6）。

第 2A 阶段的组织同时关注安全运营模式和生态系统协同这两大领域，正在将其关注点从战略转向功能。通过不断开发更高级的安全运营模式，此类组织正在依靠合作伙伴的专业技能和能力。

当作为现代安全战略的一部分发挥效用时，将安全功能扩展至生态系统可以有效打击网络犯罪，而不仅仅是引入更广泛的漏洞和风险。通过引入合作伙伴共担风险与职责，此类组织正在通过信息共享、联合防御和纵深防御等实践建立更强大的安全态势。[13]

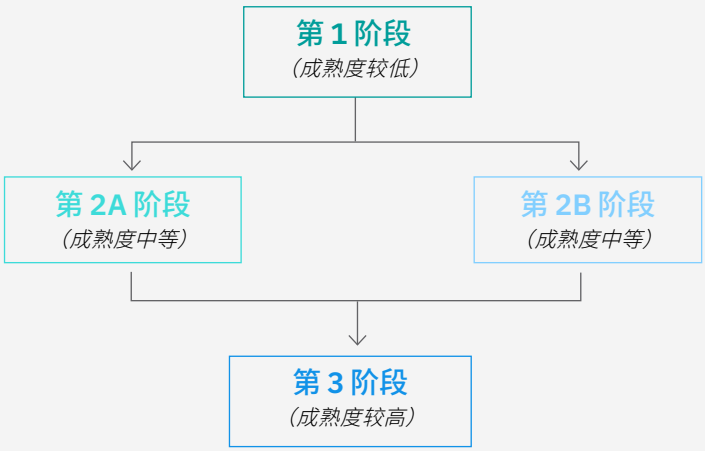
相比之下，第 2B 阶段的组织正侧重于理解网络风险，并确保安全投资与网络战略相一致。此类组织也获得了可观的回报，不仅降低了安全漏洞和安全事件的比率，而且还提高了安全运营效率。此外，第 2B 阶段的组织还在积极将安全功能整合到更广泛的企业中。

为了实现更高水平的安全功能，达到第 3 阶段，第 2A 和 2B 阶段的组织需要扩大其关注点，并扩展在其他成熟度领域的功能。这两类组织均表示意识到了安全投资在创造机遇方面的潜力 — 59% 的第 2A 阶段高管和 83% 的第 2B 阶段高管将安全投资视为收入引擎。

图 6

安全转型路径

具体路径取决于组织的业务和安全战略会对运营优先级产生哪些影响。



第 1 阶段
– 比较有限地使用新兴重大安全功能
– 技术成熟度较低
– 重大风险盲点
– 33% 的受访组织将安全投资视为收入引擎

第 2A 阶段
– 注重与合作伙伴之间的安全协同
– 先进的安全运营模式
– 安全态势与网络风险之间的协同水平较低
– 59% 的受访组织将安全投资视为收入引擎

第 2B 阶段
– 注重安全态势与网络风险之间的协同
– 与合作伙伴之间的安全协同水平较低
– 不成熟的安全运营模式
– 83% 的受访组织将安全投资视为收入引擎

第 3 阶段
– 在整个企业中嵌入安全功能
– 有效协同安全战略与业务战略
– 强大的安全治理流程
– 90% 的受访组织将安全投资视为收入引擎

回报：安全功能助力改善业务绩效以及推动转型

在第 3 阶段组织中，安全转型的累积效应非常明显。与其他任何类别相比，第 3 阶段组织正在将其先进的安全功能转化为更加卓越的业务绩效，这反映在收入增长和盈利能力等财务指标上。

在五年期间，第 3 阶段组织的平均收入增长率比第 1 阶段组织高 43%。此外，此类组织还实现了更高的盈利能力，这反映在营业利润率指标上（参见图 7）。

第 2A 阶段和第 2B 阶段组织在构建安全功能时侧重于不同领域，但这两类组织均实现了同等水平的业务绩效。这进一步反映了组织针对第 3 阶段采取的适当步骤取决于其业务和安全策略将对运营优先级产生哪些影响。

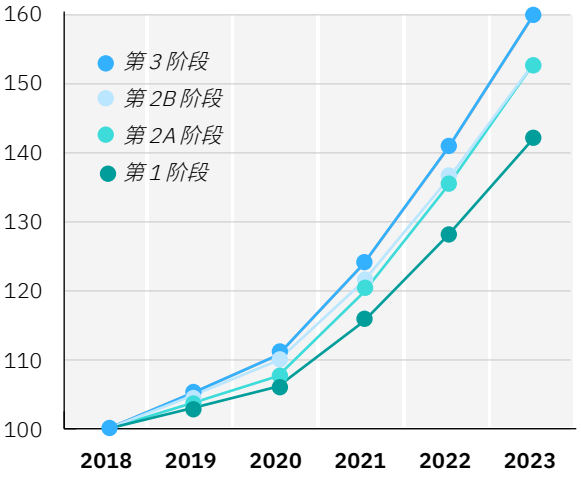
图 7

安全成熟度推动增长

与第 1 阶段组织相比，第 3 阶段组织实现了更高的收入增长率（5 年内的复合年均增长率为 43%）和盈利能力（2021 年高 41%）。

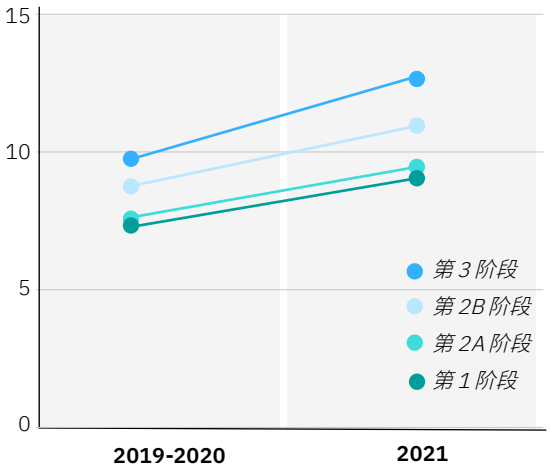
多个阶段的累计收入

收入增长百分比（2018 年指数 = 100）



多个阶段的年平均营业利润率

营业利润率占收入的百分比



基于 IBV 分析。

从其他绩效因素来看，第 3 阶段组织更有可能在敏捷性、创新、数据管理和人才发展等关键领域超越竞争对手 — 所有这些领域对于转型都至关重要。此类组织正在将其安全功能转化为切实的效益和深远的积极影响，包括在组织内部实现更高的 IT 弹性、促进生态系统合作以及积极与外部合作伙伴开展开放创新（参见图 8）。

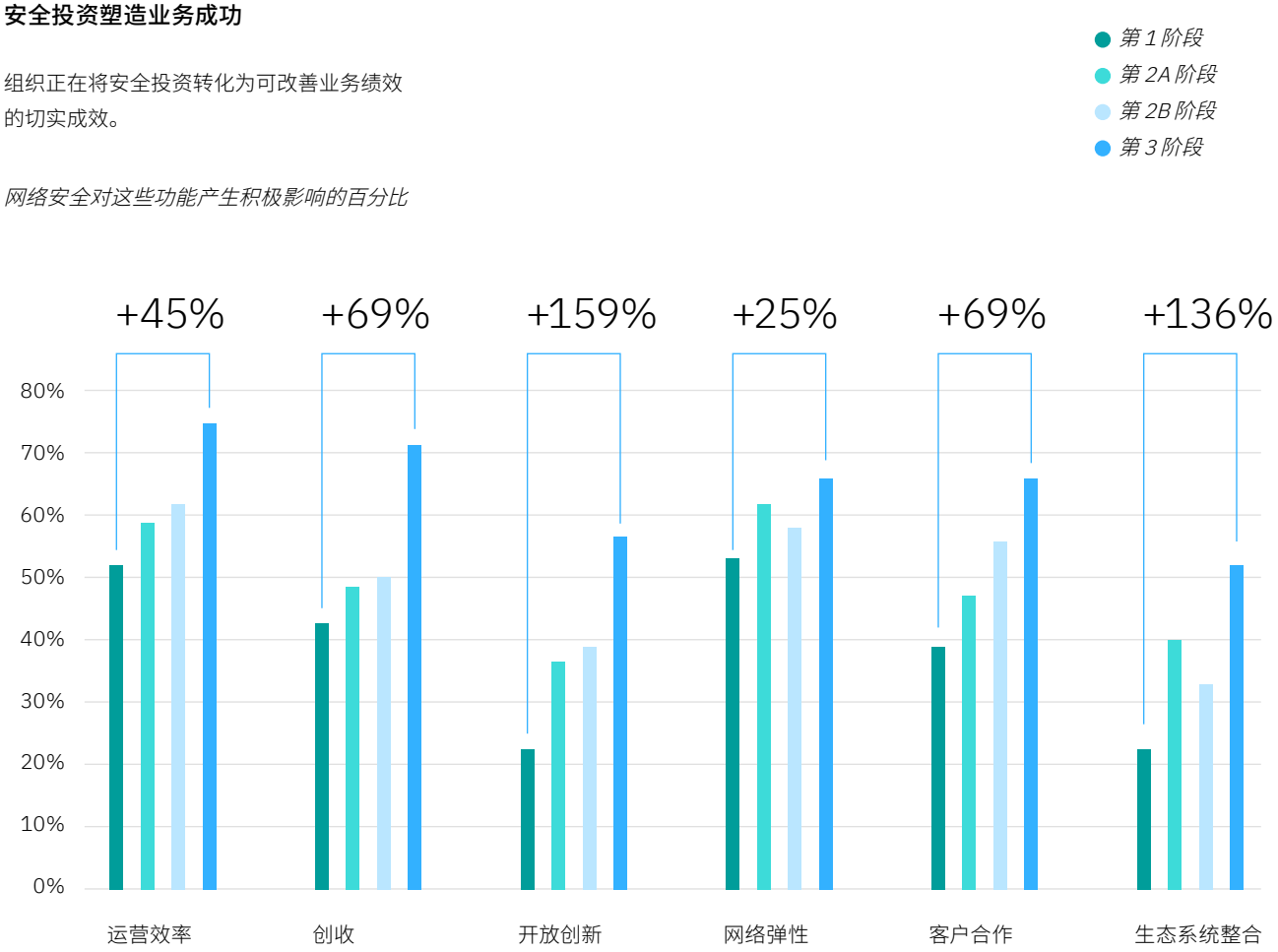
第 3 阶段组织更有可能在敏捷性、创新、数据管理和人才发展等关键领域超越竞争对手。

图 8

安全投资塑造业务成功

组织正在将安全投资转化为可改善业务绩效的切实成效。

网络安全对这些功能产生积极影响的百分比



证券投资回报率 (ROSI) 是受访高管认为在评估潜在安全投资方面最重要的一项财务指标。在这些指标上，组织普遍表示实现了可观的回报。在所有受访组织中，平均 ROI 为 184%，而平均 ROSI 为 292%。有点出乎意料的是，第 1 阶段组织的 ROSI 要高于第 3 阶段组织的 ROSI。这可能是因为边际收益发生了递减。换句话说，更复杂、更大规模运营所需的投资越高，整体 ROSI 就越低。相比之下，尚未做出重大安全投资的小型组织通常可以把握更多“易于实现”的投资机会，从而实现更高的 ROSI。

尽管成熟度最高的组织充分展现了安全投资能够成为强大的收入引擎，但不应将第 3 阶段视为安全旅程的终点。为了持续适应不断变化的安全需求，领导者需要在整个组织中另辟新径，扩展安全服务的价值，甚至扩展至生态系统中的外部合作伙伴和供应商。这样一来，他们可以有效应对新的风险向量，建立更全面的责任共担模型，并运用开放创新来实现新兴价值主张。

“增强安全投资应当成为业务引擎。安全投资应当帮助企业增加业务弹性，还应当帮助企业保护数字转型创造的生产力效益。”[14]

CrowdStrike 首席执行官 **George Kurtz**

通过共担风险、共担责任和共建弹性来释放更大的价值

从经济学的角度来看，共建弹性具有公共产品的特征 — 这是一种可广泛惠及网络经济中所有参与者的公共资源。

转变为共担责任模式标志着组织在安全战略上的重大进步。随着越来越多的组织开始将安全投资视为价值引擎而非成本中心，这种进步将日益普及。问题是：企业应当如何将共同责任转化为业务成效？

这种进步始于企业内部，主要表现就是企业最高管理层和业务线高管建立了更有效的合作关系。消除职能孤岛对于理解网络风险以及阐明协同一致的业务、IT 和信息安全战略至关重要。这样一来，企业高管就可以将安全运营提升到全新的水平。

共担责任模式还进一步涉及与生态系统合作伙伴的多边合作，其战略、风险应对方法和执行能力将形成互补。这不仅有助于增强专业能力，而且还可以充分发挥共同投资（例如，超大规模基础架构和服务）的价值。而这又有助于企业超越自身能力限制，创造更广阔的共同价值。（请参阅第 21 页的案例研究“生命科学制造商将安全投资视为业务引擎”。）

第 3 阶段的受访组织展示了成熟度最高的组织如何将能力扩展到共担责任模式之外，实现集共同价值与共建弹性优势于一体的安全框架（参见图 9）。对于此类组织，合作伙伴正在利用标准化和统一治理来扩大其共同利益。这包括建立共同的利益、知识或实践，以及跨合作伙伴运营建立标准化的事件响应程序和安全策略。

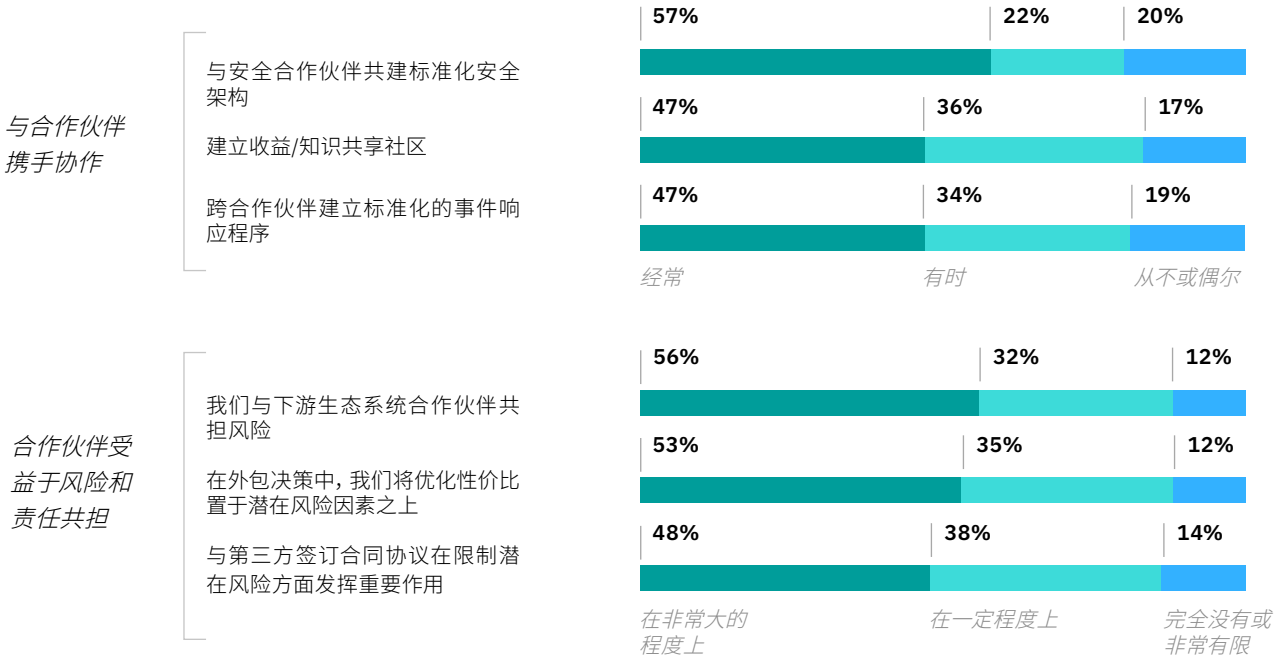
许多组织都需要通过加强协作以及增强运营整合来实现共同价值。56% 的受访高管认为与下游业务合作伙伴共担风险是最普遍的一项益处。其他益处还包括通过合同协议等方法来控制风险。此外，在选择生态系统合作伙伴时，受访高管还将性价比因素置于潜在风险因素之上。这表明，随着生态系统关系变得更加复杂，传递性风险可能会成为一个更严重的问题。

许多组织都需要通过加强与合作伙伴的协作及运营整合来创造共同价值。

图 9

将安全投资扩展至生态系统

组织更加广泛地与合作伙伴开展合作，共担风险和责任，并创造共同价值。



问：您的组织在多大程度上与合作伙伴合作实施责任共担网络安全模式？
问：您组织的网络安全投资和功能可在多大程度上惠及生态系统合作伙伴？

案例研究

生命科学制造商将安全投资视为业务引擎[15]

面对非核心职能的成本压力以及整个 IT 和信息安全产品组合的技能短缺，一家生命科学制造公司决定将其 IT 运营外包给合作伙伴。为了帮助客户在 IT 提供商与 IT 安全职能部门之间实现职责分离，该公司选择利用托管安全服务提供商 (MSSP) 作为其 IT 服务的补充，而该托管安全服务提供商可以成功与组织生态系统中的其他合作伙伴相整合。通过整合运营和统一治理，生态系统中的各方可以实现运营效益。

该解决方案的第一步是制定积极的过渡计划和相关转型路线图，旨在帮助该公司构建不断成熟的安全能力。其中包含一个提供 24x7 全天候威胁管理功能的开放平台，同时推动加速转型为新的 IT 和信息安全服务提供商。该公司建立了一个统一治理模型，可跨多个战略合作伙伴实现持续协同。

现在，通过整合安全运营和更高的安全成熟度，该公司成功改善了网络风险管理，并提高了威胁管理效率。通过运用精简化的转型方法，该公司成功扩大了成本节省，并加快了价值实现速度。通过此次转型，这家生命科学公司成功将其安全投资转化为业务引擎。

值得重点指出，第 3 阶段组织正在成功将其安全方法模型从风险价值 (value-at-risk) 转变为价值风险 (value-to-risk)，并通过组织内部的横向合作以及与外部合作伙伴之间的合作来实现风险共担，从而实现新的价值主张并有效协同运营。从安全泄漏占安全事件的比率等指标中可以看出，此类组织正在广泛联合其合作伙伴来增强整体网络弹性（参见图 10）。与其他同行相比，此类组织在一个重要方面表现出众 — 那就是此类组织将安全投资视为其整体转型计划的重要组成部分。

此类组织之所以在安全领域更加出众，一个重要原因就是更善于将机会转化为增长。它们在网络风险和生态系统合作伙伴协同方面拥有更成熟的能力，以及更高的效率、速度、专业水平和规模 — 所有这一切都得益于组织具备更高的开放水平和弹性。

第 3 阶段的组织正在保持高速发展，这主要是因为它们将安全投资视为其整体转型计划的关键组成部分。

成熟度更高的组织将安全成效视为业务成效。

这种战略转变取决于组织如何推进云转型。关键差异在于，成熟度更高的组织将安全成效视为业务成效。[16] 该组织从最初的互联服务和共享运营转变为“深度云”方法，即专注于通过业务关键价值流来改善业务绩效。如今，各种挑战和不确定性因素导致安全运营环境日益复杂。而通过转变对风险、价值和弹性的态度，企业领导者可以有效逆转这一趋势。这让他们能够优先考虑可实现最大运营和财务效益的投资。

面对日益变幻莫测的商业环境，网络经济在事实上的兴起创造了一个里程碑时刻，并且将在未来十年中产生持续而深远的影响。而积极拥抱这种全新模式的组织可以更好地把握这一未来机遇。本报告随附的“行动指南”提供了关于如何把握这一未来机遇的指导。

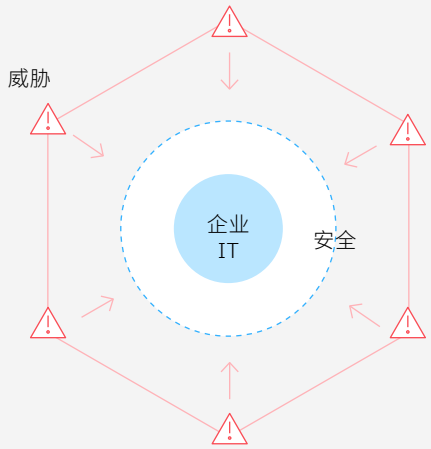
图 10

面向公共利益的安全方法

以共担责任、共建弹性和共享价值为核心的生态系统合作关系正在变革安全运营模式。

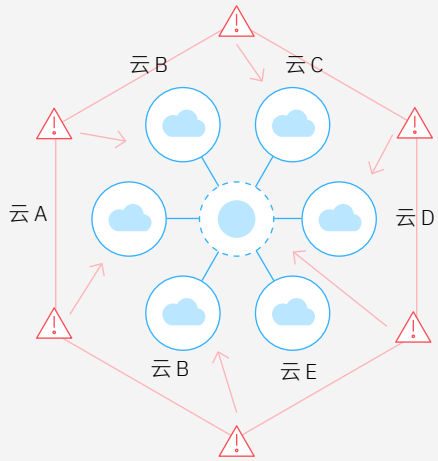
传统安全方法（前云时代）

- 企业自建安全系统来抵御网络攻击者
- 注重安全边界
- 高成本、低效能
- 协作水平较低



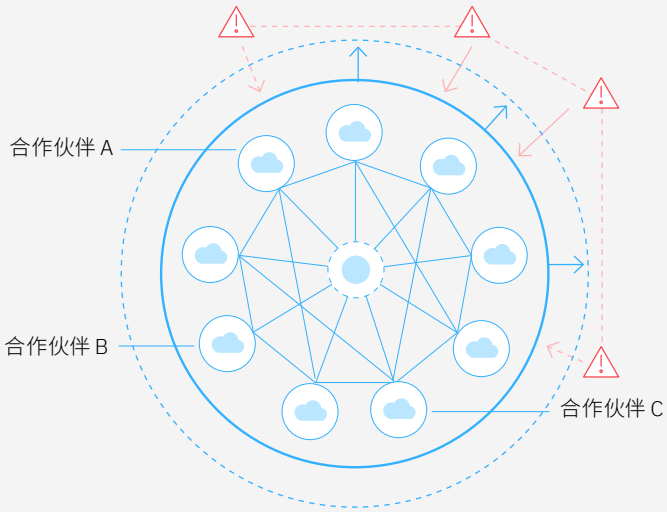
共担责任（浅层云时代）

- 一些 IT 功能迁移至不同的云并具有各自的安全态势（强于企业 IT）
- 双边安全协同
- 可提高效率并改善安全态势
- 双边方法和“锁定”阻碍了转型价值



共建弹性（深层云时代）

- 生态系统合作伙伴之间保持多边协同
- 强大的联合安全态势可主动限制攻击者的能力
- 安全方法成为共同公共利益
- 降低风险，建立开放平台，推动价值创造和转型



行动指南

针对所有阶段的一般性建议

1. 达成战略共识

- 对与组织的业务、IT、风险偏好和安全战略相关的当前安全转型路线图进行全面评估。
- 与同行企业携手合作，更深入地理解您组织的网络风险管理方法。
- 联合同行企业，加强共担责任模式，了解在哪些方面可以依靠合作伙伴来共担或转移风险。
- 着眼于共同价值，思考组织应当在哪些方面与合作伙伴开展合作，共同实现更广阔的规模经济，或者可以在哪些领域优先开展投资，从而增强专业化水平和差异化优势。

2. 消除孤岛

- 通过横向思考来增强整个组织的决策流程，请注重五个能力维度的安全成熟度，包括战略与网络风险、职能能力、安全运营模式、业务整合以及生态系统协同。
- 运用价值流评估来确定 IT 和信息安全投资组合中的哪些要素能够对整体转型工作贡献最大的价值。
- 与 IT/信息安全投资组合中的同行开展合作，通过协同业务、IT 和信息安全投资来估算共同价值池。
- 根据您的业务战略、IT/信息安全战略和风险态势，对实现预期业务成效所需的投资进行定性和量化评估。

3. 与生态系统合作伙伴共建治理和共创价值

- 积极引入内部合作伙伴，共同消除职能孤岛、提高效率以及完善战略，推动实现共同目标。将安全功能视为整个企业的横向能力，而不是垂直能力。
- 引入外部生态系统合作伙伴，积极开展开放创新，协同网络风险管理方法，并利用合作来共同实现战略目标。注重集体防御、网络弹性和纵深防御原则。

行动指南

针对特定阶段的建议

第 1 阶段

完善战略

- 调动整个组织制定转型路线图，推动将安全运营从成本中心转变为收入引擎。
- 利用广阔的高 ROI 和高 ROSI 投资机会来增强网络风险和网络安全能力，以及推动更广泛的 IT/信息安全转型。

第 2A 阶段

理解风险与回报

- 专注于增强网络风险管理成熟度。
- 继续增强运营模式和生态系统合作伙伴成熟度，同时加强业务整合与功能成熟度。

第 2B 阶段

将安全合作扩展至整个生态系统

- 利用更有效的网络风险管理来改善业务成效（例如，降低财务风险以及减少不良事件的几率）。
- 专注于增强业务整合和生态系统合作，从而提升效率以及增强规模经济。

第 3 阶段

培养把握新机遇的能力

- 请从多个维度来重新评估组织的安全战略，包括内部与外部因素、不断变化的风险状况以及业务和 IT/信息安全因素将如何创造新的挑战与机遇。
- 认识到组织仍然可以受益于不断完善的能力成熟度，并确定哪些能力可以产生最大的影响。

关于
作者

Chris McCurdy

全球副总裁兼总经理
IBM 安全服务
linkedin.com/in/chrismmccurdy/
cmccurdy@us.ibm.com

在过去 15 年以来，Chris 曾担任多个领导职位，负责指导 IBM 安全服务的销售和战略，始终一如既往地推动安全业务的快速增长。在加入 IBM 之前，他曾在 Andersen、International Network Services 和 Lucent Technologies 等多家咨询公司担任管理顾问。他还在美国的一家大型零售汽车集团担任 CIO。Chris 拥有贝勒大学信息系统工商管理学士学位，并且是一名认证信息系统审计师。

Shlomi Kramer

IBM 安全服务全球合伙人
linkedin.com/in/shlomi-k/
SHLOMIK@il.ibm.com

Shlomi 在基础设施和安全服务领域拥有超过 20 年的专业经验。他曾在多个行业开展国际性工作，协助客户简化与安全数字化转型相关的复杂业务与技术问题。多年以来，他一直担任业务领导职务，与客户和国际业务主管开展合作，帮助他们制定和执行销售转型计划，从而推动数字化转型议程。

Gerald Parham

全球研究负责人，安全和 CIO
IBM 商业价值研究院
linkedin.com/in/gerryparham/
gparham@us.ibm.com

Gerald 在 IBM 商业价值研究院负责领导安全和 CIO 研究领域。他致力于为高管和董事会成员提供技术与安全战略、网络风险和网络价值链方面的建议。Gerald 在行政领导、创新和知识产权开发领域拥有超过 20 年的经验。他拥有加州州立大学和南加州大学的科学和美术高级学位，以及约翰霍普金斯大学的写作学士学位。

Jacob Dencik 博士

全球经济研究负责人
IBM 商业价值研究院
linkedin.com/in/jacob-dencik-126861
jacob.dencik@be.ibm.com

Jacob 负责领导 IBM 商业价值研究 (IBV) 开展技术相关主题以及技术对全球经济影响的研究工作。他致力于为全球范围内的企业提供全球运营和定位战略咨询，并且拥有丰富的相关经验。他还以竞争力、外国直接投资 (FDI)、部门/集群分析和创新领域的专家和经济学家的身份向政府提供建议。Jacob 拥有英国巴斯大学公共政策和经济学专业的博士学位。

致谢

我们要感谢许多同事为本研究提供的帮助指导和支持。我们谨代表 IBV 向 Joanna Wilkins、Lily Patel 和 Kristin Biron 表示感谢。我们还要感谢 Dave Zaharchuk、Haynes Cooney、Kathleen Martin、Steve Ballou、Jana Chan 以及许多其他在编辑评审、研究部署和细部编辑方面提供帮助的同事。我们谨代表 IBM Security 向 Tanner Sandoval 和 Danielle Ivannikova 表示感谢。此外，整个 IBM Security 社区的利益相关者们在报告编制的许多阶段都提供了指导和专业知识。我们非常重视与同事之间的合作关系。

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。

相关报告

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

云安全的新时代：利用信任网络，增强网络弹性

IBM 商业价值研究院，2021 年 4 月
https://www.ibm.com/downloads/cas/LZ7MXO4M

释放混合云的业务价值：无边界企业如何推动收入增长与创新

IBM 商业价值研究院，2021 年 9 月
https://www.ibm.com/downloads/cas/QPRDPR7B

IBM 商业价值研究院

IBM 商业价值研究院 (IBV) 成立于 2002 年。凭借 IBM 在商业、技术和社会交叉领域的独特地位，IBV 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，帮助领导者做出更明智的业务决策。

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

研究和分析方法

为了更深入地理解企业对网络风险和网络安全的看法，IBM 商业价值研究院联合牛津经济研究院，针对 25 个国家/地区的 18 个行业的 2,300 多位业务、运营、技术、网络风险和网络安全高管开展了一项调研。

本研究全面分析了负责推动组织 IT 和信息安全 (IS) 转型议程的领导者的见解，包括 CEO、COO、CIO、CTO、CISO、首席风险官 (CRO)、首席供应链官、首席采购官、首席隐私官 (CPO) 和数据保护官 (DPO)，以及信息安全 (IS) 职能、网络风险管理职能和信息技术 (IT) 职能部门的高管（副总裁或以上级别）。

我们的分析侧重于安全功能对安全运营和业务成效的影响。这包括关于数据的描述性分析以及通过更详尽的分析来评估组织在五个领域的安全成熟度：

- 战略和网络风险。是否能够执行安全战略并确保控制措施与风险态势相一致
- 功能成熟度。是否能够在云安全和安全架构原则等领域打造现代化、协同一致的核心安全功能
- 安全运营模式。是否能够跨安全职能评级模型成熟度来设计、构建和编排技术、流程、技能与治理。
- 业务整合。是否能够跨核心业务职能，从战略层面扩展安全功能。
- 生态系统协同。是否能够广泛引入生态系统合作伙伴，共同设计和交付安全功能与新价值主张。

随后，我们执行了类别分析，根据这些组织在五个领域中的能力将其划分到四个不同的类别中。我们对不同类别的安全方法、安全对业务绩效的影响以及总体财务绩效进行了比较分析，从而确定安全成熟度在交付业务价值中发挥的作用。

备注和参考资料

1 “Cyber Operations and Cyber Terrorism.” US Army Training and Doctrine Command. DCSINT Handbook No 1.02. August 2005. https://nsarchive.gwu.edu/document/15676-us-army-training-and-doctrine-command-dcsint

2 Morgan, Steve. “Cybercrime to Cost the World $10.5 Trillion Annually by 2025.” Cybercrime Magazine. November 2020. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/; Upadhyay, Shailendra, Rahul Yadav, et al. “Forecast: Information Security and Risk Management, Worldwide, 2020-2026, 2Q2022 Update. https://www.gartner.com/document/4016190?ref=algobottom-rec&refval=4004647 (Access required.)

3 Payraudeau, Jean-Stéphane, Anthony Marshall, and Jacob Dencik. “Unlock the business value of hybrid cloud: How the Virtual Enterprise drives revenue growth and innovation.” IBM Institute for Business Value. July 2021. https://ibm.co/hybrid-cloud-business-value

4 “Cybersecurity is the issue of the decade: IBM chair & CEO Arvind Krishna.” CNBC. August 25, 2021. https://www.cnbc.com/video/2021/08/25/cybersecurity-is-the-issue-of-the-decade-ibm-chair-ceo-arvind-krishna.html

5 “2022 IBM CEO Study. Own your impact: Practical pathways to transformational sustainability.” IBM Institute for Business Value. May 2022. https://ibm.co/c-suite-study-ceo

6 “Cost of a Data Breach Report 2022.” IBM Security and the Ponemon Institute. July 2022. https://ibm.com/security/data-breach

7 Ibid.

8 McCurdy, Chris, Shue-Jane Thompson, Lisa Fisher, and Gerald Parham. “Getting started with zero trust security: A guide for building cyber resilience.” IBM Institute for Business Value. July 2021. https://ibm.co/zero-trust-security; Thompson, Dr. Shue-Jane, Shamla Naidoo, Shawn Dsouza, and Gerald Parham. “The new era of cloud security: Use trust networks to strengthen cyber resilience.” IBM Institute for Business Value. April 2021. https://ibm.co/cloud-security-cyber-resilience

9 Based on internal IBM client information.

10 IBM Cloud Education. “GRC.” Accessed September 27, 2022. https://www.ibm.com/cloud/learn/grc

11 Based on internal IBM client information.

12 Novet, Jordon. “Why cybersecurity stocks are beating the market.” CNBC. September 1, 2022. https://www.cnbc.com/2022/09/01/cybersecurity-stocks-are-beating-the-market-in-a-volatile-economy.html

13 Definition “defense-in-depth.” National Institute for Standards and Technology Computer Security Resource Center. Accessed September 23, 2022. https://csrc.nist.gov/glossary/term/defense_in_depth

14 Columbus, Louis. “CrowdStrike’s platform plan at Fal.Con melds security and observability.” VentureBeat. September 26, 2022. https://venturebeat.com/security/crowdstrikes-platform-plan-at-fal-con-melds-security-and-observability/

15 Based on internal IBM client information.

16 “The deep cloud alternative: Getting to the heart of business performance.” IBM Institute for Business Value. August 2022. https://ibm.co/deep-cloud

© Copyright IBM Corporation 2022

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 | 2022 年 11 月

IBM、IBM 徽标、ibm.com 和 Watson 是 International Business Machines Corporation 在世界各地司法辖区的注册商标。其他产品和服务名称可能是 IBM 或其他公司的商标。以下 Web 站点上的“Copyright and trademark information” 部分中包含了 IBM 商标的最新列表：ibm.com/legal/copytrade.shtml。

本文档为自最初公布日期起的最新版本，IBM 可能随时对其进行更改。IBM 并不一定在开展业务的所有国家或地区提供所有产品或服务。

本文档内的信息“按现状”提供，不附有任何种类的（无论是明示的还是默示的）保证，包括不附有关于适销性、适用于某种特定用途的任何保证以及非侵权的任何保证或条件。IBM 产品根据其提供时所依据的协议条款和条件获得保证。

本报告的目的仅为提供通用指南。它并不旨在代替详尽的研究或专业判断依据。由于使用本出版物对任何企业或个人所造成的损失，IBM 概不负责。

本报告中使用的数据可能源自第三方，IBM 并未对其进行独立核实、验证或审查。此类数据的使用结果均为“按现状”提供，IBM 不作出任何明示或默示的声明或保证。

扫码关注 IBM 商业价值研究院

官网　微博　微信公众号　微信小程序

YLGDAMVR-ZHCN-00