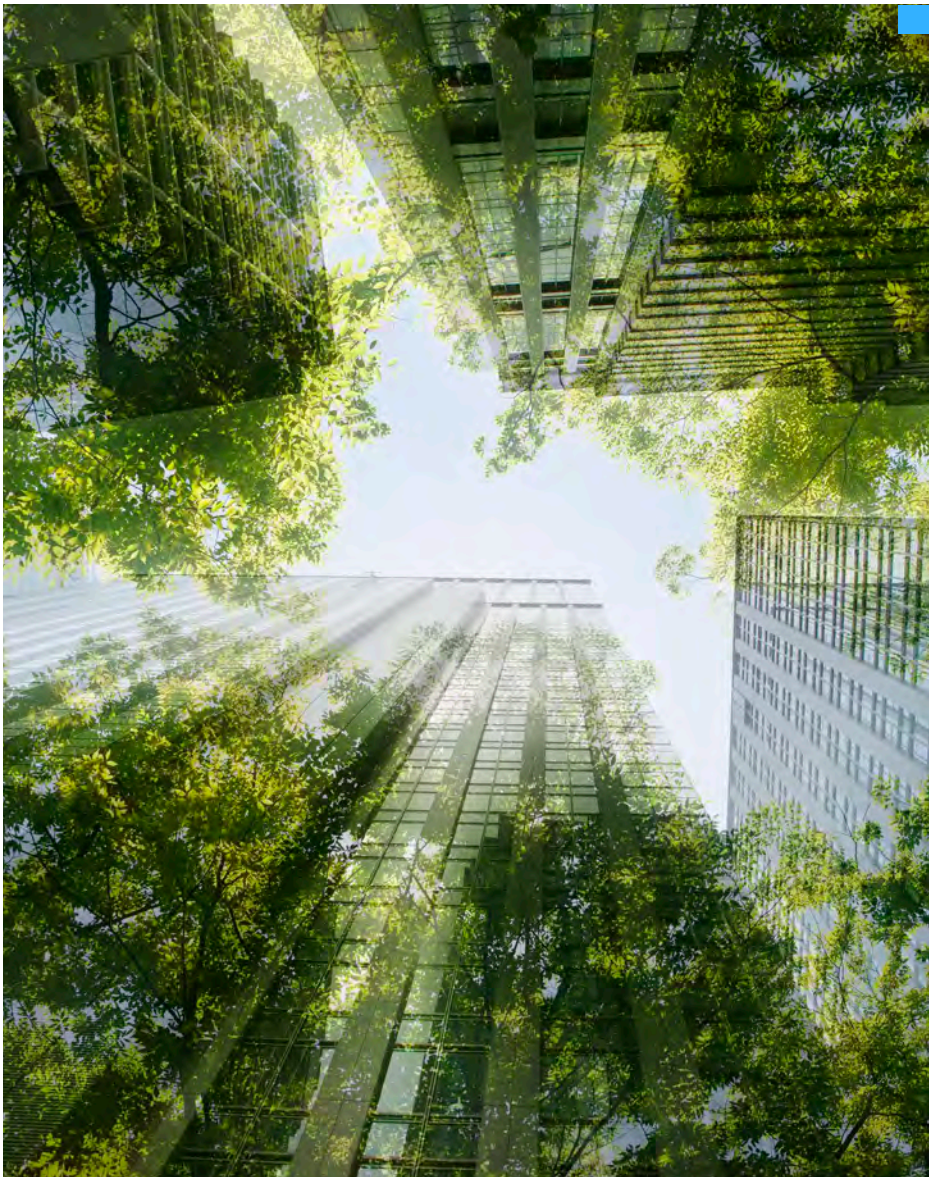


网络经济时代的发展繁荣之道

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。

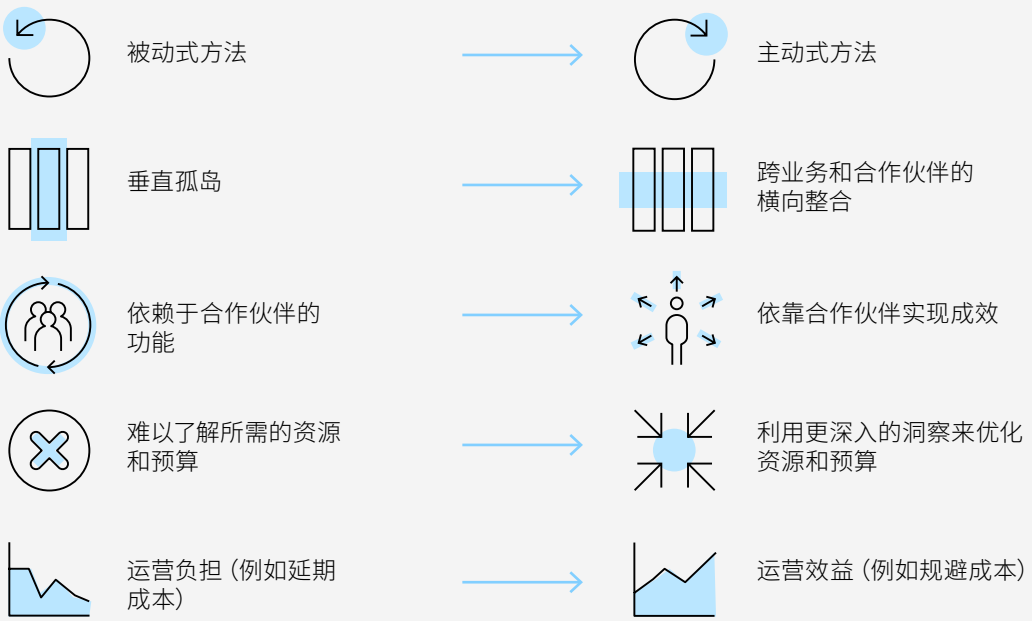
为了更深入地理解企业对网络风险和网络安全的看法，IBM 商业价值研究院 (IBV) 联合牛津经济研究院，针对 25 个国家/地区的 18 个行业的 2,300 多位业务、运营、技术、网络风险和网络安全高管开展了一项调研（参见第 28 页的“研究和分析方法”）。

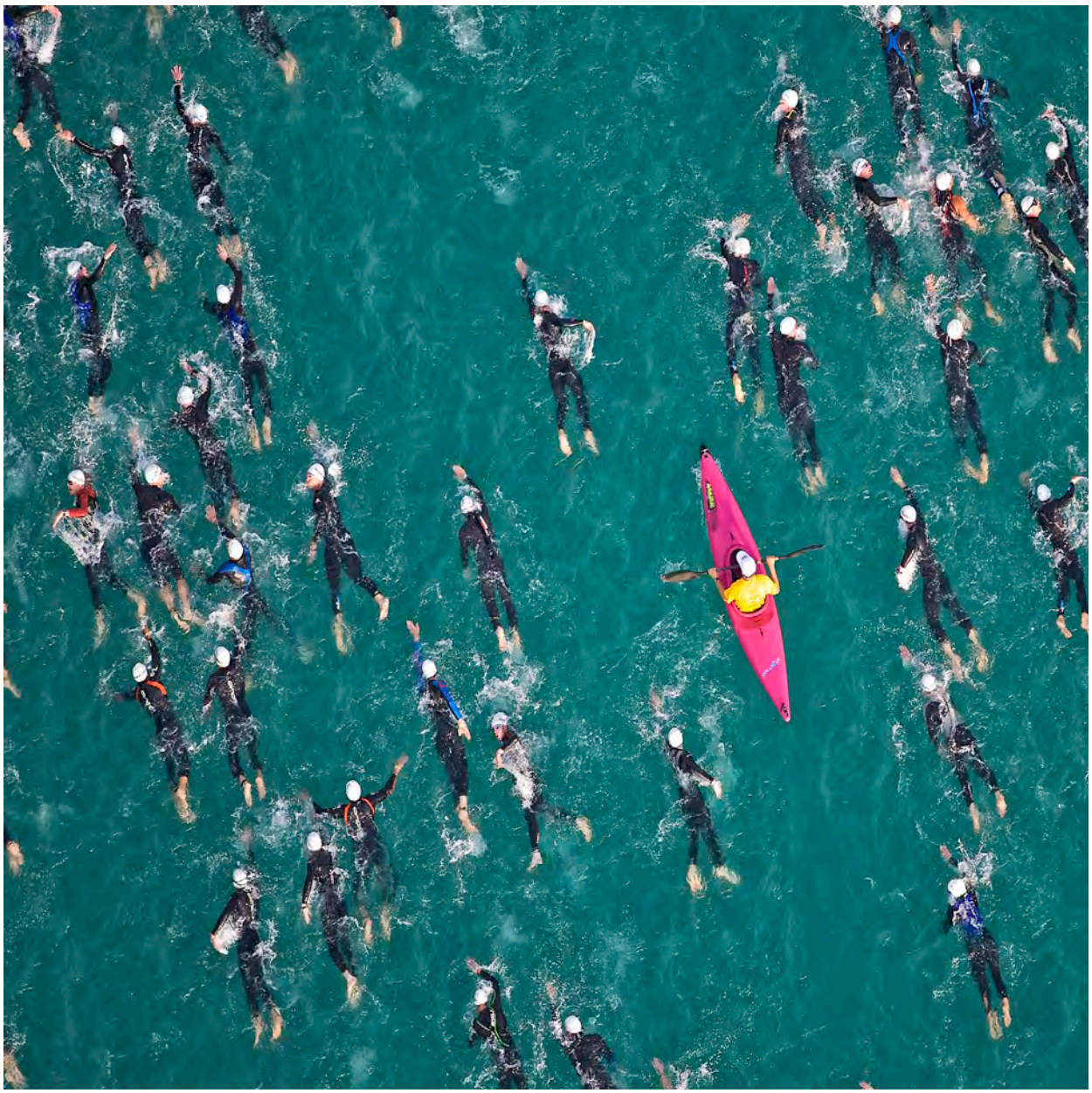
这项研究从迄今为止最全面的视角，深入分析了负责推动企业 IT 和信息安全 (IS) 转型议程的高管的独到见解。这些研究结果描绘了一幅令人信服的画面 — 网络安全正在成为一种核心战略能力，可帮助企业降低财务风险、提高运营效率以及发掘新的价值来源。

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