KPMG
毕马威

# 2025网络安全重要趋势

在由 AI 主导的商业环境中，网络安全的基本原则正变得愈发重要

毕马威国际

kpmg.com/cyberconsiderations

# 目录

# 前言

随着2025年的到来，数字环境以前所未有的速度持续演变，在带来新挑战的同时，也放大了企业对采取强有力网络安全措施的迫切需求。在此背景下，第六期年度《网络安全重要趋势》的全球发布揭示了各行业组织目前及即将面临的挑战，并强调其可采取的几项战略举措。这些举措均与本报告中深入探讨的八项关键网络安全重要趋势一致。

在科技深度渗透职业和日常生活方方面面的当下，网络安全已不仅仅是企业关注的问题，更成为了影响社会各方面的广泛议题。根据毕马威的研究，首席执行官们认为网络安全是过去十年中的首要威胁。[1]

人工智能（Artificial Intelligence，简称AI）在几乎所有工业领域的应用揭示了在AI模型和流程中嵌入信任的紧迫性，即通过建立一个全面而稳健的治理计划，使首席执行官能够借此了解各种商业案例，确定AI在组织中的使用范围和方式，并识别相关的漏洞。

智能产品的普及，从汽车和医疗器械到家用电器及其他与物联网相关的设备，持续扩大了网络攻击面，并以前所未有的方式将物理威胁和数字威胁相结合。深度伪造技术的兴起，以及加密货币等数字资产的复苏（此类资产仍基本处于无监管且波动性高的状态）进一步加剧了这些威胁的复杂性，要求人们提高警惕并采取创新对策。

在此环境中，首席信息安全官亟需专注于自身及团队对AI技术的学习，不仅要组建最佳团队，还要理解每个应用场景所带来的独特风险。至于人才招聘和开发，首席信息安全官面临着艰巨任务，即组建能够理解AI复杂性及其潜在风险的团队——由于该领域的快速创新以及整个企业中出现的难以管理的“影子AI”，这项任务变得更加复杂。

与此同时，网络安全能力的合理化或整合也已经提上日程，安全团队正在从其安全运营中心（SOC）中的数十种解决方案转向一套精简的最佳工具套件，以更有效更经济地集成解决方案，并持续利用这些工具提供商提供的新AI能力。

今天的网络安全挑战远超传统技术技能的范畴，需要采用跨学科的方法，涵盖对风险管理的深刻理解，以及问题解决、批判性思维和沟通等软技能。网络安全专业人士可以来自非传统背景，并且必须能够迅速适应并掌握超出计算机科学、软件工程或信息技术等传统学位培训通常教授的知识。[2] 对于网络安全专业人士而言，优先进行情境风险评估至关重要，但同时不能忽视明确且灵活的控制措施的需求。

1 毕马威《2024年全球首席执行官展望》（KPMG 2024 Global CEO Outlook），2024年8月。

2 世界经济论坛，《战略性网络安全人才框架》（Strategic Cybersecurity Talent Framework），2024年4月。

网络安全并非静态功能，而是一个动态且不断演变的挑战。例如，量子技术的崛起，攻击者可以通过量子计算以惊人的速度绕过加密工具，可能会破坏从银行和零售交易到商业数据、文件、电子邮件等的一切；“超级智能”AI系统的潜力，该系统能持续完善和扩展知识，并在感知危险时自我保护；以及虚假信息的传播速度，尤其是通过深度伪造的音频和视频内容的传播——这些正是导致首席信息安全官夜不能寐的新兴问题。这些威胁和其他威胁也凸显了对创新和战略远见的迫切需求。

立法环境正在向更本地化的监管方向转变，这给全球安全运营带来了多方面的挑战。这一点，再加上经济上迫切需要不仅以投资回报为基础，而且需要以缓释风险为基础来证明安全预算的合理性，使首席信息安全官处于在没有预算保证的情况下使用安全资源的危险境地。

首席信息安全官还面临日益复杂的地缘政治局势的挑战。随着国家支持的网络攻击、监管环境的变化以及跨境数据流动的不断增加，首席信息安全官必须在错综复杂的局面中有效保护企业网络。

显然，提前应对新兴威胁并确保合规的压力比以往任何时候都更加严峻。

当今首席信息安全官的广泛经验——无论是经历过重大安全事件的人，还是仅经历过小规模安全冲突的人——都强调了对动态威胁环境进行细致评估的必要性。

在本报告中，毕马威专家更深入地探讨了这些问题，提供了对当前网络安全状况的全面分析，并为首席信息安全官提供了与八项网络安全重要趋势相契合的实际策略。我们的目标是为领导者提供能够应对数字时代复杂性的知识和工具，以应对数字时代的复杂性，确保他们的组织在充满魅力和激动人心、但往往不确定的未来中保持安全和韧性。

**Akhilesh Tuteja**
网络安全全球主管
毕马威国际

> “技术格局正在迅速演变，新的威胁每天都在涌现。为了保持领先，企业必须积极主动，而不是被动应对，以保护其数字资产、确保合规性，并营造一个安全且有利发展的环境。”

**Bobby Soni**
全球技术咨询主管
毕马威国际

# 五年回顾 2020–2025

过去五年间，本报告的编写始终以不断演变的网络安全格局为核心，如今这一核心也已成为组织领导者的切实关注点。此外，许多关键主题持续引起共鸣——韧性、身份访问管理（IAM）、云安全、人才与技能缺口等，不一而足。

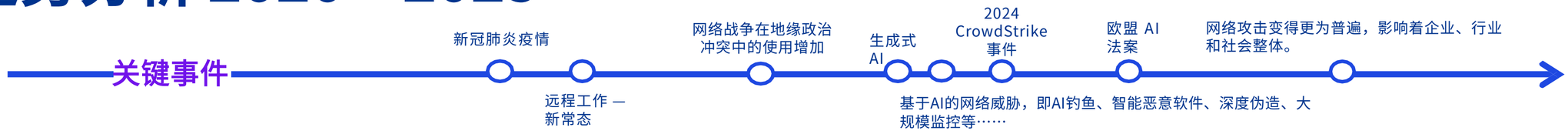
然而，这一关键领域的底层逻辑已经从传统的网络安全措施转向了全球多维数字景观中的优先事项和挑战，首席信息安全官及其团队必须近乎实时地对此作出响应。最重要的是，必须强调网络安全的普遍性，它已经超越了技术风险，涵盖了更广泛的企业威胁，影响着各行各业和社会。

让我们更深入探讨一下：

- 随着新冠肺炎疫情的暴发以及远程工作安排的常态化，云安全和AI安全已成为首席信息安全官的关键目标。
- 人才以及始终存在的技能缺口，长期以来一直至关重要，因为新兴技术的应用和发展，要求人才具备新的、多样化的技能。
- 身份管理的转变，从传统的IAM（一个重要但独立的功能）转移到了零信任战略的核心，涵盖数字身份验证和深度伪造识别。
- 韧性已成为一个核心目标，并将继续保持这一地位。
- 首席信息安全官持续努力强化网络安全措施，尤其是随着网络威胁转变为影响广泛的业务威胁，这些威胁有可能扰乱行业并危害社会。

**从下一页的趋势分析（2020-2025年）可以看出，许多基本的网络安全基础仍在当前研究中占据核心地位。但面对新技术、新的监管要求、更复杂的工具以及日益严峻的威胁态势，首席信息安全官的职责范围和责任正在显著加大。**

# 趋势分析 2020 – 2025




关键主题

| | 2020 | | 2025 |
|---|---|---|---|
| **战略与领导力** | • 首席信息安全官已成为值得信赖的内部顾问和运营领导者。 | • 将对话从成本和速度转移到战略性及有效的网络安全。<br>• 首席信息安全官的预算越来越与降低业务风险挂钩。 | • 随着网络安全在组织内部变得更加普遍，首席信息安全官面临的交付压力也在增大。<br>• 首席信息安全官的角色分散了，但问责制却因监管发展而增加。 |
| **人员与人才** | • 网络安全团队正在转型，成为战略决策桌上拥有重要话语权的关键资源。 | • 网络安全的存在是为了支持组织，而不是阻碍——从组织执行者到影响者。<br>• 将网络安全纳入组织结构中。 | • 网络技能差距依然存在——AI可能会提供一些可行的解决方案，但劳动力仍需要掌握和应用新的技能。 |
| **技术与数据** | • 新的虚拟基础设施模型和协作工具。<br>• 加速的云转型（由于 COVID-19），但网络安全问题被置于次要地位。<br>• 传统身份认证与管理（IAM）。 | • 通过自动化增强网络安全。<br>• 生成式AI 的快速发展给网络安全创造了活力。<br>• 保护一个无边界的以数据为中心的世界。<br>• 将身份置于零信任的核心。 | • 对网络AI的投资变得更具战略性和前瞻性。<br>• 企业范围的成本节约、效率、安全和创新（尤其是AI实施）推动了平台整合。<br>• 数字身份和深度伪造的兴起。 |
| **数字信任** | • 网络安全和隐私法规聚焦于业务优先事项和责任，以及信任的重要性。 | • 数字信任是一项共同责任，始于业务本身，并涉及多个利益相关者，例如：CISO、DPO、CDO、CIO 等等。 | • 在AI中嵌入信任并渗透到商业和社会的所有结构中-重点关注网络安全、隐私、物理安全、道德等。 |
| **韧性** | • 从基于场景到基于影响——重点关注批判性和监管。 | • 不再仅仅是预防——重点在于响应和恢复。 | • 首席信息官继续加强组织韧性，因为网络威胁已经从技术风险演变为企业和行业威胁，并对社会造成潜在的危害。 |

# 2025年八大关键网络安全重要趋势

**点击每个趋势以了解更多信息。**

01

### 首席信息安全官（CISO）职责持续演变

随着网络安全职能在组织内更广泛地嵌入并被深入理解，CISO及其团队的工作重点，以及与组织其他部门的协作模式将持续演变。

02

### 网络安全人才管理至关重要

面对数字化转型压力，组织普遍面临工作负荷激增的挑战，使得网络安全人员能力差距被放大。尽管AI与自动化技术可提供支持，但团队仍会面临无法解决的问题，存在人员流失风险。

03

### 构建可信人工智能

AI技术虽已与各类组织职能有了良好的结合，但其自身面临的网络安全与隐私保护风险，仍会能影响AI技术的全面推广。

04

### 驾驭AI赋能网络安全：快速前行与安全并重

从技术培训缺失到对新兴技术落后的担忧，多重因素都在推动AI应用热潮。其中一个关键挑战在于找到AI在网络安全与隐私管理领域中的潜在收益与风险的平衡点。

05

### 安全管理平台整合：平衡风险与收益

为降低技术复杂性与成本，全球企业正加速整合安全工具与服务至单一或有限平台，但需同步识别并规避集中化衍生的固有风险。

06

### 数字身份安全管理迫在眉睫

尽管全球数字身份计划加速推进，但系统互操作性仍受深度伪造技术威胁掣肘，且生物识别数据处理面临监管差异与公众信任挑战。

07

### 智能设备的“智能”安全防护

智能设备与产品的普及正颠覆传统安全范式，推动监管机构建立新制度以确保产品满足基础安全要求。

08

### 构建企业韧性：网络安全护航企业和社会安全

韧性正成为CISO议程的核心，因为攻击者使用勒索软件或其他恶意手段造成大规模工业中断的可能性仍然令人担忧，这不仅危及数据，也危及人类生命。

# 重要趋势 1

# 首席信息安全官（CISO）职责持续演变

多重因素正在重塑网络安全格局，并显著转变首席信息安全官（CISO）的角色。监管审查的加强、近乎零失败的交付压力、以及问责制和个人风险的增加，共同推进了这一角色的转变。与此同时传统的首席信息安全官职能正逐渐分散到组织各处，这引发了人们对于该角色未来定位和网络安全职能演变的思考。首席信息安全官的成功很可能取决于其能否有效建立决策权威 、管理新兴技术特别是AI的影响，以及能否适应新威胁。

### 运营模式演变下的更高期望

首席信息安全官（CISO）的角色正变得越来越复杂。监管审查以及确保整个组织具有强大的网络安全成果的需求是主要驱动因素。这种复杂性进一步因运营模式的变化以及对外部供应商依赖的增加而加剧。然而，现有的网络安全控制措施可能并不总是与组织的独特需求相符合，特别是在涉及跨越多个国家的全球运营的情况下。

首席信息安全官现在面临着管理并配置供应商提供的网络安全控制措施的挑战，他们需要确保这些控制措施符合目的并遵守当地法律法规。运营模式的转变意味着首席信息安全官对网络安全措施实施的直接控制力减弱。虽然这些供应商提供的嵌入式网络安全和隐私控制可能有益，但它们通常缺乏首席信息安全官有效管理跨多种环境风险所需的灵活性和细致程度。首席信息安全官们必须在应对这种复杂性的同时，确保员工高效工作，并保持对组织内控制操作的可视性。

> “当谈到基于云软件供应商时，情况会更加复杂，因为其控制措施通常是二元化的——要么使用要么不使用。理想情况下，首席信息安全官希望根据情况或地理位置灵活调整控制措施的开关——在美国开启，但在德国关闭；在新加坡开启，但在瑞士关闭。”
>
> **Paul Spacey**
> 全球首席信息安全官
> 毕马威国际

## 设计网络安全的组织角色和范围的蓝图

围绕CISO职位的组织结构正在演变，越来越多的趋势是如果公司设有技术信息安全官（TISO），则会将其职责与CISO分开。这种角色划分使CISO能够专注于风险管理及更广泛的网络安全规划。TISO通常嵌入在组织的技术职能中，负责监督相关控制措施的实施并管理日常运营。

此外，较大的组织可能拥有多名CISO，每位负责不同的业务线，如供应链网络或商业线上平台。这种职责划分是因为单一角色可能难以在精通所有领域细节的同时有效管理整体网络安全态势。

随着网络安全领域的不断扩大，首席信息安全官（CISOs）发现自己承担了更广泛的职责范围。他们必须成为包括控制、性能、风险、情报、身份管理以及整体网络安全等各个方面的事实来源。首席信息安全官 被要求以对企业相关且易于理解的方式呈现这些信息，从而支持管理层做出明智的决策。

虽然首席信息安全官（CISO）可以将许多安全优先事项委托给其他团队，例如报告关键风险指标、运行风险评估和执行渗透测试，但他们仍必须保持对这些活动的监督和了解。CISO面临的挑战是：如何在扩大职责范围的同时，确保组织的敏捷性、效率和态势感知能力。

## 走钢丝：在日益增长的风险面前平衡责任与权力

日益增加的监管审查和个人责任的风险突显了为首席信息安全官（CISO）明确界定责任和决策权的必要性。如果发生网络安全事件，CISO 可能会发现自己面临法律和专业后果，尤其是在受到严格监管的行业中。

为降低这一风险，组织必须建立正式的治理流程，赋予首席信息安全官（CISO）在事件发生时采取必要行动的权力，避免因犹豫而延误响应。这包括向CISO明确说明他们的权限以及他们可以操作的范围。有了这些，他们可以迅速而自信地做出关键决策。

CISO的汇报线也决定了有效管理网络安全风险的能力。虽然与高管层、总法律顾问和董事会直接沟通很重要，但CISO仍需基于技术专长保有自主决策权。

在紧急情况下，如供应链遭到破坏时，CISO需有权立即采取行动，而无需等待缺乏技术背景的上级批准。然而，这种自主性必须与

高层共同定制的明确的问责制和约束机制相平衡。首席信息安全官（CISO）应在评估网络安全事件的关键时刻综合思量，充分考虑潜在后果，并评估确定最有效的行动方案。

> “过去，CISO的首要任务是识别并保护组织的‘皇冠上的明珠’——关键数据、知识产权，商业秘密等。但如今，CISO必须聚焦于业务的网络安全和韧性。”
>
> **Wendy Lim**
> 合伙人，网络安全，咨询
> 毕马威新加坡

## 重塑未来的CISO行动指南

随着组织越来越多地采用自动化和 AI 技术，CISO 的角色预计将经历重大变化。安全运营中心（SOCs）的自动化程度不断提高，预计将导致团队规模缩小，对日常运营的关注减少。网络安全职责的庞杂性迫使企业拆分职能，CISO 将难以有效地监督技术交付团队、管理能力、解读控制信号以及处理报告、数据工程、人员管理、外联和培训等各个方面的工作。这种繁重的工作量可能会使他们在岗位上陷入困境，最终无法正常履职。

因此，首席信息安全官（CISO）需将注意力扩展到其他关键战略领域。随着生成式 AI 在各行业的迅速采用，CISO 可以在确保组织理解和缓解相关风险方面发挥关键作用。他们需要更具战略性和前瞻性，在 AI 项目的早期阶段介入，向业务部门解释潜在风险并提出必要的缓解措施。

总之，首席信息安全官需要确定如何利用 AI 更好地保护公司、员工和客户，并在AI模型中嵌入针对性的网络安全措施。毕马威研究发现，64% 的全球CEO表示无论经济情况如何都将持续投资AI。[3]

在未来，CISO很可能需要持续地在组织的其他领域之间进行权衡，平衡董事会、业务、技术管理人员以及他们自己管理内在风险的需求。这要求 CISO必须成为精明的利益相关方管理者，能够驾驭复杂的关系并有效传达网络安全优先事项的重要性。

为了实现这一目标，首席信息安全官（CISO）可以考虑在关键业务职能内嵌入安全人员，推动安全文化与优先事项的全局对齐。通过培养全局视角，CISO可以为董事会提供高价值洞察，并确保网络安全融入组织的核心结构中。

还有就是许多监管机构关注的韧性目标。韧性要求企业梳理关键业务流程及应对事件的系统性能力，而非仅靠CISO一键启动响应那么简单。

正因如此，企业开始拆分职责。公司意识到，要想实现高效运营不能只依赖于某一个人。整个安全团队必须全天候保护企业，但攻击者只需要一个漏洞就能突破防线。

显然，这是一场不公平的战争，要想赢得胜利，必须依赖企业多部门的协同作战。CISO可能是最佳指挥官，但他们绝非孤军奋战。

> “网络安全已经成为一个高度分工与协作的工作。尽管如今的首席信息安全官（CISO）与业务各部门密切合作，但他们必须用统一的方式来管理风险，同时支持组织的商业利益。”
>
> **Oscar Caballero**
> 合伙人，网络安全负责人
> 毕马威墨西哥

3 毕马威《2024年全球首席执行官展望》（KPMG 2024 Global CEO Outlook），2024年8月。

# 建议行动

随时了解法规变化，与董事会沟通，明确职权范围，以降低个人责任风险。

为由于 AI 自动化和转向基于云的服务而演变的首席信息安全官（CISO）角色做好准备。

牵头讨论采用AI等颠覆性技术，解释风险及缓解措施。

继续在 DevSecOps 过程中通过设计构建安全性，并且将专注于网络安全的团队成员嵌入到业务功能中。

随着个人数据与企业数据在基于云和AI服务之间的界限变得模糊，需对第三方供应商进行全面的尽职调查，以确保他们的合同义务清晰且与其组织的整体数据治理框架一致。

> “从根本上说，降低攻击概率始于对环境的理解。你无法保护你不了解的东西。CISO必须了解整个网络安全状况：组织的关键业务应用程序和服务、公开暴露的资产、现有控制措施、主动防御策略、安全态势以及攻击者常用手段等。所有这些都是基础。只有这样，他们才能确定如何减少坏事发生的几率。”

**Lou Fiorello**
副总裁 — 安全产品
ServiceNow

# 了解更多



# 重要趋势 2

# 网络安全人才管理至关重要

在网络安全领导层面临的一系列挑战中，人才技能缺口尤为突出。人力因素仍然是对抗网络威胁中最关键的因素。新技术的复杂性以及威胁的快速演变，正加剧本已严峻的技能缺口。为了应对这些挑战并保障其数字资产，组织必须采取全面策略，认识到人在构建韧性网络安全生态系统中的核心作用。赋能人才所需的工具，培养强大的网络安全文化，优化AI的使用，以及强化人才输送管道均是一些可行的解决方案。

## 解决网络安全技能缺口和人才留存问题

根据世界经济论坛的数据，超过一半（52%）的公共组织表示缺乏资源和技能不足是创建有效网络韧性的最大挑战。[4] 许多报道都围绕着经验丰富的网络安全人才短缺和技能缺口问题，网络安全岗位的流失率比其他职位高出近8个百分点，使得团队的稳定性难以维持。[5] 在现阶段，网络安全作为一门职业在迅速发展，对拥有专门知识人才的持续需求，已经远超教育机构培养足够合格候选人的速度。[6]

技术技能与非技术技能的割裂日益明显。虽然强大的技术能力仍然是核心关键，但沟通能力、解决问题能力、适应力和协作等非技术技能对于隐私、风险和合规专业人士而言愈发重要。为了应对这一差距，行业领导者需优先实施综合性培训计划。

人才保留是另一关键挑战，近期的毕马威安全运营中心（SOC）调查显示，近半数（47%）的安全领导者在留住优秀员工方面存在“重大问题”。[7]

随着对经验丰富的网络安全专业人士的需求持续超出供给，CISO必须制定策略吸引和保留多元化人才。这需要与人力资源（HR）合作，了解并满足多个代际员工的独特需求。

例如，职场中最年轻且增长最快的Z世代与千禧一代，他们尤为重视工作与生活的平衡、认可度以及职业发展机会。[8] 组织可通过提供灵活的工作安排、清晰的职业路径和发展专业技能的机会，为网络安全人才创造一个更具吸引力的工作环境。

包容性、多样性和公平性（IDE）倡议也将有助于解决网络安全人才短缺问题。积极鼓励和支持女性与多元群体参与网络安全，有助于组织拓宽人才池，并受益于独特的视角和创造力。然而，仅仅促进多样性是不够的；雇主还必须创造支持性和包容性的环境，使多元化的员工能够茁壮成长，特别是那些处于神经多样性谱系上的人群。

4 世界经济论坛，《战略性网络安全人才框架》白皮书（Strategic Cybersecurity Talent Framework white paper），2024年4月。
5 STI Group，《美国网络安全就业状况：分析增长、需求和留存挑战》（The State of US Cybersecurity Employment: Analyzing Growth），2024年4月5日。
6 毕马威, Matthew Miller, 关于SOC网络安全人才缺口的应对措施（Addressing the Cybersecurity Talent Gap in the SOC）, LinkedIn, 2024年8月1日。
7 毕马威网络安全调查，《安全运营中心领导者视角》（Security Operations Center Leaders Perspective），2024年4月。
8 Paychex,《驾驭新劳动力：在职场上吸引千禧一代和Z世代》（Navigating the New Workforce: Engaging Millennials and Gen Z in the Workplace），2024年4月23日。

## AI 是网络安全的核心组成部分，而不是简化因素

尽管许多组织仍处于 AI 技术应用的早期阶段，但随着网络犯罪分子越来越多地转向 AI 来增强其攻击策略，首席信息安全官(CISO) 应该探索如何安全负责地将AI整合至网络安全战略中。为了保持领先地位，AI赋能的领域（如实时威胁检测、快速事件响应和预测建模）应成为主要关注点。

AI也可以帮助缓解人员短缺的压力。在大多数情况下，AI将成为安全团队弥补技能缺口的真正助力——而非取代人类。根据毕马威 SOC 调查，至少六成的安全领导者认为 AI 是网络安全功能的“游戏规则变革者”，包括身份和访问管理、威胁检测与响应以及边界监控。[9]通过使用 AI 自动化处理常规任务，组织可以显著提高效率，使网络安全团队能够专注于更复杂、更具战略性的网络防护任务。

人为监督在AI的应用过程中发挥关键作用。CISO应确保他们的团队接受充分培训，以便与 AI 系统协同工作，理解其能力、局限性和潜在偏见。AI 也是工作场所中的焦虑来源，因此，与AI达成共识并信任AI将是进步的关键。根据毕马威的研究，超过四分之三的组织（78%）担心团队仍然认为 AI 是一个神秘的“黑盒子”。几乎同样多的人（77%）预计 AI 将引起操作挑战，导致岗位缩减并引发伦理问题。[10]

但我们相信，人类的直觉、创造力和情境理解力与AI的速度、可扩展性和数据分析能力的结合将共同构建一个更具韧性的网络安全生态系统。

为了更好地理解这种关系，毕马威与麻省理工学院（MIT）合作研究了网络安全文化、其挑战以及AI可以产生的影响。[11] 虽然许多组织在建立网络安全文化的旅程中仍处于早期阶段——尤其是在利用AI来支持这一方面——但在毕马威和麻省理工学院的一项定量调查中，74%的受访者同意建立以网络安全为中心的文化是企业范围内成功整合AI的核心。[12]

## 从意识至行动：培育主动型网络安全文化

当组织内的每个人都积极参与有效管理网络风险时，才会建立强大的网络安全文化。首席信息安全官（CISO）必须认识到，人类并不是网络安全中最薄弱的环节，当员工充分参与到网络安全建设中时就会成为组织最强的网络防御能力。如果不在整个组织中优先嵌入风险规避文化，那么主动识别风险的重担就完全落在了网络安全团队的肩上。这不仅不可持续，也会使组织容易受到潜在安全漏洞的威胁。

为了建立一个真正具有弹性的网络安全生态系统，CISO必须专注于弥合安全团队与更广泛员工队伍之间的差距。

这包括积极与团队成员和高级领导层互动，教育他们了解网络安全的重要性，并赋予他们保护组织数字资产的责任。

充分动员员工并形成对网络风险的共同理解可以转变整个组织处理网络安全的方法。因此，网络安全不仅是一个独立的功能，更是一种集体责任。这要求首席信息安全官（CISO）成为能够连接技术与非技术利益相关者的领导者。

> “人们应该认为网络安全的存在不应成为中断业务运营的障碍或减速带，而应快速、安全地解决问题，并与内部和外部利益相关者建立信任。”
>
> **Breah Sandoval**
> 首席网络安全与技术风险总监
> 毕马威美国

9 毕马威网络安全调查，《安全运营中心领导者视角》（Security Operations Center Leaders Perspective），2024年4月。
10 毕马威《2024年全球首席执行官展望》（KPMG 2024 Global CEO Outlook），2024年8月。
11 毕马威与麻省理工学院斯隆管理学院网络安全联合研究，2024年9月。
12 毕马威，《新时代的网络安全文化：如何利用 AI 促进安全的工作行为》（A new age of cybersecurity culture: How to harness AI to promote secure workplace behaviors），2024年12月。

为了创建一个对用户更友好且高效的网络安全环境，首席信息安全官应采用以人为中心的设计方法来评估和优化安全流程。这意味着识别并解决那些让员工感到沮丧或困扰的具体流程。许多此类问题可能导致生产力下降以及违规风险增加。通过仔细分析这些流程，首席信息安全官可以确定哪些控制措施对于保护关键资产是必不可少的，哪些可以简化、合理化甚至取消。

通过这种方法，首席信息安全官 可以为员工创造一个更直观且干扰更小的安全体验，从而培养合规文化和共同责任感。这有助于提升员工对网络安全的积极认知，并鼓励员工成为主动参与者。从更广泛的网络人力资源管理角度来看，首席信息安全官 可以发挥至关重要的跨职能协调作用，衡量员工的安全知识、态度和行为，揭示以人为中心的风险潜在驱动因素，并将网络安全从限制性功能转变为一种关键能力和业务推动力。

## 政府和企业间的合作可以支持网络作为一项职能，并促进其作为职业的发展

除了弥补当前的技能缺口，政府、学术机构和组织应合作推广网络安全作为有吸引力的职业选择。[13]

这一努力应尽早开始，吸引初中及以下的年轻群体——尤其是女生——但也应包括那些正在开启第二职业或重新进入职场的男女，以展示可供选择的多样机会。

政府可以通过投资网络安全教育项目、提供奖学金和实习机会，并与行业合作提供实践学习经验来支持这一倡议。让孩子们从青少年时期就开始接触网络安全，并通过活跃的生态系统激发其对网络安全的兴趣，从而鼓励更多人投身这一关键领域。

除了早期教育和意识提升外，政府和行业领袖还需共同开发个人进入网络安全劳动力市场的非传统路径。

虽然传统的计算机科学及相关领域的大学学位仍然很有价值，但它们往往无法跟上迅速变化的威胁环境以及岗位所需的特定技能。

对此，投资于短期认证项目和专项培训课程有助于快速提升技能和重新培养来自不同背景的专业人士。通过一个更加灵活和包容的人才供应链，建立一支更强壮、更有韧性的网络安全队伍，以应对未来的挑战。

> “我们面临的最大网络挑战和脆弱性不再主要存在于代码、系统、或者数字通道中，而在于日常管理并操作这些网络的人员。他们需要支持、培训和培养，以掌握他们所需的技能和防御能力来保护我们的数据和系统。”

**Dominika Zerbe-Anders**
网络安全风险合作伙伴及解决方案负责人
毕马威澳大利亚

13 世界经济论坛，《为什么弥合网络安全技能差距需要协作方法》（Why closing the cyber skills gap requires a collaborative approach），2024年7月23日。

# 建议行动

认识到CISO的角色从单一的网络防御者扩展到风险管理师、政策倡导者和影响力推动者。需要培养和提升沟通与影响能力，以有效地传达网络安全的重要性，并推动各层级和各部门的变革。

开发并部署超越传统做法的持续培训项目方法，利用创新和沉浸式的技术（如模拟演练）来推动员工行为可持续性变化。

实施以人为中心的风险降低策略，专注于解决网络安全中的人为因素，因为人为因素占了四分之三的网络入侵。[14]

通过让员工参与网络安全倡议，提供适当的教育，并营造一种认可他们作为组织最强网络防御能力的角色的文化，来增强员工的能力。

投资于 AI 技术以衡量、量化和跟踪人为风险，从而实现更有效的风险管理，并与不断演变的威胁格局保持一致。

建立一个年度网络影响力人物项目，确保与员工和高级管理层的定期互动，以提高网络安全意识并开展合作。[15]

14 Verizon，《数据泄露调查报告》（Data Breach Investigation Report），2023.
15 世界经济论坛，《弥合网络安全人才缺口》（Bridging the Cyber Skills Gap），2024。

# 了解更多



# 重要趋势 3

# 构建可信人工智能

组织持续探索如何通过 AI 增加其业务运营的价值，但领导层在 AI 的采用上仍然持怀疑态度，尤其是在安全和隐私方面。数据泄露、未经授权的访问和滥用的风险居高不下。此外，某些 AI 的具体机制仍缺乏明确性，部分算法可能导致偏见、歧视及其他意外后果。在此背景下，提升围绕AI的开发和部署的透明度、问责制的明确和治理框架的搭建很可能会继续成为首席信息安全官（CISO）的首要任务。

## 管理 AI 数据至关重要

显然，数据是组织的关键资产，为AI 系统的发展和部署提供动力。然而 许多企业仍然难以建立明确的指导方针和流程来管理其拥有的大量数据。这进一步凸显了与数据访问、使用、分类和质量相关的挑战。所有这些因素直接影响AI系统生成可靠洞察并做出合理决策——当数据质量低下时，AI模型更有可能产生不可靠的结果，导致性能欠佳和潜在的危害。

事实上，尽管许多组织正在投资于数据的可访问性，但毕马威研究表明只有 24% 的组织专注于建立以数据为中心的文化并确保数据互操作性。这种短视行为削弱了组织各层级有效使用和理解数据的能力。[16]

此外，组织拥抱 AI 的速度给数据管理实践带来了巨大的压力。积极的一面是，这凸显了可靠 AI 实践与高效数据管理之间的紧密关联。传统的数据治理通常依赖手动流程和孤立的系统，面对AI应用产生的数据规模、速度和多样性，这些方法已显不足。企业现在需要采用更敏捷和自动化的数据管理策略以跟上时代步伐。

> “无论公司是依赖自有数据还是第三方的数据来生成和训练其 AI 模型，都已清楚地表明，低质量的数据必然导致低性能AI 模型。”
>
> **Samantha Gloede**
> 执行总监，美国及全球风险咨询
> 毕马威美国

16 毕马威2024年全球技术报告，2024年9月。

这需要组织从根本上转变对数据的认知和思维方式，从静态资产转变为动态资源。为了降低低质量数据带来的风险，组织必须优先考虑强有力的信息治理机制。这包括建立明确的数据收集、存储和管理政策及流程，以及实施严格的数据验证和清理过程。这样做不仅能使企业改善其AI模型的表现，还能通过践行负责任和透明数据实践的承诺来赢得利益相关者的信任。

## 面对 AI 采纳的风险雷区

AI 的采用伴随着一系列组织必须谨慎应对的风险：运营、技术、法律、合规以及人身安全只是其中几个方面。AI 系统可能引入新的漏洞和故障点导致干扰业务流程并造成财务损失。技术风险，如算法偏见和数据漂移，会损害 AI 模型的准确性和可靠性。这就是为什么 70% 的 CEO 表示他们的组织正在增加对网络安全的投资，具体目的是保护运营和知识产权免受与 AI 相关的威胁。[17]

不遵守隐私法规、歧视受保护群体或侵犯知识产权的 AI 系统可能导致法律和合规风险。最令人担忧的风险是对人身安全的威胁，特别是在医疗保健和交通运输领域，AI 失效可能会危及生命。

与 AI 相关的另一个重要风险是“被遗忘权”的削弱，即从模型中删除个人数据。这需要基于全新数据集重新训练AI模型，程序复杂且成本高昂。

但即使个人数据被删除并且模型重新训练模型，它仍然可以通过从其他数据点学习到的模式和关联对某个个体做出相当准确的推断。在数字领域真正“被遗忘”正变得越来越难以实现。

随着 AI 更加普及并嵌入到各类“智能”产品中，许多组织，甚至是预算有限的小型企业，也开始转向第三方供应商以获取 AI 能力。虽然这可以带来成本节约和快速部署，但也引入了新的风险。组织可能无法深入了解 AI 系统的内部运作，例如模型训练所用的数据、它的算法逻辑以及可能存在的偏见。

“影子” AI——即在领导层和安全团队不知情或未监督的情况下，在组织内部使用 AI 系统——是另一种新兴风险。“影子” AI 可能在各部门或员工自行部署 AI 解决方案时出现，通常没有经过适当的检查。这种风险不仅在于未受管理的 AI 的漏洞，还在于可能无意中将潜在有偏见的结果整合到业务决策中，而未理解其影响。因此，未管理的 AI 系统可能会引入安全漏洞并损害数据隐私。

为降低这些风险，组织应主动建立围绕内部和第三方 AI 系统的采购、部署和监控的明确政策和程序。此外，首席信息安全官（CISOs）被鼓励探索新型网络安全工具和能力，以使组织能够识别和分析 AI 使用模式，降低“影子” AI 的风险。在此过程中，业务领导、IT 团队和安全专家之间的密切合作至关重要。

> “仅仅依赖首席信息安全官或首席隐私官来应对 AI 风险意味着可能会忽略透明度、可靠性、甚至可能是安全性等关键问题。”
>
> **Katie Boswell**
> 网络安全与技术风险总监
> 毕马威美国

17 毕马威《2024年全球首席执行官展望》（KPMG 2024 Global CEO Outlook），2024年8月。

## 自下而上地处理与AI相关的风险

即使AI应用速度加快，许多领导者仍缺乏对 AI 治理及其复杂的技术、伦理和法律影响的全面理解。因此，许多人采取被动应对的方式。将 AI 风险管理策略与整体业务目标和价值观保持一致的组织更有可能取得成功。

事实上，为了建立和维持对AI系统的信任，组织必须优先考虑利益相关者的利益，包括客户、员工以及更广泛的社会在AI决策中的利益。组织领导者，包括首席信息安全官、数据保护官和隐私官，在将安全和隐私嵌入AI开发生命周期方面发挥着至关重要的作用。

此外，领导层必须保持对各种 AI 业务案例的可见性，并明确识别组织内 AI 的应用范围和方式。这可以指导安全和道德的数据管理实践的发展以及更广泛的 AI 安全框架内的适当控制措施。

## 巩固信任和监控外部风险

组织需要前瞻性策略来应对AI相关风险，不仅限于对问题作出反应，而是尽早应对潜在风险。建立 AI 安全框架并非一次性项目，它必须是持续进行的，并且需要通过身份和访问管理、多重认证以及危机响应和恢复计划等现有安全领域来支持。

简而言之，应将 AI 系统的持续监控和评估纳入组织的日常业务流程中。通过绘制 AI 生态系统中的数据流，组织可以更好地评估潜在风险和漏洞，并制定有针对性的战略。

外部风险的核心之一是与 AI 相关的法规的潜在影响，例如于 2024 年 8 月生效的《欧盟 AI 法案》。该法案对任何在欧盟运营并提供可在欧盟内使用的AI产品、服务或系统的企业都具有广泛约束力。

尽管这可能是最知名和影响最深远的规则，但该法案是全球 AI 监管指南不断上升的更广泛趋势的一部分。许多世界各地的政策制定者都希望将该法案作为范例，并在安全、安全、隐私、治理和合规，以及公平性、透明度和可信度等议题上寻求某种程度的一致性。面向欧盟提供服务的企业CIOs需评估合规要求并采取行动。

组织必须密切关注所有监管动态，并主动调整其 AI 治理实践，以建立与利益相关者的信任，并在缓解 AI 的风险和挑战的同时实现其全部潜力。

> “许多企业因未看到数据项目的直接价值而长期推迟这些项目，但他们最终会意识到，清理数据并为大型语言模型（LLMs）提供相关且准确的训练信息已迫在眉睫。然而，在很多情况下，首席信息安全官并不是数据的所有者。为了建立数据团队与安全团队之间的桥梁并加强合作，企业需要建立统一的数据分类标准和跨部门协作机制，特别是在涉及 AI 时。不良的数据必将导致错误的决策。”
>
> **Erin Hughes**
> 网络安全咨询服务负责人
> SAP北美区

# 建议行动

召集跨职能利益相关者，包括 首席信息安全官、数据保护官和隐私官，共同更新政策并就组织应对 AI 实施潜在影响和风险的方法达成一致。

确定并建立必要的控制措施的所有权，以减轻与 AI 相关的风险，并明确界定谁拥有并对其负责，确保这些控制措施与组织的整体数据治理框架一致。

理解与 AI 实施相关的监管义务并评估现有的合规要求。制定并沟通清晰的 AI 使用政策、标准和程序。 与其他行业领导者以及全球政策制定者合作并保持开放对话。

建立红队结构以对 AI 模型进行测试，确保其稳健性和可靠性，避免生成不准确的结果，或者不良信息。明确第一道（业务线）和第二道（风险与合规）防线之间支持 AI 能力的角色和责任。

提升现有的治理流程，并清晰地沟通 AI 使用的政策、标准和程序。这应包括一个 AI 技术引入流程，采用一致的方法来识别 AI 风险、确定适当的控制措施并建立相应的事件管理计划以应对潜在的 AI 相关问题。

# 了解更多



# 重要趋势 4

# 驾驭AI赋能网络安全：快速前行与安全并重

AI的潜在益处持续吸引着各行业的商业领袖。对于首席信息安全官 而言，AI被视为提高效率、削减运营成本、改善风险管理以及可能应对不断增长的工作量的一种手段，特别是在安全运营中心（SOCs）中。然而，仍然存在一些疑问：组织是否全面理解AI风险范围？是否已建立稳健且专门针对 AI 的安全基础？若不知道从何入手或者如何识别 AI 最有用的领域怎么办？在此背景下，首席信息安全官 必须在企业广泛部署 AI 的诉求和优先考虑良好的网络安全实践之间取得微妙的平衡。

## 构建 AI 的强大安全基础

在不断变化的网络安全生态系统中，保持对潜在攻击者的领先不仅需要警惕，还需要创新。AI 已成为安全运营中心（SOCs）的强大工具，它改变了安全专业人士感知和应对威胁的方式。如果说 2024 年是生成式AI的一年，2025 年将是代理型AI的一年。代理型 AI 有可能变革安全操作，通过“智能体”以前所未有的方式主动分析、检测并响应网络威胁。

事实上，将近四分之三的组织已从其 AI 投资中获得了业务价值，但只有三分之一的组织能够实现这些收益的规模化。[18]

但在全面采用 AI 之前，组织必须确保他们具备坚实的基础网络安全实践。这包括从有效的补丁管理、设备加密，以及安全的身份和访问管理等各个方面。仓促部署 AI 工具可能会使组织面临更大的风险。

首席信息安全官 在这里扮演着关键的角色。他们必须评估其组织当前的网络安全态势，并识别任何可能存在的漏洞或薄弱环节，以便逐步且战略性地引入 AI。简而言之，投资应谨慎且具有战略性，以避免实施过程中的脱节。[19]

> 坦率地说，当你的补丁管理和权限控制都尚未完善时，盲目应用 AI 工具是没有意义的。基础网络安全永远是第一要务。

**Koos Wolters**
网络安全负责人
毕马威荷兰

18 19 毕马威2024年全球技术报告，2024年9月。

## 人才困境：弥合 AI 技能缺口

围绕 AI 在网络安全中的讨论不可避免地会转向人才问题。当前存在的显著技术缺口不仅在于理解 AI本身，更在于如何在网络安全领域有效利用它。AI 技术的发展速度，特别是生成式 AI，已经远超市场现有技能水平。

增强员工的 AI 技能是这一环境下的首席信息安全管理官（CISO）面临的主要挑战之一。安全团队逐渐意识到用于与 AI 模型互动和查询的指令质量会显著影响输出的准确性和相关性。如果没有对最佳实践的深刻理解，安全团队可能难以从 AI 实施中获得有价值的洞察和可操作的情报。

为了应对这一技能缺口，并确保安全团队能够跟上AI技术的快速进步，CISO们必须优先考虑推动技能培训计划——不仅针对他们的团队，也包括他们自己，以便他们能够识别正确的技能需求以及最适合招聘的人才。这包括投资专注于AI概念的教育项目，例如指令工程、数据分析和模型评估。

首席信息安全官应培养持续学习的文化，鼓励其他安全专业人士探索新的 AI 能力，与同事分享他们的发现，并确保他们及其团队具备求知欲和知识，以利用 AI 的力量、保护组织的数字资产并增强网络韧性。

## 应对 AI 炒作与现实差距

毕马威的研究发现，网络安全领域对AI的炒作已经导致组织，尤其是高级管理层，产生了一种害怕错失机会（FOMO）的感觉。事实上，82%的人承认他们正投资于AI驱动的虚拟现实（VR）与增强现实（AR）技术以保持竞争力。[20]然而，领导者需要根据 AI 当前能力和局限性做出决策。尽管 AI 具有变革网络安全的潜力，但它目前在安全运营中心（SOC）中的应用仍然相对不成熟且范围有限。

首席信息安全官 需要设定现实的期望，并向高级管理层和董事会传达 AI 的真正潜力。这包括强调当前的局限性并采取战略性的应用方法。通过鼓励实验文化，首席信息安全官 可以发现与组织的独特需求和优先事项相符合的适当用例。随着 AI 不断成熟和发展，首席信息安全官 必须保持警惕，评估其能力和局限性。

> “在网络安全领域， 我们更容忍误报而非漏报。我宁愿 AI 认为有坏事发生并促使我通过手动流程调查，以确定网络是否受到攻击， 也不 愿 实际上存在网络安全问题却不知道，并且没有采取行动来解决它。”

**Matt Miller**
首席网络安全服务合伙人
毕马威美国

20 毕马威2024年全球技术报告，2024年9月。

## 识别并部署最具影响力的用例

首席信息安全官 必须仔细评估并优先考虑那些能够产生最大影响并与组织特定需求相契合的潜在 AI 应用场景。一个有前景的领域是分析大量数据以识别潜在威胁或异常，因为 AI 在处理大量信息以提取洞察方面表现出色。此外，AI 可用于自动化重复性、手动任务，从而使人力分析师专注于更复杂和更具战略性的任务。由 AI 驱动的分析可以使开发人员在小漏洞变成大问题之前进行修复。

通过赋能团队成员探索 AI 的能力并提出实施建议，首席信息安全管理官（CISO）可以发现 AI 最有效部署的领域。仔细评估和选择解决实际问题的用例使 CISO 能够确保其 AI 投资是目标明确、有效且与组织的整体网络安全和业务目标一致的。

## 准备应对由 AI 驱动的网络安全威胁

在采用 AI 技术以增强其网络安全工作的同时，首席信息安全官也必须准备好应对由 AI 驱动的攻击所带来的新兴威胁。

一个特别令人担忧的例子是深度伪造（deepfakes）的兴起，AI算法现在可以快速、轻松且低成本地创建高度逼真且具有说服力的操纵音频和视频内容。事实上，deepfake 技术已经变得大众化，以至于任何攻击者几乎都可以轻松获取并操作它。

这种欺诈性材料越来越多地被用于社会工程攻击或传播虚假信息中，使得网络安全团队更难区分真实内容和欺诈性内容。

此外，呼叫中心中越来越多地使用 AI 进行语音检测和生物识别认证可能会无意中使其更难检测和防御深度伪造（deepfakes）。攻击者可能利用这些相同的技术绕过安全措施并操纵系统。

为了应对这些不断演变的风险，首席信息安全官必须随时了解关于AI驱动威胁的最新发展情况，并相应调整他们的防御策略。这可能涉及投资先进的由AI驱动的安全工具，如那些旨在检测和标记潜在被操纵内容的工具，以及培训员工。企业需要确保任何 AI 部署都有明确的角色、责任和背景支持，以最大限度地提高其对网络安全效率和效果的影响。

> “不幸的是，就 AI 而言，安全团队承担了很大的责任。首席信息安全官已经处境艰难，但如今AI被迅速部署的速度正在指数级地增加他们在大规模引入这些大语言模型（LLM）时对良好安全标准的压力。
> 不过，有一些有效的策略和工具可用来管理这一不断变化的环境。”

**Terence Jackson**
CISM, CDPSE, GRCP
客户安全官
Microsoft 安全解决方案

# 建议行动

首先解决基本的网络安全问题——比如补丁管理、数据保护、IAM等——然后再转向更复杂的活动，如在整个企业中实施和扩展 AI 。

明确 AI 使用者的角色和职责，并透明公开 AI 被应用的场景和计划。

提升员工和客户对企业以及对手使用 AI 所带来的风险的认知。

优先提升网络安全团队所需的必备技能，并确保他们跟上最新的 AI 发展。

继续评估将 AI 用于安全运营中心一级和二级任务的用例。

鼓励团队对 AI 保持好奇心，并提出实验想法及潜在应用场景。

# 了解更多



# 重要趋势 5

# 安全管理平台整合：平衡风险与收益

为了应对日益复杂的网络安全风险，组织不断增强用于保护其数字资产的工具和解决方案。从端点安全和安全信息与事件管理（SIEM）到漏洞管理、物联网（IoT）安全、扩展检测和响应（XDR）以及托管检测和响应（MDR），可供选择的选项数量之多令人惊叹，使得首席信息安全官（CISO）们难以管理、维护并整合这一复杂且分散的工具组合。更糟糕的是，花在整合上的时间比利用数据来获取可用的安全洞察的时间更多。因此，许多组织正在探索采用安全平台，这使他们能够提高效率、改善可见性并增强对安全环境的控制。这种向平台整合的广泛转变既带来了希望也带来了风险。

### 认识平台整合的价值

大型组织尤其热衷于转向平台整合。原因之一是不同的工具会产生大量的数据和信号，并且它们执行整体安全政策的不同方面。这种复杂性使得集成和实施一致的安全政策变得具有挑战性。通过整合不同的解决方案来精简网络安全工具集，使领导者能够更清晰、更全面地了解其组织的安全状况。这进而促进了在整个组织范围内一致执行安全政策，使组织能够填补潜在的漏洞的薄弱环节。

在零信任框架的背景下，平台整合也非常重要。零信任的核心要求是评估组织网络内每一种交互，包括访问网络所使用的设备、采用的身份验证方法以及具体请求的数据。然而，当组织依赖于分散的安全工具时，实施零信任模型可能会非常具有挑战性。平台整合可以帮助执行细粒度的访问控制并提供所需的可见性。

> “规模经济是通过与特定平台或领域（如身份）整合而产生的。让安全团队使用更精简但或许更高效的技术，有助于培养一支能力更为全面的安全人才队伍，使其在多个领域提升效能。”
>
> **Jim Wilhelm**
> 全球微软安全负责人
> 毕马威美国

此外，在管理身份、数据安全、威胁管理、端点保护和网络控制方面，组织可以通过规模经济获益。整合能显著成本节约，因为较少的工具意味着较少的维护、培训和支持成本。通过整合数据源，安全团队也可以更好地利用 AI 的力量。

理解您的安全数据（日志和监控、信号、威胁情报、身份验证策略、权限分配、用户账户数据等）对于赋能安全人员使用生成式 AI 的能力以提升安全运营中心（SOC）及更广泛领域的效率至关重要。这项工作的副产品是数据整合，并开始迈向建立一个由 AI 驱动的网络安全项目的第一步。

## 应对潜在风险和挑战

虽然平台整合提供了诸多好处，但CISO们必须意识到潜在的风险和挑战。一个虽不新鲜但重要的问题是集中风险——即组织可能过度依赖单一供应商或平台。把所有鸡蛋放在一个篮子里——这是一个自云计算采用初期就一直存在于首席信息安全官（CISO）视线中的风险——如果某个产品或平台存在漏洞或被攻破，公司将面临更高的风险。最近一些备受瞩目的IT相关中断事件凸显了这一点。因此，CISO们必须在享受精简安全栈的好处与减轻单一故障点潜在影响之间找到微妙的平衡。

从商业角度来看，另一个可能逐渐浮现的挑战是供应商锁定。随着组织越来越依赖于特定的一系列产品或服务，他们可能会发现所选择的平台已不再满足其需求。在这种情况下，切换到不同的供应商可能是必要的。这是一项成本高昂且复杂的任务。这可能涉及重大的兼容性问题和额外的培训要求。为了缓解这些风险，首席信息安全官（CISO）应考虑采用混合方法来整合平台。

通过依赖平台提供商的基础安全能力，并用专门构建的解决方案弥补不足，组织可以确保他们具备必要的弹性和灵活性以适应变化的情况。因此，首席信息安全官 可以在仍然利用平台方法的核心优势的同时，最小化对单一供应商或平台过度依赖的潜在负面影响。

整合决策很少是孤立作出的。相反，这是一个需要关键利益相关者如CISO、CIO、CFO、COO和CDO共同参与的合作过程。所有领导者都扮演着共同确保所选平台与组织的整体安全策略和业务目标相一致的重要角色。

## 人才和技能提升需同步跟进

在平台整合的趋势下，人才发展和技能提升计划也需要随之演变。网络安全专业人士需要准备好适应并驾驭这个全新的、截然不同的环境。CISO们必须优先考虑安全运营中心（SOC）到监控人员等整个安全领域内的持续学习和人才培养。

> “首席信息安全官及其所在组织担心人才短缺。在这些条件下，为了增强网络安全，有必要简化并整合用于保护数字资产的工具和解决方案的数量。”
>
> **Motoki Sawada**
> 合伙人，技术风险服务部
> 毕马威日本

通过在技能和知识上的适当投资，安全团队可以建立必要的敏捷性和专业能力，以充分利用平台整合的潜力。通过使用更精简的工具集，安全专家将能够把时间和精力投入到高价值的战略行动中，并更有效地应对威胁。

平台整合也为首席信息安全官提供了一个独特的机会来优化他们的人才培养策略。减少供应商合作数量使首席信息安全官能够简化培训工作，以更低成本更便捷的方式地提升团队技能。随着SOC工程师和分析师接受一系列整合工具的培训，他们的工作效率和效能也将提高，这有助于提升组织整体的安全态势。通过将人才培养与发展与平台整合的目标相匹配，首席信息安全官（CISO）可以创建一个持续改进和降低风险的良性循环。

## 与业务速度同步并运行

随着企业拓展新市场与新区域，网络安全团队面临的挑战也在增加。CISO们必须应对激增的用户、设备和数据点，所有这些都需要强大的保护和监控。

与此同时，据多为客户反馈，网络安全预算仍然受到限制，仅同比小幅增长。在这种情况下，证明网络安全支出的合理性并向领导层展示明确价值的压力从未如此之大，这要求CISO持续从现有投资中挖掘更多价值。重点必须放在进行明智的战略性投资上，以实现有形价值和投资回报。

此外，安全措施需要与业务速度相匹配。然而，随着业务的增长以及新技术功能的推出，与安全工具的集成不能以指数级增加成本。它必须灵活且可适应——而平台化方法有助于使这一过程在长期内更加可重复和敏捷。无论是将高级认证方法应用于新的应用程序或技术资产，还是基于信号的访问控制，常见的模式和集成平台方法都有助于提高系统的弹性和采用速度。

首席信息安全官 必须能够阐明他们在平台整合方面的投资如何有助于弥补关键能力缺口、减少漏洞降低风险，并支持整个企业的总体目标。通过在财务责任和战略性投资之间找到正确的平衡，首席信息安全官 可为企业奠定成功基础。

> “传统上，大多数网络安全独立软件供应商（ISV） 表示他们可以与不同的平台互通，但市场在互操作性和有效性的实际效果参差不齐——往往伴随着高昂的劳动力和维护成本。
>
> 新一代的网络安全独立软件供应商（ISV）则采取了不同的方法，他们将传统分散的产品整合成一个全新的、无缝的工具，该工具具有更广泛的功能和更好的数据访问性。这种方法更加有效，使公司能够为个别客户定制环境并实现情景化，从而在数据、速度、规模、效率、成本和功能等方面持续改进。”
>
> **Philip Bice**
> 全球负责人 — 服务提供商合作伙伴关系
> 谷歌

# 建议行动

评估现有供应商，评估平台与企业技术架构的兼容性，并建立明确的供应商选择和绩效监控标准，为整合奠定坚实的基础。

投资于培训并提升网络安全团队的技能，使其能够高效地使用整合工具集。

识别混合方法可带来优势的领域；在整合平台与专用工具之间找到平衡点。建立备份和恢复程序以确保企业的韧性。

实施持续监控和审计流程以确保平台性能。

认识到完全整合可能不可行；识别出可能需要专门工具或供应商的领域。制定分阶段的整合方法，优先处理高价值高影响领域。

# 了解更多



# 重要趋势 6

# 数字身份安全管理迫在眉睫

数字身份正在为一个更加敏捷和高效的数字世界铺平道路。然而，由于系统与控制措施的不足以及深度伪造技术的崛起，确保数字身份的安全性正变得越来越具有挑战。因此，迫切需要将更先进的安全机制纳入验证体系中。更重要的是，CISO和决策者需要全面理解这一领域的现状，重新审视根深蒂固的流程，并投资于基于可靠原则的创新系统。

## 数字身份管理日益复杂的局面

从根本上说，每个人拥有一个属于他们自己的独特的身份。然而，在不同的背景下——例如政府、金融或生命科学——身份被应用于各种方式以服务于特定功能或满足不同需求。CISO必须认识到，尽管个人的核心身份是单一的，但其解释和验证方式在不同的组织环境中可能会有所不同。

随着组织努力维护个人身份的完整性，它们越来越多地转向高级认证技术——包括生物识别技术，如指纹、面部、语音和视网膜扫描——以增强安全性和简化流程。然而，这些模式也带来了风险，其影响可能远远超出典型数据泄露事件。如果这些独特的标识符被泄露，例如，个人将长期面临身份盗用和滥用的风险。由于生物特征本质上是永久且不可替代的，因此一旦泄露难以补救。生物特征数据的收集和处理也引发了人们对生物特征系统中潜在的数据歧视和偏见的担忧，这使得在数据编码实践中确保多样性和准确性比以往任何时候都更加重要，从而保障公平可靠的识别。

深度伪造技术带来了另一个严峻的挑战，因为它日益模糊了现实与操纵之间的界限。随着当前AI技术更加强大、更易于获取且成本更低，个人信息、声音和面部特征尤其容易遭到窃取和利用。虽然深度伪造在假冒和虚假信息传播方面构成了重大威胁，但它们也为内容创作者和内容消费者带来了机遇。

改进的身份验证方法将有助于提升内容创作者的问责性、道德标准和透明度。由此增强的认知度可以引导出更具辨别力的消费者群体。投资更好的身份验证将有助于保护数字信息的完整性并恢复人们对所消费内容的信任。

另一个组织日益担忧的领域是机器身份的增多，特别是在与特权非人类服务账户相关的方面，这些账户可以访问敏感数据以运行特定应用程序。随着物联网越来越突出，机器身份正成为组织管理的一个重要挑战。不出所料，首席信息安全官（CISO）将其团队的大部分注意力集中在人类访问权限上，但他们也必须记录非人类网络用户的行为，以便监控他们是否以及何时会受到攻击和潜在的威胁。

## 为什么企业需要一个面向未来的数字身份策略

从商业角度来看，无论是 B2B 还是 B2C 的情境，数字身份管理都围绕着在组织与其网络访问者之间建立信任展开。通过赋予用户对其个人信息的控制权，通过提供有关其使用的信息并增强透明度，企业可以培养客户对其的信任和忠诚度。这种信任建立在个人能够访问所需资源的保障上，建立在不再需要时访问权限会迅速撤销的信心上，以及所有系统内采取的行为都将被记录并可完全追溯的确切性上。

维护这种信任需要在整个身份和访问管理生命周期中采取主动管理措施，从权限配置、持续管理到撤销访问权限。这一点尤为重要，因为长期任职的员工可能会获得多个系统的访问权限，从而掌握相当大的权力。为了降低与权限累积相关的风险，首席信息安全官（CISO）及其团队必须遵循两个关键的网络安全原则：最小权限原则和知必所需原则。

通过确保个人仅能访问与其特定角色相关的系统，组织可以大幅减少攻击者通过高权限管理员账户入侵并获取敏感数据的风险。

随着员工身份和消费者身份之间的界限日益模糊，组织必须采取整体性策略。对于员工而言，一个强大的数字身份框架确保访问敏感信息是基于明确定义的角色和责任授予的。这包括实施安全的入职和离职流程，并定期进行访问权限的审查和更新。

一个有效的数字身份策略也可以显著提升效率和用户体验。一个流程优化的过程可以减少重复填写表格的需求，例如报税、理赔保险和就医等。这可以减少员工和客户的摩擦和等待时间。

随着组织越来越依赖数字技术来推动增长和创新，强大的数字身份框架将成为其整体业务战略的基石。通过投资安全、透明且以用户为中心的数字身份解决方案，企业可以为成功奠定基础。

> “组织往往更关注网络安全中‘人’的维度，因为这更易感知。验证机器的身份、用途、以及它在系统中创建的时间则困难得多。”

**Anubha Sinha**
合伙人，数字信任与身份
毕马威澳大利亚

## 政府如何赋能受信任的数字身份生态系统

数字身份仍然是确保各类政府服务和交易中实现安全高效验证流程的关键接触点。全球各国政府和大型跨国公司正在积极寻求改进个人及企业相关数字身份的解决方案。例如，澳大利亚最近推出了一项全面的数字身份计划，名为“信任交换平台”（Trust Exchange），其核心是通过数字钱包整合需要身份认证的不同领域，如政府、社会、金融和职场身份。[21]

通过实现跨服务的数字身份验证，Trust Exchange 力求增加组织间的信任，同时赋予公民对其分享的个人信息的控制权。爱沙尼亚是另一个例子，该国在每个公民出生时就发放一个数字身份，并且这个身份在其一生中都有效。公民对其身份何时以及何地被验证具有完全透明度，这有助于缓解隐私担忧。[22]

尽管存在这些令人鼓舞的发展，但全球系统之间的互操作性仍然是一项挑战。由于不同国家在处理个人和生物识别数据方面的监管、风险偏好和公众意见存在差异，若要在全球范围内达成可信身份交换的共识，可能需要由意愿一致的企业联盟推动，例如欧盟正在开发的互操作框架以构建共享可信身份体系。然而，并非所有国家都优先考虑相同价值观，特别是隐私方面的问题，这可能在短期内限制互操作性的深度。

## 首席信息安全官如何引领实施数字身份策略的行动

在制定数字身份策略时，CISO可以充当政府、监管机构和企业的连接纽带。在日益复杂的环境中（大部分身份管理流程远超出其直接控制范围），CISO必须采取主动且协作的思维模式，自上而下地协调利益相关者，以确保认知统一并推动必要的变革。

安全领导者需要跟上用户需求和期望，确保遵守核心安全原则，并持续关注新兴技术如 AI 和深度伪造的影响。此外，首席信息安全官 必须将数字身份议题提升至董事会层面，确保高级领导理解其重要性并提供必要的支持。

通过将身份作为网络安全的新边界优先考虑并在整个组织中培育网络安全文化，首席信息安全官可为成功的数字身份管理奠定基础。

> “在数字身份的世界里透明度是信任的基石。我们相信，通过公开说明个人信息收集和使用方式，可以缓解人们对隐私的担忧，并赋予个人作出明智选择的能力。流程越透明，人们对这个系统的信任度越高。”

**Imraan Bashir**
合伙人及国家公共部门网络安全负责人
毕马威加拿大

21 澳大利亚社会服务部，《信任交换驱动安全数字服务》（Trust exchange drives secure digital services），2024年8月13日。
22 e-Estonia，《解决方案和服务：数字身份》（Solutions and services: e-Identity），2024。

# 建议行动

确保遵守核心安全原则，例如数据最小化和及时删除不必要的数据，以维持最高标准的数据保护。

调动所有相关方，从高层开始，确保提高意识并推动围绕可持续数字身份和访问管理的需求。

建立与其他业务部门的牢固关系和信任，以确保身份管理流程中的高效协作和协调。

将身份视为网络安全的新边界，明确其在保护组织资产和利益相关者方面的关键作用。

了解 AI 和 deepfakes 对数字身份的影响，主动应对新兴威胁和漏洞。

在保障网络安全的同时简化身份管理流程。通过简化凭证的发放和使用、减少密码依赖等来提升用户体验。

> 随着深度伪造技术的进步，身份操纵和欺诈的风险加剧，因此构建强大的数字身份保护机制成为保护消费者和组织免受新兴威胁的关键。

**Nancy Chase**
全球及加拿大国家风险服务负责人
毕马威国际

# 了解更多


# 重要趋势 7

# 智能设备的“智能”安全防护

随着技术的进步，智能设备和物联网产品的爆炸式增长改变了我们与世界的互动方式。从家用电器、可穿戴工业设备，以及车辆，互联设备的激增为网络安全从业者带来了需要防范的新漏洞，这同时影响着公司和消费者。许多风险仍在持续演变。保护联网设备访问的组织数据将成为维护各行业及基础设施完整性、安全性的关键。十年前的传统方法已不再适用。企业亟需制定有效的网络安全策略连接资产的整个生命周期以及整个组织生态系统。

## 首席信息安全官在智能产品安全中的角色

当各行各业——包括工业制造、能源和国防等领域——都希望提升效率并获得竞争优势时，消费者则要求便利性、可访问性和个性化体验。在此背景下，我们预计会出现一波互联智能设备的增长浪潮，这些设备将几乎改变全球经济的每一个领域，特别是医疗保健、交通运输、制造业和零售业。

随着这些由 “Smart-X”技术驱动的产品日益与公司的后端系统和数据库相连，首席信息安全官（CISO）将不得不采取更加以产品为核心的网络安全策略。他们需要深入参与组织和特定产品的流程，确保安全措施贯穿智能设备整个生命周期，从安全设计到设备退役。[23] 根据毕马威的研究，72%的组织 正在践行“设计即安全”的原则，即确保网络安全团队从初始阶段就参与相关技术项目。[24]

从初始设计和开发阶段到持续维护和更新，首席信息安全官必须与工程、开发及产品支持等团队密切合作，共同应对互联设备带来的独特安全挑战。

这些技术的发展带来了新的风险和漏洞。此外，这一新现实使得网络安全更加贴近社会整体——一旦出现问题，不再仅仅是企业层面的危机。潜在影响可能从轻微的不便到对公共安全、安全和隐私的重大威胁不等。因此，保护 Smart-X 技术的安全性不仅对于保护单一实体至关重要，更是维护整个行业和基础设施的完整性和安全性的关键。

> “CISO必须认识到智能产品供应链极其复杂。在安全层面，这些外部供应商和流程必须从端到端严格管理，因为所有环节都是相互关联的。”
>
> **Marko Vogel**
> 合伙人，网络安全
> 毕马威德国

23 毕马威，Smart-X：智能设备网络安全的全面方法，2024年1月。
24 毕马威2024年全球技术报告，2024年9月。

# 当轮胎遇到科技

一个显著改变并现在归入智能设备范畴的设备是汽车。近年来，车辆从简单的机械装置进化为复杂的联网设备。现代汽车如今配备了一系列传感器、处理器和软件系统，使自主驾驶、实时导航和空中升级成为可能。此外，OEMs（原始设备制造商）越来越多地提供“作为服务”的额外功能，这突显了向基于服务的模式转变的趋势，以便访问高级车辆功能。

显然，联网汽车已经从根本上改变了我们与汽车互动的方式。然而，随着技术的日益复杂，这也为网络安全专业人士带来了新的挑战。随着车辆越来越依赖软件和连接性，它们也变得更容易受到与其他联网设备所面临的相同类型的网络威胁，如黑客攻击、数据泄露以及恶意软件感染。智能车辆作为企业的延伸，可以直接访问企业后端系统和数据库。这可能导致敏感的组织数据暴露于潜在的黑客面前。

从消费者的角度来看，随着电动汽车、自动驾驶汽车和联网汽车越来越普遍，网络攻击的威胁显著增加。今天的汽车利用数百万行代码来支持其众多高级功能，这使它们更容易受到未经授权的访问和黑客攻击。该领域的首席信息安全官（CISO）必须研究并采用工具和策略，将相关的网络安全协议及流程落地。[25]

# 智能医疗设备的安全审视

同理，随着医疗设备的激增以及网络攻击者发现其漏洞，针对医疗设备的网络攻击频率和严重程度正在加剧。医疗设备已成为攻击者的高价值目标。尽管技术创新迅速，但仍有大量老旧的医疗设备在使用中，其中许多设备存在安全漏洞或管理不足。

存在安全漏洞的医疗设备可能会向未经授权的人员泄露敏感的患者信息，扰乱关联技术，危害患者健康甚至可能导致医院运营瘫痪。这要求所有利益相关者——从制造商和医疗服务提供商到安全团队——进行沟通并协作，主动识别网络风险及相关威胁，制定缓解和补救措施，并确保患者的持续安全与保障。

随着网络安全标准和实践的不断演变，制造商以及首席信息安全官（CISO）面临着确保这些设备符合最新安全要求这一艰巨任务。

## 物联网和工业物联网（IIoT）安全法规的演变

围绕物联网（IoT）和工业物联网（IIoT）的安全性的监管环境也在不断发展。出现了新的法规来应对人们对连接设备的隐私和安全日益增长的关注。

欧盟《网络韧性法案》（CRA），一项于2024年生效的具有开创性的欧盟法规，规范联网硬件和软件产品的制造商。CRA旨在“解决消费者和企业当前面临的如何判断哪些产品是网络安全的并如何安全配置的挑战。”所有在欧盟销售和使用产品的制造商和供应商，无论是欧盟内部还是外部，都必须遵守CRA。这对在欧盟拥有设施与供应链的全球企业尤为重要。

在英国，《产品安全与电信基础设施法案》（PSTI）为使用联网技术产品的消费者设定了保护标准。它要求制造商专注于安全设计原则，例如禁止默认弱密码，明确安全更新最低周期，并提供合规声明。[26]

PSTI为其他地区在智能产品安全监管方面树立了先例。随着物联网（IoT）和工业物联网（IIoT）设备的日益普及，组织必须应对越来越复杂的安全法规网络，特别是在欧洲。为了有效应对这一环境，公司必须开发统一的安全管理方法，考虑不同管辖区内的全部法规范围。这要求首席信息安全官（CISO）与包括法律和合规团队在内的各种利益相关者密切合作。

2024年，澳大利亚通过了类似立法，以确保智能设备的制造商和供应商符合相关安全标准。[27]

25 毕马威国际，《网络安全车辆：联网车辆数量的增长需要更好的网络安全措施》（Cybersecure Vehicles: Growing number of connected vehicles warrants better cybersecurity measures），2024。
26 网络安全政策与法律中心，英国 PSTI 法案生效，2024年4月29日。
27 澳大利亚政府，内政部，《网络安全法》（Cyber Security Act），2024年11月29日。

## 管理智能产品的长生命周期

智能产品的长生命周期为CISO及其团队带来了独特的安全挑战。与传统设备可能具有相对较短的使用寿命不同，智能产品如汽车可以使用数十年。这些设备的基础架构必须设计为能够定期更新和升级，以适应新技术、法规要求和不断演变的安全威胁。

在这样的动态环境中，CISO必须与产品开发团队密切合作，将安全考量嵌入智能产品的长期规划中，这意味着企业需要探索可能的发展趋势，如量子计算，这些趋势可能会在未来几十年影响安全格局。

与传统的IT系统不同，传统的IT系统可以轻松部署补丁和更新，而智能设备通常嵌入了软件，由于诸如连接限制和无法实时打补丁等因素限制，这些软件更难更新。因此，首席信息安全官需要制定强大的策略来管理整个产品生命周期中的软件更新。此外，CISO还需教育最终用户认识到定期更新软件的重要性，并提供清晰的指导。

围绕所有智能产品——而不仅仅是汽车和医疗设备——的供应链进一步增加了复杂性。由于组件来自不同供应商，理解构成每款智能产品的软件模块至关重要。CISO 需要通过评估潜在漏洞来确保供应链的完整性和安全性。这包括维护详细的软件物料清单，这使制造商能够快速检测并解决关键漏洞，即使在设备部署给最终用户后也是如此。

从整体角度出发，应对智能设备的安全问题和将其融入 Smart-X 生命周期的每一个方面都至关重要，不仅是为了保护敏感信息和资产，也是为了维护客户和利益相关者的信任。

## 评估新兴技术对 Smart-X 安全的影响

AI 和其他新兴技术，如自动化，robotics、5G 和边缘计算为CISO们在确保智能产品的安全方面带来了机遇和挑战。通过践行DevSecOps原则，并在开发的最早阶段将AI能力嵌入到智能产品中，组织可以创建一个更强大且适应性强的安全框架，覆盖整个产品生命周期。

然而，这也引入了新的复杂性和风险。随着这些技术变得更加先进并深入嵌入到智能产品的功能中，安全漏洞或故障的潜在影响变得更为严重。CISO应该努力加深对 AI 和其他新兴技术如何与智能设备交互的理解，识别可能存在的被恶意行为者利用的模式和潜在漏洞。这需要与产品开发团队密切合作，并致力于持续测试和评估，以确保安全措施在技术发展过程中保持有效。

AI 有望彻底改变安全威胁的检测和缓解方式，使安全团队能够主动预测并规划潜在漏洞。最终，CISO必须在拥抱智能设备中新兴技术的好处与保持强大且适应性强的安全框架之间找到平衡。

> “统一的安全观是首要任务。如果没有统一的安全观，组织将无法高效或有效地开展业务，因为如今合同中包含了许多安全要求——当然这理应如此。”
>
> **Jayne Goble**
> 合伙人，网络安全 K
> 毕马威英国

# 建议行动

实施一个涵盖 Smart-X 设备整个生命周期的安全框架，从安全设计到设备退役，包括针对物联网 IoT 和工业物联网 IIoT 设备的具体策略。

鼓励在各种网络协议和标准（如 Bluetooth、Ethernet、5G/6G）上的投资，以优化连接性和安全性。

建立早期保障机制并维护详细的软件物料清单，以实现对设备的快速检测和召回，从而管理关键漏洞。

通过透明的网络安全措施、第三方审计以及合规性管理来解决潜在的物理安全问题并建立客户信任。

制定并实施针对智能设备特定使用环境的安全计划，充分认识安全和信任在提升设备整体可靠性和客户信心方面的重要性。

# 了解更多



# 重要趋势 8

# 构建企业韧性：网络安全护航企业和社会安全

韧性已成为组织和社会关注的焦点，尤其是在关键基础设施领域以及信息技术（IT）和操作技术（OT）之间。其核心在于通过管理攻击面降低入侵概率，快速识别以及在最大限度地减少事故的同时对事故做出反应，实现迅速恢复。随着攻击者可能利用勒索软件或其他恶意手段引发大规模工业中断（危及数据与人身安全）的风险持续加剧，这一主题正成为首席信息安全官（CISO）议程的核心。为了有效地嵌入弹性，CISO需要综合考量多重因素-威胁态势、组织资产形态演变、政府角色及法规要求。

### 通过全面的资产管理增强网络安全韧性

有效的资产管理仍然是网络弹性的基石。CISO必须意识到，如果不了解自身资产，便无法保护需要保护的东西。这不仅包括维护日常运营的组织数据中心内的资产，企业IT之外的工厂运行系统、大众交通网络调控系统及能源电网管理系统等关键终端。缺乏此类监管，识别企业资源规划（ERP）系统等核心系统及其潜在威胁就会变成猜谜游戏，从而使组织暴露于风险之中。

针对关键基础设施的网络攻击频率与规模将持续攀升，动机从经济利益到地缘政治问题和恐怖主义不等。这些攻击的影响可能是毁灭性的，甚至可能导致严重的社会危害。网络犯罪造成的财务损失也在急剧上升，全球数据泄露的平均成本在2023年第一季度至2024年第一季度期间达到了近500万美元，比上一时期增加了10%。[28]

> “到2025年，我们仍在讨论如何正确地发现、理解、分类并最终保护组织的关键资产，这真是令人惊讶。”

**Jason Haward-Grau**
全球网络恢复服务主管
毕马威美国

28 IBM，《2024 年数据泄露成本报告》（Cost of a Data Breach Report 2024），2024 年 7 月。研究时间为 2023年3月至2024年2月。

为应对这一挑战，组织越来越多地采用终端检测与响应（EDR）和扩展检测与响应（XDR）解决方案。EDR专注于监控并保护终端设备，如笔记本电脑、台式机和移动设备，而XDR通过整合来自多个安全工具和系统的数据，提供更全面、高效的组织安全态势视图。尽管 EDR 和 XDR 已经被更广泛地采用，但它们尚未达到全覆盖。这些解决方案本身并不是万能药，应被视为组织建立的更广泛的安控框架中的重要组成部分，以帮助组织有效管理问题、获得可见性、快速检测异常与威胁，并高效响应事件。

## 应对生态系统扩张和第三方合作的风险

随着组织越来越多地依赖第三方供应商提供软件和服务，供应链薄弱环节的风险也在增加。生态系统不断扩张也扩大了攻击面，每增加一个第三方合作关系，潜在的入侵点也随之增多。黑客常寻找最小阻力的路径入侵网络，一台未受保护的打印机即可成为突破口。

外部供应商的安全漏洞可能会危及整个系统，可能导致诸如“蓝屏死机”之类的灾难性事件，即关键系统陷入无响应且不可访问状态。这使得首席信息安全官（CISO）必须通过评估和强化合作伙伴和供应商的安全态势来有效管理这些风险。

为了应对这些挑战并确保符合新兴法规（如欧盟的 DORA 《数字运营韧性法案》、NIS2《网络和信息系统安全指令2》和CRA《网络安全韧性法案》），组织正在采取更为积极主动的方法来管理第三方安全。这些法规旨在构建运营韧性，其中DORA特别针对金融机构的韧性要求，其目标是为韧性提供框架，包括如何为中断做准备、事件发生时的应对措施及中断报告机制。[29]

通过从合作初期明确安全预期，并要求软件和硬件供应链中保持透明度和问责制，组织可以更好地保护自己免受各种供应链攻击。值得注意的是，CRA 要求供应商除常规硬件物料清单（HBOM）外，还需提供软件物料清单（SBOM），以确保对其产品和服务中使用的库和组件有全面的理解。[30]

## 面对物理和虚拟威胁融合的局面，采取全面的安全策略

在应对网络攻击时，物理世界与虚拟世界的界限已不再分明。这意味着组织必须考虑网络威胁对其物理资产和运营的潜在影响，以及物理安全漏洞如何导致虚拟脆弱性。CISO需要将其团队的关注点从持续监控转向主动识别深度伪造等潜在攻击入口。

采用兼顾物理与虚拟属性的整体安全策略，对于防御全方位威胁至关重要。这包括为远程工作者加固VPN隧道，并确保所有设备——无论是公司配发的还是员工个人拥有的——都得到充分管理和保护。

组织也必须准备好应对网络攻击可能引发现实世界后果的事实。例如针对关键基础设施的成功攻击，可能导致大范围瘫痪、经济损失甚至人员伤亡。通过认识到物理世界和虚拟世界的相互关联性，组织可以更好地为这些类型的事件做好准备并作出响应。

> 我们每天都能听到一个国家对另一个国家发动网络攻击的消息，反之亦然。当前国际冲突中，几乎每一次实体军事对抗都伴随着同样破坏性但无形的网络攻击。这凸显了构建强大网络防御体系的迫切需求。

**Merril Cherian**
合伙人
毕马威印度

29 毕马威，迎接 DORA合规挑战, 2024.
30 《网络韧性法案》将Manifest Cyber和SBOMs置于欧盟舞台中央，2024年3月6日。

## 政府在网络安全中不断演变的角色

随着网络攻击对关键基础设施的影响越来越大，政府在保护企业免受导致重大社会危害的攻击方面的作用愈发重要。同时，组织不能仅仅依靠政府的保护，政府可以通过一些监管之外的措施支持组织网络安全工作的解决方案。

例如，政府可在促进组织间信息共享和制定法规方面发挥关键作用，以保护企业免受大规模网络攻击并增强其整体韧性。像美国的信息共享和分析中心正致力于推动跨行业情报共享。通过鼓励和支持这些类型的倡议，政府可以帮助打破历史上阻止组织公开讨论网络攻击的壁垒。

尽管政府主动针对网络犯罪集团的定向打击可能性较低，但仍有可能通过切断其资金来源、削弱其攻击能力来遏制特定组织。然而，许多此类犯罪集团活跃于难以触及的国家。

# 建议行动

- 保持对不断变化的监管环境的关注，并积极游说政府以推动其立法制定增强整体韧性的控制措施
- 实施主动安全措施，例如分析用户行为和识别异常。以增强组织的实时韧性。
- 制定一份韧性计划，明确关键资产及在遭受网络攻击时维持运营的策略。
- 定期测试和演练网络安全响应计划，为领导者应对重大攻击做好准备，并提高组织的准备度。
- 评估第三方安全漏洞，将法规视为强化组织网络安全基础的机遇。
- 优先持续学习与演进，及时了解最新的威胁、漏洞和网络安全的最佳实践。
- 开展彻底的事后分析，以识别根本原因，制定整改计划并加强网络安全防御。

# 了解更多



# 2025年网络安全战略

随着组织在未来一年战略性地投资AI及其他技术，首席信息安全官（CISO）及更广泛的业务线应采取哪些行动，确保网络安全真正成为企业目标的推动者？以下是CISO在日益复杂的全球环境中保护业务并赋能增长的关键建议清单。

## 人员

- 为由于 AI 自动化和转向基于云的服务而导致的首席信息安全官（CISO）角色的变化做好准备。
- 认识到CISO的角色从单一的网络防御者扩展到风险管理师、政策倡导者和影响力推动者。培养和提升沟通与影响能力，有效地传达网络安全的重要性，推动各层级和各部门的变革。
- 开发并部署超越传统做法的持续培训项目方法，利用创新和沉浸式的技术（如模拟演练）来推动员工行为可持续性变化。
- 确定并建立必要的控制措施的所有权，以缓解与AI相关的风险，并明确界定谁拥有并对其负责，确保这些控制措施与组织的整体数据治理框架一致。
- 提升员工和客户对企业及对手使用 AI 所带来的风险的认知。
- 明确 AI 使用者的角色和职责，并透明公开 AI 被应用的场景和计划。
- 优先提升安全团队所需的必备技能，并确保他们跟上最新的 AI 发展。
- 投资于培训并提升网络安全团队的技能，使其能够高效地使用整合工具集。

## 流程

- 继续在 DevSecOps 过程中通过设计构建安全性，并且将专注于网络安全的团队成员嵌入到业务功能中。
- 实施以人为中心的风险降低策略，专注于解决网络安全中的人为因素，因为人为因素占了四分之三的网络入侵。
- 建立红队结构以对 AI 模型进行测试，确保其稳健性和可靠性，避免生成不准确的结果，或者不良信息。明确第一道（业务线）和第二道（风险与合规）防线之间支持 AI 能力的角色和责任。
- 在保障网络安全的同时简化身份管理流程。通过简化凭证的发放和使用、减少密码依赖等来提升用户体验。
- 实施涵盖 Smart-X 设备整个生命周期的安全框架，从安全设计到设备退役，包括针对物联网（IoT）和工业物联网（IIoT）设备的具体策略。
- 定期测试和演练网络安全响应计划，为领导者应对重大攻击做好准备，并提高组织的准备度。
- 开展彻底的事后分析，以识别根本原因，制定整改计划，并加强网络安全防御。

# 2025年网络安全战略

## 数据和技术

- 牵头讨论采用AI等颠覆性技术，解释风险及缓解措施。
- 随着个人数据与企业数据在基于云和AI服务之间的界限变得模糊，需对第三方供应商进行全面的尽职调查，以确保他们的合同义务清晰且与其组织的整体数据治理框架一致。
- 首先解决基本的安全问题——比如补丁管理、数据保护、IAM等——然后再转向更复杂的活动，如在整个企业中实施和扩展 AI 。
- 持续评估AI在安全运营中心（SOC）一级与二级任务中的应用场景，投资AI技术以量化并追踪人为风险，提升风险管理效能并适应威胁态势演变。
- 识别混合方法可带来优势的领域；在整合平台与专用工具之间找到平衡点。建立备份和恢复程序以确保企业的韧性。
- 确保遵守核心安全原则，如数据最小化和及时删除不必要的数据，以维持最高标准的数据保护。
- 了解 AI 和 deepfakes 对数字身份的影响，主动应对新兴威胁和漏洞。

## 监管

- 随时了解法规变化，与董事会沟通，明确职权范围，以降低个人责任风险。
- 评估第三方安全漏洞，将合规要求视为强化组织网络安全基础的契机。
- 保持对不断变化的监管环境的关注，并积极游说政府以推动其立法制定增强整体韧性的控制措施。
- 理解与 AI 实施相关的监管义务并评估现有的合规要求。制定并传达清晰的 AI 使用政策、标准和流程。与其他行业领导者以及全球政策制定者合作并保持开放对话。
- 通过透明的网络安全措施、第三方审计以及合规性管理来解决潜在的物理安全问题并建立客户信任。
- 根据监管要求为智能设备建立早期保障机制，并维护详细的软件物料清单，以实现快速检测和召回设备，从而管理关键漏洞。

# 毕马威如何助力您的网络安全

毕马威团队拥有从董事会到数据中心的全程服务经验。除了评估您的网络安全态势并使其与业务优先级对齐外，毕马威专家还能协助开发先进数字化解决方案、实施部署、持续监控风险，并高效应对网络事件。无论您处于网络安全建设的哪个阶段，毕马威均可助您达成目标。

作为网络安全的专业服务商与实施者，毕马威专家深谙如何应用前沿安全实践并构建定制化方案。我们在网络安全领域的创新方法也体现在服务交付模式上——无论以何种方式合作，您都将与懂业务、懂技术的专业团队并肩前行。

无论您正进军新市场、推出新产品服务，还是以创新方式与客户互动，毕马威专家都能助您预见未来，通过安全可信的技术加速发展、抢占先机。因为我们汇聚了独特的技术经验、深厚的行业洞见，以及致力于助您守护并构建利益相关方信任的创新型人才。

**毕马威 创见不同 · 智启未来**

**了解更多请访问 kpmg.com/cybersecurity**

# 作者简介

**Akhilesh Tuteja**
全球网络安全负责人
毕马威国际合伙人，
毕马威印度
atuteja@kpmg.com

除了担任毕马威印度全球网络安全业务负责人外，**Akhilesh**还领导该公司的信息技术咨询与风险咨询服务。他热衷于探索信息技术的发展如何助力企业推动智能化流程并实现高效成果。**Akhilesh**已在网络安全、IT战略及技术选型领域为超过200家企业提供咨询服务，并帮助他们充分挖掘技术带来的商业价值。此外，他还精通行为心理学领域，致力于通过用户行为分析等手段，全面解决IT风险问题。

**Kyle Kappel**
网络安全服务网络负责人
高级合伙人，毕马威美国
kylekappel@kpmg.com

作为毕马威网络安全实践的美国区领导人，**Kyle**拥有超过20年的信息系统的从业经验，并在网络安全、数据隐私、监管合规、风险管理以及一般技术问题等领域具备丰富的背景知识。尽管他具备强大的技术能力，但**Kyle**更倾向于采用以业务为中心的方法来解决技术问题，即通过根治问题本质而非仅仅修复技术表象来实现目标。他是一位受众多《财富》500强企业信赖的顾问，与企业的高级管理人员（包括董事会成员、审计委员会、首席信息官、首席财务官、首席运营官、首席技术官和首席信息安全官）紧密合作。

**Dani Michaux**
EMA 网络安全负责人
合伙人，毕马威爱尔兰
dani.michaux@kpmg.ie

在超过22年的网络安全职业生涯中，Dani曾与政府机构合作制定国家网络安全战略，并与国际监管机构合作应对网络风险。她拥有丰富的经验，帮助客户提升董事会层面对网络安全问题的理解。她曾在亚洲的电信和电力公司担任首席信息安全官（CISO），负责组建并管理网络安全团队。Dani积极倡导包容与多样性，并支持女性参与计算机科学和网络安全领域。她曾领导毕马威马来西亚及亚太地区的网络安全和新兴技术风险实践，也曾担任毕马威全球物联网工作组的负责人。

**Matt O'Keefe**
ASPAC 网络安全负责人
合伙人，毕马威澳大利亚
mokeefe@kpmg.com.au

Matt负责推动毕马威在亚太地区12家成员所中的网络安全战略。他拥有超过25年的科技、财务、审计和咨询经验，主要服务于金融服务行业的客户。 Matt专精于科技咨询领域，尤其在养老基金与财富管理、银行及保险行业方面，并提供涵盖科技治理与风险、网络安全、项目管理、IT战略与绩效等多方面的服务。他热衷于利用技术推动组织目标的实现，助力客户的数字化战略与运营模式，并保护其数据、资产及系统安全。

**Prasanna Govindankutty**
美国网络安全负责人
高级合伙人，毕马威美国
pkgovindankutty@kpmg.com

Prasanna是毕马威网络安全服务团队的高级合伙人，常驻美国。他是美国网络安全负责人，拥有20年专注于网络安全和科技风险管理转型的丰富经验。此前，他曾领导毕马威的全球及美国网络解决方案业务。凭借对市场领先的网络安全与治理、风险及合规（GRC）技术解决方案的深刻理解，他协助客户实现整合转型。 Prasanna凭借其在基于技术的转型方面的丰富经验，为能源、媒体和电信行业的客户提供支持。

# 致谢

本报告的出版与全球各地同事的鼎力支持密不可分，特此感谢他们共同参与报告的设计、分析、撰写和制作。

**我们的全球网络安全团队：**

John Hodson
Samar Iqbal
Billy
Lawrence
Leonidas
Lykos
Michael
Thayer

**我们的全球合作伙伴：**

**Imraan Bashir**
毕马威加拿大
ibashir@kpmg.ca

**Katie Boswell**
毕马威美国
katieboswell@kpmg.com

**Oscar Caballero**
毕马威墨西哥
ocaballerochavanel@kpmg.com.mx

**Nancy Chase**
毕马威国际
nchase@kpmg.ca

**Merril Cherian**
毕马威印度
mcherian@kpmg.com

**Samantha Gloede**
毕马威国际
sgloede@kpmg.com

**Jayne Goble**
毕马威英国
jayne.goble@kpmg.co.uk

**Jason Haward-Grau**
毕马威美国
jhawardgrau@kpmg.com

**Matthew Miller**
毕马威美国
matthewpmiller@kpmg.com

**Wendy Lim**
毕马威新加坡
wlim@kpmg.com.sg

**Breah Sandoval**
毕马威美国
breahsandoval@kpmg.com

**Motoki Sawada**
毕马威日本
motoki.sawada@jp.kpmg.com

**Anubha Sinha**
毕马威澳大利亚
asinha12@kpmg.com.au

**Bobby Soni**
毕马威国际
bobbysoni@kpmg.com

**Paul Spacey**
毕马威国际
paul.spacey@kpmg.co.uk

**Marko Vogel**
毕马威德国
mvogel@kpmg.com

**Jim Wilhelm**
毕马威美国
jameswilhelm@kpmg.com

**Koos Wolters**
毕马威荷兰
wolters.koos@kpmg.nl

**Dominika Zerbe-Anders**
毕马威澳大利亚
dzerbe@kpmg.com.au

**我们的联盟合作伙伴：**

**Philip Bice**
全球负责人—服务提供商合作伙伴谷歌

**Lou Fiorello**
副总裁—安全产品ServiceNow

**Erin Hughes**
网络安全咨询主管—SAP北美

**Terence Jackson**
CISM, CDPSE, GRCP
客户安全官—微软安全解决方案

# 联系我们


**张令琪**
毕马威中国
科技咨询服务
主管合伙人
Tel: +86 (21) 2212 3637

**郝长伟**
毕马威中国
科技咨询技术风险管理服务
主管合伙人
Tel: +86 (10) 8508 5485

**赫荣科**
毕马威中国
科技咨询技术风险管理服务
业务合伙人
Tel: +86 (755) 2547 3398

**邬敏华**
毕马威中国
科技咨询技术风险管理服务
业务总监
Tel: +86 (21) 2212 3180

**黄芃芃**
毕马威中国
科技咨询技术风险管理服务
业务合伙人
Tel: +86 (21) 2212 2355

**周文韬**
毕马威中国
科技咨询技术风险管理服务
业务合伙人
Tel: +86 (21) 2212 3149

**宋智佳**
毕马威中国
科技咨询技术风险管理服务
业务总监
Tel: +86 (21) 2212 3306

**李振**
毕马威中国
科技咨询技术风险管理服务
业务总监
Tel: +86 (10) 8508 5397

**张倪海**
毕马威中国
科技咨询技术风险管理服务
业务合伙人
Tel: +852 2847 5026

**林海燕**
毕马威中国
科技咨询技术风险管理服务
业务合伙人
Tel: +852 2143 8803


如需获取毕马威中国各办公室信息，请扫描二维码或登陆我们的网站:
https:/home.kpmg/cn/zh/home/about/ofices.html


本刊物经毕马威国际授权翻译，已获得原作者及成员所授权。
本刊物为毕马威国际发布的英文原文“Cybersecurity considerations 2025”（“原文刊物”)的中文译本。如本中文译本的字词含义与其原文刊物不一致，应以原文刊物为准