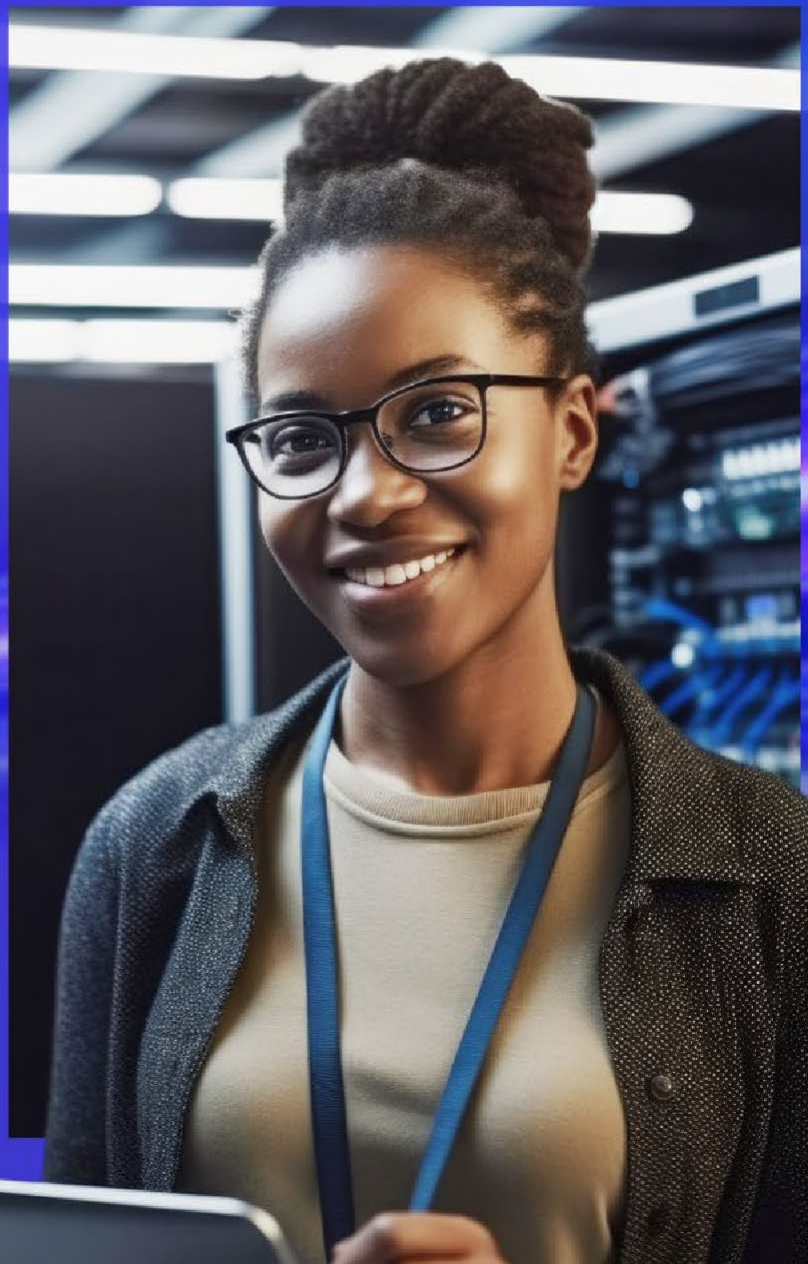
KPMG
毕马威

2024网络安全重要趋势

技术创新离不开务实战略



毕马威国际

kpmg.com/cyberconsiderations

前言

踏入2024年之际，企业的领导者们肩负着诸多责任，他们需努力应对各种挑战，包括推动企业持续增长、应对新兴技术带来的影响和风险，以及吸引和留住各类人才等。企业也意识到首席信息安全官（CISO）应积极参与达成这些业务要求，而非仅在危机时刻解决问题。

毕马威全球各领域的网络安全专家共同探讨了企业首席信息官在2024年需优先聚焦的网络安全八项要素，并形成毕马威年度《网络安全趋势》报告，为企业首席信息安全官及网络安全团队提供网络安全趋势，以期通过减轻特定网络安全事件影响和降低整体网络风险敞口来帮助实现企业的业务增长目标。

随着数字化时代的演进，全球各地的企业均面临许多网络安全挑战，企业需要实施控制措施以构建业务韧性，满足监管要求，并降低整体风险。而人工智能(AI）作为一种战略工具，无论是用于合法目的还是不当目的，其影响正迅速上升。人工智能的普及（目前通常只需一张信用卡就可以通过云端使用这些先进的技术解决方案和模型） 提供了价值创造的新途径，但与此同时也随之带来了大量的潜在风险。人工智能正成切实对企业的运营构成颠覆性影响，其中也包括安全团队。

这种愈演愈烈的威胁态势要求企业及其首席信息安全官必须从一种全新的、更为务实的角度来看待安全问题。如今，他们越发需要在数据安全、隐私与更宽泛的业务目标之间取得平衡。

随着世界各地间的联系越来越紧密，全球范围内已经几乎不存在与世隔绝的区域。全球范围内的社会、经济、政治和监管变化对网络安全的影响也日趋一致。该趋势所带来的最显著的影响体现在全球供应链中。

但是，世界各地的情况仍存在诸多细微差别。例如，世界各地的监管规定仍具有独特的区域性特征，如某些市场对个人数据的保护要求更为严格，或围绕人工智能、关键基础设施和供应链推出的全新法规要求。

在网络安全领域，全球普遍关注网络安全的合规性，重点聚焦在监管管控要求以及报告要求的多样性。因此，企业在探究如何遵守各种跨境监管要求和制度时，更加重视隐私和安全因素。

监管合规要求是企业在构建和管理人工智能系统、保障客户隐私以及围绕关键基础设施、供应链、智能产品和业务韧性制定指导方针时的重要参考。

与此同时，由于企业面临着各种经济不确定因素，网络安全领域的预算必须更加客观合理。许多首席信息安全官认为相关预算将与之前大致持平，并非一定会被调降，因为其中部分费用将被用于企业创新，尤其是人工智能和自动化解决方案等领域。这一显著变化要求安全团队须进行技术合理化及预算优化，以期达到降本增效的目的。

在经济下行给企业预算带来压力的情况下，越来越多的人认为，网络安全领域已趋于成熟，企业可以削减相关投资。此外，安全职能已被纳入其他信息技术和业务转型预算中，而不再是一个独立的预算项目。另外，企业转用基于云的安全即服务模式，也使安全成本以前所未见的方式纳入到涵盖范围更广的企业运营费用之中。

有见及此，我们建议首席信息安全官应加强网络风险量化（CRQ）流程，通过数学建模利用可度量的变量1来阐明相关风险，以财务的维度揭示网络安全风险的影响。从网络风险量化的角度来审视风险，能够有效地向领导层和董事会展示投资回报和投资重点，以确保企业从技术和财务的双重角度了解相关威胁。

本报告从多个角度探讨了企业领导者最为关心的问题，即如何确保企业韧性。当发生数据泄露或网络安全事件时，企业如何迅速恢复正常运作，以及如何将对客户的影响降至最低。

许多近期出台的法规，特别是与关键基础设施领域相关的法规更多的提及了企业韧性。与传统安全视角相比，安全事件的响应和恢复以及减轻对客户造成的损害成为当下企业的侧重点。

网络安全是一项不断变化的持续性工作。企业提高“网络安全事件不可避免但可管理“概念的认知度，将更好的协助企业在网络安全防护及网络安全事件响应和恢复之间取得平衡。

Akhilesh Tuteja
网络安全全球主管
毕马威国际

[1] Forrester，《2022年第4季度网络风险量化概览》（*The Cyber Risk Quantification Landscape, Q4 2022)*，2022年11月29日

2024年应聚焦网络安全方面八个关键词

请点击各项了解详情

01

满足客户期望，赢得更多信任

随着网络威胁和数据隐私问题愈发严峻，首席信息安全官应积极寻求与企业各利益相关者密切合作的机会，确保在发生事故时保持运营弹性，从而维护客户信任。

02

将网络安全和隐私合规无缝融入企业

将安全融入企业整体应被视为推动企业卓越运营的一项举措。

03

应对日益模糊的全球边界

对企业而言，应重点关注如何最有效地应对日益复杂的全球化业务环境，以确保具备业务韧性和连续性。

04

实现供应链安全现代化

尽管面临各种挑战和重点工作之争，但不应使保障供应商及合作伙伴业务生态体系安全成为制约因素，而应将其作为业务的推动因素。

05

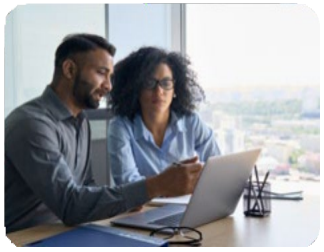
谨慎挖掘人工智能潜力

安全和隐私领域的领导者应积极支持以人工智能为依托的各种业务目标，并关注如何有效及负责任地利用这项颠覆性技术。

06

通过自动化增强安全性

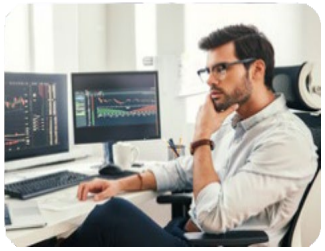
随着企业的数字化转型，安全团队必须对其流程进行自动化和升级，以跟上发展的步伐。



07

以个体而非机构的维度进行身份管理

随着业务模式的不断扩展，企业应从总体角度考虑身份管理，而不应进行割裂管理。



08

使网络安全与业务韧性保持一致

企业应建立安全韧性的企业文化，并与所有利益相关者达成共识。

聚焦事项一

满足客户期望，赢得更多信任

企业的利益相关者，包括消费者、员工、供应商在内的每一位均期望企业追求增长和利润。 然而，如今越来越多的企业也面临着以对社会负责任的方式运作的要求。企业应加强安全和隐私与环境、社会和治理（ESG）因素之间的联系。这种联系在整个业务生态系统中正日益得到重视，尤其是ESG评级机构，他们致力于寻求更高的透明度对企业进行衡量和比较。

ESG的重要性以及如何将安全和隐私纳入整体框架

根据《毕马威2023年全球首席执行官展望》所载，69%的首席执行官已将ESG融入其业务，作为创造价值的一种方式，50%的首席执行官预计这方面的努力和投入将在未来三到五年内带来巨大回报。

相较于ESG中与环境因素的备受关注，网络安全和隐私等治理因素却较少得到充分构建。随着网络威胁和数据隐私问题的日益严峻，首席信息安全官需要与ESG相关人员携手合作，以确保在发生安全事故时，企业运营具有良好的韧性，能够随时启动业务连续性计划确保业务的正常运行。

通过将网络安全和隐私安全纳入社会责任计划并保护客户数据，企业能够更好地维护其声誉及客户信任，即便是在发生重大事故之时。

对于向公共和私人服务提供商提供其个人信息的消费者而言，他们希望自己的个人信息受到保护，且不会被用于其他目的。

与此同时，人们亦期望企业在追求业务目标的过程中，能够采取对社会负责任的措施减少其碳足迹，为当地社区提供帮助，完善劳工政策、并确保员工多样性及平等性。

切实解决网络安全和隐私问题，广泛应对ESG问题，已成为企业及企业首席信息安全官的重点工作。不同的地区和行业面临不同的监管规定，这些规定需要与消费者间建立信任。从合规性的角度来看，这一点十分重要，须加以重视，因为无论是B2B还是B2C，消费者的期望值均受到各种规定的直接影响因而各不相同。

如果个人消费者对产品或服务提供商在个人信息、隐私数据以及违规处罚等方面的处理结果不满意，则可能选择购买其他产品或服务。实际上，82%的消费者更青睐与其价值观相一致的品牌；75%的消费者则表示会因为与品牌的价值观不合而放弃该品牌。2 在有选择的情况下，大多数消费者更倾向于选择那些遵守ESG准则，优先考虑安全、隐私和可持续发展的企业。

这一点在B2B领域尤为明显，这是因为企业客户非常重视保护其机密数据和知识产权。越来越多的行业被提出了网络安全和数据隐私相关的监管要求，能够遵循这些要求的企业更受利益相关方的青睐。3 对于许多B2B行业企业而言，这并非仅是“加分项”，更重要的是，监管义务会直接从受监管行业的企业扩大至供应商，如果企业遭遇重大网络安全事件，供应商因为合作关系亦可能会因此而蒙受损失。

事实上，大约有三分之二的消费者愿意为可持续产品支付更高的费用，尽管三分之二的零售企业高管对消费者是否真会如此持怀疑态度。4 虽然消费者可能愿意为安全、隐私和社会责任支付额外费用，但这些因素目前仍是“筹码”（即成本），这些“筹码”将很快初级消费者的底线。

对于涉及私募股权或风险投资的案例中，企业看待投资的道德视角尤为值得注意。如今，许多投资者注重于企业对于网络安全和隐私管理的能力，其原因是，投资者担心网络安全问题可能会对他们所投资的企业造成品牌损害。

> **网络安全在人工智能和数据伦理方面发挥着越来越重要的作用。确保用于训练人工智能算法的数据准确无误、未被篡改且不存在偏见是一项艰巨的任务，也或许最终成为不可能完成的任务，但仍然非常值得我们为之付出努力。**

Caroline Rivett
合伙人
生命科学行业网络安全全球主管
毕马威英国

[2] Google Cloud，《新研究表明消费者比以往更关注品牌价值》(New research shows consumers more interested in brands’ values than ever)，2022年4月27日。
[3] 毕马威，《ESG领域的网络安全》(Cybersecurity in ESG)，2023年。
[4] First Insight / 宾夕法尼亚大学沃顿商学院，《消费者与零售企业高管的可持续发展分歧》(The Sustainability Disconnect Between Consumers and Retail Executives)，2022年1月。

积极将网络安全纳入ESG议程的社会效益

当前在许多企业中，在ESG背景下对于网络安全和隐私问题的探讨尚不常见。 ESG领域的讨论范围需进一步扩大。

在当前的环境下，企业、员工和消费者之间的社会契约与数据保护存在着深层次的矛盾。在涉及如何利用视频和音频来制作深度伪造文件方面，提高信任度应该成为重要的网络安全议题。深度伪造文件是指将某人的图像、视频或音频替换成他人的面孔或声音，或进行篡改使其看起来或听起来像是做过或说过某些事情。

打击深度伪造文件十分困难，因为在许多情况下，需要人们自行判断视频或音频的真假。企业必须保持警惕，及时识别和删除这些深度伪造文件，并应积极向广大群众宣传相关知识。网络安全在人工智能以及数据伦理方面发挥着越来越重要的作用。确保用于训练人工智能算法的数据准确无误、未被篡改且不存在偏见是一项艰巨的任务，也或许最终成为不可能完成的任务，但仍然非常值得我们为之付出努力。

网络安全和隐私管理在保护言论自由和确保当前日益普及的数字通信渠道安全方面，也发挥着至关重要的作用。隐私控制措施在限制未经同意或不知情的情况下利用及滥用个人信息方面也蔚为关键。这对于维护公众对企业的信任非常重要。

许多脱碳以及二氧化碳减排项目均依靠数字技术和自动化系统来监控和管理能源生产、输送和使用。 尽管这些工具可以提高效率，但也可能会造成不可预见的网络安全漏洞，因此需要采取高水平的数据保护措施。 企业引入网络安全战略可有助于减轻各种威胁，降低数据泄露的风险，并确保遵循相关监管要求。

值得注意的是，网络安全和隐私管理均为企业重要的社会责任，企业应与B2C及B2B客户携手合作，帮助他们提高网络安全意识。银行已纷纷将此作为常规事务，越来越多的零售企业也正加入其中。此举与供应链及生态系统也息息相关，因为增强供应商生态系统安全十分重要。

若企业的网络安全问题能够得到管理，人们是否还会关心此类问题?

理论上，大多数人可能会表示不希望自己所使用的产品或服务的供应商发生数据泄露。但他们并不想为此支付更多费用，同时希望企业与客户的交互快速、顺畅。在未出现安全问题之前，人们大多对此并不关心，且可能希望相关工作在幕后开展。

对于企业而言，重要的是向客户阐明网络安全是当务之急，具有实际意义。企业应就此引导客户，使其了解和关注网络安全意识的影响，并证明企业所开展的工作并非仅是一般事务，而是一项至关重要的服务。

对企业外部人员进行引导本身就是一项ESG实践工作。“网络安全意识宣传月”正是政府和企业共同努力确保员工及消费者了解网络安全基础知识并避免各种重大风险的典范之举。

百分之百的安全不切实际。即便已采取各种预防措施，但网络安全事件仍会时有发生。如若发生，企业应迅速决定是否需要进行披露。如有需要，还应确定准备或必须向公众披露的信息范围。5 开诚布公对企业至关重要，网络安全事件发生后进行良好的沟通，会让客户更加信任企业。

[5] 毕马威国际，《警惕网络安全问题，维系企业弹性》 “Maintaining cyber vigilance and staying resilient,” 2023年。

措施建议

与您企业的ESG团队进行沟通，确定他们是否将网络安全视为其一大职责。如若不是，则应努力使其认识到网络安全对于ESG三个领域的重要性。

务实。有效确保网络安全不是让合作伙伴各行其是，而是在企业内部重构关系，激励企业内其他业务领域将安全融入其现有工作。

增强企业在网络安全、ESG和隐私方面的全球监管情报工作，以确保及时满足合规要求和报告要求；密切关注和洞悉不断发展的监管法规及其对企业网络安全工作的影响。

参阅以下报告了解详情

Cybersecurity in ESG
（《ESG领域的网络安全》）
从同一维度审视ESG和网络安全

KPMG global tech report: ESG
（《毕马威全球技术报告：ESG领域》）
企业如何以技术为契机实现ESG目标

Road to readiness
（《求“证”之路》）
2023年毕马威环境、社会与治理鉴证成熟度指数报告

聚焦事项二

将网络安全和隐私合规无缝融入企业

如今，无论是首席信息安全官还是其领导的团队，在安全方面均扮演着与以往截然不同的角色。企业的核心业务流程日益网络化。相应地，网络安全也正从由首席信息安全官集中管理，向联合管理模式转变。在联合管理模式中，首席信息安全官发挥着引领作用，负责建立框架，评估相关风险并提供落地支持。 从前端到后端，安全与企业各职能部门均密不可分。许多领导者都已意识到，将安全意识融入其独特的企业文化和业务流程极具价值。

业务模式和技术正不断演进，并产生安全影响

无论企业从事的是产品制造、服务提供还是信息创造，基于云的运营模式将越来越普及，并与其他新兴技术相结合，以提高可扩展性，降低成本，获取收入，扩大利润率。

汽车行业提供了很好的业务模式转型案例。现如今的汽车已然成为一台装有轮子的巨型平板电脑。人们在路上订购披萨甚至都不需要使用手机。 燃油汽车（更不用说电动汽车）的技术含量已相当高，可以说已成为零售消费者能购买到的最先进的产品。

技术的弊端在于它扩大了攻击面，从而导致了新的潜在漏洞，并提高了业务生态系统的复杂性，这些都是首席信息安全官们必须应对的问题。与此同时，应对网络安全问题的成本也在飙升，促使企业必须考虑如何更有效地提供服务。

在当下新形势中，企业无法部署数百人的安全团队，而是必须保持精简，尤其是对于那些嵌入业务线的团队而言。企业必须正确地将人员与技术相结合，广泛应用人工智能，特别是机器学习技术，来完成人类无法高效完成的工作。

人类无法对成千上万的应用程序进行及时的审查。企业必须决定从何处起将安全纳入应用程序的开发流程，并开展持续监控，以了解潜在攻击和漏洞的影响。

但是，这并不是首席信息安全官的责任。管理该等风险需要的是整个企业文化的转变，并将安全作为企业标准运营程序的一部分。首席信息安全官并不负责安装补丁，亦不负责管理运营。安全团队应确定在业务中嵌入安全任务的方式和环节，并对这些任务进行监控，以确保其正常执行。这就是我们对于安全团队发展方式的看法。

企业可以通过“内包”的方式为客户提高安全性，或通过外包给第三方服务提供商的方式有效引入自身可能缺乏的专业技能。许多企业都在努力将安全作为自身的核心竞争力，尤其是在尝试掌握大量新兴技术之时。

与企业领导者携手合作有效构建安全

当前有很多关于“安全左移”（在开发阶段提前考虑安全性）的讨论。我们认为此举极为重要，但同时也认为企业必须端到端地考虑安全问题（从概念阶段到构建，包括持续监控），并持续确保安全。在此过程中，可见性是安全的首要因素。

企业的安全专家越来越像空中交通管制员，必须保持跑道畅通。首席信息安全官必须确保“交通”（即应用程序）以高效、安全的方式运作。 安全不应妨碍产品和服务的发布，但应尽早对企业正在采用的流程进行了解。

将安全融入更广泛的业务中应被视为推动企业卓越运营的一项举措。安全团队应说明和展示何谓“安全良好”，并激励企业内部的安全专家朝着这一愿景努力做好管理工作。这就需要设置适当的“安全护栏”，以实现“设计即安全” ，并将适当的工具和模板集成至开发环境之中。

首席信息安全官及其团队，以及业务安全人员，应从整体上考虑企业的卓越运营，并分担相关责任。这意味着人员、流程、技术和监管要求均要同等考虑。

“十年或十五年前，安全专家的“80/20”法则是指80%的技术能力以及20%的软技能。如果首席信息安全官希望避免自己被视为支持人员，则必须适应新的“80/20”法则，将沟通、建立信任、解决问题和冲突管理等的重要性与确保高效的运营中心等同视之。”

Brian Geffert
合伙人
网络安全
毕马威美国

企业可通过重点关注风险管理、事件管理、治理与合规、技术解决方案以及员工培训和意识来培养可持续的安全文化。

这对于须符合美国证券交易委员会（SEC）颁布的新网络安全规则6 以及欧盟颁布的《网络与信息系统安全》第二版安全指令（NIS2 Directive）的企业尤为关键。后者要求各成员国在2024年10月7 前实施相关法律，以保护重要企业免受网络威胁。

首席信息安全官应如何保持影响力

大多数首席信息安全官对数据、应用程序和整体攻击面相关的安全影响有深刻的了解，但还可以在与人才、预算和跨组织政治等方面进行深耕，以真正展现其独特价值。那些了解如何在企业整体开展工作，将安全融入业务，同时又维持合作伙伴身份的首席信息安全官，将会实现最卓越的成就。安全团队必须深入了解各业务部门正在规划的措施，以及可能会暴露的潜在新威胁。

首席信息安全官应使用业务合作伙伴所熟悉的语言，而非深奥的技术语言来进行沟通。不应谈论诸如零日漏洞、高级持续性威胁或安全编排、自动化和响应（SOAR）策略等术语。这些术语对于大多数非安全领域的同事而言毫无意义。而应这样表述：“如果这项计划行不通，就会被市场拒之门外。如果不能保护产品线，则无法获得足够收入，因为消费者不会使用这些产品。”

安全团队不需要制造紧张。相反，应该提出旨在促进业务发展和降低风险的新观点。首席信息安全官必须让人们相信，其指导意见和策略愿景均符合企业的最佳利益。其兜售的产品叫做“信任”。

新的必备技能和能力

安全专家必须提高自身的软技能，包括谈判、时间管理、倾听和建立人脉等人际交往技能。十年或十五年前，安全专家的“80/20”法则是指80%的技术能力以及20%的软技能。

如今，这项法则已颠倒过来。如果首席信息安全官未能与企业领导层合作，阐述企业能够理解的计划，且能够有条理地提出想法以影响整体业务行动，则根本无法取得成功。

除了这些软技能以外，安全领导者还应考虑利用网络风险量化的方法，来更有效地管理整体风险敞口。 这将有助于更好地进行沟通，并阐明相关财务风险，以及企业应在哪些领域应优先进行网络安全投资。

安全团队必须意识到，自己主要是与非技术领域的同事进行沟通，帮助他们了解相关风险并采取相应行动。如果首席信息安全官希望避免自己被视为支持人员，则必须适应新的“80/20”法则，将沟通、建立信任、解决问题和冲突管理等的重要性与确保高效的运营中心等同视之。

[6] 美国证券交易委员会（SEC），《SEC出台上市公司网络安全风险管理、策略、治理和网络安全风险事件披露规则》，2023年7月26日。
[7] 欧洲议会，《NIS 2 Directive：欧盟范围内高度共同的网络安全措施指令》，2023年8月2日。

措施建议

为董事会提供全新视角，使其了解可能会阻碍业务运营的因素，以及应该如何在不影响业务运营和客户体验的情况下管理此类风险。

安全团队应确定将安全任务嵌入业务流程的方式和环节，而不是外包给第三方服务提供商，同时安全团队应监控安全任务确保安全任务的正确执行。

像管理企业一样去管理网络安全团队，即管理者应在一定程度上放松对企业其他部门安全工作的控制。

参阅以下报告了解详情

KPMG 2023 CEO Outlook

（《毕马威2023年全球首席执行官展望》）

全球超过1,300名首席执行官分享了他们对地缘政治学、办公室办公、ESG以及生成式人工智能的看法。

KPMG global tech report 2023

（《毕马威2023年全球技术报告》）

了解领导层如何自信从容应对不确定性，把握机遇创造价值。

The future of IT

（《信息技术未来展望》）

探索信息技术职能发展战略，帮助企业做好准备迎接云计算和人工智能时代的蓬勃发展。

聚焦事项三

应对日益模糊的全球边界

世界各地的企业正在日趋复杂的网络和隐私监管环境中开展业务。国家利益的不断演变，对信息主权、供应链安全、网络控制合规透明度、事件报告以及隐私等方面提出了多样化的监管要求。企业需要适应日益“无国界”化的世界，在调整其监管宝贝要求的同时也需要维持符合当地监管要求的安全控制措施。各企业应做好充分准备，以迅速应对不断变化的地缘政治形势以及各种不同的制裁规定。

安全专家面临的最大问题是如何在确保符合监管机构相关要求的同时，在企业赋能和企业价值之间取得适当的平衡。

Orson Lucas
合伙人
网络安全
毕马威美国

全球企业概况：网络和隐私目标相同，实现措施各异

多年来，全球监管环境一直极为脱节。尽管在过去几年中，部分市场优先采取了积极的监管措施，但其他许多市场并未同步跟进。因此，企业不得不面临抉择，是根据不同市场的具体情况实施更高级别的治理、流程和控制措施，还是将新出台的监管规定视作未来趋势的风向标，并对成熟、自动化和主动的隐私及安全计划进行投资。尽管有些企业选择了后者，但许多企业却因为预算、资源和其他业务优先级而选择了前者。

然而，这种情况正在慢慢发生变化。欧洲、中国和美国等市场正就此定下基调，许多其他市场亦纷纷效仿。随着安全、隐私和人工智能领域出现了若干监管模式和原则，为各龙头企业提供了机遇，使其能够在本地和全球范围内基于原则携手积极主动地保护和管理敏感信息。理想情况下，这将在全球范围内形成统一的隐私和安全计划，并兼顾特定市场在监管规定和当地实践上的细微差别。然而，对于真正的全球化企业而言，实现这一愿景仍需克服许多挑战。

例如，在考虑数据本地化和数据传输时，需切实了解内部以及与第三方业务和供应链合作伙伴之间的数据清单和数据流转 / 数据传输情况。通常情况下，企业有多种途径可供选择，但无论选择哪种途径，都必须进行大量的规划和意向设定，以确保高效、低成本以及合规地开展实施。

从业务角度考虑，无论位于哪个司法管辖区以及总部位于何处，企业都需要通过全球客户以及全球业务扩展规模。对于安全人员而言，面临的最大问题是如何既能符合监管机构相关要求，又能在企业赋能和企业价值之间取得适当的平衡。这对于首席信息安全官、首席流程官（CPO）及其团队而言是一项挑战。

监管要求不断变化，全球企业面临各种合规挑战

鉴于规定的不断变化发展，企业应谨慎应对。随着客户关系管理和市场营销技术（MarTech）工具的日趋成熟，企业纷纷借助数据提供给业务的洞察力和投资回报率（ROI）来实现数据价值。

全球多个司法管辖区的监管机构均已出台了具有针对性的隐私规则，并要求首席信息安全官、首席市场官、首席数字官和首席流程官确保自身企业已建立了健全的第二道防线，以应对和遵守当前已出台的和计划实施的监管合规要求。在监管处罚层面，许多国家和地区对侵犯隐私的行为实施了严厉的经济处罚，情节严重的将面临吊销其营业执照。

在隐私处理方面，原本“各自为政”的状况正在迅速消失。随着监管机构关注焦点的演变，在数据买卖、同意及偏好管理、数据伦理以及负责任地使用人工智能等领域，利益相关者和各业务职能之间的障碍正逐渐被打破，并促使董事会和高管层从目的出发，审视如何确保监管合规并赢得消费者信任。而消费者的信任正是龙头企业在寻求与消费者建立、维系和增进关系时展现自身与众不同之道。

“随着当今世界网络犯罪的意图和手段变得愈发险恶及复杂，客户、企业和监管机构都应采取更为全面的方法管理数据及保护信息。”

Henry Shek 石浩然
合伙人
网络安全
毕马威中国

地缘政治发展要求企业具备相应的响应速度以及适用能力

在当前环境下，企业在某个市场所使用的工具和技术可能无法用于其他市场，因此在多地开展业务颇具挑战。例如，部分企业可能会因为供应商决定不在部分国家或地区市场提供某些工具而受到影响。这种情况既是供应链问题，也是企业运营韧性问题，可能会严重影响企业的生产力。

如何最有效地应对日趋复杂的全球业务环境，以确保企业具备弹性以及业务连续性是企业必须仔细考虑的一个核心问题。要应对隐私和数据方面的挑战，企业就必须制定具体明确的治理计划，在存在严格制裁制度的司法管辖区开展业务时，此类治理计划可以协助企业迅速满足最低成熟度水平要求。

中国所采用的监管条例不同于欧盟，而欧盟所采用的相关监管条例亦有别于世界其他地区。这些监管条例在适用范围、个人信息定义、信息收集限制、问责规则以及基本法律框架等方面均存在差异。若不具备基于相关原则合理制定的企业愿景、战略、治理和策略计划，企业将面临越来越多的创新挑战，或面临发展落后的风险。

企业的政治化及其对安全的影响则是另一项需要关注的动态。例如，在美国，部分企业具有明显的政治倾向，这种情况有时是由其领导层内部的价值观所导致，但更多的是为了迎合其目标客户群体。俄乌冲突爆发后，那些继续在俄罗斯运营或开展业务的企业纷纷遭受制裁，使此类问题变得广为人知。

从安全和信息技术的角度来看，分段或微分段的概念具有启发意义，即公司可以通过细粒度的访问控制策略来管理数据中心或云环境，并限制横向扩散的威胁。具备网络控制权限的企业可以使用分段模型，并设置防火墙作出隔离。我们发现，已采用分段模型的企业在必要时更能迅速且有效地切断其相关地区业务。

全球化企业应通过不同的视角来审视各国的司法管辖情况。例如，当企业为在欧洲以外的欧盟公民提供相关服务时，则应遵守《通用数据保护条例》（GDPR）。一般而言，企业需要清楚了解其业务所在地、开展业务所依赖的对象（即供应商）、提供产品和服务的市场、以及法人实体的注册地点。

这四个主权概念之间的相互作用，形成了复杂的监管局面，而灵活的、以相关政策为基准的营运方式则能使企业最为有效地去应对这样的局面。

另一项考虑因素则是冗余性。例如，一家企业将其整个呼叫中心业务设立在某个由于某种原因而受限的司法管辖区内，且在该地的所有业务均都需要关闭。这种情况下，这个业务怎么办？当企业需要暂停某地的业务以应对当前的地缘政治挑战时，企业在业务、安全和冗余性方面做好一定程度的准备可以帮助企业减轻在此过程中企业面临更广泛的业务风险。

归根到底，首席信息安全官及其团队应始终保持企业韧性和预防视角。这有助于企业在下一次“黑天鹅”事件之前保持领先，并巩固企业迅速地做出“应急”决策的能力，而不是被迫匆忙拼凑一个战略性的局部化网络策略。

措施建议

持续关注全球监管环境变化，尤其是对司法管辖区的相关细化规则进行深入了解。

了解企业内关键数据（包括结构化和非结构化数据）的存储位置，以及与第三方合作伙伴共享的数据存储位置。

提高企业透明度，从而在全球供应链中赢得信任；不应仅仅将第三方、第四方甚至第五方供应商关系视为交易及合作关系（尽管事实确实如此），而应将其视为企业生态体系的延伸。

参阅以下报告了解详情

Privacy risk Study 2023
（《毕马威2023年隐私风险研究》）
应对不断变化的隐私风险挑战。

The hostile limelight
（《冲突聚焦》）
从地缘政治展望网络安全未来。

Global Economic Outlook
（《全球经济展望》）
2023年下半年毕马威国际全球经济展望。

聚焦事项四

实现供应链安全现代化

许多企业当前对第三方和供应链安全的处理方法有悖于当今复杂且相互依赖的合作伙伴生态体系。传统模式是围绕第三方依据交易提供服务的假设建立的，这并不能反应当今复杂的应用编程接口（API）网络和依赖复杂的“软件即服务” 依赖关系所束缚的流程。建议企业应建立更多的战略供应商合作伙伴关系，同时应重点关注供应商持续监控和管理供应商不断变化的风险状况，以增强企业运营韧性。

尽管面临各种挑战和重点工作之争，但不应使保障供应商及合作伙伴业务生态体系安全成为制约因素，而应将其作为业务的推动因素。这方面并无任何捷径可走。这也突显出现代化的迫切需求，即如何在不影响质量的前提下，更快、更高效地利用最少的资源实现目标。这将是基于风险的思维方式与智能自动化驱动的数据驱动方法相结合后可以产生切实影响的地方。

Mitushi Pitti
执行总监
网络安全
毕马威美国

不断变化的供应链格局正在影响传统的安全模式

一直以来，第三方安全模型通常侧重于时间点评估。对经常使用的供应商软件组件开展持续监控和盘点，可以帮助首席信息安全官更好地了解供应商的安全架构并识别潜在风险。考虑到这一动态因素，首席信息安全官应制定更现代化的标准，以实现实时隔绝风险的目的。

为实现这一目标，首席信息安全官及其团队可能面临下列三大挑战：

可见性

长期以来，企业面临着无法顾及其整个供应商群体的问题。大型企业可能拥有成千上万家供应商，而采用传统方法往往无法准确地评估这些供应商的活动。此类情况下通常需要大量的安全人员开展评估工作，这是人力不可为的，而且这可能要花费数千万美元，在后勤保障和预算方面都是不现实的。

可扩展性

除了了解供应商群体的风险状况外，扩展能力使企业能够应对环境不断发展变化所带来的挑战。从新技术和流程带来的风险到供应商违反企业安全协议的可能性等风险，第三方环境始终是一个不断变化的威胁向量。

第三方合作伙伴不断变化的风险状况

老的交易模式并不具备相关机制以跟踪关系的变化以及由此可能产生的新的漏洞。因此，根据供应商的成熟度，企业需要采取更多行动（实行月度审查），或采取更少行动（允许供应商有更多的自主权，并开展季度审查），以确保这些关系的高效运作，并遵循所有监管合规要求。

随着技术的日新月异以及客户要求的不断提高，各个企业都在不断寻求创新。当然，第三方和第四方供应商以及网络犯罪分子也同样如此。

例如，许多供应商正在部署人工智能，用以改进流程及提升任务效率。不过，尽管人工智能功能强大，但同时也带来了各种潜在的新风险，包括数据完整性、统计有效性和模型准确性以及透明度和可靠性问题等。在企业层面及第三方合作伙伴层面，机器模拟人类思维的功能必须得到安全和负责任的使用。在整个供应链体系中推断此类风险是首席信息安全官及其团队需要监控的新威胁。

尽管面临各种挑战和重点工作之争，但不应使保障供应商及合作伙伴业务生态体系安全成为制约因素，而应作为业务的推动因素。这也突显出现代化的迫切需求，即如何在不影响质量的前提下，更快、更高效地利用最少的资源实现目标。这将是基于风险的思维方式与智能自动化驱动的数据驱动方法相结合后可以产生切实影响的地方。

政府的职责

强监管企业必须与监管要求的变化保持同步，且在与没有相同监管约束的供应商合作时，必须设法促使这些供应商采取适当的安全控制措施。这是企业当前正面临的持续性挑战。另外，企业也正探索相关监管条例将在哪些领域帮助推动第三方提升整体的安全性。

最近，美国证券交易委员会（SEC）围绕网络安全所制定的规则对第三方作出了相关规定。监管机构已经意识到这是所有企业最关心的问题也是一个日益严峻的挑战。监管机构的助推有助于促使安全成熟度不足的供应商更好地参与网络安全体系建设并助力网络安全态势。

同样，欧盟修订后的《网络与信息系统安全指令》（NIS-2）强调企业应积极主动管理第三方所带来的风险。 此外，《数字运营弹性法案》（DORA），旨在有效监控第三方信息和通信技术提供商所带来的风险以及更好地处理供应链安全问题。

监管机构通过《数字运营弹性法案》来识别对整个供应商生态体系韧性至关重要的第三方。这些企业可能并未直接受到监管，但由于他们被识别为供应商生态体系的重要供应商，因此受监管的实体也必须将监管要求传递至此类第三方。

协作式情报共享：新兴且有价值的战略

实际上，企业与供应商之间的信息共享可能仍需数年时间的演进，但可以想象的是，企业与供应商之间的信息共享有助于巩固最佳实践并增强供应链关系。

随着恶意者带来的威胁呈指数级增长，各行各业的企业，尤其是关键基础设施领域的企业，须在威胁和风险情报方面进行更多的共享，包括内部共享、与市场共享以及与供应商和合作伙伴共享。

> **人工智能带来了各种潜在风险，包括数据完整性、统计有效性和模型准确性以及透明度和可靠性问题等。在企业层面及第三方合作伙伴层面，机器模拟人类思维的功能必须得到安全和负责任的使用。在整个供应链体系中推断此类风险是首席信息安全官及其团队需要监控的新威胁。**
>
> Elizabeth Huthman
> 总监
> 网络安全
> 毕马威英国

各企业应打破各自为政的思维模式，并鼓励业务利益相关者——采购部门、法律部门、业务部门、风险部门以及第三方等——加强沟通与合作。

协作和信息共享亦有助于企业管理供应商集中风险。 这是供应链扩展（第三方、第四方和第五方）的主要考虑因素，因为在供应链中，多个企业均依赖于相同的供应商。在这种情况下，企业应在某些竞争方面维持保密性的同时，相互联合行动，以确保第三方不会成为整个生态体系的薄弱环节。

许多企业不愿意开展这种形式的协作。考虑到这一现实情况，欧盟网络安全局（ENISA）信息共享和分析中心（ISAC）以及美国网络安全和基础设施安全局（CISA）已牵头开展各种集中式项目，对各种威胁及漏洞相关的信息进行收集和快速发布。

协作和信息共享不仅仅关系到供应商能否访问客户或企业的敏感数据。假设某供应商对企业维持运营韧性至关重要，即该供应商影响着企业生产和分销产品的能力，但从安全角度来看，供应商安全成熟度不足。在这种情况下，企业必须采取措施提高供应商的安全性，或者可能需要做出艰难的决定去寻求其他替代合作伙伴。

通过建立基于风险意识和安全的企业文化，以防任何个人或流程不会成为企业的薄弱环节或业务障碍。这种思想应贯穿企业的方方面面，其中亦包括第三方附属机构。

措施建议

采用基于风险的方法来评估第三方流程，而非对提供不同服务的不同供应商采取“一刀切”的管理方式。

利用智能自动化技术来提高对不断变化的供应商风险状况的可见性，并针对第三方建立可持续且可扩展的前瞻性计划。

建议在企业内部以及可信赖的第三方进行情报共享。

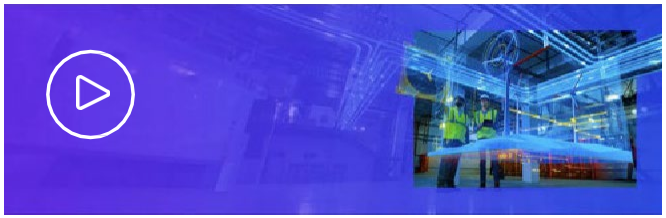
参阅以下报告了解详情

Staying ahead of cyber risk in the supply chain（《防范供应链中的网络风险》）

面对错综复杂的全球供应商网络，以及越来越多的威胁途径，了解和预防网络风险必须成为企业的一大要务。

Supply chain trends 2024: The digital shake-up（《毕马威2024年供应链趋势：数字化变革》）

随着数字化机遇席卷供应链领域，准备度和洞察力将成为取得成功的关键要素。



The future of supply chain（《供应链未来展望》）

从ESG到机器人，再到元宇宙，供应链领导企业面临全新挑战。

聚焦事项五

谨慎挖掘人工智能潜力

通过审慎规划和实施，人工智能将改变完成工作的方式、时间以及交付形式。当前所讨论的话题均围绕着生成式人工智能，但人工智能的许多其他分支（从机器人到机器学习）均在持续重塑各项业务。精确衡量人工智能技术固有的安全行、隐私行和伦理行影响并非易事，各企业正致力于建立框架为实施人工智能提供所需的风险管理和治理。

数据通常是安全领域的关键项，尤其是在隐私保护领域。人工智能行业需要世界各地政府机构作出相应协调，各国家对于该行业不同的立法（某些国家的立法较其他国家更为严格）将会阻碍该行业的创新。人工智能需要在创新需求与有效监管指引及限制之间取得平衡。

Sylvia Klasovec Kingsmill
隐私解决方案全球主管
毕马威国际/毕马威加拿大合伙人

人工智能当前的发展道路：监管限制措施有限，但机遇无所不在

企业对业务营收的担忧，以及在员工和客户，乃至整个社会之间建立信任的必要性，引起了一场关于如何以负责任、透明和诚信的方式控制及部署人工智能的广泛伦理辩论。为此，该领域的监管力度正不断加强。公共和私营机构必须携手合作，在创新和发展过程中提供切实可行的解决方案，以确保从源头将安全和隐私纳入其中。

由于各种警示性新闻报道、缺乏监管限制措施以及缺乏全球通用的人工智能标准，市场对于创新存在一定程度的担忧。然而，在人们对此感到不安的同时，也同样对人工智能推动创新的潜力充满期待。

即便是地方性的关于人工智能模型和算法的管理、部署和立法方式的规范要求目前仍不清晰。一些国家和地区交其他国家和地区在此领域建树更深。企业应保持对建立和维护信任所需的关键基本要素的认识，同时也要留意相关监管法规的发展趋势。这将在很大程度上减少企业未来合规遵从所需的资源投入。

虽然我们鼓励各企业适用人工智能开展工作，但与此同时，企业应确保充分了解人工智能的复杂性，以及如何有效降低模型的风险。随着市场的不断发展，给予全球监管机构和立法机构充裕的时间为人工智能的发展制定适当的指导方针非常重要。欧盟出台的《人工智能法案》作为典型代表，具有里程碑意义，该项法案将在人工智能领域做出与欧盟《通用数据保护条例》（GDPR）在隐私保护方面相类似的贡献，并为该领域的蓬勃发展铺平道路。

尽管在人工智能领域缺乏相关法律法规是一项明显的发展障碍，但现有的隐私法规具有类似的规范性要求，可以且应该适用于新的人工智能算法。现行法律法规已将诸如告知、同意、可解释性、透明性和损害风险等隐私因素纳入其中。

为了保持市场竞争力，首席信息安全官应与首席数据官及数据保护官携手合作，为各项依赖于人工智能的业务目标保驾护航，并确保企业可以有效且负责任地利用这项颠覆性技术。与此同时，他们也需要对那些可能已运行一段时间但基本未受监控的流程实施充分的治理和控制。这种实施与治理之间的平衡是成功应用人工智能的关键所在。

在人工智能创新与安全及隐私问题间取得平衡所面临的主要挑战

为了促进人工智能的应用，企业必须做出关键选择，此过程将影响公司的决策，如创建内部模型还是依靠第三方。

> **首席信息安全官和其他高层领导者及其团队需为各项依赖于人工智能的业务目标提供支持，并确定如何有效且负责任地利用这项革新的技术。与此同时，他们亦需要对那些可能在一段时间内基本未具备监督措施的流程进行充分的治理和控制。这种实施与治理之间的协调一致正是成功应用的关键所在。**
>
> **Katie Boswell**
> 总监
> 网络安全服务
> 毕马威美国

虽然其中一种可能具有更少的不确定性，但事实上，这两者均存在固有风险，企业必须意识到并有效的管理这些风险。

各企业必须了解与透明度、问责制、公平性、隐私和安全有关的保障措施，为创新和实施奠定基石。例如，在负责任的发展方面，企业可以向在人工智能发展领域中走在前沿的大型技术公司及司法管辖区寻求指导。

从隐私和安全的角度来看，许多企业在某种意义上处于被动跟随状态。随着众多企业全速推进人工智能的应用，首席信息安全官和首席产品官必须紧随其后，并确保必要的控制措施得以落实。开始便建立和维系人工智能解决方案的可信度，对于品牌和业务目标实现能力至关重要。

这就需要跨职能部门的合作，特别是从资金的角度来看。为了彻底把握和寻求创新机遇，企业应制定统一的战略，在安全、隐私、数据科学和法律层面达成一致。最近，美国政府借鉴欧盟所出台的《人工智能法案》，发布了一项“关于安全、可靠和可信的人工智能”的行政命令，明确了人工智能安全和保障的要求，该行政命令中包括了人工智能的安全保障、隐私、公平和公民权利以及创新和竞争等。[8]

在快速推进人工智能创新与实施健全的隐私和安全措施之间取得平衡

数据通常是安全领域的关键项，尤其是在隐私保护领域。人工智能行业需要世界各地政府机构作出相应协调，各国家对于该行业不同的立法（某些国家的立法较其他国家更为严格）将会阻碍该行业的创新。人工智能需要在创新需求与有效监管指引及限制之间取得平衡。

这不仅是一种文化的转变，也是一场技术的转变，而变革管理则是取得成功的关键要素。为了将隐私和安全设计思维与人工智能及其他新兴技术相结合，管理这些技术的专业人员（不仅仅是技术）必须培养以隐私和安全为第一优先级的思维方式。

如果企业从一开始便考虑到隐私和安全，它们就会自然而然地被纳入其运营模式当中。

如果全球都坚持采用人工智能来满足各种创新需求，那么人工智能最终将像云计算一样成为业务常态。

不久前，迁移到云端是一项艰巨的任务。如今，已经成为企业常规业务实践的一部分——没有哪项安全领域不涉及云元素。我们认为这也可能是人工智能的发展趋势， “人工智能安全”这个概念将不复存在，因为它将成为整体安全的一部分。

[8] Whitehouse.gov，白宫新闻简报室，总统行政行动，“关于安全、可靠和值得信赖地开发和使用人工智能的行政命令”，2023年10月30日。

措施建议

将人工智能框架与企业战略保持一致，通过调整企业内部各业务领导者的工作优先级，并与在人工智能领域中取得成果的业务部门开展跨职能协助，以开展人工智能治理。

确保人工智能算法的目的（无论是企业内部开发还是外部开发）被明的确定义和记录，且人工智能算法的目的与业务目标相匹配，人工智能算法仅适用相关的训练数据，人工智能算法获取相应的同意。

了解欧盟出台的《人工智能法案》以及拜登政府颁布的关于“安全、可靠和可信的人工智能”的行政命令中的相关规定。

参阅以下报告了解详情

Privacy in the new world of AI

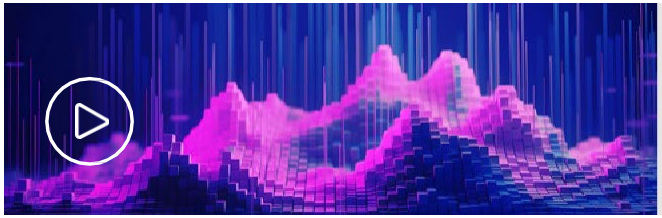
（《人工智能新世界中的隐私问题》）

如何通过隐私保护建立对人工智能的信任。

Generative AI models – the risks and potential rewards in business

（《生成式人工智能模型——对业务的风险和收益》）

ChatGPT、DALL · E 2、Bard等人工智能的崛起对企业的意义。



KPMG generative AI survey report: Cybersecurity

（《毕马威生成式人工智能调查报告：网络安全》）

毕马威独家调查报告，揭示了人工智能这一卓越技术具有巨大潜力的四个领域。

聚焦事项六

通过自动化增强安全性

越来越多的企业将系统迁移至云端，导致需要保护的数据量急剧增加，而且越来越多的人通过个人设备远程办公并访问公司网络。因此，网络攻击面正在不断扩大，随之而来的是首席信息安全官需要对骤增的警报、误报和分流事件进行处理。安全运营中心（SOC）中存在大量的误报，而且没有足够的人员或可视化界面来处理这些信息。首席信息安全官 (CISO) 如何持续不断地发现威胁，并且确保安全运营中心没有遗漏任何信息？安全运营中心必须迅速收集、关联和升级需要应对的告警。实现此目的，唯一可行的方法就是自动化。

“由多个扫描程序源识别的安全漏洞大量涌现。当务之急是关联并识别真正的威胁，并进行溯源发现问题的根本原因。此举有助于首席信息安全官和治理团队获得企业的风险视图，并揭示在哪些领域需要更多具备专业技能的人员。自动化则能帮助安全团队明确工作的优先级。”

Pratiksha Doshi
合伙人
网络安全
毕马威印度

当前实施安全自动化的原因

数字化正以惊人的速度蓬勃发展。与此同时，由于企业必须采用和掌握的新兴数字技术激增，促使许多企业将自身视作科技企业，而忽视了自身的核心业务。例如，金融机构目前在客户互动方面已几乎完全实现数字化，许多医疗服务提供商也已使用远程医疗技术、人工智能驱动的医疗设备以及基于区块链的记录存储技术。

随着企业的数字化转型，安全团队必须对其流程进行自动化和升级，以跟上发展的步伐。事实上，恶意攻击者也在使用这些新技术，导致威胁正变得越发复杂。而且，恶意攻击者不仅试图访问网络环境，还利用人工智能技术实施各种欺诈行为。网络犯罪分子正使用深度伪造技术（经过处理以模仿他人面部、声音或动作的合成媒体文件）来与呼叫中心联系，并实施更具迷惑性的网络钓鱼。

首席信息安全官必须像潜在攻击者一样老练，才能从纷繁复杂的信息中快速识别合法事件，而最有效的方法就是在安全运营中心中采用自动化和人工智能技术。通过将日志管理、威胁扫描和访问控制等简单的安全功能进行自动化，使安全团队能够更迅速、更高效地进行响应。

不同行业的许多企业都已成功实现安全职能的自动化，并通过将例行、重复但至关重要的任务自动化来释放劳动力。许多具有资深经验的专业人士以往所开展的工作（如：漏洞扫描、日志分析和合规检查）均可以标准化的方式自动执行。

自动化正不断改变整体安全格局

安全自动化已经成为每个网络安全能力的关键工具，首先是自动化预防工具。自动更新及执行预先设定的程序在组织面临恶意攻击者扩大规模和加速攻击时，对于确保组织主权防御的弹性和可靠性具有至关重要的作用。此外，自动化也能协助确保第三方生态体系的安全，评估各项漏洞并发现供应商生态体系中的薄弱环节。

在检测和响应方面，自动化技术能有效帮助首席信息安全官实现一定程度的自助服务安全性，这对完成评估和测试并将结果应用于生产网络中非常重要。这种做法大大减少了企业所需的劳动力。此外，如果企业已将特定IP地址列入黑名单，则无需人为干预便可自动进行工单分析。

恶意攻击者会利用自动化技术来扩大攻击规模和加快攻击速度。抵御这些自动化攻击最有效的方法是采用自动化检测和响应措施。在发生违规事件时，自动监控流程能够近乎实时地识别出安全问题，并通过更改访问策略规则或者隔离可疑设备或用户等方式进行补救。

首席信息安全官及其安全团队可实施自动化，通过收集现实世界的证据来验证控制措施运行的有效性。这将简化企业第一道、第二道和第三道防线的风险管理和治理。

Angela Leggett
执行总监
网络安全
毕马威美国

一些安全团队通过自动化措施收集数字取证证据，并验证控制措施是否按相关规定运行，从而简化了企业第一道、第二道和第三道防线的风险管理和治理。

监管合规则是自动化价值体现的另一种典型案例。 例如，美国证券交易委员会（SEC）在2023年7月采纳了针对上市公司的网络安全风险管理、策略和治理规范。根据此规范，重大安全事故必须在四个工作日内进行报告。为遵循此项要求，企业必须对安全事故进行检测，评估安全事故的严重程度，并提交6-K文件。建立能自动生成并提交该文件的工作流程，对企业开展合规工作具有实用价值。[9]

[9] SEC.gov，*《SEC出台上市公司网络安全风险管理、策略、治理和网络安全风险事件披露规则》，2023年7月26日。*

对于全球性企业而言，这不仅限于提交6-K表格。企业必须以不同格式、在不同时限内（有时甚至是在几个小时内）满足一系列的监管报告要求。对这些相关流程实施自动化则可能决定了企业能否满足合规性要求。

自动化技术对安全团队及业务在人员和技能方面的影响

自动化技术增强了企业的安全流程，并使首席信息安全官能够优先考虑人力部署的最佳领域。由多个扫描程序源识别的安全漏洞大量涌现。当务之急是关联并识别真正的威胁，并进行溯源发现问题的根本原因。此举有助于首席信息安全官和治理团队获得企业的风险视图，并揭示在哪些领域需要更多具备专业技能的人员。自动化则能帮助安全团队明确工作的优先级。

显然，安全团队的工作将发生改变。人们将愈发关注涉及威胁评估、意识培训和业务协调等更具战略性的问题，而非执行可以由人工智能或预测分析引擎完成的重复性任务。

这项工作需要相关人员具备新的技能。例如，首席信息安全官及其团队必须着手探究大型语言模型的工作原理，训练方法和编程方法等。此外，还需要了解并熟练掌握与云技术、物联网和人工智能相关的安全概念。

措施建议

制定企业自动化的初始愿景和战略。明确企业的短期和长期安全目标，确保其与企业的业务优先级保持一致，并确定这些目标所需的安全保护类型。

识别企业可集中访问的数据，并制定自动化的持续控制监测计划，以提高企业三道防线的效率。

确定应自建或需要采购的工具，了解供应链合作伙伴如何通过自动化技术提高企业间的信任度，并在适当的情况下运用此类经验。

参阅以下报告了解详情

Empowering security
（《增强安全性》）
通过安全编排和自动化响应，为未来保驾护航。

Building trust in cloud environments
（《在云环境中建立信任》）
2023年毕马威云转型调查

Mastering a multi-cloud environment
（《掌握多云环境》）
云端能力的演进。

聚焦事项七

以个体而非机构的维度进行身份管理

与消费者互动的企业都会为消费者分配唯一的数字身份，如用户名和密码不同一样，数字身份的验证方法也不相同。从网络安全的角度来看，身份识别模型正在不断发生演变。大多数身份和访问管理（IAM）模型最初是为单个企业管理数字身份和用户访问权限而设计的。许多IAM模型当前正被重新构建，以涵盖联合、私有、公共或多重云端计算环境所需的弹性。此举将使个人用户，无论是作为客户还是员工，每次与新机构互动时，都无需再进行繁琐、费时的身份验证流程。

采用联合式方法来改进传统的身份识别模型

在当前环境下，正确识别与企业有业务往来之人的身份是安全领导者们最为关心的问题，这也是一个不断变化的目标。在过去的10到20年里，大部分企业均设计并实施了身份管理程序。安全专业人员的想法是：“如果自己实施这些管理程序，那么我就掌握了完全的控制权。”此类身份管理程序一定程度上施加了控制措施，但这种做法会导致权限控制的割裂，并增加了需要管理的身份的数量。从客户的角度来看，他们最终会拥有数十个或数百个与不同业务一一对应的身份。

如今，B2C和B2B业务安全性之间的界线已逐渐变得模糊。虽然B2B用户访问的网络资源通常比B2C更多，但是这些用户都属于外部用户，这就使得企业在许多情况下会将两者进行合并以进行身份管理。

随着业务模式的不断扩大，企业已不能割裂地看待身份问题，而应从整体角度出发。这推动了身份模型的发展，使供应商和终端客户可以灵活地与多个部门开展互动，而不必每次都要经历复杂的身份验证流程。

消费者应对自身的数字身份具有控制权，使其数字身份能够在消费者和员工之间互相转换。

> **随着身份保障措施水平的提高，我们逐渐开始看到向联合式身份模型发展的趋势，这意味着，在不同领域需使用不同数字身份确保安全性的情况会逐步减少。**

MarkoVogel
合伙人
网络安全
毕马威德国

近年来，许多知名科技企业和社会企业提供的网络保障措施水平均有所提升，数字身份在整个数字商务生态系统中得到了广泛应用。随着人们对数字身份信任度的提高，我们逐渐开始看到向联合式身份模型发展的趋势，这意味着，在不同领域需使用不同数字身份确保安全性的情况会逐步减少。

身份识别模型发展到以具备高保障水平的数字身份作为标准时，将使企业减少收集、存储和处理个人身份信息（PII），这对消费者而言无疑是一件好事。

值得一提的是，区块链在身份管理方面所体现的价值。分布式账本系统正越来越多地被用于开发有效的联合式身份模型。企业将安全基础设施与区块链技术相结合，并通过可视性、可验证同意、加密及审计跟踪来获取信任。企业可将数据权限管理和访问控制授予信息主体而非由第三方集中处理，这将有助其解决隐私和欺诈问题。

数字身份的保障水平越高，就约具备便携性。当数字身份具备高便捷性时，将会出现消费者整体登录次数减少的趋势 – 即数字身份的减少。最终，我们不仅需要使数据身份具备便捷性——预计到2026年，全球数字钱包的用户将超过50亿，较2022年的34亿用户增长50%以上10——而且要确保数据身份具有防止篡改及可验证的功能。这正是生物识别技术（使用唯一的生物、物理和行为特征作为标识）能够发挥作用的领域。

与此相关的一个考虑因素是，企业何时或是否可能会放弃使用密码，这是因为密码是所有身份识别系统的首要问题点之一。摒弃密码模式，使用多样化的身份验证因素（设备、位置、生物特征、行为）进行安全身份验证，似乎是一项颇有成效的举措，尤其是在业务生态体系中。密码模式的消失可能还需要数年时间才能实现，但我们正在朝着这个方向发展。

深度伪造技术正在改变身份认证的格局

深度伪造技术（通过合成图像、视频或音频文件，篡改和替换个人的面部、声音或行为）带来了切实的威胁，并伴随着对财务、声誉和服务方面的影响。首席信息安全官必须加快安全创新，跟上时代发展的步伐。

随着技术的快速发展，相较于25年前人们对网络钓鱼的担忧，深度伪造技术带来的威胁和担忧正以更迅猛的速度蔓延。当下，恶意攻击者正在寻找比个人消费者或公众人物更大的攻击目标。恶意攻击者已利用最新技术，并将目标投向更有利可图的目标——企业、机构和国家——而他们大多数尚未做好防范此类威胁的准备。

问题的关键在于，能够通过基于生物特征进行身份验证的音视频深度伪造技术是如何实现的。

> **开发出一个数字身份具有高度保障的模型将使企业减少收集、存储和处理更少的个人身份信息，这对消费者而言无疑是一个积极的结果。**
>
> **Jim Wilhelm**
> 合伙人
> 网络安全
> 毕马威美国

单从成本方面考虑，攻击者需要不断学习先进的技术，但随着技术的普及，成本也将逐渐降低。这将导致恶意攻击者更容易利用深度伪造技术进行欺诈。

防范深度伪造的一项关键问题是检测深度伪造所需的资源（包括维持适当的计算能力、取证算法和审计流程，以及使用相关工具的人力资源）。首席信息安全官应与企业高层决策者达成一致，以确保相关资金预算与新出现的威胁相匹配，并确保软件更新发布后能得到及时使用，以使最新的技术得到实施。[11]

[10] Juniper Research, *Digital Wallets: Market Forecasts, Key Opportunities and Vendor Analysis 2022–2026.*（《数字钱包：市场预测，关键机遇及供应商分析》）2022年8月。
[11] 毕马威美国，“Deepfakes: Real threat,”（《深度伪造技术：真正的威胁》）2023年。

密码模式的消失可能还需要数年时间才能实现，但我们正在朝着这个方向发展。

Danny Flint
合伙人
网络安全
毕马威澳大利亚

政府在新身份认证生态体系中的作用

政府和企业机构正在身份验证话题上共同发力。 例如，某地政府正引入可信数字身份框架（TDIF）。 该框架明确了身份认证服务提供商必须遵循的最低要求，供应商须通过并定期维护TDIF认证方可向客户提供数字政府服务。

此举最终的目标则是为用户提供一个便利的平台，促进数字身份的可用性、安全性和私密性。重要的是，个人信息主体将能够使用多个身份服务提供商来维护不同或统一的个人及企业数字身份。

TDIF在保护个人信息主体的数字身份的同时，赋予了个人信息主体选择使用数字身份的类型、目的及使用时长的权利。但是，从成本效益角度出发，政府机构无法独自承担这项工作。此外，在当前环境下，企业机构似乎比政府机构更受信任。

在某些国家，由于监管活动主要基于不同地区开展，因此导致背景更为复杂。但这种问题只是冰山一角，在数字身份的认同方面还引发了一系列新的思考。 随着跨境业务的普及，其数字凭证是否会被境外的监管机构接受呢？

在公私合作方面，如果个人拥有与金融机构相关联的数字身份以及政府颁发的数字凭证，那么他们在不同情况下应使用哪一种数字身份呢？

此外，当个人信息主体出示政府颁发的数字身份时，是否应该强制其分享其中的所有信息？虽然金融机构、医疗机构或执法官员可能需要了解某些详细信息。但是，个人信息主体应对其个人信息的披露具有控制权。例如，个人信息主体应有权自主披露自己的公民身份、大学学位、专业资格 / 执照等，而不是被强制要求提供更多的个人信息。

数字身份泄露风险应由谁来承担，这是安全专家面临的另一个关键问题。倘若某人的数字身份被泄露并被用于欺诈，那么是颁发人还是持有人需要对此负责？政府应根据数字身份的预期用途，对企业施加严格但可管理的监管措施。在这个问题上，监管规范和通用标准必须被制定，以确保数字身份的提供商能够安全地协同运作。

欧盟《通用数据保护条例》（GDPR）的基本原则之一，企业在特定场景下使用个人信息主体的个人信息时，必须获得个人信息主体的同意。

但是，如果企业将个人身份信息（PII）用于其他目的或出售，则必须重新征得个人信息主体的同意。这一基本要求应成为一项全球通用标准。

同样，欧盟数字身份，即欧盟公民和居民的个人数字钱包，使个人信息主体能够自证身份或确认其个人信息。这一电子身份可被欧盟范围内线上及线下的公共服务和私人服务所使用。[12]

全球范围内涉及身份的监管要求存在分散且不一致的现状。在某种程度上，市场已经对不断发生的数据泄露事件感到麻木。个人和机构客户必须对他们披露的敏感数据以及披露的地点保持警惕。首席信息安全官及其团队在制定身份管理政策和策略时，应将客户对负责任使用及数据保护的要求作为核心要素。

[12] 欧盟委员会，“Digital Identity for all Europeans,”（《适用于所有欧洲人民的数字身份》），2021年。

措施建议

保持相关身份识别方式的灵活性以适应不断变化的监管环境，并确保企业的架构能够以超出未来二至四年发展预测的速度将新兴技术整合到安全流程中。

探索更具灵活性和互操作性的身份系统，以促进联合式身份生态体系的发展。

在不断发展的身份生态体系中，思考自身在当前和未来所承担的角色，即身份 / 凭证颁发方，依赖方、和/或数字钱包提供商。

参阅以下报告了解详情

Deepfakes rewrite the cybersecurity playbook

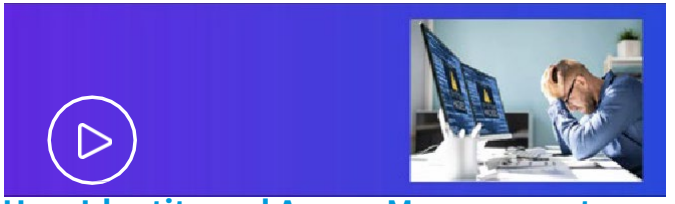
（《深度伪造技术改写网络安全策略》）

弄虚作假不再仅仅局限于愚人节，而是正向身边大大小小的事务蔓延，且很可能对危及企业的稳定性。

Fake content is becoming a real problem

（《虚假内容正逐渐发展成为切实的问题》）

先进的计算技术和人工智能的广泛应用使得几乎任何人都可以制作出高度逼真的虚假内容。



How Identity and Access Management can enhance resilience and DORA compliance

（《身份和访问管理如何增强企业弹性和DORA合规性》）

随着新出台的欧盟监管条例要求对安全问题保持警惕，强大的身份和访问管理框架将成为企业运营不可或缺的重要工具。

聚焦事项八

使网络安全与业务韧性保持一致

当发生网络安全事件时，企业应在几分钟或数小时内做出响应，而非数天或数周内作出响应。在当今动荡的环境中，业务韧性已成为能源、通信和交通等关键基础设施行业中各企业的共同话题，企业高层着重关注如何在预防性控制措施失效后进行业务恢复。企业应将业务韧性与网络安全无缝衔接，强调预防、检测以及快速响应和恢复。网络韧性对于企业维持业务运营能力、维系客户信任和降低未知攻击的影响至关重要。企业应在此领域共同发力，以管理相关风险。

具备韧性意味着能够更快速、全面地管理相关安全事件，并减少对业务的影响。而不是意味着可以杜绝类似事件的发生。首席信息安全官无法控制外部威胁，但却可以把控企业的预防工作开展。

Dani Michaux
EMA网络安全主管
毕马威爱尔兰合伙人

发生安全事件后关键的是挽回信任

当发生数据泄露或被勒索软件攻击事件时，信任作为企业的一项重要资产将最先受到影响。企业预防措施越充分，其事件响应及事件恢复的效率就越块。而事件响应及事件恢复的效率则是重新取得客户信任和投资者（对于上市企业）信任的关键决定因素。

当企业致力于获取和挽回重要利益相关者的信任时，便会坚定地走上业务运营韧性的道路。在某些情况下，挽回信任需要做到快速恢复；而在其他情况下，则需要寻找所提供服务的替代方案。在任何情况下，企业都需要识别出容易被影响和 / 或已经受到影响的利益相关者，迅速处理他们的需求并最大限度减少其损失。

全球各地的监管机构如今都更加强调业务韧性和信任。譬如，英国金融行为管理局于2021年颁布了相关规则，以确保该国金融服务业的重要业务服务在受到干扰时具备足够的韧性。企业必须证明自身具备业务连续性。这些监管规范要求的目的是避免因网络安全事件而对消费者造成广泛伤害并危及市场完整性。[13]

任务重要性：提前规划，专注重点

各企业都有自身独特的工作内容和工作方式，但从安全角度来看，在网络安全事件发生前进行结构化、基于场景的桌面演练，以确保人员、流程和技术的一致性通常具有指导意义。

场景规划不应仅作为一项应付式的任务。基于场景的演练可协助企业明确在应对诸如勒索软件攻击等重大破坏性事件时所做的战略选择，并建立领导层管理、协调响应工作流程，最终帮助企业减少安全事件对客户及客户可信的影响。企业亦必须提前识别需尽快恢复运行的关键业务流程。

网络韧性是指应对和抵御网络安全事件的能力，业务连续性则是指企业在事件发生期间所遵循的运作程序。二者有所不同。韧性具有战略性，而连续性则以流程为导向。因此，在遇到需进行业务恢复的情况前进行韧性演练所面临的压力，要比实际开展处置事项所面临的压力小得多，因为在实际开展处理恢复事项时，企业的多个业务领域可能仍处于恐慌状态。

持续评估企业网络韧性是整体预防工作开展的基石，依据优先级开展演练对于维护网络安全计划的适用性至关重要，可为企业的响应和恢复措施提供详尽的指引。

恶意攻击者会利用新的攻击方式利用不同的攻击向量给企业到来持续性的威胁。这种攻击演变的情况正是首席信息安全官所必须考虑的现实问题。企业通过制定经审批的业务连续性计划作为开展应急响应工作的出发点，比企业在遭受攻击时临时组织开展相应工作更能有效。

避免在应对不断变化的威胁时存在自满心态

企业的基础安全性正逐步提升。与此同时，业务和供应链格局也正在不断演变，企业对信息技术、软件和其他服务供应商网络的依赖性日益增加，且企业也在尝试诸如人工智能、Web 3.0和智能产品等新技术。

而作为攻击方，恶意攻击者（无论是有组织 / 国家支持的，还是单独行动的）也正变得愈发老练，恶意攻击者不断探寻新的载体，并通过盗用身份和深度伪造发起攻击。如今的攻击方式经已发生转变，包括入侵供应链以及通过复杂的“犯罪即服务”生态系统实施的双重或三重勒索软件攻击。[14]

> **“作为企业整体准备工作的主要环节以及优先开展的演练事项，持续评估企业的网络弹性状况对于维持一个既满足目的，又适合当前情况的网络安全计划而言至关重要，可为企业的响应和恢复措施提供详尽的指引。”**

Jason Haward-Grau
毕马威国际全球网络恢复服务主管
毕马威美国主管

[13] 英国金融行为管理局，政策声明 PS21/3，“Building operational resilience,” （《构建企业业务弹性》），2021年3月。
[14] 毕马威国际，“Maintaining cyber vigilance and staying resilient,” （《警惕网络安全问题，维系企业弹性》）2023年。

总而言之，企业需要采取动态的方式来提高韧性。企业不能故步自封，因为不仅威胁在不断演进，恶意者破坏企业内部流程和供应链的方式也在不断变化。

企业应不断改进和调整。具备韧性意味着能够更快速、全面地管理相关安全事件，并减少对业务的影响。而不是意味着可以杜绝类似事件的发生。首席信息安全官无法控制外部威胁，但却可以把控企业的预防工作开展。

企业对时间、人员和预算的投入不应仅仅集中在事件预防上，而应集中在保持韧性的持续性上，使其成为整体网络安全计划中不可或缺的组成部分。

企业和恶意者之间的角力从未停止，而后者由于只需专注于此，因此其发展和创新的速度更快。如果首席信息安全官能够了解并管理企业的安全趋势，便能够削弱攻击者识别和利用漏洞的能力。

企业在应对当今发杂多变的网络安全态势时，不应将业务韧性视为一系列一次性或间歇性的工作。而将其应视为一项适应性战略，业务韧性与企业网络安全目标相辅相成、保障客户利益、契合企业业务目标并注重长期价值。

措施建议

评估企业在下周、下个月或下一年再次遭受攻击时如何更好、更快地做出响应，以确定能够实现“速战速决”，譬如加快付款、确保流动性、改善沟通以及提高应对速度。

建立企业文化并确保其有效落地，并识别企业在数据、服务和基础设施方面的优先级。

定期更新相关计划和指导手册，以适应不断变化的威胁态势以及信息技术和供应链依赖关系的变化。

参阅以下报告了解详情

Maintaining cyber vigilance and staying resilient

（《警惕网络安全问题，维系企业弹性》）

如何从网络攻击中恢复，重建有效性以及避免故步自封。

Cyber and digital operational resilience

（《网络和数字运营韧性》）

以战略韧性作为目标。

Mid-market: a holistic approach to boost cyber resilience

（《中端市场：全面提升网络韧性的方法》）

在日益互联的世界中，风险和期望不断上升。中端市场可以实施全面的网络安全战略来适应当下的环境。

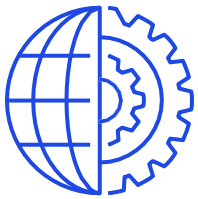
2024年度网络安全战略

首席信息安全官与其他业务线可在来年采取哪些行动确保安全成为企业保障的重要脉络？下文列举了可供首席信息安全官参考的若干可行建议，以期缩短业务恢复时间、减少安全事件对员工、客户及合作伙伴的影响、确保安全计划能为更好的支持业务发展、避免业务暴露于风险之下。

人员

- 与您企业的ESG团队进行沟通，确定其是否将网络安全视为其一大职责。如若不是，则应努力使其认识到网络安全对于ESG中所有三个领域的重要性及相关原因。
- 为董事会提供全新视角，使其了解可能会阻碍企业业务发展的因素，以及应该如何在不影响运营和客户体验的情况下管理此类风险。
- 建立企业文化并确保其有效落地，并识别企业在数据、服务和基础设施方面的优先级。
- 安全团队应确定将安全任务嵌入业务流程的方式和环节，而不是外包给第三方服务提供商，同时安全团队应监控安全任务确保安全任务的正确执行。
- 务实。有效确保网络安全不是让合作伙伴各行其是，而是在企业内部重构关系，激励企业内其他业务领域将安全融入其现有工作。

流程



- 像管理企业一样去管理网络安全团队，即管理者应在一定程度上放松对企业其他部门安全工作的控制。
- 制定企业自动化的初始愿景和战略。明确企业的短期和长期安全目标，确保其与企业的业务优先级保持一致，并确定这些目标所需的安全保护类型。
- 提高企业透明度，从而在全球供应链中赢得信任；不应仅仅将第三方、第四方甚至第五方供应商关系视为交易及合作关系（尽管事实确实如此），而应将其视为企业生态体系的延伸。
- 定期更新相关计划和指导手册，以适应不断变化的威胁态势以及信息技术和供应链依赖关系的变化。
- 采用基于风险的方法来评估第三方流程，而非对提供不同服务的不同供应商采取“一刀切”的管理方式。
- 建议在企业内部以及可信赖的第三方进行情报共享。
- 评估企业在下周、下个月或下一年再次遭受攻击时如何更好、更快地做出响应，以确定能够实现“速战速决”，譬如加快付款、确保流动性、改善沟通以及提高应对速度。

数据与技术

- 识别企业可集中访问的数据，并制定自动化的持续控制监测计划，以提高企业三道防线的效率。
- 了解企业内关键数据（包括结构化和非结构化数据）的存储位置，以及与第三方合作伙伴共享的数据存储位置。
- 确保人工智能算法的目的（无论是企业内部开发还是外部开发）被明的确定义和记录，且人工智能算法的目的与业务目标相匹配，人工智能算法仅适用相关的训练数据，人工智能算法获取相应的同意。
- 利用智能自动化技术来提高对不断变化的供应商风险状况的可见性，并针对第三方建立可持续且可扩展的前瞻性计划。
- 确定应自建或需要采购的工具，了解供应链合作伙伴如何通过自动化技术提高企业间的信任度，并在适当的情况下运用此类经验。
- 探索更具灵活性和互操作性的身份系统，以促进联合式身份生态体系的发展。
- 在不断发展的身份生态体系中，思考自身在当前和未来所承担的角色，即身份 / 凭证颁发方，依赖方、和/或数字钱包提供商。

监管

- 增强企业在网络安全、ESG和隐私方面的全球监管情报工作，以确保及时满足合规要求和报告要求；密切关注和洞悉不断发展的监管法规及其对企业网络安全工作的影响。
- 将人工智能框架与企业战略保持一致，通过调整企业内部各业务领导者的工作优先级，并与在人工智能领域中取得成果的业务部门开展跨职能协助，以开展人工智能治理。
- 了解欧盟出台的《人工智能法案》以及拜登政府颁布的关于“安全、可靠和可信的人工智能”的行政命令中的相关规定。
- 持续关注全球监管环境变化，尤其是对司法管辖区的相关细化规则进行深入了解。
- 保持相关身份识别方式的灵活性以适应不断变化的监管环境，并确保企业的架构能够以超出未来二至四年发展预测的速度将新兴技术整合到安全流程中。

毕马威的服务

上至董事会议题到数据中心运营，毕马威均具有丰富的服务经验。除了评估您的网络安全现状并使其匹配您的业务重点外，毕马威专业人士还可助您开发并实施先进的数字化解决方案、持续监控安全风险、有效应对网络安全事件。无论您的网络安全项目正处于何种阶段，毕马威均可助您实现目标。

作为网络安全服务的领先供应商和实施方，毕马威了解如何开展先进的安全服务和构建符合贵企业需求的创新方案。提供网络安全服务时，我们还可分阶段进行项目交付。因此，无论您采取何种业务合作方式，我们均可甄选了解您的产品和技术的专业人士为您服务。

无论您将进入新市场、推出新产品及服务还是以全新方式与客户互动，毕马威专业人士均可助您预测未来、迅速行动并以安全、可信任的技术建立优势。依赖我们拥有丰富的技术经验、深厚的业务知识以及致力于助您赢得并保持利益相关者的信任的创新人才，这三者的结合造就了不凡的服务体验。

毕马威，铸就不凡。

点击 kpmg.com/cybersecurity 了解更多信息

作者简介

Akhilesh Tuteja
Global Cyber Security Leader
KPMG International
Partner, KPMG in India

In addition to serving as the Global Cyber Security practice leader, Akhilesh heads the IT Advisory and Risk Consulting practices for KPMG in India. He is passionate about how developments in information technology can help businesses drive smart processes and effective outcomes. Akhilesh has advised many clients on cybersecurity, IT strategy and technology selection and helped them realize the business benefits of technology. He is also knowledgeable in the area of behavioral psychology and is enthusiastic about addressing the IT risk issues holistically, primarily through the application of user- behavior analytics.

Kyle Kappel
Cyber Security Services Network Leader Principal, KPMG in the US

As the US Leader of KPMG's Cyber Security practice, Kyle has more than 20 years of experience in the information systems field and a diverse background in cybersecurity, data privacy, regulatory compliance, risk management, and general technology issues. While he has strong technical skills, Kyle utilizes a business-centered approach to solving technology problems by addressing root causes rather than technical symptoms. He is a trusted advisor to numerous organizations, working with senior executives, including Boards of Directors, audit committees, Chief Information Officers, Chief Financial Officers, Chief Operating Officers, Chief Technology Officers and Chief Information Security Officers.

Dani Michaux
EMA Cyber Security Leader
Partner, KPMG in Ireland

In more than 22 years in cybersecurity, Dani has worked with government agencies on national cybersecurity strategies and with international regulatory bodies on cyber risk. She has extensive experience working with clients to improve Board-level understanding of cybersecurity matters. She has built and managed cybersecurity teams as a CISO at telecommunications and power companies in Asia. Dani advocates for inclusion and diversity and women's participation in computer science and cybersecurity. She previously led the Cyber Security and Emerging Technology Risk practices for KPMG in Malaysia and the ASPAC region and also led KPMG's global IoT working group.

Matt O'Keefe
ASPAC Cyber Security Leader
Partner, KPMG Australia

Matt is responsible for driving KPMG's cyber strategy within the 12 KPMG member firms in Asia Pacific. He has more than 25 years of technology, finance, assurance and advisory experience, focusing on financial services industry clients. Matt specializes in technology advisory, particularly in superannuation and wealth management, banking and insurance, and provides a range of services across technology governance and risk, cybersecurity, project management, IT strategy and performance. He is deeply interested in using technology to advance organizational goals, enabling clients' digital strategies and operating models, and protecting data, assets and systems.

Prasanna Govindankutty
Americas Cyber Security Leader
and Principal, KPMG in the US

Prasanna is a principal in KPMG's Cyber Security Services based in the US. He's the Americas Cyber leader with 20 years of specialized experience in cybersecurity and technology risk transformation. Previously, he led the Global and US Powered Cyber solution for KPMG. With a deep understanding of market-leading technology solutions for cyber and governance, risk and compliance (GRC) functions, he helps clients with their integrated transformation. Prasanna leverages his extensive experience in technology-based transformation to help his clients in the energy, media and telecom sectors.

鸣谢

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。

Our global cyber considerations team:

John Hodson
Billy Lawrence
Leonidas Lykos
Michael Thayer
Jessica Booth

KPMG firms'collaborators:

Katie Boswell
KPMG in the US
katieboswell@kpmg.com

Pratiksha Doshi
KPMG in India
pratikshadoshi@kpmg.com

Danny Flint
KPMG Australia
dflint@kpmg.com.au

Brian Geffert
KPMG in the US
bgeffert@kpmg.com

Jason Haward-Grau
Principal,KPMG in the US
jhawardgrau@kpmg.com

Elizabeth Huthman
KPMG in the UK
elizabeth.huthman@kpmg.co.uk

Sylvia Klasovec Kingsmill
KPMG in Canada
skingsmill@kpmg.ca

Mika Laaksonen
KPMG in Finland
mika.laaksonen@kpmg.fi

Angela Leggett
KPMG in the US
aleggett@kpmg.com

Orson Lucas
KPMG in the US
olucas@kpmg.com

Dani Michaux
KPMG in Ireland
dani.michaux@kpmg.ie

Mitushi Pitti
KPMG in the US
mitushipitti@kpmg.com

Caroline Rivett
KPMG in the UK
caroline.rivett@kpmg.co.uk

Henry Shek
KPMG China
henry.shek@kpmg.com

Akhilesh Tuteja
KPMG in India
atuteja@kpmg.com

Marko Vogel
KPMG in Germany
mvogel@kpmg.com

Jim Wilhelm
KPMG in the US
jameswilhelm@kpmg.com

联系我们

石浩然
网络安全和数据保护咨询服务主管合伙人
毕马威中国
电话：+852 2143 8799
邮箱：henry.shek@kpmg.com

张令琪
网络安全和数据保护咨询服务主管合伙人
毕马威中国
电话：+86 (21) 2212 3637
邮箱：richard.zhang@kpmg.com

郝长伟
网络安全和数据保护咨询服务合伙人
毕马威中国
电话：+86 (10) 8508 5485
邮箱：danny.hao@kpmg.com

张倪海
网络安全和数据保护咨询服务合伙人
毕马威中国
电话： +852 2847 5026
邮箱：brian.cheung@kpmg.com

黄芃芃
网络安全和数据保护咨询服务合伙人
毕马威中国
电话：+86 (21) 2212 2355
邮箱：quin.huang@kpmg.com

周文韬
网络安全和数据保护咨询服务合伙人
毕马威中国
电话：+86 (21) 2212 3149
邮箱：kevin.wt.zhou@kpmg.com

林海燕
网络安全和数据保护咨询服务合伙人
毕马威中国
电话： +852 2143 8803
邮箱：lanis.lam@kpmg.com

kpmg.com/cn/socialmedia

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/offices.html