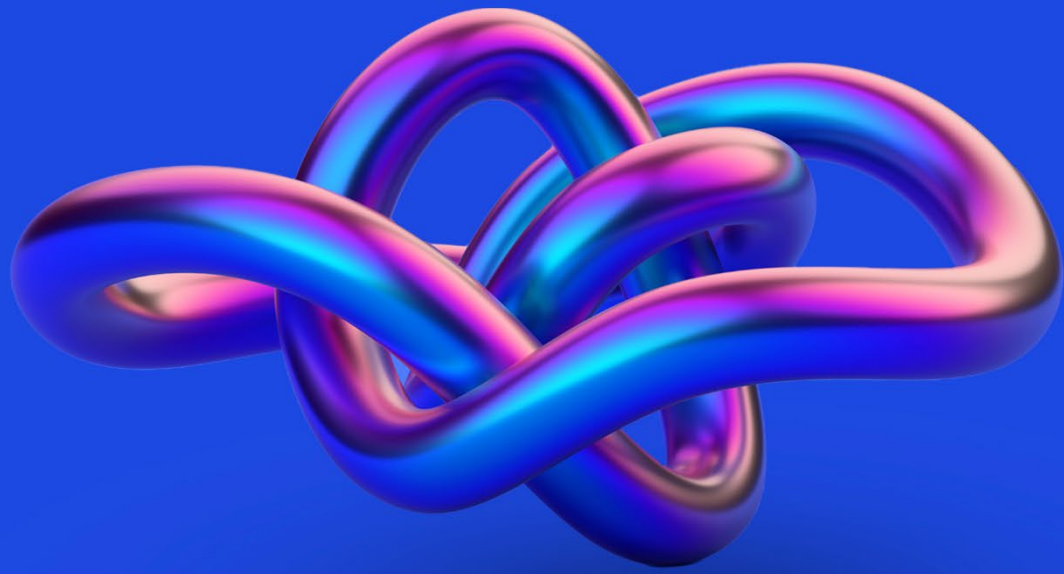
KPMG

毕马威

2023网络安全重要趋势



重要脉络

毕马威国际

kpmg.com/cyberconsiderations

前言

数据和数字化基础设施建设已渐渐成为未来发展的重要支柱。新冠疫情使全球数字化转型的进程大大加快，并使其成为焦点。全球各经济体和各行各业的供应链正经历着颠覆性变革，企业亟需重新审视自身对供应链上下游的产品、服务和数字化基础设施的依赖程度。

人工智能、区块链、生物识别、物联网和虚拟现实等突破性技术有望塑造我们的未来，但这些技术会带来新的安全、隐私和道德挑战，甚至可能使人们对数字化的发展进程提出质疑。由于国别文化观点的差异性，各国难以就上述问题的应对措施达成一致，但这正是全球化企业面临的经营环境。因此，我们应以创新方式处理当下的问题，而非被动地应对其造成的后果。

我们认为具有重要系统的行业也在变化。过去，我们聚焦基建设施、电信行业和金融服务行业。现在，我们关注更为复杂多样的公私伙伴关系、互联生态系统和信息基础设施。例如：我们注意到如今的金融市场环境就像是一个由金融机构、市场化的基础设施、数据和托管服务供商组成的具有密切关联的世界，其所有要素都具有同等重要性。随着关联性和依赖程度的增加，基础设施也逐渐成为黑客攻击及利用的对象。

这些改变也导致全球网络安全监管力度持续加强，进一步加重企业负担，企业对日益增长的监管和报告需求产生了更多的担忧。因此，企业越发重视将隐私和安全要求嵌入到日常经营过程中，这既是为了应对不断变化的网络安全威胁，也是为了满足不同国家的差异化的监管要求。

网络安全应贯穿各业务条线、职能、产品和服务中。企业应致力确保网络安全深入贯穿数字化的各个方面，并融入到企业整体战略、发展和运营中。毕马威国际首席全球数字官Lisa Heneghan表示：

“企业应将网络安全贯穿其各个方面。网络安全建设应成为支撑业务的关键要素，以及数字化的信任基础。但网络安全不能仅靠首席信息安全官及其团队完成，而应成为企业所有员工的责任。这绝非易事；员工应了解网络安全与自身的关系，再思考如何将安全纳入现有流程之中。在建设企业网络安全过程中，如果将各业务部门视作顾客，根据已有经验为其定制化安全管控策略，能够大大加强并激励企业员工的网络安全责任感，积极遵守安全行为，为企业业务经营带来巨大收益。”

首席信息安全官将在业务连续性、数字化进程的业务中断等议题的拥有更多话语权，且扮演更重要的角色，他们能够帮助企业更好地了解需要保护的资产和数字化服务，并对相关的系统提供保护以建立信任。

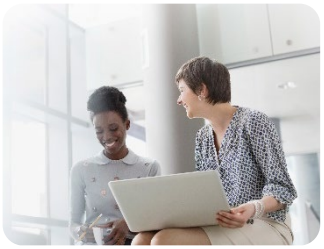
本报告旨在探讨未来一年首席信息安全官可以采取的行动，以向董事会及高管层表明：数字信任可以并且应当成为一项竞争优势。

人员、流程、数据/技术及监管建议参见第22页。

Akhilesh Tuteja
网络安全全球主管
毕马威国际

2023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

数字信任：一项共同承担的责任

企业在如何保护员工、客户、供应商及合作伙伴利益的问题上是否已进行充分考虑？

02

以“无形”措施护航安全

安全团队如何有效地将安全性整合进业务流程、敏捷开发项目和各种运营模式之中？

03

实现无边界的、以数据为中心的未来

在无边界的环境中，企业如何切实向零信任模式过渡，为生态系统寻求全方位保护？

04

新合作，新模式

企业如何在外包与托管服务与日俱增的环境中维持安全、隐私和业务连续性。

05

自动化技术可信

企业如何确保机器流程自动化、机器学习和其他形式的人工智能得到有效、合理和安全的实施和管理？

06

智能世界安全

企业目光逐步转向智能化、超连接产品，对安全及隐私团队有何影响？

07

应对多变的网络攻击

安全团队如何应对日益变化的网络攻击威胁，并应对越发猛烈的网络攻击？

08

业务连续性

为何企业在考虑应对之外，还应积极部署备份恢复计划？

聚焦事项一

数字信任：一项共同承担的责任

随着监管与公众对隐私、安全和道德的关注度日渐提升，数字信任正逐渐成为董事会的议题之一。任何通过数字化赋能业务的成功均须建立在数字信任之上，而网络安全和隐私保护正是建立此信任的重要根基。首席信息安全官必须协助董事会和高管层赢得并维持利益相关者的信任，以为自身企业创造竞争优势。此目标的实现要求所有利益相关者的共同承诺和通力合作。

全球化已令全球跨界相联，新冠疫情对全球供应链带来的颠覆影响充分反映了这一现实。为了与客户建立长久的关系（无论是B2B还是B2C），企业都必须建立和维护数字信任。

数字信任涵盖诸多领域，触及企业运营的各方面，并与企业战略存在着密切联系，这不仅因为它能为企业带来竞争优势，它还能造福行业和乃至社会。

John Anyanwu
网络安全服务合伙人
毕马威尼日利亚

信任与价值

信任是成功的关键，其牵涉的不仅是企业声誉。信任的提升可为企业带来竞争优势以及收益。

超过三分一的企业认为信任提升将可带来盈利增长。

但 65% 的企业表示，信息安全建设仅是合规驱动，而非长期战略目标。

65% 的高管依然将信息安全视为被动的降低风险手段，而非业务赋能要素。

49% 的企业认为董事会将信息安全视为必要成本，而非建立竞争优势的途径。

信息来源：《2022年毕马威网络信任洞见调查》

数字信任正引起关注

越来越多高层管理者意识到数字信任的裨益：37%的高管认为能促进盈利增长是信任提升的最大商业优势。[1]数字信任涵盖广泛。网络安全广泛关联到数字信任的问题（包括可靠性、安全性、隐私性和透明度）。它们会影响企业所采取的业务开展、价值追求方式、产品、服务，所用技术，应用系统的数据收集及使用方式，以及针对客户、员工、供应商和所有第三方合作伙伴、利益相关者所实施的利益保护手段。

相比而言，65%的高管仍然将信息安全视为被动降低风险的手段，而非业务赋能要素。[2] 许多企业仍然将网络安全视为成本开销，而非对未来的投资，这是一种错误的理念。首席信息安全官应全面接纳数字信任这一概念，并阐明安全性作为业务赋能要素将如何为企业的数字化发展提供稳健支持。

首席信息安全官须协助企业建立数字信任体系，但仅靠他们并不能完成，而应投入足够的时间，鼓励其他主要的内外部利益相关者承担在数字信任体系建立过程中的角色。事实上，首席信息安全官需要向董事会和高管层阐明此事的重要性，并说明数字信任体系与业务战略的依存关系。

世界经济论坛认为，业界已开始承认网络安全就如同企业风险、产品开发和数据管理一样，是一项重要的战略业务要素。世界经济论坛在其“Earning digital trust: Decision-making for trustworthy technologies”（《赢取数字信任：为可信任技术制定决策》）报告中提及：“获取数字信任需要一套整体的方案，而网络安全是建立信任重要维度之一。”[3]

数字信任对客户的意义

虽然一般个体消费者可能不关心企业数据保护程序中的具体措施，但一旦客户知道数据遭到泄露，便希望了解企业正采取什么应对措施，也希望确认企业会以客户的利益为重。企业能迅速、透明地应对数据安全事件，从而重新建立客户信任。

当今，消费者理解数据泄露事件不可避免，但如果企业能够持续提供有竞争力的产品价格和优良的服务，并保持良好的客户体验，当网络安全事件发生时，及时通报应对情况以及恢复措施，客户一般不会大量流失。

“透明性对不同受众有着不同的含义。当网络安全事件发生，消费者要求企业公布相关情况时，企业必须也了解其供应商和合作伙伴如何保护用户信息。这是因为企业应对客户承担更多责任，并确保在个人信息保护方面不辜负客户的信任。”

石浩然
网络安全服务合伙人
毕马威中国

[1]毕马威国际，毕马威网络信任洞见调查，《通过网络安全与隐私保护建立信任》（Building trust through cybersecurity and privacy），2022年。
[2]同上。
[3]世界经济论坛，《赢取数字信任：为可信任技术制定决策》（Earning Digital Trust: Decision — Making for Trustworthy Technologies），2022年11月。

构建有效的数字信任战略

企业应将数字信任这一概念纳入企业战略、产品开发、整体市场形象和公私客户关系中，广泛思考数字信任对不同利益相关者群体的意义，以突出网络安全以及其他建立数字信任核心要素的重要性。

信任是采取特定技术所必须具备的要素，亦是领导层决策的基础。首席信息安全官需要持续向董事会及高管层阐明网络安全为何是数字信任的关键组成部分。

简而言之，能通过其产品、服务、运营模式建立利益相关者的数字信任并妥善保护其业务信息的公司，将更可能收获商业及声誉回报。

Annemarie Zielstra
网络安全服务合伙人
毕马威荷兰

首席信息安全官需要协助选定合适的合作伙伴和供应商。评判标准须包含信息保护程序的透明度以及具备业务连续性的能力。

毫无疑问，监管机构极有可能加强对数字信任的监管，对企业公开透明程度及问责要求也可能相应提升。企业若能以数字信任原则为导向，采取更为全面的方式应对日益复杂的各类监管要求，能够有效减少以合规驱动为目的所造成的高昂成本。

数字信任战略应自上而下逐步实施，领导层应先认可上述理念，再落实到企业其他成员。这也意味着企业可将其在年报中突出展示其数字信任理念和战略。鉴于34%的企业领袖担心其企业是否有能力满足监管对于网络安全和隐私透明度的报告要求，毕马威提出了一个主动应对方案。[4]

参阅以下报告了解详情

Cyber trust insights 2022
（《2022年网络信任洞察》）
通过网络安全与隐私保护建立信任。

Earning digital trust, together
（《以合作赢取数字信任》）
信任在当今互联世界中变得空前重要的原因。

Reversing the digital trust deficit
（《弥补数字信任缺失》）
重建数字信任作为技术进化的紧迫需求

[4] 毕马威网络信任洞见调查，同上。

聚焦事项二

以“无形”措施护航安全

将安全融入企业业务，在某种程度上可以帮助员工自信工作、高效决策，并在他们的岗位上持续保护企业信息。这虽然充满挑战，但仍是首席信息安全官的关键目标。人们很容易将安全视为工作的障碍，首席信息安全官只有结合用户和业务角度考量安全性，才能改变这种观点。

最重要的一点是，我们需要了解在何时以何种方式构建信息安全管控措施，以及增强安全管控措施后对企业的影响。世上不存在绝对的安全性。若首席信息安全官试图使用最为严格的安全管控措施在任何时候保护任何信息，则可能全盘皆输，因为用户会设法规避这些安全管控措施。首席信息安全官需结合具体业务流程的重要性及其可能产生的风险，设计相应的安全控制。

最终，适当且易懂的安全控制对用户而言较能接受，用户才是您最好的防火墙。

Julia Spain
网络安全服务合伙人
毕马威英国

对首席信息安全官有信心

企业对首席信息安全官完成重要任务的能力表现出高度的信心。

79% 的企业对首席信息安全官能够绘制企业内部关键数据流转情况具有信心。

3/4 的企业对首席信息安全官能够识别其最有价值数据具有信心。

78% 的企业确信首席信息安全官充分了解有多少敏感数据已被传送到第三方，以及这些数据已受到妥善保护。

信息来源：《2022年毕马威网络信任洞见调查》

企业不应以对立的方式考虑企业安全性。如今，企业安全目标并非一成不变，“安全”与“不安全”的概念也只是暂时性的。首席信息安全官应更多致力于安全宣贯；为员工设计简单、直观的安全流程；打造一个安全意识较好的文化氛围和高效的安全团队。

企业安全也应考虑客户体验

企业更应重点关注，为有能力和意愿检测和响应恶意行为的员工设计并建立落地的恶意行为检测和响应流程。考虑易用性、客户体验，将安全规划纳入其他企业级别的重要事项（例如：业务需求），而不是将其纯粹视为监管的当务之急。

最新的技术发展可为此提供帮助。从防御性人工智能、机器学习和聊天机器人，到云加密、区块链和增强型检测及响工具等，均是上述重要事项的核心部分。此外，提升员工的安全意识，建立统一IT治理策略，倡导员工审慎对待数字化通信，也将有助安全性提升。首席信息安全官应思考如何帮助员工自发采取正确措施，并制定合适的安全管控措施予以支持。

单凭技术不能解决问题。数十亿资金用于网络安全领域，数千家网络安全公司也已提供各类网络安全工具，但企业仍然易受攻击，因为攻击者也知晓并精通同样的工具。

Prasad Jayaraman
网络安全服务主管
毕马威美国

网络安全将持续变化，企业可引入新的网络安全工具和控制措施。但我们仍然希望企业能够在构建之初就考虑到人为因素。企业进行重大变更时需要考虑很多因素，安全性应是其中之一。将安全性嵌入企业日常运行流程中（如“开发、安全、运营”（DevSecOps）和运营技术与采购）或是一种适当且有效的途径，激励员工安全行事，以发挥人的防护作用，而非过度管控。

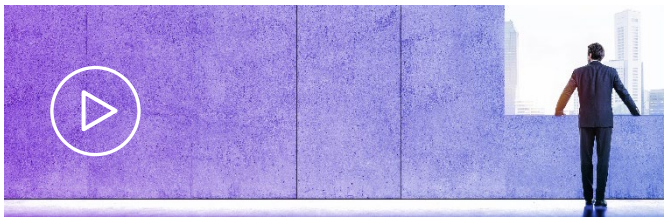
在技术范畴外，首席信息安全官还应关注人为因素。对员工的信息安全意识进行教育与培训，企业应在内部建立良好的信息安全文化氛围。

Eddie Toh
网络安全服务合伙人
毕马威新加坡

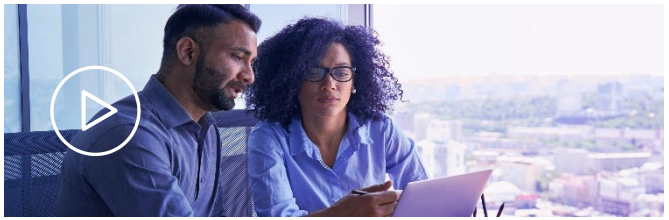
安全团队可从企业提升用户体验的方式中汲取大量经验。内部信息安全流程应简单、直观，否则员工可能会规避相关流程；企业可考虑在信息安全流程的设计中纳入用户体验专员。

对内部用户而言，安全流程也可适当“私人化”。企业可要求员工作出自我判断，根据事件场景，将私人生活与工作中安全行为进行比较，使他们“寓教于乐”。 如此，员工便可在企业安全中发挥作用，并摆脱薄弱环节的形象。

参阅以下报告了解详情



Human firewalling（《以人为盾》）
克服网络安全中人的风险因素。



Synthetic identity fraud（《虚假身份欺诈》）
一个价值60亿美元的问题。

Want better cybersecurity? Don't check that box
（想要更好的网络安全？不要勾选那个框）
对企业安全性构成最大威胁的可能不是勒索软件或网络钓鱼攻击，而是您的行为取向。

聚焦事项三

实现无边界的、以数据为中心的未来

显而易见，过去十年的商业模式发生了根本性的变化，逐步演变以数据为中心，由企业内部与第三方合作伙伴、服务提供商组成的互联生态系统。在当前的分布式计算世界中，为缩小任何潜在服务中断或安全事件的影响范围，首席信息安全官和信息安全团队必须采用全新的方案，如“零信任、安全访问服务边缘（SASE）和网络安全网格模型。”

如今，企业的当务之急是使员工、客户、供应商和其他第三方能够无缝、远程和安全地联接。但安全挑战也随之而来：在如今的无边界环境中，企业再也无法信任每一个用户和设备。

对无边界业务零信任

零信任的处理方式有助缩小服务中断或安全事件的影响范围，使企业能够更好地管控安全事件的影响。

传统的网络边界安全管理策略在如今的互联数字化世界中已过时。首席信息安全官须为基于公共及私有基础设施，以及分布式用户生态系统的更为广泛的受攻击范围提供保护。因此，他们必须以信任为基础，确保所有设备在任何时候，任何地点的安全性，从而为业务提供保障。

Natasha Passley
网络安全服务合伙人
毕马威澳大利亚

数据安全对利益相关者至关重要

在无边界环境中，企业如何保护、使用和分享数据的难点，是削弱利益相关者对企业数据使用及管理能力信任度的首要因素。

28% 的高管认为“对已实施的安全治理机制缺乏信心”是削弱利益相关者对企业的数据使用及管理能力信任度的首要因素。

32% 的高管还认为“对于某一服务为何需要数据支持，以及提供/共享这些数据将使企业如何受益缺乏清晰的表述”是另一个因素。

36% 的高管尤为关注对其数据的保护方式。

35% 的高管尤为关注对其数据的使用或共享方式。

信息来源：《2022年毕马威网络信任洞见调查》

以零信任为基础的安全访问服务边缘（SASE）和网络安全网格模型在网络整体安全性的构建、分布和统一方式上有着共同的原则。但最重要的是，随着更多企业采用以云为中心的理念，安全机制应更多的考虑对数据保护。

作为当前无边界业务环境的保护伞，零信任框架对身份鉴别、访问控制的设计和赋能如何顺应时代变化提供了思路。零信任为基于安全访问服务边缘（SASE）模型以及全面的分析性网络安全网格架构的业务融合提供了支持。

新的身份鉴别与访问控制模型

去中心化的身份鉴别与访问控制是首席信息安全官的核心职责，亦是一项网络传输议题。南北向传输，即用户到资源，其主要关乎身份识别；而东西向传输，即系统间横向传输，则与网络区域划分和其他控制领域相关。

数据资源的访问应与用户身份进行匹配。在一个无边界环境中，若不重视身份和数据治理，便不存在零信任、安全访问服务边缘（SASE）或网络安全网格。

对首席信息安全官而言，实施零信任的挑战在于验证设备和用户身份及其可信度。这要求首席信息安全官从身份校验角度思考安全性问题，并重点关注企业内用户和第三方供应商的最小权限访问。

零信任实践运用

企业应根据各场景、用户和资源定义零信任，这也是企业信息安全建设的关键和核心原则。首席信息安全官不仅应建立零信任体系，还应确立相关政策、准则、和设计系统解决方案，同时成立由安全技术人员和领导层组成的信息安全委员会。

另一个挑战是资金和预算。首席信息安全官应能够阐明零信任相关框架，以让董事会和其他企业领导理解该投资不仅是一项新的技术，还有助于建立全新理念以实现安全、无边界未来。

显然，在本地部署和云端部署方案中找到平衡点是一大挑战，尤其当企业采用云端开发的技术时。许多企业正考虑将多个系统迁移到云上，但通常现有的基础设施不能完全满足安全访问服务边缘（SASE）所需的技术需求。

大型复杂机构的首席信息安全官会面对同时管理云端和本地部署的安全运营环境且短期内运营成本较高的挑战。对于希望完全采用云端部署的客户，应考虑在部署到云上的系统中采用与本地部署同样的零信任原则。同时也应考虑运营模式改变带来的影响，譬如，使用云服务商提供的合理管理的责任模型可有助确保云架构的安全。

> **“身份生态系统在当今的零工经济世界中已经迎来爆发式增长。因此，企业仅能通过身份鉴别准确识别人与机器。”**

Deepak Mathur
网络安全服务主管
毕马威美国

参阅以下报告了解详情

The convergent future of identity（《未来身份融合》）

身份识别与访问管理的发展趋势。

Assume nothing, verify everything（《不做假设，只做验证》）

零信任为何是未来的发展方向。

Safeguard your digital environments from all angles（《全方位保护您的数字化环境》）

开始零信任之旅的五个步骤。

聚焦事项四

新合作，新模式

对于企业安全团队而言，仅关注自身企业的IT系统安全的日子已过去。在网络安全工作外包问题上，首席信息安全官需要了解何时叫停、何时应继续推进，并决定当前与未来应在企业内部保留哪些职能。安全性已成为业务的优先考虑事项，并通过企业与服务供应商之间的共同担责的模式落地。

如今，首席信息安全官应从技术安全、产品安全和复杂的供应链安全为企业内部的信息安全流程实施提供支持。企业越发意识到，通过供应链、客户服务、企业设计以及信息安全共同协作能够提升创新。

以具有竞争力的价格向客户提供此类创新组合，企业可建立竞争优势。

然而，部分企业难以大规模地有力开展信息安全工作，其主要原因是缺乏信息安全的专业人才与技能。因此，他们把目光投向服务外包、托管服务、系统上云等模式。

“虽然许多企业已将部分业务流程外包给第三方服务供应商，但数据安全及身份与访问管理相关控制仍然属于内部职责。”

Markus Limbach
网络安全服务合伙人
毕马威德国

受信任的生态系统

外部合作也将是企业在超连接生态系统中取胜的关键，但企业的协作之路上存在着实际的障碍。

79%的受访者表示，与供应商和客户建立信息安全合作至关重要，但仅有

42%的受访者表示已据此行事。

60%的受访者承认，他们的供应链使其容易受到攻击。

78%的高管对首席信息安全官能确保供应链上下游数据安全表示有信心。

信息来源：《2022年毕马威网络信任洞见调查》

了解应保留的安全职能

企业不能将所有的安全管理职能外包，还需要在企业内部保留适当的专业人才与技能。企业应具备专业知识，以建立能使内部员工和第三方服务供应商有效运营的内部控制及安全架构。其中一个要点是，企业应了解其内部应保留哪些安全职能，然后制定有针对性的人才招聘策略。

以应用系统上云为例，首席信息安全官需同时扮演经纪人、协调者和统筹者等多重角色，以协调相关员工和第三方服务提供商，并进行风险识别、治理与汇报。上述职能不能完全外包。虽然企业可以将计划与准备阶段的部分工作进行外包，但应由企业内部了解业务与企业安全现状以及潜在网络安全事件影响的人员，来进行整体把控以及质量控制。

“与传统的信息安全工程技能对比，在云生态环境中搭建网络安全控制需要完全不同的技能。许多企业不具备按照业务增速需求管理复杂的组织架构的网络安全、API接口、不同技术设备的能力。首席信息安全官应致力于培养此项技能。”

Matt O’Keefe
网络安全服务合伙人
毕马威澳大利亚

寻找合适的技能组合

首席信息安全官应了解自身的内外部职责，有效应对不同模式和领域之间的灰色地带，建立适当的控制以应对复杂多变的环境。然而，这知易行难。

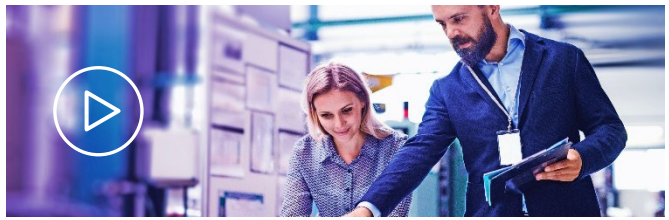
与外部安全服务供应商合作同样要求企业具备独特的技能。企业须注重流程管理和安全治理技能，而非技术能力。无论将多少工作外包，企业内部都应具备充分的安全知识和技能。同时各方应开展定期、清晰的沟通，以保障对已实施的管控措施以及关键绩效指标的妥善管理。此外，企业还应商定明确的安全事件响应流程，并开展应急演练以测试相关系统。

首席信息安全官应定期评估其自身的专业技能，并努力确保企业具备与云、托管服务供应商有效协作的能力。为此，首席信息安全官应了解企业的未来信息安全基础设施建设需求，并确定安全管理体系以提供最佳支持。企业应着眼于“未来”，即展望未来三至五年的安全需求，而不应仅仅着眼于企业当下的安全需求。

参阅以下报告了解详情

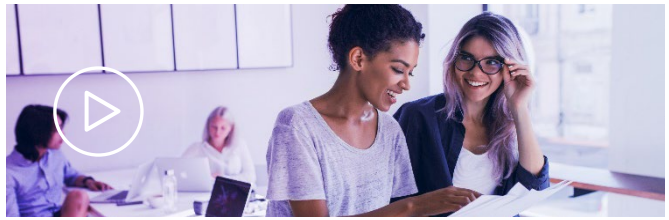
Third-party risk management outlook 2022（《2022年第三方风险管理展望》）

是时候立即行动。



Evolving vendor, operational and strategic risks（《不断演变的供应商、运营与战略风险》）

第三方风险管理。



Third party and cloud: Regulatory challenges（《第三方与云：监管挑战》）

企业正更频繁地与第三方建立更复杂的关系，导致风险增加和升级。

聚焦事项五

自动化技术可信

企业在参与创新与驾驭新兴科技的竞争中，安全性、隐私性、数据保护和道德问题在受到越来越多关注的同时，也常常被忽略和遗忘。企业对这些问题的疏忽可能会对自身发展构成阻碍，尤其在人工智能相关监管要求仍在逐步明确的时代背景之下。

过去人工智能长期停留在数据科学实验阶段，其中只有少数项目真正实现投产。而现在有实际应用价值的机器学习时代已经到来。在未来18到24个月，将可能会有更多此类项目上线。

该领域已进行长期反复试错，但这些机器学习将最终带来巨大的成功，如智能推荐引擎、决策支持工具、精细模拟和神经网络等，可为企业带来巨大的价值。

将单调、重复工作的自动化处理，可节约员工时间和提升效率，令他们能专注于需要进行复杂、周密和细致思考的工作。因此，人工智能正在多个行业中应用。在银行业，机器人正协助客户选择最合适的产品和服务；在保险业，企业正在开发如何通过自动化策略对申请人进行信用评估。

“安全团队应了解业务对机器学习应用的理解和构想，才能为企业赋能。基于对业务构想的理解，安全团队能够着眼于他们将使用的系统、识别合适的输入数据并开展工作，以应对使用人工智能系统可带来的负面风险。”

Michael Gomez
网络安全服务主管
毕马威美国

人工智能/机器学习带来的挑战

社会和市场愈发关注在大数据分析中使用人工智能和机器学习技术所带来的道德、安全和隐私相关的问题。

78% 的受访者同意，人工智能和机器学习会带来网络安全上的独特挑战。

3/4 的受访者表示，人工智能与机器学习引发了基本的道德问题。

76% 的高管同意，企业需要对训练、监控人工智能和机器学习系统产生额外投入。

76% 的高管同意，企业应对自身如何使用人工智能和机器学习技术保持一定透明度。

信息来源：《2022年毕马威网络信任洞见调查》

建立可信任的人工智能模型

企业是否正合理应用人工智能以获得最高产的输出？在某些保险业用例中，算法会自动对生活在特定区域的申请人作出分级。生活在较不富裕区域的人士与在较上层地区的人士会分为不同级别。保险费会根据申请人的地址而异。人工智能具有偏见或歧视性，因此需要加以调节。

过去应用系统的开发常基于固定的模式，即输入与对应输出之间的关系不变。开发者也会对此进行测试。终端用户会决定他们是否喜欢使用该应用，以及是否希望继续与开发者进行业务往来。

机器学习和人工智能设备旨在不断学习和进化。在此技术特性下，企业将根本性地改变他们对这些系统的看法以及系统的优化方式和使用目的。

人们对人工智能有着不同的理解和喜恶情绪，而许多企业根本不具备足够了解人工智能的专业人员，所以更谈不上如何安全应用此技术。

> **人工智能十分强大，但如果自动化决策无意中产生偏见或歧视，则可能会对个体造成伤害。**

Sylvia Klasovec Kingsmill
隐私业务合伙人
毕马威加拿大

如研发运维一体化平台（DevOps）一类的机器已能够缩短开发周期并确保持续交付。但如果企业还未将安全性整合进机器赋能的环境中，则大规模应用或许永远无法实现，因为员工根本不会信任该技术。为此，76%的高管同意，企业需要对训练、监控人工智能和机器学习系统产生额外投入。[5]

人工智能和数据隐私

人工智能使许多核心隐私原则得到增强，例如，安全团队需要更深入地分析用户数据。企业需要考虑其收集的数据类型符合某些法规的数据最小化收集要求。此外，鉴于人工智能可能会存在偏见，因此，企业必须对人工智能的产出保持公开透明。

监管机构、政府和相关行业必须携手合作。人工智能监管并非仅是隐私问题，还要求数据科学家与隐私专家合作以确定技术方案应嵌入哪些要求以确保方案的安全性、可信度和隐私敏感性。此外，政府需要订立基本要求，并制定数字化建设方向，以号召相关行业对人工智能创新进行投资。

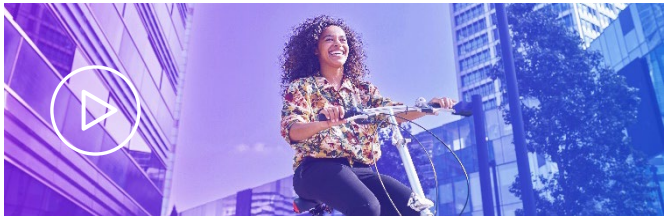
各地政府机构似乎往往会将人工智能视为一种竞争，监管机构也正在开始尝试限制新兴人工智能技术带来的干扰性及高风险性应用。

在二十国集团通过可信任人工智能原则后，人工智能风险管理及监管领域有了重大进展。新加坡首先颁布了人工智能安全标准；美国国家标准与技术研究所公布了人工智能风险管理框架；欧盟也在同年颁布人工智能法案。正如《通用数据保护条例》对隐私产生巨大影响一样，这些法规也最终将在人工智能领域带来重大影响。企业需要为此做好准备。

参阅以下报告了解详情

Is my AI secure?
（《我的人工智能是否安全？》）

了解人工智能为您的企业带来的网络风险。



Trust in artificial intelligence: Global insights 2023
（《信任人工智能：全球洞察2023》）

探讨人们对人工智能的信任以及人工智能为企业和社会带来的裨益与风险的全球调研。

The path to transparency — and trust
（《通往透明度与信任之路》）

企业数据责任调研。

[5] 毕马威网络信任洞见调查调研。同上。

聚焦事项六

智能世界安全

几乎所有行业的企业均在转变其产品思维，以专注于开发互联网赋能的服务并管理配套设备。随着企业逐渐意识到产品安全具有同等重要性后，首席信息安全官及其团队开始被邀请参与工程、开发及产品支持团队的讨论。

在今天这个以智能产品为重的环境中，以下新兴技术起着主导作用：

5G
实现高速、超连接和减低延迟

量子计算
大幅减少处理及计算时间

信任架构
有助确保互联设备之间传输的数据和身份认证是安全可靠的

软件 2.0
通过人工智能快速编写代码能够降低复杂度并提升开发速度（从数月缩减到数周）

应用人工智能
将人工智能大力应用于真实世界，协助智能产品研发

技术创新的步伐并不会减慢，并常常迫使监管机构和安全团队全力追赶。首席信息安全官不应被动地等候下一波法规的到来，也不应仅依赖监管，而是要主动、务实地在产品生命周期和供应链中实施安全控制措施。这绝非小事，首席信息安全官与企业内其他职能的合作程度决定了此事的成功与否。

Walter Risi
网络安全服务合伙人
毕马威阿根廷

首席执行官网络安全见解

对网络安全挑战的不断深入了解也让首席执行官们更清楚其企业的准备程度。

24% 的首席执行官承认他们对网络攻击准备不足（2021年为13%）。

56% 表示他们已作好准备。

3/4 表示其企业已实施相关方案应对勒索软件攻击。

3/4 的首席执行官表示，确保合作伙伴的安全和供应链安全与在企业自身内部建立网络防线同等重要。

信息来源：《2022年毕马威首席执行官展望》

智能设备也面临许多风险，如存在使用弱密码，使用不安全的加密算法或未加密，未更新软件、病毒库，缺乏DDOS防护等。首席信息安全官必须认识到，智能设备安全并非仅涉及系统的保密性、完整性和可用性。由于这些智能设备在现实世界中的使用，现实世界中使用该技术的安全性也应纳入考虑范畴。由于有较大可能会出现大规模针对性攻击，因此，网络安全专家必须将这些风险纳入到一个涵盖保密性、完整性、可用性和安全性（“CIAS”）的架构中。

随着我们迈入一个由不同的生态、产品、设备与传感器组成的世界中，且这些组成部分日益成为网络攻击的目标，监管机构越来越关注企业如何在产品生命周期中考虑安全性。

在智能产品生命周期中嵌入安全性存在多种挑战，包括主动监控、识别和处理相关的网络漏洞等。首席信息安全官的关键挑战之一是如何与质量控制部门合作，将安全性嵌入产品设计及装运前检测流程中。

Motoki Sawada
科技风险服务合伙人
毕马威日本

在智能设备互联世界中应用CIAS框架

首席信息安全官应考虑智能设备产品生命周期中四个组成部分的相关风险，其中各个组成部分有着不同的“开发-安全-运营”（DevSecOps）要务。这些组成部分包括：从设计实施到发布的产品开发流程，管理不断延伸的供应链，维护和持续更新软件以及终端用户（无论是另一家企业还是个人消费者）。这四个组成部分有助首席信息安全官制定安全规划并确保产品的安全性。首席信息安全官必须洞悉业务的所有领域。

首席信息安全官应与企业内各部门合作，以确保整个企业将网络安全性视为一项风险管理要务。此外，认为安全性仅与可在设备内应用的技术流程有关是一个狭隘的想法。企业还应考虑安全性对供应链等领域的广泛影响。

Jayne Goble
网络安全服务总监
毕马威英国

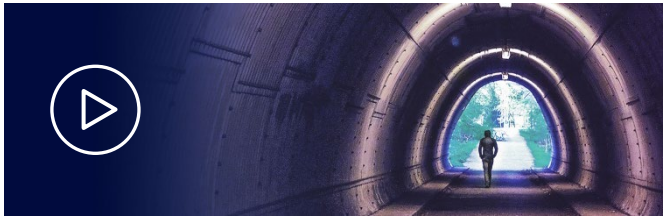
智能设备内部的软件系统往往不能轻易地进行更新，主要是因为考虑到设备与现实环境的连接性，不能在使用过程中进行补丁修复。这同样也取决于设备的重要性。这为开发者带来了额外的挑战，即必须嵌入保障机制以及制定适当的软件清单，让企业能够在设备使用过程中发现重大漏洞时并尽早召回设备。

网络安全已成为一项市场差异化因素。或许这已不言而喻，但企业有必要让现有和潜在客户以及整个市场知道其正不断提高网络安全能力（尤其是设备控制）并从设备全生命周期着眼进行管理。预计全球监管机构将日益关注这些系统的安全性以及最低标准要求。

参阅以下报告了解详情

Control systems cybersecurity report 2022（《工业控制系统网络安全报告2022》）

在发展进程上克服不断增长的网络威胁路障。



A pathway to cyber resilience（《建立网络空间恢复补救能力》）

评估及防范各个行业的网络漏洞。

Accelerating OT security for rapid risk reduction（《提升运营技术安全性以快速降低风险》）

在运营技术环境的数字化和互联程度不断提升的同时确保安全性。

聚焦事项七

应对多变的网络攻击

非法攻击者从入侵企业到全范围激活勒索软件的时间所需的时间越来越短，越来越多的非法攻击者以及有国家队攻击者通过自动化渗透工具，加速对企业系统的渗透。企业应优化和标准化安全运营流程，使其能在安全事件发生时尽快恢复核心业务和服务，从而降低安全事件对客户及合作伙伴的影响。

网络攻击者有两项明显动机：利用漏洞与制造混乱。他们利用漏洞系统是为了窃取或篡改数据，无论是出于获取情报还是欺诈目的；制造混乱是为了勒索或获取政治利益。其中的攻击手法各不相同。

某些有国家背景的攻击者专门攻击关键的基础设施，如输油管、电力公用设施和金融系统。他们的目的是造成伤害或混乱并施加政治或经济影响，从而为攻击者及其支持者谋利。其意图是从其他人的不幸中获利。

网络攻击事件的成功率已大幅增加，导致近几年勒索软件攻击数量激增。如果安全人员不能有效应对这些攻击，此情况仍将可能持续。

攻击者始终能够完成入侵，企业不得不接受此现实。关键在于要减少其入侵的时长，以及发现攻击者入侵行为所需的时间，是数小时、数日、数周还是数月。

Charlie Jacco
网络安全服务主管
毕马威美国

网络安全团队正奋力赶上

网络安全团队正奋力应对多变的威胁，而专业人才短缺却常常对安全工作构成阻碍。

超过1/2 的企业承认他们的网络安全水平落后于原定规划。

逾50% 的企业对网络威胁应对表示非常自信，包括应对来自有组织犯罪集团、内部人员或被入侵的供应链。

59% 的企业同意，攻击者利用的是供应链上下游企业的漏洞，但不清楚其安全防线能否阻挡攻击者的入侵。

实现网络安全目标的 **首要** 内部挑战是缺乏关键技能人才（40%）。

信息来源：《毕马威全球科技报告2022》

此外，混合工作模式扩大了被攻击面，增加了潜在的易受攻击的终端数量，令安全问题雪上加霜。另一个挑战是，企业内部Shadow IT的情况，存在未受管控的应用和SaaS系统，首席信息安全官和首席信息官对这些应用的潜在风险常常缺乏足够的了解。

优化安全运营战略

时间是安全防御关键。企业能多快侦测到攻击者、能多快遏制住他们的攻击、多快能恢复服务？ 与此同时，企业如何降低信息和系统损害？最大的问题不在于攻击者如何进入，而是已经获得了哪些信息，是否是关键信息。应用系统是否具有后门，还是被内部人员进行攻击?

攻击者从初次入侵到成功攻破系统所需的时间正在缩短。现在，攻击者仅需数日或更短时间便能在企业内部成功部署勒索软件。攻击者还不断提升自动化的攻击手段，甚至利用人工智能来协助其规划及实施攻击。首席信息安全官及其团队须在更短时间内识别入侵行为并采取快速、果断的遏制行动。

安全运营中心通常呈三角形结构：顶部是规模较小，但专业化威胁搜寻团队，中部是二级调查员，底部是许多一级威胁要预警分析员，对不断增加的威胁预警信息进行分类。但是，这个三角形结构应倒转过来。

如今的安全运营中心需较少的一级人员、更多二级调查员以及大量威胁搜寻人员，以侦测潜在的灾难事件。为实现此目的，满足日益增加的外部攻击者和外部威胁频率，企业需要实现安全运营第一层级的自动化。

一个有效的安全运营中心需要利用更先进的科技、汇集相关数据，信任已有的安全产品和设备管理安全预警事件，并结合人工分析和先进机器学习和机器人流程自动化能力。在此过程中，您可通过新的业务相关数据源以分析潜在攻击，并进一步探索安全运营、物理安全、预防舞弊和内部威胁管理。

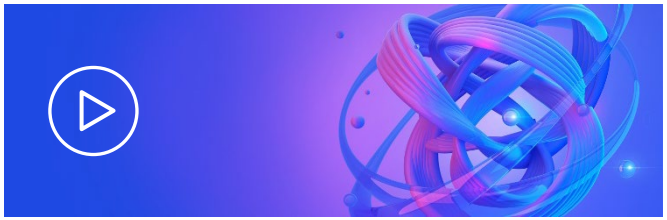
对多数安全组织而言，建立充分的信任是一项挑战。假设首席信息安全官及其团队能够利用人工智能执行上述工作，统筹管理防火墙、安全日志和SIEC，并评估各类威胁情报源和漏洞扫描工具，那可以称得上开始建立信任。这也是安全运营中心的目标，但目前该目标仍未实现。

驾驭及留用网络技术专才

人才的流失与留用问题，必然是最优先考虑事项。许多企业需要为安全运营中心建立可持续的发展途径与模式。在团队疲于监控系统之时，他们会调配更多人手应对，而非向在职人员提供合理培训。

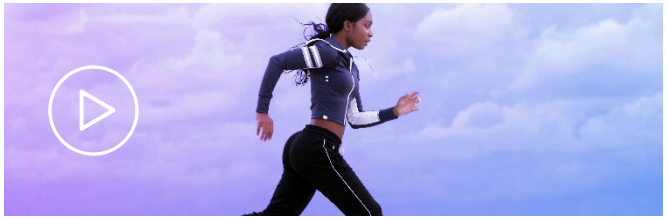
因此，员工会感到发展停滞并最终选择离开，造成安全运营中心的人员不断流失。这完全归因于他们不重视人才培训。在攻击者不断提升自身技术、手段和策略，使攻击变得更有效、快速的同时，首席信息安全官却缺乏所需的人力资源来抵御攻击。

参阅以下报告了解详情



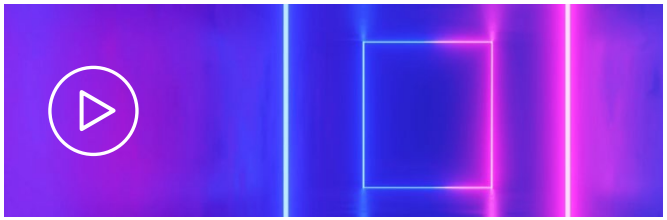
KPMG global tech report 2022
（《毕马威全球科技报告2022》）

探讨企业领导者正如何利用科技驱动业务发展并持续提升数字化成熟度。



Really ready for a ransomware attack?
（《您真的准备好应对勒索软件攻击吗？》）

当下与未来应对风险挑战的业务前提。



A triple threat across the Americas: KPMG 2022 Fraud Outlook
（《美洲区面对的三重威胁：毕马威欺诈形势展望2022》）

回顾美洲区面对的欺诈、合规与网络安全风险。

聚焦事项八

业务连续性

每个安全系统都有自身的缺陷。几乎所有企业终将在某个时刻遭遇或大或小的安全事件，很可能不止一次。监管机构日益关注高风险企业——尤其是能源、金融和医疗保健等具有战略重要性的行业中的企业——需关注业务连续性并做好恢复计划。

最引人瞩目的问题或许是，企业通常未意识到网络安全事件的影响时间以及业务恢复时间过长的问题，通常不止72小时或96小时。企业应预想到最坏的情况是网络安全事件造成了大规模业务中断。在很多案例中，企业高管不能完全理解其内部的技术关联关系，以及业务运营对这些关系的依赖性，如向员工、供应商付款以及与客户和投资者沟通等。

首席信息安全官应该提早与企业沟通，以提前建立一个明确又具弹性的业务恢复计划，而不是等网络安全事件发生时才验证此类计划。

Dani Michaux
网络安全服务合伙人
毕马威爱尔兰

监管形势展望

法律制定者和监管机构的关注度已经提升，即对透明度与全局观提出更多要求。许多企业正担心如何应对日益复杂的全球监管态势。

36% 的企业担心由于其业务已外包到数字服务供应商，他们能否满足现行或新的网络安全法规。

31% 的企业担心关键基础设施要求增加。英国、欧盟和美国正对此领域实施越来越严格的监管。

28% 的企业担心现行或新的与关键系统业务连续性有关的法规。

26% 的企业担心面临更严格的安全事件上报机制。

信息来源：《2022年毕马威网络信任洞见调查》

此外，许多企业尚未真正考虑过他们需要主动作出哪些行动才能保持业务连续性。他们认为自己已制定备份计划，便具备充足的安全控制措施。没有考虑针对特定场景未制定响应的应对计划，从而导致业务运营停止，那将如何应对？这将产生严重的财务及声誉影响，并造成重大监管后果。另外，这一问题还存在心理因素。首席信息安全官需要持续与高管层和董事会沟通，让他们了解攻击者的性质和动机，即网络攻击对企业影响越大，才更有可能获得预算，他们也深知此点。然而，多数企业仍然难以看清目前所面临的情况。

主动协调在事件发生前后的作用

在应对网络攻击事件的过程中，首席信息安全官的主要目标是为企业提供所需的专业见解以维持业务正常运行。他们必须摒弃日常的技术细节，并有策略地主动与企业进行沟通，以说明事件的严重性以及告知企业须如何应对，从而实现快速恢复。

首席信息安全官的主要工作是作为沟通者，向企业阐明安全事件的潜在业务影响以及网络安全的价值。除此之外，还需综合考虑事件响应和事件恢复这两大业务连续性的重要组成部分。

此事可通过建立小型“危机委员会小组”实现。该小组应由首席信息安全官、首席执行官、首席财务官和首席法律顾问组成。

遗憾的是，多数企业并没有正式成立这个重要的小组，因为他们认为信息安全事件不太可能会发生。如果真的发生，他们也认为自己的业务连续性计划（多数是数年前制定，并基于过时的场景组合）已足够应付，但事实并非如此。

保障最低业务运行

此举不仅是为了在控制失效时保持良好的安全性，还在于弄清楚企业需要采取什么措施才能恢复业务。企业领导者往往只会着眼于眼前境况，因为多数人在危机过程中往往无法做到高瞻远瞩。此时，首席信息安全官便须发出理性的声音，务实地建议企业应恢复最低限度的业务运行流程，即维持日常基本运营、支付员工薪酬和确保业务系统持续运行。

此恢复过程耗时越久，便越有可能出现生存危机。攻击者总会出其不意制造问题。他们在金钱的驱动下会快速创新，迫使首席信息安全官始终被动挨打。

监管在企业业务连续性中的作用

在业务连续性方面，监管法规对部分企业可能仅是基本要求，而对某些企业则极难实现。多数企业为后者，因此，他们会仅按最低限度履行法规义务。监管法规也可被视为基本要求，因为企业往往可在此基础上采取新的或不同的行动。

监管在企业业务连续性方面发挥着关键作用，但往往需要协调与对接。这已成为首席信息安全官面对的最大挑战之一，因为监管要求已扩展涵盖企业的供应链。他们需要担心的不再仅是企业的整体情况，还需要考虑供应商与其他主要的合作伙伴的影响及其是否符合相关法规，也需考虑客户和投资者对企业在European Cyber Resilience Act遵从度方面的影响。

业务连续性最终是一个企业层面的问题，网络安全连同业务连续性等其他恢复能力和要素在其中扮演关键的角色。首席信息安全官可协助企业主动为重大网络安全事件做好规划，此类事件在性质、规模和处理方式可能与传统的技术或资产事件有所不同。随着企业日益关注此类情况及其影响，许多首席信息安全官还可能应承担范围更广的企业业务连续性职责。这是首席信息安全官角色的又一次蜕变。

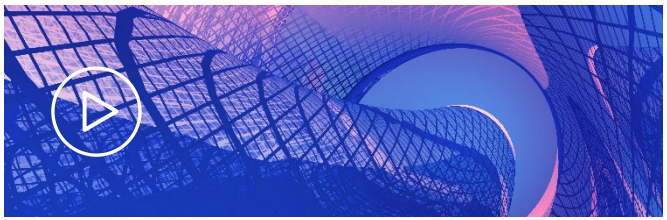
参阅以下报告了解详情

The day after（《遭遇网络攻击后》）

遭遇网络攻击后的抵抗、恢复。

From continuity to resilience（《从业务连续性到韧性》）

随着人们对电力的依赖性增大，企业更应增强主动性和韧性，以确保业务连续性。



Incident readiness: A playbook for your worst day（《安全事件准备度：最坏情况应对攻略》）

为网络安全事件做好准备可尽量减少关键电力及公用基础设施运行中断。

2023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，以助确保安全性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考虑的若干可行步骤，以助缩短业务恢复时间、减少安全事件对员工、客户及合作伙伴的影响，并确保安全计划能为企业赋能，避免其暴露于风险之下。

员工

- 优先建立完善的网络安全培训体系和文化，并确保此类培训有趣、富有吸引力，以激励员工正确行事并发挥防护作用。
- 构建一支具备管理无边界企业（包括云平台与第三方供应商）能力的安全团队。
- 开展广泛、清晰的沟通。询问企业的其他职能领导以了解其痛点和自动化流程可提供的帮助。
- 采取跨领域、跨文化方法，建立一个包含内部业务专员、安全专业人员、数据科学家、隐私案件律师和外部政策及行业专业人士的安全生态系统。
- 将自身融入企业，作为同行、参谋及顾问。

流程

- 确立网络风险管理方案，并了解威胁场景和攻击路径，以协助企业缩小被攻击面并识别控制优化重点。
- 重点关注有效且用户可接受的信息安全流程。
- 建立严格的身份鉴别和访问控制机制，并致力实现良好的身份治理及服务水平。
- 对旧环境进行区域划分以减少受攻击面并协助遏制网络攻击。
- 制定恢复计划，重点关注组织最关键的工作流程，并经常进行沟通结构和压力测试。

数据与技术

- 顺应安全职能自动化这一必然趋势，对先进技术工具赋予信任，如机器人流程、“安全调度、自动化及响应”（SOAR）及扩展侦测及响应（XDR）系统。
- 通过与云服务供应商合作了解如何进行云上产品与服务配置，以避免操作失误中产生的漏洞。
- 在探索新兴技术时首先考虑网络安全及隐私问题，包括与人工智能系统应用有关的多变风险。
- 就如何处理和管理关键数据以及关键数据如何支持关键业务流程，分配职责并建立问责制度。
- 为提升速度、可扩展性和信任度，企业应尽早采用 “身份即服务”技术。

监管

- 持续跟踪不断变化的监管趋势和影响因素，以及它们对公司的未来科技战略、产品开发和运营意味着什么。
- 考虑监管对人工智能和自动化的影响。明确企业在这些领域中哪些可行、哪些不可行；并灵活应对公众疑虑和不断变化的期望。
- 在合规监控与报告自动化上作出尝试，并指派专人关注隐私及安全监管的最新发展。
- 根据公司的整体业务战略调整安全与隐私合规战略，以确保企业上下全体利益相关者一致行事。
- 在致力遵循监管规定外，深入思考数字信任的含义以及如何使之成为战略思维的核心。

毕马威可提供的专业服务

上至董事会议题到数据中心运营，毕马威均有着丰富的服务经验。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。

作者简介

AkhileshTuteja
Global Cyber Security Leader
KPMG International
Partner, KPMG in India
E: atuteja@kpmg.com

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 over 200 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
E: kylekappel@kpmg.com

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's a trusted advisor to numerous Fortune 500 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
E: dani.michaux@kpmg.ie

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
E: mokeefe@kpmg.com.au

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.

Prasad Jayaraman
Americas Cyber Security Leader
Principal, KPMG in the US
E: prasadjayaraman@kpmg.com

With more than 17 years of experience in identity management practice, Prasad is an intuitive and results-oriented leader with a strong track record of performance in technology-related professional services organizations. He has superior interpersonal skills and can resolve multiple complex challenges in all aspects of business, from sales, human resources and legal to finance and operations. He has directed cross-functional teams with motivational leadership and a personal touch that inspires loyalty and a willingness to give 100 percent.

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。

The Global cyber considerations team

Jessica Booth
David Ferbrache
John Hodson
Billy Lawrence
Leonidas Lykos
MichaelThayer

Our Global collaborators

John Anyanwu
Partner, KPMG in Nigeria
john.anyanwu@ng.kpmg.com

Jonathan Dambrot
Principal, KPMG in the US
jdambrot@kpmg.com

David Ferbrache
Head of Cyber Innovation
KPMG International
david.ferbrache@kpmg.com

Jayne Goble
Director, KPMG in the UK
jayne.goble@kpmg.co.uk

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

Lisa Henegan
Global Chief Digital Officer
KPMG in the UK
lisa.heneghan@kpmg.co.uk

Charles Jacco
Partner, KPMG in the US
cjacco@kpmg.com

Prasad Jayaraman
Principal, KPMG in the US
prasadjayaraman@kpmg.com

Sylvia Klasovec Kingsmill
Partner, KPMG in Canada
skingsmill@kpmg.ca

Markus Limbach
Partner, KPMG in the US
mlimbach@kpmg.com

Deepak Mathur
Principal, KPMG in the US
deepakmathur@kpmg.com

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

Matt O'Keefe
Partner, KPMG Australia
mokeefe@kpmg.com.au

Natasha Passley
Partner, KPMG Australia
npassley@kpmg.au

Walter Risi
Partner, KPMG in Argentina
wrisi@kpmg.ar

Motoki Sawada
Partner, KPMG in Japan
motoki.sawada@jp.kpmg.com

Henry Shek
Partner, KPMG China
henry.shek@kpmg.com

Julia Spain
Partner, KPMG in the UK
julia.spain@kpmg.co.uk

Eddie Toh
Partner, KPMG in Singapore
eddietoh@kpmg.com.sg

Akhilesh Tuteja
Partner, KPMG in India
atuteja@kpmg.com

Annemarie Zielstra
Partner, KPMG in the Netherlands
zielstra.annemarie@kpmg.nl

联系我们

毕马威中国

张令琪
网络与信息安全咨询服务合伙人
毕马威中国
电话：+86 (21) 2212 3637
邮箱：richard.zhang@kpmg.com

黄芃芃
网络与信息安全咨询服务合伙人
毕马威中国
电话：+86 (21) 2212 2355
邮箱：quin.huang@kpmg.com

郝长伟
网络与信息安全咨询服务合伙人
毕马威中国
电话：+86 (10) 8508 5498
邮箱：danny.hao@kpmg.com

周文韬
网络与信息安全咨询服务总监
毕马威中国
电话：+86 (21) 2212 3149
邮箱：kevin.wt.zhou@kpmg.com

邬敏华
网络与信息安全咨询服务总监
毕马威中国
电话：+86（21）22123180
邮箱：fm.wu@kpmg.com

李振
网络与信息安全咨询服务总监
毕马威中国
电话：+86 (10) 8508 5397
邮箱：jz.li@kpmg.com

石浩然
香港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 8799
邮箱：henry.shek@kpmg.com

林海燕
香港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

张倪海
香港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

毕马威国际

Akhilesh Tuteja
全球网络安全主管
毕马威国际
合伙人，毕马威印度
atuteja@kpmg.com

Kyle Kappel
网络安全服务主管
网络业务主管
毕马威美国
kylekappel@kpmg.com

Dani Michaux
欧洲、中东与非洲网络安全主管
合伙人
毕马威爱尔兰
dani.michaux@kpmg.ie

Prasad Jayaraman
美洲区网络安全主管及
毕马威美国主管
prasadjayaraman@kpmg.com

Matt O'Keefe
亚太区网络安全主管
合伙人
毕马威澳大利亚
mokeefe@kpmg.com.au

KPMG 毕马威

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