KPMG

共同关注：2020网络安全要点

网络安全威胁日益严重

保护经营环境，你准备好了吗？

kpmg.com/cybersecurity

企业经营不断变化，第四次工业革命蓬勃发展。随着董事会想方设法利用数字经济的潜力，打造新的客户体验，进行服务转型，推动效率提升和成本节约，数据已成为企业的生命线。新业务模式、新技术和新的合作关系融为一体，将创造崭新的未来。

在这个千变万化的世界，有一些不计后果的企业家，他们利用新经济的机会赚取丰厚利润。很可惜，他们是网络犯罪分子，站在了法律的对立面。他们对遵纪守法的企业造成新的挑战。对于如何保护自己的竞争优势，开发新的业务模式以实现和保持网络安全，企业需要转变思想。

网络安全专业人员需要证明，虽然网络犯罪分子犯罪行为的节奏和速度很快，但自己能够利用灵活的思维和行动保护转型企业的核心竞争力。

他们需要汇聚整个企业内擅长于合作的人才，这种人才能够采取积极主动的态度，直面难题。首席信息安全官无法事必躬亲，需要建立新的合作方式。技术发展是机遇而非威胁，网络安全正在成为一股主要的业务推动力量。

我们*选取了将影响今后网络安全处理方式的六大关注点，请我们的专业人士分享他们的见解和经验，以帮助企业应对未来的挑战。

- **协调业务目标与安全需求**
- **数字信任与消费者验证**
- **与时俱进的安全团队**
- **迎接下一轮监管潮**
- **云转型与韧性**
- **自动化安全功能**

> **持续有效的网络空间安全性管理需要将事件处理、业务连续性与灾难恢复计划统一协调起来，这需要整个企业从前台到后台的全方位合作。**
>
> **Akhilesh Tuteja**
> 全球网络安全
> 联合主管
> 毕马威国际

> **在安全运维(SecOps)团队努力整合重点安全工作与软件及流程开发的过程中，为提高效率和节省成本，分析型解决方案的核心任务应尽可能自动化，包括访问与欺诈预警、数据隐私与风险降低等。**
>
> **Tony Buffomante**
> 全球网络安全
> 联合主管
> 毕马威国际

**除非另有所指，否则本文件中，“我们”和“毕马威”是指毕马威以及与毕马威国际相关联的独立成员所网络，或指一家或多家相关成员所，或指毕马威国际。毕马威国际不提供任何客户服务。成员所与第三方的约定对毕马威国际或任何其他成员所均不具有任何约束力；而毕马威国际对任何成员所也不具有任何上述约束力。

协调业务目标与安全需求

无论在工具还是人员方面，很多企业对网络安全投入了大量资源，但如今一些企业认为有必要收缩投资。在这个意义上，网络安全成本已成为主要关注点，可能变得与安全本身一样重要。为了管理成本，并确保业务与安全的协调，企业通过制定数字化网络安全风险管理流程，使相当部分的网络安全功能自动化，确保网络安全与企业最重要的运营和业务战略相协调。

目前的形势

我们研究了大量风险模型，发现其中缺乏业务驱动的风险场景概念。业务团队的观点需与网络安全团队的观点密不可分，但在太多企业中却并非如此。确定这些风险场景应由业务团队牵头。

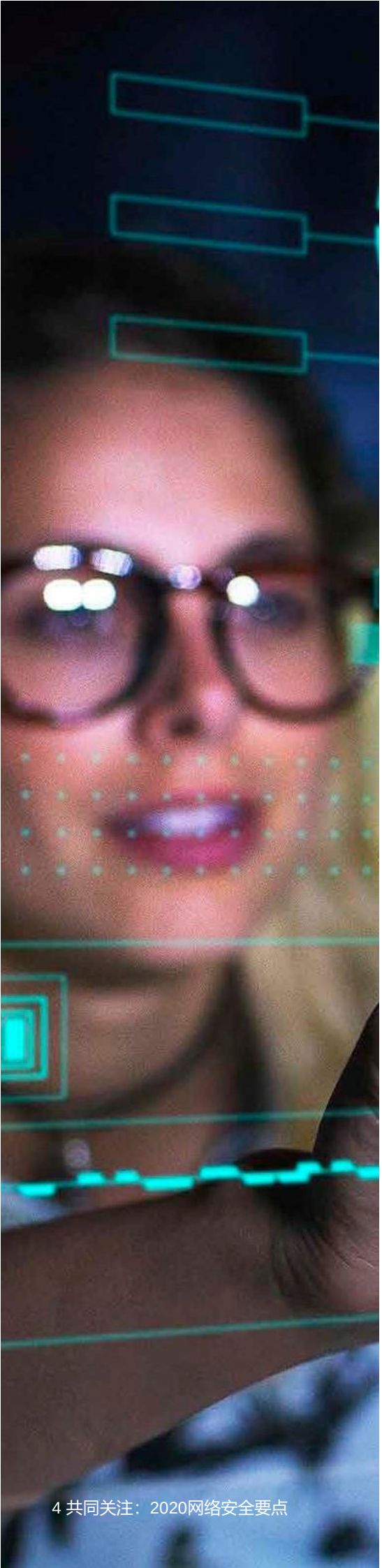
如果能通过模型，使业务领导更深入地了解安全控制对风险场景可能产生的影响，流程的效率将显著提高。很多企业不能一贯地获得这种洞见，从而难以在控制措施和业务之间建立顺畅、持续的关系。

对于网络世界可能发生的最坏情形，我们试图未雨绸缪，但很多事件的发生不太引人注目，影响不大，更不用说对业务造成震动。我们从这一角度发现，很多企业不仅设法将安全嵌入第二道防线，而且还将其嵌入以经营为主的第一道防线和审计推动的第三道防线。

大型企业在过去10至15年间对信息技术安全投入大笔资金，如今他们承认需要开发一种着眼于降低成本的新模型，将安全自动化，使员工各司其职，以降低成本。

> **在很多国家，企业（尤其是大银行）正在建设共享服务中心，以集成各种网络功能。这些企业显然发现，全凭企业自身建设共享服务中心不具成本效益，但一般的外包又不可行，因为外包第三方不清楚从业务角度出发应保护的对象。**
>
> **John Hermans**
> 合伙人
> 毕马威荷兰

> **我们需要对整个企业进行风险分析，并通过业务风险的方式发现信息技术风险，从而对企业风险有全局的了解。网络安全职能部门需要更深入地分析业务重点，以确定可能存在的薄弱之处，以及这些缺陷被利用可能造成的影响。**
>
> **Ben Krutzen**
> 合伙人
> 毕马威荷兰



企业应采取的行动

全面分析哪些领域需要投资。考虑需要控制哪些风险场景，哪些控制措施与之最相关。绝大多数企业正在进行数字化转型，这意味着他们还应探索网络与风险管理流程的自动化。

如果业务中嵌入安全政策和有关控制，很多事件都能轻易发现。总之，建议企业在全部三道防线中整合网络安全措施，而不是三道防线各自为政。

使安全成为一项端到端优先工作。根本措施是建立安全部门与企业其他部门的持续对话，以确保在战略和经营规划方面安全与业务同步。

为达此目的，通过实施工程方法（如安全设计和隐私设计），使开发运维团队开发新的应用程序和服务时将安全意识注入其日常思维。

最后，我们希望看到网络安全专业人员的职能不再仅仅由IT驱动。网络安全团队需要以业务为导向，具有义务意识。否则，业务与网络安全之间的共生关系永远不会巩固。

数字信任与消费者验证

显然，年轻的消费者正在把他们的消费期待延伸到网络生活，尤其是在银行和金融服务方面。于是众多全球大品牌感到威胁。实体店逐渐消亡，谁在数字化客户体验方面占上风，谁就可能占有最大的市场份额。

目前的形势

最终消费者很可能会选择交互最简便并使他们感到安全的品牌。

在目前的环境下，提升客户体验的办法是减少摩擦。对于忘记密码的客户，通过短消息向其手机发送验证码，要求重新输入验证码并确认的做法就是摩擦。

为此，很多企业依靠基于机器学习的方法，以了解客户常见而独特的特征与行为模式（比如指纹、声纹和各种物理生物特征）。特别是金融机构，他们正在努力了解客户与金融机构的交互方式：客户通常如何及何时登录，执行交易的类型，经常提取或转移的资金金额范围等。企业可以归集这些要素，生成独特的客户快照。

对于保有用户交互界面的企业来说，减少客户体验摩擦就是优化客户旅程、建立信任，使客户之旅足够短而高效，以维持客户参与。如果客户认为自己经历了太多复杂程序，他们很可能一走了之而与其他企业做生意。虽然达到客户想要的结果需要客户感到愉快和顺畅，但产品或服务提供商有责任保证整个过程的安全。

> **企业必须开始反思获取数据的方式，使其能够与特定威胁的场景相关。“数据湖”(data lake) 概念其实并不新鲜，但汇入的数据，数据如何保持安全，以及确保只有最相关的人士才能访问和利用这些数据都是重要考虑因素。**
>
> **Charlie Jacco**
> 主管合伙人
> 毕马威美国

> **对于安全融合中心，近年来人们主要关注一个核心问题（尤其是在美国），就是使工作方式转变为数据推动，以监测安全事件，打造精简但随网络威胁形势而变化的响应流程，且一直比网络攻击领先一步。**
>
> **Alex Anisie**
> 总监
> 毕马威美国

企业应采取的行动

首先，最重要的是，任何行业的企业都应努力将数据、验证和反欺诈团队系统化、程序化地联系起来。了解监管规定、所收集的数据、数据所有者、数据来源及利用方式。打造全面的安全文化。

在此基础上思考，如果要求客户回答问题以通过验证，如何提升客户体验，从而使得客户更方便地验证身份，但在客户作出异常交易时需加强验证要求。尽可能使客户的日常交互简便轻松，但可以基于常见行为模式分析，在有必要的情况下略微增加摩擦。

优先考虑隐私，了解企业数据将如何使用及被谁使用的问题。今后很多数据可能都在云端，企业需要研究如何加密和保护这些数据。这是企业层面可以通过技术解决的问题，但最终需要企业以提升客户体验为目标，即在客户与企业进行数字交互的每一环节提升端到端用户体验。

企业还应反思对数据的评价方式。对各种数据集应用大量规则的传统方法已不再可行，传统方法会产生大量误报，造成太多用例漏网，使骗子有机可乘。关键的想法是利用机器学习算法更有效地分析这些数据以识别行为趋势。

最后，企业需要时刻注意整个防护/检测/反应流程中人员与技术之间的相互关系。安全流程不仅从内部横跨整个企业，同时还影响字面和引申意义上的外部世界，因为第三方也可能会触发企业的安全事件。最后，还需要吸取经验教训。对于用户验证，企业应花时间研究过去发生的事件，将其重新应用到企业的安全协议进行压力测试，以避免类似事件再次发生。

与时俱进的安全团队

最近几年，企业董事会为提高网络安全的重要性进行了广泛的努力。2020年，很多董事会成员对网络安全工作日程有着清晰认知。虽然董事会成员了解网络安全的重要性，但安全专业人员面临一项重大挑战，即理解网络安全对业务的重要意义，并将这种认知转变为可行的深刻理解。

目前的形势

很多企业的网络安全团队仍然由技术、经营合规专业人员组成，但这种局面正在转型，网络安全团队逐渐成为更具战略性、前瞻性的资源，利用其宏大的视野影响业务动态。

在许多行业，不少首席信息安全官(CISO)及其团队正在针对不断变化的业务格局努力调整，以便在进行战略讨论时发出受信赖的、有价值的声音。他们还努力构想企业的特定经营重点，与内部业务领导合作，尽可能迅速地将这些分析纳入企业的网络安全方案。安全团队的另一项主要关注点，尤其是在金融服务和医疗健康行业，是如何高效低成本地满足监管要求。

安全专业人员的技能不断在进步。总体而言，核心团队需增强其整体业务卓识和具体产品知识，从而更明确地表达与企业风险相关的网络安全风险。

企业应采取的行动

安全团队应走出自己的领域，倾听不同的观点，加强与业务领导的沟通，去理解企业面对不断演变的生态系统真正需要担心的问题。

对于正在进行数字化转型的企业（这种企业占多数），网络安全团队应从战略角度参与数字化转型计划，展示自己作为业务、数字和安全的桥梁作用。树立共同的目标。

识别企业计划存放在云端的数据类型。了解开发和生产环境之间所需交互的类型，然后将交互的需求与安全方案相协调。

与企业公关团队和密切参与客户体验工作的团队紧密合作。应用信息传递策略，即使最糟糕的情形出现，也要确保企业继续向消费者输出信任。

明确哪些任务人工智能能够处理，哪些工作需要人工参与。努力实现企业安全环境中基本控制的自动化，力争至少实现50%的自动化。

最后，使倡导网络安全成为企业环境、社会和治理(ESG)议程的一个突出特点，以展示对网络安全治理的全面观点和处理广泛事件的能力。

> **接受事实，新世界已不同于往昔。不是侃侃而谈，“我们做了20年的网络安全工作，一直是这样或那样做——此外别无他法。”而是虚心请教，“我们作为一家企业到底应当怎么做？”然后评估可用技术，设计适应企业环境的最佳方案。**
>
> **Dani Michaux**
> 合伙人
> 毕马威爱尔兰

> **首席信息安全官已成为受信赖的内部顾问和重要的运营领导。在进行数字化转型、数据资产价值提取和全球重点工作之间，如果网络管理层具有业务思维与战略意识，每一家企业都将因此得益。他们率领强大、专心致志的团队，在企业追求增长的新阶段保护和赋能企业。**
>
> **Rik Parker**
> 主管合伙人
> 毕马威美国

迎接下一轮监管潮

当你审查技术风险时，其实你说的是信息技术风险。但你讨论网络安全风险时，所有权和责任划分则不在技术部门的职责范围内。我们发现，网络安全监管的方向和规模正在向更加全面的方向发展，主要关注在于业务和责任划分，比如面向客户的信任输出活动，中、后台操作，以及董事会推动的企业治理职能等。简而言之，其实重点在于第一道防线内的管理。

目前的形势

我们预计，在2020年及以后，各类监管部门将继续加强各种专项监管。具体来说，我们发现亚洲对网络安全的新监管规定实际上已使用“网络”一词，而之前的用词是“技术”，具有“IT”的意味。用词的精确性提高是令人欣喜的进展。

很多国家遵循欧盟《一般数据保护条例》（GDPR）的某些内容发布了相关规定，或本国已有隐私法律，我们发现企业（特别是大型跨国企业）成立了积极的数据管理部门。核心是，企业希望将数据分析作为一种规章，不仅要了解数据在企业中的存储，还要了解数据所有者、数据处理过程，以及更重要的，用户对该数据拥有的权利和许可。

企业认识到有必要为网络安全增加投资，不仅是工具和流程开发方面，更是针对网络安全人才的匮乏，需要从网络安全治理、风险战略到配置和维护方面加大投入。这方面的投资仍然存在很大的缺口，而且令人遗憾的是，很多企业招聘的IT专业人才缺乏关于监管环境的网络安全思维。因此他们提出的建议常常无效，或者虽然目的很好，但被管理层和董事会误解或无法贯彻执行。

> **我成为多层网络攻击模拟（即所谓的红队行动和道德黑客行为）的超级粉丝。对安全运营进行测试至关重要，以了解是否能够检测出不同类型的攻击。如果检测出攻击，对应对方案和程序进行压力测试。越来越多的监管团队在其核心流程中考虑这一因素。**
>
> **Ton Diemont**
> 总监
> 毕马威沙特阿拉伯

> **网络安全监管着重于三大领域（我称之为监管三部曲）：基础性的运营技术、通过第三方处理的数据外包及韧性，即企业监测、应对网络攻击并恢复的整体能力。**
>
> **Daryl Pereira**
> 合伙人
> 毕马威新加坡

企业应采取的行动

对于三道防线模型，我们建议在第一道防线嵌入网络安全责任与首席信息安全官的角色（建议正式化），并将这些工作与年度业绩目标挂钩。首席信息安全官的核心职责应在第一道防线，以涵盖安全战略目标和愿景，而且，首席信息安全官对于日常监控和工具配置的安全运营应有明确的层级概念或至少功能性划分。

第二道防线（即信息技术风险）应对设计质量和韧性政策与标准提供支持，向管理层和董事会汇报。第三道防线应对前两道防线进行审核与评估。三道防线互相配合的理想状态力求扩大整个组织内的网络安全需求，其中包括监管合规需求。

我们还认为，为识别改进空间，在设计、实施和效果方面对监管合规计划进行持续检验很重要。此外，确保网络安全运营韧性嵌入整体架构和流程，以加强信息技术和运营技术的安全。

应任命严格说来非IT专业人员负责监管合规。事实上，新首席信息安全官应该更加熟练运用业务语言，以确保其信息得到理解和执行。合适的人选应该对企业的运营模式具有开阔的思路，首席风险官、首席财务官或副首席执行官是理想的人选，因为他们还对企业的整体风险议程有认识。合适的人选应该是整个企业网络安全的主持者或捍卫者，与首席运营官和首席信息安全官密切合作。

从内部控制政策到各种地区性国家的监管规定，企业花时间将各种监管规定纳入“统一控制框架”，以提高内部治理、风险、合规、测试工作的成效。在隐私、韧性和安全监管规定所要求的控制措施之间的寻找协同效应，其结果可能出人意料。

建议企业将重点从系统和技术转移至信息。确定赋予企业市场竞争力的因素，这些因素可能是知识产权、供应链或定价能力。但无论什么因素，从网络安全角度来看都是需要企业保护的对象。

云转型与韧性

随着云技术的成熟应用，很多企业需要使首席信息安全官的团队与企业的其他部门协调。企业可能会说，我们准备在接下来的18个月通过云技术做这样那样的工作。与此同时，首席信息安全官及其团队正在开发有关流程和工具，这些流程和工具对业务推动力和实现理想业务成果所需的技术至关重要，但不一定与其协调。这种情况必须改变。

目前的形势

过去IT一直负责提供基础设施，而且在云技术出现之前，主要着眼于“地面”的挑战。安全团队负责扫描基础设施的漏洞，但他们经常不清楚扫描什么，因为威胁更新列表常常与IT脱节。管理基础设施和相关资产一直很不容易，但是在云端，一切更加瞬息万变，提前进行安全考量并嵌入云解决方案是很多企业正在竭力应对的挑战。

就云技术而言，很多行业内的首席信息安全官团队主要不是准备在技术或人才方面赋能业务。在云端，信息保护是优先工作。我们发现，数据在云端部署的方式常常不一定具有韧性，这种情况越来越多。我们不只是在讨论多可用区域，而且还在讨论发生重大破坏的情况下恢复关键资产的能力。

我们发现，很多企业存在两个阵营，在安全方面似乎走向两个极端。一派是传统的工作人员，他们在安全架构领域工作了20多年，但未充分适应云端的生活。另一派是走在前沿的安全专业人员，他们浸淫当今技术，努力推动和实现云思想，以便能够通过设计和规模化嵌入安全。让两派达成共识是一项重点工作。

> **安全团队必须认识到破旧没有问题，只要能够从中迅速获得借鉴，并卓有成效地应用学到的知识。但是大量企业不敢这样想。一种积极尝试和学习的企业文化，将吸引企业在当今迅速演变的市场形势下所需的那类网络人才。云技术能使企业迅速破旧立新、进行重建和一步步地走向成功。**
>
> **Caleb Queern**
> 总监
> 毕马威美国

> **我们发现，具有计算机科学背景、对代码编写流程有所涉猎的安全架构师越来越多。他们明白自己必须做出表率，让同事能够使用这套新的云工具并支持安全设计。所以我们开始发现，云和安全（云安全专业人员）的连接开始出现，但这种现象仍然十分少见。**
>
> **Katherine Robins**
> 合伙人
> 毕马威澳大利亚

安全团队行动建议

成为学习型企业。吸引云人才的除了高工资，还有企业文化。潜在员工想知道他们入职的不是一家古板、高度厌恶风险和行动迟缓的企业。通过培育勇于创新和尝试的文化，企业能够吸引优秀的云人才。

同样企业还应小处着眼，但迅速行动。宣传企业能够迅速破旧立新、然后吸取经验教训重建。安全能使企业一步步走向成功，例如，逐渐适应数据容器保护新战略，使业务迅速发展。

在软件开发生命周期中，尽早进行测试左移和推进控制，以便为客户和用户提供最大价值。在生命周期中，尽可能逐步地左移安全应用，这通常需要“基础架构即代码”的设计。赋能开发者在不用安全团队参与的情况下硬编码所需的安全措施，即可实现“基础架构即代码”，而云技术可以促进这一变革。

理解底层代码，具备读写代码能力能够赢得开发运维工程师的尊重。抓住机会真正理解自己应当所处的位置。我们会发现，安全专业人员越来越具备读写代码的能力，因为我们日益脱离传统的安全架构角色，即推敲架构图、将其转交方案设计师或方案架构师供其打造解决方案，然后交给工程师建立实际基础架构。

努力理解并向整个企业沟通业务赋能、业务韧性和信息保护之间的联系。这与本地部署的工作方式差别不大，但将关键数据跨区域放在云端略有不同。将云技术融入企业的基因能使企业根除运营“噪音”，从而让企业专注于更重大的安全重点工作。

自动化安全功能

我们发现，从身份验证到威胁检测和响应，数据融合现象出现在安全自动化方面。金融服务、电子商务/零售、科技、媒体与通讯、汽车等众多行业正在收集、分析一系列“了解你的客户”数据。这些信息通常彼此严重孤立。但是企业开始认识到自己坐拥一座数据宝库，如果数据组织更加得当、访问效率提高，企业可以从中提取、分析数据以提升价值。

随着首席信息安全官设法减少开支和提高团队效率，自动处置过时数字资产应成为其首要战略的一大支柱。通过与领先的云服务提供商及安全信息和事件管理提供商的合作，他们同样应探索自动化安全运营中心手册、反欺诈决策和网络安全响应。

Anthony Gawron
总监
毕马威美国

企业正在投资有关技术，以帮助确定其对客户数字行为的了解程度。其目的不仅在于从验证角度验证客户的身份，而且从行为上了解他们如何与环境互动。这些企业其实在效仿过去十年十分高效地完成这种工作的情报界。

Ronald Plesco
主管合伙人
毕马威美国

目前的形势

通过整合历来迥异的数据集，企业正在努力将仍依然依赖人工的功能实现自动化。

不仅企业能够更好地确认数字客户所展示的身份，还能获取更深入的信息，比如谁的电脑有病毒，谁最近收到了钓鱼邮件，谁试图进入没有访问权限的网络。

安全专业人员结合第三方工具和内部解决方案，尽可能多地使整个网络安全手册自动化，使其与企业的业务发展和客户体验目标一致。企业考虑通过云技术自动化第一道和第二道防线，以便在不用人工操作的情况下更好地应对整个企业的威胁，同时确认所部署的安全控制的确按照预期运行。

企业应采取的行动

始终牢记：谁控制数据谁就拥有权力。牢记这一点，第一步便是将关键企业数据从管理许多企业系统数据的第三方供应商处转移至一个集中的可访问位置。

我们还建议在企业内部倡导数据正常化计划，以清理和恰当标记数据，从而了解企业拥有什么数据、如何发布数据及数据集可用的特征。

数据正常化还不成熟的企业，可能不具备条件通过人工智能和机器学习直接收获洞察的阶段。对于这些企业来说，重要的是区分企业希望应用的使用案例的优先级（比如欺诈检测、客户体验提升、运营效率提升等），然后确定如何插入合适的工具、技术和高级分析方法，以便当数据可提供时加以利用。

毕马威可提供的支持

毕马威成员所的网络安全专业人员遍布全球，熟悉企业业务，深知业务不能受到网络安全风险阻碍。毕马威成员所专业人员认为，网络安全就是管理风险，而不是消除风险。

无论企业的网络安全历程处于哪一阶段，毕马威成员所都能助其实现目标，即具备网络安全事件不会造成严重破坏、企业能够照常运营的自信。毕马威成员所专业人员与您同心协力，助力企业完成战略和治理、组织转型、网络安全防御和网络安全应急响应。我们的网络安全专业人员不止于推荐解决方案，他们还协助企业实施。从渗透测试、隐私战略到访问管理和文化变革，毕马威成员所能够对企业提供全方位的帮助。

kpmg.com/cybersecurity

联系方式

石浩然
毕马威中国
网络与信息安全咨询
合伙人
Tel: +852 2143 8799
henry.shek@kpmg.com

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

郝长伟
毕马威中国
网络与信息安全咨询
总监
Tel: +86 (10) 8508 5498
danny.hao@kpmg.com

张倪海
毕马威中国
网络与信息安全咨询
总监
Tel: +852 2847 5062
brian.cheung@kpmg.com

黄芃芃
毕马威中国
网络与信息安全咨询
总监
Tel: +86 (21) 2212 2355
quin.huang@kpmg.com

李振
毕马威中国
网络与信息安全咨询
副总监
Tel: +86 (10) 8508 5497
jz.li@kpmg.com

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

宋智佳
毕马威中国
网络与信息安全咨询
副总监
Tel: +86 (21) 2212 3306
jason.song@kpmg.com

王晖
毕马威中国
网络与信息安全咨询
副总监
Tel: +86 (10) 8553 3630
oh.wang@kpmg.com

冯俊
毕马威中国
网络与信息安全咨询
副总监
Tel: +86 (21) 2212 2496
jeffery.feng@kpmg.com

邬敏华
毕马威中国
网络与信息安全咨询
副总监
Tel: +86 (21) 2212 3180
fm.wu@kpmg.com

本报告所载的部分或全部服务可能未获准提供予毕马威的审计客户及其附属公司或关联主体。

home.kpmg/socialmedia

刊物名称：《共同关注：2020年网络安全要点》
刊物编号：136862-G
发布日期：2020年3月