



消费者流失 晴雨表

信任经济学



目录

1	信任经济学	04
	前言	05
2	消费者视角	08
	消费者对网络安全风险的认识和担忧不断上升	09
	信任经济学 — 金融服务	10
	信任经济学 — 云与互联设备	14
	信任经济学 — 移动设备	16
	信任经济学 — 汽车业	19
	信任经济学 — 零售业	22
3	安全管理者视角	24
	作出改变	25
	安全挑战	27
4	结论：网络安全，从顾虑到信任	31



1

信任 经济学



前言

科技颠覆时期的消费者信任

在科技颠覆中寻找正确的发展方向已成为业务常态，驱使企业不断尝试和配备最先进的数字化产品和服务来收集和运用海量数据并从中创造价值。科技发展的持续性以及数字化转型促进企业与顾客互动和绩效提升能力不但是企业获取竞争优势的机遇，还是科技颠覆的催化剂，企业董事层对此极为振奋。企业在当前持续的转型及创新过程中能够保持灵活性正快速地定义企业成功，而对那些能理解及应对客户关注点的企业而言，如何在顾客至上的时代保持消费者信任正成为它们的独有优势。

随着数字化互动不断演进，期望值不断提升，客户已成为数字化转型中的关键驱动要素。因客户对可信信任及数字化服务体验的需求提升，成功企业应能预知并抓住由此带来的商业机遇

充分了解客户个体需求对业务成功至关重要，而这要求企业收集大量数据。

为了充分利用科技带来的裨益，企业必须更好地立身于抓紧消费者信任计划带来的机遇；在同时对企业和使用其产品的客户产生的新网络威胁下，这些客户信任计划已成为当务之急。

在本次调研中，我们的目标是评估客户对数字化信任程度的预期是否已发生改变，以及企业在其数字化产品供应中是否将客户安全置于首位。我们还探讨了在出现问题时如何才能令客户对品牌保持忠诚，以及企业在发生危机时是否真正地将客户利益置于首位。

本报告其中一个关键议题是了解消费者与为他们提供服务的企业之间的网络安全认知差异。我们相信，消除此认知差异可提升客户信任，而信任则会推动业务发展。

“

消费者的需求及期望值对业务决策的影响不断增大，并主导着企业有关数字化转型的议题，”毕马威客户及市场全球主管 *Gary Reader* 表示。随着越来越多顾客使用数字化渠道进行沟通，并将更多数据交付至企业，企业是否已执行充分的工作以应对消费者需求。

”

关注数据安全的数字化消费者的崛起

随着科技创新的发展，消费者对企业的数字化产品和服务交付有着越来越高的要求，并期望数据安全成为数字化体验中的必要组成部分。

我们的调研显示，多数消费者更主动接受新型、

个性化及操作简便的技术。但同时，消费者对数据安全的关注也在增加；在多数情况下，消费者对企业解决数据安全问题的方式并不满意。

面临抉择的董事会

数字化转型现已成为企业日常运营的一部分，但大部分董事会似乎仅主动参与部分转型议题。多数董事会更乐意面对转型的有利方面，即应用新技术和数据战略以促进企业增长，但忽视与此相关的潜在风险。

此现象从我们从安全主管获得的回应中可以看出，多于三分一的安全总监认为自身企业的信息安全预算不足。

令人担忧的是，某些安全主管受访者表示，他们的企业主要将信息安全视为合规及风险管理问题，其中12%的受访者向董事会汇报工作的频率为一年一次甚至更低。

我们认为，若网络安全问题不被纳入企业价值链，便不能建立信任生态系统，并会错失巨大的商业机会，增加各项业务风险。

董事会应在增长议题和顾客信任议题之间取得平衡。

“二十一世纪的企业利用科技来增进消费者互动，实现无形资产价值和培育未来员工”毕马威网络安全全球联席主管**Greg Bell**表示。“但这些业务模式应作扩展以使网络安全成为投资的一部分，使企业能在加快转变的同时降低风险。”

管理滞后和期望差距

仅有少部分一流企业从转型开始便将网络安全考虑完全整合进业务转型方案中，以打造同时满足消费者的功能及安全性预期的数字化产品和服务。其它企业一般是对已建立或接近完成的转型成果进行安全性更新。企业在计划后期才添加安全性要求，必然会产生管理滞后问题，并会延误或甚至终止数字化转型目标的实现。

如果董事及业务主管未在转型开始便将网络安全考虑嵌入自身的业务战略中，他们的商业战略便可能出现碎片化，仅可满足部分消费者期望。



“首席信息安全官的职责已改变。他们在支持自身组织的增长战略中起到关键作用，主要是通过提升客户对其数字化产品和服务的信任度，”毕马威网络安全全球联席主管**Akhilesh Tuteja**表示。实际上，调研反映，首席信息安全官认为自己是企业增长的必要部分，但仍未充分整合进业务转型计划中。“他们仍有理由保持乐观；多数首席信息安全官认为他们获得组织的支持，有充足的预算和投资，”他说道。随着消费者信任对业务成功的影响愈加重大，企业越来越有必要将网络安全视为董事层面的优先投资项目以及业务增长的关键驱动因素。

在危机中留住顾客信任

信任是吸引和留住客户的关键，但在危机发生时，信任往往需经受严峻考验。毕马威《二零一八年全球首席执行官展望》（“2018 Global CEO Outlook”）指出，半数受访首席执行官认为自身企业经受网络安全事件仅是时间问题。但如果企业能小心谨慎地、以一种能增强客户信任度的方式处理安全事件，这实际上可强化信任生态系统和帮助企业留住客户。

调研发现，在安全事件发生时，安全总监和消费者的关注点存在严重错位。

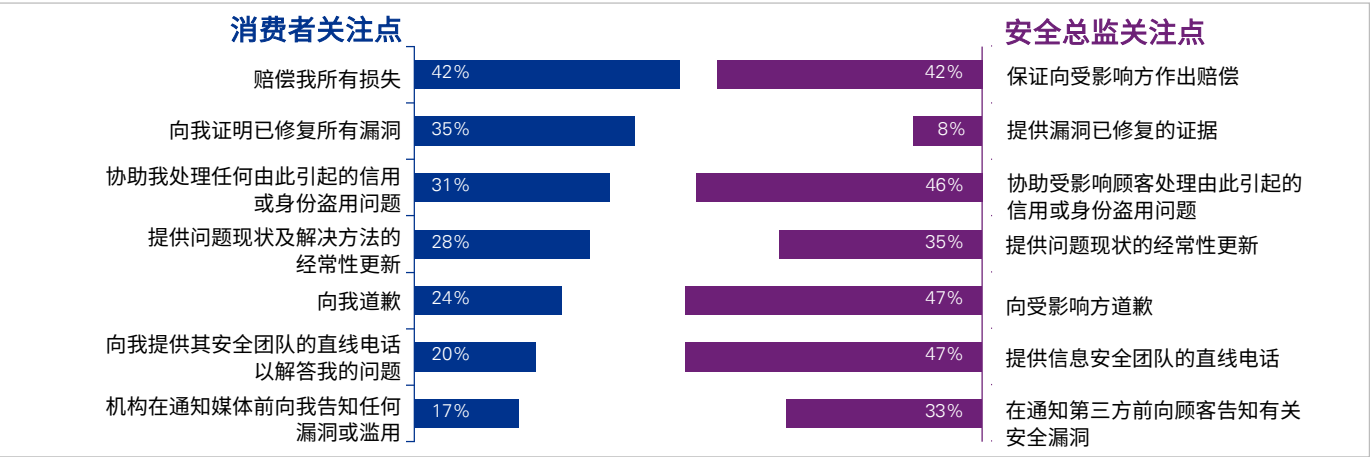
安全专家真的了解消费者想要什么吗？

消费者关注点：如果由于安全漏洞，您的财务账户出现资金流失，或您的个人数据被窃取或滥用，您的财务服务提供商需作出什么行动才能留住您？选出所有符合的选项。

多于三分之一的消费者希望企业证明其已修复相关问题；但仅有8%的受访安全总监会优先提供此类证据。相反，只有24%消费者希望企业先作道歉，而约半数受访安全总监则将此列为优先事项。

我们认为，随着消费者的安全期望值提升，安全组织的职责将从保护组织核心技术驱动型流程扩展至提升数字化产品和服务的价值主张。那么，安全主管便有必要了解终端消费者的需求，并从后台职能转变为消费者体验的核心元素。

安全总监关注点：当贵企业发现并修复安全漏洞后，一般采取哪些行动来回应顾客和其它相关方？选出最优先的三项。



资料来源：消费者流失晴雨表：信任经济学。2019年。

以顾客为中心的安全事件响应

企业应在问题发生前提前计划，充分考虑对安全事件的合理应对方式。安全专家应重点思考自身的行动能如何服务于信任。

生态系统的建设，准备更充分的企业更有可能在安全事件发生后留住客户。

企业对重大网络危机的响应要求组织上下、从技术人员到董事及高管层的共同行动。只有妥善组织及企业内部全体参与的响应方案才能交付有意义的结果和行动。

信任的保持是关键，尤其是对外部利益相关者而言。安全专家和事件处理人员在此发挥重要作用，且需要获得董事会及所有面对顾客的员工的支持。

”了解安全事件中的客户期望和制定响应计划可提升企业恢复能力，有助客户重新获取受影响客户的信任。” 毕马威英国网络安全合伙人Paul Taylor表示。

A woman with curly hair and a man are sitting on the floor, looking at documents and a laptop. The woman is smiling and pointing at a document. The man is looking at the document with a thoughtful expression. They are in a bright, modern setting with large windows in the background.

2

消费者 视角

消费者对网络安全风险的认识和担忧不断上升

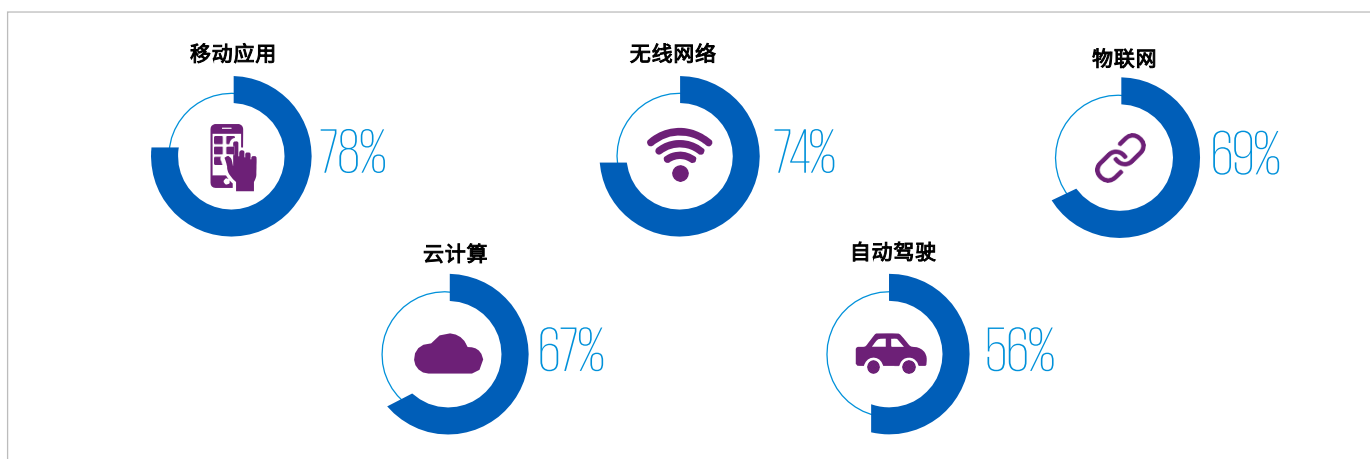
与董事会的高管一样，消费者已欣然接受科技为日常互动带来增值的作用，其中包括他们与企业之间以及消费者之间的互动。从消费者角度而言，科技变革和应用正快速或已经成为一种生活方式，并不断简化和提升消费者的交流方式。

与企业高管一样，消费者同样认识到技术进步带来好处的同时，亦存在风险。

我们的调研发现，大部分受访消费者对科技应用表现了较程度的担忧，而一项技术的成熟度或熟悉度与客户对该项技术表现出的担忧程度有着较高的相关性。

我们至少可以确定，企业为表明数字化产品和服务的安全性做的并不够。我们相信，那些能跨越消费者期望与担忧之间的落差的企业可在赢取客户方面取得竞争优势，并使信任经济学成为关键战略特点。

对技术安全问题表示顾虑的受访者百分比



资料来源：消费者流失晴雨表：信任经济学。2019年。

应用程序和无线网络是消费者最担心会出现安全问题、也是最常用的两项技术。当交付数字化顾客互动模型时，应用程序尤其受到企业的特别关注。

消费者对自动驾驶的担心程度较低，该技术相对较低的成熟度和全范围应用可能是产生原因；受访者表示这将是未来的一个关注重点（本报告下文再作探讨）。



“消费者对数据泄露的顾虑是合理的；我们经常在新闻中看到影响数百万人的安全事件，其中泄露的个人信息包括密码、活动日志和财务记录，” 毕马威网络安全全球联席主管Akhilesh Tuteja表示。

比起数据泄露对被入侵企业的影响，消费者更担心该类事件对自身的影响。”在企业转型过程中，那些能够有效回应消费者忧虑的企业将可获得竞争优势。”

信任经济学 — 金融服务

无论是发达市场还是新兴市场，数字银行普遍存在；全球超过三分之二的消费者正使用数字银行平台；5.15亿消费者通过移动支付供应商开立银行账户。

数字金融服务展现的机遇是明显的，已得以证实的。在成熟市场，金融服务机构能直接与客户交流，从而提升进入市场速度、根据客户需求定制产品和服务并降低或控制运营成本。

在新兴市场，数字银行能够在无须设立实体的情况下吸引以往没有银行账户的消费者，并因此减少巨额的资本投入。当然，此目标的实现需要消费者的高度信任。

金融机构面对的额外挑战是，财务信息及消费者的信任生态系统往往涉及第三方，

即为完成交易而收集及传递财务信息的产品及服务供应商；而随着开放式银行和其它方案成为主流，此生态系统的复杂性亦在提升。

这些信息对攻击者极具吸引力；全球37%的受访消费者表示他们的财务信息曾被盗取，其中拉丁美洲和北美洲超过三分之一的受访者曾遭受财务信息被盗取的情况。对需在执行数字化转型计划的同时运营业务及保持客户信任的金融机构而言，此背景构成了一个挑战。

此外，企业数字化转型计划的相对成熟度与区域内财务信息曾被盗取的消费者的百分比也存在明确的相关性。据此，我们可推断，随着数字化转型不断推进，消费者承受的风险将加大。

财务信息曾被盗取的受访者百分比，按地域



欧洲、中东和非洲
35%



亚太地区
39%



美洲地区
43%

认为自身企业的数字化转型计划为“先进”或“成熟”的受访安全总监百分比，按地域



欧洲、中东和非洲: 22%



亚太地区: 31%



美洲地区: 40%

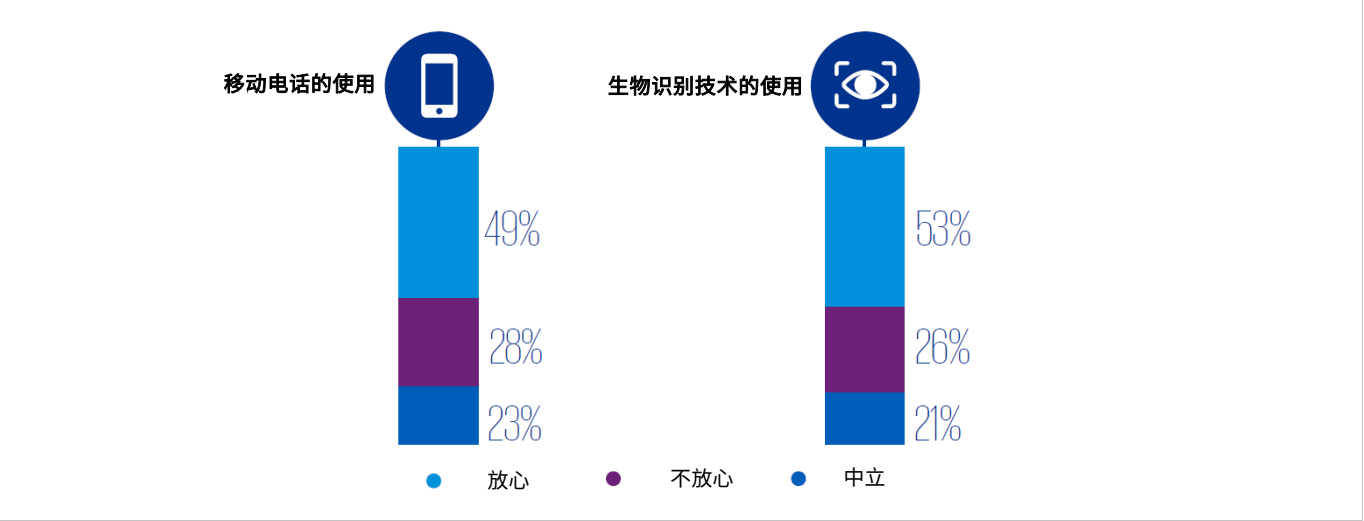
“我在数家全球最大的金融机构工作的过程中，亲身感受到组织的复杂性和规模是如何对数据安全战略的重新制定带来挑战的。

一个全面数据安全战略的实现（涵盖业务、技术和多个安全层面）要求董事会的强力参与和实质性支持。若成功做到这点，便可通过提升协调性及敏捷度来实现企业增长。”

Bia Bedri
毕马威英国
银行业及资本市场网络主管

资料来源：消费者流失晴雨表：信任经济学。2019年。

为技术变革释疑

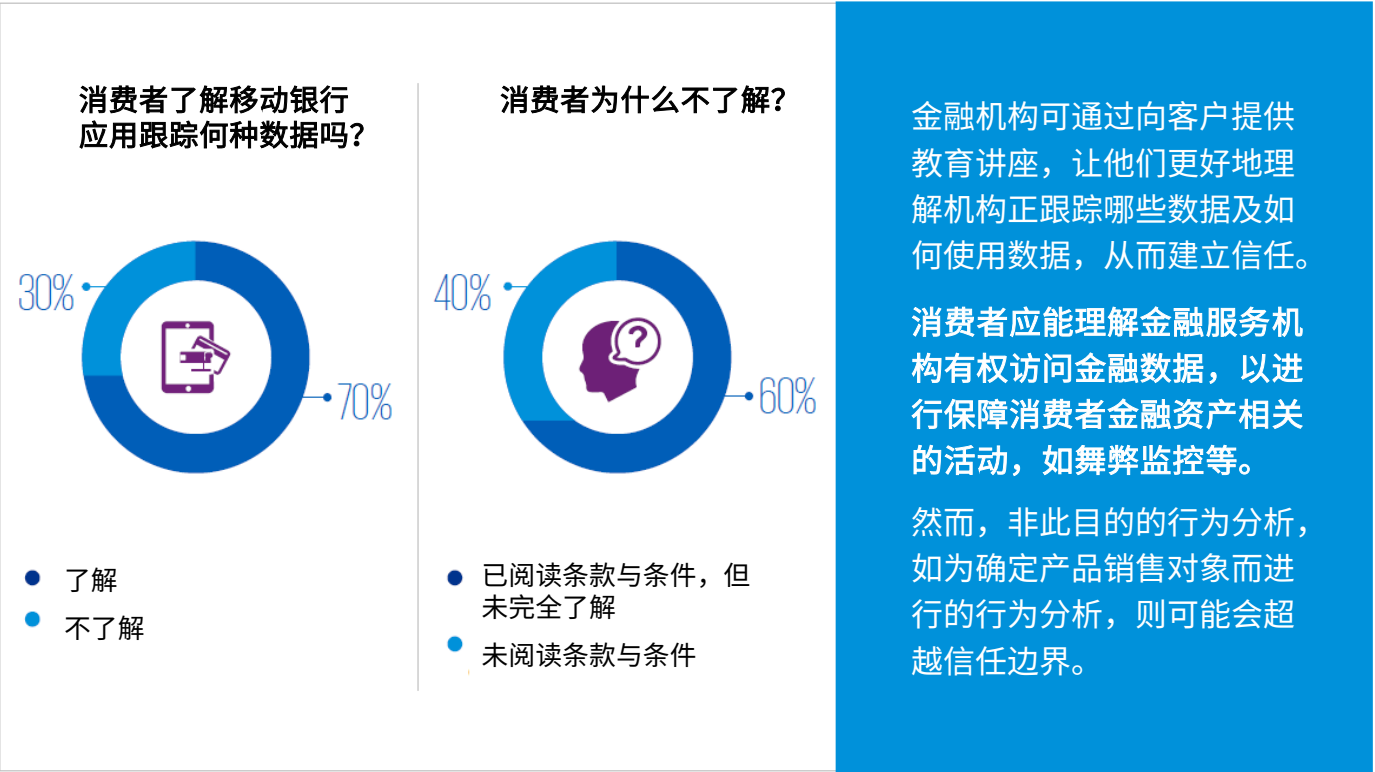


资料来源：消费者流失晴雨表：信任经济学。2019年。

虽然数字银行已日渐流行，金融机构各年龄组别的用户中仍有一大部分不放心使用数字化技术，如移动电话（28%）和生物识别技术（26%）。

因此，随着托管数据日益增多，金融机构应加大力度以解释数字化技术的好处，并表明他们理解顾客的顾虑。譬如，银行应更好地向消费者解释生物识别技术对比密码技术的优势。

认清细则

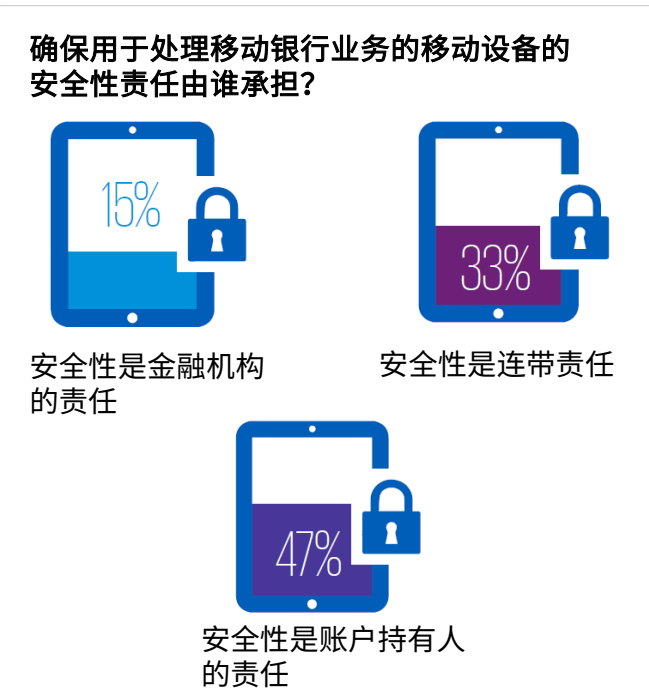


资料来源：消费者流失晴雨表：信任经济学。2019年。

承担责任

近半数消费者认为他们的金融机构应有完全或连带责任确保处理银行业务的移动设备是安全的。无论金融机构是否将此视为自身责任，都需要展示在与顾客的互动中，以及对消费者更广泛的安全需求而言，他们都是认真对待客户信息安全的。

“金融机构在满足消费者的安全性期望方面面对真正的挑战，” 毕马威全球银行业及资本市场主管**Judd Caplain**表示，“一小部分主要企业的做法是正确的，它们将灵活的安全性融入数字化转型计划中，同时认识到转型计划本身是不断变化的，再向客户展示相关工作成果，如向客户提供网络安全认知和舞弊监控的快速访问渠道。”



资料来源：消费者流失晴雨表：信任经济学。2019年。

从消费者的角度解决问题

在调查中我们发现，仅有1.2%的受访者在其财务信息泄露后肯定会变换金融服务供应商。相反，2%的受访者在发生数据泄露后肯定会继续使用原服务供应商，虽然此类受访者中的过半数是因为不想麻烦才不更换供应商，其它96.8%的受访者愿意继续使用原金融服务供应商，前提是原供应商采取了解决数据泄露问题的适当措施。

这反映了消费者接受网络攻击不能完全避免的现实，但他们希望企业对数据泄露事件做出快速、有效的应对措施。

我们的调查发现，在数据泄露事件发生后，若服务供应商的应对工作符合消费者的期望，并重点处理消费者的优先关注点，那么多数消费者会愿意继续使用原服务供应商。消费者在数据泄露事件中的优先关注点包括就所有损失获取赔偿、取得漏洞已被修复的证明和就由此产生的任何信用或身份盗用问题获得协助。



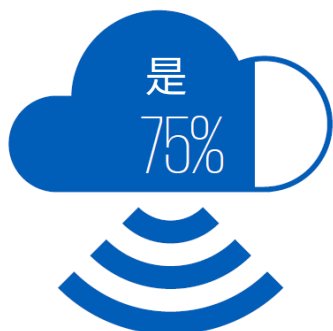
信任经济学 — 云和互联设备

互联设备安全是成本、投资还是竞争优势？

在我们的调查中，四分之三的消费者表示他们希望互联设备中嵌入额外的安全及隐私保护机制。但事实未必是这样的：仅有32%的受访者限制这些设备的使用，且同样仅有32%受访者愿意为更安全的设备支付更高价格。这对设备制造商构成了挑战，因消费者虽然希望获得更高的数据安全，但并不一定愿意支付更高的价格。

企业必须认识并利用安全性高的好处，即可驱动企业增长的信任经济。对设备安全性进行投资以作为常规预防措施可降低消费者疑虑，并通过增加销售获得回报，与此同时，在市场上的同类设备出现问题时提升品牌忠诚度。鉴于互联设备可观的增长预期，这是一项重要的竞争优势。

新型“互联”设备的设计是否应该加入额外的隐私保护及安全机制？



您是否因安全性或隐私方面的顾虑而限制新型“互联”设备的使用？



您会为某些新型“互联”设备的额外安全保障进行支付吗？



资料来源：消费者流失晴雨表：信任经济学。2019年。



2018年，全球物联网设备的数量为70亿（不含智能电话、平板电脑和手提电脑），此数字预计在2022年翻三倍。“互联及物联网设备的快速增长将对数据安全及隐私等领域带来跨行业影响。作为回应，监管机构需建立强制性数据安全要求。”毕马威印度信息技术咨询服务主管 **Atul Gupta**表示。“机构也可借此机会建立一个信任环境，并将其打造成为一个卖点。信任便成为影响消费者‘购买’决定的差异因素。”

云平台

社交媒体平台是否本来就应当不被信任？

在调查中，我们发现超过半数用户限制了线上的个人数据储存量。对于内容交付由用户数据驱动的社交媒体和其它平台（提供内容并以实现个性化营销为最终目的）而言，它们可能不能获取所需信息以使算法发挥最大优势。

从其它角度而言，这些平台也需要保护自身的内容交付战略、算法及向终端用户交付的内容。将内容交付平台“武器化”以左右舆情和争议正受到媒体的广泛关注，同时，机构的信任方程式亦会受到双重影响。

短期而言，机构似乎还有轻微的喘息机会——当消费者感觉到隐私被侵犯时，他们一般不可能会更换或停用社交媒体账号（46%的受访者选择此做法）。但长期而言，社交媒体及云平台须考虑如何重建客户信任度，或如何面对来自新兴企业的挑战或监管机构的要求，后两者将更多地考虑消费者的利益。

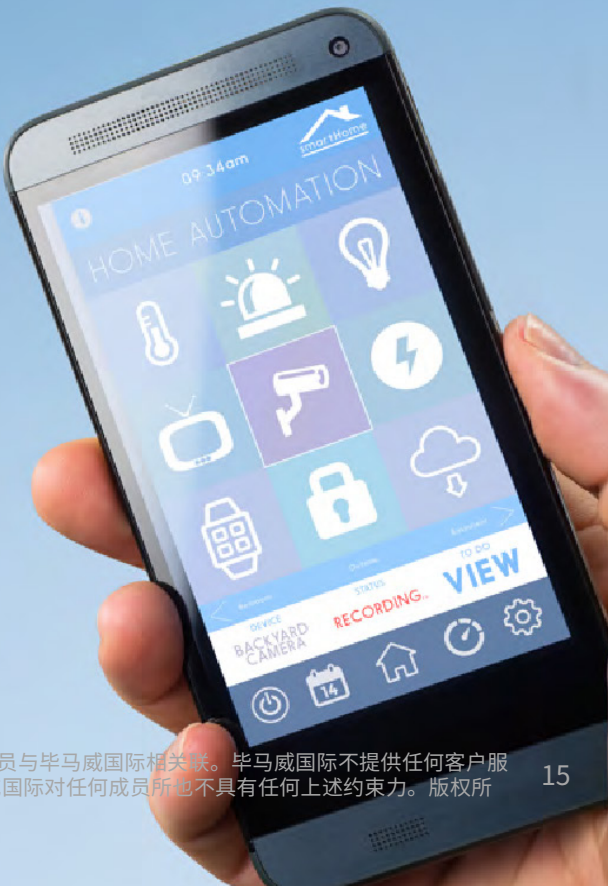
您是否由于安全和隐私考虑而限制存储于云/社交媒体平台上的数据量？



资料来源：消费者流失晴雨表：信任经济学。2019年。

“各行各业正实施由技术创新支持的数据驱动战略以提升企业敏捷度及市场化速度。一部分先行企业亦在这些战略的支持下走在监管机构之前，并以此建立竞争优势：保持领先，积极展示对安全及隐私管理的强烈关注。”

Jitendra Sharma
风险咨询全球主管
毕马威国际



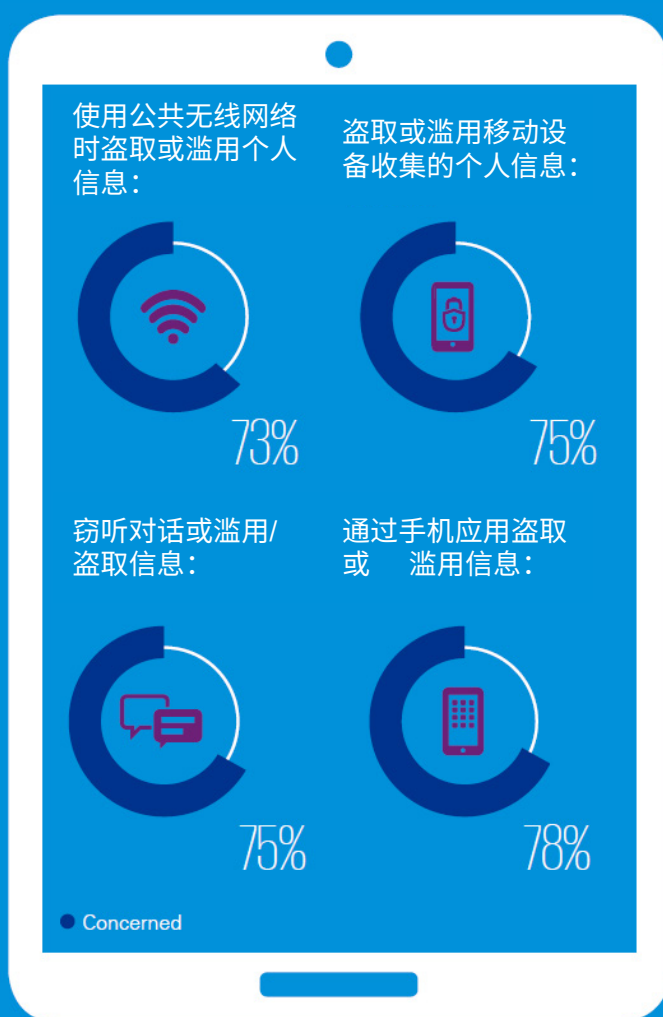
信任经济学 — 移动设备

信任经济的支柱

作为数字化经济的核心技术，移动设备生产商和网络运营商所处的位置是信任经济的关键 — 不仅须建立客户对自身产品和服务的安全信任，还须创建可信任的渠道和平台，使消费者能利用其它企业的数字化产品及服务。

然而，我们的调查发现，消费者在此方面的忧虑水平极高 — 平均有四分之三的消费者对他们的设备、运营商、网络连接或手机软件的安全性表示顾虑。

移动消费者的重点关注事项



消费者非常担心移动技术的安全问题。他们意识到相关风险，这对购买及使用移动技术趋势产生影响。

成功解决消费者对自身产品和服务以及更广泛的数字化经济的安全性疑虑的移动供应商可获得竞争优势。

随着消费者越来越依赖移动技术，他们愈加关注使用移动技术的后果。同样地，有组织犯罪已意识到移动技术对我们全球经济的重要性，并加大力度发起攻击，作为回应，供应商也在致力提升安全性。

资料来源：消费者流失晴雨表：信任经济学。2019年。



消费者对通讯供应商亦有高要求

在我们的调查中，消费者明确表示，当自身数据被泄露时，无论是由于外部攻击还是内部滥用，他们都会考虑更换通讯供应商。与通讯供应商被非法入侵的情况相比，在通讯供应商滥用数据的情况下，考虑更换供应商的消费者增多。

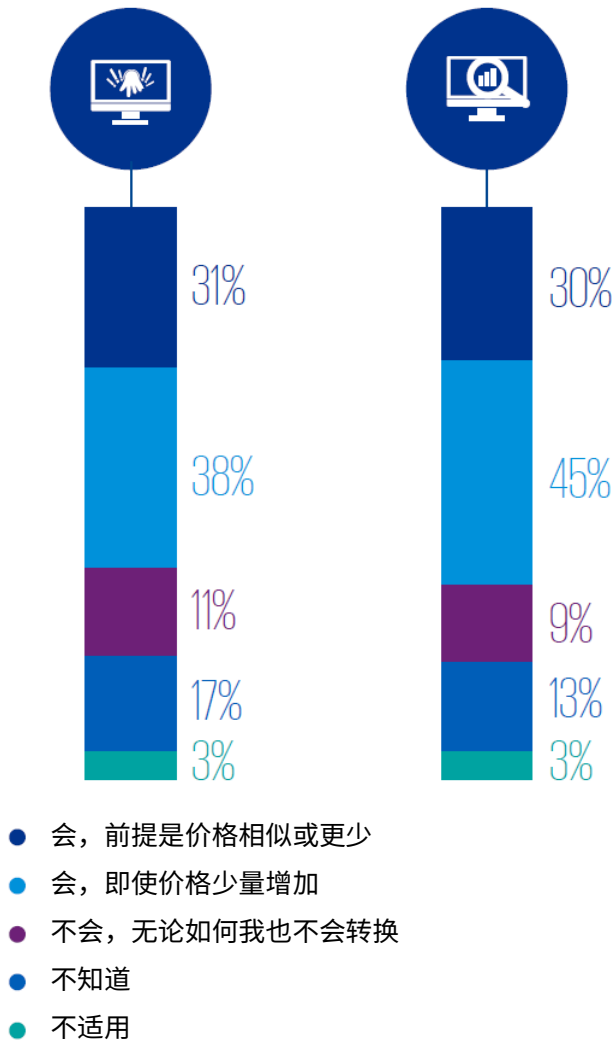
但目前消费者并不一定真的会更换供应商，因这样消费者便需缴纳高昂的合同退出费。但若未来监管机构或市场要求为移动通讯消费者提供更便捷的供应商转换方式时，便会产生问题。

“移动设备制造商和网络供应商的经济及社会影响远远超越自身的产品和服务。它们构成了我们大部分个人及工作数字生活的基础，” 毕马威媒体及电信服务全球主管 Alex Holt表示。“这些企业不仅在自身的移动产品及服务中，还可在医疗保健及银行业等行业的数字化渠道中建立客户信任，从而在市场中脱颖而出。通过此种方式，它们可增加新服务的接受量，创造新的收入流。”

在哪种情况下，您对数据安全或隐私的忧虑会使您更换通讯服务商？价格会否影响您的决定？

如果您得知您的通讯服务商被黑客入侵，其收集的个人信息被盗取，您是否会转用其它保证限制或停止收集个人信息的服务商？

如果您得知您的通讯服务商正滥用或售卖您的个人数据，您会否转用其它不会这样做的服务商？



资料来源：消费者流失晴雨表：信任经济学。2019年。

信任经济学 — 汽车业



“数据及网络安全，和背后的总拥有成本，是最重要的采购标准。在未来五年，无论是购买汽车还是使用移动服务，近60%的高管绝对同意，不重视数据和网络安全的企业将极有可能牺牲它们的品牌声誉，且不能在数据使用中提供真正价值，”毕马威汽车业全球主管 *Dieter Becker* 表示。“在此背景下，企业更有必要建立一个安全的数字化环境，并具备无缝连接及额外功能以使客户信任最大化。”

快车道中的变革

汽车业正面临着其它行业难以企及的技术颠覆，其消费者产品不再只是硬件和机械的结合，而正逐步发展为一个涵盖物联网设备、数据处理、自动化、连接性、软件和单一品牌下集结多个服务商的完整体验。随着技术企业纷纷进入汽车市场并带来不同的移动性模式，传统汽车品牌急需进行快速数字化转型。

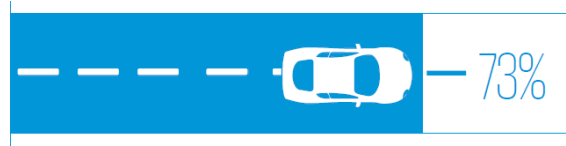
消费者认识到汽车业的数字化程度在不断提升，因此更容易被非法入侵，他们对五年期间内的网络安全忧虑水平快速提升。

将网络安全纳入汽车安全考量，特别是当现实世界的安全要求成为必要时，可成为未来令品牌脱颖而出的价值主张，类似现在新车评估中的安全等级评估。

您担心您的汽车现在会被黑客入侵吗？



您担心五年后您的汽车会被黑客入侵吗？

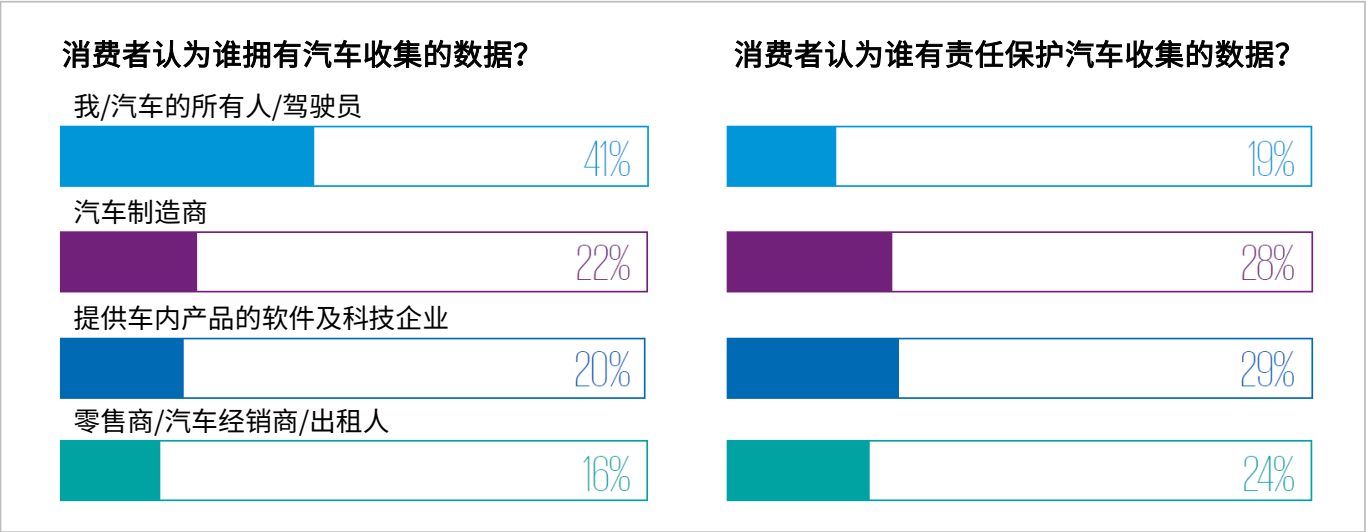


资料来源：消费者流失晴雨表：信任经济学。2019年。

在不断发展、互联的网络中的责任

使问题进一步复杂化的是，汽车制造商被要求保护客户的个人数据及汽车数据。同时，多数消费者认为汽车制造商拥有汽车收集的数据，认为他们将个人数据托付给汽车制造商，则需由汽车制造商分担其数据的保护责任。

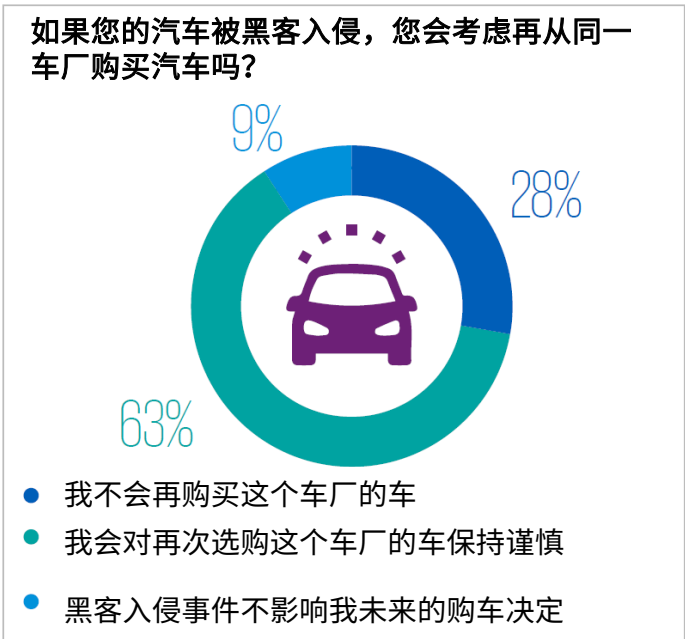
汽车制造商要想成功，就需要确保客户信任其汽车数据的安全性。汽车制造商有责任在一个复杂的供应商生态中建立信任，这个生态包括经销商、软件商、硬件商、电信服务商和消费者。



资料来源：消费者流失晴雨表：信任经济学。2019年。

对品牌忠诚度的影响

如果汽车被黑客入侵，28%的消费者表示将不会再购买相关车厂的产品；另有63%的消费者表示再次购买相关车厂的时将保持谨慎。此调研结果意义重大，反映了一个处理不当的安全事件会严重影响重复销售，这对一个品牌忠诚度过去依赖机械和相对较低科技含量的驾驶体验的汽车业而言也不例外。



资料来源：消费者流失晴雨表：信任经济学。2019年。

现实世界的影响

“汽车数据安全不仅关系到汽车组装者，”毕马威德国网络安全主管Marko Vogel表示。“每一件硬件、软件和网络架构均需整体考量，包括其构成的不断扩大的生态体系。这不仅关系到品牌信任，还关系到消费者保护的核心，即保护消费者及其周围的人的生活以及他们的数据。”



信任经济学 — 零售业



“对竞争激烈的零售商而言，收集和利用个人及交易数据是了解、识别和服务客户的关键，但此做法存在固有风险。数据作为一种资产，若处理不当，可成为损害品牌和信任的负累”，毕马威消费者及零售业务全球主席 *Willy Kruh* 表示。

“此外，零售商从客户收集的海量支付信息及其它个人信息使它们成为网络罪犯的热门目标。”

“然而，虽然黑客可对零售商和客户造成损害，但实际上客户更担心零售商可能滥用他们的数据。

在如今不断变化的环境下，企业应超越客户许可及同意这样的概念，认识到数据隐私不单是一项合规主导、形式化的工作。它要求高透明度，允许客户对自身数据如何及在哪里被使用有完全控制权。”

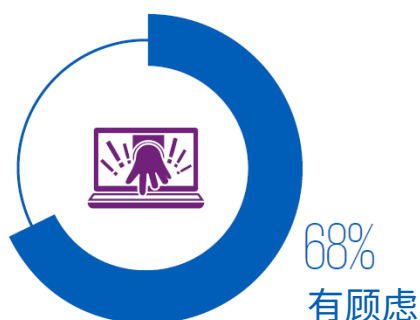
消费者不信任零售商

我们在消费者调查中发现了一组惊人的数据，即与个人信息被外部黑客盗取相比，消费者更担心零售商滥用个人信息。企业须极其认真看待此问题，因了解消费者及他们的行为是交付独特客户体验的关键。

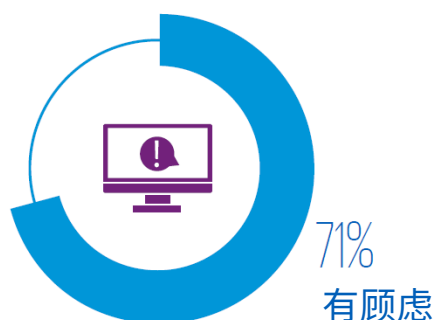
其中一个必要的资源增长是了解消费者，了解他们想买什么和在哪里买，然后利用这些数据来提升销量和管理供应链。

这有助于建立一个高效组织，以应对新的市场进入者的竞争和颠覆。随着顾客个性化成为打造独特购物体验和提升销量的主要策略，零售商须考量“画蛇添足”和“恰如其分”之间的微妙平衡。此处的焦点问题是：企业可在多大程度上分析消费者数据，而不会使消费者产生被打扰或被操纵的感觉？

您担心您经常光顾的大型零售商被黑客入侵吗？



您担心某零售商滥用或不当披露您的信息吗？



资料来源：消费者流失晴雨表：信任经济学。2019年。

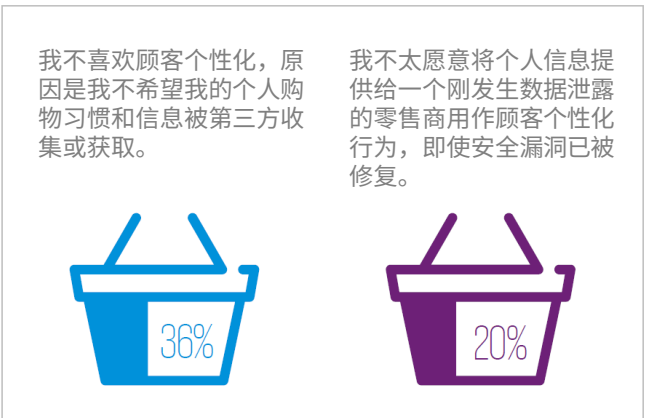
顾客个性化

当消费者被问到在何种情况下，重视或愿意将他们的数据用于顾客个性化时， 他们一边倒地表示，若零售商要进行个人化操作，则希望拥有一定程度的控制力或获得直接利益。



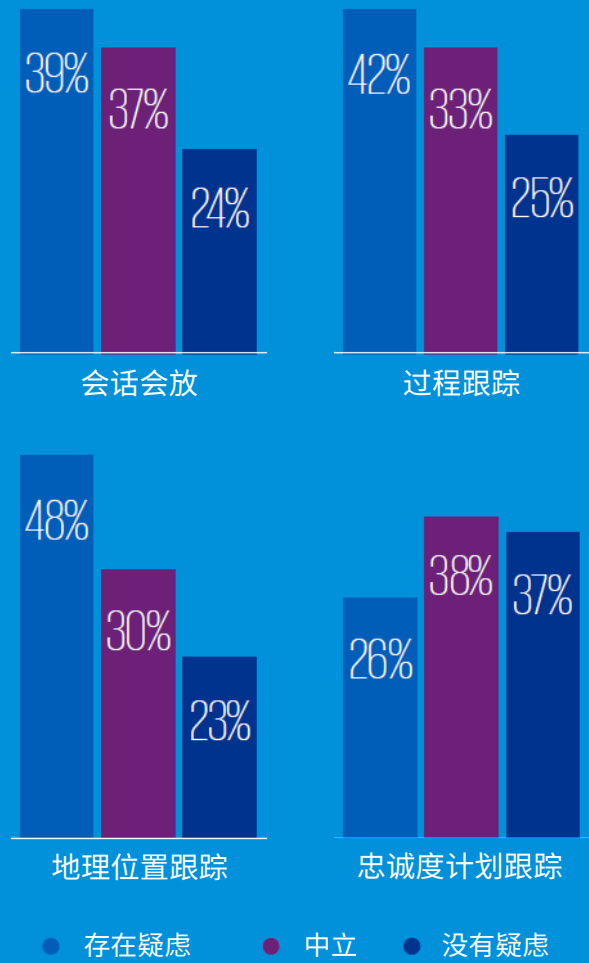
资料来源：消费者流失晴雨表：信任经济学。2019年。

同样地，我们询问消费者对零售商收集客户数据用于顾客个性化的行为有何不满。有趣的是，与非法入侵相比，消费者更担心零售商与第三方分享用户信息。此做法加剧了本行业的固有不信任，亟需零售商认真对待，因以消费者钱包和利润为目标的竞争正不断激烈化。



资料来源：消费者流失晴雨表：信任经济学。2019年。

客户可接受哪种数据跟踪？



资料来源：消费者流失晴雨表：信任经济学。2019年。

我们进一步向受访消费者提问，他们接受哪些数据跟踪方法。消费者最接受的是忠诚度计划跟踪，最不接受的是地理位置跟踪。消费者对忠诚度计划十分熟悉，这或可解释他们相对较高的接受水平。然而，确切知道某人的行踪可能会增加地理位置跟踪的“画蛇添足”感；人们也会联想到“老大哥”理论，因而可被视为越过底线并侵犯了个人隐私。



3

安全管理者 视角

© 2019 毕马威国际合作组织（“毕马威国际”）——瑞士实体。毕马威独立成员所网络中的成员与毕马威国际相关联。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。版权所有，不得转载。

作出改变

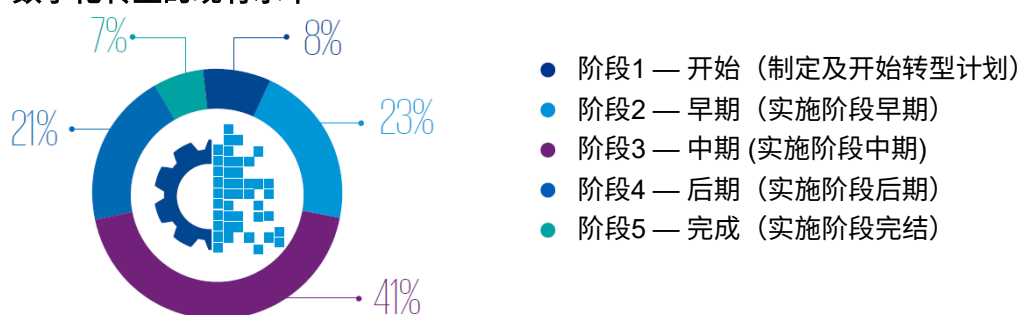
数字化转型现已成为各行各业日常运营的主要部分：我们调研的所有企业均正寻求在数据及技术的支持下创造更多商业价值，并使自身的核心业务流程更为灵活。然而，技术进化的规模和速度意味着企业须不断整合数据和技术以创造新的价值源头，使转型具备了持续性。

如毕马威的“2018全球首席执行官展望”
(2018 Global CEO Outlook)

调查所反映，这些转型活动正由高管层领导，而不是IT。我们的调研发现，各行业的企业领导均亲自主导数字化转型项目，其中72%的首席执行官表示他们已准备好实施彻底的组织变革。

大部分受访者表示，他们正处于数字化转型的中期阶段，而科技及电信业在这方面比金融服务、零售或汽车制造业走得更远。

数字化转型的现有水平



资料来源：消费者流失晴雨表：信任经济学。2019年。

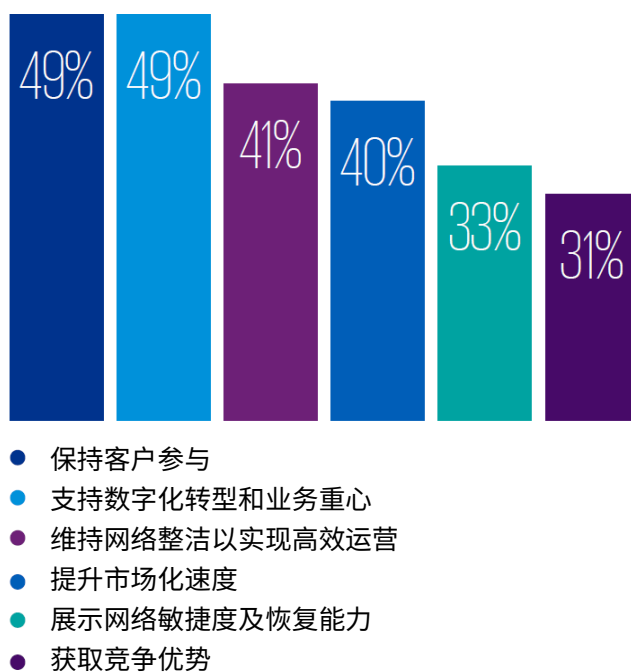
安全职能的转变能否跟上业务变化？

随着数字化转型成为企业常态和业务需要，企业的网络安全职能须作相应转变以实现技术的灵活应用、试验和实施。如果网络安全职能仍属针对已建立的IT及相关流程的响应性或基于合规的职能部分，则将在转型计划中被淘汰。我们相信，将网络安全深植于数字化创新及以客户为中心的职能的企业，若能进一步提升速度和敏捷度，将可跨越消费者与企业之间的网络安全鸿沟。这将有助于建立客户信任度和促进企业增长。

令人倍受鼓舞的是，受访的安全高管一致同意网络安全可为企业带来业务目标的潜在增值机会，而保持客户参与度和支持数字化及业务转型计划是网络安全带来的最重要机会。

对金融服务业和零售业而言，保持客户参与度是网络安全支持组织增长的最有利途径。这些行业均是以消费者为导向的，而这些市场中的消费者却有很多选择。在我们调查的所有行业中，消费者参与度均是网络安全带来的最优先机遇。

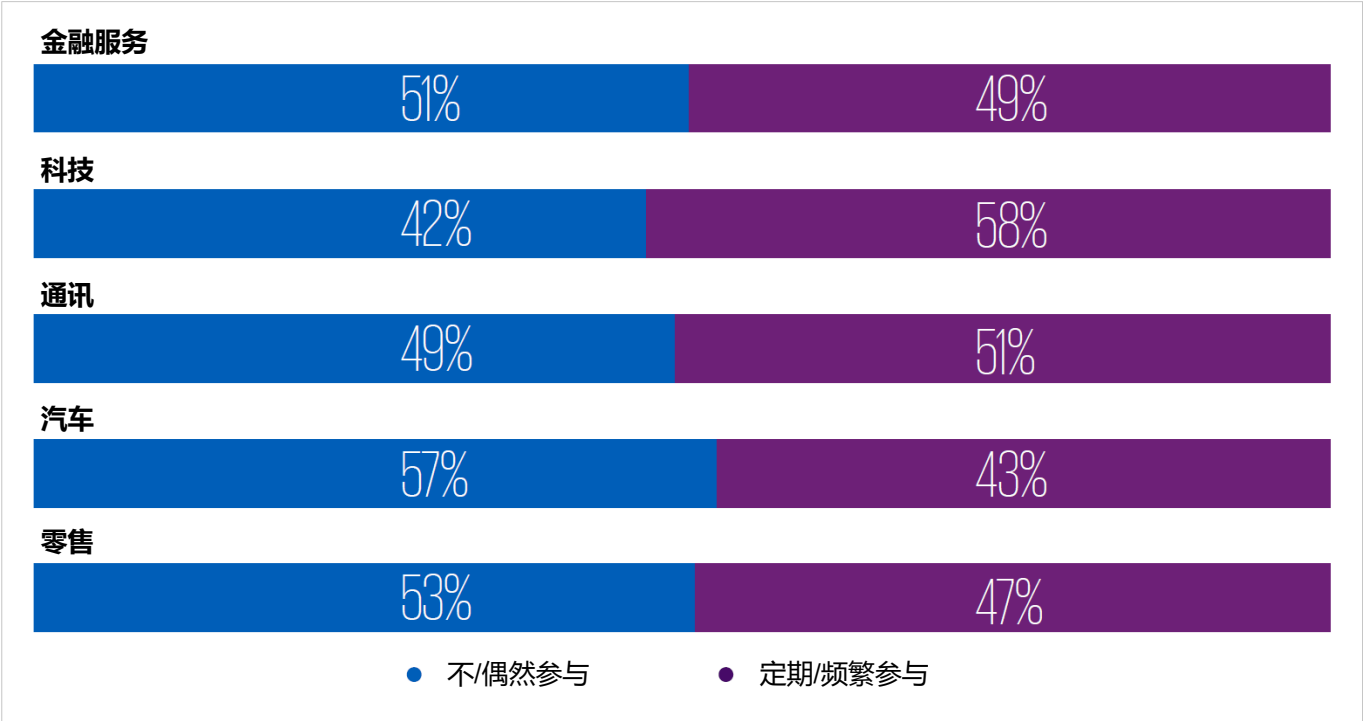
我们询问受访者网络安全是如何支持企业增长的：



数字化转型中的网络安全

虽然受访安全管理者珍惜网络对业务增长的潜在价值，但其中的不利因素是安全团队仍未融入数字化转型计划中。部分原因可能是即便数据流和业务流程正加速变化，安全专业人员仍偏爱在固定的技术架构下工作。

其中一个影响因素可能是网络安全团队在组织中的职能，其在组织中通常兼顾IT和风险管理两方面的工作，而较少关注业务战略增长计划相关工作。网络安全团队须配合数字化组织的变化，以适应利益相关者快速变化的需求，并具备合理权限以推动数字化转型。



资料来源：消费者流失晴雨表：信任经济学。2019年。

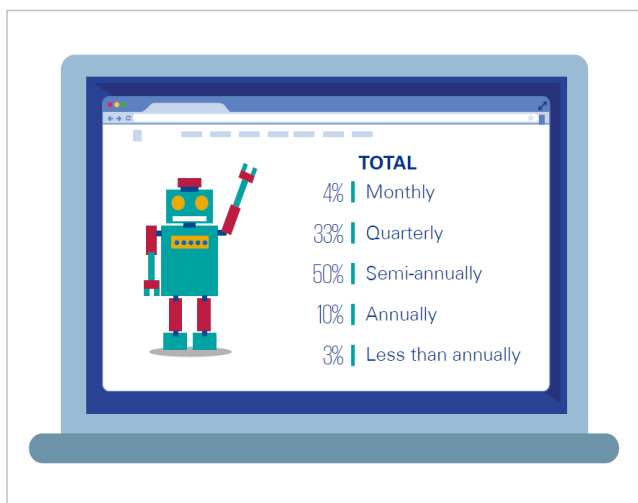


安全挑战

从业务角度考虑网络安全

不出所料，网络安全正越来越受高管层关注；大多数受访者至少每季度或每半年向高管作汇报网络安全工作。这支持了毕马威“2018全球首席执行官展望”中的发现，即企业高管将网络安全威胁列为企业未来发展的第二大风险。

一定数量的受访者表示其所在企业的高管甚少听取网络安全汇报



资料来源：消费者流失晴雨表：信任经济学。2019年。

令人忧虑的是，虽然所有受访者均表示他们已开展数字化转型工作，但仍有24%来自汽车行业及零售业的受访者表示，网络安全问题仍仅是高管层面的议题，且讨论频率仅为每年一次或更少。

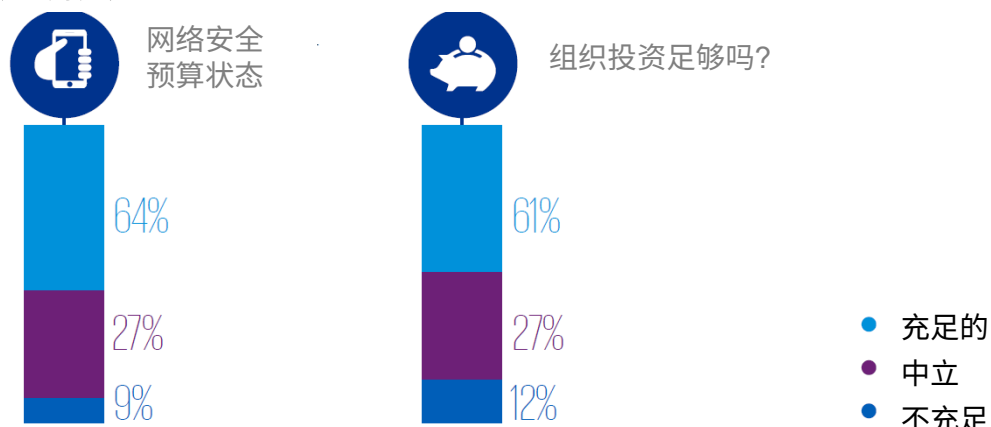
“首席执行官需要将‘网络忧虑’转变为‘网络信任’，” 毕马威马来西亚网络安全主管 **Dani Michaux**表示。“他们必须积极参与网络安全讨论，同时确保所有高管了解网络是其中一个战略重心。令人振奋的是，59%的首席执行官认为保护客户数据是重要的个人责任。现在，他们是时候将承诺转化为行动了。”

安全专业人员是否获得充足的资源？

大部分受访安全专业人员表示，他们的数据安全预算和投资水平目前足以应付他们的工作目标。但至少三分之一受访者认为他们未获得组织充分的财务支持。

安全团队的另一个挑战是展现一个可接受的投资回报率。董事会通过良好的治理可更好地分配开支，确保开支方案最优化，并与业务及技术重点项目高效挂钩。

信息安全是否获得足够的财务支持？

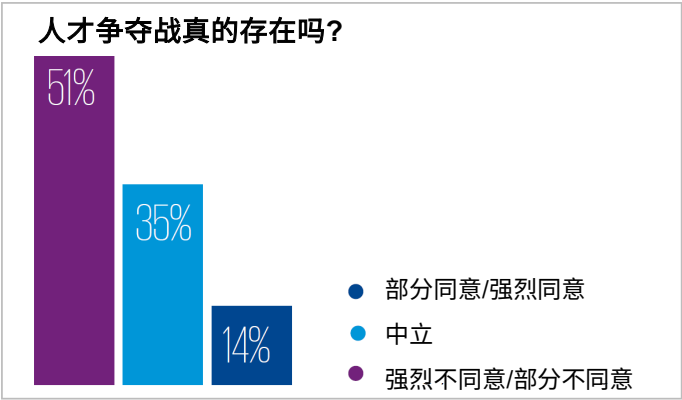


资料来源：消费者流失晴雨表：信任经济学。2019年。

人才争夺战真的存在吗？

招聘并留住合适的网络安全人才是组织安全战略的关键因素，也是对大部分受访安全管理人员的挑战；超过半数受访者表示难以找到满足他们需求的合适人才。为应对此挑战，企业需转变自身的运营模式，运用创新方法来创建全新人才库。譬如，聘用从未接受过传统科学、技术、工程及数学教育的人员，或提升现有员工技能以提升人才指数。

此外，企业还可通过建立新的员工模型来应对人才争夺战。员工短缺的解决途径包括提升自动化程度、众包和聘用合格的供应商。



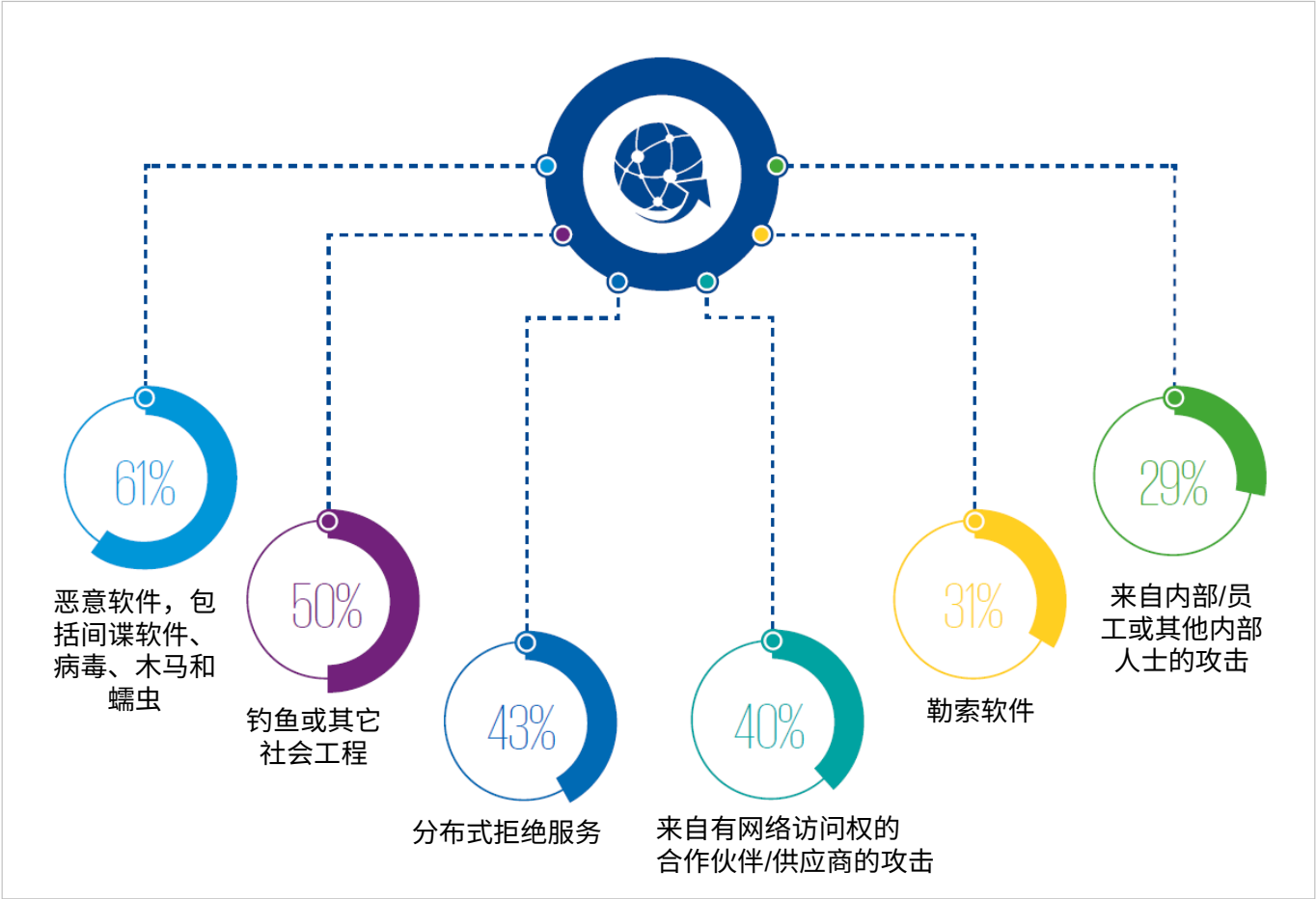
资料来源：消费者流失晴雨表：信任经济学。2019年。



“每一个企业须分析怎样做来吸引及留住人才，并思考哪些做法有效？哪些无效？人才争夺战中不会有停火，只有更好的策略及战术，” 毕马威全球首席信息安全官Brian Geffert表示。“未来，网络领域中要求的技能将是数字创新支持下的业务能力、数字化和安全技能。”



安全专业人员关注的是什么？



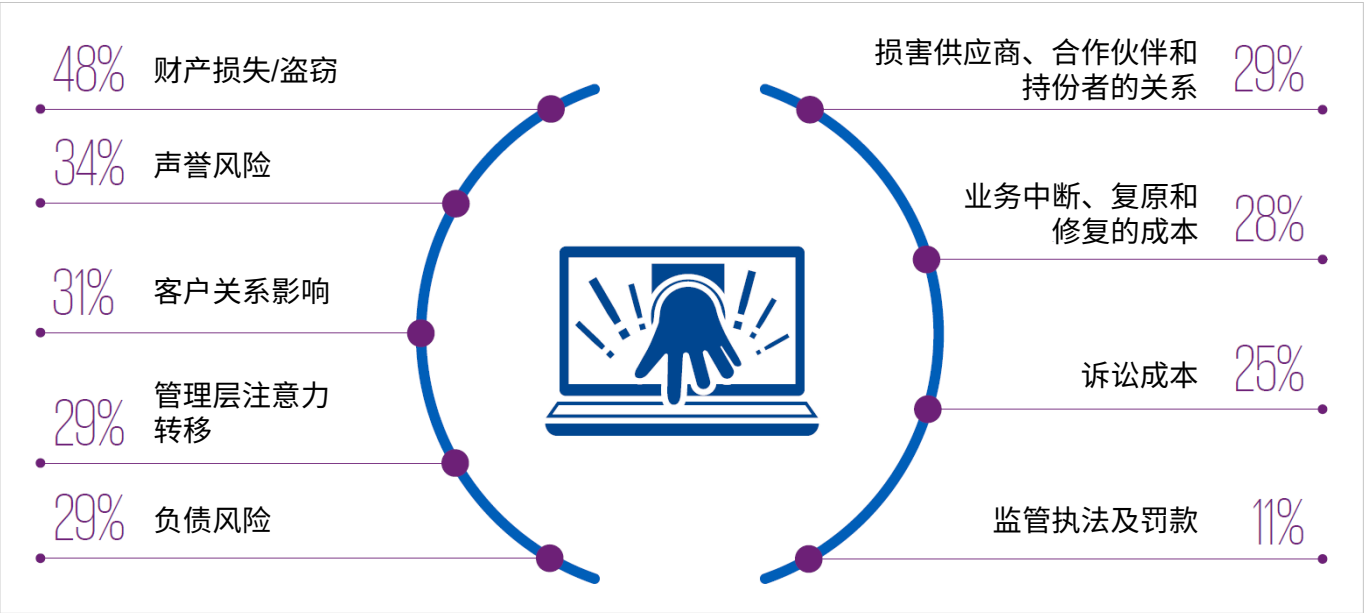
资料来源：消费者流失晴雨表：信任经济学。2019年。

根据我们的调查，安全管理者们最关注的是恶意软件，紧随其后是钓鱼及其它社会工程。分布式拒绝服务攻击可直接影响企业提供数字化产品和服务的能力，是处于第三位的关注事项。虽然2018年发生了数起引人关注的有关勒索软件的全球性事件，但NotPetya等勒索软件仅令不足三分一的受访者忧虑，位于来自第三方访问的攻击之后。

安全专业人员担心来自合作伙伴及供应商的网络攻击是正确的，因网络攻击者已将攻击重点转向供应链以及托管服务提供商的薄弱环节，而不是大型、成熟、更难入侵的企业。电子商务、数字化渠道以及加密数字也逐渐成为被攻击目标。

“网络罪犯的目标是花最小的成本得到最大的收益。由于他们追求投资回报最大化，因此着眼于可为他们赚取最大收益的活动 — 目前这些活动包括通过鱼叉式网络钓鱼及其它社会工程（所谓的“首席执行官舞弊”）使企业转出资金，以勒索软件进行勒索及对加密货币进行攻击。” 毕马威英国网络安全首席技术官 **David Ferbrache**表示。

当安全事件发生时，安全主管担心什么？



资料来源：消费者流失晴雨表：信任经济学。2019年。

出乎意料地，虽然安全管理者认为网络安全有助提升客户参与度，但仅不足三分一的受访者担心安全事件对组织客户关系的影响。

在这个客户至上的时代，企业须为网络攻击做好准备，并制定战略以在整个响应过程中保持客户信任度。只有这样，消费者才不会在安全事件中被忽略。



“《通用数据保护条例》（“GDPR”）等新法规可能要对违反消费者相关条例的企业实施巨额罚款。消费者和监管机构均要求信任，而当出现安全问题时，企业的钱袋便会感受到来自这两方的压力，” 毕马威网络安全欧洲、中东及非洲主管 **John Hermans**表示。

结论： 网络安全， 从顾虑到信任

在科技的快速发展中，消费者不断提升他们的数字化体验预期。但企业的步伐跟不上不断提高了的数字安全标准。企业的董事会层面仅关注数字化转型的有利方面，但这不足以应对转型带来的风险。

随着网络威胁的持续增加和复杂化，企业能否成功越来越取决于其能否在数字化服务及产品中建立客户信任。企业必须尽早开展安全性投资，并向消费者保证他们正解决消费者的疑虑。当安全事件发生时，企业必须在响应计划中考虑消费者的需求及预期，并开展相关工作以减轻数据泄露对消费者信任的影响。

消费者与企业之间的预期差距为某些前瞻性企业提供了宝贵机会，让它们可重新设定以信任为核心的客户关系。对于重点为建立网络适应能力的组织而言，现在是时候向消费者传达将此信息了。通过应用比竞争对手更强大的消费者保障措施，企业还可赢得巨大商机。

要实现此目标，企业须重新思考网络安全在企业中的角色和地位。

网络安全不应再被视为单纯的IT或风险职能，因将网络信任融入企业战略可带来巨大的商业机会。安全主管必须积极推动数字化转型计划；未来的人员招聘应注重业务技能以及数据安全技能；董事会亦必须发挥其作用，将数据安全因素纳入整体业务战略，而不是仅在网络风险管理中考量。

做好上述工作是新世纪企业生存的关键。

本报告贡献者



Ivan Atanasov,
Manager,
Cyber Security,
KPMG in the UK



Dieter Becker,
Global Automotive Leader,
KPMG International



Bia Bedri,
Banking and Capital
Markets Cyber Leader,
KPMG in the UK



Greg Bell,
Global Co-Leader,
Cyber Security,
KPMG International



Judd Caplain,
Global Banking and Capital
Markets Leader,
KPMG International



David Ferbrache,
CTO, Cyber Security,
KPMG in the UK



Tim Fletcher,
Director,
Cyber Security,
KPMG in the UK



Akhilesh Tuteja,
Global Co-Leader,
Cyber Security,
KPMG International



Marko Vogel,
Partner,
Cyber Security,
KPMG in Germany



John Hermans,
EMA and Cyber
Security Leader,
KPMG in the Netherlands



Alex Holt,
Global Chair, Media &
Telecommunications,
KPMG International



Willy Kruh,
Global Chair,
Consumer & Retail,
KPMG International



Dani Michaux,
Cyber Security
Leader,
KPMG in Malaysia



Thomas Nash,
Manager,
Cyber Security,
KPMG in the UK



Gary Reader,
KPMG Global Head of Clients
and Markets,
KPMG International



Jitendra Sharma,
Global Leader,
Risk Consulting,
KPMG International



Atul Gupta,
Cyber Telco and Cyber
Security Leader,
KPMG in India



Paul Taylor,
Partner,
Cyber Security,
KPMG in the UK

联系我们

石浩然

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

赫荣科

毕马威中国
网络与信息安全咨询
服务合伙人
Tel: +86 (755) 2547 1129
jason.rk.he@kpmg.com

Bhagya Perera

毕马威中国
网络与信息安全咨询
总监
Tel: +852 2140 2825
bhagya.perera@kpmg.com

沈俊伟

毕马威中国
网络与信息安全咨询
副总监
Tel: +852 2847 5044
darryl.sim@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

郝长伟

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

罗圣涛

毕马威中国
网络与信息安全咨询
副总监
Tel: +86 (755) 2547 3421
stuart.luo@kpmg.com

张令琪

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

黄财明

毕马威中国
网络与信息安全咨询
总监
Tel: +852 2140 2823
patrick.c.wong@kpmg.com

张倪海

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

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

调查方法

本报告发表的数据来自涵盖12个行业、24个市场中的1,802名安全总监（或同等职位）的调研。所有受访者均来自年收益在1亿美元至100亿美元之间或以上的企业。安全总监（或同等职位）的调研被翻译为九种语言。消费者数据来自24个市场中2,151名消费者的调查。调查样本包含所有年龄组别，其中千禧世代和X世代占比较高，并按性别分类。消费者调查被翻译为八种语言。

毕马威网络安全服务

毕马威网络安全服务协助全球性组织将安全性、隐私性和业务延续性控制转变为业务驱动型平台，同时保持关键业务职能的保密性、完整性和可用性。毕马威网络安全方案战略性对标客户的业务重点和合规需求。

kpmg.com/cn

所载资料仅供一般参考用，并非针对任何个人或团体的个别情况而提供。虽然本所已致力提供准确和及时的资料，但本所不能保证这些资料在阁下收取时或日后仍然准确。任何人士不应在没有详细考虑相关的情况及获取适当的专业意见下依据所载资料行事。

© 2019 毕马威企业咨询 (中国) 有限公司 — 中国外商独资企业，是与瑞士实体 — 毕马威国际合作组织（“毕马威国际”）相关联的独立成员所网络中的成员。版权所有，不得转载。中国印刷。

毕马威的名称和标识均属于毕马威国际的商标或注册商标。