KPMG

# 网络安全与物联网生态

# 前言

就物联网而言，业界的大肆宣传也并无言过其实。事实上，物联网的发展很可能会超出多数人的预期。但要在物联网领域取得成功，拥有灵巧的应用、互联的设备和先进的分析能力还不够，更需要的是寻找到能提升安全性、隐私性和信任度的可靠途径。

经营者和消费者对技术行业的需求十分明确：大胆、创新并且安全。

对于那些已在这个不断壮大的市场中占据领导地位的技术企业和物联网开发者来说，物联网显然可以为其带来巨大增长。但随着市场成熟度的提升和竞争的加剧，现有和潜在物联网用户对网络安全的关注亦随之增加。

正如本报告所述，技术企业和物联网服务供应商需快捷、持续和果断地应对用户对网络安全（设备和基础设施的控制程度如何?）、隐私（数据如何保密?）和信任（如何提升客户信心）方面的关注，以避免问题出现。不能满足这点的企业将难以在这个新环境中取得增长。

我们认为物联网行业必须纵向和横向地与同一生态中的企业联合，以建立统一的、每个企业均可接受并遵循的网络安全规范和标准以实现共同增长。当前行业标准的碎片化和竞争只会增加用户的使用难度，并因此妨碍物联网行业的发展。

© 2016毕马威会计师事务所 — 香港合伙制事务所，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。

本报告旨在深化讨论并扩充物联网安全性方面的知识。本报告开篇将指出正在影响物联网环境的网络安全、隐私和信任等方面的挑战，并深入探讨当前市场中涌现的机遇和模式。本报告根据一份近期进行的针对100家物联网用户组织的全球调查，以及与行业领袖、学者和毕马威物联网专家的一对一访谈，深入剖析物联网安全性、隐私性和信任度问题，并为这个新兴行业生态中的从业者提供切实可行的建议。

在未来，毕马威国际将更深入地探讨这些问题。在毕马威全球技术网络和物联网专家的支持下，我们将探索如何在不同行业、应用和行业生态中管理这些关键要素。

**Gary Matuszak**
全球主席
信息技术、媒体和电信业

**Greg Bell**
主管和服务总监，毕马威信息网络服务
毕马威美国

**Danny Le**
合伙人
毕马威美国

## 整合物联网

合数据、云、连接性、分析技术和其他技术，通过互联网建立一个物物相联的智能环境，以提升物件的功能性和互动性。

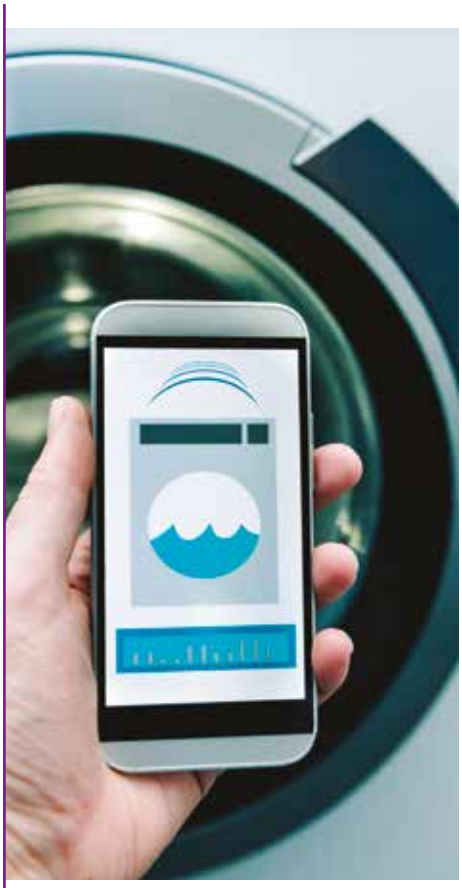
© 2016毕马威会计师事务所 — 香港合伙制事务所，是与瑞士实体 — 毕马威国际合作组织（“毕马威国际”）相关联的独立成员所网络中的成员。版权所有，不得转载。

# 目录

## 02

## 网络安全成为必备要素

© 2016毕马威会计师事务所 — 香港合伙制事务所，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。










© 2016毕马威会计师事务所 — 香港合伙制事务所，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。

# 网络安全成为必备要素

**92%**
物联网用户关注网络安全

资料来源:《毕马威网络安全及物联网调查》

行业领袖在认识到物联网可以带来的潜在优势的同时,亦对相关风险深感忧虑;其中大部分承认未能完全了解物联网可能带来的网络安全威胁。

虽然物联网客户仍不愿为网络安全付出额外成本,但最近在消费者数据和系统中出现的安全漏洞事件反映了他们会对不能采取适当措施以保护其信息安全的解决方案供应商失去信心,并且甚至可能放弃选用此类供应商。

每个人都想在物联网方案或产品投放上领先别人我们调查中89%的受访者认为物联网市场中的先行者将会获得明显的竞争优势。技术企业和物联网服务供应商纷纷迫不及待地推出自己的产品,希望在这个具有巨大增长潜力的新兴领域中获益。

其中道理非常明显。能成功取得市场先机并在物联网价值链中占据领导地位的企业可以利用自身的领导地位获取快速、可持续的增长。但现实是,过去已有许多重视投放市场的速度而轻视产品实质的产品及理念,它们正是由于重速度、轻实质而很快丧失了对其他反应较慢但更稳健的竞争者的比较优势。

© 2016毕马威会计师事务所 — 香港合伙制事务所,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。

简单来说，企业在开发及运营物联网方案时，应将安全性连同速度、可用性等关键因素一起视为重点。

近期事件已充分反映这点。据报导，一批新型汽车的软件漏洞已迫使某些大型汽车制造商做出大规模召回的举措。整个夏天，各大媒体都在议论黑客如何透过汽车软件漏洞来“劫持”汽车。

## 认真应对威胁

多数企业已就如何提高物联网安全性形成更清晰的思路。“在英特尔，我们认为在平台和芯片中植入安全配置是提升物联网应用及可扩展性的关键。在物联网方案源头应用安全配置是建立客户信任的关键”。英特尔集团物联网组执行董事Bridget Karlin表示，“我们已准备推出一批优秀的物联网产品，它们可通过英特尔物联网平台索引

> “我们公司对物联网安全风险的认识仍十分有限，因此把它作为头号工作重点。”
>
> – 某欧洲物联网用户组织首席执行官

## 物联网：快速增长，巨大潜力

物联网可以为商业、消费者和技术企业带来重大机遇这一点毋庸置疑。但大多数企业仍未充分了解物联网的巨大潜力。

对于设备制造商和应用开发者而言，物联网设备的快速应用有望使设备安装数量激增，并带来新一轮增长和扩张。根据互联网数据中心调查，物联网设备的安装基数将每年增长17.5%。该调查预测，未来五年内市场价值将高达7.1万亿美元[1]。

但我们相信，随着消费者越来越清楚物联网可带来的便利，如智能设备、自动驾驶、可穿戴设备等，他们对网络安全、隐私及信任度的关注亦会随之增加。

[1] 全球及区域性物联网 2014–2020 预测，互联网数据中心调查，2014年

© 2016毕马威会计师事务所 — 香港合伙制事务所，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。

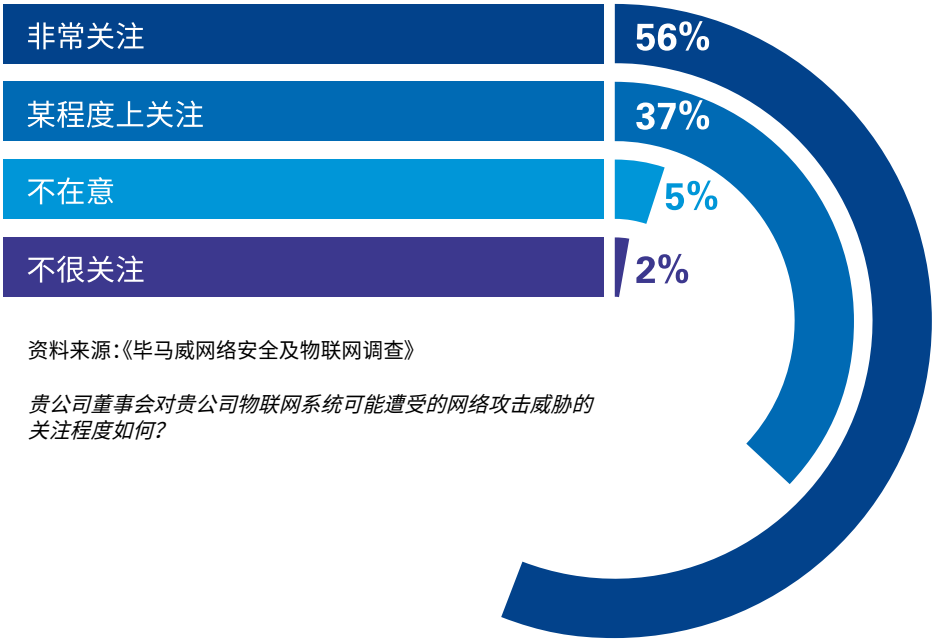
架构及配置了完整性和隐私性功能的软硬件产品组合，提供安全且可扩展的端对端物联网服务。”

物联网用户肯定非常关注其物联网系统内部的网络安全风险。我们的调查中超过半数（56%）的受访者表示他们的董事会“非常关注”网络攻击风险。

超过三分之一的受访者表示他们的董事会在某种程度上“关注”。

一位负责亚太区业务的首席风险官反映，“鉴于网络犯罪发生数量及频率的飙升以及物联网系统以及物联网系统所依赖的系统的技术复杂性，我们的管理层十分关注网络攻击威胁。由于整个IT系统已与新型物联网设备整合，因此任何威胁都可能影响到我们的业务连续性。”

## 物联网用户企业及其董事会愈加关注物联网系统遭受网络攻击的风险




资料来源：《毕马威网络安全及物联网调查》

*贵公司董事会对贵公司物联网系统可能遭受的网络攻击威胁的关注程度如何？*

© 2016毕马威会计师事务所 — 香港合伙制事务所，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。

## 风险与机遇

由于网络安全风险可导致数据丢失以及设备拒绝服务或丧失控制等，物联网安全的提升亦可带来重大优势。我们的经验表明，树立增强网络安全意识，建立公认的标准和采取强有力的措施建立和提升客户信任，是确保企业保持长期优势的关键，并将最终促进企业发展的网络安全意识、公认标准及采取有力的行动以赢取客户信任是确保企业保持长期优势的关键，并将最终促进企业发展。

“技术企业和物联网方案开发者必须将物联网安全、隐私及信任作为重中之重，”毕马威美国合伙人Danny Le提到。“网络安全的优势将逐渐显现。实际上，我们在不久的将来将可看到企业将网络安全技术转化为真正的利润增长点，譬如通过身份识别及用户使用模式获利。但企业在获取回报的同时，亦伴随着固有的风险。”

某些公司已在利用客户的个人数据获益。

举例来说，电信企业在许可的情况下使用客户定位数据来定制并提供第三方供应商（如保险公司、零售商等）服务；或根据客户驾驶模式组建汽车“社群”。然而，这些模式的持续扩张将需要生态系统中所有环节均能确保数据隐私、安全和保密。

选择稳步发展并投入适当时间和资源来将安全、隐私及信任理念整合到物联网方案中的技术企业和物联网方案开发者势必战胜那些不顾发展规律、以速度优先的企业。

> “物联网系统的初始设计阶段嵌入安全配置是很有必要的。你需要在硬件、固件、软件和服务层面上进行设计，并且需要不断实施监控以防范风险。”
>
> —Florence Hudson，
> Internet 2高级副总裁、首席创新官（曾任职IBM）

© 2016毕马威会计师事务所 — 香港合伙制事务所，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。

# 标准制定

物联网具有超速增长、应用急速扩散和使用案例快速涌现的特点，可以说是一个虚拟世界的“西大荒”，这里没有规则，缺乏监管，只有无数淘金者相互竞争。因此，从业者、监管者和用户将需要联合起来制定公认的标准并构建行业生态。

为了提高物联网方案的互用性和制定最低限度的安全标准，大多数企业现已同意行业标准发展是促进物联网普及的最重要途径。很多创新应用往往是在公认标准制定后才真正成为主流应用。

就此，规模不一但理念相似的技术企业开始组建联合体以共同制定新标准并对其进行商业化。每隔几个月就有新的联合体和标准发布，导致行业内竞争激化并对市场参与者构成重大不确定性。

比如，Goodle的Nest产品已与Samsung Electronics、ARM Holdings、Freescale Semiconductor 和 Silicon Labs 联合以制定“线程”网络协议，旨在统一家用物联网通讯标准。于此同时，Intel已与Cisco、AT&T、GE和IBM联合起来以制定物联网工业应用标准。Cisco也是AllSeen Alliance的一员，该组织由Qualcomm联合Microsoft、LG、HTC等龙头企业创建，目的是构建互用互联的通讯架构。于2015年8月正式成立的Online Trust Alliance，其成员包括，成员包括Microsoft、Symantec、Target和ADT。该联盟计划在消费物联网设备方面为物联网制造商、开发者和零售商提供指引。

© 2016毕马威会计师事务所 — 香港合伙制事务所，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。

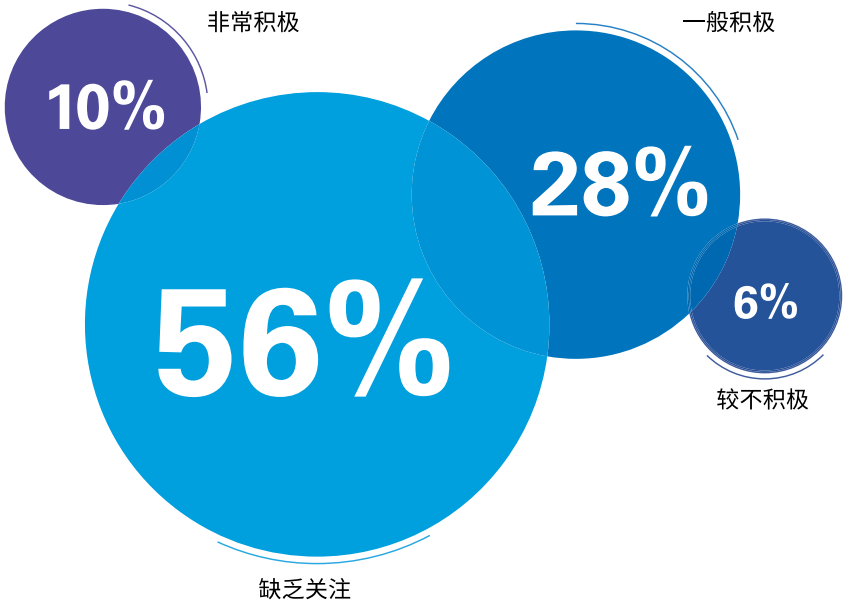
> “企业不应将规则视为成本，而应把目光放得更远，即应思考如何影响规则的发展以及其对市场发展和业务成功的作用。”
>
> —Michael Geist博士，渥太华大学互联网及电子商务法Canada Research Chair教授

“行业碎片化十分严重，很多标准及类标准制定组织在重复应对类似问题，因此，行业准则及标准的统一需要更广泛的协调和参与，”Cisco战略创新副总裁Maciej Kranz说道。

## 合作还是竞争？

鉴于物联网的广泛应用及系统与数据的敏感性，所有从业者均同意有必要理清物联网的规则及标准。Jibestream首席执行官Chris Wiegand表示：“物联网需依靠从业

## 大多数物联网用户企业对物联网方面的讨论不积极




资料来源：《2015毕马威网络安全及物联网调查》

*您的企业在行业内展开物联网讨论的积极性如何？*

© 2016毕马威会计师事务所 — 香港合伙制事务所，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。

企业才得以发展，我们应确保自己做对，而不是误用或滥用这项技术。”

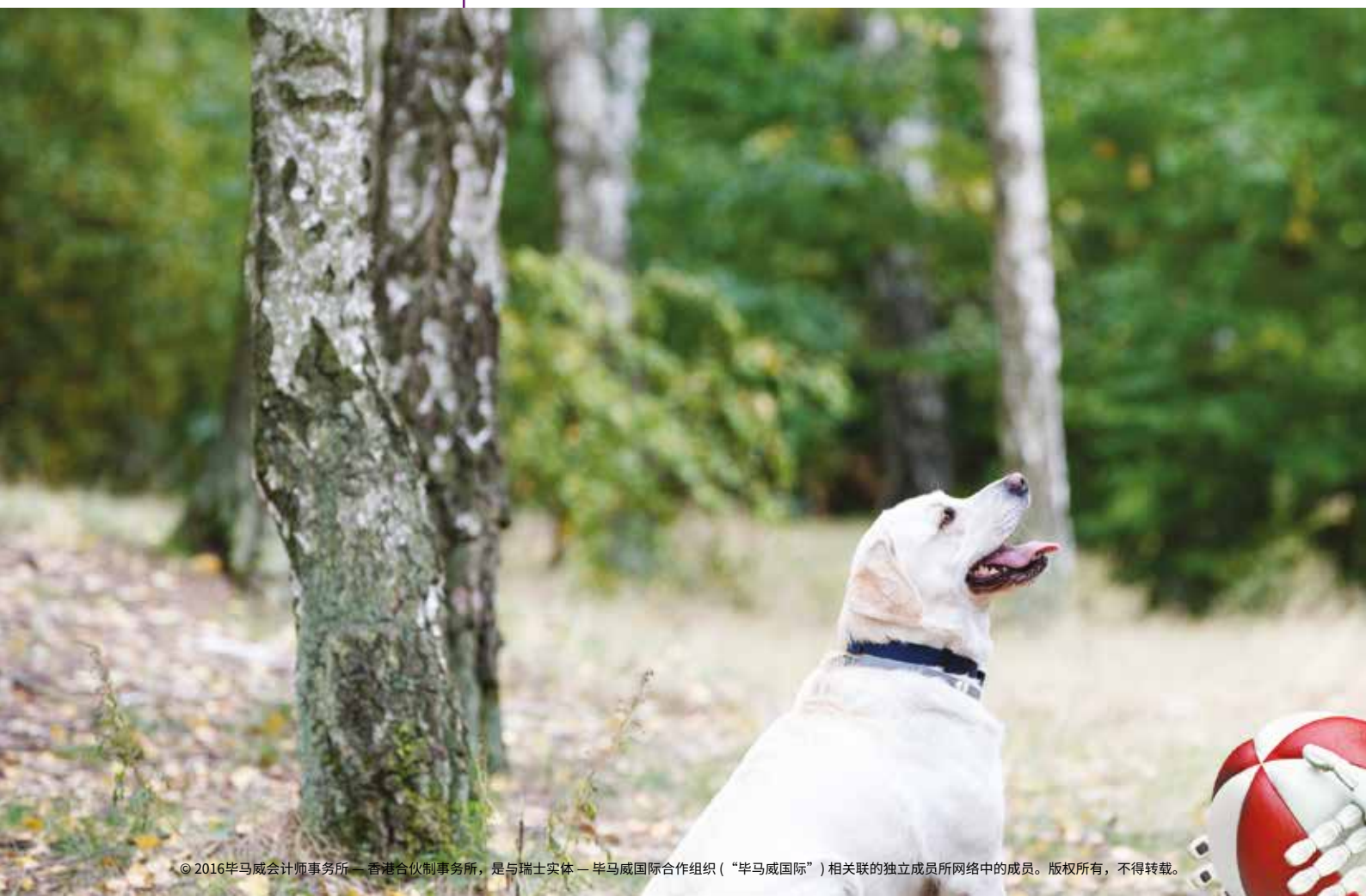
但部分市场参与者担忧标准上的竞争只会损害行业发展。 Internet2的Florence Hudson认为，“当前所有人都想成立联合体，但同时也在争取战胜对手，分裂亦由此产生。因此我的想法是在行业内部建立统一生态以制定安全及隐私等方面的准则，然后通过联合体来执行这些准则。”

监管和指引的完善亦将促进物联网发展。将近三分之一的正在应用物联网的企业表示，规则和监管的缺失对物联网的应用形成挑战。

金融服务、医疗保健和公用设施等高度监管行业对此特别关注。

“监管者通常不能及时了解行业创新，即使了解后，也很少会真正理解行业的变化；很多美国医疗保健企业会反过来告诉美国食品和药物管理局哪些可穿戴设备适用于美国医疗保健行业，对此我们毫不意外，”毕马威信息网络服务主管和服务总监Greg Bell补充道。“监管是一把双刃剑，一方面要求企业在合规和汇报上投入，另一方面则界定行为准则，使企业可推进投资及计划。”

但在某些行业，监管缺失或正阻碍物联网方案的应用。举例来说，特斯拉产品现已配有“自动驾驶”功能，该功能声称可减少意外并提高安全，当发展到自动驾驶汽车时更能减少意外发生。但目前道路监管者仍不愿意允许该功能用于公共道路，因此大大限制了这项创新技术可带来的竞争优势。



© 2016毕马威会计师事务所 — 香港合伙制事务所，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。

## 未来工作

事实表明，极少技术企业和物联网方案开发者是在积极编制标准。而与监管者沟通以了解或提议未来监管方向的企业则更少。

“行业生态内多数规模较小的技术企业似乎只是场外旁观，和他们的客户一起等待标准和规则出台；他们将决定权拱手让给大企业，”毕马威网络安全全球主管Malcolm Marshall说道。“采取被动的姿态已不可行，技术企业应积极与联合体合作，以了解并在可能的情况下影响标准的制定。”

另一方面，Cisco的Maciej Kranz重申，“现在至少有10到15个不同标准制定组织正在研究物联网安全、隐私及信任的不同方面。因此，我们应整合这些研究以推行统一及全面的标准，而不是每个行业各自编制自身的最佳实践及标准。”

© 2016毕马威会计师事务所 — 香港合伙制事务所，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。

# 以安全、隐私和信任为重

我们认为最成功的物联网解决方案供应商和技术企业应该是那些能同等重视安全性提升、隐私保护及信任建立的企业。这三个要素是企业在物联网领域确立市场份额的关键。

虽然网络安全似乎已成为物联网用户及开发者的关注重点，但经验表明，他们对其责任的理解仍十分狭义。

我们认为一个稳健的网络安全机制应不仅专注于保护作为系统基础的设备和基础设施，同时亦应重视建立合理程度的数据隐私性和增进客户及监管者的信任。

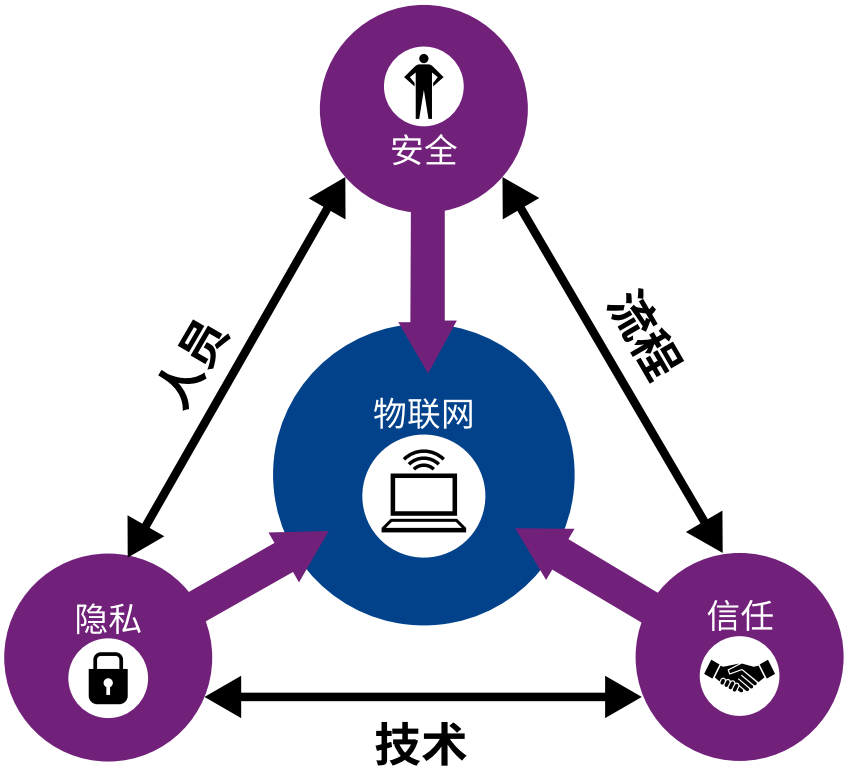
## 何为物联网生态中的安全、隐私和信任？

成功的物联网方案、产品和创新要求技术企业和方案开发者专注于安全、隐私和信任这三个关键要素，以提供有价值的用户体验，而这三个要素往往被混为一谈。

安全——通常被定义为组织管控其环境、设备和软件的能力，是行业会议及论坛的最常见议题，通常会被嵌入代码编写或生产流程并作定期更新。

而隐私则涉及保密及数据控制，因此难以“嵌入”方案或产品。

© 2016毕马威会计师事务所 — 香港合伙制事务所，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。




隐私不仅在于如何保护客户数据，而且还关系到客户如何进行数据权限分配以及信息如何在第三方之间共享和使用。

当前最少被议论的是信任对物联网生态的影响。

这里所指信任不仅是简单的“品牌信任”或信誉，物联网开发者和技术企业应在用户、合作伙伴、供应商和客户之间建立以信任和诚信为本的良好“生态”，为客户提供更多价值驱动的机遇。在合适的情况下，可通过能有效保护消费者或用户的可信任第三方来提升客户信任度。

© 2016毕马威会计师事务所 — 香港合伙制事务所，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。

### 毕马威观点

为使物联网安全措施生效，这些安全配置应与技术整合，并与软硬件紧密结合：设备应配置安全控制；软件应设置安全代码。安全机制应设置失效保险控制，即系统因故障而“离线”时仍然是安全的。我们不建议提供开放式设备或集中管控安全的平台，原因是相关风险实在太大。

“黑客会随时发起攻击。”IBM的Florence Hudson提醒。“我最担心的是医疗保健、汽车和交通运输以及关键基础设施的安全。”

## 以安全为重

当想到物联网设备将在未来所起到的作用（管理从房间温度到驾驶速度等日常方方面面）时，我们意外地发现很多物联网用户并没有积极采用传统的、目前流行的网络安全措施。

我们的调查显示，只有约40%正在使用物联网的企业已采取相关安全措施，其中包括提升防火墙控制、加强身份管理程序和加载反入侵软件等。

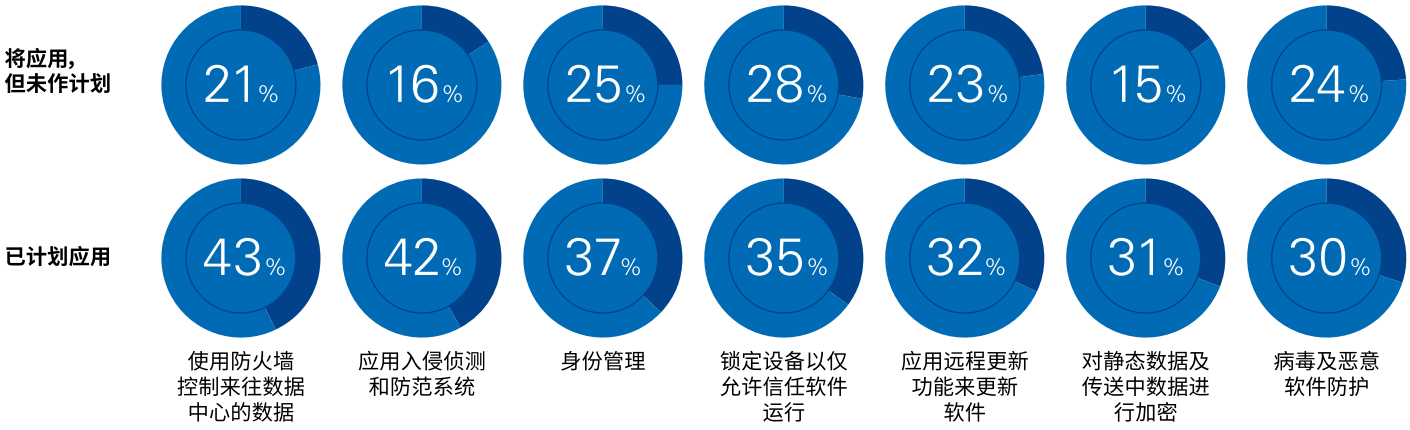
但网络攻击已是常态。2014年，工业控制系统网络应急小组（隶属美国国土安全部，专门应对网络安全威胁）汇报了245起针对控制系统（通常是工业物联网设备整合和控制平台）的威胁事件，其中55%为高级持续性威胁，即针对高价值商业目标的高级攻击；另外42%则以通讯、水利和交通基础设施[2]为目标。

事实表明，随着越来越多设备上线，网络攻击发动者将会变本加厉地对物联网设施发起进攻，无论是出于经济利益、政治目的或仅仅是为了练手。

与此同时，随着企业愈加依赖物联网数据，这些目标对网络攻击发动者的吸引力将大大增加。

为了营造一个更安全的物联网环境，技术企业和方案开发者应带头提升设备和方案的安全性。“设计者应在设计阶段就仔细考虑安全性，并在开发阶段不断测试和更新，”信息技术、媒体和电信业全球主席Gary Matuszak认为。“有能力进行售后更新和升级的企业不但可为客户增值，还有利于巩固自身的市场信誉。”

**物联网用户及方案供应商希望通过应用一篮子现有亟待开发的技术方案来应对网络攻击风险。**




资料来源：《毕马威网络安全及物联网调查》

*您的企业计划采取以下哪些措施以应对网络攻击风险？*

[2] https://ics-cert.us-cert.gov/monitors/ICS-MM201502

© 2016毕马威会计师事务所 — 香港合伙制事务所，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。

## 以隐私为重

现今的消费者越来越意识到个人信息对技术企业和服务供应商的价值，他们开始接受通过分享个人信息以获取服务提升或资费下降这一模式。

但这种以信息换价值的契约的基础是对哪些信息可以共享、与谁共享和用于何种目的等方面的明确协定。比如，使用联网心脏监护器的消费者会同意与医疗服务供应商共享个人数据，但很可能不希望与销售人员或医疗保险公司分享个人信息。

然而，对隐私的讨论很快演变为机会方面的讨论，而不只是针对风险方面。

简单来说，消费者已经开始意识到个人信息的价值，其中不仅包括交易记录信息，还有行为数据及其元数据，并已实质上与服务供应商“交易”个人信息以获取更好的服务、更低的价格或优惠。这对物联网公司来说代表着新的机遇和潜在价值。

“个人信息很快地变为一种新型货币，只要合适的状况和适当的回报，物联网用户将会很乐意分享他们的个人信息，”毕马威中国合伙人石浩然表示。“但这也意味着物联网供应商、企业客户及物联网价值链中的所有人需十分明确允许分享的信息种类以及分享对象。”

### 毕马威观点

企业将与用户商讨，以适当回报换取使用用户个人数据的权限。就此，技术企业和物联网方案开发者将获得难得机会为客户提供和管理增值服务，这些增值服务可在管理权限的同时安全地整合和合并数据。

© 2016毕马威会计师事务所 — 香港合伙制事务所，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。

### 毕马威观点

由于企业专注于为终端用户提供更全面和无缝的用户体验，物联网将进一步促进产品和服务的整合，如将可监察交通流量的地图服务整合到汽车上，或为手机开发支付应用等。

## 以信任为重

正如个人信息可转化成消费者的价值，信任亦可转化为技术企业和物联网解决方案供应商的价值。已有海量案例证实“品牌信任”、客户体验和销售额之间存在确凿联系。

客户信任度高的品牌产品和服务不仅与客户联系更密切，而且可实现更大范围的交叉销售。譬如，某些技术企业已成功将某个服务领域的品牌和客户信任转化为另一全新领域的市场领导地位——正如手机支付，可以说这项服务是全新的、且没有任何经验可循。由此可见，客户信任度是物联网领域长期成功的关键。

“信任的建立基于企业保持系统安全性的能力和保护客户信息的能力，但同时亦应考量品牌形象、客户沟通方式以及对意外安全或隐私漏洞的处理方式，”毕马威英国网络安全服务高级经理Richard Marriott如是说。“你不能假定只要保证安全了，信任就自然来。你必须用心建立这份信任。”

> “当前业界的热点话题是如何保持客户信任度、以及隐私、安全和数据完整性问题。”
>
> —Danny Le,
> 毕马威美国合伙人

### 毕马威观点

一部分市场参与者将最终成为行业生态内的“可信任供应商”。当“可信任供应商”（而不是设备制造商或服务供应商）占据主导地位时，挑战亦随之显现，原因是行业生态中的其他市场参与者可能会被“去中介化”。

© 2016毕马威会计师事务所 — 香港合伙制事务所，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。

© 2016毕马威会计师事务所 — 香港合伙制事务所，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。

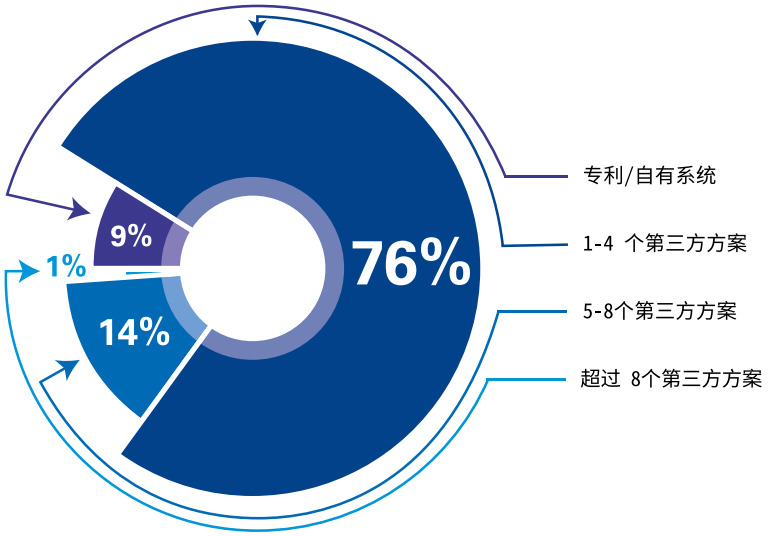
# 全面提升行业生态的安全性、隐私性和信任度

在物联网领域，没有企业可以通过单干取得成功；成功必须依靠企业间的合作、价值链的创建和行业生态的蓬勃发展。但随着物联网用户将越来越多的市场参与者、服务供应商和第三方供应商引入其价值链，技术企业和物联网解决方案供应商将面对更大的安全压力。

为创建一个有效运作的物联网生态，用户企业需使用多个不同领域的服务供应商。已有超过四分之三的物联网用户表示他们使用一到四个第三方供应商来管理物联网方案；15%的用户表示他们使用五个以上第三方供应商。

“单打独斗是不可行的。Cisco也正在大力发展横向及纵向的合作伙伴，以开发和交付平台功能和解决方案，”Cisco的 Maciej Kranz表示。

**物联网生态正在形成，用户愈加意识到他们需要依赖第三方和服务供应商才能制定强而有力的市场策略**




资料来源：《毕马威网络安全及物联网调查》

*您的物联网方案包含多少第三方服务供应商？*

© 2016毕马威会计师事务所 — 香港合伙制事务所，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。

## 毕马威观点

行业生态将由客户位于末端的线性模型转变为客户居中、生态组成者围绕四周的模式。在这个环境中，随着生态组成者开始承担不同的角色和呈现不同的整体价值取向，我们将会看到传统角色的转变。

过去的技术生态是线性的：


物联网生态中，生态组成者围绕着客户运转


然而，数据显示极少物联网用户会考虑他们新的价值链对物联网方案整体安全性的影响。44%受访者承认他们从未关注过第三方合作伙伴是如何看待安全风险的。

“物联网设备上的网络攻击已成为确实的风险。为规避风险，我们应选择具备一定水准风险管理或安全机制的供应商，并远离那些将物联网世界视为狂野西部而在安全性上有所松懈的供应商，”Jibestream的Chris Wiegand说道。

相反，小型的新创办企业和品牌认可度较低的企业却往往发现他们可以凭借合作伙伴的优势而迅速建立客户信任。

© 2016毕马威会计师事务所 — 香港合伙制事务所，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。

## 第三方评估

随着物联网市场的发展和应用的增加，未来物联网用户将要求物联网生态中的供应商本身亦应具有与客户一致的政策和安全措施，以确保安全性、隐私性和信任度。有的企业应用了相关技术和工具（如远程流程监控）来跟踪供应商表现。其他企业则要求供应商获取认证或执行审计以确保一致性。

一名北美公司的首席信息官提到，“我们已委派一家经认证的评估机构来评估外部合作伙伴的安全标准，合作伙伴亦同意接受评估，为此我们支付了预算中的合理数额。

企业的普遍做法是执行第三方尽职调查或现有的标准和鉴证项目来评估第三方安全状况，其中包括服务组织控制第2类 – 鉴证报告（SOC2，对组织控制的设计和运行效力进行测试和报告）。SOC 2 基于五个“可信任服务原则”：安全性、可用性、流程完整性、保密性和隐私性。举例来说，美国医疗保健行业越来越多地使用SOC2来确保第三方不但已取得高水平的安全性、隐私性和信任度，而且还遵循包括HIPAA法案在内的主要数据安全法律法规。

### 毕马威观点

物联网生态中的所有参与者应有责任保护系统的安全性、隐私性和信任度以便执行“协议握手”，从而确保终端用户安全。

© 2016毕马威会计师事务所 — 香港合伙制事务所，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。

# 五大要点

1 **联网市场正不断演变。**物联网行业飞速发展，未来很可能会经历数次转型。物联网安全性、隐私性和信任度方面的关注亦会随着市场变化而演变。因此，用企业以广泛的基础来制定安全策略以预知及应对潜在的、可能影响当前市场定位的重大变革。

2 物联网生态在确保物联网安全方面起关键作用。企业应认真评估第三方供应商、确定合格的合伙伙伴，以及投入资源以全面整合行业生态的安全性、隐私性和信任度。企业应评估各种方法以在行业生态中建立所需功能，其中包括是否可以通过购入、建造、合伙、投资或创建联盟以实现业务企业目标。

3 **应从客户角度考虑，在系统设计初期嵌入安全配置。** 消费者和业务伙伴希望将安全配置嵌入系统；技术设计者应遵循“永远在线”原则，确保方案具有高水平的控制和适当的失效保险机制。考虑到物联网增长规模之大、速度之快，安全漏洞可能为企业带来严重问题。

4 **在物联网安全领域中提升价值。**安全方案设计者应重新评估安全模式以识别安全领域中可带来价值提升的机遇。譬如，以安全、隐私和信任这个“溢价概念”来进行推广以使产品与众不同。物联网安全不仅在于保护高价值数据，更可以带来从信息中获益的机会。

5 **参与行业及监管活动以加速物联网规范化和标准化进程。** 行业和监管部门的合作有助降低政策的不确定性，并提高企业在一个可持续的业务生态中推出产品和服务的能力。同时，监管者亦需要参与行业讨论以更好地保障市场和消费者利益。技术企业应积极地协助监管者以支持物联网发展。

© 2016毕马威会计师事务所 — 香港合伙制事务所，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。

## 联络方式

如需更多关于本刊及毕马威信息技术、媒体和电信业服务的信息，请联系以下人士：


石浩然
网络服务合伙人
毕马威中国
电话: +852 2143 8799
电邮: henry.shek@kpmg.com

梁景丰
网络服务总监
毕马威中国
电话: +852 2847 5052
电邮: kk.leung@kpmg.com

崔巍
网络服务总监
毕马威中国
电话: +86 (10) 8508 5470
电邮: calfen.cui@kpmg.com

张令琪
网络服务总监
毕马威中国
电话: +86 (21) 2212 3637
电邮: richard.zhang@kpmg.com


## 鸣谢


本文是《网络安全和物联网生态》的修订，由Gary Matuszak，Greg Bell和Danny Le编写。

我们希望在此感谢以下对本研究报告作出特别贡献的人士：

所有调查受访者，Florence Hudson，Michael Geist，Bridget Karlin，Maciej Kranz，Chris Wiegand和外部作者 Peter Schram.

为本文提供专业见解的毕马威合伙人和主管：Malcolm Marshall，Richard Marriott和石浩然。

毕马威国际项目小组：Sunitha Shivakumar，Alise Barnes和 Carolyn Forest。


**kpmg.com/cn**


本刊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。

© 2016毕马威会计师事务所 — 香港合伙制事务所，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。香港印刷。

毕马威的名称和标识均属于毕马威国际的商或注册商标。



Evalueserve设计。

刊物名称：Security and the IoT ecosystem（《网络安全和物联网生态》）

出版日期：2016年1月