加速车辆信息安全

赢得车辆完整性和数据隐私性竞争

IBM 商业价值研究院

执行报告
汽车制造业

IBM 如何提供帮助

如今，车辆正逐渐从一种交通工具转变为新型的移动数据中心，车载传感器和计算机能够即时捕获有关车辆的信息。利用此类实时数据，IBM 可以帮助汽车制造业的高管提供全新的服务，满足互联互通时代的消费者对于车辆体验的新要求和期望。我们既拥有丰富的制造业经验，也拥有深厚的全球汽车行业专业知识，可以消除消费者对行车安全和车辆质量的顾虑。通过使用 Watson 等创新技术，我们可以满足汽车制造商 (OEM) 和供应商的各种需求，提供更安全可靠的产品和服务，从而实现更高的品牌忠诚度和客户满意度。请访问 ibm.com/industries/automotive

预防、检测和响应

*2014 年，IBM 发表了研究报告“促进安全：*新一代车辆的网络保障”，阐述了我们对于汽车信息安全的观点，介绍了汽车信息安全生命周期的“设计，制造，驾驶”方法。[1] 现在，我们希望更深入地推进这种方法。*尽管从“设计”阶段开始的汽车信息安全生命周期中，每个阶段都可能出现安全问题，但有关信息安全的大多数话题都主要聚焦于使用中的车辆和数据隐私所面临的威胁，也就是集中在“驾驶”阶段。因此，我们重点关注这个阶段，消费者可以轻松发现并评价汽车制造商如何利用技术来预防漏洞，检测可疑行为，以及通过稳妥安全的恢复措施应对威胁。*

执行摘要

消费者催生了互联互通式汽车。我们总是希望在行驶旅途中有美妙的音乐陪伴，曾几何时，我们在车上听的是 8 音轨磁带中的音乐，而现在，移动手机可以存储成千上万首歌曲，当然，要通过汽车的扬声器来播放。

这听起来很简单，但汽车与外部设备的连接还是存在一定复杂性的。如果汽车可以提供蓝牙服务，为什么不能作为 WiFi 热点为所有乘客提供服务呢？在我们最近的“人车新关系”调研中，我们发现 49% 的受访消费者希望未来 10 年内汽车可以成为物联网 (IoT) 中安全的集成设备。[2]

现代的出行者既希望在不同的交通方式之间无缝切换，又希望保持一致而个性化的数字化体验。许多技术共享有关出行者的信息，而且这些技术各自独立地参与联合运输体验，因此监管和隐私就成为需要关注的问题。当出行者从一种出行模式切换到另一种时，必须确保车辆上的个人数据被清除，并对旅行期间所捕获的持久数据进行适当保护和加密，在最终删除之前最大程度缩短数据保留时间。

好消息是到目前为止，互联功能还没有给威胁分子可乘之机。尽管研究人员最近的试验证明，控制车辆是可能的，但是车辆的漏洞还没有被广泛地利用。[3] 目前，通用的计算平台，例如台式电脑、笔记本电脑甚至是移动手机和平板电脑都很容易成为恶意软件和勒索软件的目标；然而，因为安全控制使得攻击者危害这些目标变得更加困难，所以他们将攻击目标转向物联网，包括互联互通的车辆。[4]

56% 的消费者表示信息安全和隐私保护将成为他们未来做出车辆购买决定时的主要考虑因素

在互联互通式汽车时代，**没有信息保护的车辆就不是完全安全的**

信息安全必须融入到企业的文化精髓之中，并在车辆的整个生命周期确保信息的安全性

在互联互通的汽车时代，不仅仅是消费者的安全和隐私处于风险之中，汽车制造商和移动生态系统中的其他参与者(例如电信和保险公司)更是责任重大。我们无法阻止攻击者和研究人员探测漏洞。汽车制造商需要尽自己最大的努力生产没有漏洞的产品，持续对产品进行全面测试，并随时准备好了解、修复和公开回应调查人员的发现以及出现的各种事故。随着汽车不断朝着“轮子上的数据中心”发展，亟需一种多学科的方法，涵盖传统和非传统的参与者以及各种能力，应对网络安全和数据隐私方面的挑战。

汽车制造商还必须确保涉及行车安全、信息安全和隐私保护的工作公开透明。56% 的受访消费者表示，安全和隐私将是他们未来做出车辆购买决策时的关键考虑因素。[5] 尽管消费者需要最新的技术，但是他们也希望这些技术以确保行车安全、信息安全和数据隐私为前提。

为成功打下坚实基础

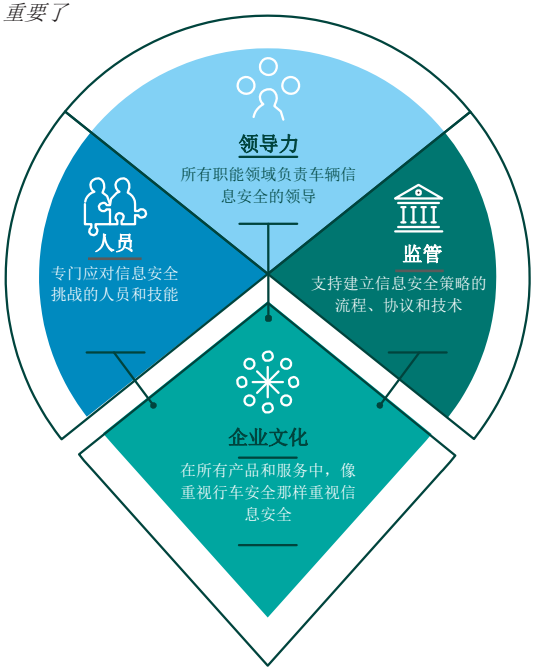
如果汽车制造商能够做好充分准备，那么他们在设计有效的信息安全解决方案时就能取得最大的成功。成功的基础主要有两个方面：一是确保将信息安全融入企业的文化精髓之中；二是为汽车制造商和消费者（尤其是后者）建立强大的数据模型，能够全面理解数据使用、隐私和所有权等各个方面。只有这样，汽车制造商才能真正落实“设计，制造，驾驶”信息安全方法所有阶段，尤其是“驾驶”阶段，从而能够有效预防、即时检测和从容应对各种威胁。

将信息安全融入企业的文化精髓之中

互联互通汽车的信息安全始于企业层面，应当渗透到汽车制造商的企业文化之中，上至领导，下至员工，贯穿整个监管领域（见图 1）。“设计，制造，驾驶”方法需要一种新的观念，将信息安全上升至与行驶安全相同的重要性水平，在物联网时代，没有信息安全就没有行驶安全，也就不可能实现互联互通汽车。信息安全并非大多数员工固有的关注点，包括有些身处领导岗位的人员；因此他们必须学着将信息安全作为优先任务来抓。特别是汽车制造商，需要将信息安全落实到每个流程之中，通过反复强调，使之成为员工的自然条件反射。

图 1

如果汽车制造商接受信息安全观点，并在企业文化中践行这个观点，车辆信息安全就变得与行车安全一样重要了



欢迎非传统的行业参与者

汽车行业无疑非常清楚自己的技术和行车安全模式，但信息安全研究人员则更了解网络安全形势和威胁分子。在 IBM 商业价值研究院的最新报告“2025 汽车展望：大业无疆”中，我们发现与消费者最有共鸣的数字体验都是由外部合作伙伴而不是汽车制造商所设计。[6] 这是因为，这些接口基于消费者的设备，比如移动手机，能够营造更亲密的用户互动体验。以下是一些建议：应当与非传统的行业参与者合作，因为他们拥有深厚的多学科专业知识，可以设计出最理想的解决方案。

因为设计、制造和管理车辆的整个周期非常复杂，涉及许多不同的组织实体，所以必须有一个主体单位来定义信息安全战略和实践，并监管各个实体的实施和协作。这个主体的负责人通常被称为“网络安全沙皇”，无论叫什么，这个职位必须有权与设计、生产和服务等各个组织实体开展合作。该主体必须确保在各个实体中进行宣传和沟通，鼓励每个人在“设计，制造，驾驶”阶段创建和管理方案时，考虑安全问题和威胁模式。

汽车制造企业还必须从行业外部聘用具备信息安全知识的人才担纲各种关键职位。此类专家能够发现信息安全实践的漏洞，推动改进措施，还能够向周围的人宣传信息安全理念。

汽车行业正不断扩大自己的边界，超越特定于汽车的技术，涉足汽车制造商所不熟悉的领域。汽车制造企业必须和物联网技术和信息安全方面的专家合作，包括软件和固件分析师、通信和网络工程师、云架构设计师、移动设备开发人员、威胁分析师以及数据科学家。汽车制造商还必须在汽车行业内开展合作，共享威胁情报，而且他们必须跨行业进行合作，以便尽早检测到常见威胁，例如国家的间谍活动。

合作还意味着邀请研究人员测试汽车产品，第一时间与汽车制造商分享他们的发现。可以通过表彰和奖金来激励研究人员：抓错奖励计划是一种有效的方法，鼓励他们发现更多的现实攻击情况，这不是内部质量评估团队可能找到的问题。

最后，消费者需要了解汽车制造商正在积极采取步骤，解决信息安全问题和提高信息安全水平，确保互联互通汽车的行车安全和隐私更有保障。汽车制造商必须做到公开透明，也就是要列出具体内容，比如漏洞的详细信息，并为客户提供工具，帮助他们确认车辆是否处于最新状态。与研究人员合作并与消费者联系，是建立信任关系和保持品牌忠诚度的关键。

评估数据使用和所有权

在评估信息安全和隐私保护时，强大的数据使用和所有权模式非常重要。这包括生成的数据以及有关收集、传输和存储数据的位置和方式等方面的信息。此外，汽车制造商必须对数据进行分类。数据是属于车辆使用者还是属于汽车制造商？如何根据这些信息保护数据安全？

汽车制造商一直在谁最终拥有数据的问题上犯难。比如天气和地图等信息很明显属于汽车制造商。手机联系人、通话记录和短信息很明显属于消费者。但谁是车内传感器遥测信息的所有者？除非法律特别规定，否则汽车制造商会认定这些数据属于车辆使用者，只有在消费者通过某种选择机制同意的情况下，他们才能对这些数据进行传输、存储和使用。[7]

可识别个人身份的敏感信息可能会归入“数字化个人”类别。举例来说：

- 汽车可能通过驾驶风格“了解”您的感受，并相应地做出响应。如果驾驶风格非常大胆奔放，汽车可能会从重金属电台切换到舒缓的爵士乐电台，帮助您平静下来。
- 汽车可能会在方向盘上安装心率监控器。如果监控器检测到您的心率出现严重异常情况，就会切换至完全自主驾驶模式，并发出紧急情况警报。

当今车辆中的个人数据

当今的车辆中，个人数据无处不在。例如，导航系统可能会收集车辆位置坐标数据，并将数据发送给汽车制造商的后台系统，以便对驾驶模式进行分析，然后反馈给导航应用。车辆必须将这些数据进行匿名化处理，删除有关车主或车辆使用者的个人信息。如果消费者将手机与车辆配合使用，并且同步联系人、通话记录和短信等信息，车辆必须对这些数据进行加密。车辆使用者离开该车，并且手机和车辆的距离超出一定范围时，车辆必须清除这些数据，这样，后来的使用者便无法访问这些数据。

- 如果您发生事故或遇到紧急健康问题，汽车可能访问您的病历，并将这些信息传输给急救人员。

对于汽车制造商来说，这个领域的复杂性只会越来越高。消费者直到确信自己的数据受到保护时，才会真正意识到互联互通汽车可以带来的好处。

接受“设计，制造，驾驶”信息安全方法

尽管本文的重点是深入探讨“驾驶”阶段，但是简单概括一下前两个阶段的关键组成部分也非常重要，因为所有三个阶段的工作结合在一起才能形成一个值得信赖的生态系统（见图 2）。

设计信息安全指的是规划如何抵御攻击，不仅仅是考虑车辆内部的信息安全，还包括车辆与基础架构之间互动的安全。实现这种信息安全的指导原则是假设最糟糕的情况，为应对故障而设计。例如，总线系统上的每次互动都可能会受到威胁，因此电子控制单元（ECU）不应盲目地对每条控制消息采取行动。

在设计安全的汽车时，设计流程必须从一开始就关注信息安全问题。这包