汽车行业工业物联网

实施迅速，保护滞后

IBM 商业价值研究院

对标分析报告

汽车行业

IBM 的能力

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，也具备深厚的全球汽车行业专业知识，可以帮助消除消费者对安全和质量的顾虑。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。敬请访问：**ibm.com**/industries/automotive。

本报告亮点

汽车行业工业物联网 (IIoT) 的网络安全风险与采用进展情况

表现出众的企业在保护 IIoT 安全环境方面展现出三大独特的优势

九项重要的网络安全实践

智能工业物联网的网络安全

互联自主驾驶汽车的安全问题备受关注。但企业更应当专注于基本层面，即用于制造汽车以及科技含量日益提升的零部件的工业系统。如果在没有实施有效的网络安全措施的情况下，匆忙上马“智能工业物联网”，会让整个企业处于风险之中。IBM 商业价值研究院 (IBV) 的一项调研表明，87% 的汽车企业在工厂和装配线上实施了工业物联网 (IIoT) 技术，但没有充分评估风险或准备有效的应对措施。汽车企业需要提升网络安全能力，能够以认知方式自动适应所处环境，持续发现、缓解和预防风险。

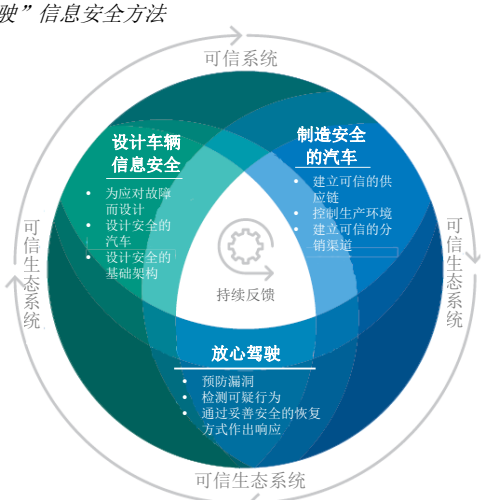
危机四伏

随着工业物联网技术的实施，制造设备和流程变得越来越智能化和自动化，但企业所面临的网络攻击风险也与日俱增。网络入侵可能来自于网络黑客、竞争对手、进行商业间谍活动的国家或地区，或者是心怀不满的员工，这都可能导致大量设备损坏、关键数据丢失、企业声誉受损甚至人身安全受到威胁。

在 IBV 调研“加速车辆信息安全：赢得车辆完整性和数据隐私竞争”中，我们介绍了“设计、制造、驾驶”信息安全方法（见图 1）。[1] 这种方法中的“制造安全的汽车”阶段明确了控制生产环境的要求。

图 1

“设计、制造、驾驶”信息安全方法



来源：IBM 商业价值研究院分析

87%

的受访汽车企业正在部署 IIoT 技术，但未对风险进行全面评估

86%

的受访汽车企业没有定期进行 IIoT 网络安全评估

87%

的受访汽车企业没有正式制定 IIoT 网络安全计划

虽然工业物联网的实施有助于大幅提升运营效率，但如果没有得到适当保护，它们也会暴露出潜在的新安全隐患。无论是高价值的资产或服务、云端关键工作负载、信息物理融合系统中的流程控制系统，还是关键的业务和运营数据，任何事物都可能成为网络攻击的突破点。

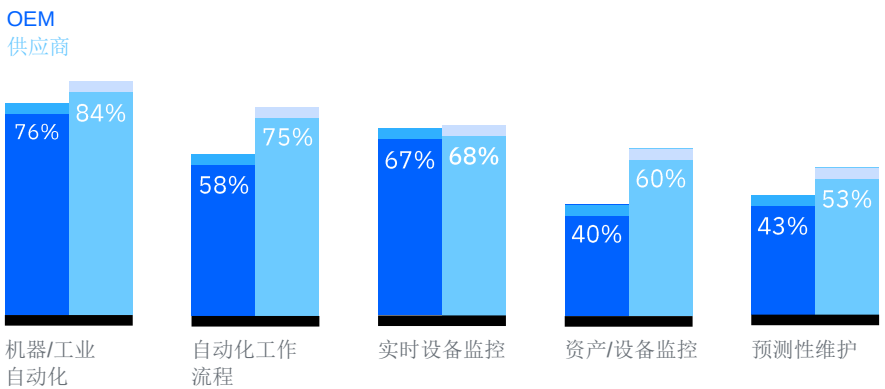
为了更好地理解工业物联网的安全风险和影响，IBV 与牛津经济研究院合作，对 700 位最高层主管进行了调研。他们代表了 18 个国家或地区能源和工业领域的 700 家在工厂中实施了 IIoT 的企业（其中 135 家是汽车企业）。

机器/工业自动化是企业应用 IIoT 技术最多的领域，有 76% 的整车厂 (OEM) 和 84% 的供应商选择了这一项（见图 2）。58% 的 OEM 和 75% 的供应商表示他们具有自动化的工作流程应用。令人惊讶的是，预测性维护方面的应用并不像预期的那么多。

汽车企业似乎认识到了网络安全风险，并在一定程度上相应调整了 IIoT 支出（见图 3）。但他们并不清楚如何将多种 IIoT 网络安全能力（技能、控制、实践和保护技术）有机结合起来，以保护目前和未来的业务免受 IIoT 威胁。

图 2

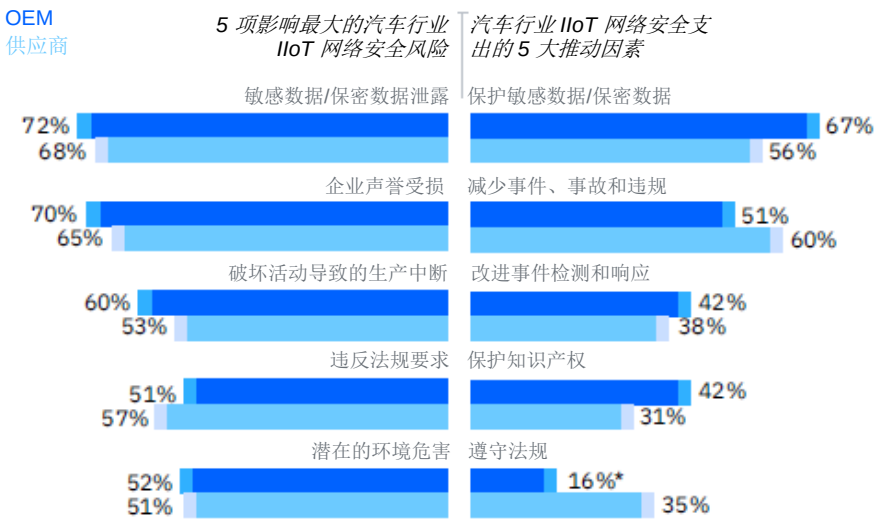
IIoT 技术在汽车制造工厂和装配线上的前五大应用



来源: IBM 商业价值研究院对标分析调研，2018 年，n=135。

图 3

IIoT 网络安全风险与支出推动因素对比



来源: IBM 商业价值研究院对标分析调研，2018 年，n=135。计数较低 (n<20) 在统计学上不具有可靠性，但与其余受访者做比较时可以视作方向性推论。

由于未能实施适当的网络安全保护措施，汽车企业将面临重大风险。特别是：

1. *敏感数据/保密数据泄露*。受访高管认为这是他们面临的最大风险。72% 的 OEM 和 68% 的供应商敏锐地意识到，客户知识产权和高级工程设计等数据的泄露可能会对企业发展产生非常不利的影响。
2. *企业声誉受损，公众信心丧失*。70% 的 OEM 和 65% 的供应商认为，安全漏洞可能会对汽车企业的形象和声誉造成巨大的负面影响。企业品牌的公信力和可信度很容易受到损害，业务和客户关系会遭到不可挽回的破坏。
3. *破坏活动导致生产中断*。60% 的 OEM 和 53% 的供应商表示，这种风险非常巨大，可能会导致物理设备损坏、零部件报废或车辆产生缺陷。网络攻击者可能会入侵企业的工业系统并操纵网络基础设施（见插图：“对工业控制系统的攻击 — 简图”）。他们会修改机器软件程序或监视控制和数据采集系统 (SCADA)。
4. *违反法规要求*。2018 年 5 月生效的《通用数据保护条例》(GDPR) 和类似法律增加了不合规的风险。51% 的 OEM 和 57% 的供应商表示，他们高度关注不合规的潜在影响以及由此可能导致的巨额罚款。

对工业控制系统的攻击 (ICS) 简图 [2]

5. *潜在的环境危害。*52% 的 OEM 和 51% 的供应商高度关注当违反控制措施，有害物质被释放到环境中的情形。

从支出的角度来看，保护敏感数据是最重要的任务，67% 的 OEM 和 56% 的供应商将其列为 IIoT 网络安全预算的主要推动因素，超过 50%