IBM

首席视野
科技启迪商业变革

让汽车企业的物联网技术扬长避短，这些办法切实可行

IBM 季刊 2019 001

虽然工业物联网的实施有助于大幅提升运营效率，但如果没有加以有效防护，工业物联网也会暴露新的潜在安全隐患。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。

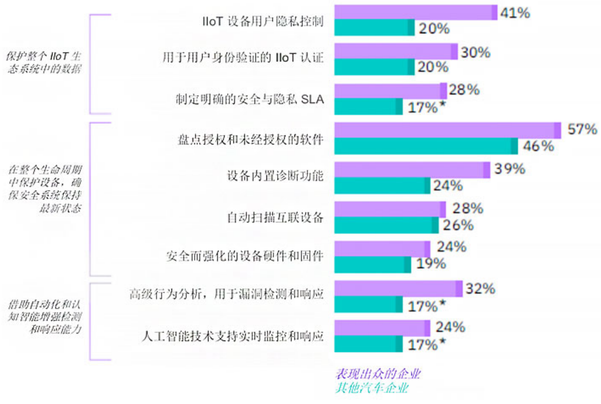
认清 5大潜在风险

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工业物联网的支出。但他们并不清楚如何将多种物联网安全能力（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工业物联网威胁。由于未能实施适当的网络安全保护措施，汽车企业将面临以下重大风险：

- 敏感/保密数据泄露威胁企业发展
- 企业声誉受损致使公众信心丧失
- 网络安全破坏活动导致生产中断
- 违反相关法规要求并遭巨额罚款
- 网络隐患会对环境造成潜在危害

采取 9大实践措施

那些积极部署工业物联网技术并认清了网络安全隐患的企业，在保护工业物联网环境方面一直处于领先地位。他们在处理以上 5大风险方面主要采取以下 9大措施：



IBM 予您更多思考：

您的工业物联网安全计划如何解决风险管理与合规问题？
您如何将工业物联网安全策略整合到业务和运营流程中？
表现出众的汽车制造商部署了那些独具特色的安全实践？

下载完整报告，寻找智慧答案

《汽车行业工业物联网—实施迅速，保护滞后》

IBM 全球领先科技实践分享，启迪商业领袖变革，尽在首席视野。

订阅获取全部期刊

进入官网探寻更多

分享您的观点或需求，IBM企业咨询顾问：

400-810-1818 转 2396 工作时间

或关注微信，
及时了解更多要闻及全球实践