



对标洞察

工业物联网 安全之交通 运输行业

降低风险，建立弹性

IBM 商业价值研究院



IBM 如何提供帮助

如果不实施充分的保护，就将用于监测和控制物理环境的系统冒然连接到互联网，不但会带来风险，而且代价可能十分沉重。如果基于工业物联网 (IIoT) 的交通运输运营系统被成功入侵，很可能带来灾难性的后果。但也不必过分担心，许多风险都可以避免或缓解。**IBM** 可以帮助交通运输行业高管轻松应对愈发频繁的网络攻击。我们将认知方法应用于安全领域，帮助保护关键基础设施资产，采用新型服务为平台和生态系统提供支持。我们的全球行业和安全专家具备深厚的专业技能，完全有能力保护您的资产和流程，同时提升产品和服务的质量。**IBM** 应用认知方法，帮助降低安全风险。如欲了解更多信息，请访问 ibm.com/industries/travel-transportation。

扫码关注 IBM 商业价值研究院



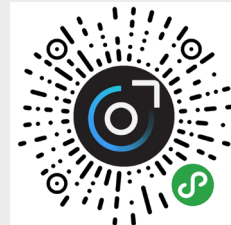
官网



微博



微信



微信小程序

作者：Eric Maass、Gerald Parham、Julian Meyrick、Keith Dierkx、Lisa-Giane Fisher 和 Steve Peterson

要点

如果没有有效的安全措施，工业物联网可能让企业付出惨重代价

许多交通运输服务提供商依靠 IIoT 解决方案来管理运营，但将近 1/3 的网络安全事故都与 IIoT 有关。如果没有充分的保护措施，交通运输运营系统就很容易受到网络攻击，很可能在多个行业引发灾难性后果。

传统系统中未打补丁的漏洞存在重大风险隐患

许多工业控制系统 (ICS) 依托传统系统支持交通运输运营，而部分传统系统存在未打补丁的严重软件漏洞。这些系统往往依靠 IIoT 设备执行路线确定、定位、跟踪和导航等操作，以及与公共应用进行互动。

运用十大控制措施和实践，增强工业物联网的弹性

我们的研究发现，一些特定的安全控制措施和基于 AI 的实践可帮助企业调整预防、检测和响应能力，更有效地做好准备，快速应对与 IIoT 相关的网络攻击，缓解攻击影响并快速从中恢复。

边缘技术有助于推动交通运输运营转型，但也会带来风险

交通运输行业地位独特，是联结企业与消费者的纽带。但交通运输提供商严重依赖于第三方，而许多行业也完全仰仗交通运输提供商才能实现持续运营以及商品和服务的交付。交通运输供应链覆盖全球，高度整合，薄弱环节众多，因此成为恶意攻击者的理想目标。

IIoT 解决方案有望颠覆交通运输行业的运营模式；特别是在管理遍布全球、日益互联和无处不在的车队、船队或机队资产方面。但这也带来了新的运营挑战 — 成为网络攻击的新目标。设想一下，无人驾驶的半挂货车独自行驶在公路上，这种场景既令人兴奋也让人害怕。随着越来越多互联互通、自主运行的智慧设备投入生产环境，交通运输企业需重新审视自身的安全运营状况。

由于该行业越来越依靠 IIoT 平台和数据服务来发掘洞察和实现自动化，因此未经授权访问专有数据和关键系统的可能性与日俱增，导致实体和数字资产面临重大风险。随着互联服务和生态系统逐渐成为关键基础设施网络不可或缺的组成部分，风险范围不断扩大，覆盖整个价值链（请参阅：“洞察：旅游行业与交通运输行业共享关键基础设施”）。

无论是以牟利为目的的网络犯罪分子，还是带有政治动机的国家或地区，一旦成功入侵交通运输行业的任一环节，都将造成十分危险的后果。交通运输中断的潜在公共安全影响和严重经济后果尤为突出。



79%

的交通运输行业主管表示，DDoS 是与 IIoT 相关的最严重威胁



59%

在我们的调研中，59% 在安全方面表现出众的企业调整了事故响应计划，以有效修复受到攻击的 IIoT 组件；相比之下，仅有 34% 的其他企业这样做



2倍

这些表现出众的企业能够迅速检测和应对与 IIoT 相关的事故和安全违规情况并从中恢复，速度至少比其他企业快 2 倍

主要的 IIoT 网络安全指标表明，一些企业的网络弹性明显优于其他企业。他们不仅能够更好地保护企业抵御和 IIoT 相关的攻击，更善于检测和及时应对安全事件并从中恢复。

我们经过深入研究和分析，最终确定了十项有助于实现这种高水平网络弹性的高效控制措施和实践。这些控制措施和实践基于互联网安全中心 (CIS) 的关键安全控制措施以及 IBM IoT 安全研究机构的 AI 驱动的实践，我们将在本报告中详细说明。¹

另外，我们还提出建议：交通运输企业如何采用三步法推行高效控制措施和实践，帮助改善 IIoT 网络安全态势，建立弹性？

1. 建立牢固的 IIoT 防御基础。
2. 调整 IIoT 事故响应和管理机制。
3. 大规模实现 IIoT 安全自动化。

随着对第三方的依赖性越来越强，安全成为保障正常运营和弹性的重要环节。

交通运输行业的 IIoT 技术：机遇与挑战并存

“订单到收款”流程、库存管理、订单履行和物流服务构成了交通运输提供商的业务核心。许多提供商成功应用智能化自适应技术，解决了困扰行业数十年的传统问题，比如路线优化问题。

为了更深入地了解最新行业动态，IBM 商业价值研究院 (IBV) 与牛津经济研究院合作开展了一项调研。我们的调研深入分析了以下几个问题：交通运输服务提供商如何应用 IIoT 技术？他们对相关网络安全风险的认识程度如何？他们的风险缓解能力的成熟度和有效性如何？（请参阅第 17 页的“调研方法”。）

我们采访了许多负责企业 IIoT 部署和环境的信息技术 (IT) 和运营技术 (OT) 高管。受访者来自全球 11 个地区的 300 家企业，其中 225 位受访者从事交通运输行业。

我们通过分析，确定了一组“在安全方面表现出众的企业”，其安全关键绩效指标 (KPI) 明显优于其他企业。此外，这组受访者对自己的漏洞管理能力也更有信心，确信能够防范各类最新威胁（请参阅：“洞察：在安全方面表现出众的企业数量”）。

洞察：旅游行业与交通运输行业共享关键基础设施

旅游行业与交通运输行业提供商有着很多相似之处 — 最显著的共同点在于，他们的关键基础设施具有相同的支柱。此外，他们还拥有一组相同的安全用例：

1. 身份。识别乘客、客户、员工和合作伙伴的身份。
2. 安全。不仅需要安全访问设备和设施，还有数字软件和数字存储。
3. 供应链完整性。披露商品和服务来源，据此建立信任。
4. 可视性和分析。监控车队、船队或机队资产，保持网络弹性，了解各种风险对业务运营上游和下游的影响。

对于交通运输提供商而言，关注点应当放在供应链完整性以及增强“从生产到履行”流程的可视性、责任制和效率。而旅游行业则应优先考虑安全性和消费者体验。尽管用例一再表明旅游行业与交通运输行业提供商采用相同的安全架构，但他们所面临的风险却截然不同：旅游行业以消费者为中心 (B2C)，而交通运输行业则以企业为中心 (B2B)。

交通运输提供商的关注重点是管理复杂供应链及多个第三方产品和服务供应商，他们所处的监管环境通常十分复杂，而且因行业和国家 / 地区而异。各参与方之间频繁进行沟通和交换数据，这是日常业务运营的重要一环。

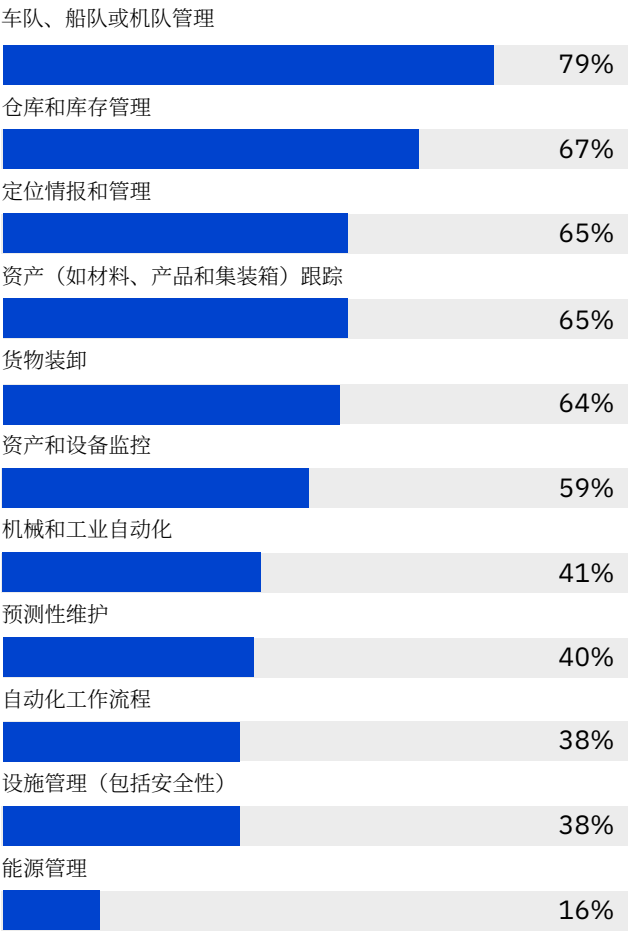
风险存在共通之处，凡危及交付和履行能力的威胁，都可能对业务成果产生不可估量的影响。尽管消费者数据极少面临危险，但宝贵商业机密和知识产权却频繁陷入危机。

很明显，安全战略应表明企业如何从辨别威胁、控制影响及实施补救三个层面应对风险。由于企业对第三方及合作伙伴的依赖性越来越强，因此安全成为保障正常运营和弹性的重要环节。在依托数字渠道推动运营现代化的过程中，安全治理是成功的重要保证。

调研结果证实，IIoT 技术得到迅速采用。车（船机）队、仓库、库存和定位管理是受支持的主要用例（见图 1）。

图 1

IIoT 技术在交通运输运营中的应用



来源：IBM 商业价值研究院对标调研，2019 年。
问：贵企业如何在运营中应用 IIoT 技术？选择所有适用项。

洞察：在安全方面表现出众的企业数量

在 300 家来自于旅游和交通运输行业的受访企业中，有 59 家企业在安全方面表现出众，其中有 36 家从事交通运输行业。我们根据以下三项指标进行评选，平均成绩排名前 20% 的企业视为表现出众的企业：

1. IIoT 网络安全在网络安全预算中所占的百分比。
2. 安全控制措施修复的已知 IIoT 漏洞的百分比。
3. 应对 IIoT 网络安全事故并恢复正常运营的周期时间。

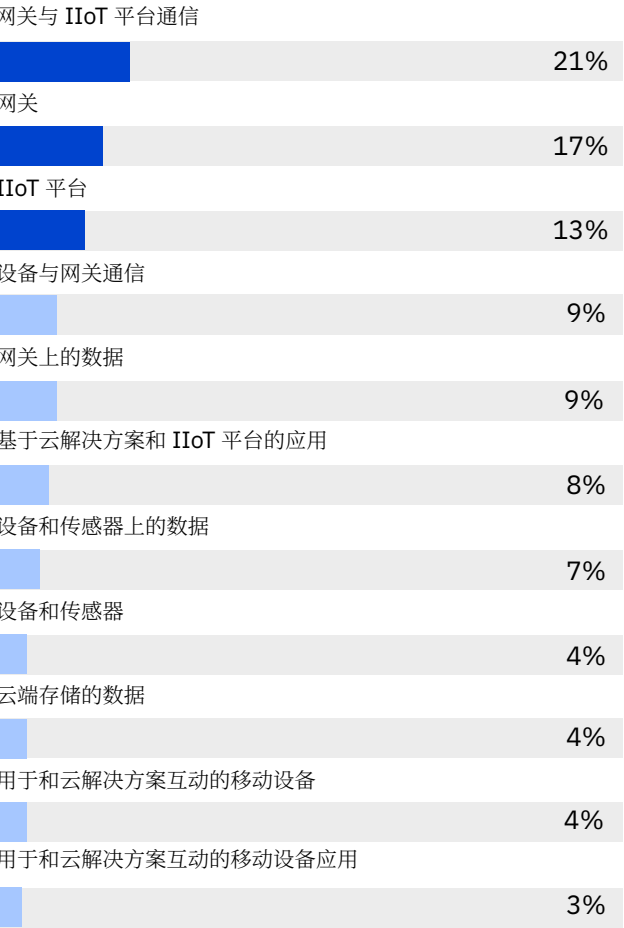
出于本次调研的目的，“在安全方面表现出众的企业”是指所有者 59 家企业，包括 36 家交通运输企业。“所有其他企业”则指另外 241 家受访旅游企业和交通运输企业。

交通运输行业主管对与 IIoT 相关的安全漏洞可能引发的灾难性后果表示担忧。

但是，受访高管普遍对运营网络、企业网络和 IIoT 网络中信息流动面临的安全隐患表示担忧。他们指出，网关以及与网关相关的连接是最薄弱的 IIoT 组件（见图 2）。

图 2

交通运输行业 IIoT 部署中最薄弱的环节



来源：IBM 商业价值研究院对标调研，2019 年。
问：对于贵企业部署的 IIoT 解决方案，哪一部分最容易受到攻击？请选择一项。

交通运输企业认识到，将用于监控物理环境的系统连接到公共网络（如互联网）可能会带来风险（见图 3）。然而，仅有 16% 的企业对相关风险开展了全面评估，制定了正式的 IIoT 网络安全计划，建立、管理和更新了消除风险所需的工具、流程和技能。

我们请受访者对各种与 IIoT 相关的网络安全风险进行评估，根据发生可能性和潜在影响给出评分。以下章节将深入探讨交通运输行业高管最担心的一些问题：

企业声誉受损和公众信心丧失

超过 2/3 的高管对这项风险的评分是“高”或者“非常高”。除可能导致运营中断及暴露敏感数据以外，一旦犯罪分子在交通运输行业成功发动与 IIoT 相关的网络攻击，还可能造成人员伤亡。这些后果很可能对企业形象和声誉造成灾难性的负面影响。不但品牌信用和信誉受损，业务和客户关系也可能遭受不可挽回的损失。

敏感数据泄露

21% 的高管敏锐地意识到，因数据泄露直接导致的损失可能十分严重，因此他们将数据泄露评为风险“非常高”。据估算，自 2018 年 1 月以来，交通运输行业泄露或被窃的记录超过 5.66 亿条（包括未加密的护照号码、客户付款详细信息及其他数据）。估计这些企业遭受的损失高达 600 亿美元。²

危害个人安全

40% 的受访交通运输行业高管将危害个人安全及其对企业产生影响的风险评为“高”或“非常高”。哪怕交通信号灯计时仅仅调整几秒，也可能造成人身伤亡。恶意攻击者篡改机械或电气设备（如铁路信号控制装置）也可能导致类似的后果。例如，波兰罗兹市一名 14 岁少年改装电视遥控器，通过它来变更铁轨道岔。结果导致四节车脱轨，12 人因此受伤。³

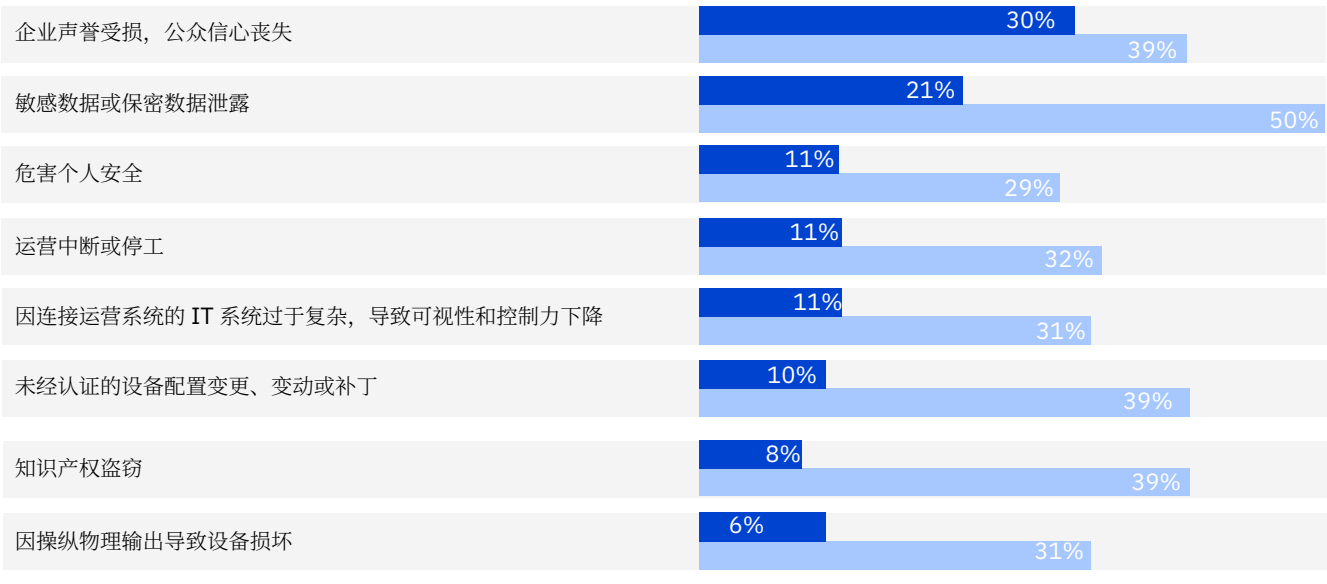
运营中断或停工

2017 年 6 月，一家全球性航运公司遭到勒索软件攻击，这是交通运输行业运营中断所产生的连锁反应的典型例子。此次攻击导致全球近 80 个港口和码头停摆或发生严重延误。此次中断不仅波及海港和集装箱货轮，发往内陆设施的卡车也被迫滞留港口，等待系统恢复上线，以便处理、接收或运送货物。此次中断大大延长了产品分销时间。该航运公司不得不重建大部分 IT 基础架构，预计损失高达 3 亿美元。⁴

因连接运营系统的 IT 系统过于复杂，导致可视性和控制力下降

IIoT 解决方案广泛覆盖 IT、OT 和消费者技术。这些系统通常由专业领域各异的不同团队单独管理。因此，针对网络攻击的防御变得极其困难，IIoT 相关事故和入侵的检测面临重大挑战。

图 3
评分最高的 IIoT 网络安全风险



预览已结束，完整报告链接和二维码如下：

https://www.yunbaogao.cn/report/index/report?reportId=1_38382

