对标洞察

–

工业物联网安全之旅游行业

保护旅游运营安全

IBM 商业价值研究院

IBM

IBM 如何提供帮助

如果您将物理环境监视和控制系统连接到互联网，但却不对其进行充分的安全保护，您将会面临风险，而且可能会产生巨额成本。针对基于物联网的旅游服务运营开展的网络攻击，一旦成功就可能会带来灾难性的后果。不过，许多此类风险实际上可以得到解决或缓解。IBM 可帮助旅游行业高管管理不断增加的攻击面。我们将认知方法引入到了安全学科之中，帮助企业保护关键基础架构资产并为其提供用以支持多种平台和生态系统的新服务。我们广泛的全球行业和安全专家可在确保安全质量的同时助力保护资产和流程的安全。IBM 采用认知方法帮助客户降低安全风险。有关更多信息，敬请访问：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：Lisa-Giane Fisher、Greg Land、Eric Maass、Julian Meyrick、Gerald Parham 和 Steve Peterson

要点

IIoT 的优势伴随着高成本

许多旅游服务提供商采用工业物联网 (IIoT) 解决方案来管理复杂的运营，但在旅游公司中，仍有三分之一的网络安全事件与 IIoT 有关。如果不采取充分的保护措施，旅游运营就很容易遭受网络攻击，造成灾难性的后果。

遗留系统中未修复的漏洞是一个巨大风险

许多旅游公司依赖于旧的工业控制系统，而其中一些系统存在着严重的软件漏洞。由于这些系统难以更新，因此存在固有的安全隐患，但旅游公司仍旧会将 IIoT 设备接入到这些系统中，以供运营应用使用，包括旅客所用的一些应用。

十种控制措施与实践有助于改善网络弹性

我们的研究揭示了一些特定的安全控制措施和 AI 驱动型实践，这些措施和实践可帮助公司调整其预防、检测和响应功能，更好地在如何快速响应、缓解 IIoT 相关网络攻击并从中恢复方面做好自身定位。

—

虽然由于 COVID-19 危机的出现导致全球游客及旅游服务人员的数量有所减少，但针对航空领域的威胁活动却依然如故。旧金山国际机场披露的、发生在 2020 年 3 月的一次数据泄露便是其中一个示例。据报道，该攻击是由俄罗斯的国家赞助黑客组织 Dragonfly 实施的。[1] 该组织通常以关键基础架构领域的组织为攻击目标，目的是从事侦察攻击、内网漫游和网络间谍等活动。[2]

如何维持并保护关键基础架构，例如旅游服务和运输公司所共享的基础架构，一直都是挑战。与 COVID-19 相关的担忧给公司的安全性、灵活性和连续性计划带来了前所未有的压力。旅游行业肯定会从 COVID-19 疫情中恢复过来，但却永远无法免疫网络攻击。若要克服这一全球性挑战，就需要适应性，以及创新的安全和风险管理实践。

对于恶意攻击者而言，旅游业是一个极具吸引力的目标。该行业为支持运营而对信息技术 (IT) 产生的依赖、与第三方供应商集成的普遍需求，加上旅游服务供应链的全球范围和一体化集成，这些都意味着一个广泛、多元化的攻击面。

随着该行业越来越依赖支持自动化的 IIoT 平台和数据服务，一些新的漏洞已开始显现。对这些平台和服务的使用增加了非授权访问专有数据和关键系统，进而破坏物理资产的可能性。无论是由网络犯罪分子出于经济动机而执行，还是由国家出于政治动机而执行，针对旅游行业的成功攻击都可能导致严重的连锁反应，影响旅游服务总体需求，进而影响整个全球经济。

随着攻击向量的成倍增加，以及关键漏洞在短期内即被加以利用，受攻击的风险呈指数级增长，通常都是快速发生且没有先例可循。2001 年 9 月 11 日美国遭受的攻击之所以如此严重，其中一个因素便是攻击者具备躲避多种安全协议的能力，同时又编排了多个攻击向量。此次攻击仅财产损失就近 1,000 亿美元，经济损失总额估计高达 2 万亿美元。[3]

68%

的旅游企业高管表示 DDoS 攻击是他们所面临的最大 IIoT 相关威胁。

59%

的安全领导者已经调整了他们的事件响应计划，以处理针对已受损 IIoT 组件的行动方案，相比其他公司，此占比只有 34%。

2 倍

安全领导者检测、响应 IIoT 相关事件及破坏并从中恢复的速度至少比其他公司快 2 倍。

随着生态系统的增多，公司变得更加易受攻击。此外，整个行业的持续创新使旅游服务生态系统有可能继续扩展和演变。为了面向未来做好准备，旅游服务组织应着重于在当下提升其网络弹性。

我们的研究和分析揭示了十种安全控制措施和 AI 驱动型实践，它们可以对 IIoT 网络安全性能产生积极影响。它们结合了来自 IBM IoT 安全研究部门的互联网安全中心 (CIS) 关键安全控制措施和 AI 驱动型实践。[6] 在本报告中，我们就旅游服务公司如何将其实施为双阶段方法的一部分提供了一些建议，旨在帮助他们改善其 IIoT 网络安全态势和弹性：

第 1 阶段：定义和实施 IIoT 网络安全战略和计划，然后专注于高效的保护和预防控制措施和实践，以此方式建立强大的防御基础。

第 2 阶段：运用高效的检测、响应和恢复控制措施，并运用构建和测试自动响应功能的实践，以此方式规模化实现旅游服务安全自动化。

对于恶意攻击者而言，旅游业是一个极具吸引力的目标。

IIoT 技术对于旅游业而言：喜忧参半

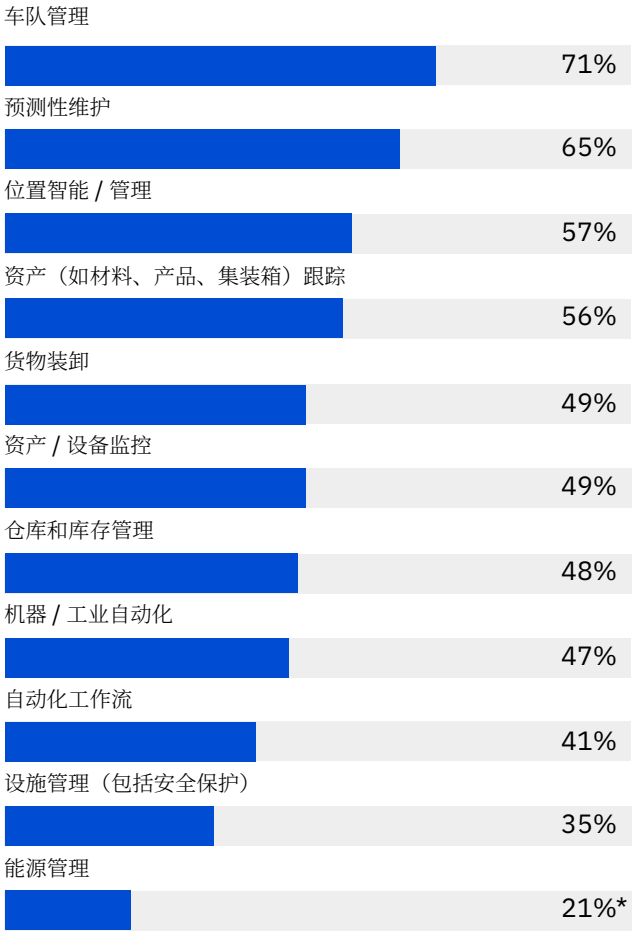
旅游公司已开始在整个运营过程中广泛采用 IIoT 技术。这方面的示例不胜枚举，几乎涵盖了航空公司和地面运输运营的各个方面，以及许多旅游服务机构、旅游运营商和相关旅游服务中介的销售、营销和客户服务等各个方面。这些旅游服务组织对相关的网络安全风险以及可用于缓解这些风险的功能的成熟度和有效性究竟有多少程度的了解，目前尚不清楚。

为了更好地了解某些组织比其他组织更安全、更具网络弹性的原因，IBM 商业价值研究院 (IBV) 与牛津经济研究院合作，对来自 11 个地区的 300 个旅游服务和运输组织的 IT 和运营技术 (OT) 领导者进行了调研，其中有 75 家是旅游服务组织。受访的领导者都是在其组织中负责 IIoT 部署和环境的安全性保障（见“调研方法”部分）。

我们的调研结果证实了 IIoT 技术正在各种功能领域中被迅速采用。许多公司已开始在其供应链和物流流程中运用这些技术 - 用于车队管理、预测性维护和位置管理（见图 1）。

图 1

旅游服务运营中如何运用 IIoT 技术



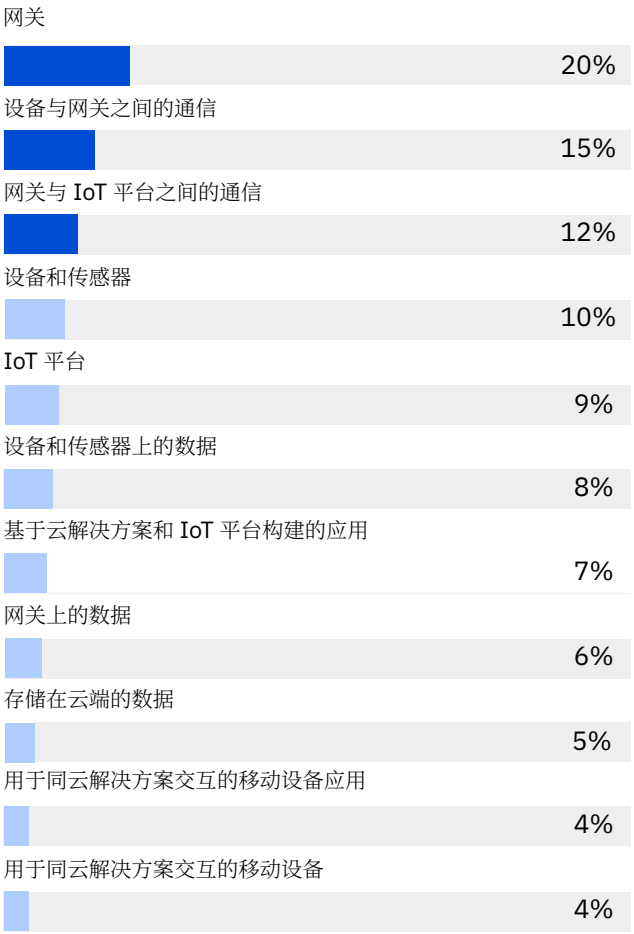
来源：IBM 商业价值研究院 2019 年对标调研。
** 标星数据表示样本数量较少 (n<20)，这种数据从统计学上来讲是不可靠的，但与其余受访数据相比，可以将它们视为指向性数据。*
问：贵组织如何在运营中运用 IoT 技术？请选择所有的适用项。

许多旅游服务公司都在继续部署 IIoT 技术，但并未以相同的速度对其进行安全保护。

不过，企业高管普遍对在运营、公司 IT 和 IIoT 网络之间流动的信息的安全性感到担忧。据受访旅游服务公司称，网关及网关相关连接几乎占了他们最易受攻击 IIoT 组件的“半壁江山”（见图 2）。

图 2

旅游服务 IIoT 部署中最易受攻击的组件



来源：IBM 商业价值研究院 2019 年对标调研。问：贵组织已部署的 IoT 解决方案中最易受攻击的组件是什么？请选择一项。

将物理环境监视和控制系统连接到互联网等公共网络可能会带来风险，尤其是当这些系统未根据更广泛的安全性管理策略进行安全保护时。潜在风险包括数据泄露对个人造成的影响，以及消费者信任度下降等。

尽管旅游服务公司可能已经意识到了这些风险，但许多公司仍旧继续以高于安全保护速度的步伐部署 IIoT 技术。由此产生的配置和控制缺口就会被攻击者所利用。几乎有三分之二的受访高管表示，他们至少具备提供支持 IIoT 的新产品和服务的能力，但只有一半的受访高管表示，他们能够以安全的方式提供此类产品和服务。这些调研结果再次印证了运营基础架构安全保护方面存在差距所带来的风险。

我们要求受访者对各种网络安全风险进行评估，并根据各个风险的可能性和潜在影响打分（见图 3）。以下各节将探讨旅游企业高管最关注的一些风险：

旅客数据暴露

旅游服务高管将旅客数据暴露视为其所面临的最大两个 IIoT 网络安全风险之一。除了造成公关责任外，数据泄露也可能会带来重大的财务责任。

举例来说，2019 年，一家大型航空公司发生数据泄露，违反了《一般数据保护条例》(GDPR)，并导致 500,000 名客户受到影响，被罚款 2.3 亿美元。由于安全控制不力，各种个人信息遭到攻击，包括登录信息、支付卡信息、旅游服务预订详细信息以及姓名和地址信息等。该笔罚款占该航空公司年总收入的 1.5%，是英国信息专员办公室因数据泄露而开出的最高罚款单。[7]

损害旅游品牌声誉和公众信心

除了潜在的数据泄露和运营中断外，针对旅游行业的网络攻击一旦成功还可能会导致人身伤害和死亡。对公司声誉的负面影响可能是不可逆转的影响。

不仅品牌在现有客户中的信誉会受到损害，潜在业务和客户关系也会受到不可挽回的损害。这也无怪乎受访者将对品牌和公众信赖的影响视为其所面临的两个最大 IIoT 相关风险之一。

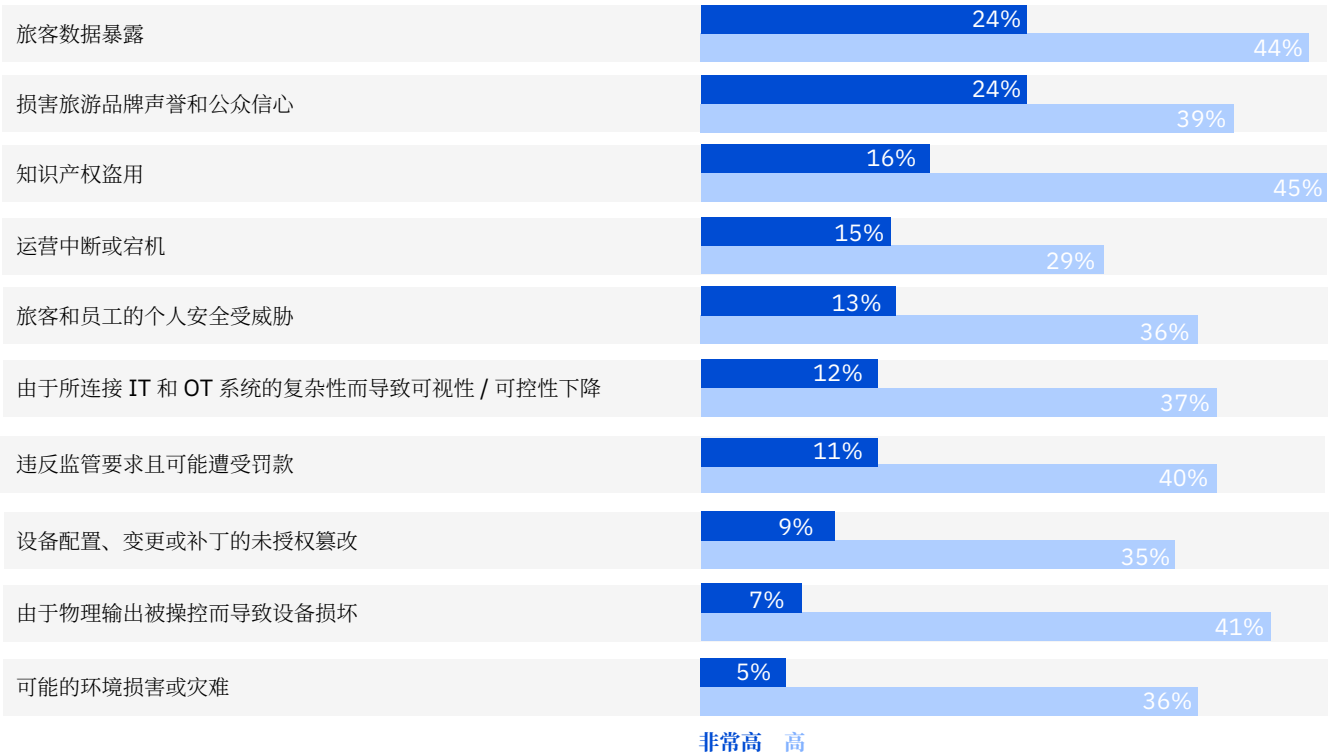
知识产权 (IP) 盗用

许多旅游公司已投入了大量的资金来建立品牌资产和专有知识产权，以实现自身优势。商标、地理标志（认证标志、集体标志或特殊制度）、工业品外观设计，以及专利、版权和商业机密等其他形式的 IP 都是企业竞争优势的来源。旅游企业高管们已经认识到 IP 盗用可能会影响他们的未来增长，而且将其视为第三大 IIoT 安全风险。

运营中断或宕机

15% 的旅游企业高管将运营中断视为极高的风险。2016 年，旧金山的轻轨系统遭受了恶意软件攻击。黑客强占了代理机构电子邮件和后台计算机系统，要求使用比特币来交换他们捕获的代理机构数据。[8]

图 3
得分最高的 IIoT 网络安全风险



来源：IBM 商业价值研究院 2019 年对标调研。问：下列各种 IoT 网络安全风险在贵组织中发生的概率是多少？如果发生的话，将会对贵组织造成什么样的影响？按 1 到 5 分对每种风险的发生概率和影响进行打分，其中：1 分 = 非常低；2 分 = 低；3 分 = 中等；4 分 = 高；5 分 = 非常高。

亚特兰大市交通部门也曾遭受过一次勒索软件攻击，该攻击导致该部门服务中断了数个月，恢复成本高达 260 万美元。[9] 对于物流运营商而言，整个卡车车队也可能会因病毒攻击路线规划系统而陷于瘫痪。

旅客和员工的个人安全受威胁

13% 的旅游企业高管表示，旅游者和员工受到安全威胁的风险也非常高。即使交通信号灯的时间进行几秒钟的更改，也可能会导致人身伤害或死亡。对机械或电气设备（如铁路信号控制设备）的篡改，也可能会造成类似的结果。

举例来说，波兰罗兹市的一名 14 岁波兰人改装了一个电视遥控器，并用它更改了铁路轨道点。结果造成四辆列车出轨，导致 12 人受伤。[10]

改善 IIoT 安全性的双阶段方法

利用我们的调研数据，我们基于受访者的 IIoT 网络安全预算、安全控制措施所解决的已知漏洞以及响应和恢复时间，确定了我们称之为“安全领导者”的一组公司（见侧边栏“洞察：基于数据列出的安全领导者”）。我们发现安全领导者更有可能全面评估 IIoT 网络安全风险，而且非常了解缓解风险所需的网络安全功能。

这些公司在安全 KPI 方面的表现更好，并且在自己组织的漏洞管理功能可以保护他们免受最新威胁的影响方面更有信心。他们也更有可能将安全控制措施视为高效的安全推动和保护因素。[11] 不过，真正使安全领导者与众不同的在于他们的网络弹性：他们能够以至少两倍于其他公司的速度检测和响应 IIoT 相关事件并从中恢复。

洞察：基于数据列出的安全领导者

安全领导者中既有旅游服务公司，也有运输公司。在受访的 300 家公司中，有 59 家属于安全领导者，其中有 23 家来自旅游行业。这些安全领导者在以下三个指标方面被评为表现最佳的前 20%：

1. IIoT 网络安全所代表的网络安全预算所占百分比。
2. 安全控制措施解决的已知 IIoT 漏洞所占百分比。
3. 响应 IIoT 网络安全事件并从中恢复所需的周期时间。

在本次调研中，“安全领导者”一词是指符合条件的所有 59 家公司，其中包括 23 家旅游服务公司；但凡是提及“所有其他公司”，则是指其他 241 家旅游服务公司和运输公司。