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

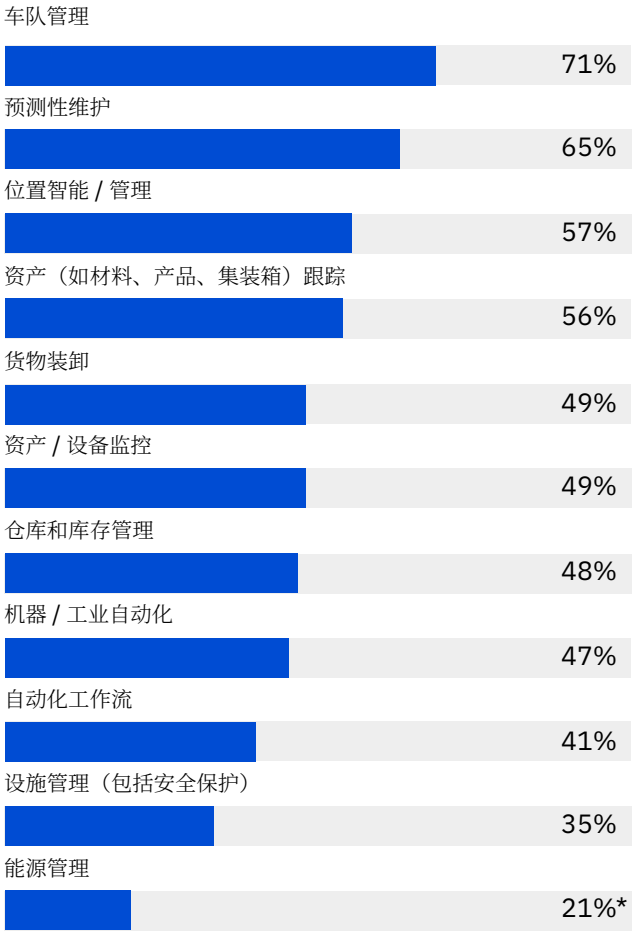
旅游公司已开始在整个运营过程中广泛采用 IIoT 技术。这方面的示例不胜枚举，几乎涵盖了航空公司和地面运输运营的各个方面，以及许多旅游服务机构、旅游运营商和相关旅游服务中介的销售、营销和客户服务等各个方面。这些旅游服务组织对相关的网络安全风险以及可用于缓解这些风险的功能的成熟度和有效性究竟有多少程度的了解，目前尚不清楚。

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



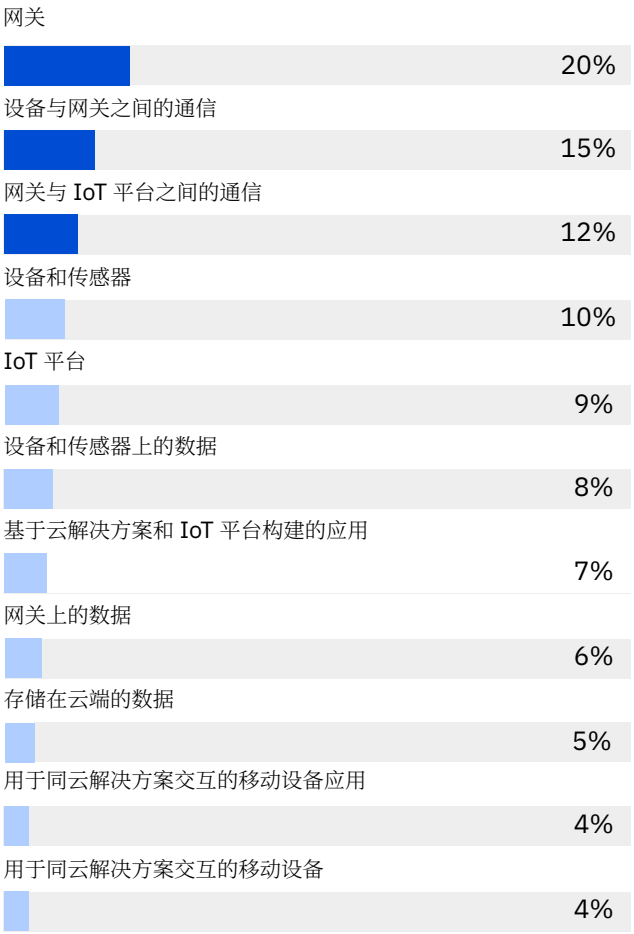
来源：IBM 商业价值研究院 2019 年对标调研。
** 标星数据表示样本数量较少 (n<20)，这种数据从统计学上来讲是不可靠的，但与其余受访数据相比，可以将它们视为指向性数据。*
问：贵组织如何在运营中运用 IoT 技术？请选择所有的适用项。

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。

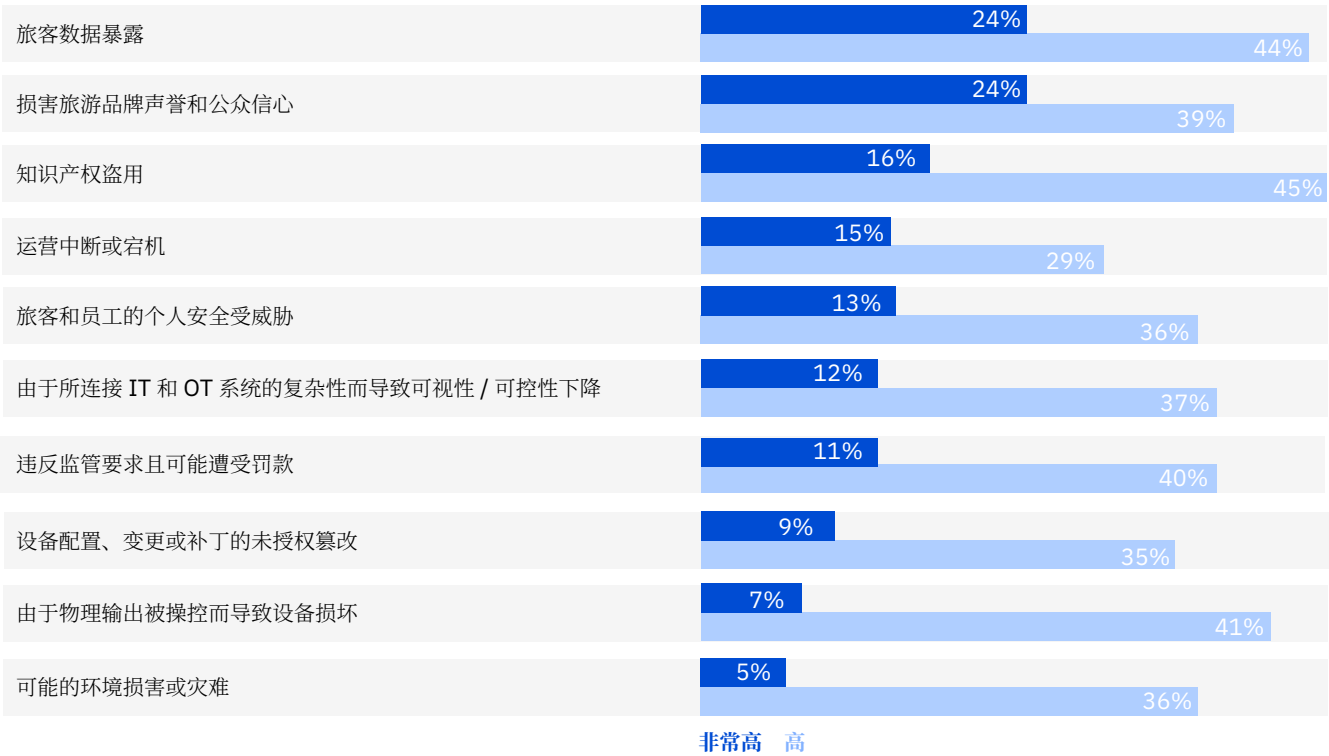
知识产权 (IP) 盗用

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。

我们建议采用双阶段的方法来改善 IIoT 网络安全态势和弹性。

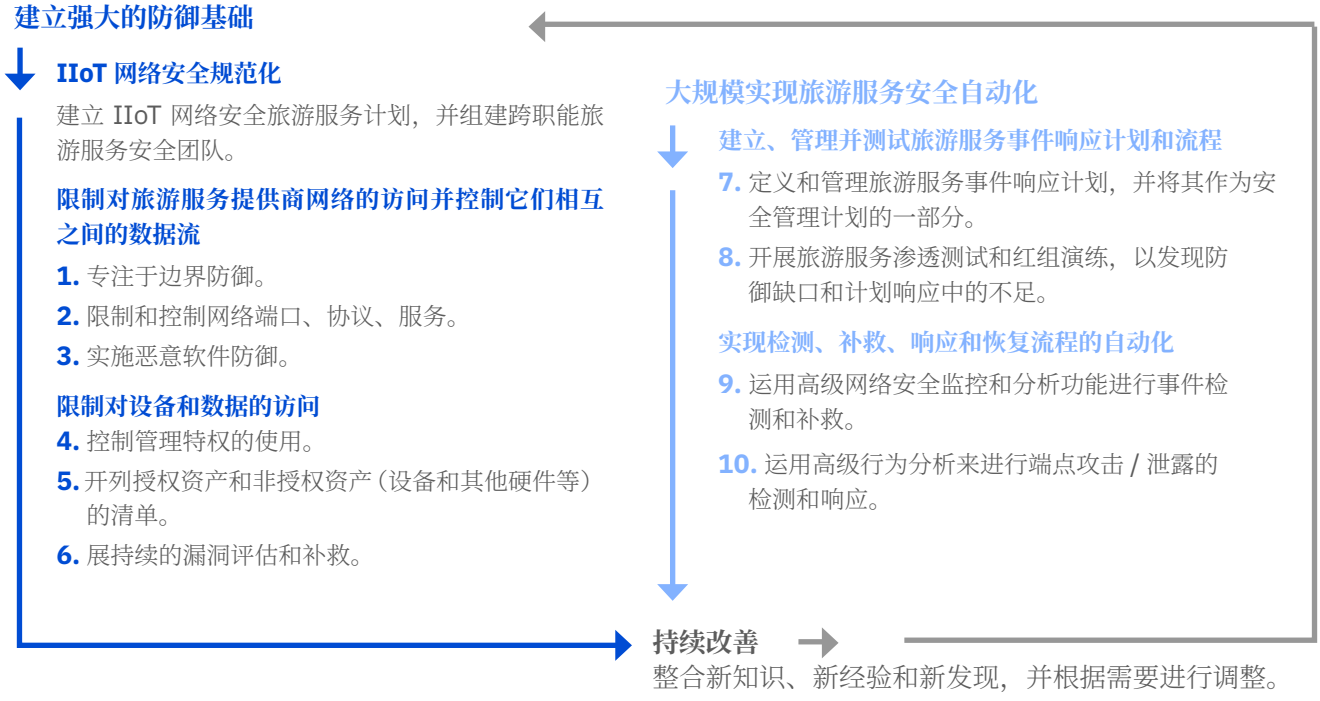
我们的研究表明，这种表现在很大程度上受互联网安全中心 (CIS) 关键安全控制措施以及许多旅游服务公司所采用的更高级的、由 AI 驱动的实践所影响。[12] 此类措施和实践共有 10 种，每一种都与保护和预防或检测、响应和恢复这几种安全功能中的某一种有关。我们建议将这些高效的控制措施和实践作为双阶段方法的一部分予以实施，以改善 IIoT 网络安全态势和弹性（见图 4）。

为 IIoT 建立强大的防御基础

第一阶段由三个指令构成。第一个指令用于促进建立 IIoT 网络安全战略和计划，该战略和计划应与组织更广泛的 IT 和 OT 风险与安全框架保持一致。第二和第三个指令用于指导高效保护和预防控制措施和实践及其相关技术的运用，以增强防御能力。

图 4

有助于改善 IIoT 网络安全态势和弹性的双阶段方法。



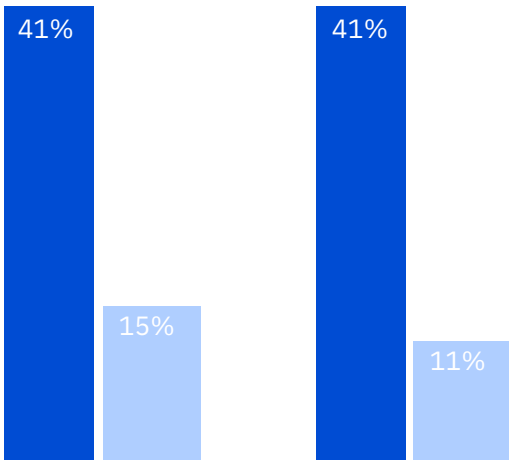
来源：IBM 商业价值研究院分析结果。

IIoT 网络安全规范化。

借助有效的 IIoT 网络安全旅游服务计划，旅游服务公司便能够定义、管理和更新所需的 IIoT 网络安全工具、流程和技能。41% 的安全领导者已经建立了此类计划，而只有 15% 的其他公司建立了此类计划（见图 5）。对于和 IIoT 相关的风险，应将其作为旅游服务组织更广泛安全风险管理框架的一部分加以解决（见侧边栏“洞察：IIoT 风险管理框架”）。首先评估风险并对其进行优先排序。然后使用跨 IT 和 OT 学科的通用风险方法，确保它们的可视性并在企业级对其进行管理。定期进行风险评估，以识别 IIoT 环境（包括所连接的 ICS）中的漏洞。记录并执行缓解计划。

图 5

IIoT 网络安全规范化



安全领导者 所有其他公司

来源：IBM 商业价值研究院 2019 年对标调研。
问：哪项描述最能体现贵组织对 IoT 网络安全的了解?
问：为减缓 IoT 网络安全风险，贵组织对以下运营方法的实施程度如何?
注：图 5-9 所示为选择了“4 = 正在实施”和“5 = 已完全实施”的公司所给出的回答。

洞察：IIoT 风险管理框架

安全和治理框架的组合（如美国国家标准和技术研究院 (NIST) 关键基础架构网络安全框架及 ISO/IEC 27000-1），可用作以下措施的基础：

– 识别关键数据、资产和安全边界。

– 识别 IIoT 系统、已连接的生产环境及人员资产中的漏洞。

– 建立并定制风险管理框架。

– 评估风险，然后制定并执行风险减缓计划。

– 确保对最紧迫的安全计划的投资并沟通这些计划的进度。

– 实现可接受的风险水平与业务目标和合规要求之间的平衡。[13]

如今，恶意软件会进行定制化，以达到影响 IIoT 设备和平台的目的。

如图所示，41% 的安全领导者已认识到，跨职能协作可以帮助旅游服务组织更清楚地了解 IIoT 系统、公司 IT 系统与运营设备之间的差异（见图 5）。通过组建由来自 IT 安全、工程、运营、控制系统等部门及安全供应商的人员组成的跨职能旅游服务安全团队，旅游服务公司便可充分利用 IT 和 OT 专业知识，对安全控制措施进行适当的优先排序，实现最佳的风险减缓。[14]

限制对旅游服务提供商网络的访问并控制它们相互之间的数据流。

IIoT 设备会生成大量数据，而这些数据会自然地流经公司和受保护程度较小的 IIoT 网络。定义角色和权限，限制对这些网络的访问以及控制流经这些网络的数据流，对于维持一致的安全态势至关重要。关于这一点，三种高效的控制措施可为您提供帮助。

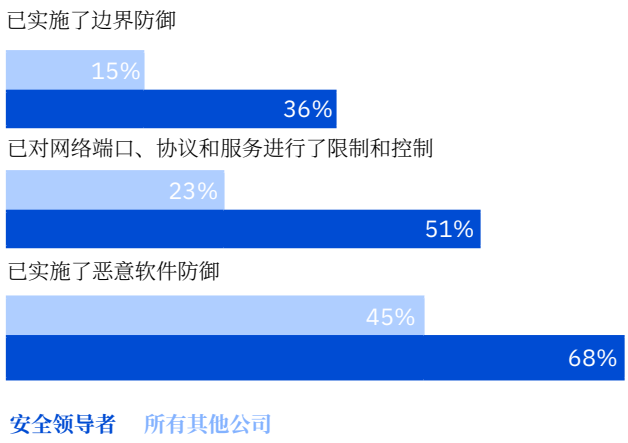
1. 专注于边界防御。我们的调研结果显示，这种控制措施对 IIoT 网络安全性能的影响最大。它针对的是检测、预防和纠正跨不同信任级别的网络之间的信息流，重点针对的是安全性遭受损害的数据。使用隔离战略使 IIoT 组件保持在其自己的区域中或在其自己的独立网络中运行的安全领导者数量，是采用此类实践的其他公司的两倍（见图 6）。[15] 这种实践有助于减轻信任度较低的 IIoT 网络会对更安全的公司 IT 网络所造成的负面影响。

2. 限制和控制网络端口、协议和服务。在本次调研中，积极定义并执行 IIoT 设备在其运营环境中可能使用的端口、协议和服务的安全领导者数量，是采用此类实践的其他公司的两倍多（见图 6）。由于某些设备可能会实施不使用公司网络的通信协议（如蓝牙），因此充分了解每种设备采用的协议（即哪些协议与组织的安全策略相符），有助于显著减小漏洞窗口。组织应测试 IIoT 设备，以评估它们对不符合预期的消息传递的敏感性。[16]

3. 实施恶意软件防御。如今，恶意软件和漏洞利用程序会进行定制化，以达到影响 IIoT 设备和平台的目的。组织应制定战略来控制整个组织中多个位置恶意代码的安装、传播和执行。同时还应持续监控 IIoT 设备信息（更新和数据）流动所经过的网关，以检测恶意软件，或将观察到的活动与已知、合法的计划中活动相关联。

图 6

限制对网络的访问并控制它们相互之间的数据流。



来源：IBM 商业价值研究院 2019 年对标调研。
问：为减缓 IoT 网络安全风险，贵组织对以下关键安全控制措施的实施程度如何？

具有关键系统访问权限的员工通常是恶意黑客的目标。

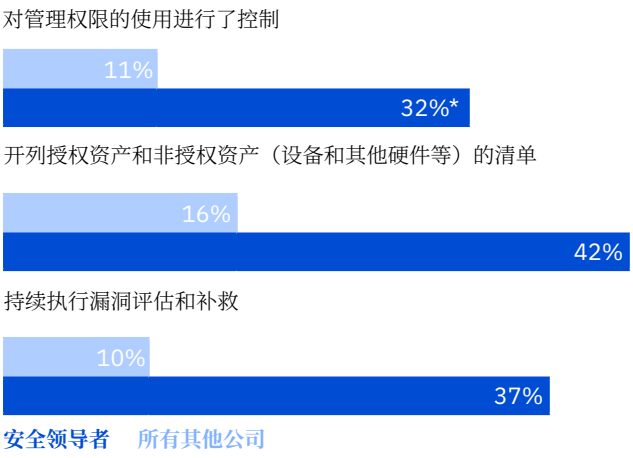
限制对设备和数据的访问。

对网络访问和数据流进行管理，只能算是进行了一半的防御。另一半的防御则是要对设备和数据（在用、动态及静态）进行的访问管理。三种高效的安全控制措施可帮助您实现这一目标。

4. 控制管理特权的使用。有权访问关键系统的员工通常会因为恶意或无意的行为给企业网络安全带来最大威胁。因为与外部的恶意黑客相比，这些员工拥有更多的信息和关键基础架构访问权限，因此经常成为网络攻击的目标。安全领导者在维持敏感数据访问的控制框架，以抵御此类攻击方面要优于其他组织（见图 7）。

图 7

限制对设备和数据的访问



来源：IBM 商业价值研究院 2019 年对标调研。
问：为减缓 IoT 网络安全风险，贵组织对以下关键安全控制措施的实施程度如何？

有效的安全程序会限制特权访问，记录有权访问敏感功能 / 数据的人员，并监控整个公司网络中所有用户的活动。对于旅游行业来说，存在着一个特殊的风险，即负责管理 IIoT 设备的技术人员使用共享帐户。在不安全地区部署 IIoT 资产也会带来另一个风险。若要在整个运营生命周期中加强控制，应考虑采用更多自适应方法，例如限制物理访问；限制管理权限；提供更具细粒度的基于角色的权限。[17]

5. 开列授权资产和非授权资产（设备和其他硬件等）的清单。28% 的旅游企业高管表示，非授权资产和设备的可视性是确保其 IIoT 部署安全的最大挑战之一。非授权 IIoT 设备和网络（即“影子 IIoT”的示例）会在组织传统安全策略的监控下运行，使其难以被检测出。

识别并分析所有 IIoT 端点，将其添加到资产清单中并对其进行监控，有助于解决这一问题。仅提供对授权设备的访问，同时阻止对已确定的非授权设备和不受管理设备的访问。

6. 开展持续的漏洞评估和补救。IIoT 设备和工业控制系统（包括监督控制和数据采集 (SCADA) 系统）中的缺陷和安全漏洞，使得旅游服务公司容易受到传播分布式拒绝服务 (DDoS) 攻击恶意软件的僵尸网络（如 Mirai、Aidra、Wifatch 和 Gafgyt）的攻击。[18] 旅游企业高管表示，在他们遭受的所有网络安全事件中，有 33% 的攻击为 DDoS 攻击。68% 的受访者将这些攻击称为与 IIoT 相关的最大威胁。

因此，组织应定期安排漏洞评估，以识别配置不正确的 IIoT 设备，以便管理员删除或重新配置这些设备。在运营环境中进行主动漏洞扫描会破坏系统的稳定性。如果自动扫描不适用的话，则应执行被动监控。

大规模实现旅游服务安全自动化

一旦建立了 IIoT 网络安全防御基础，便可在下一个阶段中基于该基础通过遵循两个指令来构建安全。这两个指令包括剩余的四个高效检测、响应和恢复控制措施和实践，它们支持自动、自适应响应功能的部署。

建立、管理并测试旅游服务事件响应计划和流程。

有助于针对事件和数据泄露做出快速、动态且有组织的响应的技术和流程至关重要。以下所述的高效组织控制措施可帮助您解决流程方面的问题：

7. 定义和管理旅游服务事件响应计划，并将其作为安全管理计划的一部分。59% 的安全领导者已经调整了他们的事件响应计划，以解决针对易受攻击 IIoT 组件的行动方案，而在其他公司中，这么做的公司占比只有 34%（见图 8）。定期对计划进行测试的 IR 团队能够进一步增强响应能力。

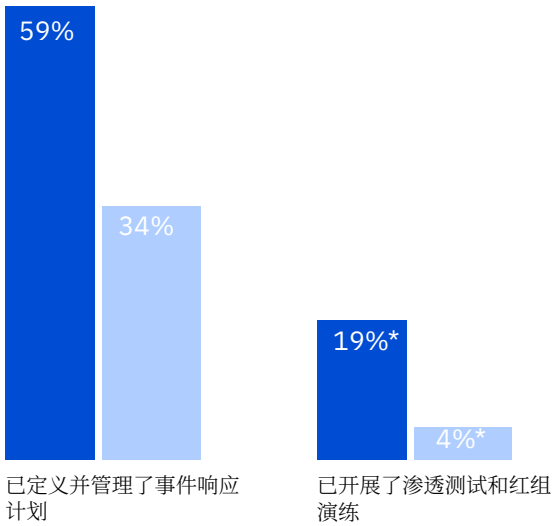
执行数据泄露模拟，以识别在发生数据泄露时要激活的流程、人员和工具。使用生态系统内部的共享资源，如拥有市场短缺专业技能的 ICS/SCADA 安全专家。公司还可以通过涵盖与任务关键型 IIoT 平台相关的业务中断和勒索要求的网络保单来降低风险敞口。然而，我们的调研结果显示，购买了网络保险的旅游服务公司屈指可数。

8. 开展旅游服务渗透测试和红组演练。此类演练有助于您更详细地了解 IR 计划的有效性。红组是一群道德黑客，他们的职责是模拟网络攻击，以便安全领导者对其 IR 计划进行压力测试，找出差距并进行相应调整。渗透测试有助于发现临时漏洞，并维持与安全策略和数据隐私法规的合规性。

我们发现，有 19% 的安全领导者正在实施此类进攻性防御策略，而在其他公司中，采用此类做法的比例只有 4%（见图 8）。在 IIoT 环境中，扫描错误可能会严重影响业务运营，因此必须加以考虑并解决。

图 8

建立、管理并测试旅游服务事件响应计划和流程



来源：IBM 商业价值研究院 2019 年对标调研。
问：为减缓 IoT 网络安全风险，贵组织对以下关键安全控制措施的实施程度如何？

实现检测、补救、响应和恢复流程的自动化

采取更好的保护和预防实践并不能保证绝对的安全。恶意攻击者会不断开发渗透系统的新方法。由于关键的网络安全技能通常都供不应求，因此必须借助自动化机制来检测和补救数据泄露。以下所述是两种可帮助组织实现这一目标的高效人工智能方法：

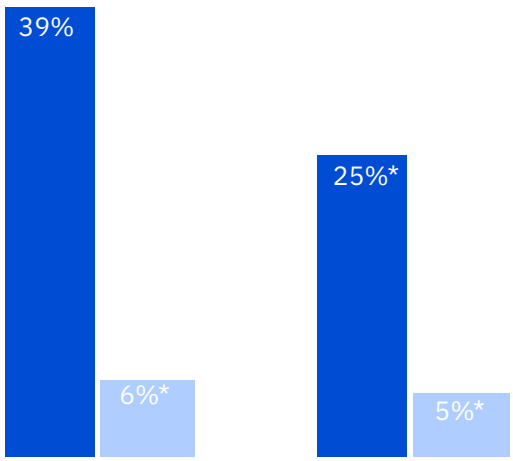
9. 运用高级网络安全监控和分析功能进行事件检测和补救。为了实时了解整个运营环境中的 IIoT 信息，39% 的安全领导者（7% 的其他公司）已建立了综合性安全遥测功能，此类功能可自动收集、集成和分析来自所有可能监控点的数据。这些数据包括系统日志、网络流、端点数据、云使用情况和用户行为数据等；借助这些数据，旅游业安全运营 (SOC) 团队便可快速了解警报的情境信息，并区分误报和真实警报。借助主动的方法，SOC 团队可以分析从内部 IIoT 数据中提取的信息以及外部来源的威胁情报数据，并运用机器学习来预测攻击者的下一步行动。

10. 对端点进行高级行为分析数据泄露检测和响应。可以在企业级别上运用支持 AI 的威胁检测，以发现异常的用户活动并对风险进行优先排序。25% 的安全领导者已部署了利用机器学习的用户行为分析功能（见图 9）。他们在借助机器学习实现自适应模型自动化成为“常态”方面也处于领先地位，这使他们能够跟踪这些正常行为签名并标记可能暗示新威胁的异常活动。

IIoT 代表了 IT 和 OT 解决方案集的融合，其中许多解决方案是在网络安全进入人们的视野之前设计的。这就增加了复杂性并引入了一系列独特的风险。借助将安全作为运营不可或缺的一部分的 IIoT 安全战略，旅游服务公司可以从这些新技术中受益，而不会给公司（或员工和旅游者的福祉）带来风险。

图 9

实现检测、补救、响应和恢复流程的自动化



来源：IBM 商业价值研究院 2019 年对标调研。问：为减缓 IoT 网络安全风险，贵组织对以下基于人工智能 (AI) 及分析的方法的实施程度如何？

您的旅游服务组织能否保护关键基础架构?

– 您如何确保 IIoT 安全实践与贵组织的企业风险管理框架保持一致?

– 您如何将安全工具和管理流程集成到贵组织的安全框架和运营流程当中?从某种程度上来说,这是否是您在整个运营生命周期中保持可视性、透明性和问责制的一种方式?

– 您如何增加隔离来优化安全性较低的 IIoT 网络的隔离?

– 您如何加强事件响应计划,使其在压力下更容易执行?

– 您如何预防威胁影响、减少业务中断并构建快速从攻击中恢复的功能?

行动指南

有助于提升网络弹性的双阶段方法

为 IIoT 建立强大的防御基础。

将 IIoT 网络安全控制措施和实践及其相关技术整合到总体 IIoT 安全战略中。然后专注于增强保护和预防功能。

IIoT 网络安全规范化。

– 建立 IIoT 网络安全旅游服务计划。

– 组建跨职能旅游服务安全团队。

限制对旅游服务提供商网络的访问并控制它们相互之间的数据流。

– 专注于边界防御。

– 限制和控制网络端口、协议和服务。

– 实施恶意软件防御。

限制对设备和数据的访问。

– 控制管理特权的使用。

– 开列授权资产和非授权资产(设备和其他硬件等)的清单。

– 开展持续的漏洞评估和补救。

一旦建立了防御基础之后,大规模实现旅游服务安全自动化。

将 IIoT 网络安全整合到旅游服务安全运营中,使您的组织能够快速有效地应对与 IIoT 相关的事件和数据泄露:

建立、管理并测试旅游服务 IIoT 事件响应计划和流程。

– 定义和管理旅游服务 IIoT 事件响应计划,并将其作为安全管理计划的一部分。

– 开展渗透测试和红组演练,以发现防御能力和计划响应中的不足。

恶意攻击者不断开发渗透系统的新方法,而且网络安全技能常常处于供应短缺的状态。大规模部署自动化的自适应响应功能:

实现检测、补救、响应和恢复流程的自动化。

– 运用高级网络安全监控和分析功能进行事件检测和补救。

– 运用高级行为分析来进行端点攻击 / 泄露的检测和响应。

关于作者

Lisa-Giane Fisher
linkedin.com/in/lisa-giane-fisher
lfisher@za.ibm.com

Lisa-Giane Fisher 目前担任 IBM 商业价值研究院在中东及非洲所开展对标调研的负责人。她负责并购和安全对标调研，还与 IBM 行业专家合作开发和维护行业流程框架。Lisa 目前居住在南非。

Greg Land
linkedin.com/in/gregland
greg.land@us.ibm.com

Greg (James) Land 目前担任 IBM 酒店与旅游相关服务细分领域的全球总监。在整个 25 年的职业生涯中，Greg 一直浸淫在旅游服务行业，曾担任过战略咨询师、顾问和高管。他曾与多家全球航空公司、旅游技术提供商和酒店企业开展过合作，在数字化转型方面积累了独到的见解。Greg 目前常驻纽约。

Eric Maass
linkedin.com/in/ezmaass/
emaass@us.ibm.com

Eric Maass 目前担任 IBM Security Services 战略与新兴技术总监，负责领导该组织产品组合（包括高级安全技术和新兴安全技术）的业务和投资战略。作为安全行业的一名资深人士，他在商业、国防和情报等领域积累了大约 20 年的公司和启动经验。Eric 曾是一家云安全初创公司的创始人兼首席技术官，该公司于 2014 年被 IBM 收购。Eric 目前居住在大纽约地区。

Julian Meyrick
linkedin.com/in/julianmeyrick
julian_meyrick@uk.ibm.com

Julian Meyrick 负责 IBM Security 的全球安全战略风险与合规和云安全实践。Julian 的工作是帮助客户针对他们所面临的网络业务风险制定安全战略。他还特别负责就网络安全对业务的潜在影响向董事会提供建议。Julian 目前居住在伦敦。

Gerald Parham
linkedin.com/in/gerryparham/
gparham@us.ibm.com

Gerald Parham 目前担任 IBM 商业价值研究院全球安全与 CIO 主管。Gerald 负责针对整个网络产品组合开展研究 - 探索战略、安全运营、风险、身份、隐私和信任之间的关系。他在执行领导、研究、创新和知识产权开发方面拥有 20 多年的经验。Gerald 目前居住在南加州。

Steve Peterson
linkedin.com/in/stevenjohnpeterson
steve.peterson@us.ibm.com

Steve Peterson 目前担任 IBM 商业价值研究院全球旅游服务和运输主管。Steve 曾编写过众多行业研究报告，自 1998 年以来一直担任旅游服务行业的战略顾问。他的研究报告在 IBM 全球客户中备受欢迎，而且在业界和大众媒体中广受赞誉。Steve 目前居住在丹佛。

选对合作伙伴，驾驭多变的世界

在 IBM，我们积极与客户协作，运用业务洞察和先进的研究方法与技术，帮助他们在瞬息万变的商业环境中保持独特的竞争优势。

IBM 商业价值研究院

IBM 商业价值研究院 (IBV) 隶属于 IBM Services，致力于为全球高级商业主管就公共和私营领域的关键问题提供基于事实的战略洞察。

了解更多信息

欲获取 IBM 研究报告的完整目录，或者订阅我们的每月新闻稿，请访问：ibm.com/iibv

访问 IBM 商业价值研究院中国网站，免费下载研究报告：https://www.ibm.com/ibv/cn

调研方法

IBV 与牛津经济研究院合作，对负责所在组织 IIoT 环境和部署安全的 300 位 IT 和 OT 高管进行了调研，其中有 75 位来自旅游服务行业，225 位来自运输行业，所有这些受访者所在组织均已部署了 IIoT 应用来支持供应链和物流。受访者包括来自除中东及非洲之外所有主要地区的高管（首席执行官、首席技术官、首席信息安全官、首席运营官、首席风险官）、IT 主管和副总裁以及业务线经理和内部审计经理。本次调研所代表的行业包括深海、沿海和大湖水上运输；一般货运；铁路运输；非定期航空运输；定期航空运输。每种运输方式（陆运、航空、水运）各占总样本的三分之一。

为了确定一些公司更加安全、更具网络弹性的原因，我们通过在线调查分两个部分对其 IIoT 网络安全性能和成熟度进行了对标调研：1) 我们询问了受访组织识别和保护其自身免受 IIoT 相关网络安全风险而部署的功能，以及他们检测、响应事件并从中恢复的能力。2) 我们收集了成本、周期时间、质量和效率指标，以衡量风险和事件管理功能的有效性。

我们分两部分对受访者的回答进行了分析。首先，我们基于三个关键绩效指标 (KPI) 计算了每个公司的平均分数：IIoT 网络安全所代表的网络安全预算所占百分比、安全控制措施解决的已知 IIoT 漏洞所占百分比、通过安全控制解决的已知 IIoT 漏洞的百分比以及响应 IIoT 网络安全事件并从中恢复所需的周期时间。通过这种方法我们将安全领导者确定为绩效指标达到 80% 的那些公司。其次，为了了解 20 个 CIS 关键安全控制措施和 6 个 AI 驱动型实践中哪些措施和实践对 KPI 的影响最大，我们进行了回归分析，按影响力对所有 26 个因素进行了排名。前 10 名是影响力高于平均水平的因素。所有数据（无论是财务数据还是其他数据）均为受访者自己报告的数据。

IBM 商业价值研究院相关报告

Hahn、Tim、Marcel Kisch 和 James Murphy 合著。“充满威胁的网络：保护面向工业和公用事业企业的物联网”。IBM 商业价值研究院。2018 年 3 月。
https://www.ibm.com/downloads/cas/71NNBNMA

Fisher、Lisa-Giane、Giuseppe Serio 和 Ben Stanley 合著。“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。2018 年 8 月。
https://www.ibm.com/downloads/cas/MQEWKE4Q

Borrett、Martin、Lisa-Giane Fisher、Cristene Gonzalez- Wertz 和 Peter Xu 合著。“电子行业的工业物联网：补齐短板，取得成功”。IBM 商业价值研究院。2018 年 10 月。
https://www.ibm.com/downloads/cas/53GRRGOG

Dougherty、Steven、Cristene Gonzalez-Wertz、 Lisa-Giane Fisher 和 Mark Holt 合著。“关注公用事业网络安全缺陷：从东拼西凑防线，转变为成竹在胸，安心无忧”。IBM 商业价值研究院。2019 年 1 月。 https://www.ibm.com/downloads/cas/X4O2LAED

备注和参考资料

1 Muncaster, Phil. “San Francisco Airport Attack Linked to Russian State Hackers.” Information Security Magazine. April 2020. https://www.infosecurity-magazine.com/news/ san-francisco-airport-attack/

2 “DragonFly: Energy sector attacks.” IBM X-Force Exchange. https://exchange.xforce.ibmcloud.com/collection/Dragonfly-Energy-Sector-Attacks-d4cf1567963a2cdbd24fae1fbff27111

3 Riedel, Bruce. “Al Qaeda’s 9/11 Obsession.” Brookings. July 15, 2011. https://www.brookings.edu/opinions/ al-qaedas-911-obsession/

4 Bonderud, Douglas. “Loco Motives? Hacker Attacks Could Derail Train Cybersecurity, Researchers Say.” IBM Security Intelligence. January 12, 2016. https://securityintelligence.com/loco-motives-hacker-attacks-could-derail- train-cybersecurity-researchers-say/

5 Alvarez, Michelle. “Industry Overview – Critical Infrastructure (Basic Needs).” IBM Managed Security Services (MSS). March 25, 2015. https://portal.sec.ibm.com/ mss/html/en_US/support_resources/pdf/industry_ overview_crit_infra_3-25-2015.html?cm_mc_uid=48776590151015659713589&cm_mc_sid_50200000=52979001567332373470&cm_mc_sid_52640000=66539761567332373474

6 “CIS Controls™.” Center for Internet Security. https://www.cisecurity.org/controls/; Hahn, Tim, and JR Rao. “IoT Security: An IBM Position Paper.” Watson IoT. IBM. October 2016. https://www.ibm.com/internet-of-things/spotlight/ iot-security. For direct link to paper, go to https://www-01. ibm.com/common/ssi/cgi-bin/ssialias?htmlfid= WWW12379USEN

7 Lunden, Ingrid. “UK’s ICO fines British Airways a record £183M over GDPR breach that leaked data from 500,000 users.” Techcrunch. July 8, 2019. https://techcrunch. com/2019/07/08/uks-ico-fines-british-airways-a-record-183m-over-gdpr-breach-that-leaked-data-from-500000-users/

8 Rodriguez, Joe Fitzgerald. “Alleged Muni ‘hacker’ demands $73,000 ransom, some computers in stations restored.” *San Francisco Examiner. November 28, 2016. https://www.sfexaminer.com/news/alleged-muni-hacker-demands-73000-ransom-some-computers-in-stations-restored/*

9 Newman, Lily Hay. “Atlanta Spent $2.6M to Recover From a $52,000 Ransomware Scare.” Wired. April 23, 2018. https://www.wired.com/story/atlanta-spent-26m-recover-from-ransomware-scare/

10 Baker, Graeme. “Schoolboy hacks into city’s tram system.” The Telegraph. January 11, 2008. https://www.telegraph.co.uk/news/worldnews/1575293/Schoolboy-hacks-into-citys-tram-system.html

11 该数据点表示安全领导者对其 IIoT 网络安全功能的相对信心。该数据点样本数量较少 (n<20)，因此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。

12 “CIS Controls™.” Center for Internet Security. https://www.cisecurity.org/controls/; Hahn, Tim, and JR Rao. “IoT Security:An IBM Position Paper.” Watson IoT. IBM. October 2016. https://www.ibm.com/internet-of-things/spotlight/iot-security.For direct link to paper, go to https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=WWW12379USEN

13 “National Institute of Standards and Technology (NIST) Risk Management Framework.” NIST Computer Security Resource Center website. https://csrc.nist. gov/projects/risk-management/risk-management framework-(rmf)-overview; “NIST Special Publication 800-series General Information.” NIST Information Technology Laboratory. https://www.nist.gov/itl/nist special-publication-800-series-general-information; “ISO/IEC 27000 family - Information security management systems.” International Organization for Standardization. https://www.iso.org/isoiec-27001-information-security.html

14 Hahn, Tim, Marcel Kisch, and James Murphy. “Internet of threats: Securing the Internet of Things for industrial and utility companies.” IBM Institute for Business Value. March 2018. https://www-935.ibm.com/services/us/gbs/thoughtleadership/iotthreats/

15 “CIS Controls Internet of Things Companion Guide.” Center for Internet Security. July 27, 2019. https://www.cisecurity.org/white-papers/cis-controls-internet-of-things-companion-guide/

16 Ibid.

17 Ibid.

18 “IBM X-Force Threat Intelligence Index 2019.” IBM Security. February 2019. https://www.ibm.com/security/data-breach/threat-intelligence

关于对标洞察

对标洞察致力于就重要的业务话题及相关技术话题为企业高管提供洞察。洞察根据针对绩效数据的分析结果及其他对标调研结果而得出。要了解更多信息，请联系 IBM 商业价值研究院：iibv@us.ibm.com。

IBM Corporation
New Orchard Road
Armonk, NY 10504
美国印刷
2020 年 4 月

国际商业机器中国有限公司
北京朝阳区北四环中路 27 号
盘古大观写字楼 25 层
邮编：100101