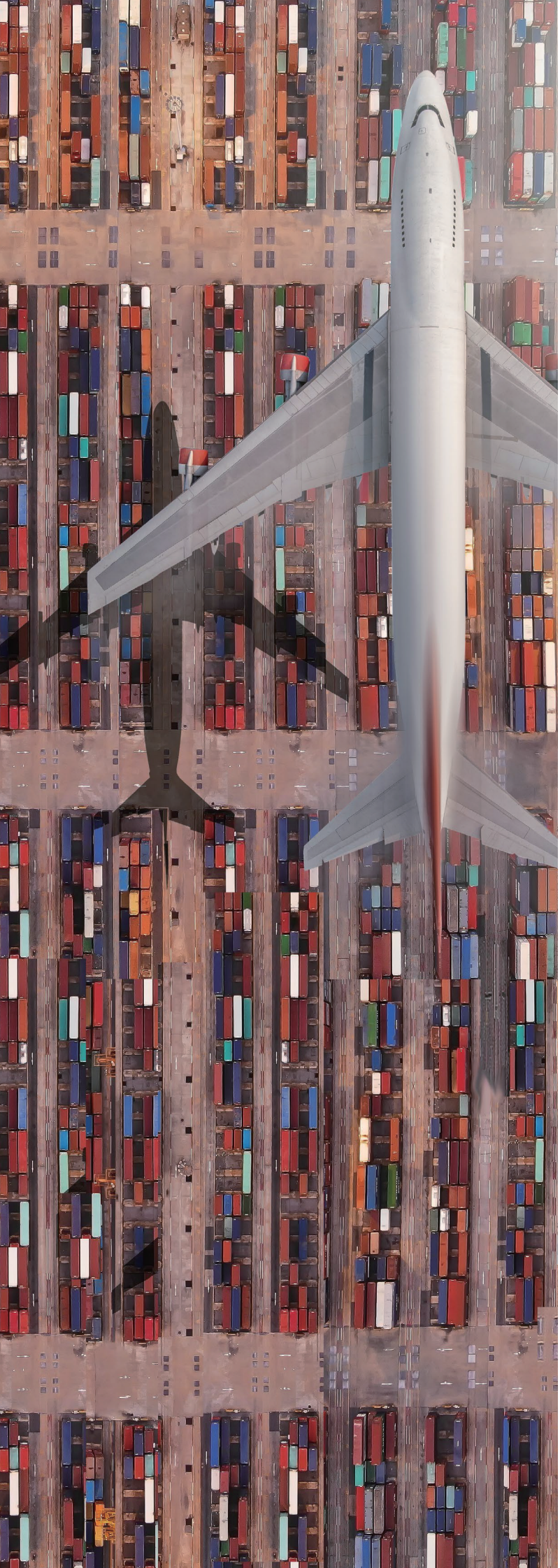


对标洞察

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

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，我们将在本报告中进行详细说明。[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。

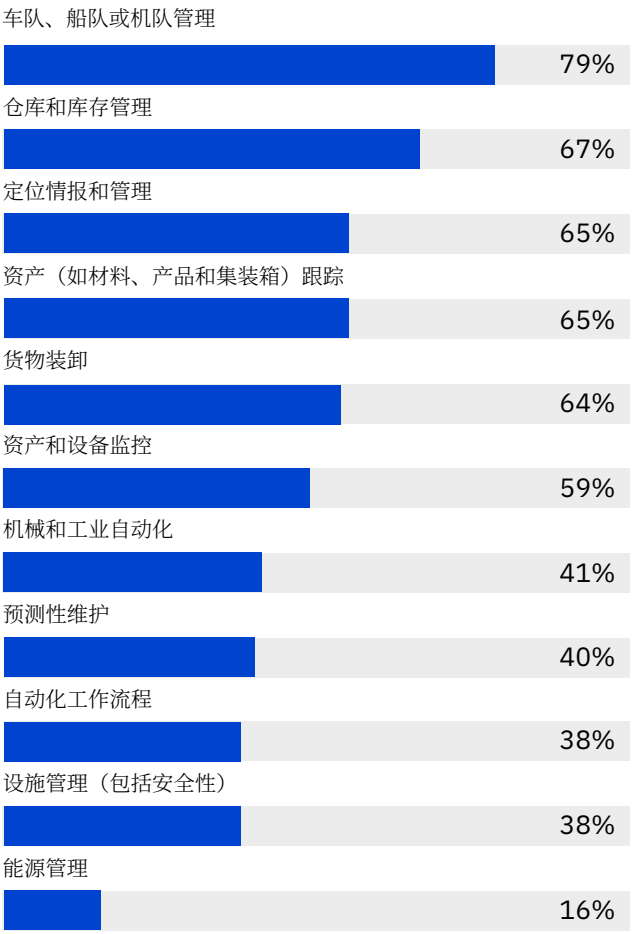
风险存在共通之处，凡危及交付和履行能力的威胁，都可能会对业务成果产生不可估量的影响。尽管消费者数据极少面临危险，但宝贵商业机密和知识产权却频繁陷入危机。

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。

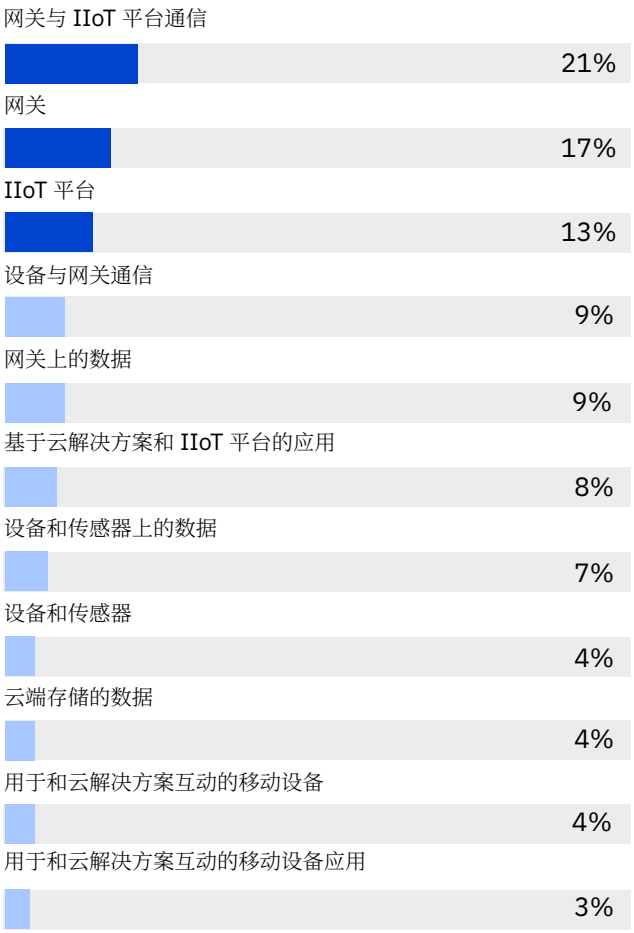
出于本次调研的目的，“在安全方面表现出众的企业”是指所有者 59 家企业，包括 36 家交通运输企业。“所有其他企业”则指另外 241 家受访旅游企业和交通运输企业。

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

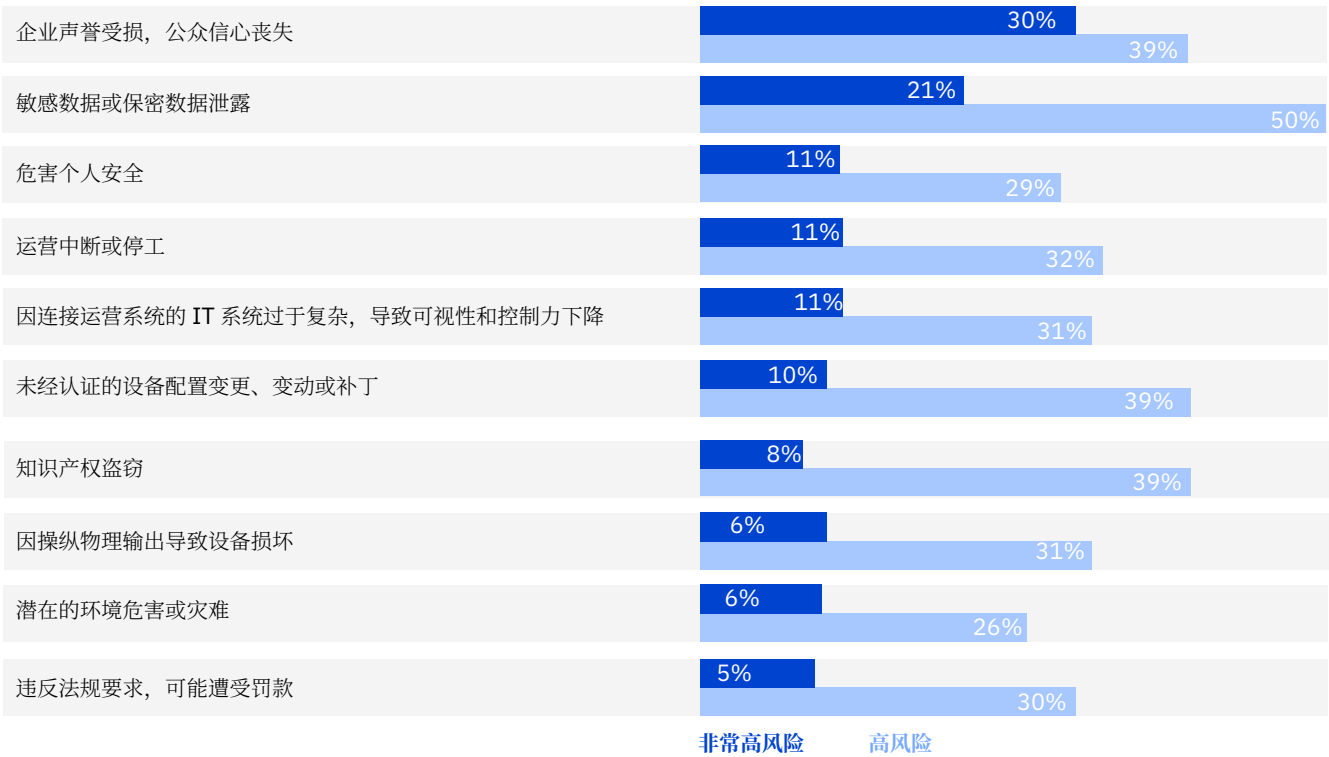
2017 年 6 月，一家全球性航运公司遭到勒索软件攻击，这是交通运输行业运营中断所产生的连锁反应的典型例子。此次攻击导致全球近 80 个港口和码头停摆或发生严重延误。此次中断不仅波及海港和集装箱货轮，发往内陆设施的卡车也被迫滞留港口，等待系统恢复上线，以便处理、接收或运送货物。此次中断大大延长了产品分销时间。该航运公司不得不重建大部分 IT 基础架构，预计损失高达 3 亿美元。[4]

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



来源：IBM 商业价值研究院对标调研，2019 年。问：贵企业发生以下每种 IIoT 网络安全风险的概率是多少？一旦发生此类风险，将对贵企业产生什么影响？指定发生风险的概率，以及一旦发生风险将对企业产生的影响，其中：1 = 非常低，2 = 低，3 = 中等，4 = 高，5 = 非常高。

三大步骤帮助改善 IIoT 网络安全状况，增强弹性。

三步改善 IIoT 网络安全，建立弹性

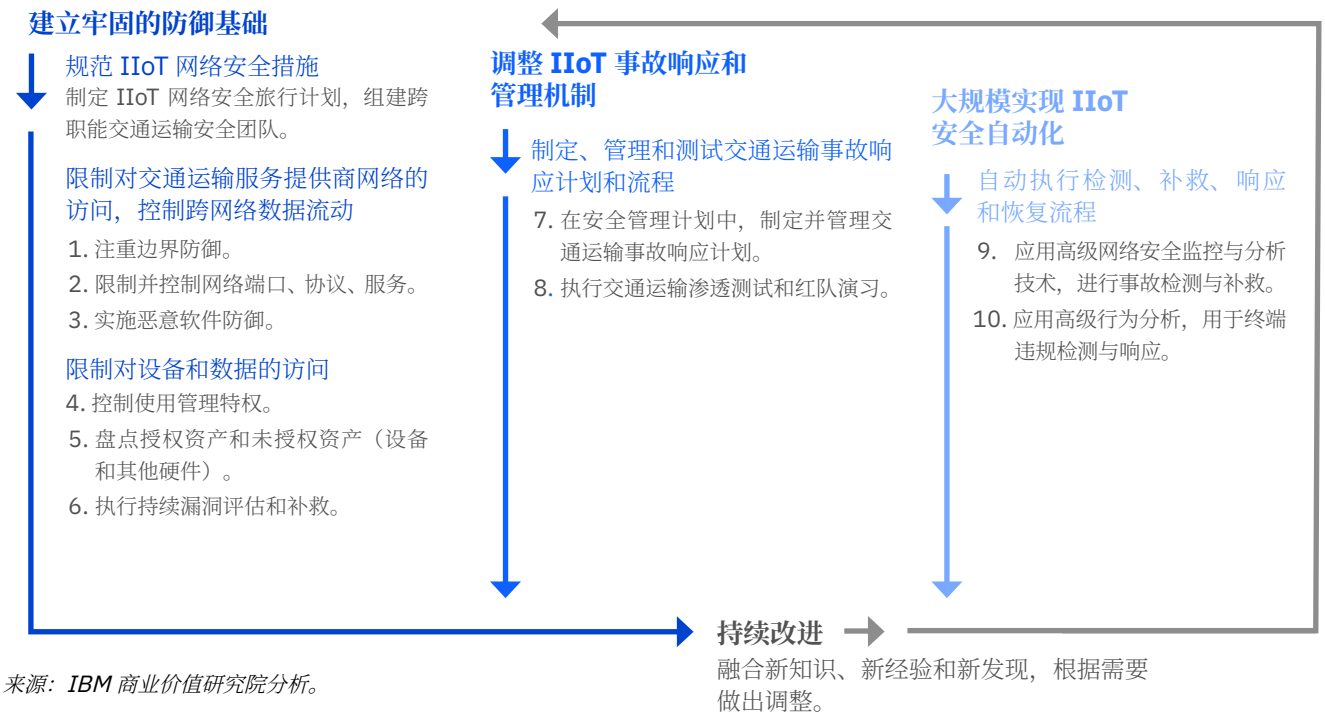
我们发现，在安全方面表现出众的企业更有可能充分评估 IIoT 网络安全风险，而且对缓解风险需要具备的网络安全能力有着深入的认识。此外，这些企业也更有可能将安全控制视为高效的推动力量和保护措施。然而，真正让他们独树一帜的是网络的弹性：这些企业能够更迅速地检测和应对 IIoT 相关事故和违规情况并恢复正常运营，速度至少比其他企业快 2 倍。

我们的研究表明，在 20 项 CIS 关键安全控制措施中有 8 项措施，以及在 6 项更高级的 AI 驱动的实践中有 2 项实践都会影响到网络的弹性，而许多交通运输企业都采用了相应的措施和实践。所有这些高效控制措施和实践均与安全功能有关 — 保护和预防，或者检测、响应和恢复。

这些控制措施和实践可采用以下三个步骤实施（见图 4）：

- 制定并实施 IIoT 网络安全战略和计划，建立牢固的 IIoT 防御基础。然后，重点落实六项控制措施和实践，帮助加强保护和预防能力。
- 调整 IIoT 事故响应和管理：采取两项控制措施，将 IIoT 网络安全整合到安全运营流程之中，更有效地应对与 IIoT 相关的事故和违规。
- 大规模实现 IIoT 安全自动化：实施两项人工智能 (AI) 驱动的实践，在各个业务部门、平台和生态系统中自动执行检测和响应功能。

图 4
三大步骤改善 IIoT 网络安全，增强弹性



来源：IBM 商业价值研究院分析。

建立牢固的 IIoT 防御基础

第一步，建立 IIoT 防御基础。首先，将 IIoT 网络安全控制措施和实践（以及相关技术）整合到总体 IIoT 安全战略之中。然后，应用高效的保护和预防控制措施，帮助增强防御能力。

制定 IIoT 网络安全计划。

这项活动有助于定义、管理和更新所需的 IIoT 网络安全工具、流程和技能。41% 在安全方面表现出众的企业实现了这一目标；相比之下，仅有 15% 的其他企业做到这一点（见图 5）。与 IIoT 相关的风险应当在交通运输企业更广泛的安全风险管控框架中加以解决（请参阅：“洞察：IIoT 风险管控框架”）。

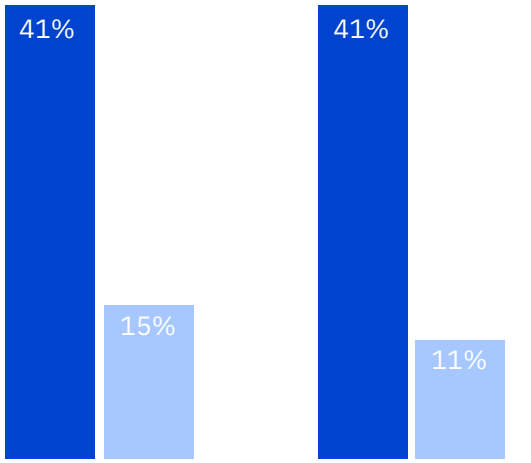
首先，评估风险并确定优先顺序。然后，采用覆盖 IT 和 OT 领域的常用风险方法，在企业层面监控和管理风险。定期执行风险评估，发现 IIoT 环境（包括互联 ICS）中的安全漏洞，记录并落实风险缓解计划。

组建跨职能交通运输安全团队。

表现出众的企业更清楚跨职能合作的价值。通过在团队中汇集 IT 安全、工程、运营、控制系统和安全供应商的代表，就可以更清晰地了解 IIoT 系统、企业 IT 系统及运营设备中存在的差异。然后，有效运用 IT 和 OT 专业知识，对安全控制措施划分适当的优先排序，帮助优化风险缓解措施。[5]

图 5

规范 IIoT 网络安全措施



来源：IBM 商业价值研究院对标调研，2019 年。
问：以下哪项描述最能体现贵企业对 IIoT 网络安全的理解？
问 贵企业在多大程度上实施以下运营方法以缓解 IIoT 网络安全风险？
注：图 5 显示选择 4 和 5（4 = 计划推出，5 = 全面实施）的企业数量。

边界防御对 IIoT 网络安全性能的影响最大。

限制对交通运输服务提供商网络的访问，控制跨网络数据流动。

IIoT 设备会生成海量数据，这些数据自然会流经企业 IT 网络以及保护措施比较薄弱的 IIoT 网络。为始终如一地保障安全，定义角色和权限、限制网络访问以及控制网络中的数据流动都至关重要。以下三项高效控制措施可能会有所帮助：

1. 注重边界防御。我们的研究表明，这项控制措施对 IIoT 网络安全性能的影响最大。边界防御的目的在于检测、预防和纠正不同信任等级的网络之间的信息流动，重点关注会损害安全的数据。

36% 在安全方面表现出众的企业采取隔离战略，确保 IIoT 组件在各自的专属区域或独立网络中运行（见图 6）。[8] 这种做法有助于缓解信任等级较低、受到入侵的 IIoT 网络可能对更为安全的企业 IT 网络造成的负面影响。

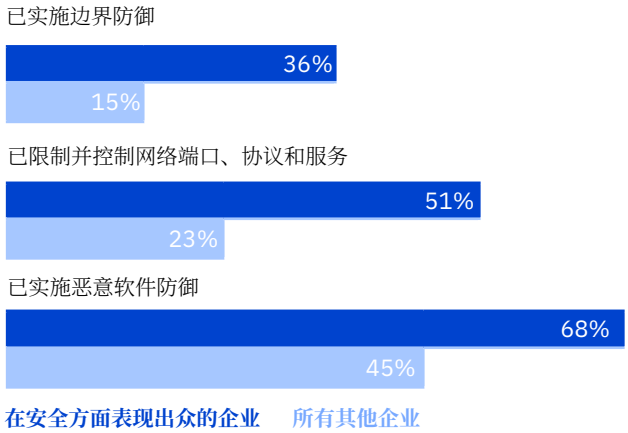
2. 限制并控制网络端口、协议和服务。在积极定义并实施可供运营环境中 IIoT 设备使用的端口、协议和服务的企业中，在安全方面表现出众的企业要比其他受访企业高出两倍还多。

某些设备可能实施并非依托企业网络运行的通信协议，比如蓝牙。在这种情况下，如果全面掌握哪些协议符合企业安全策略，有助于显著缩小漏洞范围。测试 IIoT 设备，评估设备的消息传递操作不符合安全要求的程度。[9]

3. 实施恶意软件防御。目前的恶意软件和攻击手段都针对 IIoT 设备和平台精心设计。因此必须制定战略，在整个企业的多个环节控制恶意代码的安装、传播及执行。持续监控 IIoT 设备信息（更新和数据）所流经的网关，帮助检测恶意软件，或者将观察到的活动与已知的计划内合法活动关联起来。

图 6

限制对网络的访问，控制跨网络数据流动



来源：IBM 商业价值研究院对标调研，2019 年。
问：贵企业在多大程度上应用以下关键的安全控制措施，以缓解 IIoT 网络安全风险？

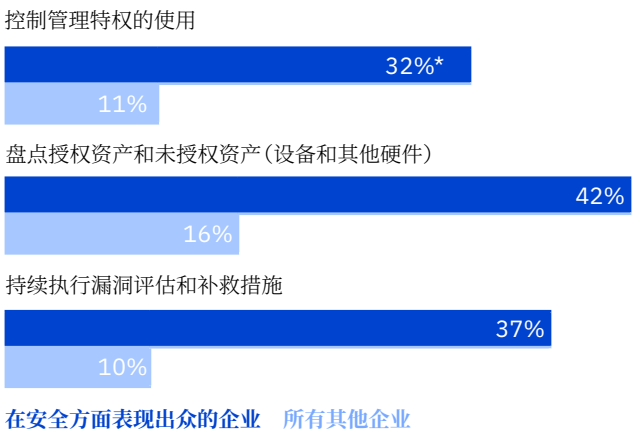
限制对设备和数据的访问。

在防御“方程”中，一边是管理网络访问和数据流动，另一边是管理对设备和数据（包括使用中、传输中和静态存储的数据）的访问。以下三项高效控制措施有助于实现这一目标：

4. 控制使用管理特权。无论是出于恶意还是纯粹因为疏忽，员工往往是企业网络安全的最大威胁。因为与外部恶意黑客相比，员工能够更方便地访问信息和关键基础架构，所以必须有针对性地加以限制。在安全方面表现出众的企业领先一步，妥善限制特权访问，记录有权访问敏感功能和数据的用户，监控企业网络中所有用户的活动（见图 7）。

图 7

限制对设备和数据的访问



来源：IBM 商业价值研究院对标调研，2019 年。
** 在所有数据中，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。*
问：贵企业在多大程度上应用以下关键的安全控制措施，以缓解 IIoT 网络安全风险？

洞察：IIoT 风险管控框架

综合运用多种安全和治理框架作为基础（例如美国国家标准与技术研究院 (NIST) 的关键基础设施网络安全框架，以及国际标准化组织 / 国际电工委员会的 ISO/IEC 27000-1[6]），以帮助：

– 确定关键数据、资产和安全边界。

– 确定 IIoT 系统、连接的生产环境和人员资产中的漏洞。

– 构建和定制风险管理框架。

– 评估风险，记录并执行计划以减轻风险。

– 保护最紧迫的安全计划的投资并沟通进度。

– 根据业务目标与合规要求，平衡可接受的风险水平。[7]

为支持有效应对与 IIoT 相关的事故和违规情况，必须将 IIoT 网络安全整合到安全运营之中。

5. 盘点授权资产和未授权资产（设备和其他硬件）。未经授权的 IIoT 设备和网络属于“影子 IIoT”的范畴，它们游离在企业传统的安全策略之外，因而难以检测。为弥补这一漏洞，一种方法是确定并分析所有 IIoT 终端，将它们添加到资产清单中并实施监控。仅提供对授权设备的访问权限，阻止访问已发现的未经授权的设备和不受管理的设备。

6. 执行持续漏洞评估和补救。79% 的交通运输行业高管指出，分布式拒绝服务 (DDoS) 攻击（以应用或设备为攻击目标或主体）是目前面临的最严峻的 IIoT 相关威胁。IIoT 设备和 ICS（包括监督控制与数据采集 (SCADA) 系统）不免存在缺陷和漏洞，导致交通运输企业极易受到僵尸网络（例如，Mirai、Aidra、Wifatch 和 Gafgyt）的攻击，从而传播 DDoS 攻击恶意软件。[10]

交通运输行业高管表示，此类攻击占企业网络安全事故总数的 35%。因此，应当定期安排漏洞评估，帮助发现配置不当的 IIoT 设备，以便管理员可以移除或重新配置有问题的设备。在运营环境中执行主动漏洞扫描可能会破坏系统稳定性；因此，如果无法实施自动扫描，则进行被动监控。

调整 IIoT 事故响应和管理机制

建立防御性 IIoT 网络安全基础之后，第二步是将 IIoT 网络安全整合到安全运营之中。这项操作有助于高效响应与 IIoT 相关的事故和违规。采取更有效的保护和预防实践，确保安全地开发和部署系统，并不能保证万无一失。企业必须做好充分准备，一旦发生违规，迅速采取果断行动。

制定、管理和测试交通运输事故响应计划和流程。

7. 在安全管理计划中，制定并管理交通运输事故响应计划。大多数在安全方面表现出众的企业已调整事故响应 (IR) 计划，针对受攻击的 IIoT 组件制定合适的行动方案（见图 8）。例行测试计划有助于增强响应能力。执行违规模拟，确定发生违规时应当激活的流程、人员和工具。

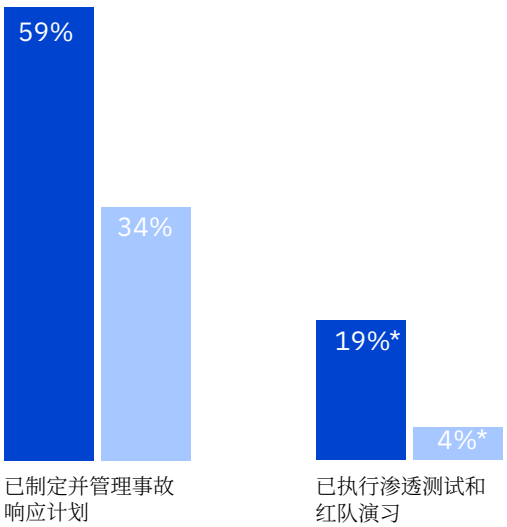
运用生态系统中的共享资源，比如具备稀缺技能的 ICS/SCADA 安全专家。另外，还可以通过网络保险（覆盖与任务关键型 IIoT 平台相关的业务中断和敲诈勒索）缓解风险。只有极少数受访高管表示自己的企业购买了此类网络保险。

8. 执行交通运输渗透测试和红队演习。这些活动可以更细致地洞察 IR 计划的有效性。红队是指模拟网络攻击的道德黑客团体，旨在帮助企业对 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，确保持续遵守安全策略和数据隐私法规。

我们发现，在实施此类进攻性防御战略的企业中，在安全方面表现出众的企业要比其他受访企业高出近五倍（见图 8）。在 IIoT 环境中，一旦扫描环节出错，很可能严重影响业务运营，因此必须充分考虑并应对这种可能性。

图 8

已制定、管理和测试旅行事故响应计划和流程



在安全方面表现出众的企业 所有其他企业

来源：IBM 商业价值研究院对标调研，2019 年。
问：贵企业在多大程度上应用以下关键安全控制措施，以缓解 IIoT 网络安全风险？

大规模实现 IIoT 安全自动化

该过程的第三步是部署自动化自适应的交通运输安全能力。这个步骤至关重要，因为恶意攻击者会不断探寻新的系统渗透方法。由于企业通常缺乏必需的网络安全技能，因此务必部署自动化机制，帮助检测违规并实施补救措施。

自动执行检测、补救、响应和恢复流程。以下两种基于 AI 的高效实践有助于推进这些流程：

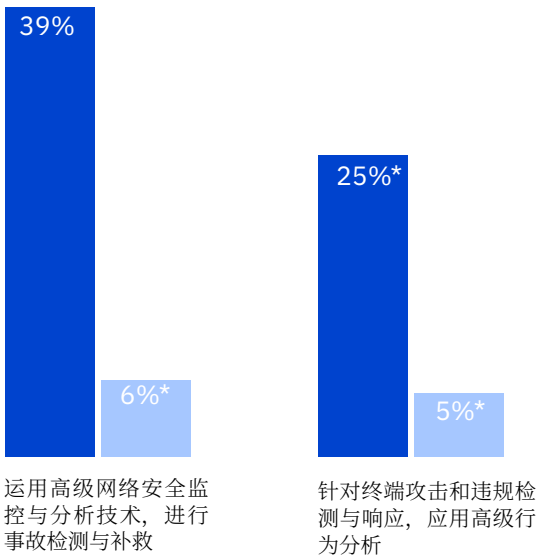
9. 应用高级网络安全监控与分析技术，进行事故检测与补救。为实时掌握各个运营环境中的 IIoT 信息，39% 在安全方面表现出众的企业建立了全面的安全遥测能力，相比之下，仅有 6% 的其他企业这样做。这些企业自动收集、整合并分析所有可能监测点的数据（见图 9）。这包括系统日志、网络流、终端数据、云使用情况和用户行为，从而帮助安全运营中心 (SOC) 团队快速了解警报的背景信息，有效区分误报与真实警报。

SOC 团队可主动出击，对照外部收集的威胁情报数据，分析从内部 IIoT 数据提取的信息。然后，机器学习功能可帮助预测攻击者的下一步行动。

随着软件服务和生态系统合作伙伴网络的兴起，整合安全治理与运营凸显出前所未有的重要意义。

10. 应用高级行为分析，用于终端违规检测与响应。可在企业层面应用基于 AI 的威胁检测，帮助揭示异常用户活动，划分风险的优先顺序。25% 在安全方面表现出众的企业已具备使用机器学习分析用户行为的能力（见图 9）。此外，在应用机器学习以自动运行已成“常态”的自适应模式方面，他们同样遥遥领先。这项能力帮助他们跟踪正常行为特征，标记可能预示新威胁的异常活动。

图 9
自动执行检测、补救、响应和恢复流程



来源：IBM 商业价值研究院对标调研，2019 年。
问：贵企业在多大程度上实施以下基于 AI 和分析的方法，以缓解 IIoT 网络安全风险？

实现 IIoT 安全永续

交通运输企业依赖于大量在互联网络安全概念出现之前设计的 OT 系统。为率先实现规模经济，许多交通运输提供商往往先采用新技术，但安全防护措施明显滞后。随着软件服务和生态系统合作伙伴网络的兴起，整合安全治理与运营凸显出前所未有的重要意义。

IIoT 是 IT 与 OT 解决方案的交汇融合点，IT 系统和网络日益广泛地应用于 OT 环境。但这一趋势增加了复杂性，带来了一系列独特的风险。IIoT 安全战略将安全视为运营中不可或缺的关键环节，因此对 IT 和 OT 基础架构的投资有助于提高效率，帮助改善企业的安全态势，增强弹性。

贵企业是否做好了从关键基础设施攻击中恢复的准备？

如何保证 IIoT 安全实践与组织确立的企业风险管理框架保持一致？

如何将安全工具和管理流程整合到企业安全框架和运营流程之中？如何在整个运营生命周期内保持可视性、透明度和责任制？

如何加强隔离措施，帮助最大程度隔离安全等级较低的 IIoT 网络？

贵企业打算如何改进事故响应计划，在压力环境下轻松实施？

如何遏制威胁影响、减少中断以及建立从攻击中快速恢复的能力？

行动指南

降低风险，建立弹性

1. 首先，建立牢固的 IIoT 防御基础。

将 IIoT 网络安全控制措施和实践（以及相关技术）整合到总体 IIoT 安全战略之中。然后，重点加强保护和预防能力：

规范 IIoT 网络安全措施。

– 制定交通运输 IIoT 网络安全计划。

– 组建交通运输跨职能安全团队。

限制对交通运输服务提供商网络的访问，控制跨网络数据流动。

– 注重边界防御。

– 限制并控制网络端口、协议和服务。

– 实施恶意软件防御。

限制对设备和数据的访问。

– 控制使用管理特权。

– 盘点授权资产和未授权资产（设备和其他硬件）。

– 执行持续漏洞评估和补救。

2. 建立防御基础后，针对 IIoT 调整事故响应措施。

将 IIoT 网络安全措施整合至交通运输安全运营流程之中，帮助企业更迅速、更有效地响应与 IIoT 相关的事故和违规：

制定、管理和测试交通运输 IIoT 事故响应计划和流程。

– 在安全管理计划中，制定并管理交通运输 IIoT 事故响应计划。

– 执行渗透测试和红队演习，寻找防御漏洞和响应计划中的弱点。

3. 最后，通过自动化系统增强交通运输 IIoT 安全能力

恶意攻击者不断探寻新的系统渗透方法，而且网络安全技能通常较为稀缺。因此，必须大规模部署自动化、自适应、响应迅速的功能：

自动执行检测、补救、响应和恢复流程。

– 应用高级网络安全监控与分析技术，进行事故检测与补救。

– 针对终端攻击和违规检测与响应，应用高级行为分析。

关于作者

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

Eric Maass 是 IBM Security Services 的战略和新兴技术总监，负责领导针对企业产品组合（包括先进新兴安全技术）的业务和投资战略。Maass 先生是安全领域的行业资深专家，拥有约 20 年大型企业和初创企业的工作经验，服务的客户涵盖商业机构、美国国防部 (DoD) 和情报机构等。他是一家云安全初创企业的创始人兼首席技术官 (CTO)，2014 年这家企业被 IBM 收购。Eric 目前在大纽约地区工作生活。

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

Gerald Parham 是 IBM 商业价值研究院全球安全与 CIO 负责人。Gerald 在整个网络领域开展研究 — 探索战略、安全运营、风险、身份、隐私和信任之间的关系。他拥有超过 20 年高管领导、研究、创新和知识产权开发的经验。Gerald 目前在南加州工作生活。

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

Julian Meyrick 负责领导 IBM Security 全球安全战略风险与合规及云安全实践工作。Julian 帮助客户制定安全战略，应对面临的网络业务风险。他尤其关注从网络安全的潜在业务影响角度向董事会提出真知灼见。Julian 目前在伦敦工作生活。

Keith Dierkx
linkedin.com/in/keith-dierkx-bb510a/
kwdierkx@us.ibm.com

Keith Dierkx 是 IBM 货运、物流和铁路领域全球行业负责人。他拥有超过 30 年运输行业从业经验，一直担任高层管理人员和战略顾问。他为众多初创企业提供咨询服务，还发表过大量有关数字化转型的文章。Keith 目前在旧金山工作生活。

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

Lisa-Giane Fisher 是 IBM 商业价值研究院中东和非洲对标分析负责人。她主要负责并购和安全对标分析，并与 IBM 行业专家合作开发并维护行业流程框架。Lisa 目前在南非工作生活。

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

Steve Peterson 是 IBM 商业价值研究院的全球旅游和交通运输业主管。他是众多行业调研报告的作者，从 1998 年起一直担任该行业的战略顾问。他的工作受到全球 IBM 客户的交口称赞，并得到了业界和大众传媒的广泛赞誉。Steve 目前在丹佛工作生活。

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，致力于为全球高级业务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，采访了 300 位企业 IT 和 OT 部门负责 IIoT 环境和部署安全的领导，其中 75 位来自旅游企业，225 位来自交通运输企业。所有受访企业均已部署 IIoT 应用，用于支持供应链和物流流程。

受访者包括中东和非洲以外各主要地区的最高层主管（CEO、CTO、CISO、CSO、COO 和 CRO）、IT 总监和副总裁，以及业务部门和内部审计经理。

调研涉及了五个领域：远洋、沿海和大湖水上运输；普通卡车货运；铁路运输；非定期航空运输；以及定期航空运输。每种运输模式（海陆空）各占整体受访企业的 1/3。

为探索某些企业安全性更高、网络弹性更强的真正奥秘，我们开展了在线调研，按两部分对企业 IIoT 安全网络的表现和成熟度进行了对标分析。

第一部分，调查企业发现及防范 IIoT 相关网络安全风险的能力，以及检测和应对相关事故并恢复正常运营的能力。在调研的第二部分，我们收集了成本、周期时间、质量和效率指标，衡量风险和事故管理能力的有效性。

我们分两部分对调研结果进行分析。首先，按以下三个关键绩效指标 (KPI) 计算每家企业的平均分数：

– IIoT 网络安全在网络安全预算中所占的百分比。

– 安全控制措施修复的已知 IIoT 漏洞的百分比。

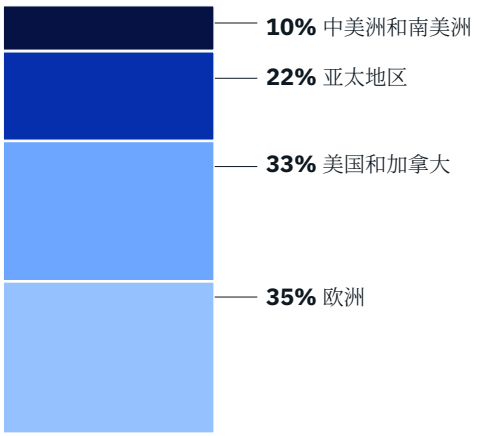
– 应对 IIoT 网络安全事故并恢复正常运营的周期时间。

按照这种调研方法，我们确定了 20% 在安全方面表现出众的企业，将其与其他企业区分开来。

其次，为了解 20 项 CIS 关键安全控制措施及 6 项 AI 驱动实践中哪些对 KPI 的影响最为明显，我们开展了回归分析，从影响力的角度对全部 26 项要素进行了排名并编制成表。排名前十位的要素的影响力高于平均水平。所有数据（无论财务数据还是其他数据）均由受访者自行提供。

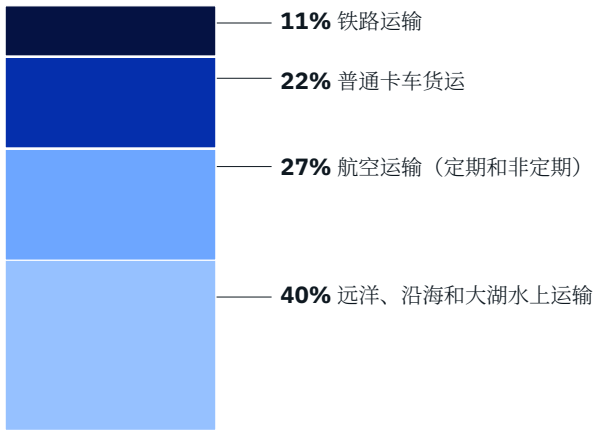
受访者（按地区划分）

100%



受访者（按类型划分）

100%



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 CIS Controls.” Center for Internet Security. https://www.cisecurity.org/controls/

2 Caleb Barlow. “Why Cybercriminals Are Targeting Travel and Transportation.” IBM Security Intelligence. July 10, 2019. https://securityintelligence.com/posts/why-cybercriminals-are-targeting-travel-and-transportation/

3 Shelley Smith. “Teen Hacker in Poland Plays Trains and Derails City Tram System.” In Homeland Security. February 12, 2008. https://inhomelandsecurity.com/teen_hacker_in_poland_plays_tr/

4 John Callon. “Cyber pirates targeting logistics and transportation companies.” Cyren Security. May 14, 2018. www.cyren.com/blog/articles/cyber-pirates-targeting-logistics-and-transportation-companies

5 Tim Hahn, 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/

6 “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/publications-0/nist-special-publication-800-series-general-information.” International Organization for Standardization. https://www.iso.org/isoiec-27001-information-security.html

7 Steven Dougherty, Cristene Gonzalez-Wertz, Lisa-Giane Fisher, and Mark Holt. “Mind the utilities cybersecurity gap - Move from pieced together to peace of mind.” IBM Institute for Business Value. January 2019. https://www.ibm.com/thought-leadership/institute-business-value/report/utilitiesiiot

8 “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/

9 Ibid.

10 “2019 IBM X-Force Threat Intelligence Index.” IBM Security, 2019. https://dd80b675424c132b90b3-e48385e382d2e5d17821a5e1d8e4c86b.ssl.cf1.rackcdn.com/external/finalibmthreatintelligenceindex022619127023627usen.pdf

11 Francis Knott. “The Threat of Cybercrime for State and Local Transportation Systems.” Attila Security. November 5, 2018. https://attilasec.com/blog/transportation-systems-cybercrime/

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

美国出品
2020 年 3 月