

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

对标分析报告

汽车行业

IBM 的能力

如今，车辆正逐渐从一种交通工具转变为新型的移动数据中心，车载传感器和计算机能够即时捕获有关车辆的信息。利用此类实时数据，IBM 可以帮助汽车制造业的高管提供全新的服务，满足互联互通时代的消费者对于车辆体验的新要求和期望。我们既拥有丰富的制造业经验，也具备深厚的全球汽车行业专业知识，可以帮助消除消费者对安全和质量的顾虑。通过使用 Watson 等创新技术，我们可以满足汽车制造商 (OEM) 和供应商的各种需求，提供更安全可靠的产品和服务，从而实现更高的品牌忠诚度和客户满意度。敬请访问：**ibm.com**/industries/automotive。

本报告亮点

汽车行业工业物联网 (IIoT) 的网络安全风险与采用进展情况

表现出众的企业在保护 IIoT 安全环境方面展现出三大独特的优势

九项重要的网络安全实践

智能工业物联网的网络安全

互联自主驾驶汽车的安全问题备受关注。但企业更应当专注于基本层面，即用于制造汽车以及科技含量日益提升的零部件的工业系统。如果在没有实施有效的网络安全措施的情况下，匆忙上马“智能工业物联网”，会让整个企业处于风险之中。IBM 商业价值研究院 (IBV) 的一项调研表明，87% 的汽车企业在工厂和装配线上实施了工业物联网 (IIoT) 技术，但没有充分评估风险或准备有效的应对措施。汽车企业需要提升网络安全能力，能够以认知方式自动适应所处环境，持续发现、缓解和预防风险。

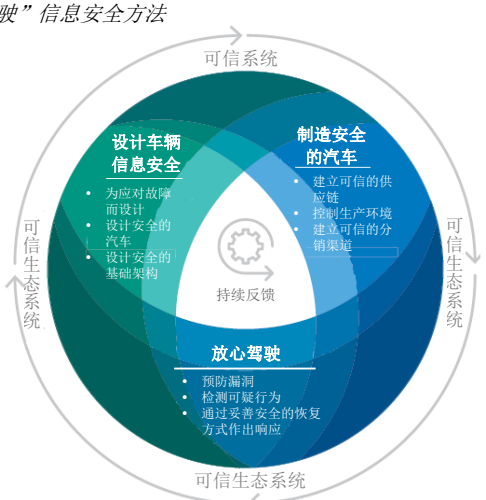
危机四伏

随着工业物联网技术的实施，制造设备和流程变得越来越智能化和自动化，但企业所面临的网络攻击风险也与日俱增。网络入侵可能来自于网络黑客、竞争对手、进行商业间谍活动的国家或地区，或者是心怀不满的员工，这都可能导致大量设备损坏、关键数据丢失、企业声誉受损甚至人身安全受到威胁。

在 IBV 调研“加速车辆信息安全：赢得车辆完整性和数据隐私竞争”中，我们介绍了“设计、制造、驾驶”信息安全方法（见图 1）。[1] 这种方法中的“制造安全的汽车”阶段明确了控制生产环境的要求。

图 1

“设计、制造、驾驶”信息安全方法



来源：IBM 商业价值研究院分析



87%

的受访汽车企业正在部署 IIoT 技术，但未对风险进行全面评估



86%

的受访汽车企业没有定期进行 IIoT 网络安全评估



87%

的受访汽车企业没有正式制定 IIoT 网络安全计划

虽然工业物联网的实施有助于大幅提升运营效率，但如果没有得到适当保护，它们也会暴露出潜在的新安全隐患。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。

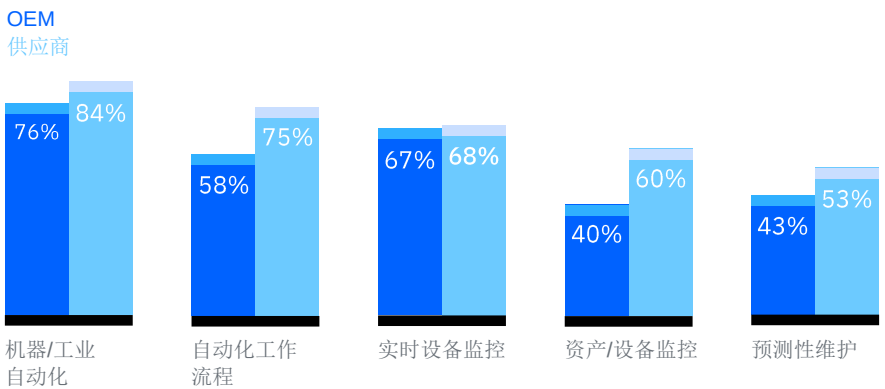
为了更好地理解工业物联网的安全风险和影响，IBV 与牛津经济研究院合作，对 700 位最高层主管进行了调研。他们代表了 18 个国家或地区能源和工业领域的 700 家在工厂中实施了 IIoT 的企业（其中 135 家是汽车企业）。

机器/工业自动化是企业应用 IIoT 技术最多的领域，有 76% 的整车厂 (OEM) 和 84% 的供应商选择了这一项（见图 2）。58% 的 OEM 和 75% 的供应商表示他们具有自动化的工作流程应用。令人惊讶的是，预测性维护方面的应用并不像预期的那么多。

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 IIoT 支出（见图 3）。但他们并不清楚如何将多种 IIoT 网络安全能力（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 IIoT 威胁。

图 2

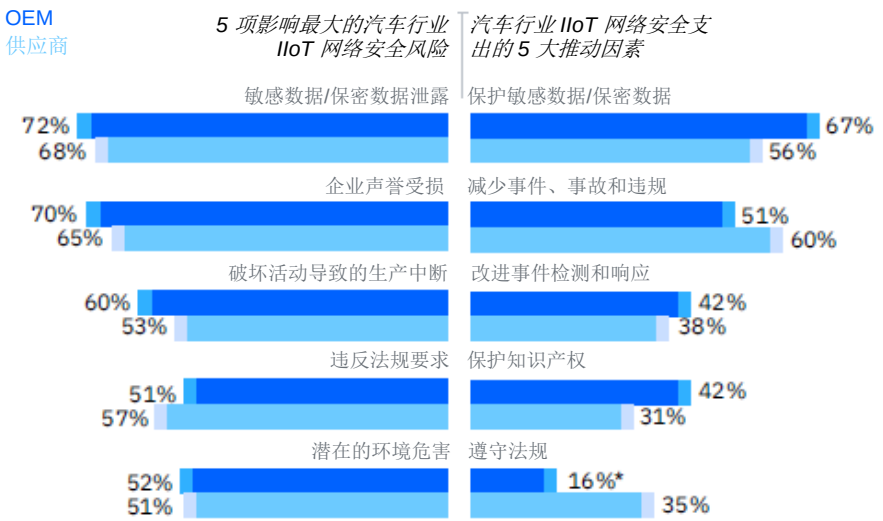
IIoT 技术在汽车制造工厂和装配线上的前五大应用



来源: IBM 商业价值研究院对标分析调研，2018 年，n=135。

图 3

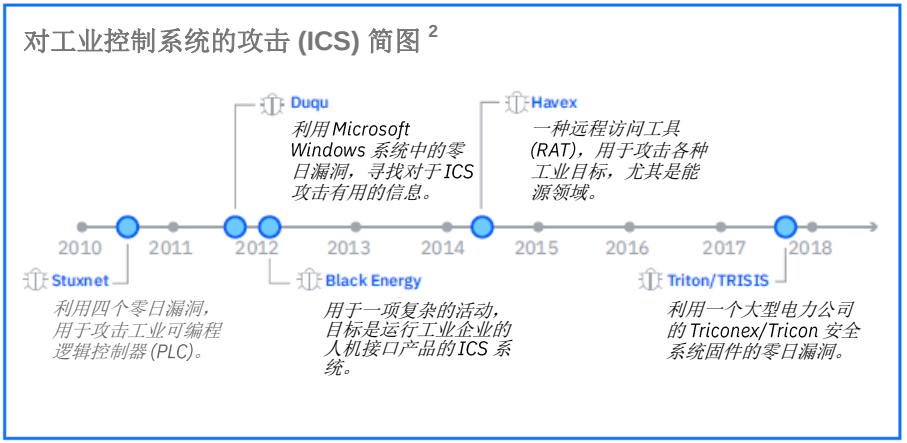
IIoT 网络安全风险与支出推动因素对比



来源: IBM 商业价值研究院对标分析调研，2018 年，n=135。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。

由于未能实施适当的网络安全保护措施，汽车企业将面临重大风险。特别是：

1. *敏感数据/保密数据泄露*。受访高管认为这是他们面临的最大风险。72% 的 OEM 和 68% 的供应商敏锐地意识到，客户知识产权和高级工程设计等数据的泄露可能会对企业发展产生非常不利的影响。
2. *企业声誉受损，公众信心丧失*。70% 的 OEM 和 65% 的供应商认为，安全漏洞可能会对汽车企业的形象和声誉造成巨大的负面影响。企业品牌的公信力和可信度很容易受到损害，业务和客户关系会遭到不可挽回的破坏。
3. *破坏活动导致生产中断*。60% 的 OEM 和 53% 的供应商表示，这种风险非常巨大，可能会导致物理设备损坏、零部件报废或车辆产生缺陷。网络攻击者可能会入侵企业的工业系统并操纵网络基础设施（见插图：“对工业控制系统的攻击 — 简图”）。他们会修改机器软件程序或监视控制和数据采集系统 (SCADA)。
4. *违反法规要求*。2018 年 5 月生效的《通用数据保护条例》(GDPR) 和类似法律增加了不合规的风险。51% 的 OEM 和 57% 的供应商表示，他们高度关注不合规的潜在影响以及由此可能导致的巨额罚款。



5. *潜在的环境危害。*52% 的 OEM 和 51% 的供应商高度关注当违反控制措施，有害物质被释放到环境中的情形。

从支出的角度来看，保护敏感数据是最重要的任务，67% 的 OEM 和 56% 的供应商将其列为 IIoT 网络安全预算的主要推动因素。超过 50% 的 OEM 和供应商还表示，减少事件、事故和违规是高优先级任务领域。

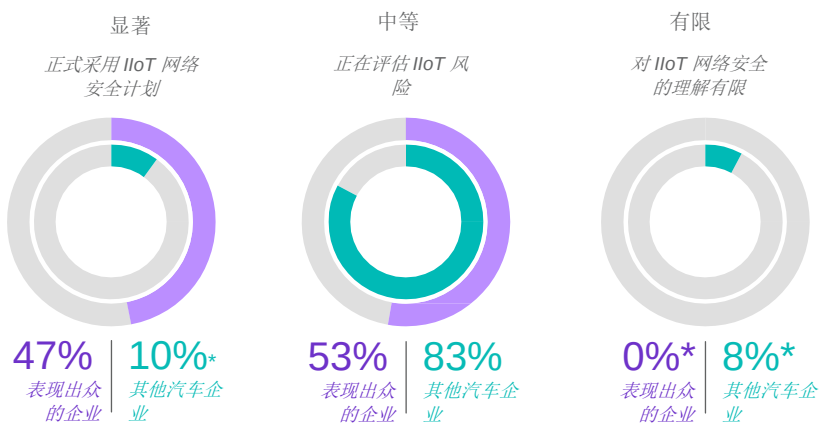
表现出众的企业一马当先

我们发现了一组表现出众的企业，他们在保护 IIoT 环境方面处于领先地位（请参阅侧边栏“表现出众企业的数量”）。

虽然表现出众的企业在真正做到有效保护这些环境方面也有很长的路要走，但他们确实比同行企业更好地掌握了要领。47% 表现出众的企业已经创建了正式的网络安全计划，用于建立、管理和更新所需的 IIoT 网络安全工具、流程和技能，而其他汽车企业中只有 10% 做到了这一点（见图 4）。

图 4

理解 IIoT 网络安全并采用正式的网络安全计划



来源: IBM 商业价值研究院对标分析调研，2018 年，表现出众的企业：n=76；其他汽车企业 n=115。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。注：本图和其他图中提及的“表现出众的企业”包括所有受访行业，其中有来自汽车行业的 20 家企业。提及的“其他汽车企业”包括另外 115 家汽车企业，不包含 20 家表现出众的企业。

表现出众企业的数量

我们所调研的各个行业中都有表现出众的企业，包括汽车业。在受访的 700 家企业中，有 76 家属于这一类，其中包括 20 家汽车企业。这组企业以下所有三个指标的表现都排名前四分之一：

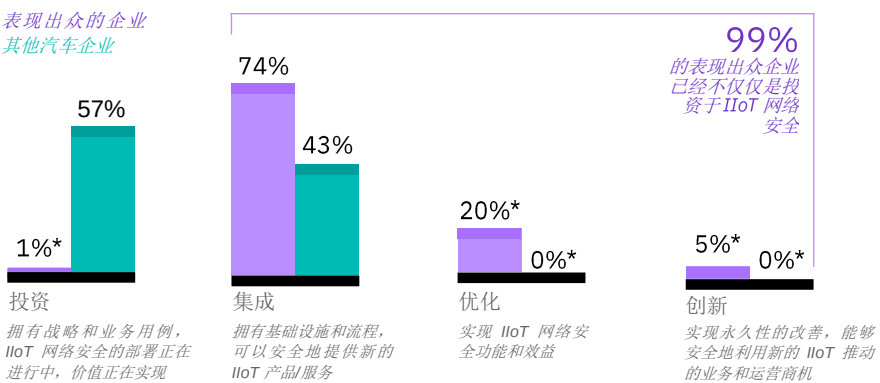
1. 由安全技术措施解决的已知 IIoT 漏洞的百分比。
2. 发现和检测 IIoT 网络安全事件的周期时间。这排除了驻留时间（即成功入侵和发现入侵之间的时间）。
3. 应对 IIoT 网络安全事件并从中恢复的周期时间。

出于本次调研的目的，提及的“表现出众的企业”涵盖所有受访行业，包括来自汽车行业的 20 家企业。提及的“其他汽车企业”包括另外 115 家汽车企业，不包含 20 家表现出众的企业。

表现出众的企业还以更快的速度将 IIoT 集成到业务和运营流程中（见图 5）。20% 表现出众的企业优化了 IIoT 网络安全功能并实现了效益，而其他汽车企业无一做到这一点。另外，5% 表现出众的企业实际上正在进行基于 IIoT 网络安全集成的创新。

图 5

IIoT 网络安全集成成熟度

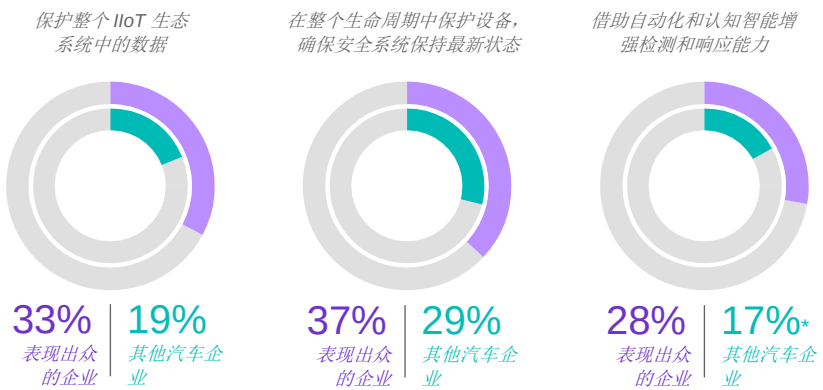


来源: IBM 商业价值研究院对标分析调研，2018 年，表现出众的企业：n=76；其他汽车企业 n=115。计数较低 (n<20) 在统计学上不具有可靠性，但与其余受访者做比较时可以视作方向性推论。

在使用网络安全解决方案保护数据和设备，以及使用自动化和认知技术检测和响应安全威胁方面，表现出众的企业在三个方面与其他企业有所区别（见图 6）。

图 6

表现出众企业的优势



来源：IBM 商业价值研究院对标分析调研，2018 年，表现出众的企业：n=76；其他汽车企业 n=115。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。

*保护整个 IIoT 生态系统中的数据。*企业行业供应链中共享了大量的敏感数据和知识产权 (IP)。如果这些数据泄露或被盗，可能会将企业的未来业务置于风险中。值得注意的是，33% 表现出众的企业与 19% 的其他汽车企业在实施特定网络安全解决方案方面处于领先地位。

*在整个生命周期中保护设备；实时更新安全系统。*不受保护的传感器和设备会将操作技术 (OT)/IIoT 网络暴露在网络攻击之下，这可能会带来灾难性的实际损害和经济损失。37% 表现出众的企业能够充分保护其 IIoT 设备，相比之下，其他汽车企业中这一比例为 29%。

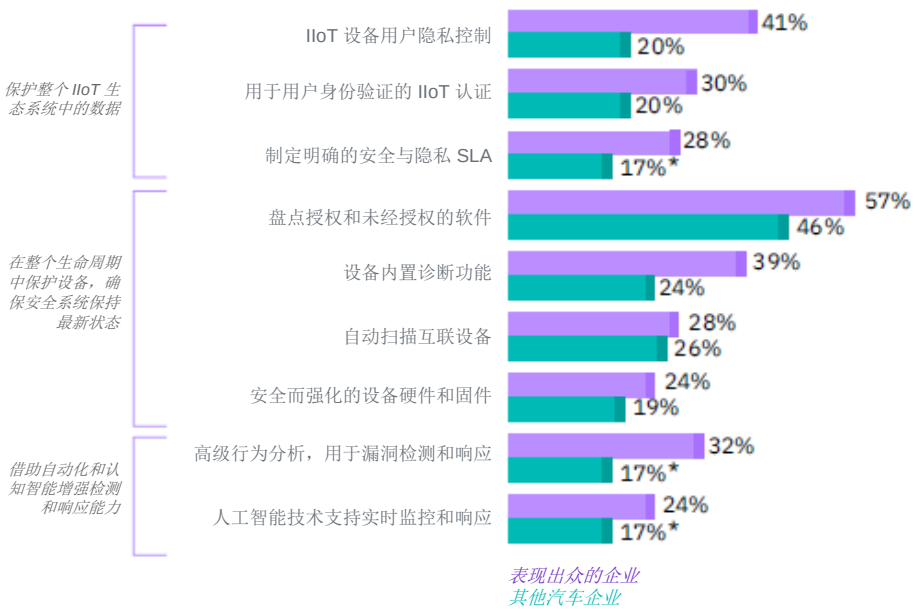
*借助自动化和认知智能增强检测和响应能力。*保护和预防并不能解决所有问题。企业必须部署适当的系统，用于检测漏洞和减轻损害。传统的检测系统旨在解决已知的攻击和威胁载体以及漏洞。认知能力，比如人工智能 (AI)、机器学习和高级行为分析，均有助于处理未来可能出现和被利用的“未知状况”。28% 表现出众的企业在将这些实践结合使用方面处于领先，而其他汽车企业的这一比例为 17%。

必要实践

表现出众的企业将基于风险与合规的方法应用于安全领域，重点关注九项实践（见图 7）。

图 7

表现出众的企业部署的九项独具特色的安全实践



来源: IBM 商业价值研究院对标分析调研，2018 年，表现出众的企业：n=76；其他汽车企业 n=115。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。

保护整个 IIoT 生态系统中的数据

对于汽车企业而言，与 IIoT 相关的最大风险是敏感数据的外泄。排名第一的事故类型是数据泄露。在该行业的 IIoT 网络安全事故中，它占了四分之一以上（OEM 占 32%，供应商占 28%）。考虑以下三种实践，有助于保护整个 IIoT 生态系统中的数据：

1. *实施 IIoT 设备用户隐私控制。*如果使用数据可以链接到设备，那么用户就可以推断出有关公司生产和流程的机密信息。[3] 41% 的表现出众企业和 20% 的其他汽车企业已经实施了控制措施，允许用户指定其数据在设备上的存储方式，以及第三方的使用和共享方式。类似的策略在其他情况下也很重要，比如所有权的变更。[4]
2. *针对用户身份验证实施 IIoT 认证。*30% 的表现出众企业和 20% 的其他汽车企业处于采用这种实践的高级阶段。验证 IIoT 设备身份的能力至关重要，特别是对于设备通常无人值守的 IIoT 机器对机器 (M2M) 场景。[5]
3. *定义明确的安全与隐私服务级别协议 (SLA)。*28% 的表现出众企业和 17% 的其他汽车企业通过这种方式来监控和执行安全要求。为了帮助阻止内部攻击和防止信息被盗或泄露，实施对数据的受控访问。了解谁被授予访问敏感功能或数据的权限。更密切地监视和审计这些特权用户的行动。

在整个生命周期中保护设备，实时更新安全系统

在受访汽车行业的高管中，有超过三分之一的人表示，设备和传感器是 IIoT 部署中最容易受到攻击的部分。几乎一半的受访者表示，对互联对象应用软件补丁是实施保护所面临的最大挑战。保护设备的四项实践包括：

1. *盘点授权和未获授权的软件*。57% 的表现出众企业和 46% 的其他汽车企业在这一领域一直很活跃。控制用于驱动 IIoT 组件的软件版本、审查与版本控制相关的威胁和建立安全基线，这三点至关重要。实施这些举措的同时，还应深入了解终端 — 它们有什么功能、与谁通信。必须分析每个终端，然后将其添加到资产库存清单中以进行监控。[6]
2. *部署内置了诊断功能的 IIoT 设备*。39% 的表现出众企业已经部署了相关设备，用于检测因零部件失效或篡改行为而导致的故障，而在其他汽车企业中，这一比例为 24%。IIoT 终端通常能够在恶劣环境中长时间运行，不需要人工干预。虽然这些终端的安全性和隐私性非常重要，但是在硬件和软件中添加加密安全功能的机会通常很有限。[7]

3. *自动扫描互联设备*。持续进行漏洞评估和补救也非常重要。表现出众的企业和其他一些汽车企业已经实施了相关策略，用于解决扫描和补救问题，他们基本处于同一水平。然而，进行主动漏洞扫描会对工业控制系统 (ICS) 网络通信造成不利影响，从而影响产品和系统的可用性。如果自动化扫描不可行，那么需要使用被动监控工具。[8]

4. *部署安全而强化的设备硬件和固件*。更换设备往往成本高昂。此外，较新的设备也可能无法提供更高的安全性。尽管每天都要面对更新设备的固有挑战，企业仍需要始终如一地安装配套的补丁和更新。对于旧设备而言，这一点尤为重要，因为许多设备都存在安全性不足的情况。[9] 所有受访企业高管都意识到了这个问题，并在一定程度上给予关注。而表现出众企业 (24%) 在实施这一举措方面略微领先于其他汽车企业 (19%)。

增强检测和响应能力

保护和预防措施并不能解决所有问题，安全地开发和部署的系统也不能保证万无一失。攻击者不断寻找新的方法来渗透系统，因此企业必须建立自动机制，持续检测和修复漏洞。

网络安全资源十分有限，这是可以理解的，所以汽车企业需要通过人工智能和自动化技术来实施检测过程，减少由人员进行的威胁检测工作（请参阅侧边栏“通过自动化减轻损失”）。通过定义敏感数据和资产、网络分段和云服务，可以对自定义警报进行系统优先级排序。采用由人工智能支持的威胁检测和补救措施的两项实践是：

1. *应用高级行为分析，用于漏洞检测和响应。*32% 的表现出众企业已经具备用户行为分析能力，可以进行机器学习，而在其他汽车企业中的这一比例仅为 17%。人工智能支持的威胁检测可以实现企业范围的应用，发现异常用户活动，并对风险进行优先排序。在应用机器学习以自动执行自适应模型，跟踪所确定的正常行为方面，表现出众的企业也领先于其他汽车企业。这种方法可以跟踪正常的行为模式，并标记可能表明出现新的威胁迹象的异常活动。
2. *实施人工智能技术，支持实时安全监控和响应。*在执行这个实践方面，表现出众的企业略高于其他汽车企业，比例分别为 24% 和 17%。如果企业能够应用数据驱动的技术，创建实时的外部和内部威胁情报源，就可以更快速地检测和修复问题。

通过自动化减轻损失[10]

Ponemon 近期报告称，完全部署安全自动化解决方案的企业，数据泄露的平均成本比没有部署的企业要低 35%。

安全自动化是指实施安全技术，增强或取代人为干预，更有效地发现和控制网络攻击或漏洞。此类技术依赖于人工智能、机器学习、分析以及指挥与自动化管理技术。

IIoT 需要 IT 与 OT 融合。这就带来了复杂性和一系列独特的风险。IIoT 技术必须得到妥善的保护，这一点至关重要。否则，它们所带来的运营和财务方面的直接效益可能会以企业的未来发展为代价。

制定明确的 IIoT 安全策略。将安全实践与企业更广泛的风险框架结合起来，并将安全技术整合到运营流程中。积极采取行动。平衡预防与检测。使安全能力“智能化”，能够应对当前和未来的高级威胁以及未知威胁。做好充分准备，在出现漏洞时迅速修复。未雨绸缪，提前准备好应对措施和沟通计划。

您的企业是否面临风险？

您的 IIoT 网络安全计划如何解决风险管理与合规问题？

您如何将 IIoT 网络安全整合到业务和运营流程中？

您如何帮助员工深入了解 IIoT 网络安全运营？

为了让企业做好准备，您会进行哪些类型的网络安全漏洞模拟？

您如何确保了解企业最具价值的资产和最危险的漏洞，提供指导，智能、有效地对风险划分优先级？

相关 IBV 出版物

Guiseppe Serio 与 Ben Stanley 合著。“加速车辆信息安全：赢得车辆完整性和数据隐私竞争”，IBM 商业价值研究院，2017 年 1 月。
https://www.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=GBE03797CNZH&dd=yes&

Tim Hahn、Marcel Kisch 与 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/common/ssi/cgi-bin/ssialias?htmlfid=62013962CNZH&dd=yes&

“智能互联 — 借助智能物联网重塑企业”，全球最高管理层调研（第 19 期），IBM 商业价值研究院，2018 年 1 月。
https://www.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=32012632CNZH&dd=yes&

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。

从应用商店下载免费“IBM IBV”应用，即可在手机或平板电脑上访问 IBM 商业价值研究院执行报告。

访问 IBM 商业价值研究院中国网站，免费下载研究报告: http://www-935.ibm.com/services/cn/gbs/ibv/

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 商业价值研究院隶属于 IBM 服务部，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。

作者

Giuseppe Serio 是 IBM 全球汽车、航空航天与国防行业网络安全解决方案负责人，拥有 20 多年的丰富经验。他主要负责与客户讨论各种信息安全项目和信息安全挑战，包括互联汽车的信息安全问题。他与其他 IBM 职能部门密切合作，包括 IBM 研究院、安全部门和物联网业务部门，共同开发和调整安全解决方案，使之适应特定行业的需求。Giuseppe 的联系方式为 giuseppe.serio@de.ibm.com，可访问他的 LinkedIn 主页：linkedin.com/in/giuseppe-serio-183582

Ben Stanley 是 IBM 商业价值研究院的汽车行业调研主管。他负责为 IBM 汽车行业事务开发思想领导力和战略业务洞察。Ben 拥有超过 40 年的汽车制造业工作经验，在业务战略和业务模式创新领域，与全球多家主要的汽车行业客户合作。Ben 的联系方式为 ben.stanley@us.ibm.com，可访问他的 LinkedIn 主页：linkedin.com/in/benjamintstanley

Lisa-Giane Fisher 是 IBM 商业价值研究院中东和非洲对标分析负责人。她主要负责保修和物联网安全对标分析，并与 IBM 行业专家和美国生产力与质量中心 (APQC) 合作开发并维护行业流程框架。Lisa 拥有超过 10 年的咨询和跨学科团队管理经验，能够跨多个行业交付复杂的 IT 项目。Lisa 的联系方式为 lfisher@za.ibm.com，可访问她的 LinkedIn 主页：linkedin.com/in/lisa-giane-fisher

备注和参考资料

1 Serio, Guiseppe and Ben Stanley. “Accelerating security: Winning the race to vehicle integrity and data privacy.” IBM Institute for Business Value. January 2017. https://www-935.ibm.com/services/us/gbs/thoughtleadership/acceleratesecurity/

2 “Attacks on Industrial Control Systems.”IBM Security.2015. http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=SEL03046USEN&attachment=SEL03046USEN.PDF; “TRISIS/TRITON.”New Jersey Cybersecurity & Communications Integration Cell. Dec. 14, 2017. https://www.cyber.nj.gov/threat-profiles/ics-malware-variants/triton

3 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

4 Maxim, Merritt. “TechRadar™: Internet Of Things Security, Q1 2017.” Forrester. January 19, 2017. https://www.forrester.com/report/TechRadar+Internet+Of+Things+Security+Q1+2017/-/E-RES117394

5 Ibid.

6 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/

7 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

8 “CIS Controls Version 7 Implementation Guide for Industrial Control Systems.”Center for Internet Security.2018. https://www.cisecurity.org/white-papers/cis-controls-implementation-guide-for-industrial-control-systems/

9 Grau, Alan. “What’s the Difference Between Device Hardening and Security Appliances?” Electronic Design. August 3, 2017. https://www.electronicdesign.com/industrial-automation/what-s-difference-between-device-hardening-and-security-appliances

10 “2018 Cost of a Data Breach Study: Global Overview.”Benchmark research sponsored by IBM Security. Independently conducted by Ponemon Institute LLC. July 2018. https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=55017055USEN

© Copyright IBM Corporation 2018

IBM Corporation
New Orchard Road
Armonk, NY 10504

美国出品
2018 年 9 月

IBM、IBM 徽标、ibm.com 和 Watson 是 International Business Machines Corp. 在世界各地司法辖区的注册商标。其他产品和服务名称可能是 IBM 或其他公司的商标。Web 站点 www.ibm.com/legal/copytrade.shtml 上的“Copyright and trademark information”部分中包含了 IBM 商标的最新列表。

本文档为自最初公布日期起的最新版本，IBM 可随时对其进行修改。IBM 并不一定在开展业务的所有国家或地区提供所有产品或服务。

本文档内的信息“按现状”提供，不附有任何种类（无论明示还是默示）的保证，包括不附有关于适销性、适用于某种特定用途的任何保证以及非侵权的任何保证或条件。IBM 产品根据其提供时所依据协议条款和条件获得保证。

本报告的目的仅为提供通用指南。它并不旨在代替详尽的研究或专业判断依据。由于使用本出版物对任何企业或个人所造成的损失，IBM 概不负责。

本报告中使用的数据可能源自第三方，IBM 并不独立核实、验证或审计此类数据。此类数据使用的结果均为“按现状”提供，IBM 不作出任何明示或默示的声明或保证。

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

