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

对标分析报告

电子行业

IBM 的能力

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贸然连接到互联网，不但会带来风险，而且代价可能十分沉重。一旦网络攻击成功入侵 IoT 支持的电子行业运营环境，很可能会导致灾难性的后果。但也不必过分担心，许多风险都可以避免或缓解。IBM 可以帮助电子行业的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，帮助保护设备和生产线，采用新型服务为平台和生态系统提供支持。我们既拥有丰富的制造业经验，也具备深厚的全球电子行业专业知识，完全有能力保护您的资产和流程，同时提升产品质量。IBM 应用认知方法，帮助降低安全风险。欲知详情，敬请访问 **ibm.com**/industries/electronics。

本报告亮点

电子行业中工业物联网 (IIoT) 的网络安全风险与采用进展情况

先行者在保护 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

电子行业期待加强网络安全

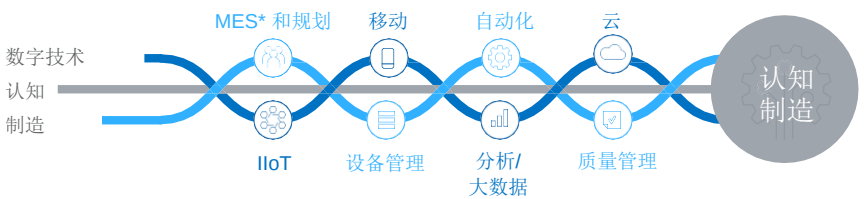
互联消费者设备的安全问题备受关注。但是，电子企业还必须密切关注工业系统的安全，以便能够顺利制造各种零部件以及科技含量不断提高的产品。“智能工业产品”的生产流程也必须实施有效的网络安全措施，否则可能使企业的整个生态系统面临风险。我们的研究发现，80% 的电子企业在工厂和装配线上实施了工业物联网 (IIoT) 技术，但没有充分评估风险或准备有效的应对措施。电子企业需要具备网络安全能力，能够以认知方式自动适应所处环境，持续发现、缓解和预防风险。

危机四伏

工厂大门基本上都会上锁，是吧？但电子制造商的智能设备和自动化流程仍可能会陷入更危险的境地。制造工厂的物联化和互联化程度日益提高，逐步向信息物理系统转型，而 IIoT 逐渐成为认知制造的核心组成部分（见图 1）。IIoT 设备和传感器嵌入实体资产，提供有关系统运行的数据。分析这些数据后，企业可以更有效地掌握制造流程的运行情况，揭示新的商机和运营机遇。[1]

图 1

IIoT 技术是实现智慧制造的基本推动力量。



*来源：IBM 服务部。*制造执行系统*

82%

的受访电子企业未充分评估风险就贸然部署 IIoT 技术

91%

的受访电子企业没有定期进行 IIoT 网络安全评估

82%

的受访电子企业没有正式制定 IIoT 网络安全计划

制造运营是电子行业价值链中成本最高的环节之一。虽然 IIoT 可提供洞察，但也可能增加潜在的网络攻击风险并对很多方面造成损害。每一个环节都会暴露弱点，为非法入侵创造新的可乘之机。无论是网络黑客、竞争对手、从事商业间谍活动的国家/地区还是心怀不满的员工，一旦发起攻击，损失可能直线攀升。由此造成的风险可能包括设备故障、关键数据丢失、企业声誉受损，甚至导致人身伤害和死亡。

IIoT 技术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。由于每台机器均与其他 IIoT 设备相连，因而都是“系统之系统”的一部分。技术扩展（如 5G）提供了承载海量数据所需的基础架构，很可能扩大 IIoT 技术的应用范围。[2] 但是，攻击面也将随之扩大。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子系统，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。

设想一下，一家电子品制造商采用安全物联化 (SIS) 控制器从工业设备中读取数据，帮助确保机器正常运转。一旦这些系统遭到破坏，很可能实际损坏机器，中断业务运营。事实上，2017 年 12 月，犯罪分子借助 Triton/Trisis 恶意软件，利用一家大型电力公司的 Triconex/Tricon 安全系统固件的零日漏洞实施了攻击。此次事故导致应急保护系统出现故障（见图 2）。[3] 这不仅可能导致资产损失，电力网络本身也面临风险。

图 2

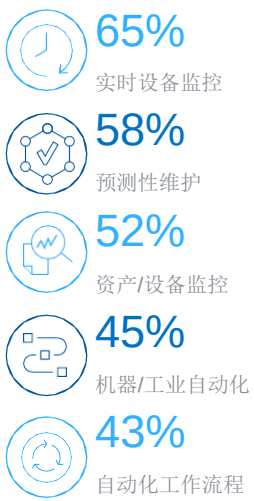
对工业控制系统 (ICS) 的攻击 — 简图[4]

企业需要具备卓越的网络安全能力，不仅要保护自身资产和网络，还要对整个 IIoT 生态系统实施防护。此外，必须能够在发生安全违规事件时快速有效地做出响应，这一点同样十分重要。几乎所有类型的企业都必须与时俱进，紧跟不断发展的 IIoT 威胁形势。

为了更好地理解工业物联网的安全风险和影响，IBM 商业价值研究院 (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 家企业（其中 269 家是电子企业）。所有企业均在工厂中实施了 IIoT。

图 3

IIoT 技术在电子产品工厂和装配线上的前五大应用



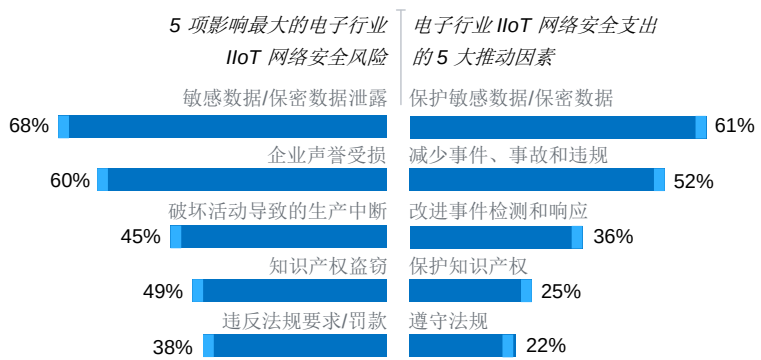
n=269。

实时设备监控和预测性维护是最常见的两大应用形式，占比分别为 65% 和 58%（见图 3）。机器和流程自动化应用也很常见，运用 IIoT 技术实现机器和工作流程自动化的企业比例分别为 45% 和 43%。

电子企业认识到了网络安全风险，相应地调整安全支出（见图 4）。但他们并不太清楚如何将多种 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 4

IIoT 网络安全风险与安全支出推动因素对比



n=269。

随着新技术快速得到采用，如果不优先部署适当的网络安全保护措施，企业必将面临严重风险：

1. *敏感数据泄露。*受访高管认为这是他们面临的最大风险。68% 的高管敏锐地意识到，客户和员工数据、供应商/合作伙伴知识产权与合同等敏感数据或保密数据的泄露可能会对企业发展产生非常不利的影响。后果可能十分严重：收入和投资损失；丧失率先进入市场的优势；将业务拱手让给竞争对手或造假者。

2. *企业声誉受损，公众信心丧失。*60% 的高管认为，安全漏洞可能会对电子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可能受到损害，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。*45% 的受访高管表示，这种风险非常巨大，可能会导致物理设备损坏及车间员工受伤。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（见第 3 页图 2）。入侵者可能修改机器软件程序或监视控制和数据采集系统 (SCADA)。

4. *知识产权 (IP) 盗窃。*IP 是推动未来发展的关键。工程计划和专有制造流程等商业机密是竞争优势的重要来源。40% 的电子企业认识到 IP 盗窃可能对未来发展产生的严重影响。哪怕一次微不足道的入侵也可能使产品设计 IP 陷入风险。
5. *违反法规要求。*2018 年 5 月生效的《通用数据保护条例》(GDPR) 及用于监管产品和生产流程的环保法规增加了不合规的风险。38% 的受访高管表示，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。虽然 GDPR 保护个人数据，但实际运营政策还要求重点关注排放、能源使用、资源可回收性和资产/废物处理等方面。

从支出的角度来看，61% 的电子行业受访高管表示，保护敏感数据是 IIoT 网络安全开支的主要推动因素。超过 50% 的受访高管还将减少事件、事故和违规行为视为主要推动因素。

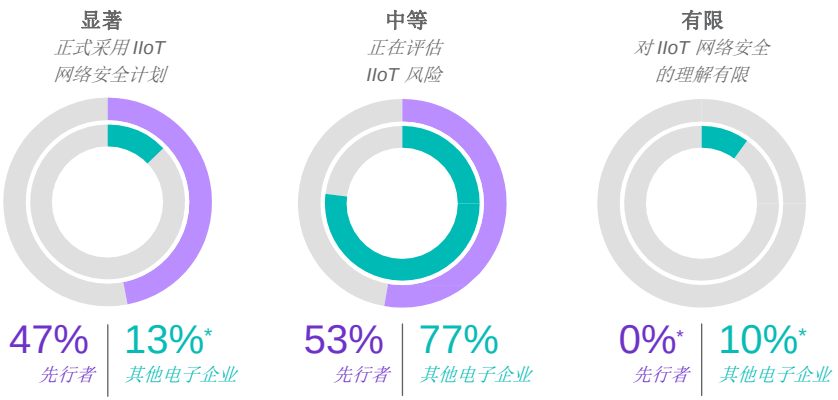
意识和行动：先行者抢先一步，积极实现安全环境

我们发现了一组先行者，他们已在采取措施保护 IIoT 环境（请参阅侧边栏“先行者的数量”）。

虽然先行者距离真正保护自己的环境还存在一些差距，但在掌握 IIoT 部署以及互联化工业控制系统 (ICS) 的安全要求方面，确实明显领先于同行企业。47% 的先行者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，而其他电子企业中只有 13% 做到了这一点（见图 5）。

图 5

理解 IIoT 网络安全并采用正式的网络安全计划



先行者 n=76；其他电子企业 n=233。

**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：有关更多信息，请参阅侧边栏。

先行者的数量

我们所调研的各个行业中都有先行者，包括电子行业。在受访的 700 家企业中，有 76 家属于这一类，其中包括 36 家电子企业。这组企业以下所有三个指标的表现都排名前四分之一：

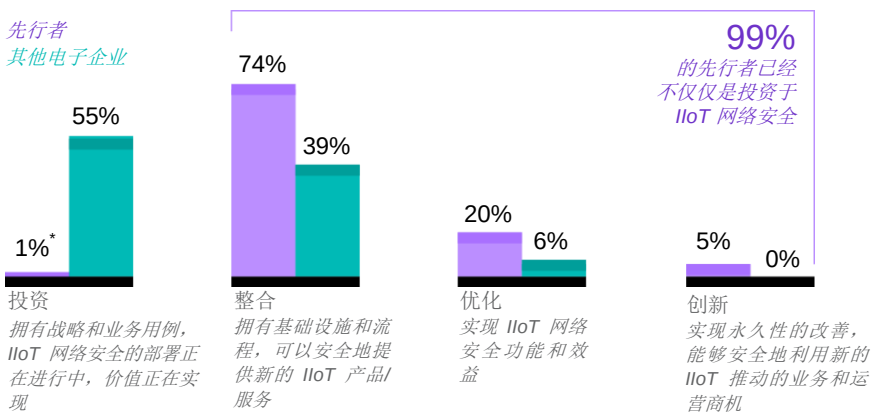
1. 由安全技术措施解决的已知 IIoT 漏洞的百分比。
2. 发现/检测 IIoT 网络安全事件的周期时间。这排除了驻留时间（即成功入侵和发现入侵之间的时间）。
3. 应对 IIoT 网络安全事件并从中恢复的周期时间。

出于本次调研的目的，提及的“先行者”涵盖所有受访行业，包括来自电子行业的 36 家企业。提及的“其他电子企业”包括另外 233 家电子企业，不包含 36 家先行者。

先行者在将 IIoT 网络安全整合至业务流程和运营流程方面更加成熟，99% 的企业不再单纯投资这一领域（见图 6）。20% 的先行者优化了 IIoT 网络安全功能并实现了效益，而其他电子企业中只有 6% 做到了这一点。

图 6

IIoT 网络安全集成成熟度



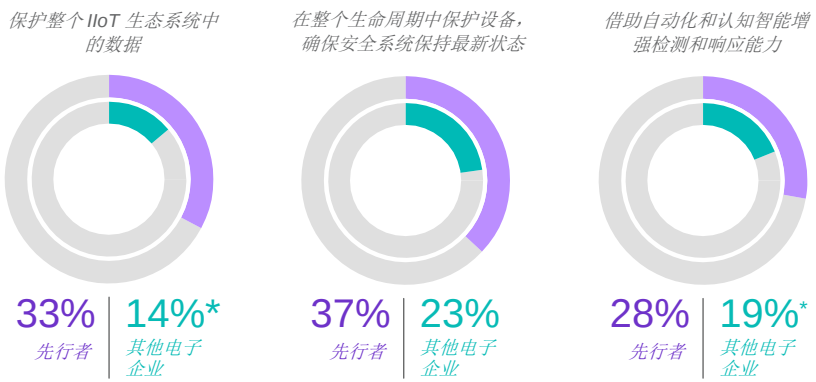
先行者 n=76；其他电子企业 n=233。

**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，先行者在以下三个方面与其他企业有所区别（见图 7）：

图 7

先行者具有明显的差异化优势



先行者 n=76，其他电子企业 n=233。

**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。*电子行业供应链中共享了海量的敏感数据和 IP，一旦泄露或被盗，可能导致企业的未来业务及其供应链与合作伙伴面临风险。值得注意的是，33% 的先行者与 14% 的其他电子企业在实施特定网络安全解决方案方面处于领先地位。

*保护 IIoT 设备；实时更新安全系统。*不受保护的传感器和设备会将 IT-OT（运营技术）-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% 的先行者与 23% 的其他电子企业在保护 IIoT 设备方面处于领先地位。

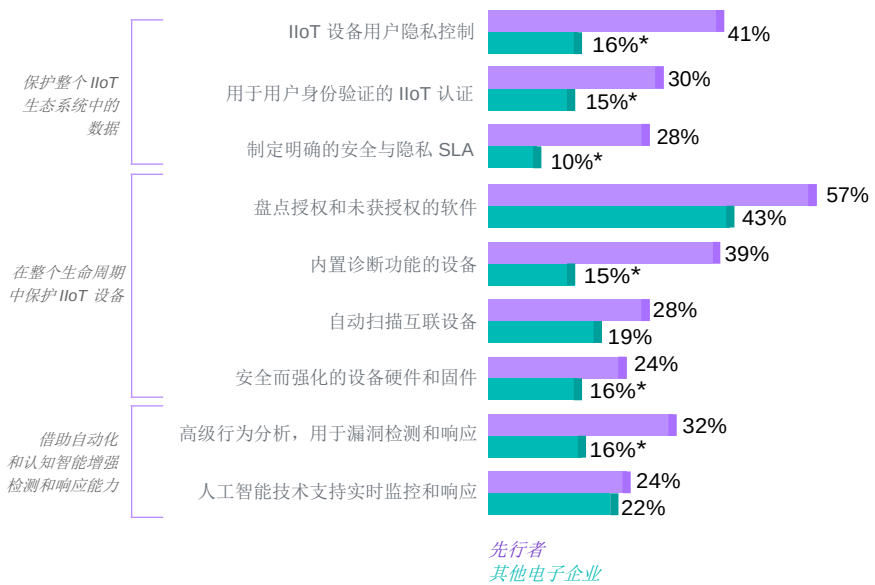
*借助自动化和认知智能增强检测和响应能力。*保护和预防并不能解决所有问题。部署系统以检测漏洞，减轻损害。传统的检测系统旨在解决已知的攻击、威胁载体以及漏洞。认知能力，比如人工智能 (AI)、机器学习和高级行为分析，均有助于处理未来可能出现和被利用的“未知状况”。28% 的先行者在结合使用这些实践方面处于领先，而其他电子企业的这一比例为 19%。

建议：必要实践

先行者将基于风险与合规的方法应用于安全领域，重点关注九项特定实践（见图 8）。

图 8

先行者采用独具特色的安全实践



先行者 n=76；其他电子企业 n=233。

**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。*

保护企业自身、生态系统和客户：SLA 是帮助企业取得成功和确保安全的关键任务。了解谁被授予访问敏感功能或数据的权限。

保护整个 IIoT 生态系统中的数据

对于电子企业而言，与 IIoT 相关的最大风险是敏感数据的外泄。事实上，在电子行业发生的各类 IIoT 网络安全事件（疑似入侵、企图入侵和成功入侵）中，数据泄露排名榜首，占事件总数的 26%。以下实践可能有所帮助：

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，则可以推断出有关公司生产和流程的机密信息。[5] 为解决这一问题，企业应实施控制措施，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。[6]
2. *针对用户身份验证实施 IIoT 认证。*处于采用这种实践的高级阶段的先行者是其他电子企业的两倍（30% 对 15%）。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。[7]
3. *定义明确的安全与隐私服务级别协议 (SLA)。*通过这种方式监控和执行安全要求的先行者是其他电子企业的近三倍（28% 对 10%）。为了遏制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。密切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

23% 的受访高管认为平台是电子行业 IIoT 部署中最容易受到攻击的部分，22% 的受访高管认为设备和传感器最容易受到攻击。为应对这一领域的关键挑战，建议采用以下四项实践：

1. *盘点授权和未获授权的软件。*控制用于驱动 IIoT 组件的软件的版本，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。[8]

2. *部署内置了诊断功能的 IIoT 设备。*先行者部署设备，用于检测因零部件失效或篡改行为而导致的故障。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。[9] 虽然这些终端的安全性和保密性非常重要，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。[10]

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。进行主动漏洞扫描会对 ICS 网络通信造成不利影响，从而影响产品和系统的可用性。如果自动化扫描不适用，那么可使用被动监控工具。[11]

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。尽管每天都应面对更新设备的固有挑战，企业仍需要始终如一地执行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。[12]

借助自动化和认知智能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。

44% 的受访高管表示，缺乏高技能网络安全人才是保护电子行业 IIoT 部署所面临的最大挑战。电子企业可实施 AI 驱动型自动化检测流程，从而减少由人员进行的威胁检测工作。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。*采用机器学习进行行为分析的先行者是其他电子企业的两倍。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，用于跟踪正常的行为模式以及标记可能表明出现新威胁迹象的异常活动方面，先行者同样遥遥领先。
2. *实施人工智能技术，支持实时安全监控和响应。*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。

IIoT 需要 IT 与 OT 融合 — 将这些监测和控制物理环境的系统整合起来。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整个生态系统的未来发展为代价。

通过自动化减轻损失 [13]

研究机构 Ponemon 近期报告称，发现并控制数据泄露事件的速度越快，产生的成本就越低。他们发现，广泛应用 IoT 设备会使每条记录泄露的平均成本提高 5 美元，而完全部署安全自动化解决方案的企业的数据泄露平均成本要比没有部署自动化的企业低 35%。

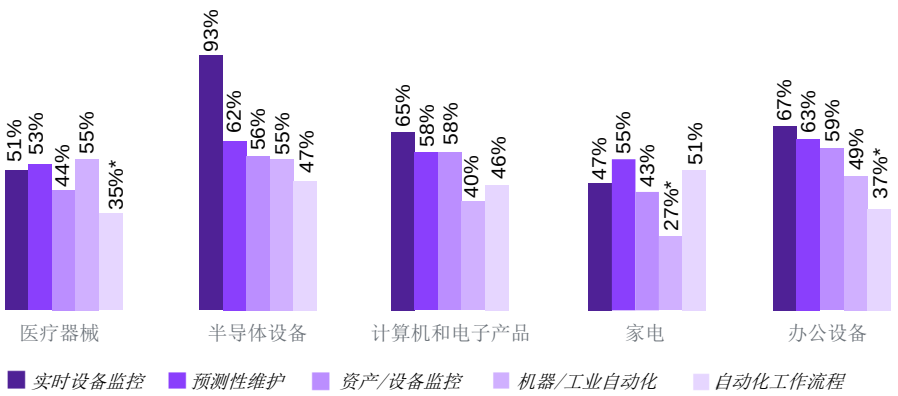
安全自动化是指实施安全技术，增强或取代人为干预，更有效地发现和控制网络攻击或漏洞。此类技术依赖于人工智能、机器学习、分析以及指挥与自动化管理技术。

行业领域观点

挑战：在建立整个电子行业广泛视角的同时，还应适度探索行业中各个领域的细微差别。然而，电子行业中各个领域存在明显差异。为掌握这些差异，IBV 针对关键问题进行了详细的领域细分，以便让高管更深入地探讨他们对 IIoT 的网络安全担忧。图 9 展示了各行业领域如何在工厂和装配线中应用 IIoT 技术。

图 9

IIoT 在电子产业各个领域的工厂和装配线上的前五大应用



n=269。

**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。*

下表汇总了电子行业各个领域面临的与 IIoT 相关的三大主要漏洞、威胁和事故。

前三名		医疗器械制造商	半导体设备制造商	计算机和电子产品制造商	家电制造商	办公设备制造商
IIoT 漏洞	**1**	**24%** IoT 平台	**22%** IoT 平台	**32%** IoT 平台	**37%** 基于云解决方案和 IoT 平台的应用	**27%** 设备和传感器
	2	**24%** 设备和传感器	**22%** 设备和传感器	**28%** 设备和传感器	**20%** IoT 平台	**24%** 存储在云端的数据
	3	**16%** 存储在云端的数据	**15%** 设备与网关之间的通信	**19%** 存储在云端的数据	**14%** 存储在云端的数据	**16%** IoT 平台
与 IIoT 相关的威胁	**1**	**56%** 信息收集、数据泄露	**55%** 信息收集、数据泄露	**44%** 信息收集、数据泄露	**69%** 未经授权的访问	**45%** 未经授权的访问
	2	**42%** DOS/DDoS 攻击	**45%** 未经授权的访问	**40%** 未经授权的访问	**51%** 访问权或凭证滥用	**43%** DOS/DDoS 攻击
	3	**38%** 未经授权的访问	**42%** DOS/DDoS 攻击	**30%** DOS/DDoS 攻击	**45%** 信息收集、数据泄露	**35%** 信息收集、数据泄露
IIoT 网络安全事故	**1**	**25%** IP 遭窃/数据泄露	**28%** IP 遭窃/数据泄露	**26%** IP 遭窃/数据泄露	**32%** 内部盗窃/欺诈	**27%** IP 遭窃/数据泄露
	2	**23%** 隐私泄露	**19%** 内部盗窃/欺诈	**21%** 隐私泄露	**23%** IP 遭窃/数据泄露	**23%** 内部盗窃/欺诈
	3	**19%** 内部盗窃/欺诈	**18%** 隐私泄露	**16%** 内部盗窃/欺诈	**21%** 隐私泄露	**17%** 隐私泄露

IIoT 网络安全重要结论

- 制定明确的 IIoT 安全战略。
- 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”和自动化，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，提前制定应对措施和沟通计划。

相关 IBV 出版物

Cristene Gonzalez-Wertz、John Constantopoulos、Qin XK Deng 、Hiroshi Yamamato 与 Quentin Samelson 合著，“认知制造技术对电子行业至关重要：助力下一代生产模式取得成功”，IBM 商业价值研究院，2017 年 2 月。
https://www.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=GBE03806CNZH&dd=yes&

Hahn Tim、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&

您是否准备好按优先顺序处理网络安全问题？

- 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、有效地对威胁划分优先级？
- 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？

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

Cristene Gonzalez-Wertz 是 IBM 商业价值研究院的电子、环保、能源与公用事业行业领域的主管。她负责为客户提供人工智能、分析技术、物联网、安全性和客户体验方面的技术、趋势和战略定位建议。Cristene 提供新价值机遇方面的指导，尤其擅长数据化经济。她的联系方式为 cristeneg@us.ibm.com，可访问她的 LinkedIn 主页：https://www.linkedin.com/in/cjgw1/

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 行业专家合作开发并维护行业流程框架。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

Peter Xu 目前担任 IBM 全球电子行业首席技术官。在过去 20 年里，Peter 一直致力于新兴的信息、运营和通信技术交叉领域的工作。他擅长运用深度行业洞察和广博的第一手技术专业知识，指导客户应对复杂的业务挑战。Peter 的联系方式为 peteryxu@us.ibm.com，可访问他的 LinkedIn 主页：linkedin.com/in/peteryxu/

Martin Borrett 是 IBM Security 欧洲的首席技术官，负责向高级客户提供与安全相关的政策、业务、技术和架构问题的建议。Martin 领导 IBM 安全蓝图工作，并且参与编著了两部 IBM 红皮书。他是英国计算机协会会员、特许工程师 (CEng)，还是英国工程技术学会成员。Martin 的联系方式为 borretm@uk.ibm.com，可访问他的 LinkedIn 主页：linkedin.com/in/martinborrett/

备注和参考资料

1 Gonzalez-Wertz, Cristene, John Constantopoulos, Qin XK Deng, Hiroshi Yamamato and Quentin Samelson. “Why cognitive manufacturing matters in electronics: Activating the next generation of production.” IBM Institute for Business Value. February 2017. http://www-935.ibm.com/services/us/gbs/thoughtleadership/cognitivemanufacturing/

2 Moore, Mike. “What is 5G? Everything you need to know.” Techradar. September 2018. https://www.techradar.com/news/what-is-5g-everything-you-need-to-know

3 “TRISIS/TRITON.” New Jersey Cybersecurity and Communications Integration Cell (NJCCIC). December 24, 2017. https://www.cyber.nj.gov/threat-profiles/ics-malware-variants/triton

4 “Attacks on Industrial Control Systems.” IBM Security.2015. https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03046USEN. “TRISIS/TRITON.” New Jersey Cybersecurity & Communications Integration Cell.Dec. 14, 2017. https://www.cyber.nj.gov/threat-profiles/ics-malware-variants/triton. “Threat Landscape for Industrial Automation Systems H1 2018.” Kaspersky ICS CERT.2018. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/09/06075839/H1_2018_ICS_REPORT_v1.0_ENG_05092018.pdf

5 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

6 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

7 Ibid.

8 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/

9 “Five indisputable facts about IoT security.” IBM Security. February 2017. https://www-01.ibm.com/common/ ssi/cgi-bin/ssialias?htmlfid=SEF03018USEN&appname=skmwww

10 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

11 “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/

12 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

13 “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

IBM Corporation
New Orchard Road
Armonk, NY 10504

美国出品
2018 年 10 月

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

85020085CNZH-00