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

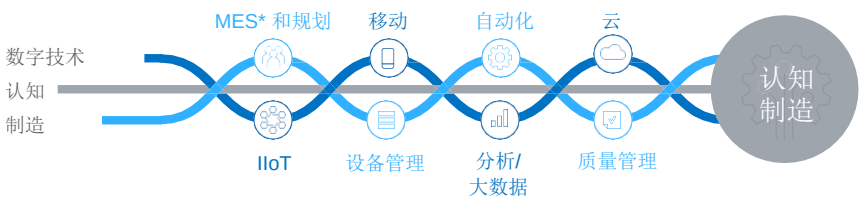
互联消费者设备的安全问题备受关注。但是，电子企业还必须密切关注工业系统的安全，以便能够顺利制造各种零部件以及科技含量不断提高的产品。“智能工业产品”的生产流程也必须实施有效的网络安全措施，否则可能使企业的整个生态系统面临风险。我们的研究发现，80% 的电子企业在工厂和装配线上实施了工业物联网 (IIoT) 技术，但没有充分评估风险或准备有效的应对措施。电子企业需要具备网络安全能力，能够以认知方式自动适应所处环境，持续发现、缓解和预防风险。

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

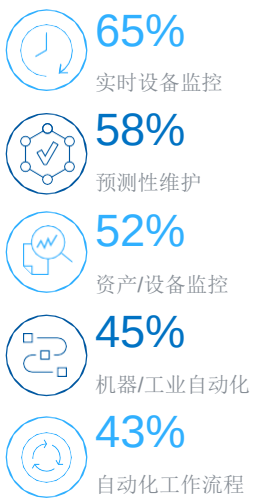
对工业控制系统 (ICS) 的攻击 — 简图[4]

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



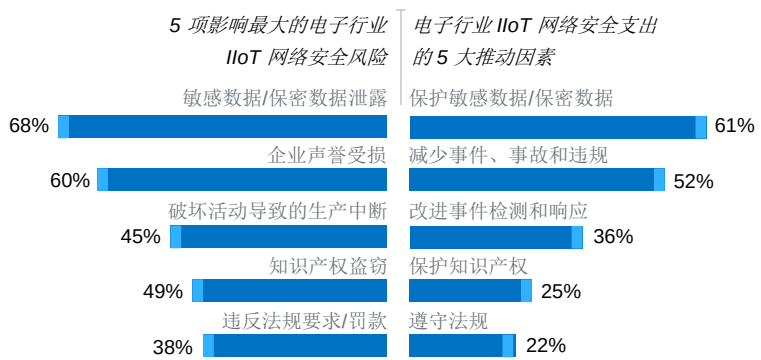
n=269。

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。

预览已结束，完整报告链接和二维码如下：

https://www.yunbaogao.cn/report/index/report?reportId=1_38812