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

实现牢不可破

物联网 (IoT) 席卷全球，无处不在。各行各业都在利用来自互联设备的数据洞察，以提高生产力，解决问题，创造新的业务机会并提升运营效率。但是风险也一并存在。安全性是许多早期物联网应用事后才考虑的问题，以致于网络漏洞百出，并可能导致工业流程发生中断、被操纵或遭遇间谍软件。但是物联网不能成为充满威胁的网络。工业和公用事业企业需要尤为注意，制定新的战略，缓解并管理网络风险。

飞行途中造飞机

物联网技术在各个行业的蓬勃发展速度令人难以置信，工业和公用事业行业也不例外。到 2020 年，物联网市场的设备安装基数预计将从 2015 年的 150 万台增长到 300 万台，到 2025 年，这一数字将增至 750 万。[1] 到 2020 年，每年生成的数据量将达到 600 ZB。[2]

工业环境物联网主要由新一代制造技术所驱动，也被称为“工业物联网 (IIoT)”。这一市场规模庞大，到 2030 年，将为全球经济带来 14 万亿美元的效益。[3] IIoT 可以利用来自机器和设备的数据，彻底转变现代工厂环境中的流程和系统。从智能计量表到传感器和警报器，公用事业行业中充斥着各种物联网设备。这些行业使用物联网跨企业边界开展实时数据分析、设备监控、预测性维护和机器自动化，也就是顺理成章的事情了。

但是，关于设备安全和漏洞的深深忧虑也不无道理。根据 IBM 商业价值研究院 (IBV) 开展的 IBM 全球最高管理层调研第 19 期报告，36% 的受访高管表示，保护物联网平台及其设备的安全是他们企业面临的首要难题。[4] 一项针对 700 位工业和公用事业行业 IT 与 OT 负责人开展的 IBV 对标分析调研发现，设备、传感器以及物联网平台是物联网部署中最脆弱的环节。[5]

物联网解决方案遍布于信息技术 (IT)、运营技术 (OT) 以及消费技术 (CT) 领域。若企业部署物联网技术的速度超过实施安全保护的速度，则会使企业暴露在比负面舆论更大的危险之下。对于工业制造、化工、石油和天然气以及公用事业行业来说，安全漏洞会导致大范围的污染、环境灾难甚至人身伤害。运营技术领域日益成为攻击目标，占所有网络攻击的 30%。[6] 在中东地区，50% 的网络攻击主要针对石油和天然气行业，对安全、生产力和效率造成了重大影响。[7]

从起步到实施

IBV 对标分析调研揭示了工业和公用事业行业目前的物联网安全状况。

大部分工业和公用事业企业都处于采用实践和保护性技术来缓解物联网安全风险的早期阶段。只有一小部分企业已经完全实施运营、技术和认知实践或特定于物联网的安全技术。[8]

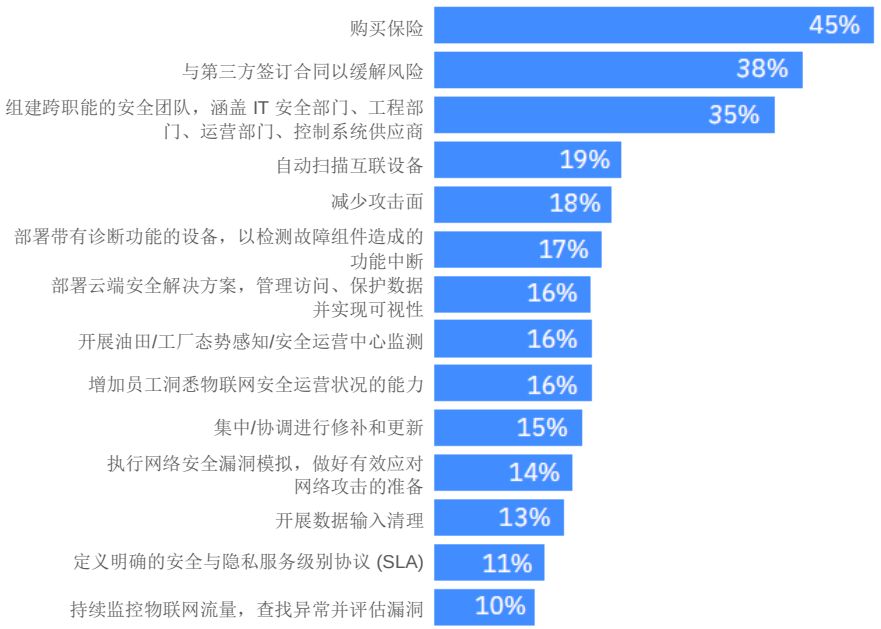
因此，大部分企业的物联网安全能力建设仍处于起步阶段（见图 1）。投资已经到位，物联网部署也在进行中，但是网络安全风险评估仍在继续，且基于特定基础。已知的问题和挑战有可能妨碍企业采取全面的物联网安全实践。这些问题包括：

- *网络安全必备技能持续短缺*。高技能人才短缺是保护物联网部署的最大挑战。落实优秀人才储备举措势在必行。除了要擅于处理 IT 网络安全风险，员工还应当做好以下准备：
  - 覆盖更多、更分散的设备
  - 处理设备安全、隐私和可靠性方面的权衡和考虑问题
  - 创建和使用自动化与持续工程、交付与集成技术，在这个更大的计算环境中提供持续的保护。

– *物联网安全意识有限。*对物联网部署所带来的风险理解不全面，再加上没有正式的物联网安全计划，导致物联网采用与保护能力之间存在差距。以 IT 为核心的安全框架和组织结构往往不足以满足物联网设备永续运行的可靠性和可预测性需求。

– *物联网安全标准发展缓慢。*已有的互联网安全中心 (CIS) 控制措施、运营和技术实践、保护性技术和物联网认证方法，必须统统得到妥善实施。CIS 控制措施包括盘清授权设备和软件，部署带有内置诊断功能与安全性能加固硬件和固件的设备。

图 1
在缓解物联网安全风险的实践方面处于高级阶段的企业

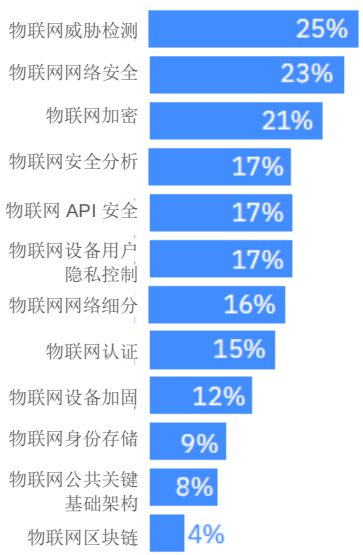


来源：IBM 商业价值研究院对标分析调研

赶上威胁增长的速度

图 2

在实施保护性技术来缓解物联网安全风险方面处于高级阶段的企业



来源：2018 年 IBM 商业价值研究院对标分析调研

物联网安全并非存在于真空环境中。企业必须遵循流程，采用实践和技术并采取措施，才能满足关键性能指标 (KPI)。为缓解物联网安全风险并提高性能，企业可以实施以下方法：

- *制定正式的物联网安全计划。*采用涵盖人员、流程和技术的卓越运营模式，建设物联网安全保护能力。增加员工洞悉物联网安全运营、IT 和 OT 的能力。新一代互联设备和服务供应商可能考虑针对软件故障和黑客可能造成的任何破坏购买保险。
- *了解每个终端及其作用和交互对象。*必须识别和注册每个物联网终端，然后将其添加到资产库存并进行监控。定义明确的 SLA，这主要依赖合作伙伴和系统集成商。组建由 IT 安全部门、工程部门、运营部门、控制系统供应商构成的跨职能安全团队。
- *了解何时以及如何主动出击。*为做好有效应对网络攻击的准备，必须执行漏洞模拟、定期的油田和工厂态势感知以及安全运营中心监测。

IBV 对标分析调研评估了受访者使用相关重要技术来实现物联网安全的情况（见图 2）。
其中包括：

- 实施加密，防御攻击，保护敏感信息安全，避免财产和设备损坏，确保员工人身安全。
- 实施网络安全和设备认证，保护物联网设备、边缘设备与后端系统和应用之间的部署。
- 开展安全分析，识别可能绕过传统安全控制措施的潜在物联网攻击和入侵。
- 执行身份和访问管理，帮助企业和服务供应商管理和保护身份和物联网设备之间的关系。

确保安全无虞

长期以来，风险一直被用于识别、评估、控制、监测和响应运营中存在的危险，包括安全方面的危险。随着工业企业快速采用物联网技术，他们也必须协调物联网安全实践与更广泛的风险框架保持一致。要想开启更加有力的安全对话，交付优化的技术解决方案，领导者可以采取以下措施：

- 在企业层面管理物联网网络安全风险。执行定期风险评估，识别物联网系统和互联生产环境中的漏洞，并制定和执行缓解潜在风险的计划。建设或增强网络安全情报能力，了解企业中易被利用的最脆弱的攻击载体。
- 了解物联网系统、标准企业 IT 系统以及运营设备之间的不同，分享 IT 和 OT 安全专业知识以提供更好的保护。在决定安全控制措施的正确优先顺序，以最大限度地缓解风险时，将这些差异考虑在内。
- 打破 IT 和 OT 组织之间的孤岛。制定跨领域的通用风险方法，管理传统上以 IT 为核心的信息处理技术和以 OT 为核心的技术，以便监测并控制信息物理系统环境。

关于对标洞察@IBV 报告

对标洞察@IBV 汇集了思想领导者关于具有新闻价值的业务和相关技术主题的看法，以及 IBM 商业价值研究院 (IBV) 对标分析团队得出的研究结果。这些报告的编制基础是与全球领先主题专家的对话，以及从 IBV 对标分析团队开展的调研中得来的相关数据。如欲了解更多信息，请联系 IBM 对标分析团队成员 Lisa-Giane Fisher：global.benchmarking@us.ibm.com。

主题专家

Tim Hahn
首席架构师
IBM 物联网安全
hahnt@us.ibm.com
linkedin.com/in/hahnt/

Marcel Kisch
IBM Security 全球能源与公用事业和制造业安全解决方案主管
marcel.kisch@de.ibm.com
linkedin.com/in/highpotential/

James Murphy
IBM Watson and Cloud Platform 全球物联网、安全性和区块链解决方案负责人
jamesmur@uk.ibm.com
linkedin.com/in/jamesmurphygb/

2018 New Orchard Road
Armonk, NY 10504

美国出品
2018 年 3 月

62013962CNZH-01

备注和参考资料

1 Columbus, Louis.“Roundup of Internet of Things forecasts and market estimates.”Forbes.2016. https://www.forbes.com/sites/louiscolumbus/2016/11/27/roundup-of-internet-of-things-forecasts-and-market-estimates-2016/#789467a8292d

2 McKendrick, Joe.“With Internet of Things and big data, 92 percent of everything we do will be in the cloud.”Forbes.2016. https://www.forbes.com/sites/joemckendrick/2016/11/13/with-internet-of-things-and-big-data-92-of-everything-we-do-will-be-in-the-cloud/#18a41ee74ed5

3 Gerbrandt, Ryan.“IIoT for Utilities:Lessons learned, opportunities ahead.”Internet of Things Institute.January 2018. http://www.ioti.com/smart-energy-and-utilities/iiot-utilities-lessons-learned-opportunities-ahead

4 Nordman, Carl, Cristene J Gonzalez-Wertz and Karen Butner.“Intelligent Connections:Reinventing enterprises with Intelligent IoT.”IBM Institute for Business Value.January 2018. https://www-935.ibm.com/services/studies/csuite/iot/

5 “Benchmarking survey.”IBM Institute for Business Value.2018.(unpublished data)

6 Menachery, Martin.“New study:Middle East oil and gas sector needs readiness boost as industrial cyber risk increases.”Arabian Oil and Gas.November 2017 .http://www.arabianoilandgas.com/article-18052-new-study-middle-east-oil-gas-sector-needs-readiness-boost-as-industrial-cyber-risk-increases/

7 Ibid.

8 “Benchmarking survey.”IBM Institute for Business Value.2018.(unpublished data)