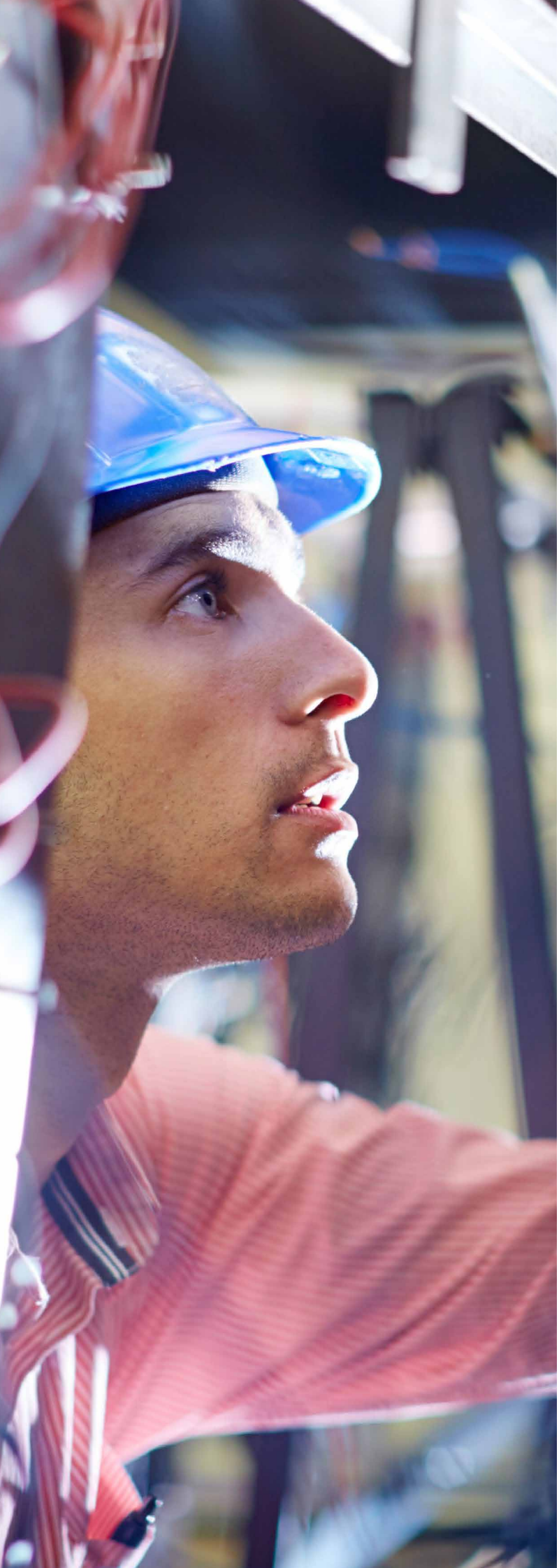


对标洞察

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

IBM

作者：Cristene Gonzalez-Wertz、Lisa-Giane Fisher、Steven Dougherty 和 Mark Holt

谈话要点

IIoT 在公用事业领域的运用

公用事业领域既是 IIoT 技术的早期采用者，也是广泛采用者。我们的调研揭示了 IIoT 技术的采用领域和方式。

网络安全之窘境

公用事业企业意识到了存在网络安全风险。但为什么他们仍难以实现全方位的 IIoT 网络安全?

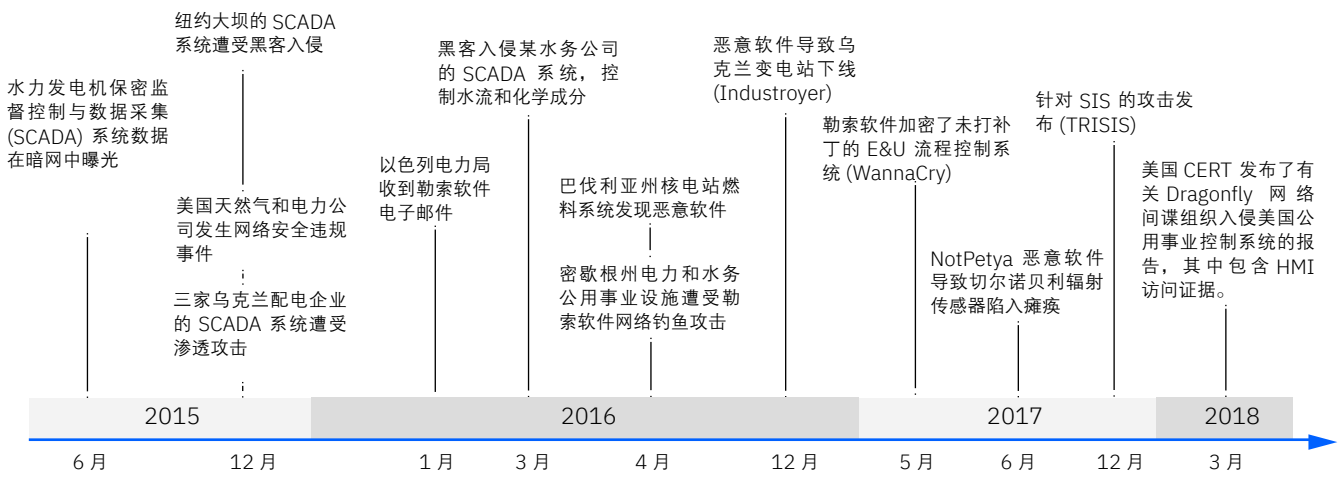
五大具体战略

了解如何通过奠定强有力的网络安全基础，运用人工智能和自动化技术，获得更先进的能力，从而实现并提高 IIoT 卫生水平。

随着工业物联网 (IIoT) 技术日益普及，自动化设备和流程变得越来越智能，而公用事业遭受网络攻击的风险也与日俱增。无论是由恐怖分子、网络黑客还是国家发动，攻击一旦成功，都可能引发毁灭性的后果。入侵核电厂和电网可能会影响电力供应，而针对供水设施的网络攻击则可能导致饮水污染或断供。公民安全、关键基础设施和环境面临严峻风险。由自动化和人工智能 (AI) 辅助实现的基本 IIoT 网络卫生成为确保公用事业运营和服务连续性的关键所在。

目前，公用事业企业利用 IIoT 技术收集数据，以监测资产，获得深入的运营洞察，同时提高效率和安全水平。然而，随着 IIoT 的扩展，破解并访问工业控制系统 (ICS) 网络的恶意行为仍在继续。针对使用 IIoT 环境的攻击目标不仅涵盖高价值资产或服务，还包括云端的关键工作负载。另外，还可能包括信息 / 实体系统中的流程控制子系统以及关键的业务、运营和消费者数据。例如，美国国土安全部 (DHS) 最近报告称，Dragonfly 间谍组织入侵了用于控制若干北美发电厂流程的 Human Machine Interfaces (HMI)。入侵系统后，该间谍组织不仅复制了配置信息，还可能破坏或控制设施。[1]

针对 ICS 网络的攻击：简图



来源：IBM Security 研究。

公用事业运营领域中的 IIoT 网络安全

70%

的公用事业企业打算部署 IIoT 技术，但他们对 IIoT 网络安全技术至多只是泛泛了解

64%

的电力企业将生产中断 / 停工及公众信心丧失视为最严重的 IIoT 网络安全风险

公用事业企业自己检测到的 IIoT 网络安全事故不到实际发生数量的

50%

为了更好地了解 IIoT 安全现状，IBM 商业价值研究院 (IBV) 与牛津经济研究院合作，对 18 个国家或地区的 700 多位工业与能源企业高管（包括 120 位公用事业高管）进行了一次调研。调研期间，所有 700 家企业全部在运营中实施了 IIoT。

研究确认，公用事业领域既是 IIoT 技术的早期采用者，也是广泛采用者。广大受访者普遍表示，所在企业主要应用 IIoT 技术发出警报、读表以及实时监测设备，因此会生成大量数据，并通过监测与控制网络传输相关数据。

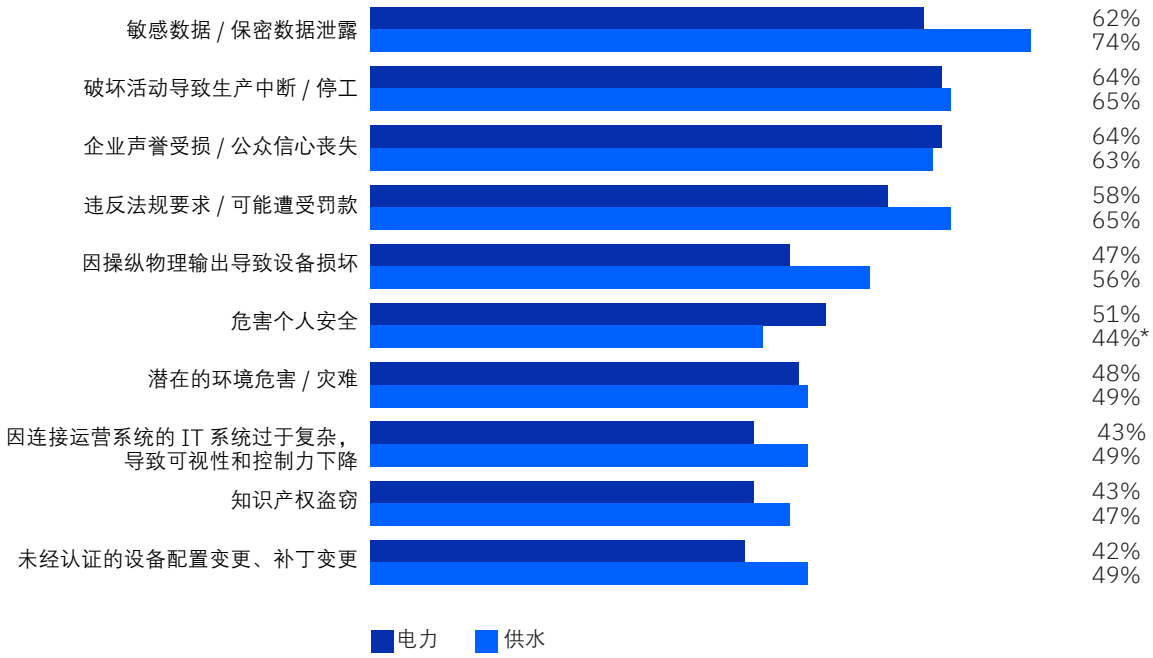
然而，公用事业企业高管对 IIoT 终端的安全倍感担忧。24% 的受访者认为设备和传感器是 IIoT 部署最薄弱的环节。另外，公用事业企业高管担心这些设备、传感器及网关上的数据未得到充分保护。12% 的公用事业企业担心云端数据的脆弱性。

公用事业领域网络攻击可能会产生严重的健康、经济、环境和心理影响。

平均而言，公用事业企业将敏感数据曝光视为影响最严重的 IIoT 相关风险。这包括计费和收入信息（来自智能电网和智能电表系统）、控制系统信息以及员工和客户数据。电力公用事业企业更担心生产中断或停工，以及由此引发的声誉损害。半数以上的公用事业企业担心监管违规和设备损坏带来的潜在影响（见图 1）。

图 1

公用事业市场：影响重大的 IIoT 网络安全风险



来源：IBM 商业价值研究院对标调研，2018 年。

n = 120；电力 = 77；供水 = 43

** 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。*

什么是网络卫生？ [2]

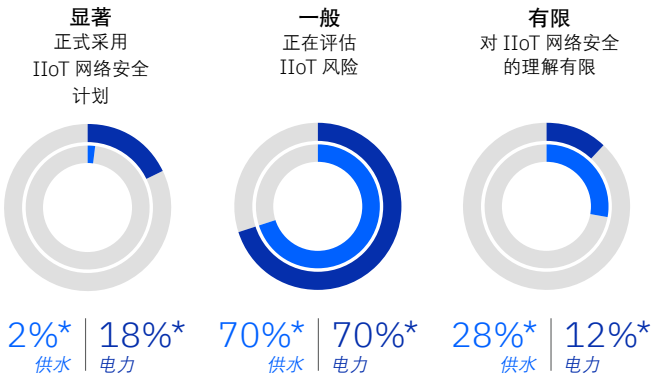
网络卫生是指企业在网络安全计划中采用的基准网络实践，以及使用计算机和其他设备的企业和用户为维护系统正常运行和提高在线安全性所采取的步骤。通常，此类实践属于日常工作，旨在帮助确保身份及其他可能被盗或遭受破坏的详细信息的安全性。与身体卫生一样，定期实施网络卫生工作有助于防止自然损耗和常见威胁。

为什么公用事业企业未能缩小差距？

公用事业企业很清楚网络安全风险的存在，但 70% 的受访者表示他们对 IIoT 网络安全技术至多只是泛泛了解。调研结果表明，公用事业企业缺乏基本的 IIoT 网络卫生战略 — 也就是缓解风险所需的组织、技术和流程。虽然电力企业还未真正实现“安全”运营，但他们对 IIoT 部署和所连接的信息 / 实体系统安全需求的认识，要比供水企业更胜一筹。18% 的电力企业已经制定了正式的 IIoT 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，而供水企业中只有 2% 做到了这一点（见图 2）。

图 2

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调研，2018 年。

n = 120；电力 = 77；供水 = 43

** 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。*

大多数公用事业企业对 IIoT 网络安全只有一定程度的了解。

虽然平均而言，电力企业的网络安全计划日渐成熟，但电力企业和供水企业这两个群体的 IIoT 网络安全能力还不成熟。他们面临巨大挑战，致使 IIoT 技术与网络安全部署之间存在巨大差距，妨碍实现全方位的 IIoT 网络安全（见图 3）。

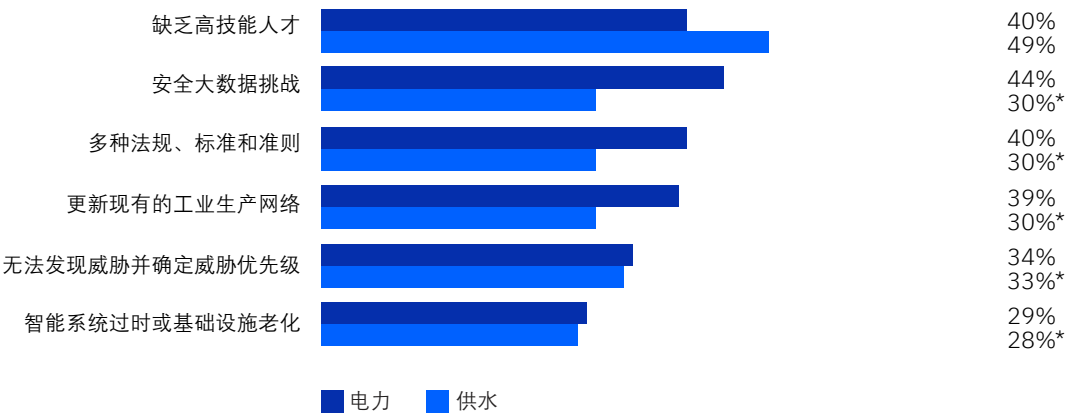
在接受调研的供水企业和电力企业高管中，有 49% 的供水企业高管和 40% 的电力企业高管面临网络安全人才短缺问题。此外，在运用众多 IIoT 技术保护复杂公用事业基础设施时，面临速度和规模方面的难题。我们的研究表明，44% 的供水企业高管和 30% 的电力企业高管面临巨大的数据挑战。

这些企业为了有效管理、分析和应用安全工具所采集的数据，以便支持检测和补救工作而疲于奔命。

近期发表的一份关于攻击活动全球趋势的报告指出，2017 年，从成功入侵到检测到威胁之间的时间中位数为 101 天。[3] 我们的调研数据表明，电力企业和供水企业分别需要 14 天和 18 天才能做出响应并恢复运营。此外，受访者表示，约半数公用事业企业的 IIoT 网络安全事故（53% 的电力企业事故和 48% 的供水企业事故）由第三方检测出，而不是由他们自己检测出。

图 3

保障公用事业 IIoT 部署安全面临的最大挑战



来源：IBM 商业价值研究院对标调研，2018 年。

公用事业企业选择最多的三项。n = 120；电力 = 77；供水 = 43

** 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。*

保护基于云的公用事业企业数据

智慧城市中的电力控制基础设施不断产生海量数据，不仅涉及车流量、街道照明和安全传感器，还涵盖分配的电力资源、电力流动和使用情况。为使公用事业企业利用不断增长的 IIoT 传感器数据，在云端托管的计算和存储资源提供了多种有效方法。

但是，北美发电或输电企业必须遵守北美电力可靠性公司 (NERC) 关键基础设施保护 (CIP) 委员会制定的“关键国家基础设施”法规。因此，目前无法将控制系统信息传输到公开共享的云托管计算环境。联邦能源监管委员会 (FERC) 采用 NERC CIP 标准，帮助保护和监管大规模电网，要求公用事业企业了解谁有权访问其数据以及如何对数据实施保护。[7]

IBM 与 NERC 开展合作，共同开发“联邦风险与授权管理计划”(FedRAMP) 模型，这是美国政府用于评估云系统安全性的标准化方法。CIPC 正在评估这个流程，确定是否可以在符合“CIP 可靠性标准”的环境中进行使用。FedRAMP 模型通过值得信赖的第三方来验证是否已实施并监控控制措施，从而增强合规性，加快让 IIoT 数据上云的速度。[8]

极速应对安全违规事件至关重要。Ponemon 近期发表的数据泄露成本报告显示，发现并控制数据泄露事件的速度越快，成本就越低。报告发现，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。相比之下，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约 35%。[4]

另外，受访者还表示，他们需要应用或遵守太多的法规、标准和准则，感到压力巨大（请参阅侧边栏“*保护基于云的公用事业企业数据*”）。此外，在接受调研的电力企业和供水企业中，39% 的电力企业和 30% 的供水企业具有工业生产网络以及难以更新的老化基础设施。安全性是许多早期工业控制系统应用（如智能电网）事后才考虑的问题，而传统设备在制造之时通常对安全性关注不足。

因此，更换此类设备既昂贵又不切实际，因为新式设备并不总是采用现代安全功能制造，而且全天运行的设备的更新时间窗口期非常有限。[5] 这种情况近期内不大可能发生转变：截至 2018 年 9 月，加利福尼亚州是美国唯一出台物联网安全法规的州，而且直到 2020 年才会生效。[6]