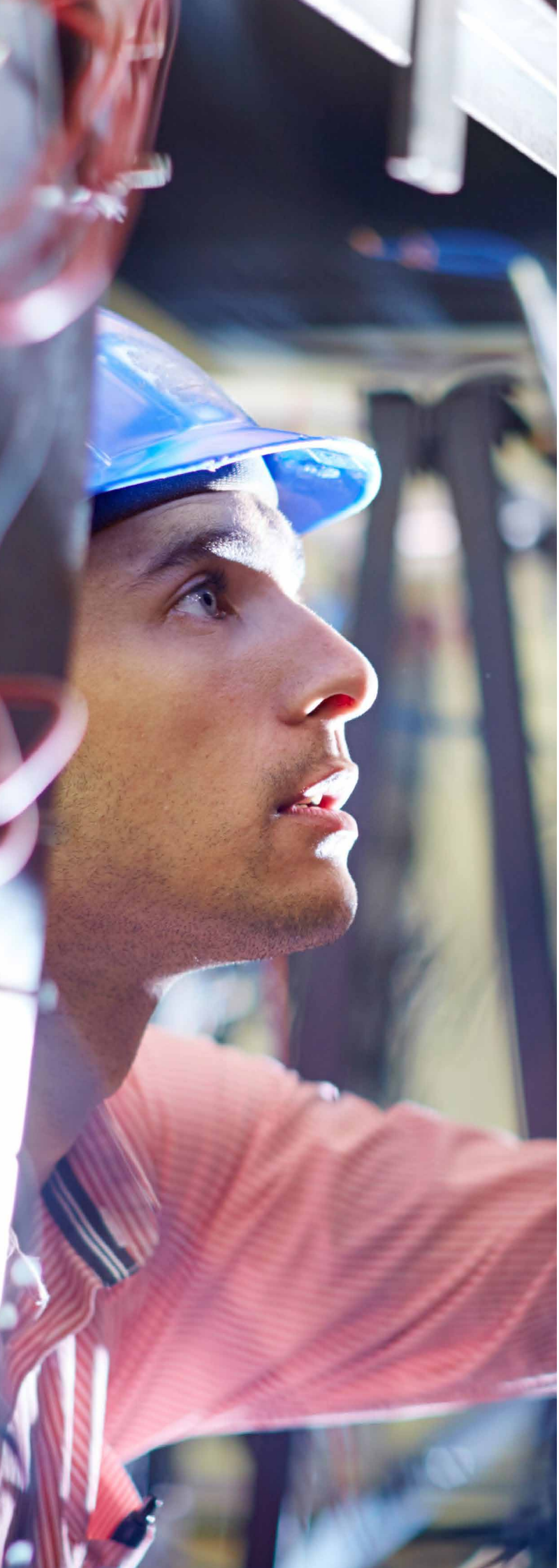


对标洞察

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?

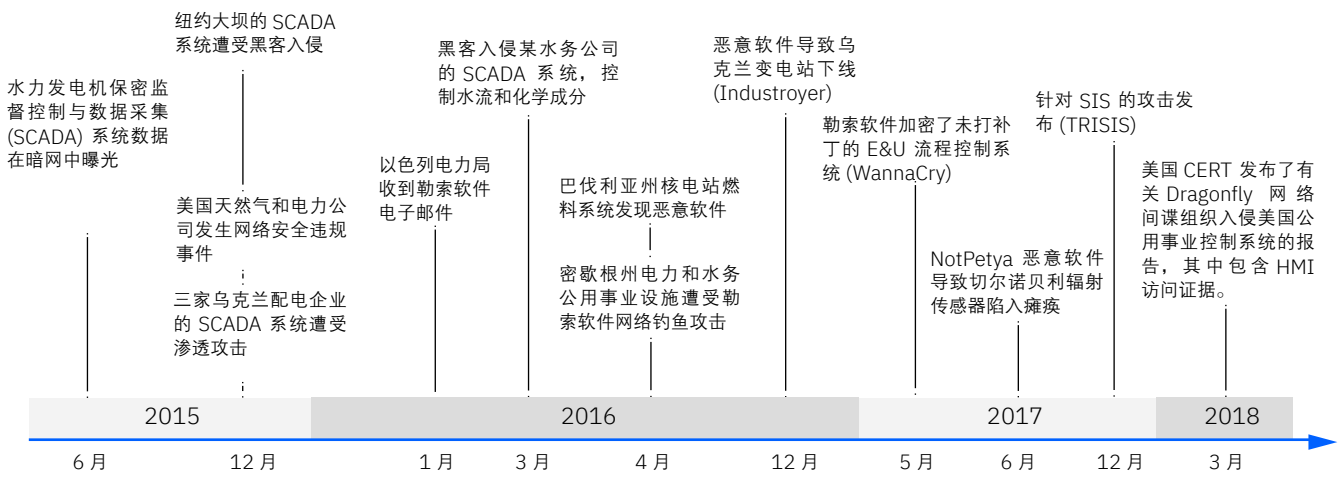
五大具体战略

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。

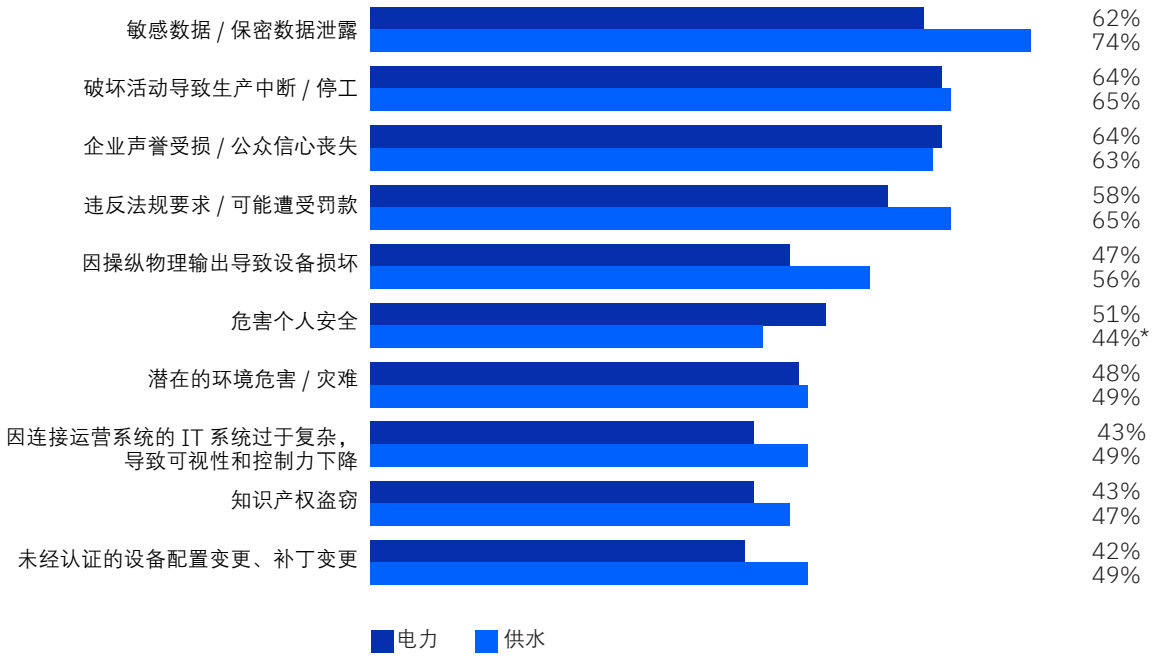
然而，公用事业企业高管对 IIoT 终端的安全倍感担忧。24% 的受访者认为设备和传感器是 IIoT 部署最薄弱的环节。另外，公用事业企业高管担心这些设备、传感器及网关上的数据未得到充分保护。12% 的公用事业企业担心云端数据的脆弱性。

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]

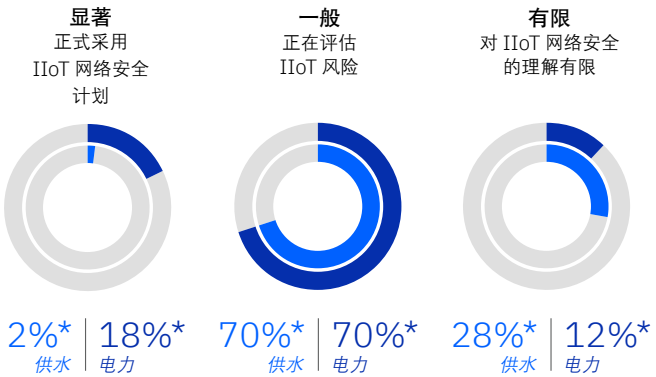
网络卫生是指企业在网络安全计划中采用的基准网络实践，以及使用计算机和其他设备的企业和用户为维护系统正常运行和提高在线安全性所采取的步骤。通常，此类实践属于日常工作，旨在帮助确保身份及其他可能被盗或遭受破坏的详细信息的安全性。与身体卫生一样，定期实施网络卫生工作有助于防止自然损耗和常见威胁。

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）。

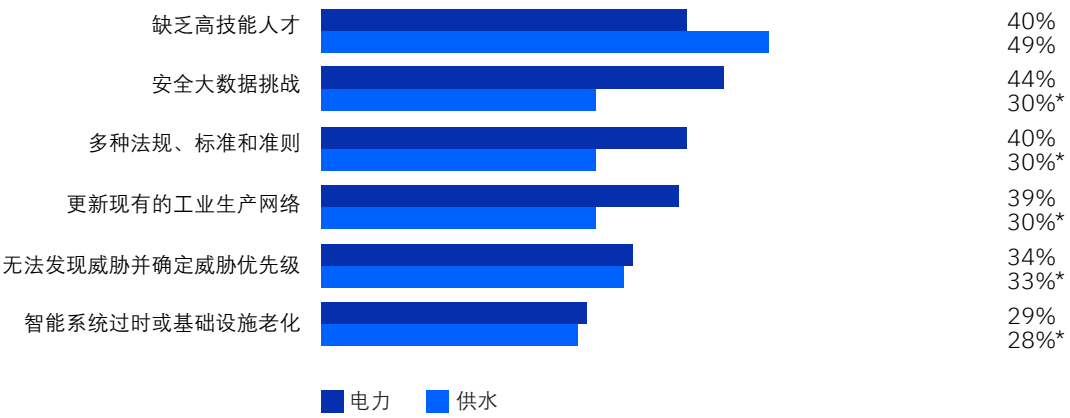
在接受调研的供水企业和电力企业高管中，有 49% 的供水企业高管和 40% 的电力企业高管面临网络安全人才短缺问题。此外，在运用众多 IIoT 技术保护复杂公用事业基础设施时，面临速度和规模方面的难题。我们的研究表明，44% 的供水企业高管和 30% 的电力企业高管面临巨大的数据挑战。

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]

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]

缩小差距：构筑有力的防御屏障

我们建议双管齐下，缩小网络安全差距。首先，企业应专注于构筑强大的 IIoT 网络安全基础，并制定基本的网络卫生战略。建立防御基础后，公用事业企业可通过使用人工智能和自动化技术，重点培养更高级的安全能力。这样，不仅可以进一步克服挑战，还能确保实现持续运营和服务交付。

以下是帮助公用事业企业奠定坚实的 IIoT 网络卫生基础的四项战略：

1. 在企业层面管理 IIoT 网络安全风险。

如果公用事业 IIoT 环境保护不力，会对社会各界造成风险。因此，整个公用事业领域均应了解并管理这些风险。定义明确的 IIoT 安全战略后，公用事业企业可以应用三项实践，为整个生态系统注入 IIoT 网络安全能力：

— *正式制定 IIoT 安全计划*，定义、管理和更新所需的 IIoT 网络安全工具、流程和技能。

— *应用安全和监管框架组合*（如美国国家标准与技术研究院 (NIST) 风险管理框架、NIST 800 标准和 ISO/IEC 27000-1），以此作为基础：[9]

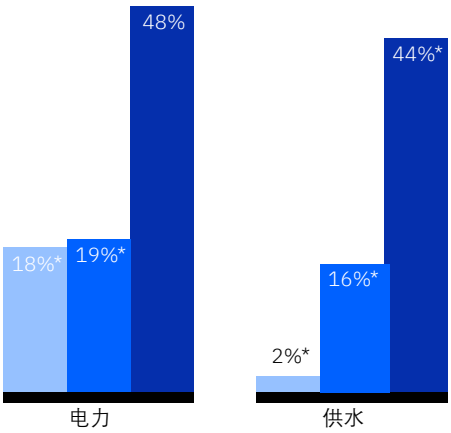
- 确定关键数据、资产和安全边界。
- 确定 IIoT 系统、连接的生产环境和人员资产中的漏洞。
- 构建和定制风险管理框架。
- 评估风险，记录并执行计划以减轻风险。
- 保护最紧迫的安全计划的投资并沟通进度。
- 根据业务目标与合规要求，平衡可接受的风险水平。

— *组建跨职能安全团队*，广泛覆盖 IT 安全、工程、运营、控制系统和安全供应商。在接受调研的电力企业和供水企业中，49% 的电力企业和 44% 的供水企业部署了这样的团队。跨职能工作方法有助于企业更清晰地了解物联网系统、标准企业 IT 系统和运营设备之间的差异。同时，还可以帮助公用事业企业利用 IT 和运营技术 (OT) 专业技能，更有效地保护系统和设备（参见图 4）。[10]

员工网络安全教育有助于增强安全意识，提高安全运营有效性。

图 4

在企业层面管理 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。*

2. 落实并执行 IIoT 网络安全。

随着 IIoT 技术成为公用事业关键架构的一部分，安全功能也应同步融入。以下三项实践有助于将安全功能融入架构，将它们整合到运营之中，并且在企业之外发挥作用：

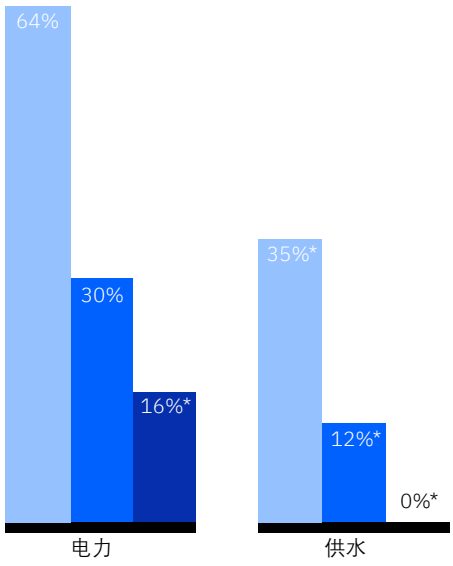
— *将 IIoT 网络安全整合到 IT、OT 和 IIoT 运营流程中。*64% 的电力企业表示，他们至少部署了安全提供基于 IIoT 的新产品或新服务所需的基础架构和流程。只有 35% 的供水企业做到这一点。为部署高风险的复杂 IIoT 系统，不仅需要网络安全专家，还要由 OT 专家提供信息 / 实体系统设计和运行方面的指导。我们建议采用安全系统开发生命周期 (SDLC)（如 DevSecOps），整合各种活动，以便尽早发现并消除漏洞。

— *增强员工洞悉物联网安全运营、IT 和 OT 运营的能力。*[11] 8% 的电力企业和 12% 的供水企业将此作为重点预防性措施。网络安全教育和安全意识活动对于实现 IIoT 网络卫生至关重要（见图 5）。

— *定义明确的安全与隐私服务级别协议 (SLA)。*在依赖第三方的情况下，这一点尤其重要。只有 16% 的电力企业通过 SLA 来监控和履行安全要求，没有供水企业受访者表示这样做。确保对数据的受控访问有助于抵御内部攻击，防止信息被盗或受到损害。务必记录有权访问敏感功能或数据的人员，密切监控和审计这些特权用户的行为。[12]

图 5

落实并执行 IIoT 网络安全



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。*

3. 了解并限制事故和违规的影响。

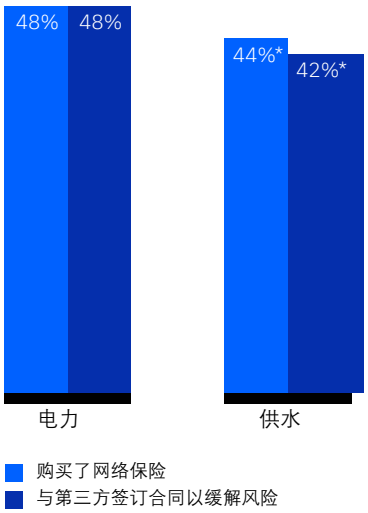
综合考量违规的所有成本：响应和通知、关键基础设施损坏、监管罚款、额外的安全和审计要求，以及其他赔偿责任和估算的损失。了解哪些成本可以消化，哪些成本可能产生灾难性影响，将有助于企业正确划分网络安全投资的优先级。以下两项实践尤其有助于限制违规行为的影响：

— *购买网络保险以减轻残余风险。*46% 的电力企业和 44% 的供水企业购买网络保险，抵消违规或类似事件后的恢复成本。

— *与第三方签订合同以降低风险。*42% 的电力企业和 48% 的供水企业采用这种方法（见图 6）。

图 6

了解并限制事故和违规的影响



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。*

4. 精心策划响应措施，应对事故和违规

公用事业企业面临诸多难题：难以捉摸的复杂网络攻击、异常繁复的基础设施、网络安全技能不足等。用于实现快速动态、统筹协调的响应的技术和流程至关重要。我们发现了四项帮助建立相关能力的实践：

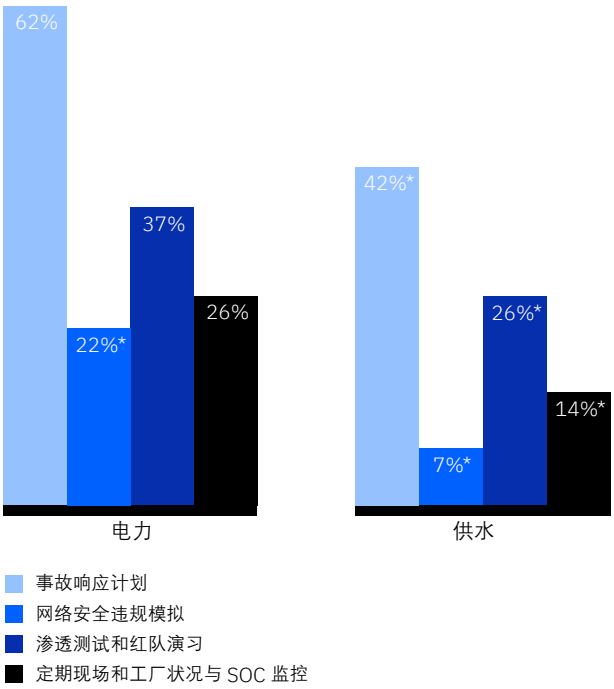
— 在安全管理计划中，*制定事故响应计划*。如有必要，与第三方事故处理公司合作，以便获得专业技能。62% 的电力企业和 42% 的供水企业制定了事故响应计划，确立了针对受损 IIoT 组件的行动预案。

— *执行网络安全违规模拟*。22% 的电力企业通过执行安全违规模拟以进一步实施事故响应，帮助确定发生违规时要激活哪些流程、人员和工具。只有 7% 的受访供水企业执行模拟。

— *执行渗透测试和红队演习*。红队是指模拟网络攻击的道德黑客团体，旨在帮助安全负责人对事故响应计划进行压力测试、找出差距并进行相应调整。渗透测试有助于发现临时漏洞，确保持续遵守安全策略和数据隐私法规。我们的研究表明，37% 的电力企业和 26% 的供水企业正在实施此类进攻性防御战略。

— *定期进行现场和工厂状况感知以及安全运营中心 (SOC) 监控*。现场和工厂状况感知演习应在 SOC 团队的辅助下完成，SOC 团队将持续评估企业的安全状况，监督安全运营并与组织事故响应团队密切合作。超过 1/4 的电力企业正在不断深化自身对于复杂运营环境（如发电厂）的认识，这对于决策者而言至关重要；相比之下，只有 14% 的供水企业做到这一点（见图 7）。

图 7
精心策划响应措施，应对事故和违规



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。*

确立防御基础后，公用事业企业可以专注实施第五项战略，培养更高级的能力。

5. 应用智能化、自动化的威胁检测和响应技术

为减轻安全人员的负担，可通过实施人工智能驱动的自动化调查流程来减少手动威胁检测。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。安全工具可以利用人工智能，理解所采集的大量数据。以下是实现这些功能的五种方法：

— *应用高级网络安全监控与分析技术，进行事故检测与补救*。37% 的电力企业和 12% 的供水企业专注于分析 IIoT 信息，而不是收集数据以生成事后审计和报告。

— *实施人工智能技术，实时进行安全监控与响应*。为实时跟踪 IIoT 信息并全面了解环境中发生的情况，20% 的电力企业已自动收集、集成和分析所有可能监测点的数据。包括系统日志、网络流、终端数据、云使用情况和用户行为。只有 2% 的供水企业实施类似的功能。

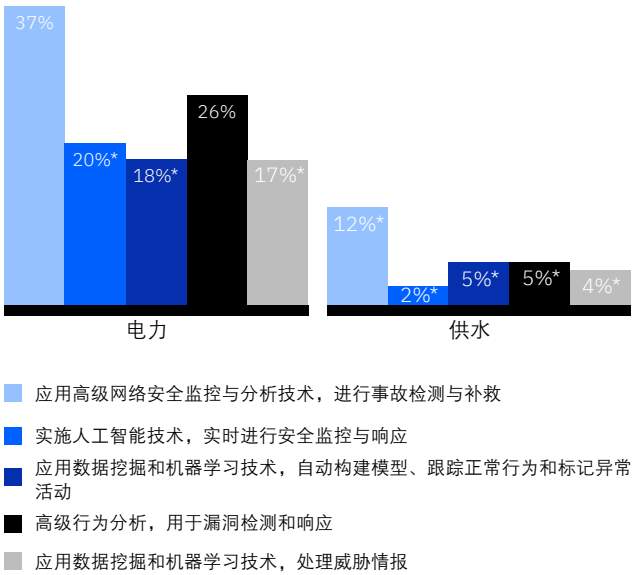
— *应用数据挖掘和机器学习技术，自动构建模型、跟踪正常行为和标记异常活动*。各监测点的 IIoT 信息有助于理解深入到网络层面的“正常”标准。机器学习可以自动构建正常自适应模型、跟踪正常行为以及标记可能表明出现新威胁迹象的异常活动。18% 的电力企业和 5% 的供水企业表示自己具备这些能力。

— *应用高级行为分析，用于终端违规检测与响应*。运用终端检测和响应机制补充现有技术，监测恶意软件创建者在近期攻击中采用的技术，进而利用由机器学习提供支持的模式识别技术来弥补差距。26% 的电力企业表示已采用能够利用机器学习的行为分析，只有 5% 的供水企业做到这一点。

— *应用数据挖掘和机器学习技术，处理威胁情报*。SOC 团队可适时获得适当的威胁情报，实时阻止攻击，预测攻击者的下一步行动并主动猎杀威胁。只有 17% 的电力企业和 4% 的供水企业具备相关系统，能够从 IIoT 数据流和外部来源中提取信息，并且应用机器学习技术来检测异常行为，预测存在严重威胁的项目（见图 8）。

图 8

应用智能化、自动化的威胁检测和响应技术



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。*

为制定强有力的安全战略，必须进行全方位的 IIoT 风险评估。

对于公用事业企业而言，必须确保家家户户“电灯长明”或“流水不断”，因而可用性成为主要的安全优先事项。但是，倘若未全面评估 IIoT 风险即实施多项 IIoT 安全控制、实践和技术，将会导致战略重点不明，进而造成 IIoT 网络安全投资重点错位。若未开展强有力的评估，公用事业企业最终可能达不到关键防御措施的要求。在实施总体 IIoT 安全战略和计划的过程中，必须采用网络安全实践和技术，并且符合更广泛的企业 IT 和运营技术风险与安全框架。这并非某一种特定工具或某一项特定技能。安全性与人员、技术和流程息息相关，各要素环环相扣，必须精心统筹策划才能有效运行。这是整个生态系统发挥合力的结果，包括公用事业企业、政府、设备提供商和安全供应商。

贵组织能否保护基础设施、国民经济乃至整个社会?

» 如何保证贵组织的运营技术安全战略与总体安全战略保持一致?

» 如何保证 IIoT 安全实践与组织确立的企业风险管理框架保持一致?

» 如何将安全工具和管理流程整合到企业安全框架和运营流程之中?

» 如何采用“安全第一”战略，将基本安全功能融入 IIoT 设计的方方面面?

» 如何遏制威胁影响、减少中断以及建立从攻击中快速恢复的能力?

关于作者

Cristene Gonzalez-Wertz
linkedin.com/in/cjgw1
cristeneg@us.ibm.com

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。

Lisa-Giane Fisher
linkedin.com/in/lisa-giane-fisher
lfisher@za.ibm.com

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。

Steven Dougherty
linkedin.com/in/steven-a-steve dougherty-cissp-cfe-4585b7
sdougherty@us.ibm.com

Steven Dougherty 是 IBM Security 能源、环境与公用事业业务开发主管。他在为全球客户设计、交付和运行创新型解决方案、工业控制和技术战略方面拥有 30 多年的丰富经验。Steven 是 IEEE 资深成员、经过认证的信息系统安全专家 (CISSP) 和经过认证的欺诈检验师 (CFE)。

Mark Holt
linkedin.com/in/lmarkholt
mholt@us.ibm.com

Mark Holt 是 IBM 全球能源、环境与公用事业行业安全业务开发负责人。Mark 不仅在工程系统、资产管理和物联网方面拥有丰富经验，还领导实施了 IBM 系统工程战略。目前，Mark 负责在全球将 IBM 安全能力应用于公用事业领域。

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：https://www.ibm.com/cn-zh/services/insights/institute-business-value。

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 (IBV) 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。

相关 IBV 出版物

Gonzalez-Wertz、Cristene、Lisa Fisher、Peter Xu 与 Martin Borrett 合著，“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，2018 年 10 月。https://www.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=85020085CNZH&

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&

“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&

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 支持的公用事业行业运营环境，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 可以帮助公用事业行业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，帮助保护关键基础设施资产，采用新型服务为平台和生态系统提供支持。我们的全球公用事业专家具备深厚的专业知识，完全有能力保护您的资产和流程，同时提升产品和服务的质量。IBM 应用认知方法，帮助降低安全风险。请访问 ibm.com/industries/energy。

备注和参考资料

1 “Alert (TA18-074A) Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors.” United States Computer Emergency Readiness Team alert. March 15, 2018. https://www.us-cert.gov/ncas/alerts/TA18-074A

2 Aldorisio, Jeff. “What is Cyber Hygiene? A Definition of Cyber Hygiene, Benefits, Best Practices, and More.” Digital Guardian.September 26, 2018. https://digitalguardian.com/blog/what-cyber-hygiene-definition-cyber-hygiene benefits-best-practices-and-more

3 “M-Trends 2018.” Mandiant, a FireEye company. 2018. https://www.fireeye.com/content/dam/collateral/en/mtrends-2018.pdf

4 “2018 Cost of a Data Breach Study: Global Overview.” Ponemon Institute LLC.July 2018. https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=55017055USEN

5 Gonzalez-Wertz, Cristene, Lisa Fisher, Peter Xu, and Martin Borrett. “Electronics Industrial IoT cybersecurity: As strong as its weakest link.” IBM Institute for Business Value. October 2018. https://www-935.ibm.com/services/us/gbs/thoughtleadership/electronicsiiot/

6 Robertson, Adi. “California just became the first state with an Internet of Things cybersecurity law.” The Verge.September 28, 2018. https://www.theverge.com/2018/9/28/17874768/california-iot-smart-device-cybersecurity-bill-sb-327 signed-law

7 “Mandatory Reliability Standards for Critical Infrastructure Protection: A Rule by the Federal Energy Regulatory Commission.” Federal Register.January 18, 2008. https://www.federalregister.gov/documents/2008/02/07/E8-1317/mandatory reliability-standards-for-critical-infrastructure protection; “Critical Infrastructure Protection Committee (CIPC).” North American Electric Reliability Corporation (NERC) website, accessed December 26, 2018. https://www.nerc.com/comm/CIPC/Pages/default.aspx

8 “Critical Infrastructure Protection Committee (CIPC) Meeting Minutes.” North American Electric Reliability Corporation (NERC).June 5-6, 2018. https://www.nerc.com/comm/CIPC/Agendas%20Highlights%20and%20Minutes%202013/CIPC%20June%20 2018%20minutes%20DRAFT%20v0.pdf

9 “National Institute of Standards and Technology (NIST) Risk Management Framework.” NIST Computer Security Resource Center website. https://csrc.nist.gov/projects/risk-management/risk-management-framework-(rmf)-overview; “NIST Special Publication 800-series General Information.” NIST Information Technology Laboratory. https://www.nist.gov/itl/nist special-publication-800-series-general-information; “ISO/IEC 27000 family - Information security management systems.” International Organization for Standardization. https://www.iso.org/isoiec-27001-information-security.html

10 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

11 Ibid.

12 Gonzalez-Wertz, Cristene, Lisa Fisher, Peter Xu, and Martin Borrett. “Electronics Industrial IoT cybersecurity:As strong as its weakest link.” IBM Institute for Business Value. October 2018. https://www-935.ibm.com/services/us/gbs/thoughtleadership/electronicsiiot

13 Ibid.

关于对标洞察

对标洞察反映的是主管对于重要业务和相关技术主题的洞察。对标洞察基于性能数据分析以及其他一些对标评测结果。要了解更多信息，请联系 IBM 商业价值研究院：iibv@us.ibm.com。

IBM Corporation
New Orchard Road
Armonk, NY 10504
美国出品
2019 年 1 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