机械装备行业工业安全态势调研报告

前言

随着工业互联网、大数据、云计算、5G 等新一代信息技术与制造业进一步深度融合，更多机器和设备实现互联，工业互联网应用需要采集各类设备和机器的数据，实现多种数据的集中，工业大数据的集中也意味着风险的高度集中。同时，随着工业互联网业务、平台、设备、用户的多样性不断丰富，传统的网络安全边界加速瓦解，传统的边界安全架构无法满足工业互联网时代的安全需求。制造企业在享受新一代信息技术成果的同时，也面临着制造环境走向开放、跨域、互联所带来的一系列安全性问题。

大规模、高强度的工业信息安全事件频发，工业领域成为网络攻击重灾区。放眼全球，2019 年全球各地大约有 329 件工控安全问题事件，涉及的领域越来越广泛，包括天然气、制造、能源、电力、汽车、化工等。聚焦国内，根据国家工业信息安全产业发展联盟统计数据显示，我国每年新增的工业控制系统漏洞数量持续增长，从 2014 年 133 个升至 2019 年 567 个，其中高危漏洞占比达到 45.3%。

漏洞病毒问题依旧突出，新一代信息技术与制造业深度融合带来新风险。一方面，作为传统意义上相对封闭的工业系统，工业设备软件更新缓慢，用户及厂商通常无法及时发现或修复漏洞，这些旧的安全漏洞将面临安全考验。另一方面，随着工业互联网、5G 等新技术在制造业深化应用，制造企业网络日益开放，大量设备和系统都将暴露在互联网上，增加了信息泄露、数据窃取的风险。这些对制造业工业安全都提出了巨大挑战。

为切实了解当前制造企业工业安全建设现状和面临问题，IBM 联合 e-works 开展了多轮在线调查，并通过机械装备行业作为突破口，深入剖析新时代新形势下制造企业在工业安全方面所面临的“困境”，了解企业真实的需求，帮助企业探寻构建企业安全体系的“道”与“法”。

一、新时代机械装备行业工业安全之“困”

机械装备制造业作为我国工业领域的重要行业，生产设备众多，工业软件多种多样且集成关系复杂，大量的数据需要采集、传输、分析与挖掘，甚至产品的远程运维服务，都离不开工业安全的保驾护航。尤其是机械装备行业企业普遍应用大量数控装备、工业机器人和外置传感器，设备复杂度比较高，接口协议复杂，在设备联网、设备上云以及设备远程运维等环节的安全风险很高。当前，随着制造环境更加开放、互联，机械装备行业企业面临多方面的安全挑战。

复杂的工业环境。机械装备企业典型的工业环境一般包括控制器(PLC、DCS)、工业计算机、工业软件、网络、交换机、路由器、工业数据库等，潜在攻击面很大，其中任意一个环节或者部件出现问题就有可能导致整个工控系统被攻击。

繁复的通讯协议。机械装备业生产线普遍应用大量自动化设备，包括很多进口的高精类机床设备，各设备生产及集成商工业协议标准不统一、不兼容，接口开放程度不同，都使得协议解析、数据采集过程容易产生安全隐患。

开放的生产设备。越来越多的机械设备应用通用 IT 技术及开放式网络协议进行数字化、信息化、网络化改造，比如远程运维，但企业安全防护建设速度落后于数字化信息化建设速度，导致越来越多的生产设备暴露于互联网中。

紧密的供应链协同。机械装备行业一般产业链长、主体多，随着信息技术持续深入，供应链概念从企业内部进行前伸和后延，企业加强了与上下游供应商、物流企业、分销商等的信息交互，增加了供应链上主体的安全风险。

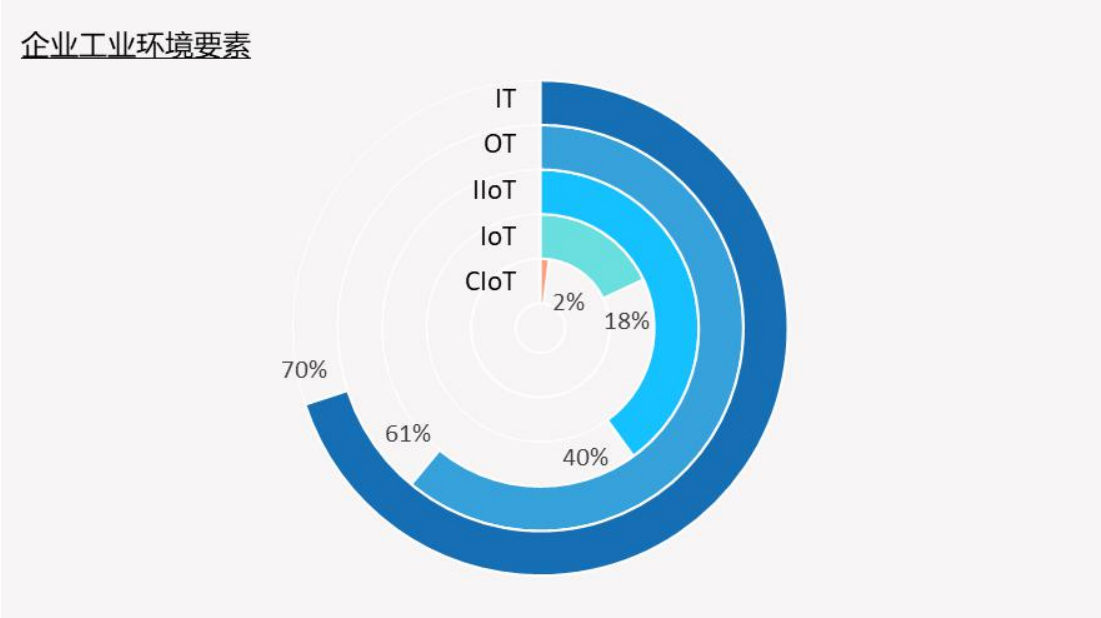
敏感的企业数据。机械装备行业涉及工艺、生产、设备等数据，工艺数据随着多品种、小批量特点更明显变得更复杂，生产数据、设备数据采集的全面性和实时性带来巨大的数据存储要求，数据加密、传输、存储等都容易存在安全隐患。

受质疑的云安全。国内很多机床厂商、数控系统厂商建立云平台及服务，对设备进行在线实时监控，提供设备状态分析与故障预警，此类场景也面临着虚拟化中常见的违规接入、内部入侵、多租户风险等内外部安全挑战。

本次调研结果显示，受访的机械装备行业企业普遍认识到工业安全的重要性，也意识到企业面临工业安全威胁，但尚未建立有效的工业安全防护体系，安全业务人员配置和资金预算有限，应对安全威胁的能力不足。

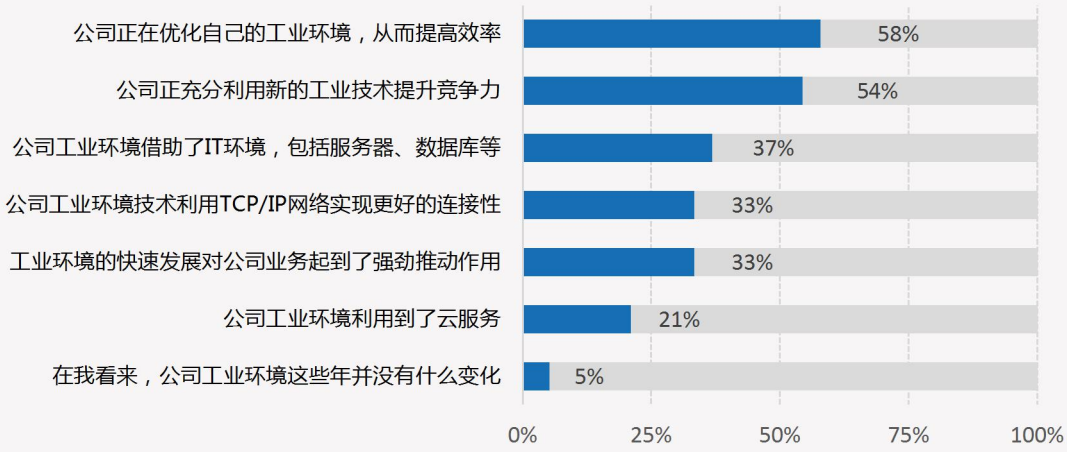
1.工业环境优化成企业发展重要“推力”

伴随新一代信息技术与制造业不断融合，企业所在工业环境越来越复杂。目前，在 IT 和 OT（运营技术，如 DCS、PLC、RTU）的基础上，企业所在的工业环境已经开始融入 IIoT(工业物联网，如智能传感器)、IoT(物联网，如汽车管理、空调系统)、CIoT（消费物联网，如可穿戴设备、智能家居）的元素。调研结果显示，工业环境中增加了智能传感器等 IIoT 元素的机械装备企业已经达到 40%，增加了 IoT 元素的企业达到 18%，还有 2%企业应用了 CIoT 元素。



机械装备行业企业通过不断优化其工业环境，赋能企业发展，提高企业效率和竞争力，例如借助 5G 通信技术实现工厂内大规模制造装备实时互联，通过 AR 技术实现设备远程运维诊断，通过云服务实现资源动态配置、网络化协同制造等。调研显示，57.9%的受访企业表示通过优化工业环境在提高效率，54.4%正充分利用新的工业技术提升企业竞争力，33.3%企业表示快速变化的工业环境对公司业务起到了强劲推动作用。

企业工业环境现状

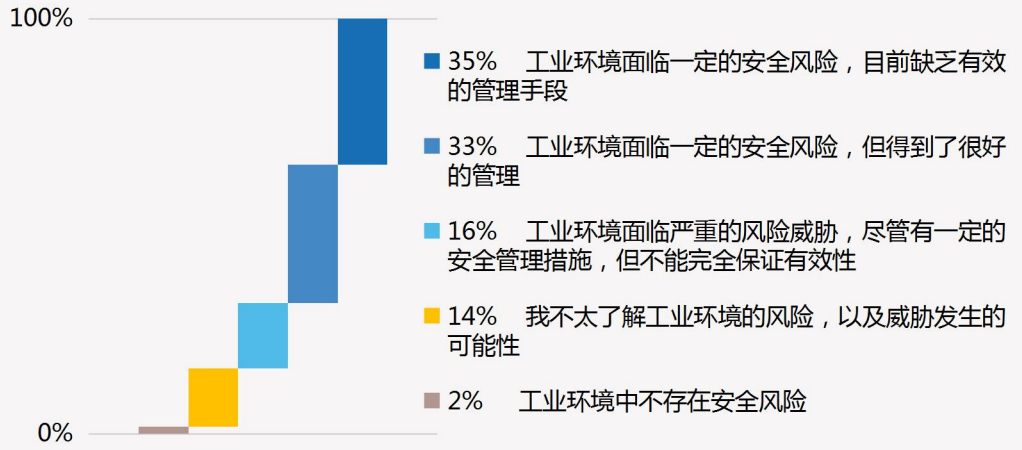


随着物联网、5G、边缘计算、云平台等新兴技术在制造业应用场景加速落地，企业工业环境元素将更为丰富，也将进一步赋能制造业数字化转型、新业务新模式探索。

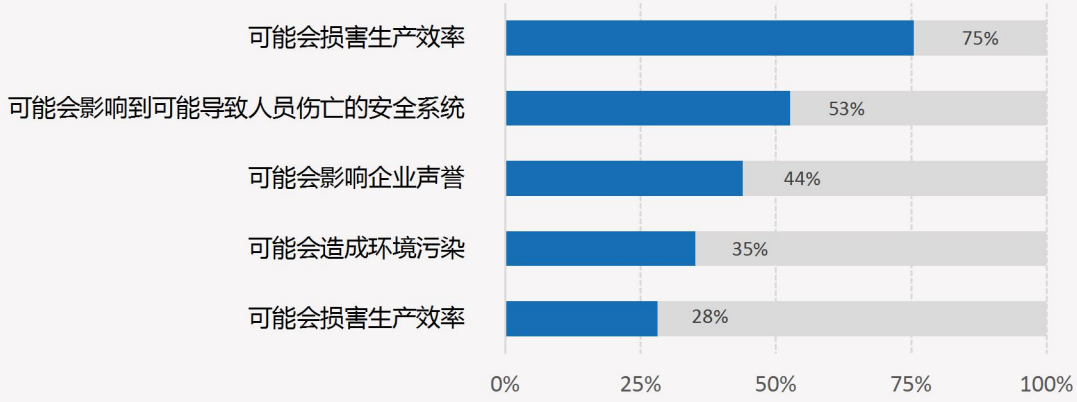
2.安全防护尚未进入企业发展“核心”

面对越来越复杂的工业环境要素，**机械装备行业企业虽普遍认识到工业安全风险的存在，以及风险会造成负面影响，但是对安全防护的重视程度仍然不够。**调研结果显示，84.2%的受访企业意识到其工业环境面临安全威胁，75.3%的企业认为可能会影响生产效率，52.6%认为可能会间接导致人员伤亡，43.9%认为可能会直接影响企业声誉。但是，绝大多数国内制造企业的安全防护能力跟不上企业发展速度，尤其缺乏有效的安全管理机制与应对措施。35.1%受访企业表示缺乏有效管理手段，15.8%受访企业虽然制定了安全管理措施但不能保证有效性。

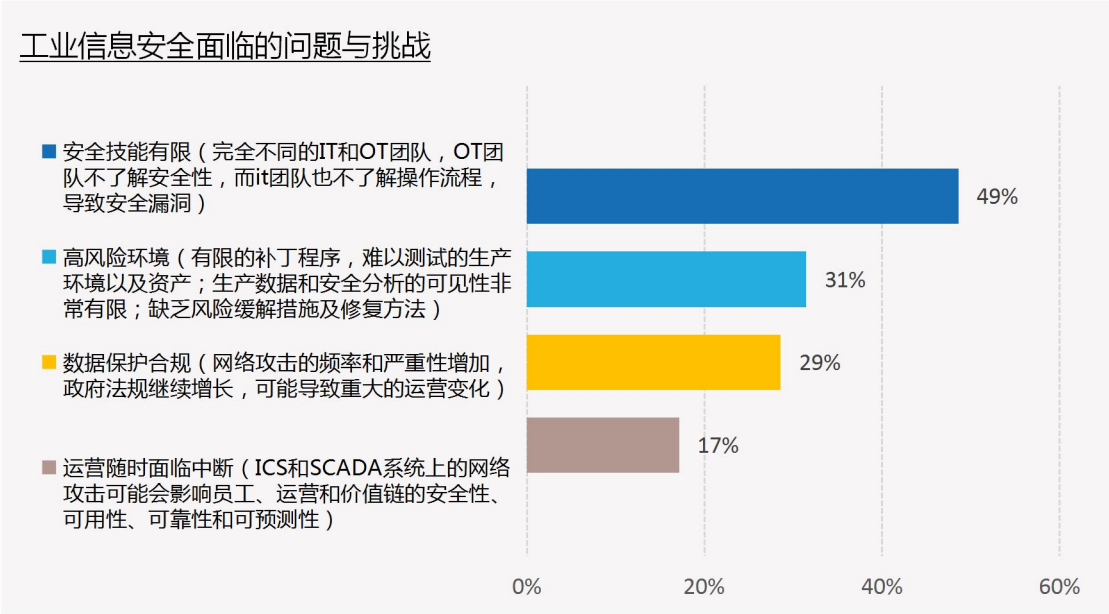
工业环境面临的安全风险与挑战



工业环境风险可能会导致的影响



相对于 IT 安全，工业安全是一个新战场，企业面临着人员、技能、规范、环境等多方面挑战。48.6%的受访企业认为工业信息安全面临的挑战主要来自于企业安全技能水平有限，包括 IT 和 OT 团队人员配置不同，IT 和 OT 团队对安全性缺乏了解。31.4%的企业认为主要挑战来自于当前高风险的环境，包括有限的补丁程序，难以测试的生产环境以及资产，有限的安全分析展示，欠缺的风险应对措施和修复方法。28.6%认为网络攻击的频率增加，安全方面法规和标准制定还不完善。

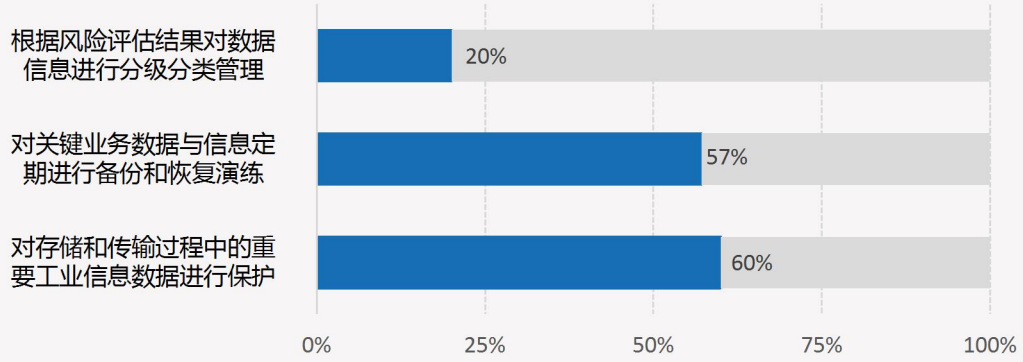


根据国家工业信息安全发展研究中心监测数据，我国暴露在互联网上工业控制系统数量增幅尤其明显，增速超过了全球平均水平，且其中相当大一部分都存在高危安全漏洞。在未来很长的一段时间内，我国制造企业将适应这种新常态，并不得不应对这场严峻的安全大考。

3.应对安全风险的措施依旧“匮乏”

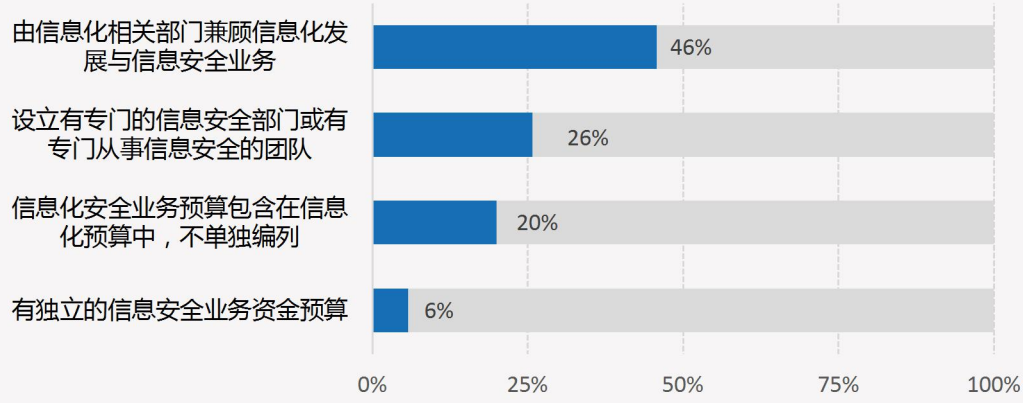
机械装备企业和大多数制造企业一样，在面对工业安全的问题时往往一筹莫展。调研结果显示，60%受访企业对存储和传输过程中重要信息数据有保护措施，57%对关键业务数据进行定期备份和恢复演练，仅有 20%的企业根据风险评估结果对数据信息开展了分级分类管理。**企业当前应对工业信息安全风险和威胁的措施比较有限。**

企业信息安全管理与保护的主要措施



企业在信息安全方面资金和人员投入不足。人员配置方面，仅 26%的受访企业设立有专门的信息安全部门或专门从事信息安全的团队，将近一半的企业是由信息化部门负责信息安全业务。资金配置方面，只有 6%的受访企业在信息安全业务上设置有独立资金预算，20%企业将信息安全预算纳入在信息化预算中，并未单独编列预算。

企业在信息安全方面投入

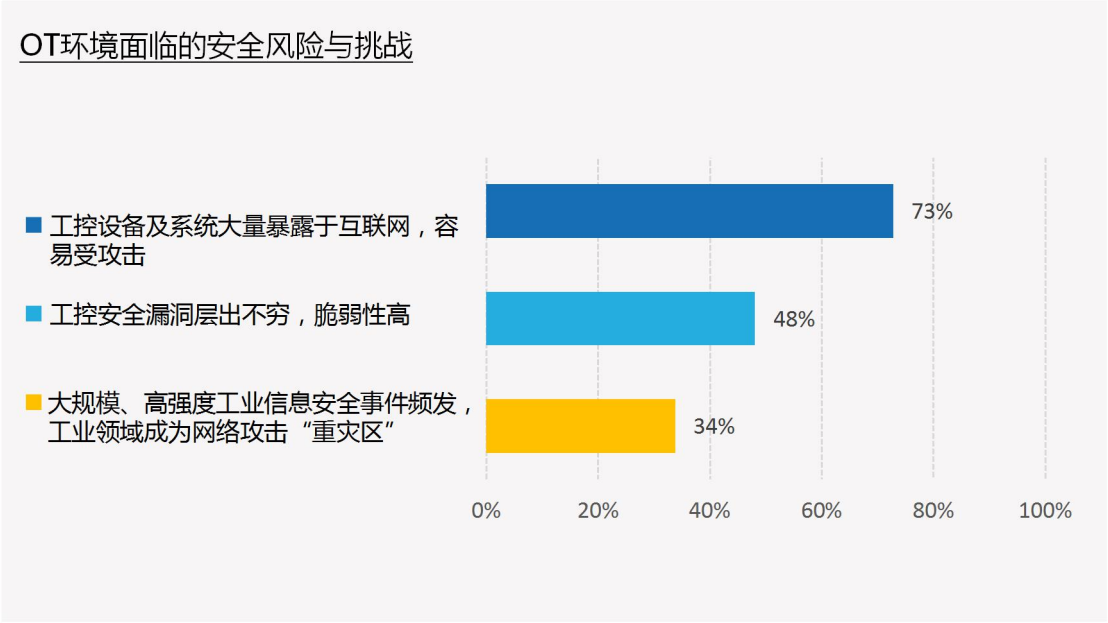


近年来发生的典型工业信息安全事件来看，工业信息安全威胁往往针对一个或几个具有脆弱性的生产系统进行渗透和攻击，进而危害整个工业信息系统。缺乏有效防范手段，也是制造业频发信息安全事件的关键原因之一。因此，对制造业企业来说，化被动为主动，建立有效的安全风险应对机制，刻不容缓。

4.OT 和 IT 加速融合带来新“风险”

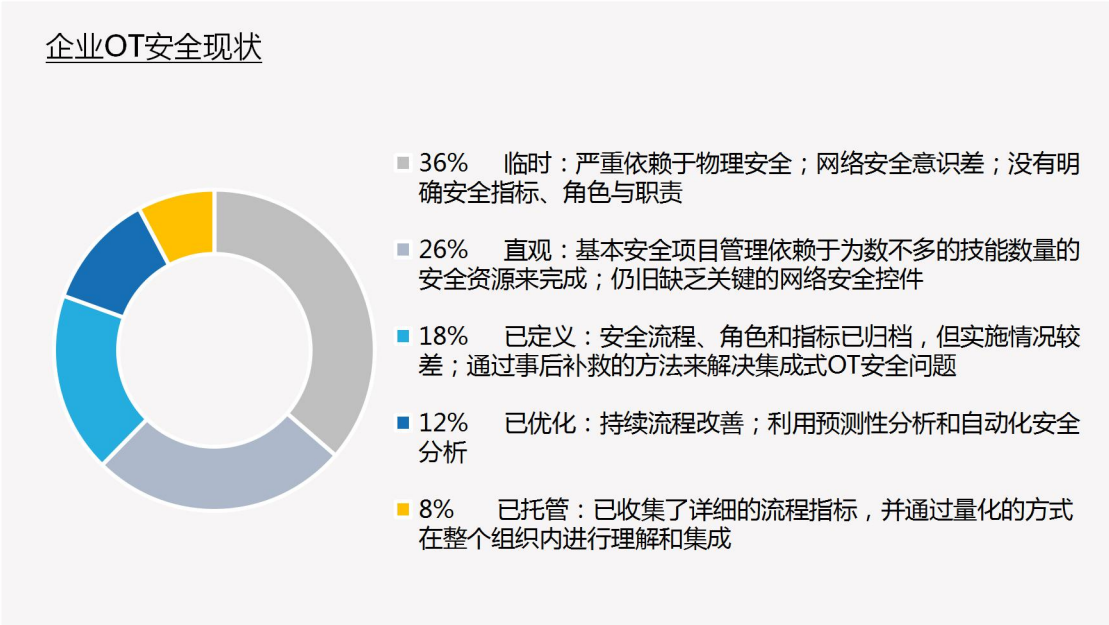
工业企业为了实现管理和控制的一体化，实现生产和管理的高效率、高效益，将 IT/OT 技术进一步深度融合，在拓展了工业控制系统发展空间的同时，也带来了一系列的工业网络安全问题，比如 IT 和 OT 职责分工不同，安全防护协同困难；OT 设备与系统更加重视功能实现，安全防护策略考虑欠缺；OT 设备与系统必须保证高可用性，往往不允许频繁和长期的调试。

机械装备行业企业在推进数字化转型过程中，将工业控制系统（ICS）、智能传感器、工业机器人等添加到生产制造过程中，实现海量工业设备的泛在连接，在带来数据共享和效率提升的同时，也将**原本封闭的 OT 系统置于更加开放与不确定的环境之中**。调研显示，受访企业认为 OT 环境安全面临的风险主要来自于：工控设备及系统大量暴露于互联网，容易受攻击（72.7%）；工控安全漏洞层出不穷，脆弱性高（48.1%）；工业领域成为网络攻击的“重灾区”（33.8%）。



在 OT 安全管理方面，绝大多数的企业缺乏识别和应对安全威胁的能力。不足 50%的受访企业对 OT 安全开展了初步定义和初步分析，但超过 36%的企业在安全防护上仍严重依赖于物理层的安全技术，企业不仅没有形成良好的网络安全防护意识，也没有明确的安全指标、角色与职责，23%的企业虽然建立了明确的安全流程、角色和指标，但实施情况却较差，通常都是通过事后补救的方法来解决集成式 OT 安全问题。仅 12%企业的 OT 安全制定了管理流程，并开展了自动化和预测性分析。这意味着大部分企业并未就如何应对 OT 安全风险做好准备，一旦

遭遇网络威胁和攻击，很容易因此受到严重影响。



在 IT 与 OT 加速朝着全方位深度融合的方向发展形势下，工业控制网络的隔离边界慢慢消失，以工业控制系统为代表的 OT 安全防护体系越来越脆弱，OT 安全不容忽视。

在后疫情时代，国家出台了一系列关于数字化转型、数字新基建、工业互联网平台建设的政策措施，特别是在工业安全方面的支持力度在持续加大，全面助推制造业转型升级，为制造业发展注入了新的动能。机械装备行业作为资产密集、技术密集产业，对设备安全、数据安全要求很高，面临着设备安全、网络安全、数据安全、平台安全等多重安全挑战。尽管机械装备行业企业普遍认识到工业安全的重要性，但多数企业安全防护处于起步阶段，尚未建立全面的工业安全防护体系，工业安全管理制度和防护策略缺乏、应急响应流程缺乏、工业安全产品和服务部署率不高、组织机构人员职责不完善、专业安全人才缺乏，未来应加强工业安全事件的应对能力，并上升到企业发展战略的高度，以抵御未知的安全风险对企业发展的冲击。

二、探寻机械装备企业工业安全之“需”

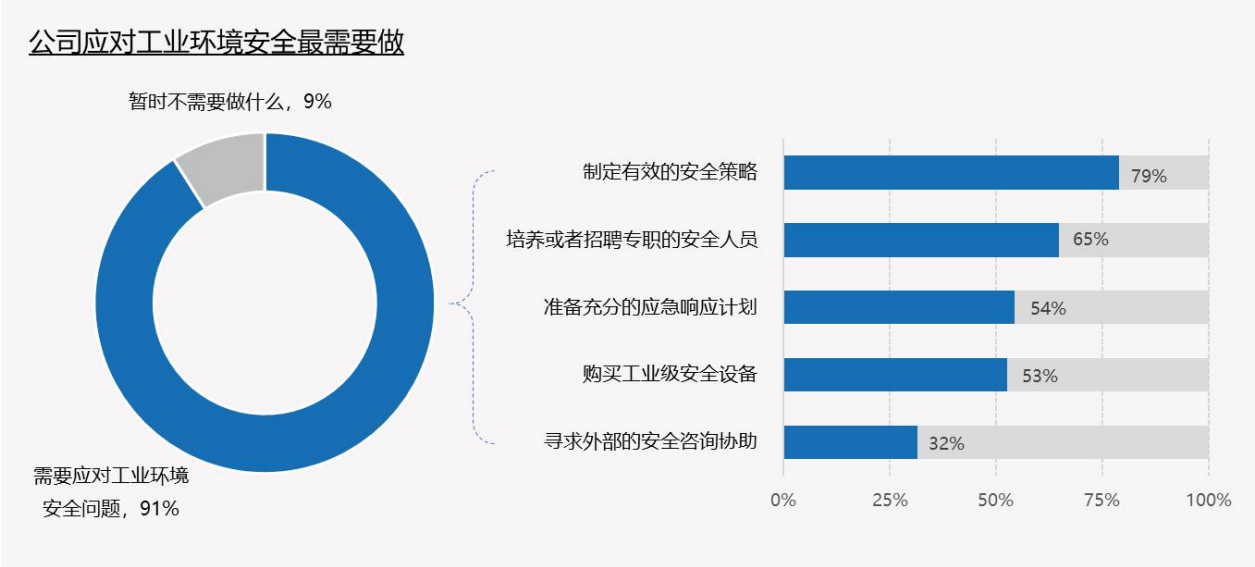
随着工业环境的愈加复杂以及安全事件对企业的影响不断加深，**应对工业环境安全已逐渐成为制造企业的重要内生需求。**

1.机械装备企业提升工业环境安全的内生动力强劲

调研结果显示，高达 91%的机械装备行业企业认为需要针对工业环境安全制定应对措施。目前国内工业安全政策法规体系、技术保障体系、产业生态体系等还未完善，绝大多数企业尚未构筑全方位的工业安全防护体系，还处于自主摸索阶段。不过，**在未来建设方向方面，受访企业均释放出诸如制定有效的安全策略、构建安全管理团队、制定应急响应计划等共同需求。**

制定有效的安全策略的需求最旺盛，占比达到近 80%。安全策略与管理制度是企业当前工业安全问题应对工作的重中之重，“攻击只需一点即可得手，而防守必须全面设防”，因此制定全面的、满足自身业务特点的安全策略，并依据策略制定管理流程和应急响应机制，是确保企业工业安全的基础。

部分企业将借助外部资源来增强企业应对安全问题的能力。企业工业安全体系建设离不开技术保障。53%的受访企业将通过购买工业级的安全设备，增强企业设备级防护能力。一部分企业考虑通过外部咨询服务机构的协助，快速获取工业安全相关知识和技能，增强企业解决安全问题的能力，受访企业中 32%有安全咨询协助方面的需求。



2.安全风险与漏洞评估成为企业应对风险的最优先级

在企业关注的安全问题方面，安全风险与漏洞评估、安全威胁监测与预警、数据安全与合规是 TOP3 关注点。

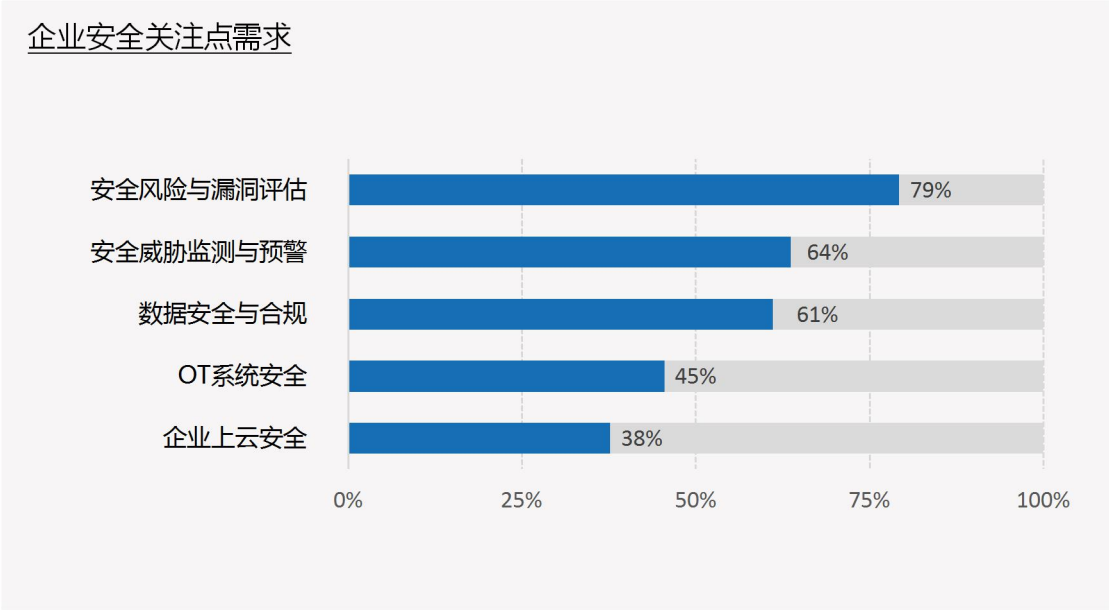
安全风险与漏洞评估是企业工业安全关注的核心问题。调查结果显示，近

80%的机械装备行业企业关注安全风险与漏洞评估。安全风险与漏洞评估可以发现并定义安全风险，制定安全战略，包括安全战略与计划，安全风险、合规性与漏洞评估，安全治理政策与要求等的评估与制定等。有效的安全计划首先要评估风险，了解企业当前工业环境中易受攻击的对象、潜在的漏洞来源，然后再依此制定治理政策和要求。

有效的、持续的安全威胁监测与预警必不可少。安全威胁监测与预警可以对工业生产与办公网络等多维度安全信息进行采集和分析，对潜在的威胁和攻击行为进行预测、响应和溯源，通过多维度可视化展示，使整体安全状态可感知。因此，企业不仅需要了解和评估风险，还需要持续的监测工业环境安全，在第一时间（甚至是提前）发现、定位并解决问题。

数据安全与合规关注度也非常高。调查结果显示，61%的机械装备行业企业关注数据安全与合规。对于制造业企业而言，诸如生产工艺参数、设备运行数据、生产数据、控制指令等工业数据是影响企业生产活动的关键业务数据，数据的篡改、丢失或错误都可能造成不小损失此外，政府对企业数据治理与数据合规的要求越来越严格，企业也将面临数据合规性问题。以上都促使企业重视数据安全与合规。

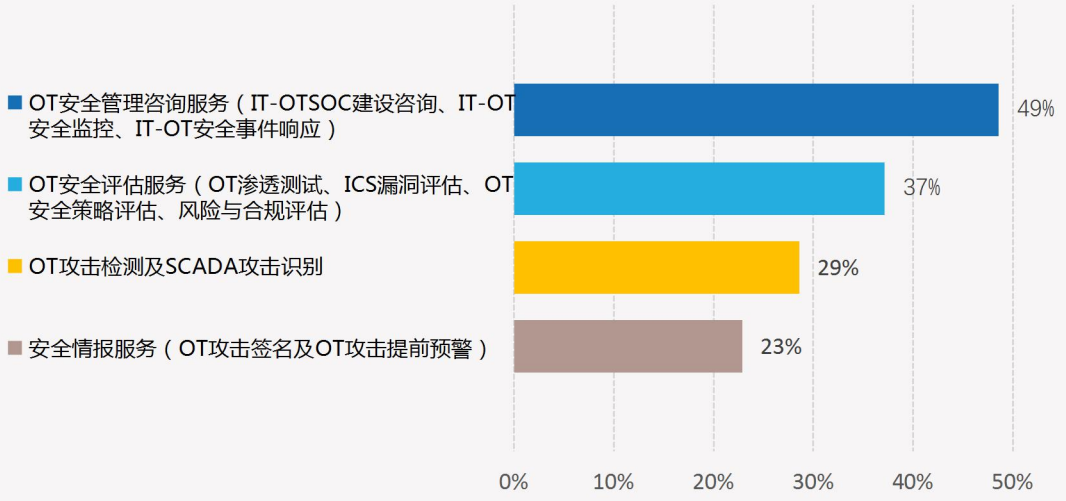
企业上云安全需求有待进一步释放。调查结果显示，38%的机械装备行业企业已经关注企业上云安全。最新发布的工业互联网平台发展指数（IIP10）显示：上云设备规模爆发式增长，2020 年工业设备连接指数增长率高达 58.7%；运营管理、设备运维、生产制造等类型工业 APP 成为当前平台开发的热点。随着工业互联网与制造业的深度融合，以及制造企业数字化转型的驱动，越来越多的企业为打破数据孤岛、加快数据流动以及数据价值挖掘，把业务系统、工业设备向云端迁移，将进一步激发制造企业对上云安全的需求。



3.咨询服务是企业构建安全防护体系的主要投入方向

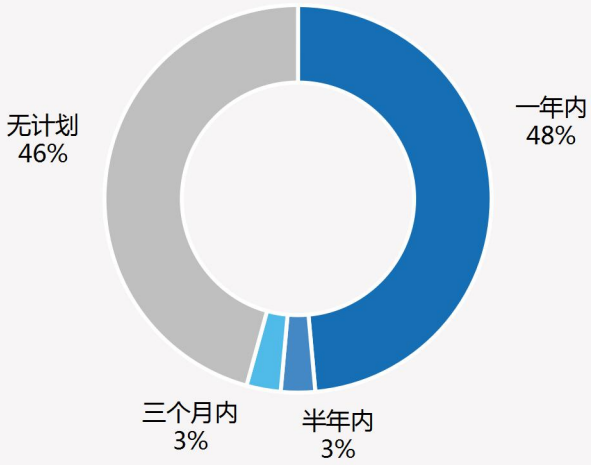
新一代信息技术与制造业深度融合将大量的 ICT 系统威胁和挑战带入工业 OT 网络，使得新形势下的工业安全与传统的工控系统安全和 IT 安全相比，其挑战更为艰巨。对于制造企业来讲，传统 IT 安全防护经验仅能作为 OT 安全体系参考，企业需要结合工业场景特点探索适用于自身安全防护特点的 OT 安全防护体系，这无疑也增加了企业 OT 安全建设难度。因此，**OT 安全服务，特别是 OT 安全管理咨询服务，成为企业的迫切需求。**调查结果显示，近 50%的机械装备企业亟需 OT 安全管理咨询服务，如 IT-OT SOC（Security Operation Center，安全运营中心）建设咨询、IT-OT 安全监控、IT-OT 安全事件响应。其它所需 OT 安全服务还有 OT 安全评估服务（如 OT 渗透测试、ICS 漏洞评估、OT 安全策略评估、风险与合规评估）、OT 攻击检测及 SCADA 攻击识别、安全情报服务（如 OT 攻击签名、OT 攻击提前预警）。

企业亟需的OT安全服务



由于制造企业普遍缺乏对工业信息安全防护策略的落地能力，安全体系设计和规划服务需求应运而生。特别是近年来工业信息安全事件频发，比如 2018 年台积电三个重要生产基地因为病毒入侵而导致生产线全数停摆事件，2019 年委内瑞拉电力控制系统遭受连续三个阶段攻击导致其区域电力系统瘫痪，且极度干扰事故后的应急工作，也进一步催化了制造企业对风险评估、应急处置、攻防演练等工业信息安全服务价值的认可。调查结果中，54%的受访企业表示一年内有采购工业信息安全服务的计划。

近期采购工业信息安全服务的计划



当前，机械制造行业企业已经意识到工业安全的重要性，同时也在释放出更

多工业安全建设需求。总体方向方面，需求主要集中在安全策略与管理制度、构建专业安全团队、制定应急响应计划。很多企业还表现出利用工业安全产业来加快自身工业安全建设步伐的需求，一方面，通过购买工业安全产品（如工业级安全设备），结合传统 IT 信息安全管理，来加强企业工业环境风险应对能力；另一方面，通过购买第三方安全服务，来应对工业安全专业人才的短缺和安全态势的复杂紧迫。细分领域方面，工业安全涉及工业领域各个环节，一般包括工业控制系统安全、工业互联网安全、工业大数据安全、工业云安全、工业电子商务安全、关键信息基础设施安全等内容。目前，企业更多关注安全风险与漏洞评估、安全威胁监测与预警，以及数据安全与合规、OT 系统安全、上云安全。

三、破解制造企业工业安全威胁之“道”

面对日益严峻的安全问题，制造企业已经表现出积极应对安全问题的需求。然而，如何破解工业安全威胁，对于制造企业来讲仍然是一个巨大的挑战。

1.“破”工业安全之困局

目前，制造企业普遍缺乏安全策略和管理制度，尚未建立专业安全队伍，尚无应急响应计划。在安全威胁攻击面前，制造企业是非常缺乏有效防护措施的。与此同时，制造企业的潜在攻击面正随着越来越开放的工业环境不断扩大，已经远远超出了传统的 IT 安全，涵盖设备安全、工控安全、数据安全、上云安全等。

面对如此严峻的形势，制造企业究竟该如何应对工业安全风险？

在当前工业环境中，OT 环境的目标价值及安全系统的复杂程度相对更高。机械装备行业尤为如此，设备种类多、通讯协议复杂，设备供应商多、工控系统繁杂，数据种类多、数据量大，设备远程运维、预测性维护需求不断增多，使得 OT 环境中风险来源更多，全球范围内针对 OT 系统的复杂攻击也确实正在增加。而且 OT 环境一旦受到攻击，更容易带来严重的破坏。

制造企业 OT 环境是独一无二的，其面临的 OT 安全挑战也是不尽相同的。首先，IT 安全的机密性、完整性和可用性的典型 KPI 在 OT 安全并不完全适用，以 IT SOC 与 OT SOC 为例，IT SOC 重点保护信息的机密性、完整性和可用性，OT SOC 必须满足可用性、可见性、稳定性等方面的严苛需求。其次，从安全性的角度来看，OT 环境是非常新颖或不成熟的，比如渗透测试也可能会导致停机，企业工控系统常常会在没有进行补丁修复的情况下运行。再者，每个企业的应急

事件响应机制不同，同一份响应计划可能不适用于其他企业。

因此，OT 安全必须得到重视，并成为机械装备行业等企业的优先事项。

IT SOC

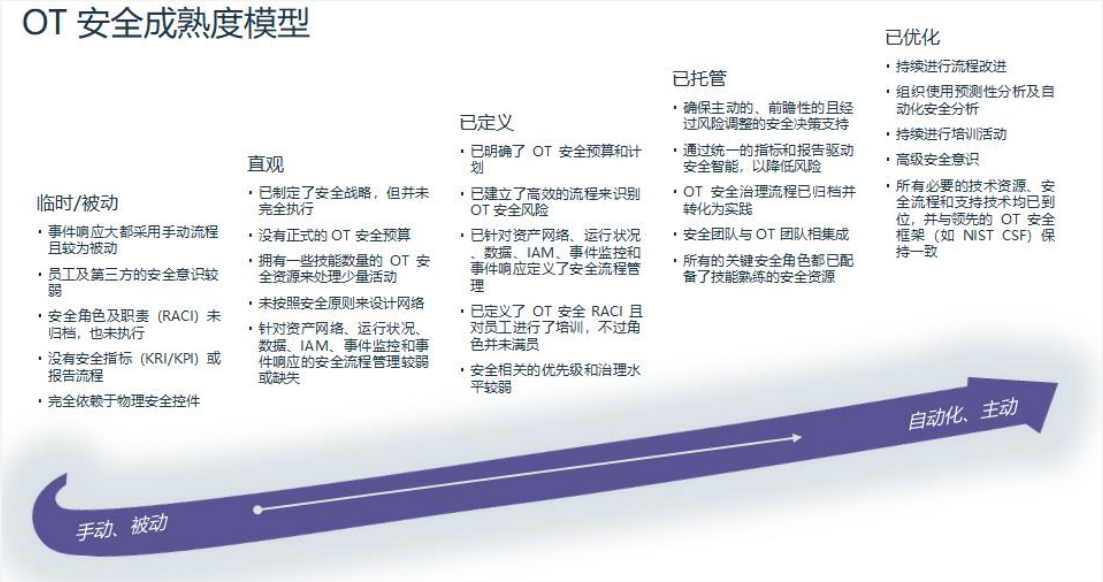
- 重点保护信息资产的机密性、完整性和可用性
- 底层业务流程上下文对于管理安全威胁/事件并不总是至关重要的
- 通常由10名员工组成的团队负责全天候运营
- 通常位于单独的设施中，由不同的IT组管理升级
- 每天记录在仪表板中的事件/违法事件数可以成百上千地运行，这取决于范围和已建立的详细级别
- OT过程安全监控范围通常限于网络边界
- 通过取证分析和逆向工程建立攻击者动机的深厚技术专长

OT SOC

- 专注于确保保持支持核心业务的流程或系统的最佳运行状态，而不是数据丢失。例如：在水处理中使用适当的氯剂量，以避免中毒
- OT SOC员工需要了解工业过程和支持功能，以识别、响应和管理事件
- 员工人数通常是IT SOC的一半，具有类似的监控范围，但是，需要OT技术方面的技术能力
- OT SOC通常可集成在现有的过程控制室内，以实现有效的OT运行响应。上报涉及IT和非IT组
- 设计目标是对误报有零容忍度。因此，由于封闭的环境，事故的数量通常很低
- 围绕与设施用途相关的特定工业过程设计的用例。例如：锅炉温度传感器信号/遥测网络受到操纵/干扰，导致测量不准确或偏离控制室接收到的温度设定值
- 串行协议、无日志、非IT协议，如IEC 61850 GOOSE、IEC 104、MODBUS和其他需要特定解析器/协议分析仪来收集数据并转发给OT SOC系统的其他协议

2.“立”工业安全之法则

每个企业都有其独特的安全建设征程。尽管当前各个企业的征程互不相同，一部分企业已经快要达到成熟度目标，一部分企业刚刚起步，但有一点是共通的：企业均希望改善其安全计划。为此，IBM 建立了一个 OT 安全成熟度模型，以帮助企业准确定位其 OT 安全建设现状以及未来改进方向。对于大多数企业来说，首先要做到的关键步骤是第三阶段，即“已定义”这一阶段，也就是“已在整个组织内定义、标准化并集成了流程”。



IBM 的 OT 安全成熟度模型所表现的总体趋势是将企业 OT 安全管理从人工、被动的方法向更加自动化、更加主动的方法转型。针对企业 OT 安全建设需求，IBM 也提供了完善的安全解决方案组合，通过风险评估、扩展可视化、减缓威胁三大步骤，帮助企业加快其 OT 安全成熟之旅。

在了解风险阶段，主要是了解企业业务所拥有的独特风险，比如当前企业风险有哪些？减缓风险的整体安全战略是什么？在扩展可视性阶段，将获得对企业工业环境的可视性，比如需要保护的设备数量有多少？企业网络情况如何？拥有哪些类型的用户？解决方案情况如何？在减缓影响阶段，为企业规划、实施和管理解决方案。

（1）了解风险

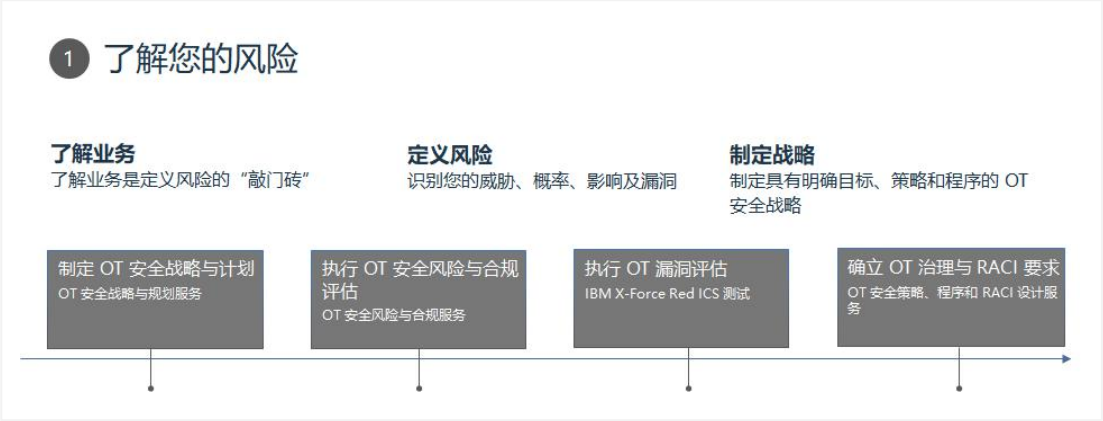
通过了解企业自身业务现状和发展战略，识别企业所拥有的独特风险及其属性，比如流程可靠性、数据完整性、正常运行时间、合规性、隐私性等，评估风险发生概率和影响，由此制定明确的安全目标、策略和要求。整个阶段将以符合 OT 生态系统特点的独特方式完成。同时，IBM 将与企业的运营部门共同建立联合风险试图。

此阶段安全建设需要分阶段采取行动，包括：

- 制定 OT 安全战略与计划
- 执行 OT 安全风险与合规评估
- 执行 OT 漏洞评估

- 确立 OT 治理与 RACI 要求

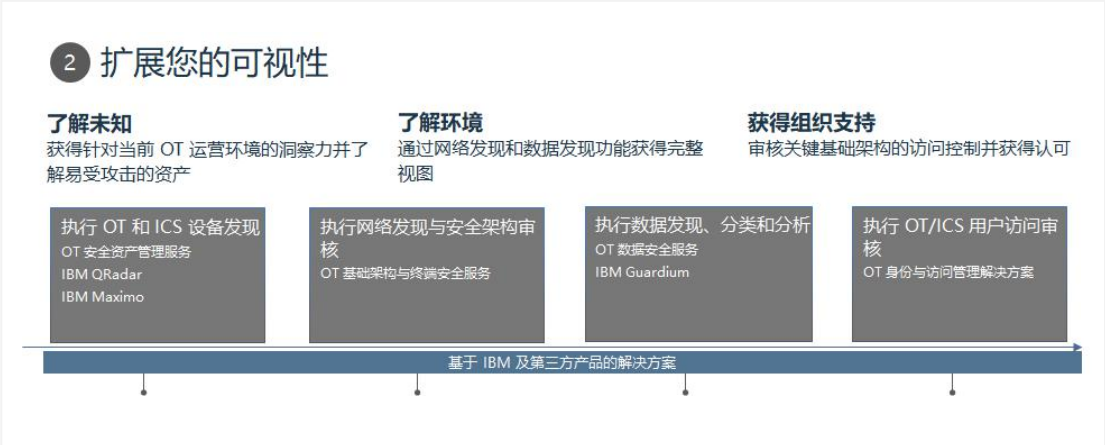
在这个领域，控制和治理的确非常重要，大多数制造企业内部都没有能力和技能做到这一点。IBM 专家可以通过相应解决方案为企业提供服务。



（2）扩展可视性

在了解企业面临的风险，并且制定了减缓风险的战略之后，需要确保企业基础架构的可视性，因为通常无法保护看不到的东西。这一阶段将考虑网络设计和架构，是否需要重新设计，以提高网路性；考虑数据分类，用户访问是否合理，以实现安全性。IBM 的合作伙伴生态系统可为制造企业提供支持：

- 获得针对当前 OT 运营环境的洞察力
- 了解易受攻击的资产
- 预测攻击向量和路径
- 异常检测
- 网络发现和架构
- 数据发现和分类
- 访问审核
- 调整优先事项并获得支持

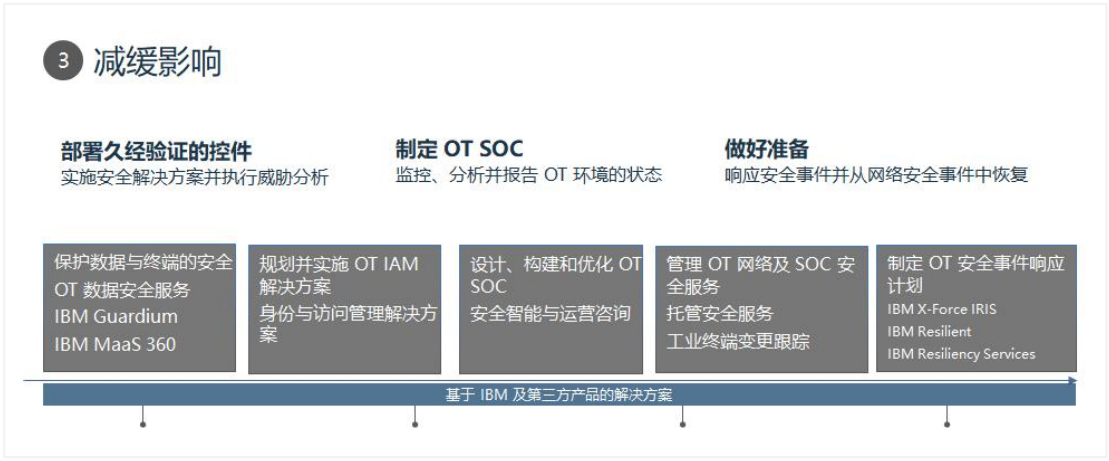


（3）减缓影响

在对企业具体的业务和工业环境完成全面分析和评估之后，将进行具体解决方案的设计、实施和管理，将会涵盖：

- 保护数据与终端的安全
- 实施 IAM
- OT SOC
  - 实施安全解决方案
  - 监控、分析和报告安全状态
  - 维持安全状态
  - 管理用户访问
  - 执行威胁分析
  - 响应安全事件
  - 从网络安全事件中恢复
  - 提升安全意识

在此阶段，OT SOC 构建是一个难点。工业领域目前还没有 SOC，OT SOC 与 IT SOC，无论是在用例与策略上，还是对事件和特定事件的响应方式上，都截然不同。IBM 及合作伙伴可以为制造企业设计、构建和优化 OT SOC，以监控、分析并报告 OT 环境的状态。



制造企业工业安全建设是一个全新的领域，也是一场持久战，对于机械装备行业企业也是如此。在企业 OT 安全起步建设和持续完善过程中，丰富的行业专业知识和经验将起到非常关键的作用。IBM 作为全球最大的安全供应商，拥有深厚资源、专业知识、先进技术以及众多合作伙伴，已经并正在帮助全球范围内的许多企业推动他们的 OT 安全旅程，构建企业工业安全的坚固堡垒，为企业发展保驾护航。