中国工业互联网安全调研报告（2018）

工业控制系统安全国家地方联合工程实验室**2019.3**

主要观点

* 工业企业对工业互联网安全的重视程度越来越高，安全投入呈现增加趋势，工业互联网安全市场将有巨大的需求；
* 虽然多数工业企业对工业网络安全重视程度越来越高，但对自身网络安全建设处于一种过度乐观的状态，较低的估计了自身遭受网络攻击的可能性，对于生产车间网络安全事件处于“不知情”的状态；
* 将近一半工业企业遭受过生产设备安全故障、电脑蓝屏、重启等安全问题，但确有69.4%的企业表示没有发生过网络安全事件。当企业内部电脑出现大量蓝屏、重启等现象时，往往意味着企业已经遭到了攻击，但企业管理者未作为安全事件来进行响应和调查，错过处置最佳时机；
* 防护类产品需求较高，网络安全关注度高；非防护类产品比例相当，呈现多样化趋势；安全服务市场总体形式较乐观；工业安全产品和服务体系日益完善；
* 目前看不到收益、人才缺乏是阻碍安全投资建设的重要因素。工业互联网安全建设最大的难处在于没有造成安全事故，企业高层较难理解安全建设短时间内给企业带来的收益，工业互联网安全建设不被工业企业理解；
* 多方协作趋势明显，构建产业协同的联合防御体系。安全企业需要不断深入与更多的工业企业、工控系统集成商、安全厂商进行生态合作与交流，为工业企业客户提供更加优质的工业互联网安全解决方案。

摘要

* 工业企业对自身安全建设程度普遍“自我感觉良好”，实际上是一种过度乐观的状态。绝大多数工业企业的实际安全状况都让人十分堪忧；
* 国内53.1%的企业遭受过生产设备安全故障、电脑蓝屏、重启等安全问题，仅有不足25%的企业没有出现过蓝屏、重启现象，我国工业互联网安全建设情况并不乐观；
* 将近有1/4的被调研企业表示对生产车间设备、电脑是否出现过蓝屏、重启现象表示“不掌握”。“不掌握”也就意味着企业其实并没有部署足够的网络安全监测措施以实时了解其工业系统的网络安全状况；
* 多数工业企业过低的估计了自身遭受网络攻击风险的可能性；
* 国内76.1%的工业用户非常重视工业互联网安全的建设；将近49.1%的工业企业在安全方面的投入有明显增加趋势；超过1/4的企业对安全的投资金额在10-100万之间；国内43.9%的被调查者认为工业互联网安全投入应该占工业互联网投入金额的5%-10%；
* 人才的缺乏是影响工业互联网建设的首要因素，看不到收益仍然是阻碍安全投资建设的最主要因素；
* 国内69.1%的工业企业有专门的人员/部门负责安全，但负责安全的人数差距较大；
* 八成以上的国内工业企业有意愿部署工业互联网安全服务，39%的企业能够接受的采购费用低于20万；
* 安全问题发生后，国内51.8%以上的企业愿意选择一家综合能力强的规模较大的安全厂商解决安全问题；
* 防护类产品需求较高，网络安全关注度高；非防护类产品比例相当，呈现多样化趋势；安全服务市场总体形式较乐观；工业安全产品和服务体系日益完善；
* 多方协作趋势明显，构建产业协同的联合防御体系。

目 录

[研究背景 1](#_Toc3216106)

[第一章 工业企业视角下的安全现状 2](#_Toc3216107)

[一、 工业企业对自身安全建设水平的认知 2](#_Toc3216108)

[二、 工业企业对自身面临安全风险的感知 2](#_Toc3216109)

[三、 工业企业对网络安全事件影响的认知 4](#_Toc3216110)

[四、 工业企业对工业安全重视程度的感知 5](#_Toc3216111)

[五、 工业企业对工业网络安全团队的认知 6](#_Toc3216112)

[第二章 企业在工业互联网安全上的投入分析 7](#_Toc3216113)

[一、 工业互联网用户每年在工业互联网网络安全中的资金投入分析 7](#_Toc3216114)

[二、 阻碍工业互联网安全投资建设的主要因素 8](#_Toc3216115)

[第三章 工业企业网络安全市场需求 10](#_Toc3216116)

[一、 工业互联网安全产品需求 10](#_Toc3216117)

[二、 工业互联网安全服务需求 10](#_Toc3216118)

[三、 工业互联网安全应急响应需求 11](#_Toc3216119)

[第四章 工业企业网络安全发展趋势 12](#_Toc3216120)

[一、 工业企业安全意识有所提高，安全服务市场扩大 12](#_Toc3216121)

[二、 多方协作趋势明显，构建产业协同的联合防御体系 13](#_Toc3216122)

[三、 技术层面深度创新 13](#_Toc3216123)

[第五章 总结 14](#_Toc3216124)

[附录一 工业控制系统安全国家地方联合工程实验室 15](#_Toc3216125)

研究背景

在政策与技术的双轮驱动下，工业控制系统正在越来越多地与企业内网和互联网相连接，并与新型服务模式相结合，逐步形成了工业互联网架构。工业互联网是数字浪潮下，工业体系和互联网体系的深度融合的产物，是新一轮工业革命的关键支撑。工业互联网的发展一方面极大的促进了生产效率和服务水平的提高，另一方面也使原本封闭的系统变得越来越开放，致使系统安全风险和入侵威胁不断增加，网络安全问题日益突出。

工业互联网目前已经广泛应用于电力、交通、石油、取暖、制造业等关键信息基础设施领域，一旦发生安全事件，往往会造成巨大的损失和广泛的影响。但是，由于工业互联网环境的特殊性，传统的IT信息安全技术并不能完全有效的保护工业系统的安全，甚至很多常用的安全技术都不能直接应用于工业网络的安全防护。对于工业互联网安全的分析与防护，需要使用一些专门的方法和专用的技术。

工业控制系统安全国家地方联合工程实验室（以下简称“联合实验室”）于2017年发布《IT/OT一体化工业信息安全态势报告》，总结分析IT/OT融合带来的新挑战，给出工业信息安全建议和展望。

联合实验室为了更全面的了解工业互联网企业网络安全现状，本报告特别对近400家工业企业进行了问卷调查，深入研究工业企业视角下的网络安全感知、资金投入、市场需求、发展趋势等，最终形成《中国工业互联网安全调研报告》，供合作伙伴及企业客户决策参考使用。

《中国工业互联网安全调研报告》内容被综合收录到 《IT/OT一体化工业信息安全态势报告（2018）》年度报告中。《IT/OT一体化工业信息安全态势报告（2018）》是续2017年发布《IT/OT一体化工业信息安全态势报告（2017）》后，总结分析2018年工业互联网IT/OT融合带来的新挑战，安全现状、产业发展趋势、重大应用案例等，给出2019年工业信息安全建议和展望。

最后，希望本报告能够帮助读者对工业互联网安全有一个更加全面、前沿的认识。

1. 工业企业视角下的安全现状

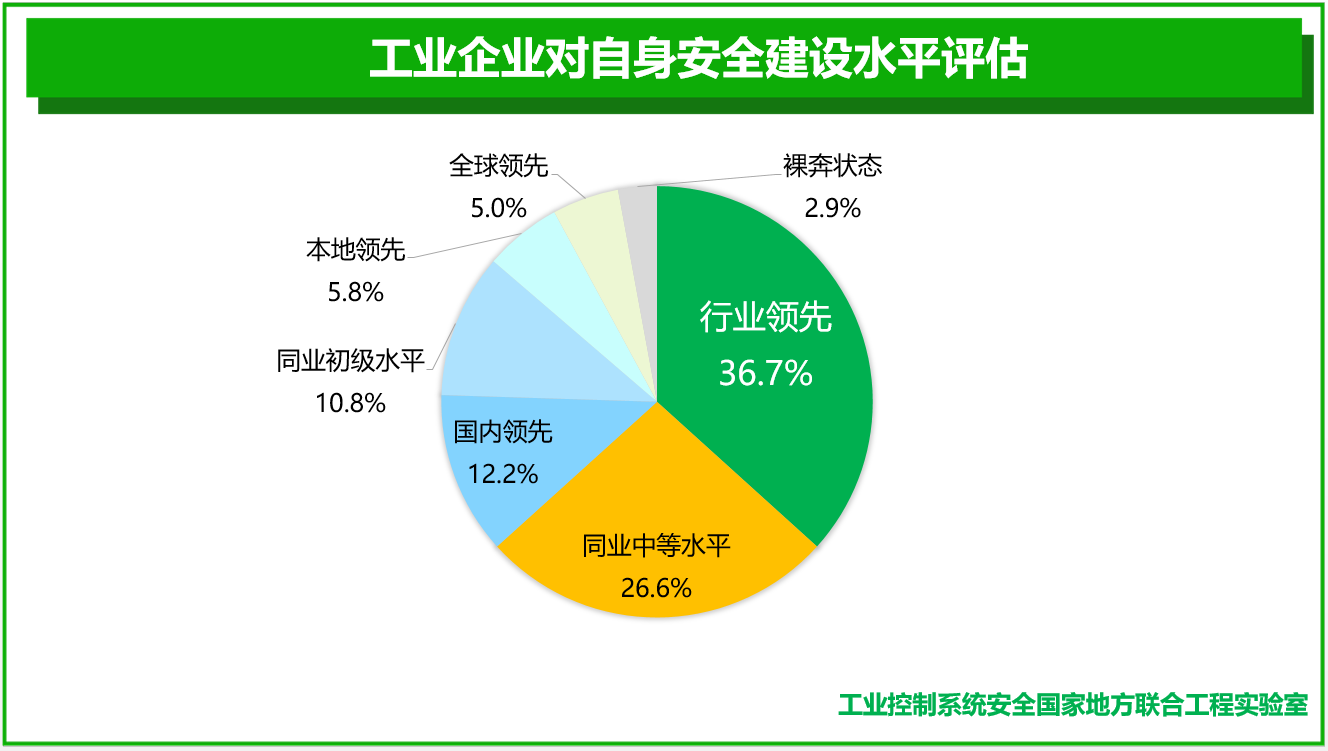
2018年，联合实验室在全国范围内对工业企业用户进行了一次系统的深入调研。根据参与行业的单位属性将制造业、市政/交通、通信/网络、石油石化/化工、能源电力用户填写的问卷作为有效数据进行分析。关于本次调研的详细情况，可参见本报告“研究背景”一节的相关介绍。

本小节将主要从工业企业对自身网络安全状况的认知和感知、安全团队情况，来分析工业企业的安全现状。

1. 工业企业对自身安全建设水平的认知

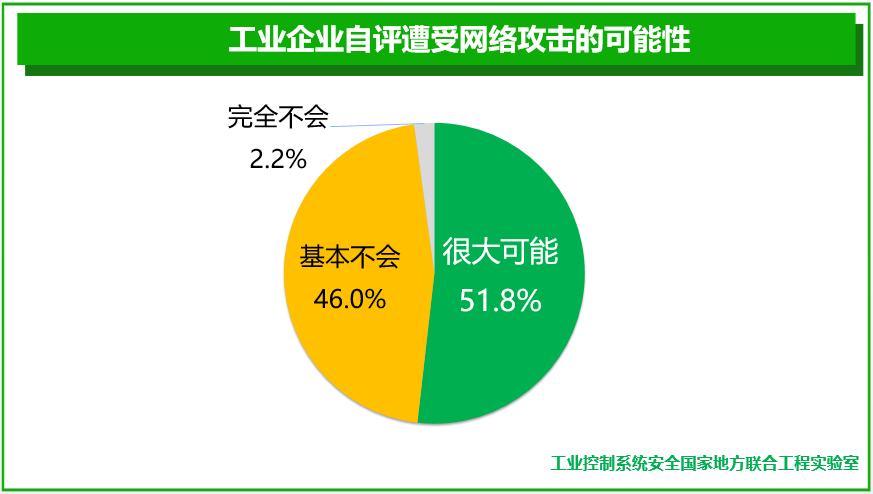
调查显示，工业企业对自身企业安全建设水平普遍有较高的认识，**36.7%的被调查者认为自己所在企业网络安全建设水平达到行业领先**；仅有2.9%的被调查者认为，自己所在的企业网络安全建设水平处于“裸奔”状态。

需要说明的是，根据联合实验室在全国各地工业企业的实地考察情况来看，工业企业对自身安全建设程度普遍“自我感觉良好”，实际上是一种过度乐观的状态。绝大多数工业企业的实际安全状况都让人十分堪忧。



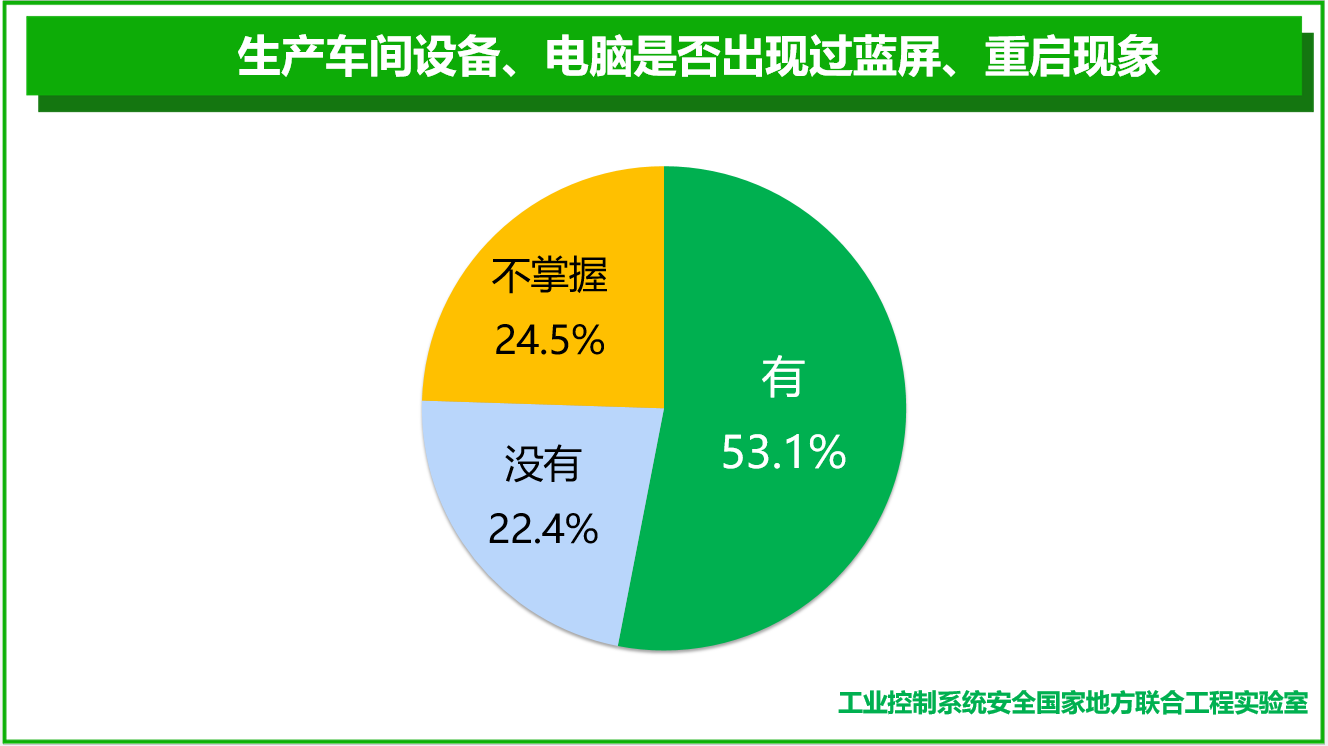
1. 工业企业对自身面临安全风险的感知

调查还显示，在被问及自己所在的工业企业是否会遭受网络攻击时，认为会遭到攻击的人和认为不会遭到攻击的人几乎各占一半。

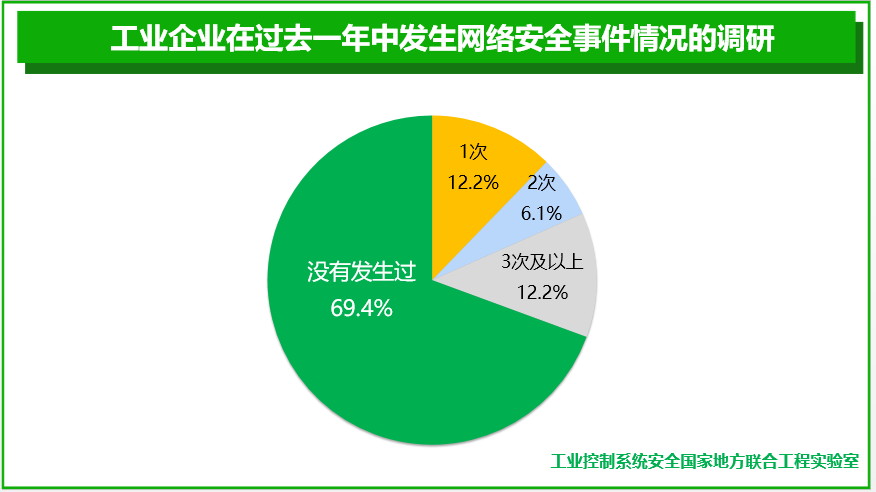


针对生产车间设备、电脑出现蓝屏、重启现象进行调研分析发现，超过50%的企业遭受过生产设备安全故障问题，仅有不足1/4的企业没有出现过这些现象；另有约1/4的企业对此问题表示 “不掌握”相关情况。详见下图。

其实“不掌握”，这一结果可能是最可怕的一种风险。因为“不掌握”也就意味着企业其实并没有部署足够的网络安全监控措施以实时了解其工业系统的网络安全状况。这也说明，很多工业企业对自身网络安全建设水平处于业内领先地位的评估可能是过于乐观。



在被问及过去一年中，是否发生过网络安全事件时，69.4%的被调查企业表示没有发生过；表示发生过1次的有12.2%；2次的6.1%；3次及以上的占比12.2%。



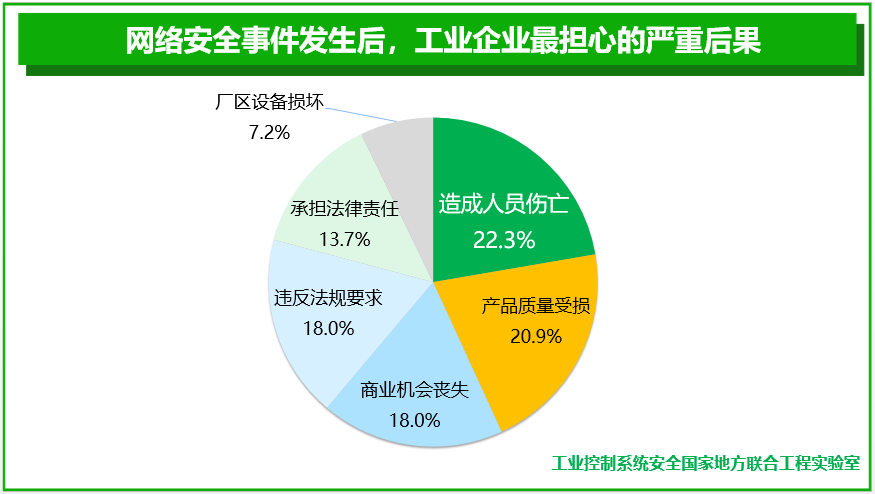
将上述三组数据的结果进行对比分析，我们就会发现：**多数企业确实过低的估计了自身遭到网络攻击风险的可能性**。事实上，当企业内部电脑出现大量蓝屏、重启等现象时，往往意味着企业已经遭到了攻击，只是很多企业的管理者并没有把这些事件作为安全事件来进行响应和调查，而只是当作一般的系统故障而已，从而可能导致其错过发现问题的最佳时机。

一句话，企业认为自己没有遭到过攻击，但实际上有迹象表明他们可能已经遭到了攻击，只是自己不知情或没有意识到这些现象可能与攻击有关。

此外，从应急响应或现场处置过的大量事件看，绝大多数自认为没有安全问题的工业企业，往往都存在着巨大的安全漏洞，他们对于安全事件只是处于“不知情”的状态。

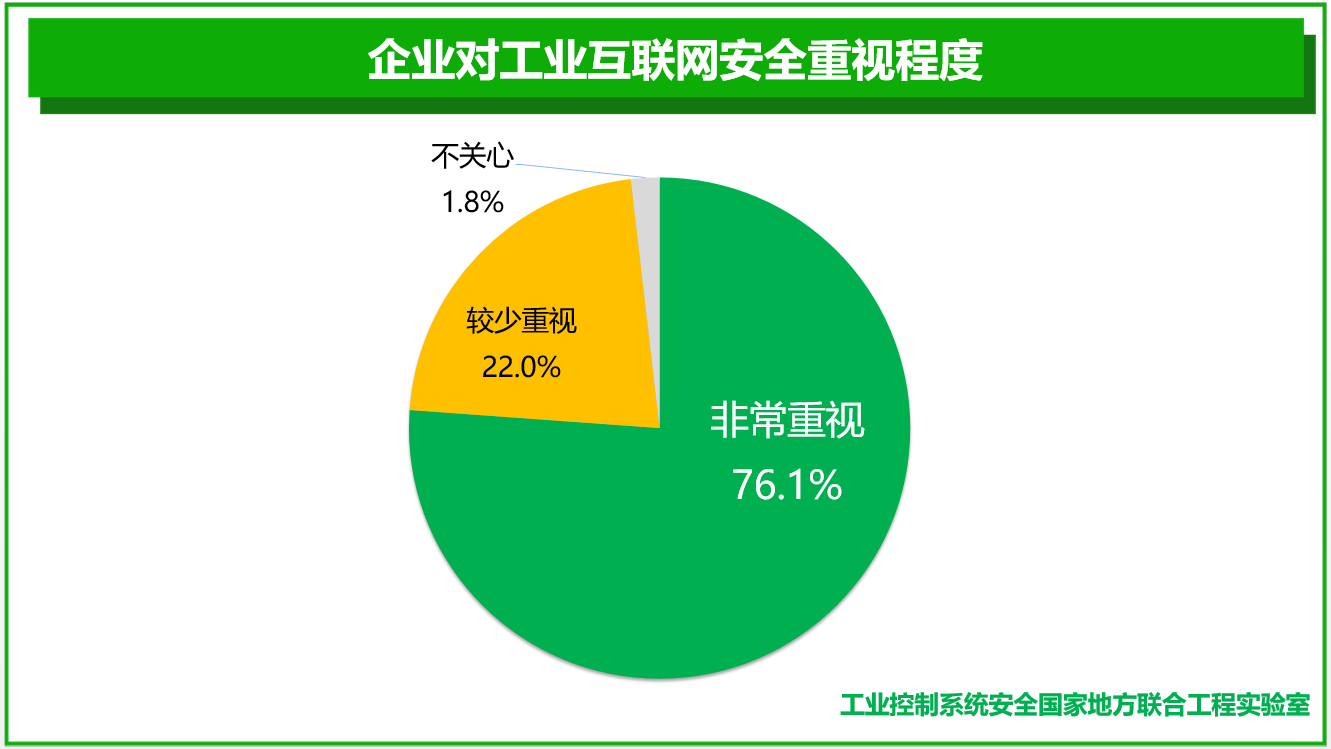
1. 工业企业对网络安全事件影响的认知

调查显示，一旦遭遇网络安全事件，22.3%的工业企业最为担心的严重后果是造成人员伤亡；其次为产品质量受损，占比20.9%，接下来是商业机会丧失、违反法规要求、承担法律责任、厂区设备损失等。需要特别说明的是，**人员伤亡和产品质量受损，是工业企业遭遇网络安全事件时所需面对的特殊风险**，一般的政府机构、企业，或IT、互联网公司都无需面对此类风险。

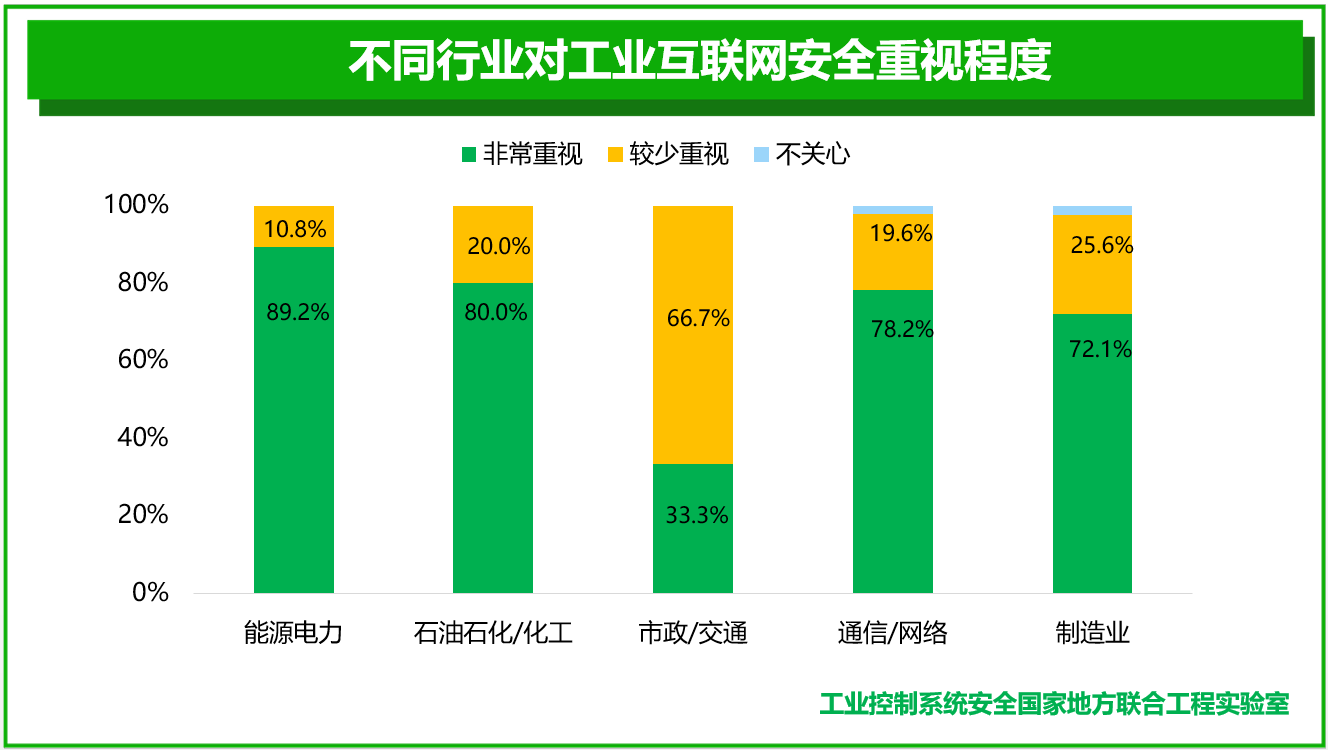


1. 工业企业对工业安全重视程度的感知

通过对问卷调查数据统计发现，2018年工业互联网行业用户对安全的重视程度较高，有**76.1%的工业用户非常重视工业互联网安全的建设**，根据卡巴斯基《2018工业网络安全现状》中统计结果，77%的受访者认为网络安全是重中之重。国内外的工业企业都已经非常关注工业互联网安全的建设和部署。

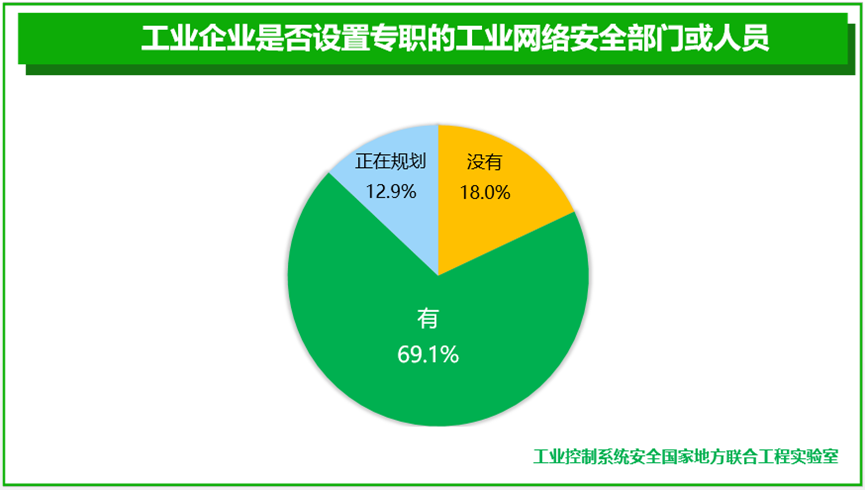


针对不同行业对工业互联网安全重视程度进行分析，统计结果发现，**市政/交通行业、制造业对工业互联网安全重视程度相对较低**，其中市政/交通行业重视程度最低。

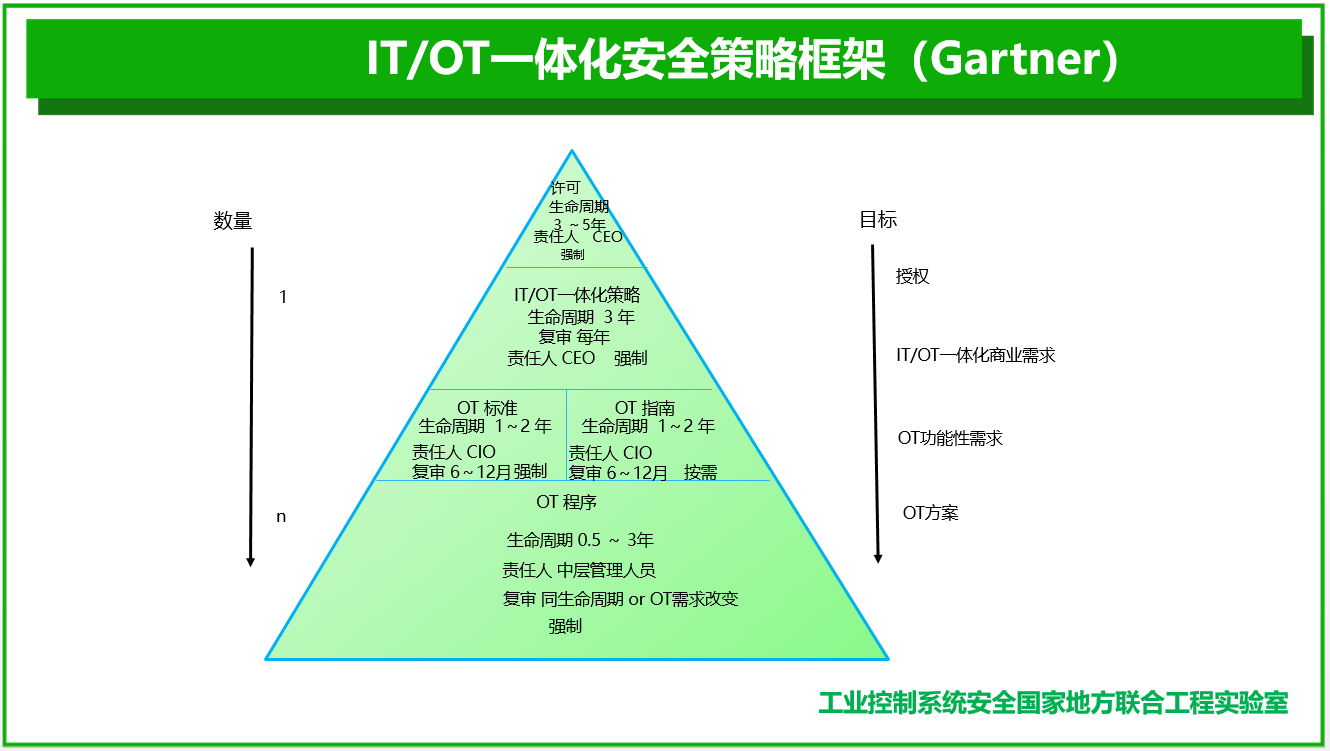


1. 工业企业对工业网络安全团队的认知

是否设置专职的工业网络安全部门或人员在一定程度上反映出工业企业自身网络安全建设水平。对工业企业是否设置专职的工业网络安全部门和人员进行统计分析发现，**69.1%的工业企业有专门的人员/部门负责安全**，12.9%的企业正在规划，可见多数企业已设置或者正准备设置安全部门或人员。

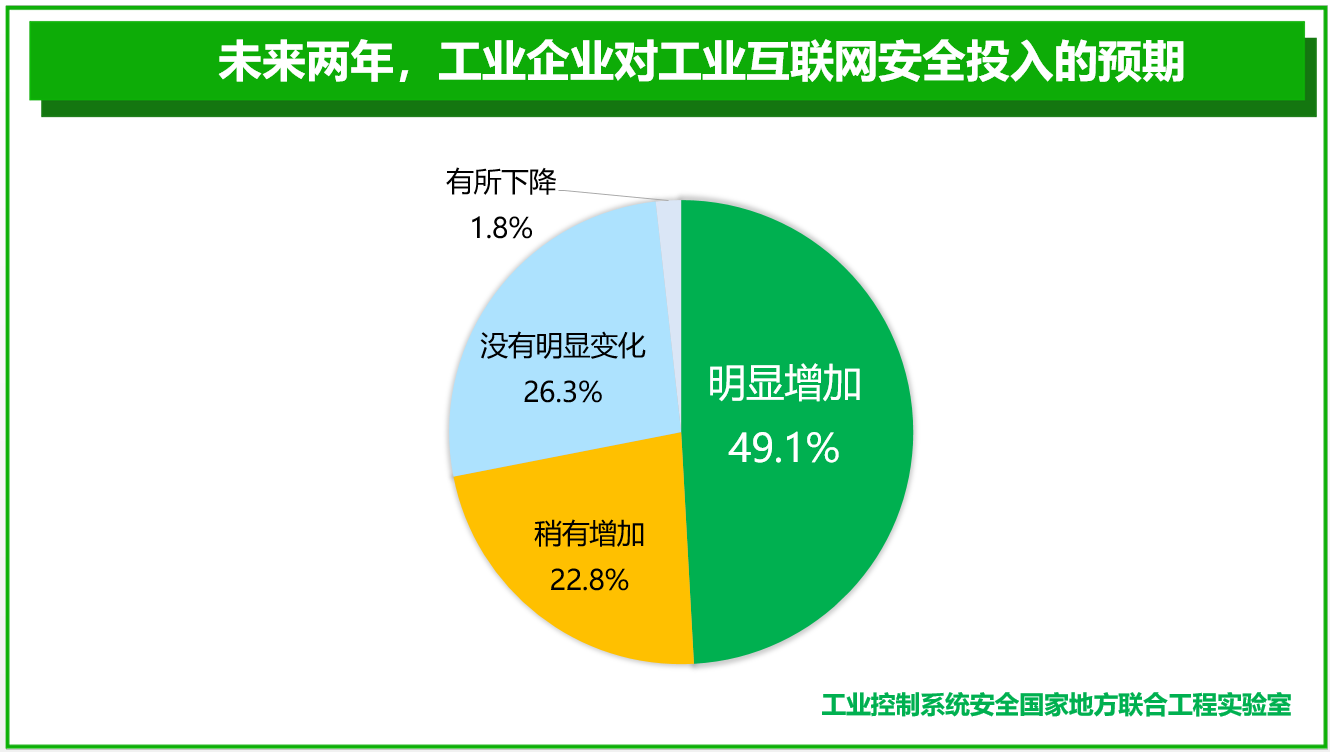


**除了工业网络安全团队外，在工业网络安全建设方面，IT部门参与程度最高，达到37%**。董事长或高级管理人员的参与程度相对较低，仅占到10%。根据Gartner发布的IT/OT一体化安全策略框架，从上层到下层，其都有企业高层或者管理人员参与，高层领导对工业互联网安全的重视程度在一定程度上能够促进工业安全的落实与发展。



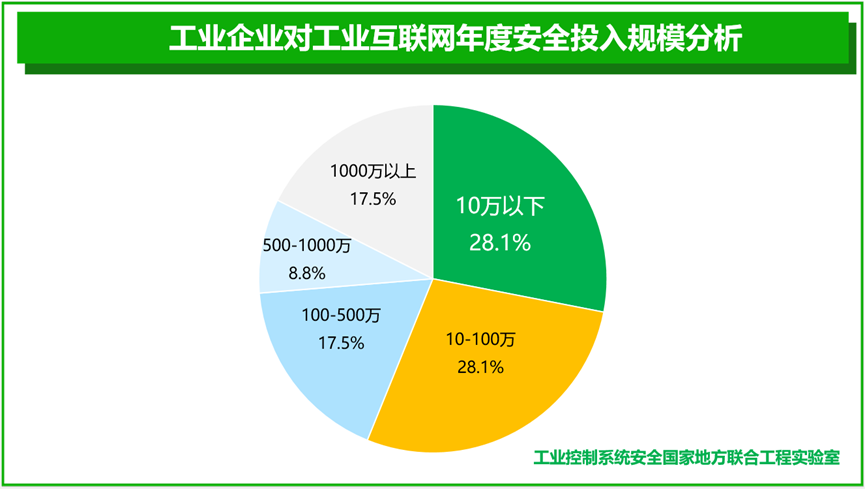
1. 企业在工业互联网安全上的投入分析
2. 工业互联网用户每年在工业互联网网络安全中的资金投入分析

未来两年，有49.1%的被调查工业企业在安全方面的投入有明显增加趋势，22.8%的企业投入的资金稍有增加。总体来看，工业互联网企业对安全的投入有一个良好的趋势，也充分说明了工业互联网用户对工业互联网安全的重视程度越来越高。

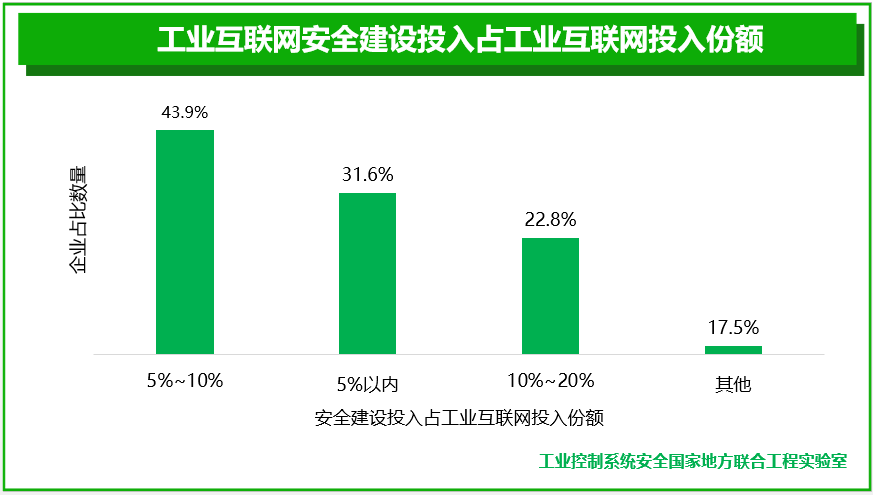


被调查的工业互联网企业计划在工业互联网网络安全方面投入的资金规模集中在10万以下或者10-100万之间，占比均为28.1%。**超过1/2的被调查企业对安全的投资金额集中在此范围内**。由此可见，工业互联网安全市场还有较大的提升空间。

值得关注的是，大型制造企业和通信/网络对安全投入规模较大，其中17.5%的被调查企业年度安全投入超过1000万，呈现一个跨越式进阶投资，一部分企业已经非常重视工业互联网安全的建设，纷纷开始布局。

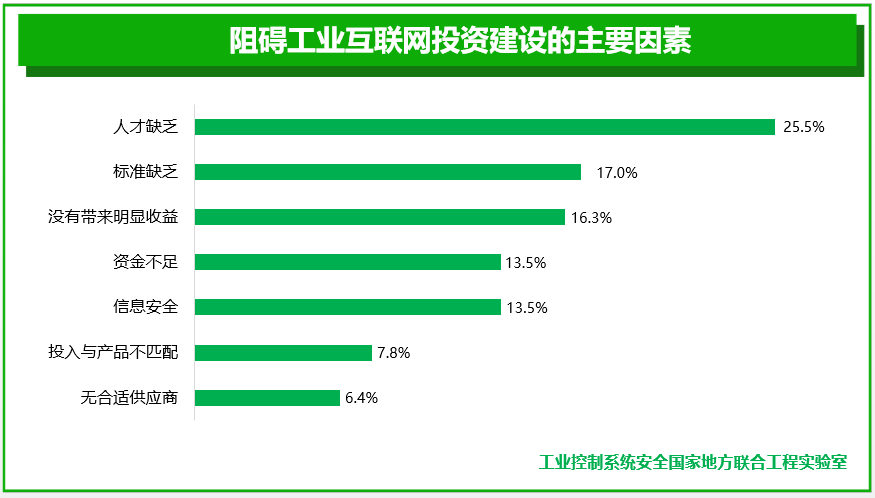


针对工业互联网安全建设费用占工业互联网投入份额进行统计分析发现，43.9%的被调查者认为应该占工业互联网投入金额的5%-10%之间，投入份额在10%以下的企业达到3/4以上。可见，**针对工业互联网安全建设的投入金额比例总体还是偏低的**。虽然工业企业对工业互联网安全的重视程度相对提高，但总体资金投入仍不足。

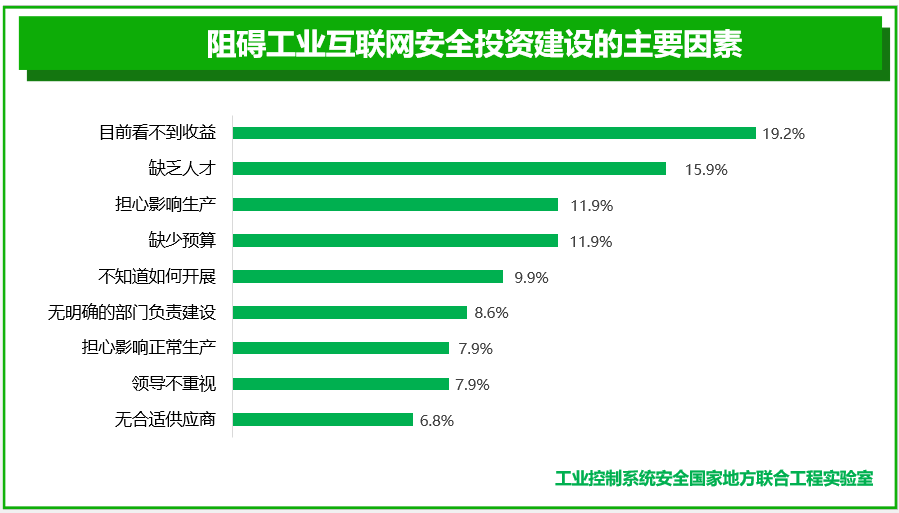


1. 阻碍工业互联网安全投资建设的主要因素

为了更全面的了解总体资金投入不足的影响因素，首先分析阻碍工业互联网投资建设的原因。经过统计分析发现，**人才缺乏是影响工业互联网建设的首要因素**，值得注意的是信息安全和资金不足占据相同的比例。可见信息安全在工业互联网投资建设中影响越来越大。



针对工业互联网安全投资建设的影响因素分析发现，**目前“看不到收益”仍然是阻碍安全投资建设的最主要因素**。工业互联网安全建设最大的难处在于没有造成安全事故，企业高层较难理解安全建设短时间内给企业带来的收益，工业互联网安全建设不被工业企业理解。



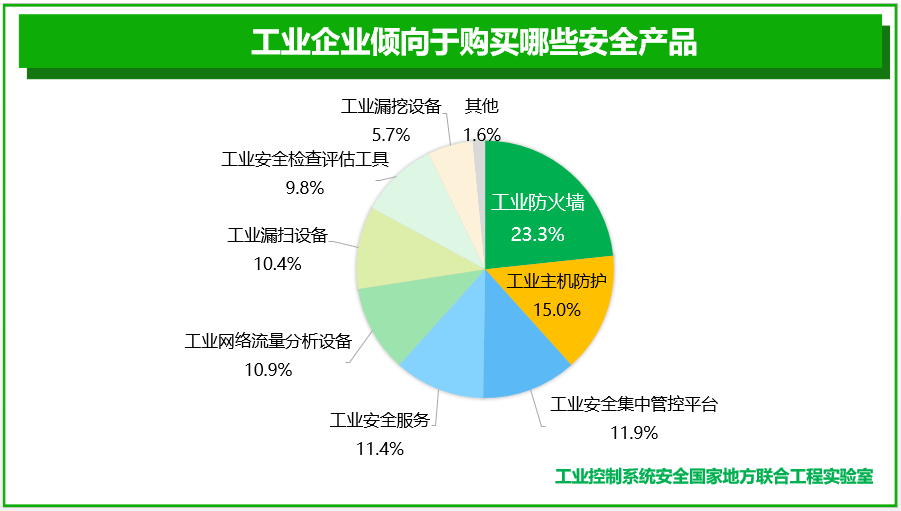
无论是工业互联网建设还是工业互联网安全建设，人才的缺乏都是阻碍发展的重要因素。根据国际非盈利会员学会（ISC）2 2018年网络安全劳动力研究表明，北美、拉丁美洲、亚太地区以及欧洲、中东和非洲的**全球网络安全人才缺口已扩大至近300万**。根据360互联网安全中心和智联招聘联合发布的《2018网络安全人才研究状况研究报告》统计，2018年上半年，网络安全人才需求规模指数较2017年上半年同比增长了44.9%，与2017年下半年相比环比增长了9.4%。可见，对网络安全人才的强劲需求还将持续较长时间。

1. 工业企业网络安全市场需求
2. 工业互联网安全产品需求

**防护类产品需求较高，网络安全关注度高。**工业防火墙、工业主机防护、工业安全集中管控平台三个产品所占比例高达50.2%，占据工业安全产品比例的一半，工业安全集中管控平台主要为防护类产品做管控，将其归为防护类。由统计结果可见，防护类产品需求总体较高，工业防火墙占比23.3%，在工业安全产品体系中所占比重最高，可见工业企业的首要关注点在工业企业的网络安全建设方面。

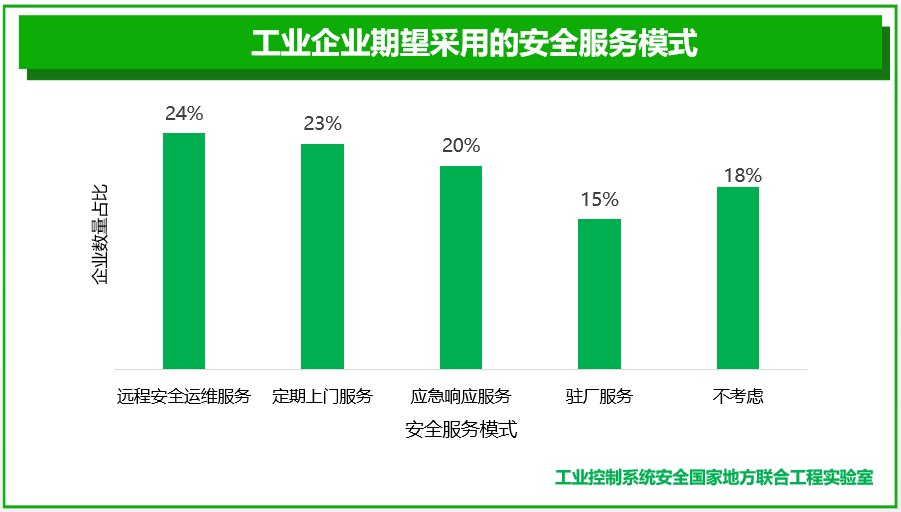
其次为工业主机防护，工业主机老旧操作系统较多，工业主机在投运后会运行很多年，硬件资源受限，同时存在老旧操作系统，往往难以安装杀毒等IT安全防护软件。因此，工业主机目前基本处于没有任何安全防护软件的裸奔状态，而且运行时间较长存在众多的漏洞，因此工业主机的安全防护也是势在必行。

**非防护类产品比例相当，呈现多样化趋势。**工业网络流量分析设备占比10.9%、工业安全服务占比11.4%、 工业漏扫设备占比10.4%、工业安全检查评估工具占比9.8%、工业漏挖设备占比5.7%。相对来说，各产品所占比例相当，呈现多样化趋势。安全检测类、安全评估类、安全服务类、安全研究类产品发展平衡，工业安全产品和服务体系日益完善。

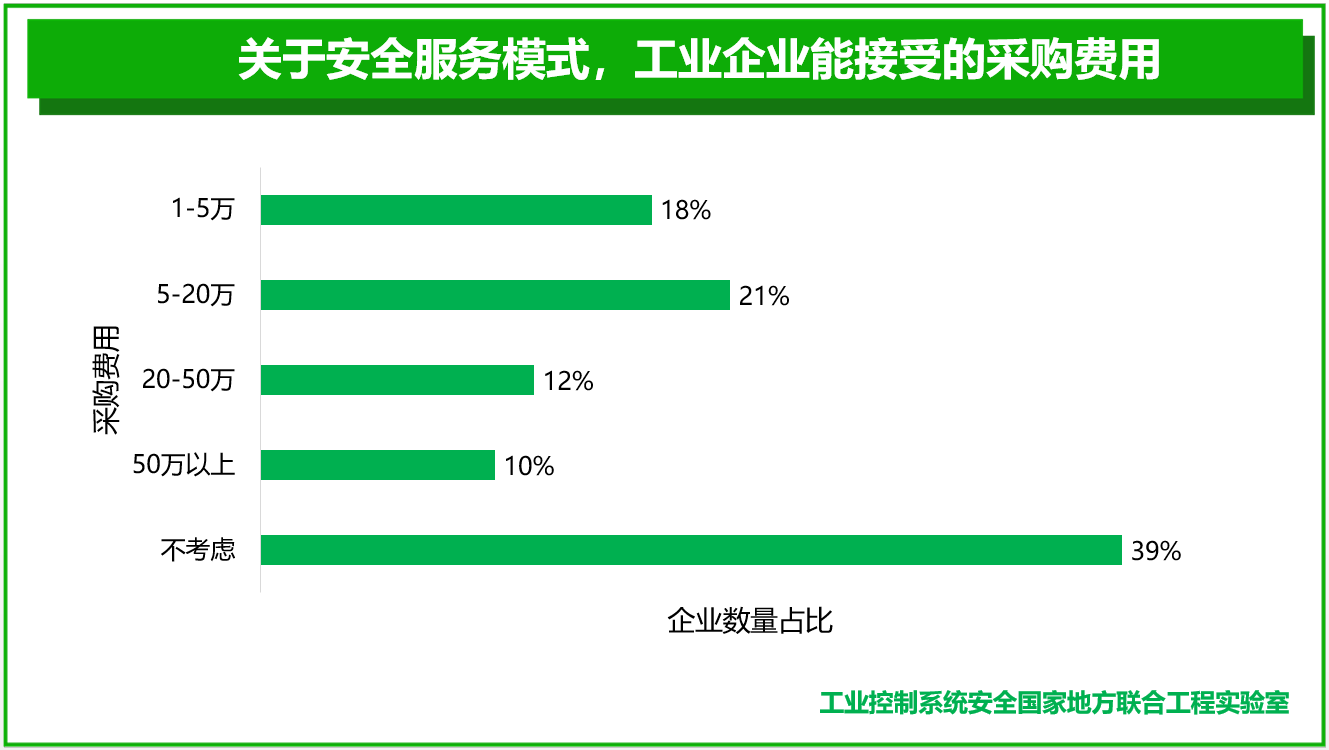


1. 工业互联网安全服务需求

对被采访者进行工业互联网安全服务的调查分析，82%的被采访者企业考虑采用“工业互联网安全托管服务”，仅有18%的企业不考虑。其中远程安全运维服务占比最高，达到24%，驻场服务相对较少，占比15%。远程安全运维服务相对而言，所需成本较低，驻场服务成本偏高。企业所选择的工业互联网安全服务随着各服务成本的增多，其选择的比例相对较少。不管是选择何种安全服务，**总体有意愿部署工业互联网安全服务的企业达到4/5以上**，安全服务市场总体形式较乐观。

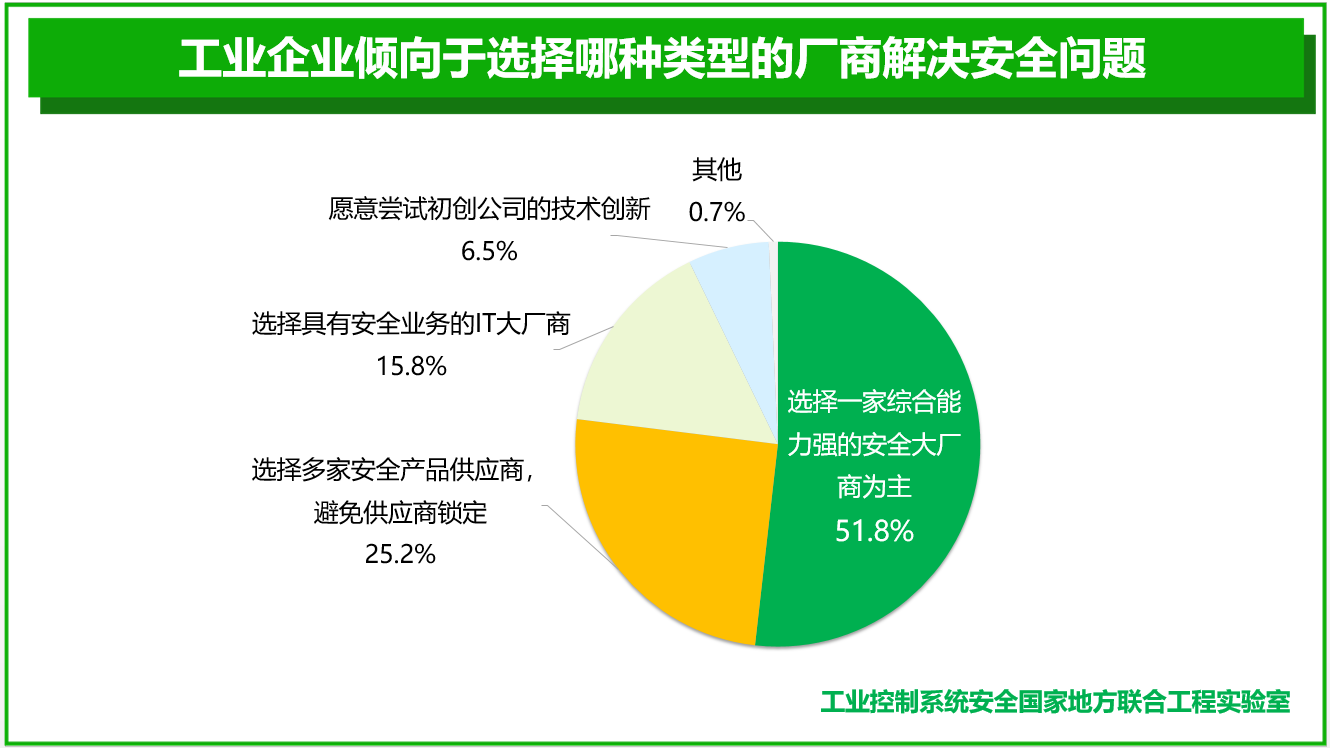


针对工业互联网安全服务所能接受的采购费用进行分析，**低于20万的企业占比达到39%，**从采购费用的占比上也一定程度反映出企业选择相对费用较低的安全服务模式的原因。



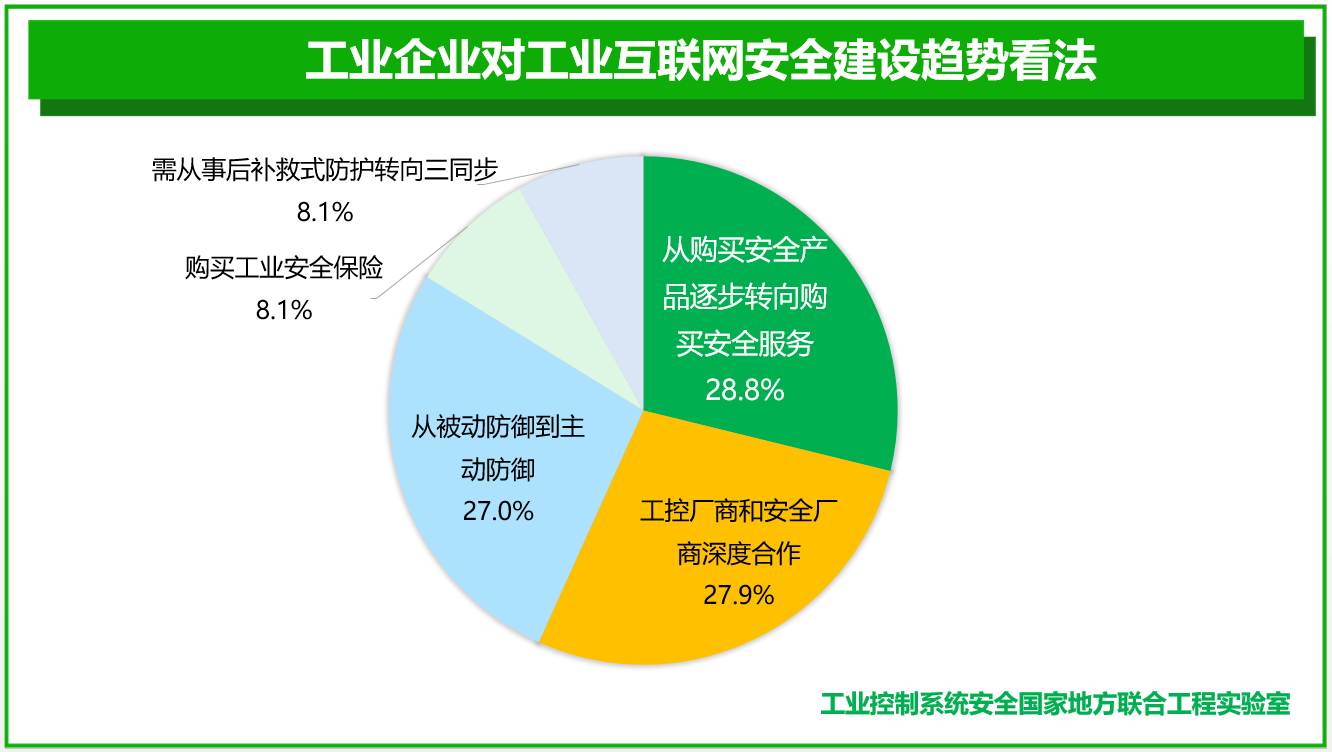
1. 工业互联网安全应急响应需求

针对安全问题应急响应解决方案，超过一半的被调查企业愿意选择一家综合能力强而且规模较大的安全厂商解决安全问题，25.2%的企业愿意选择多家安全产品供应商，避免供应商锁定现象，仅有6.5%的企业愿意尝试初创公司的技术创新。



1. 工业企业网络安全发展趋势

针对工业互联网安全建设进行调研分析，我们发现如下几点趋势：



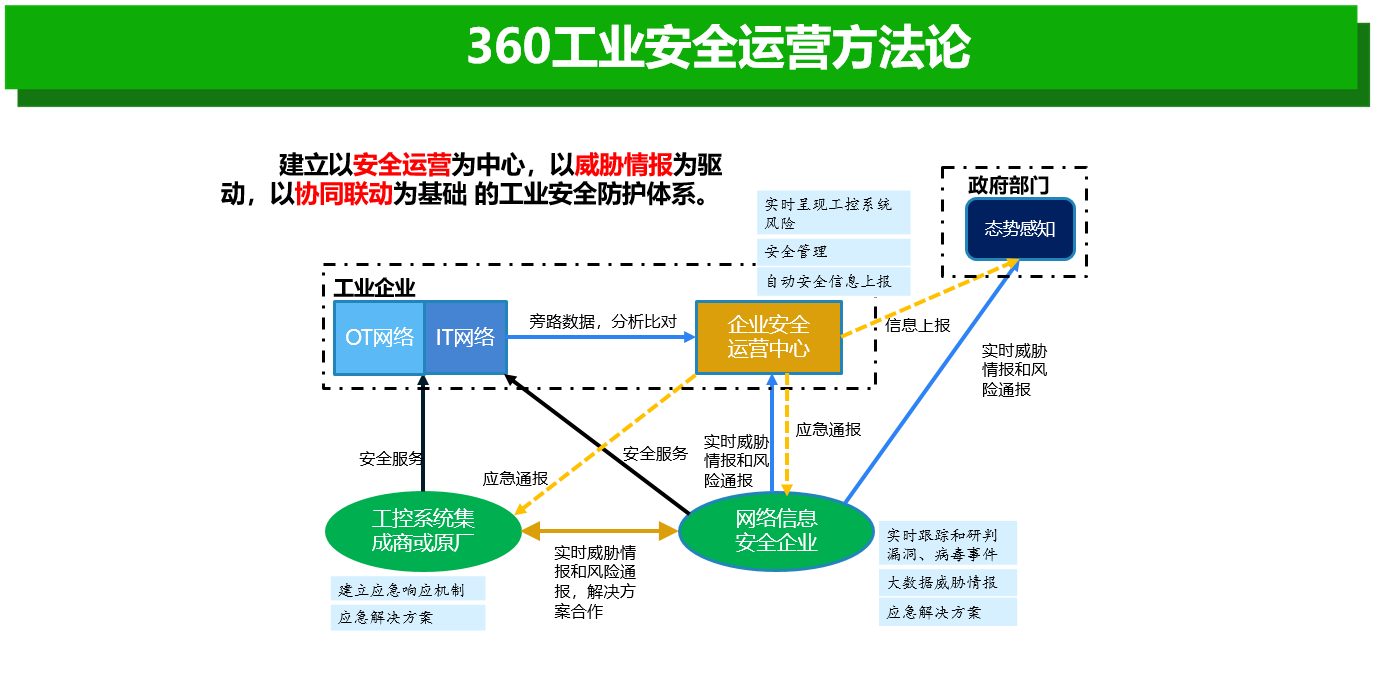
1. 工业企业安全意识有所提高，安全服务市场扩大

从购买安全产品逐步转向购买安全服务占比达到28.8%，可见工业企业已不完全满足于工业安全产品的部署，安全服务的购买更有效的保障工业企业的安全，提供工业生产的信息安全整体保障。提供产品+服务的整体性解决方案是工业互联网安全发展的主要趋势。Gartner在《2018工业安全市场指南》中也扩展了OT安全性的概念，将OT安全服务纳入OT安全范围内，安全厂商在深度挖掘工业企业安全需求做好工业安全产品的同时，也需考虑安全服务的建设。

1. 多方协作趋势明显，构建产业协同的联合防御体系

工控厂商和安全厂商深度合作占比达到27.9%。工业互联网是工业互联网是互联网和新一代信息技术（IT）与操作技术（OT）全方位深度融合所行成的产业和应用生态，工业互联网安全的建设发展首先需要熟悉工控背景，无论是做软件、硬件、系统集成都需要深入具体的应用场景，因此需要多方的通力协作。

此调研趋势和360工业安全运营方法论如出一辙，360工业互联网安全建设倡导以安全运营为中心，以威胁情报为驱动，以协同联动为基础的工业安全防护体系。



安全企业需要不断深入与更多的工业企业、工控系统集成商、安全厂商进行生态合作与交流，为工业企业客户提供更加优质的工业互联网安全解决方案。

1. 技术层面深度创新

从被动防御到主动防御占比27.0%，需从事后补救式防护转向三同步（同步建设/规划/运营）占比8.1%，两者均可以归为从技术层面创新来解决工业互联网安全问题。

工业安全信息安全目标重要性排序不同造成了工控系统与IT系统在风险评估、安全需求、标准要求、实现方案、部署实现、安全运维整个安全生命周期过程都有很大不同。因此，传统的IT信息系统的网络安全技术并不能直接应用于工业控制系统，从以“黑名单”为主的被动防御体系到以“白名单”为主的主动防御体系的转变从技术层面打破壁垒，强化工业互联网安全防护能力。

1. 总结

现阶段，工业企业对工业互联网安全的重视程度越来越高，安全投入呈现增加趋势，工业互联网安全市场将有巨大的需求，总体来说，工业互联网企业对安全的投入呈现一个良好的趋势。

69.4%的被调查企业表示没有发生过网络安全事件，但53.1%的企业表示生产车间设备遭受过蓝屏、重启现象。事实上，当企业内部电脑出现大量蓝屏、重启等现象时，往往意味着企业已经遭到了攻击，只是很多企业的管理者并没有把这些事件作为网络安全事件来进行响应和调查，而只是当作一般的系统故障而已，从而可能导致其错过发现问题的最佳时机。

24.5%的企业表示“不掌握”生产车间设备是否出现蓝屏情况，“不掌握”也就意味着企业其实并没有部署足够的网络安全监控措施以实时了解其工业系统的网络安全状况。这也说明，很多工业企业对自身网络安全建设水平的评估可能是过于乐观。

工业互联网安全建设最大的难处在于没有造成安全事故，企业高层较难理解安全建设短时间内给企业带来的收益，工业互联网安全建设不被工业企业理解。

工业防火墙、工业主机防护、工业安全集中管控平台三个产品所占比例高达50.2%，可见工业企业的首要关注点在工业企业的网络安全建设方面。非防护类各产品所占比例相当，安全检测类、安全评估类、安全服务类、安全研究类产品发展平衡，工业安全产品和服务体系日益完善。

工控厂商和安全厂商深度合作占比达到27.9%。工业互联网是工业互联网是互联网和新一代信息技术（IT）与操作技术（OT）全方位深度融合所行成的产业和应用生态，工业互联网安全的建设发展首先需要熟悉工控背景，无论是做软件、硬件、系统集成都需要深入具体的应用场景，因此需要多方的通力协作。

此趋势和360工业安全运营方法论如出一辙，360工业互联网安全建设倡导以安全运营为中心，以威胁情报为驱动，以协同联动为基础的工业安全防护体系。

安全企业需要不断深入与更多的工业企业、工控系统集成商、安全厂商进行生态合作与交流，为工业企业客户提供更加优质的工业互联网安全解决方案。

附录一 工业控制系统安全国家地方联合工程实验室

工业控制系统安全国家地方联合工程实验室（简称：工业安全国家联合实验室）是由国家发展与改革委员会批准授牌成立，由360企业安全集团承建的对外开放的工业控制安全技术方面的公共研究平台。

实验室依托360企业安全的安全能力和大数据优势，同时联合了公安三所、信通院、国家工业信息安全发展研究中心、中科院沈阳自动化所、东北大学等科研院所及大学。实验室以对工业控制系统安全领域有重大影响的前沿性、战略性技术作为研究目标，建立以工程实验室为主，联合高等院校、科研院所和国家需求部门、企业共同参加的，产、学、研、用相结合的合作机制，发挥高等院校、科研院所在基础理论研究方面的力量和优势，发挥国家需求部门、企业在技术创新和应用方面的主体作用，共享科研成果。

实验室积极吸纳国内外优秀的科技人才，建立高水平专业人才培养基地。目前实验室已与北京大学、西安电子科大、吉林大学、武汉大学、北京理工、信息工程大学等均建立了人才联合培养机制。

实验室拥有软件著作权7项，专利16项，创新地提出了工业互联网自适应防护架构（PC4R），推出了工业主机防护、工业防火墙/网关、工业互联网安全监测预警系统、工业安全监测等工业安全领域完整解决方案及产品，并已经在众多央企和工业企业中进行应用。未来，工业安全国家联合实验室将充分利用科技资源，发挥产学研联盟作用，打造产业链合作，与产业链企业实现互利共赢，在合作中共同壮大，努力成为工业互联网安全产业创新的龙头。