中国安全防范产品行业协会
China Security & Protection Industry Association
中国安防行业网 www.21csp.com.cn

奇安信
新一代网络安全领军者

中国安防行业数字安全建设与发展

白皮书

中国安全防范产品行业协会
China Security & Protection Industry Association
中国安防行业网 www.21csp.com.cn

奇安信
新一代网络安全领军者

2025 年 1 月

摘　　要

✧ 本次白皮书，共发放并回收安防企业调研问卷 100 份，其中，76%的调研对象为 200 人以下中小企业。47%安防企业年营收规模在 2000 万元以下，营收过亿元的企业共占比 22%。16%的受访企业已在海外拓展业务，9%的受访企业在未来 3 年内有望拓展海外业务。

✧ 从主营业务来看，主营安防产品平台建设业务的安防企业占比最高，达 72%；其次是安防系统集成服务，主营企业占比为 40%，主营安防产品硬件制造的企业占比为 22%。安防企业服务客户主要行业分布依次是：公安、事业单位、教育、交通和居民社区。

✧ 14%的安防企业早在 10 年之前，就已经全面启动了关键生产流程的自动化与数字化转型工作。但也仍有 38%的安防企业尚未启动数字化转型工作。其中，人事、财务等办公相关的业务系统，数字化转型率最高。特别的，调研还发现，有 38%的安防企业存在跨地区联网办公和跨地区联网生产的情况。

✧ 从产品的数字化、智能化角度看，国内安防产品的平均联网工作率约为 56%，72%的安防企业计划或已经将 AI 技术用于安防产品或安防系统。在 AI 模型的技术路线选择方面，选择传统 AI 技术的安防企业占比达 45%，高于选择通用大模型技术的 43%，而且有 22%的安防企业认为，垂直领域大模型技术会比通用大模型更适合安防行业。

✧ 从运营的数据规模来看，21%的安防企业仅能达到 GB 级，不足 1TB；17%的安防企业达到了 TB 级，即在 1TB~1PB 之间；而

运营和处理数据规模超过 1PB 的安防企业仅有两家，占比 2%，其中一家运营和处理数据的规模超过了 50PB。

- ✧ 仅有 20%的安防企业会设立专门的网络安全部门或团队，团队规模平均为 4~5 人。有 16%的安防企业，单位一把手（董事长、总裁）就是网络安全工作第一责任人。另有 9%的安防企业，网络安全工作的第一责任人是副总裁以上级别。
- ✧ 安防行业企业每年用于网络安全的平均预算投入水平约为 85~90 万元。对于自家产品存在的网络安全漏洞，62%的安防企业都会主动为客户提供免费上门漏洞修复服务，这表明，绝大多数安防企业都能够对自家产品负起安全责任。
- ✧ 安防企业最为关注的政策法规依次是：网络安全法、数据安全法、个人信息保护法和网络安全等级保护制度。
- ✧ 安防企业最为担心的网络攻击者依次是：竞争对手、个人黑客和黑产团伙；最为担心的网络攻击影响依次是：数据泄露、声誉受损和行政处罚；最担心数据泄露的数据类型依次是：办公系统数据、客户服务数据和商业机密文件。
- ✧ 当前国内安防行业的数字安全发展，主要呈现以下特点和趋势：内生安全是安防企业普遍共识、历史包袱问题制约安防企业发展、数据安全解决方案亟待全面提升、安防行业客户普遍忽视网络安全、安防企业普遍期待行业指导标准、安防企业走出去面临多重安全挑战。

关键词： 安防行业、视频监控、数字化转型、数字安全、网络安全、数据安全

目　　录

研究背景

2024 年 6 月 21 日，中国安全防范产品行业协会数字安全专业委员会（以下简称：中安协数安委）在北京成立。中安协数安委立足于数字安全发展全局，旨在推动包括安防行业数字化转型在内的所有数字安全领域的发展与合作，促进产学研用深度融合，建立涵盖技术研发、产品推广、体系建设、产业咨询、合作交流、人才输出等多方面的综合机制。

中安协数安委是由全国从事网络安全、数据安全、信息安全、物联网安全、工控安全、隐私保护、密码技术、数字安防、数字安全法规政策、网络犯罪防范和人工智能、云计算、大数据等与数字安全相关前沿领域的企事业单位、科研院所、教培机构、数字化专业机构、高等院校、行业专家，以及有志于数字安全专业发展的人士自愿组成，是中国安全防范产品行业协会的分支机构。

为贯彻落实二十届三中全会关于“聚焦建设更高水平平安中国”，“完善促进数字产业化和产业数字化政策体系”的精神，贯彻落实国家和公安部关于网络安全的相关部署，促进全国安防行业数字安全建设与发展，更好地服务安防企业数字安全体系建设，中安协数安委特别组织进行了本次“中国安防产业数字安全建设与发展情况调研”，并联合奇安信行业安全研究中心，共同编撰和发布本次白皮书。本次调研，重点关注安防企业的数字化转型情况和数字安全建设水平。

2024 年 9 月，中安协数安委共向全国各地安防企业发放并回收调研问卷 100 份。9 月 24 日~25 日，中安协数安委又与浙江

省安全技术防范行业协会，联合组织了十余家国内网络安全领军企业共同赴杭州展开“推进安防行业数字安全发展调研会”，深入走访海康威视、大华、宇视科技等安防行业领军企业，并与25家当地安防行业龙头企业举行座谈交流。

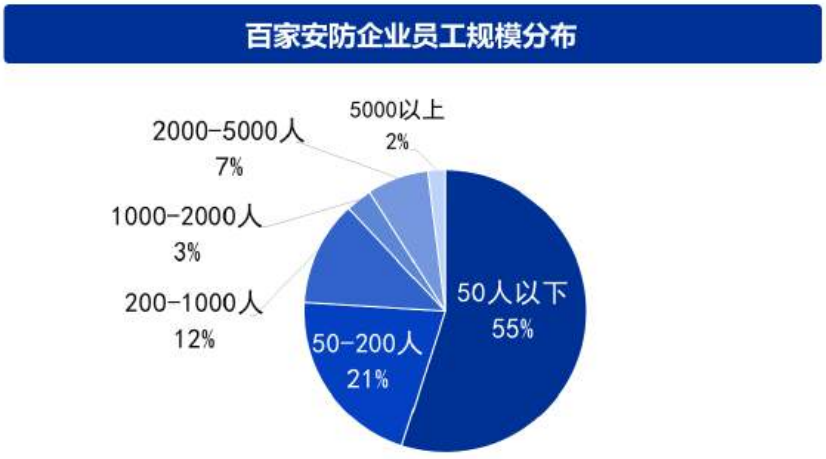
本次白皮书给出的主要观点和结论，均来自上述调研问卷和调研会研讨成果。希望能够对国内广大安防企业的数字化转型和数字安全建设有所参考和帮助。

第一章 安防企业经营现状分析

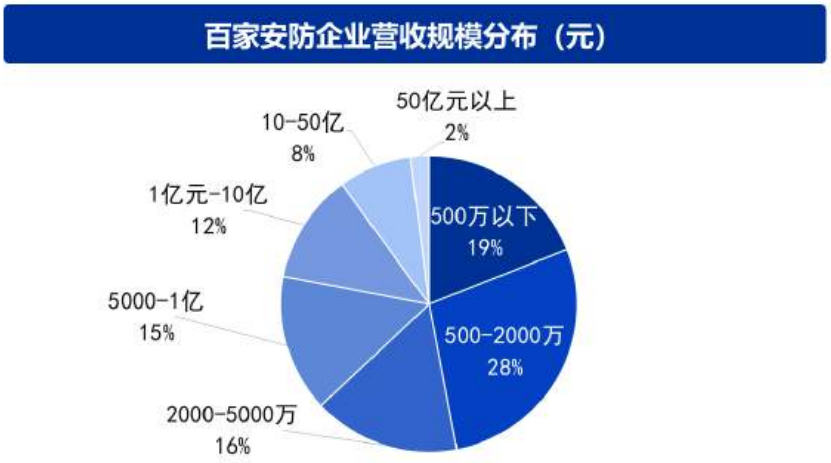
本章主要介绍本次调研涉及的 100 家安防企业的基本情况和业务范围，以帮助我们更好的理解安防企业的数字化转型需求与数字安全建设目标。

一、 企业规模

本次调研的 100 家安防企业中，员工人数在 50 人以下的小型安防企业占比 55%，50~200 人的中小企业占比 21%，员工人数 200~2000 人的中等规模企业占比 12%。此外，员工人数超过 5000 人的大型安防企业 2 家。总体而言，76%的调研对象为 200 人以下的中小企业。



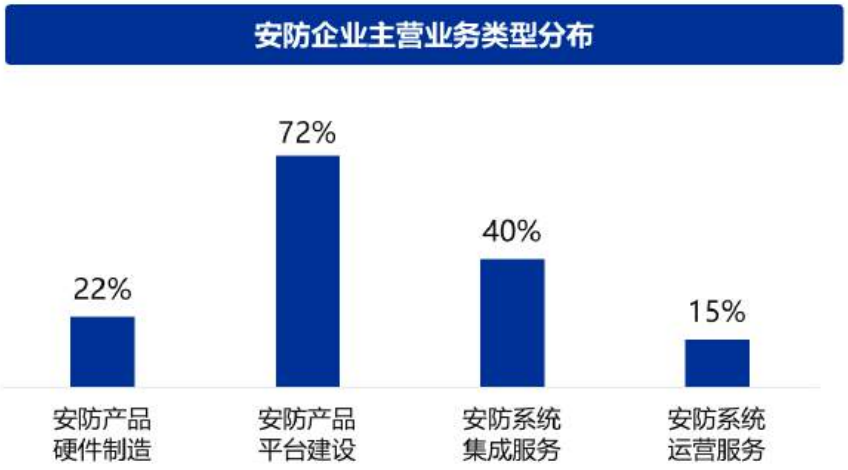
从营收规模来看，本次调研的 100 家安防企业中，47%安防企业年营收规模在 2000 万元以下，营收过亿元的企业共占比 22%。总体来看，绝大多数安防企业的营收并不足以支撑过高的网络安全预算。



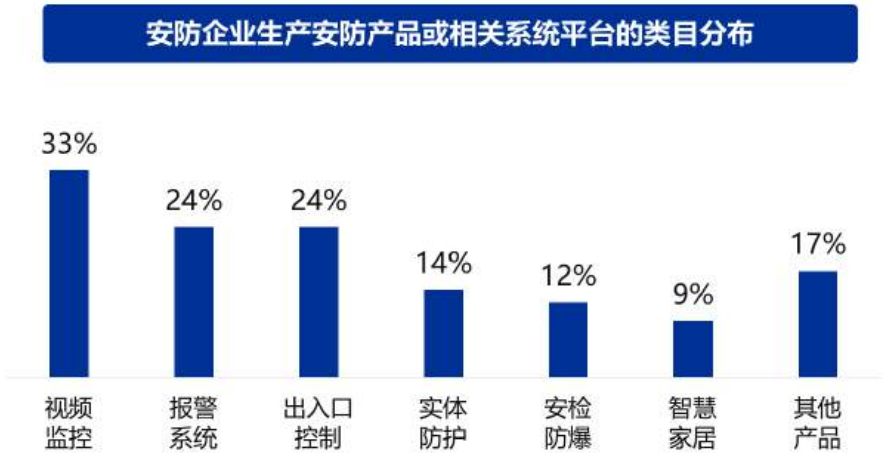
二、 业务范围

想要更好的支持安防企业数字化转型，就必须全面了解安防企业的业务范围和生产方式。本次调研，特别针对安防企业的主营业务范围、生产产品类型、运营系统类型及服务客户的行业分布进行了全面调研。

从主营业务来看，主营安防产品平台建设（包括开发平台、软件平台、系统平台等）业务的安防企业占比最高，达 72%；其次是安防系统集成服务，主营此类业务的安防企业占比为 40%；主营安防产品硬件制造的企业占比为 22%，主营安防系统运营服务的企业占比为 15%。可见，安防产品及服务的平台化是行业发展重要趋势。

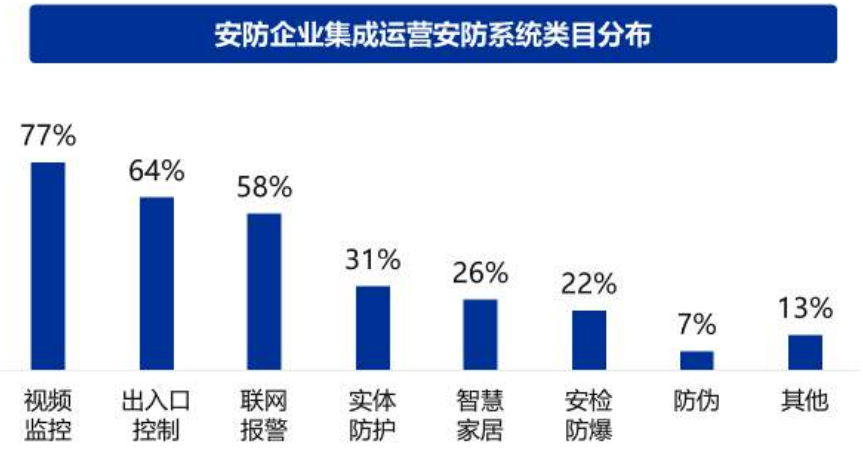


从产出类目来看，45%的调研企业对象，至少制造或生产 1 款安防产品或系统平台。生产视频监控类产品或系统平台的企业最多，占比为 33%。其次是报警系统和出入口控制，占比均为 24%。此外，实体防护占比 14%，安检防爆占比 12%，智慧家居占比 9%，生产其他各类安防产品的企业占比 17%。特别说明，同一家安防企业可能同时生产多种安防产品。

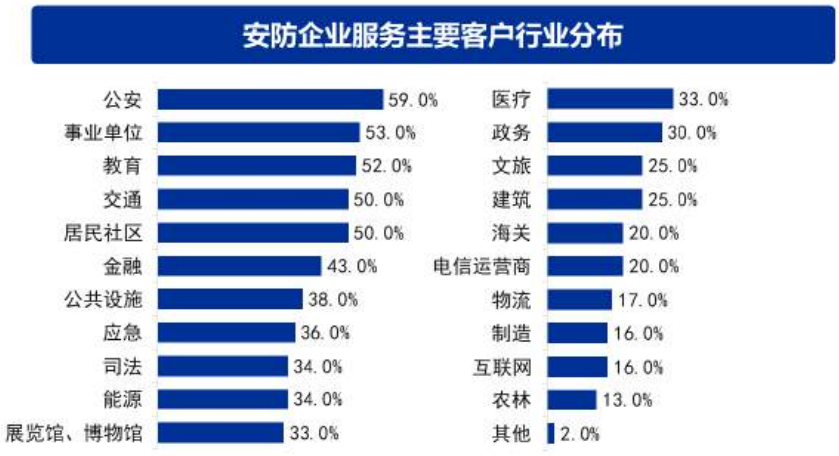


除了直接生产安防产品或系统平台外，还有 81%的安防企业会参与安防系统的集成和运营服务。而集成运营的安防系统，与

社会民生、社会安全紧密相关，正是当前亟需加强数字安全建设的重要领域。调研显示，77%的安防企业参与过视频监控系统的集成运营；其次是出入口控制系统，占比64%；联网报警系统排第三，占比58%。此外，实体防护系统、智慧家居系统、安检防爆系统、防伪系统等也都是安防企业参与集成运营较多的类型。



从安防企业服务主要客户的行业分布来看，59%的安防企业为公安部门提供安防产品及服务，还有超过半数的安防企业为事业单位、教育行业、交通行业和居民社区提供安防产品及服务。安防企业服务主要客户行业类型分布如下图所示。



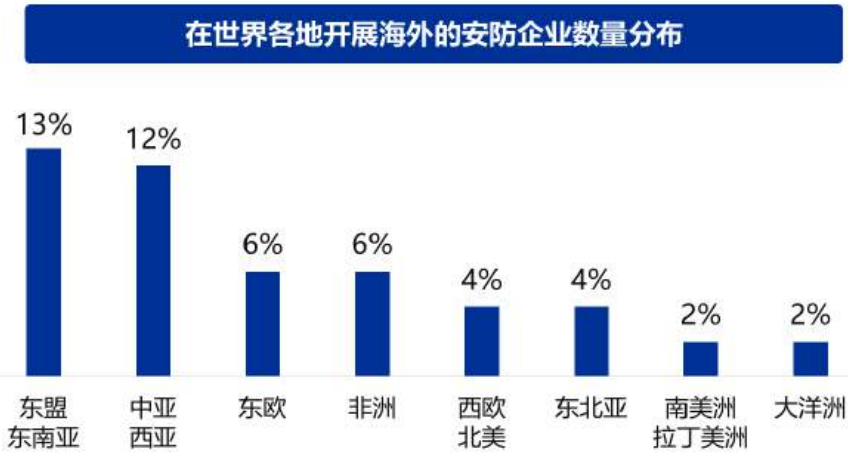
三、 短期发展

对于未来一段时期的发展空间，安防企业有哪些预期呢。本次调研，特别针对年度增长预期和海外扩展预期两个方向，对安防企业展开了调研。

下图给出了安防企业对于本企业年度营收增长情况的预期（2024 年与 2023 年相比）。其中，18%的调研对象企业做出了悲观的营收下降预期，其中，3%的安防企业预期年度营收会下降 50%以上。而预期 2024 年能够实现营业收入增长的企业，总占比为 40%，其中，6%的企业预期年度增收超过 20%。另有 30%的企业预期年度营收将与 2023 年持平，12%的企业表示无法预测。总体来看，看涨企业多于看跌企业。

走出去，是国内安防企业的重要发展方向，某些头部安防企业，甚至一半以上的营收都来自于海外。那么其他安防企业对于“走出去”持何种态度呢。本次调研显示，75%的调研对象企业暂无任何拓展海外业务的计划，9%的企业在未来 3 年内有望拓展海外业务，目前仅有 16%的安防企业已经在海外开展业务。

下图给出了目前已经“走出去”的安防企业在海外的业务分布情况。可以看出，东盟及东南亚地区、中亚和西亚地区，是国内安防企业“走出去”的首选目的地，分别有 13%和 12%的安防企业在这些地区开展业务。其次是东欧和非洲，各有 6%的国内安防企业在这些地区开展业务。

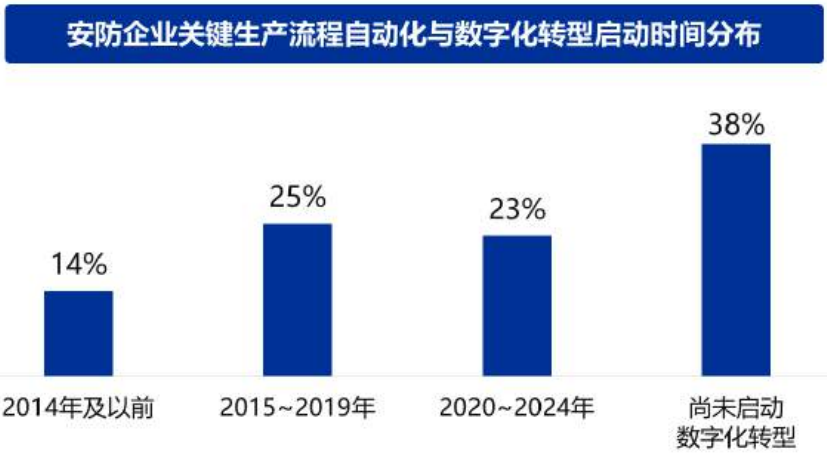


第二章 安防企业数字化转型分析

企业的数字化程度越高，对于数字安全建设的需求也越高。了解安防企业目前已经进行或计划进行哪些数字化建设，是制定安防行业数字安全建设发展战略的重要基础。

一、 生产数字化

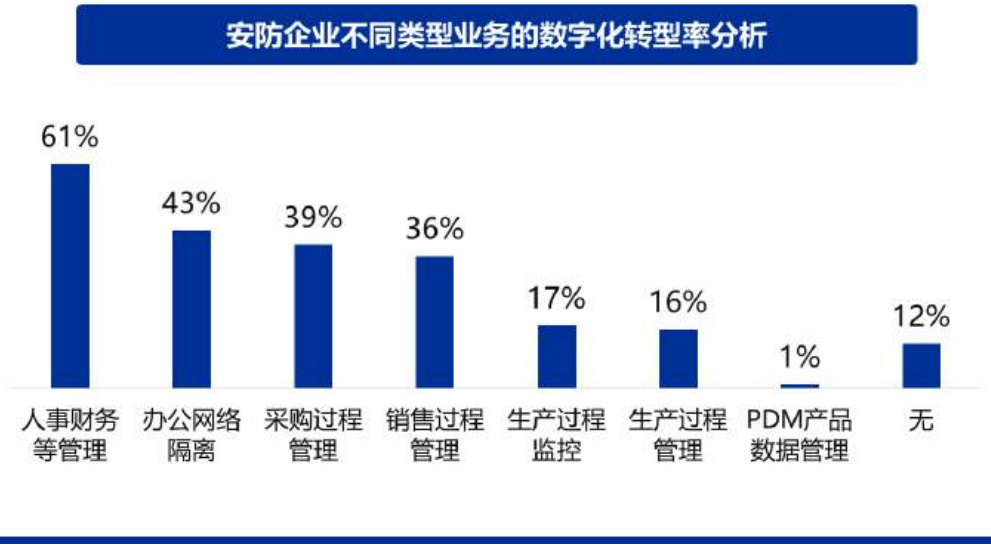
生产活动的数字化，是企业数字化转型的核心问题。调研显示，14%的安防企业早在 10 年之前，即 2014 年及 2014 年以前，就已经全面启动了关键生产流程的自动化与数字化转型工作。2015~2019 年启动数字化转型工作的企业占比为 25%。而最近 5 年间，即 2020 年~2024 年的疫情及后疫情时期才开始数字化转型的企业，占比为 23%。特别值得注意的是，目前仍有 38%的安防企业尚未启动关键生产流程的数字化转型，仍在采用比较传统的方式进行生产活动。



安防企业具体在哪些方面开展了深入的数字化转型工作呢？调研显示，88%的企业或多或少的都开展了一定程度的办公和生

产的数字化转型工作。其中，数字化转型率最高的是人事、财务等办公相关的业务系统，数字化转型率达 61%。其次是企业办公网络的安全隔离，43%的安防企业建立了与互联网相互独立的、隔离的办公网络。

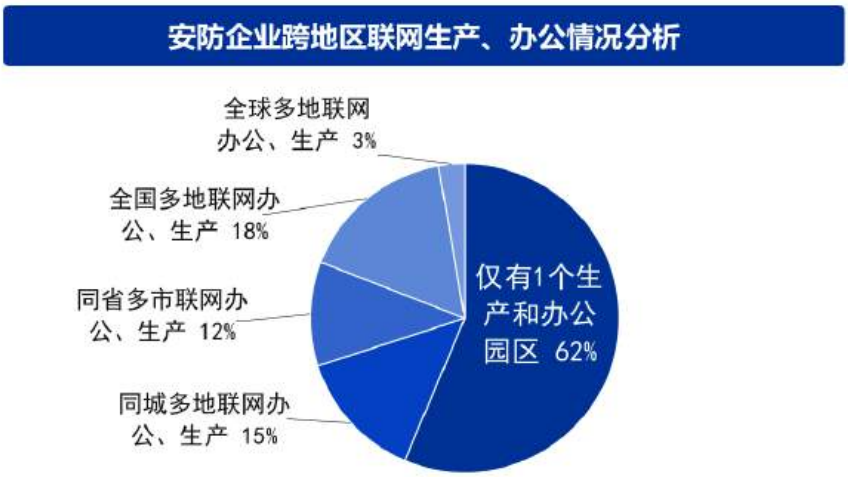
此外，39%的安防企业实现了采购过程的数字化管理、36%的安防企业实现了销售过程的数字化管理。不过，真正实现生产过程监控和生产过程管理数字化的安防企业，仅有 17%和 16%，实现 PDM 产品数字化管理的安防企业仅为 1%。这表明，对于中小型安防企业（本次调对象的主体构成）来说，数字化生产还是有一定的门槛的。



由于很多大中型安防企业拥有多个生产和办公园区，这些园区可能在同一个城市、但也可能在不同的城市，甚至在不同的国家，由此就会形成“跨地区”联网办公、联网生产的问题。需要有力的网络安全保障措施，才能实现真正的生产安全。

调研显示，尽管在本次调研中，76%的调研对象均为中小安防企业，但仍有 38%的安防企业，存在跨地区联网办公和跨地区

联网生产的情况。其中，存在同城多地联网办公、生产情况的安防企业，占比为 15%；存在同一省内多个城市联网办公、生产情况的安防企业，占比为 12%；在全国多地拥有办公和生产园区，需要网络相互联通的安防企业占比为 18%；仅有约 3%的安防企业存在跨国联网生产和办公的情况。



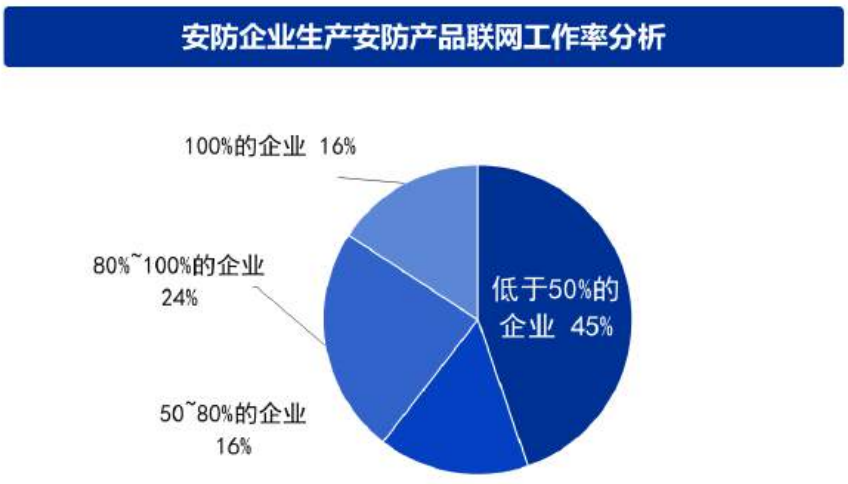
对于“跨地区”联网办公的情况，企业不仅需要做好每个园区自身的网络安全和数据安全工作，还必须在正常业务互联互通的情况下，做好网络安全的区域化隔离，以防止攻击者在成功入侵某个园区网络后，便可以畅通无阻的进入其他园区的网络。从实践来看，大型企业由于园区之间缺乏有效的网络安全隔离措施，导致全国、甚至全球多个生产园区同时中招，并造成巨大损失的网络安全事故，在国内外都时有发生，不得不防。

特别的需要强调的是，对于“走出去”的头部安防企业，面对的网络安全风险是极其复杂的。首先，国外的网络环境，特别是欠发达地区的网络环境，远远没有国内安全，企业有必要投入更多的资源进行网络安全建设，以适应当地的环境和法规要求。

此外，企业还必须高度重视数据安全问题，特别是数据的跨境流动问题。不论是在生产过程中，还是安防产品在使用过程中，都会不断的产生大量的数据，其中不乏敏感的商业机密数据和敏感的个人信息。这些数据在跨国流动过程中，不仅存在巨大的安全风险，还存在诸多合规问题：数据出境需要符合国内法律法规要求，而数据入境也要符合当地的法律法规要求。这是一个复杂的问题。

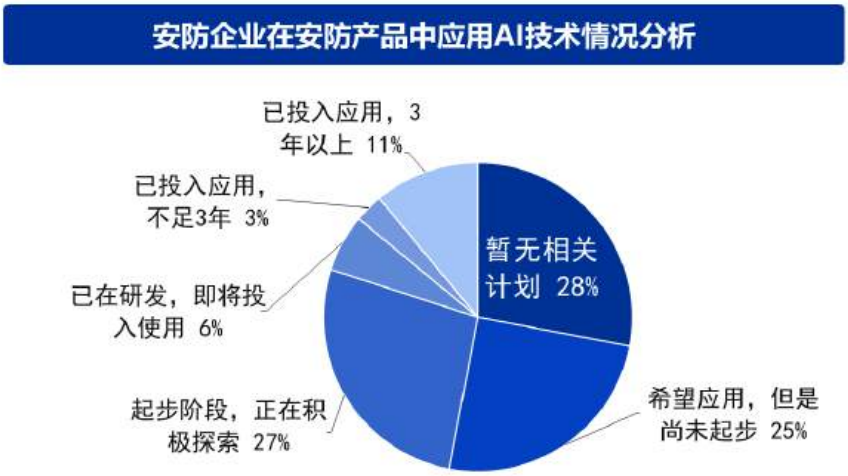
二、 产品数字化

安防产品本身的数字化，是安防企业数字化转型的重要组成部分。其中，安防产品是否需要联网工作，是安防产品数字化的重要参考指标。调研显示，国内各类安防产品的平均联网工作率约为 56%，即市面上可见的各类安防产品，有 56%都是需要或可以联网工作的。有 16%的安防产品制造企业只生产联网工作的安防产品，而产品联网工作率不足 50%的安防产品制造企业，占比仍有 45%。

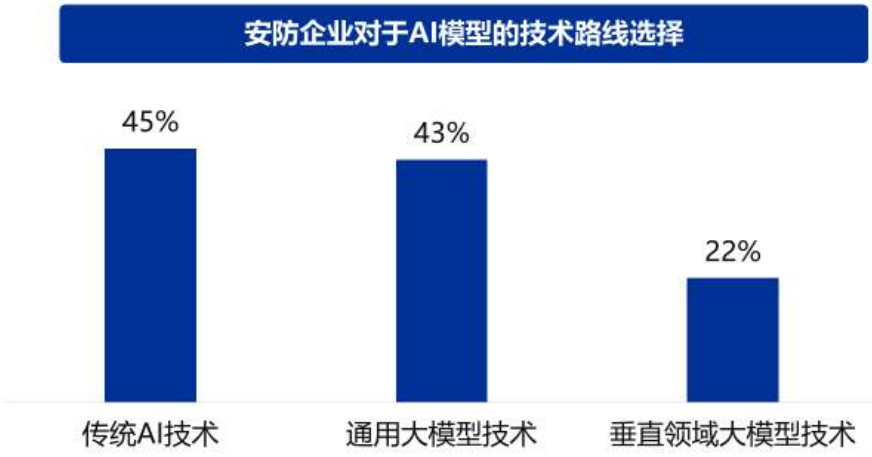


当然，从产品使用环境来看，并非所有的安防产品都一定需要联网。但联网运行，把防范和监控融合起来，无疑是安防产品制造发展的重要趋势。而产品一旦联网，如果不能做好产品内生的安全措施，那么产品就极易遭到黑客的攻击，进而被操控或造成数据泄露。

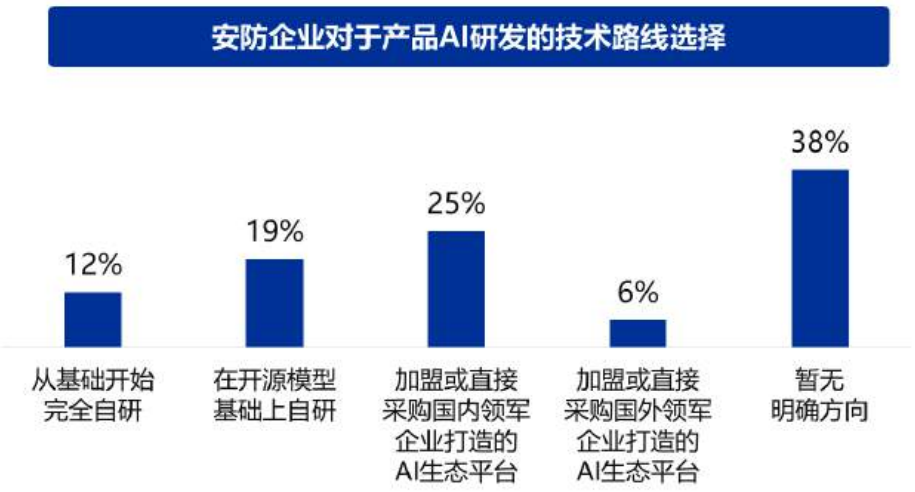
随着大模型技术应用的持续深入，AI 技术已经向各行各业深度普及。越来越多的安防企业计划把 AI 技术应用到自己的安防产品之中。调研显示，72%的安防企业计划或已经将 AI 技术用于安防产品或安防系统。其中，希望应用 AI 技术但尚未起步的安防企业占比为 25%；已经起步，正在积极探索的企业占比 27%；已在研发，即将投入使用的企业占比 6%；已经投入应用，但不足 3 年的占比 3%；而已经投入应用 3 年以上的企业占比为 11%。从这组数据中，我们可以看出，AI 技术在安防企业应用过程中，已经出现了一批头部企业遥遥领先（投入应用已超 3 年），但其他企业还没有跟上的情况，从而使一批头部企业在 AI 技术应用方面与其他企业形成“技术代差”。



对于如何将 AI 技术应用于安防产品，实现安防产品的智能化，不同的企业会选择不同的技术路线。调研显示，在 AI 模型的技术路线选择方面，更加倾向于选择传统 AI 技术的安防企业占比达 45%，高于选择通用大模型技术的 43%，而且有 22%的安防企业认为，垂直领域大模型技术会比通用大模型技术更适合安防行业。



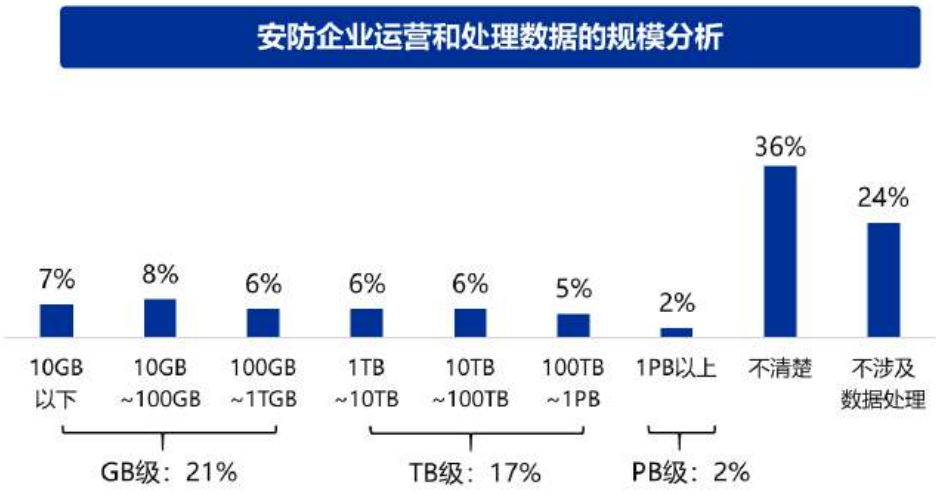
同时，在研发技术路线选择上，只有 12%的安防行业领军企业会选择从基础开始完全自研 AI 技术；19%的企业选择在开源模型基础上进行自研。当然，更多的中小安防企业会选择加盟或直接采购“大厂”打造的 AI 生态平台，不过，优先选择国内领军企业打造的 AI 生态平台的安防企业占比为 25%，远高于选择国外领军企业 AI 生态平台的的 6%。这表明，绝大多数国内安防企业对于国内领军品牌在 AI 方面的技术能力更有信心。



需要特别强调的是，对于已经投入使用且应用了 AI 技术的安防产品来说，AI 技术或大模型本身的安全问题就必须提上议事日程。包括漏洞利用、模式欺骗、样本投毒、大模型越狱等网络攻击手段，已经对大量 AI 应用系统构成了严重的安全威胁。

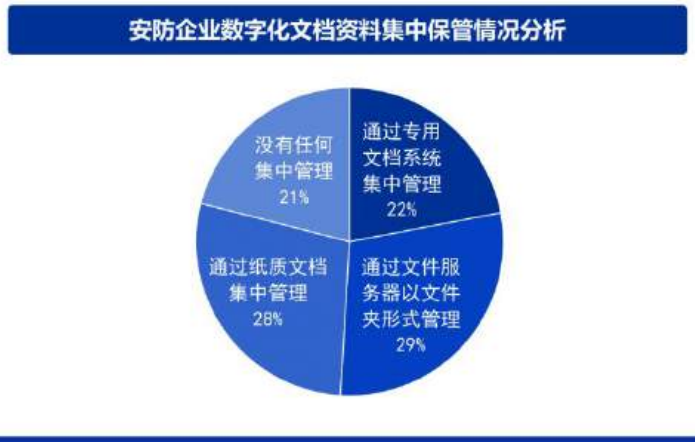
三、 运营数字化

生产数字化和产品数字化带来的直接结果，就是企业生产数据和产品运营数据的持续积累。调研显示，21%的安防企业，运营和处理的数据规模为 GB 级，不足 1TB；17%的安防企业，运营和处理的数据规模为 TB 级，即在 1TB~1PB 之间；而运营和处理数据规模超过 1PB 的安防企业仅有两家，占比 2%，其中一家运营和处理数据的规模超过了 50PB。详见下图。



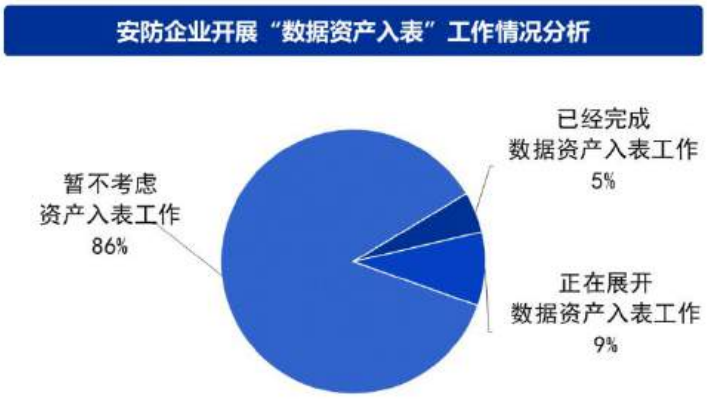
特别值得注意的是，在本次调研中，有36%的安防企业表示，并不清楚自家企业运营的数据规模。这一点十分令人担忧。因为“不清楚”也就意味着这些企业尚未开展有效的数据安全与数字安全建设，缺乏对需要进行安全管理的数据规模的基本认识。此外，还有 24%的安防企业，完全没有任何与“数据运营和处理”相关的业务。

对于办公文档、设计资料、解决方案书、投标资料、合同等重要的数字化文档资料进行保管，也是数字化转型工作的重要组成部分。调研显示，仅有22%的安防企业，能够通过专用文档系统集中管理数字化文档。还有29%的安防企业是通过文件服务器，以文件夹的形式对数字化文档进行集中管理。虽然这也可以算是一种数字化方案，但由于方式过于“老旧”和“传统”，很难实现“细粒度”的“权限管理”，所以是一种低效且不安全的文档管理方式。

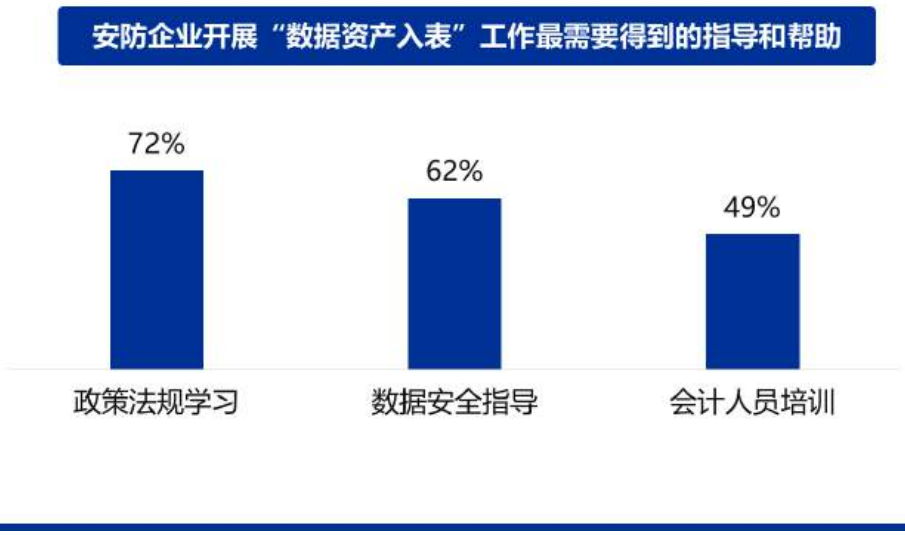


此外，有 28%的安防企业仍在使用纸质文档方式进行内部文档的集中管理，更有 21%的安防企业，完全没有采取任何集中管理措施，各类文档资料全部分散在部门和员工个人手中。这就为企业埋下了巨大的安全隐患，难免内部数据不会从员工电脑中被泄露出去。

2024 年 1 月 1 日，由财政部制定的《企业数据资源相关会计处理暂行规定》开始实施。规定首次提出“数据资产入表”的概念。对于数据资产入表问题本次白皮书也进行了调研。调研显示，目前仅有约 5%的安防企业已经完成数据资产入表工作，正在展开数据资产入表工作的安防企业占比为 9%。其他的绝大多数安防企业选择了“暂不考虑资产入表工作”。



对于如何顺利开展数据资产入表工作，安防企业最需要得到哪些支持、指导帮助的问题，调研显示，安防企业最关注的是政策法规的学习，其次是数据安全的指导，会计人员培训排在第三。详见下图。



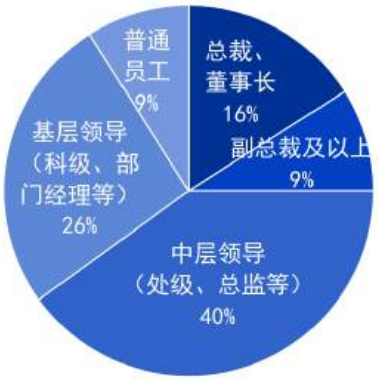
第三章 安防企业数字安全建设分析

数字安全建设，是安防企业成功实现数字化转型的重要基础。本次调研，从组织建设、预算投入、安全意识、安全风险等方面，对安防企业的数字安全建设水平进行了深入分析。

一、 组织建设

在一家企业中，网络安全工作第一责任人的行政级别，是这家企业对于网络安全工作重视程度的重要标志。调研显示，有 16%的安防企业，单位一把手（董事长、总裁）就是网络安全工作第一责任人，足见这些企业对于网络安全工作的高度重视。网络安全工作第一责任人是副总裁以上级别（不含董事长、总裁）的企业，占比为 9%；中层领导（处级、总监等）主管网络安全工作的占比最高，为 40%；基层领导（科级、部门经理等）主管网络安全工作的比例是 26%；而完全由普通员工主管网络安全工作的安防企业占比为 9%。

安防企业网络安全工作主管领导的行政级别分布

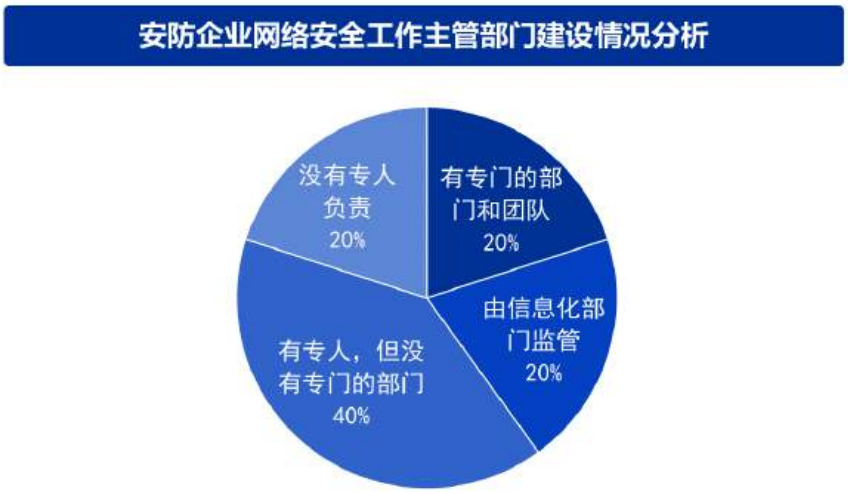


从各行各业的实践经验来看，大中型企业，由副总裁以上级

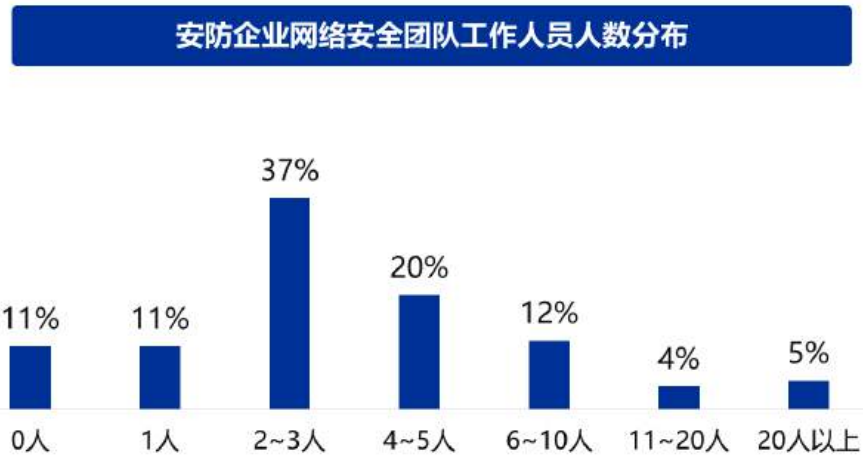
别的领导主管网络安全工作并担当第一责任人，对于企业的网络安全、数字安全保障是非常有必要的。因为只有负责人的级别足够高，才能确保充分且必要的网络安全投入，确保当突发网络安全事件发生时，网络安全团队有能力充分调动企业内部各方资源，实现快速应急，并最终将事件带来的影响和损失降到最低。

网络安全部门， 是企业网络安全工作的主要的执行者和管理者。小微企业一版不会有独立的网络安全部门，信息化和数字化程度较低的企业通常也不会设置网络安全部门。但对于大中型企业、信息化和数字化程度较高的企业，设立专业、独立的网络安全部门是很有必要的。

调研显示，仅有 20%的安防企业会设立专门的部门或团队主管网络安全工作；另有 20%的安防企业，网络安全工作是由信息化部门监管的；此外，还有 40%的安防企业只是设立了专人负责公司的网络安全工作，但没有成立网络安全相关的部门。还有 20%的安防企业，完全没有任何人为网络安全工作负责，这种情况令人担忧。



调研显示，安防企业网络安全团队工作人员的平均人数为4~5人。其中，有11%的安防企业，没有为网络安全工作设立任何的专门编制，而编制仅1人的安防企业占比为11%。编制为2~3人的情况最为常见，占比为37%。而网络安全团队超过20人的安防企业，占比仅为5%。

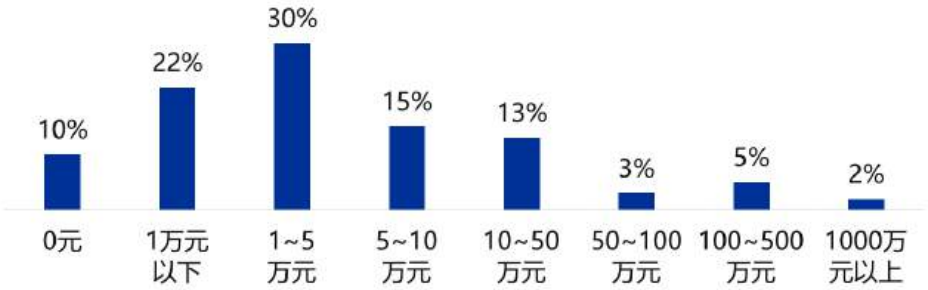


二、 预算与服务

年度预算水平，同样是衡量一个企业对于网络安全工作重视程度的重要指标。调研显示，安防行业企业每年用于网络安全的平均预算投入水平约为85~90万元。其中，至少有10%的安防企业，完全没有任何网络安全预算。网络安全预算在1万元以下的，占比也高达22%。预算在1~5万元的企业最多，占比为30%。而年度网络安全预算超过100万元的安防企业，占比总和约为7%。其中有2%的安防企业，年度网络安全预算会超过1000万元。

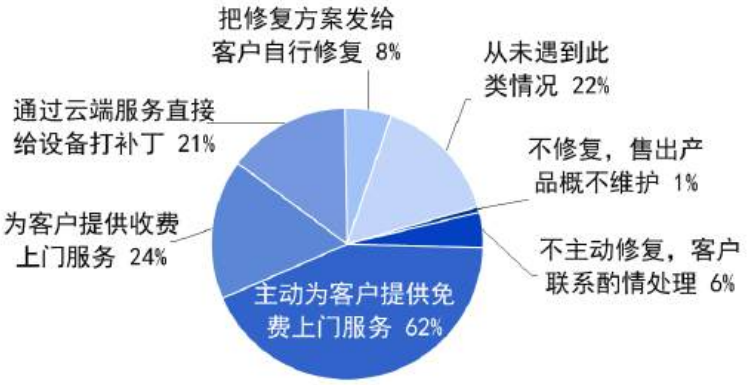
这表明，尽管很多中小型安防企业对于网络安全的预算投入十分有限，但头部企业还是十分舍得在网络安全工作中“重金投入”的。

安防企业网络安全年度预算水平分布



对于已经出售的安防产品，一旦出现重大安全漏洞，企业是否能够主动出击，帮助客户解决安全问题，也是考验企业数字安全建设水平和建设意愿的重要标志。调研显示，62%的安防企业都会主动为客户提供免费上门漏洞修复服务，这表明，绝大多数安防企业都能够对自家产品负起安全责任。还有 24%的安防企业会为客户提供收费的上门漏洞修复服务，21%的安防企业会通过云端服务直接给客户的设备打补丁。

安防企业修复自家产品安全漏洞的服务方式



三、 安全意识

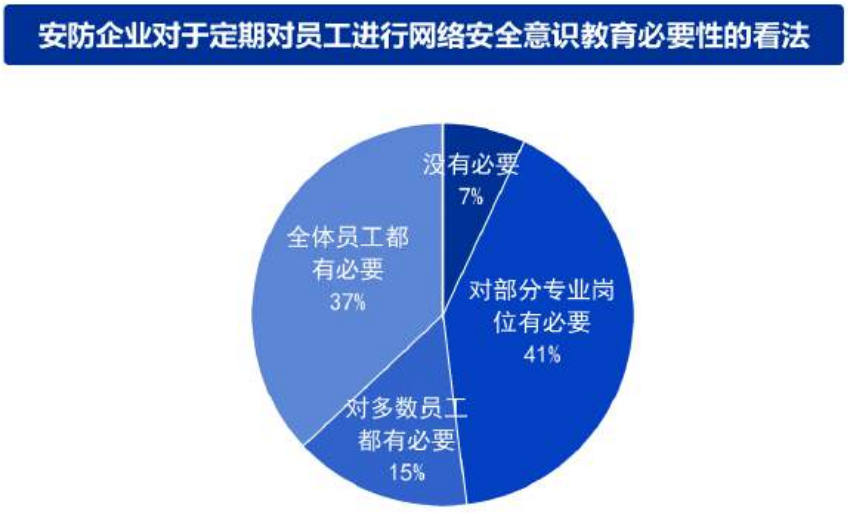
企业要实现安全生产，维护数字安全，还需要遵循相关法律法规。调研显示，最受安防企业关注的、对安防企业生产经营影响最大的政策法规文件依次是：网络安全法、数据安全法和个人信息保护法，企业关注度分别高达 74%、57%和 43%。下表给出了安防企业最关注的网络安全政策法规排行。

表 1 安防企业最关注的网络安全政策法规排行

法律法规	关注度
中华人民共和国网络安全法	74%
中华人民共和国数据安全法	57%
中华人民共和国个人信息保护法	43%
网络安全等级保护制度	41%
工业和信息化领域数据安全管理办法	31%
网络产品安全漏洞管理规定	26%
加强工业互联网安全工作的指导意见	19%
工业互联网安全分类分级管理办法	17%
车联网网络安全和数据安全标准体系建设指南	11%

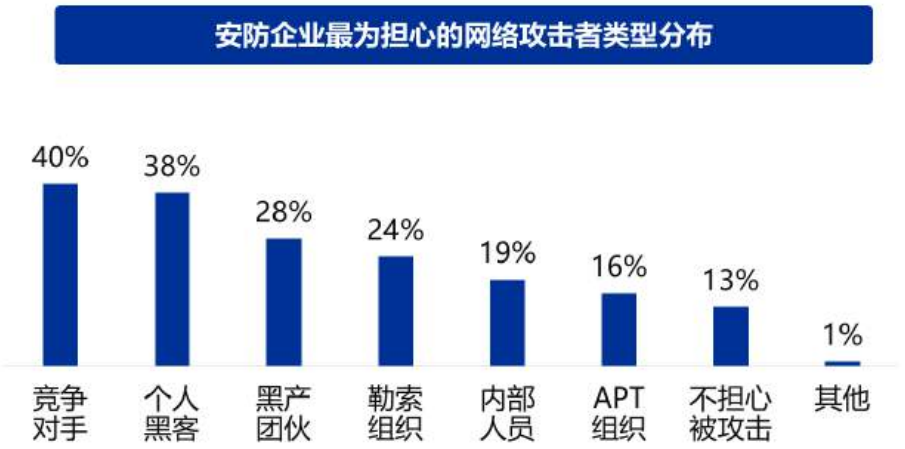
人，往往是网络安全工作中最大的漏洞，经常对普通员工及信息化人员进行网络安全意识教育，是非常必要的。在被问及是否有必要每年组织至少 1 次以上的网络安全意识培训时，7%的安防企业认为完全没有必要；41%的安防企业认为，仅对部分专业

岗位有必要，没有必要对多数员工或全体员工进行网络安全意识培训。认为有必要对多数员工，甚至全部员工进行定期网络安全意识培训的企业，占比为 52%，刚刚过半。总体而言，仍有相当数量的安防企业，对于网络安全意识教育非常不重视。

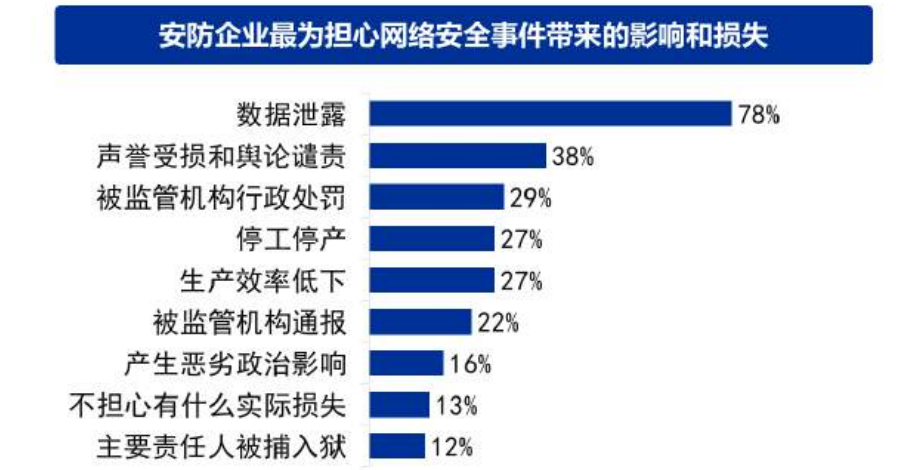


四、 安全威胁

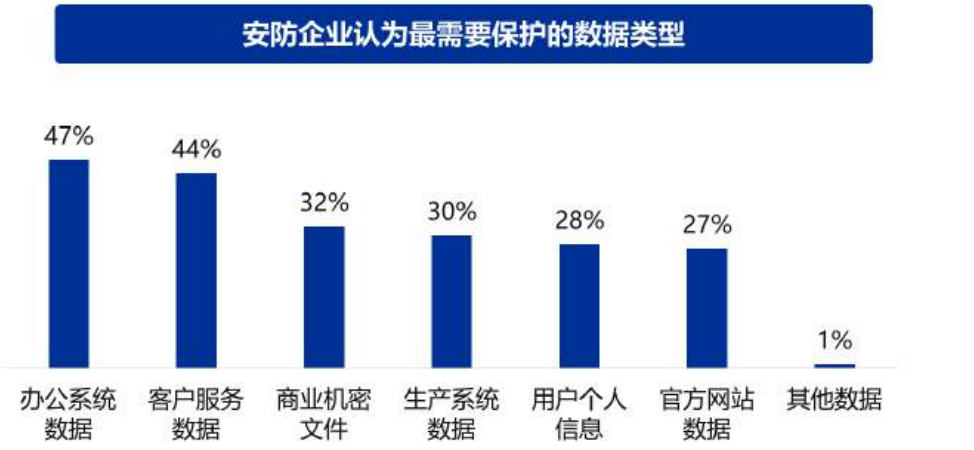
从生产到运营，安防企业面临诸多的网络安全威胁。调研显示，在被问及“贵单位及贵单位生产的安防产品、系统，最有可能被哪些类型的网络攻击者盯上”时，尽管有多达 38%的企业选择了个人黑客，28%的企业选择了黑产团伙，24%的企业选择了勒索组织，但却有高达 40%的安防企业选择了“竞争对手”。也就是说，至少有四成安防企业最担心的网络威胁，其实是自己的竞争对手过来窃取商业机密。此外，还有 19%的企业选择了内部人员（内鬼）、16%的企业选择了 APT 组织（网络战组织）。不过，也有 13%的企业表示，完全不担心自家的产品或运营的系统遭到网络攻击。



那么，网络安全威胁最有可能给安防企业带来哪些影响和损失呢？调研显示，最让安防企业担心的是“数据泄露”，78%的企业担心网络安全事件会造成企业商业机密数据或用户数据的泄露。这一比例远远高于排名第二的“声誉受损和舆论谴责”，后者占比是38%。特别值得一提的是，在现场调研会中，一些头部安防企业表示，其重金投入网络安全建设的首要原因，其实就是担忧网络安全问题引发负面舆论，从而对其声誉造成持续性的影响。此外，行政处罚、停工停产和生产效率低下等问题，也都是安防企业比较担心的问题。详见下图。



既然数据泄露问题是安防企业最为担心的问题，那么，安防企业最担心被泄露，也是认为最需要保护的数据是什么呢？调研显示，47%的安防企业选择了办公系统数据，44%的安防企业选择了客户服务数据，32%的企业选择了商业机密文件。这三类数据被最多的安防企业选中。关于安防企业认为最需要保护的数据的类型排行，详见下图。



第四章 安防企业数字安全建设展望

本章内容，主要是对 2024 年 9 月 24 日~25 日，中安协数安委与浙江省安全技术防范行业协会联合组织的“推进安防行业数字安全发展调研会”研讨成果的总结。

一、 内生安全是安防企业普遍共识

所谓内生安全，就是指信息化系统自身具备的、内在的安全能力，是以自身产品或系统业务特点为基础建立的安全机制，而非单纯的通过外部安全措施来保障产品或系统的安全。

调研显示，绝大多数安防企业都高度认可内生安全的技术理念，并且已经在生产和运营实践中有了大量成功的实践经验。主要体现在以下几个方面：

1. 产品设计与开发

很多安防企业表示，其近几年生产的新一代安防产品，普遍是从设计之初就全面的考虑系统的安全性问题：首先是设计架构的安全性，即在产品代码的设计架构中，就包含了大量加密、鉴权、认证等安全机制，为产品或系统奠定良好的安全基础；第二是开发过程的安全性，即通过严格的安全开发流程管理和安全编程技术要求，确保程序从开发之初就是高效且安全的；第三是源代码的审计，不论是使用自研代码还是开源组件，都需要进行严格的代码缺陷审计；第四是产品上市前的安全测试，由专业白帽子协助共同检测产品的安全性。

调研显示：设计架构的安全性、开发过程的安全性、源代码的审计和上市前的安全测试，在头部安防企业中已经普遍得到了

系统性的实施，其他安防企业也正在逐步跟上。

2. 产品升级与运维

安防产品的固件升级和漏洞修复，一直是很多安防行业的“心头之痛”。同时，随着产品应用场景的不断丰富，很多新的安全需求也在不断产生，而老款产品无法满足新生安全需求的问题也日渐突出。

调研显示：很多安防企业，特别是头部安防企业，已经开始为自家产品提供简易、高效的固件升级方案或安全管控平台，以方便客户监控产品运行状况，及时、快速且安全的给产品升级、打补丁。此外，一些监控设备制造企业还提出了“功能管控盒子”与监控设备级联使用的解决方案，对于新的功能要求、新的安全管控要求，只需要对“功能管控盒子”进行升级，就可以使监控设备完成系统要求的各项新功能。

此外，还有部分安防企业已经建立了自己的 SRC（安全响应中心），向全社会广泛征集自家产品的安全漏洞并予以一定程度的奖励。这对于提升安防产品的网络安全性有很大的帮助。

3. 数据的采集与应用

除了安防产品自身的安全问题外，由安防产品互联组成的业务系统的安全性，也是非常重要的安全问题。这种业务系统整体的安全性问题，不是加装安全软件或安全设备就能够解决的，而是需要在业务实现的过程中，将网络安全需求内置其中。

以视频监控系统为例，视频数据的采集、传输、云端存储、综合应用等各个环节，都必须全面、充分的考虑安全性问题，全

面部署加密、鉴权、认证、防泄露等安全措施。唯有如此，才能确保视频监控系统的整体安全性。调研显示，目前已经有不少安防企业在业务系统的内生安全能力建设方面取得了长足的进步。

二、 历史包袱问题制约安防企业发展

谈到“历史包袱”问题，很多安防企业都是大吐苦水。这实际上是一个由于“质量太好”而引发的安全问题。一方面，受到当时技术水平和认知水平的限制，早期生产的安防产品普遍没有深入考虑网络安全问题，因此难免存在这样或那样的安全漏洞且不易修复。另一方面，很多已经使用了 10 年、甚至是 20 年以上的安防产品，由于质量过硬，仅从功能角度看仍然能够正常使用，因此被很多用户持续使用；但由于这些产品早已停产，且早已超过了厂商的维保期限，厂商也已无力对其进行升级和维护。这也就造成了大量“超期服役”（超出设计使用预期年限后仍在被继续使用）的安防产品在市面上仍被广泛使用的客观现实。

实际上，“历史包袱”、“超期服役”等问题，是几乎所有物联网设备和工业控制系统中都普遍存在的问题，只不过由于安防行业自身的“敏感”特性而更受社会关注。从消费者或政企客户的角度看，在设备还能“正常使用”的时候，就将设备全部做报废处理，无疑是一种巨大的浪费、而从生产企业的角度看，也不太可能对一款产品承诺永久的安全维护，其研发投入和运维成本通常来说是不可承受的。某些大型安防企业生产过的安防产品，可能有数千款甚至上万款之多，对如此之多的产品进行长期持续的安全维护，其成本是难以想象的。

尽管理论上说，安防企业可以对“历史包袱”选择不闻不问，

可一旦“超期服役”的安防产品因网络安全漏洞而引发重大网络安全事故，安防企业通常仍然会被问责，并产生负面舆情。因此，很多安防企业在调研中都表示，希望安防产品也能如汽车一样，有法定的强制报废期，从而减轻安防企业的“历史包袱”。

需要特别说明的是，很多安防企业其实早已开始着手解决新一代安防产品的运维升级问题。一方面，安防产品在设计之初，就要从框架层面预留出固件的升级空间。另一方面，可以通过将安防产品与“功能管控盒子”级联的方式，用盒子保护安防设备，并为安防设备提供更大的升级扩展空间。不过，这些方法的使用，只能在一定程度上缓解“历史包袱”问题，并不能从根本上消除“历史包袱”。因为固件升级是与硬件驱动相结合的，随着硬件技术的升级换代，老旧硬件被逐步淘汰后，与之相配的固件系统停止升级，也是必然的。

仅仅从生产企业的角度看，“历史包袱”在相当长的一段时间里可能都无法得到有效解决。当然，如果客户愿意支付费用，专门邀请网络安全团队帮其运营升级老旧的安防设备未尝不是一种解决办法，但如果这只是个别客户的孤立行为，其成本之高仍然是难以想象的。谁会愿意为了修一个旧电器，花上足够买一件新电器的费用呢？

三、 数据安全解决方案亟待全面提升

调研显示，数据安全问题，是安防企业最为关注的网络安全问题。不过，从行业整体实践来看，包括很多头部企业在内，普遍仍在单纯的采用传统安全技术方法解决数据安全问题，而没有采用新型的、专用的数据安全方法体系。

从传统意义上的网络安全方法来看，部分安防企业，特别是部分头部安防企业，可以说已经“武装到了牙齿”，已经部署和运营了非常系统、非常全面的网络安全措施。这些安全措施的采用当然是非常必要且有效的。但从数据安全的角度看，这些传统方法并不能解决：企业有哪些数据、企业有哪些接口、数据都传给了谁、数据都传到了哪等数据安全基本问题，从而使数据安全保护缺少着力点。

传统网络安全方法，更多的是用来保障设备、系统或网络不被入侵、破坏和非法使用。但数据安全方法则是以具体的数据为保护对象，在数据大范围流转的前提假设之下，确保数据不被非法/越权访问、不被超范围获取、不被窃取、篡改或破坏。传统网络安全方法主要防范的对象是黑客和内鬼；而数据安全方法防范的对象则是所有不合规的数据访问者。而这些不合规的数据访问者，可能是一个用户，也可能是一个应用，或者仅仅是一个接口。这些访问者在访问某些数据的某些字段时，可能是合规的；而当它们访问另外一些数据的另外一些字段时，可能就是不合规的。

现代数据安全方法会通过流量检测来监控数据、特别是敏感数据的流动状况和潜在的网络攻击；通过 API 接口的监测与保护，来实现数据流转过程中的安全管控；通过数据安全态势感知平台，来跟踪敏感数据的流转和使用情况，确保数据被合规的使用。

随着数据安全法、个人信息保护法等法律法规的深入实施，数据安全问题将成为所有安防企业不得不认真面对的重要问题。未来 3~5 年内，能否实现从传统网络安全方法向数据安全方法的升级改造，将是安防企业能否实现数字经济时代健康发展的关键。

四、 安防行业客户普遍忽视网络安全

调研显示，孤立存在的安防产品，通常不会引发重的大网络安全事故。真正引发安全事故、造成大量数据泄露的，通常是那些正在实际运行和使用中的安防系统。但是，绝大多数安防系统的运营和使用方，也就是各类政企单位，对于网络安全工作普遍存在轻视和忽视的态度，主要体现在以下几个方面：

1. 图便宜，拒绝在安防系统中集成网络安全方案

很多安防企业都为客户设计了集成网络安全方案的安防系统设计方案，但这些方案的推广非常困难，绝大多数政企单位都拒绝为此买单，不愿意采购网络安全方案和网络安全运行服务。

2. 轻运营，网络安全设备与系统往往形同虚设

即便某些大型政企单位在安防系统中集成采购了网络安全方案，也仍有很多单位不愿意投入专业人员对系统进行运维，网络安全设备不进行任何规则配置，网络安全系统也没有进行持续的有效运营。

3. 无意识，运营人员消极对待网络安全意识培训

很多头部安防企业，都为客户设计了网络安全意识培训课程，甚至有时会强制要求客户运营人员进行学习，内容即包括安防设备本身的安全运营要求，也包括系统使用过程中运营人员需要提升的网络安全意识。但这些培训的效果往往也非常有限，客户单位还是频频发生因网络安全意识不足而导致的网络安全事故。

总体而言，安防系统的集成和运营单位，普遍缺少有效的强力监管，运营人员网络安全意识淡漠，“只要不出事，就不在意网络安全”的情况非常普遍，这也给整个行业带来了巨大的隐患。

五、 安防企业普遍期待行业指导标准

很多安防企业在调研中表示：现有的、通用的网络安全政策法规和技术标准，并不能完全反映出安防行业生产、经营和运营的实际需求。网络安全企业推出的各类网络安全产品、服务和解决方案，也很难直接有效的应用于安防行业的生产和安防系统的运行，无法提供符合安防行业技术和业务特点的内生安全保障。

多数参与研讨会的代表均表示：由安防企业代表和网络安全企业专家，组成联合小组，共同研发和制定一套适合安防行业的，涵盖网络安全、数据安全、工控安全、物联网安全等多个方面的技术标准或技术指南，对于促进安防行业健康发展，促进安防企业数字安全建设水平的快速提升，很有必要。

六、 安防企业走出去面临多重安全挑战

如前述调研结果显示，目前，已经有 16%的受访企业在海外拓展业务，9%的受访企业在未来 3 年内有望拓展海外业务。部分安防企业的海外业务营收，甚至已经超过国内。总体而言，“走出去”将是越来越多的安防企业发展壮大的必然趋势。

不过，由于国外网络环境、政策环境都与国内有很大的不同，走出去的安防企业迫切需要海外环境下的网络安全、数据安全等方面的技术支持。但考虑到要符合各国当地的政策法规要求，很多走出去的安防企业，会在海外优先选择与当地或国际大牌网络安全企业合作，这是对国内的网络安全企业提出的巨大挑战。

从需求来看，“走出去”的安防企业普遍存在以下网络安全建设与服务需求：

1. 合规建设。生产经营活动即要符合当地的法律法规，也

要符合中国的法律法规。

2. 能够在海外的网络环境中，实现安全组网和基本的网络安全运行。

3. 能够对来自敌对势力的网络战攻击进行有效的识别和防御，避免企业技术机密外泄。

4. 能够为当地员工提供有效的网络安全意识培训。

对于国内的网络安全企业来说，如何才能服务好“走出去”的国内安防企业，是一个非常重要的时代命题。