

2020 年全国网民网络安全感满意度调查 专题报告 (网络安全行业发展报告)

指导单位：公安部网络安全保卫局

发起单位：全国 135 家网络安全行业协会及相关社会组织

承办单位：广东新兴国家网络安全和信息化发展研究院

2020 年 11 月

本报告数据来源于 2020 网民网络安全感满意度调查活动，任何组织和个人引用本报告中的数据和内容须注明来源出处。

组委会欢迎有关研究机构合作，深入挖掘调查数据价值，有需要者请与组委会秘书处联系。

报告查询（总报告及区域、专题、行业报告）：



网络安全共建网：www.iscn.org.cn “网安联”公众号：

联系方式：办公室 020-83113010 / 林先生 13911345288

邮箱地址：cinsabj@163.com

目录

一、前言.....	1
二、主要发现.....	4
2.1 网络安全行业发展前景看好，政策环境有利行业发展	4
2.2 网络安全面临挑战，供应链安全风险受到关注	4
2.3 打击网络犯罪任重道远，痛点多关注度高	5
2.4 行业生态建设有待加强，服务体系建设受到关注	5
2.5 企业安全管理措施有所加强，等级保护制度取得成效	6
2.6 网络安全人才建设有待加强，培训制度逐步落实	6
2.7 新技术应用登场，安全风险受到关注	7
三、网络安全行业发展状况.....	8
3.1 从业人员状况	8
3.2 行业发展状况	13
3.3 网络安全态势	17
3.4 行业发展前景	24
四、专题分析.....	28
4.1 等级保护实施与企业合规	28
4.2 行业发展与行业生态建设	43
4.3 新技术应用前景与制约因素	52
4.4 科技创新与人才培养	65
五、结论和展望.....	71
5.1 主要结论	71
(1) 行业发展前景看好，网络安全领域成为热点.....	71
(2) 疫情影响对行业冲击有限，市场需求增长前景看好.....	71
(3) 网络安全形势严峻，病毒勒索等网络黑灰产业比较活跃....	72
(4) 网络安全监管得到加强，企业合规自律水平有较大提升....	72
(5) 供应链安全问题比较突出，自主创新带来新机遇.....	73
5.2 未来展望	73

（1）网络安全市场持续快速增长，新基建等领域成为热点.....	73
（2）新技术加快更新换代，智能化与可信安全成为热点.....	74
（3）服务体系逐步完善，质量为本品牌效应更突出.....	74
（4）产业生态建设初具规模，形成中国特色的发展路径.....	75
附件一：调查方法与数据样本情况.....	77
附件二：调查报告致谢词.....	82
附件三：调查活动指导单位、联合发起单位和组委会名单.....	83
附件四：调查活动发起单位及支持单位名单（排名不分先后）.....	85

网络安全感满意度调查



广东新兴国家网络安全和信息化发展研究院

图表目录

图表 3.1-1: 从业人员网民性别分布图	8
图表 3.1-2: 各地从业人员网民性别分布对比	9
图表 3.1-3: 从业人员网民年龄分布 2019-2020 对比图	9
图表 3.1-4: 从业人员所在行业的分布图	10
图表 3.1-5: 从业人员学历分布图	10
图表 3.1-6: 从业人员答卷各省分布图	12
图表 3.2-1: 从业人员对当前网络安全行业市场的需求变化的评价	13
图表 3.2-2: 目前网络安全行业提供的网络安全保障水平评价	14
图表 3.2-3: 各地从业人员对行业提供的网络安全保障水平的评价	14
图表 3.2-4: 各地从业人员对当前网络安全产品与服务的资费水平评价 ...	15
图表 3.2-5: 当前网络安全产品与服务存在的不足之处	16
图表 3.3-5: 在工作中最常面对的网络威胁	20
图表 3.3-6: 网络安全事件出现的原因	21
图表 3.3-7: 不同单位对网络安全事件出现的原因的排列比较	22
图表 3.3-8: 互联网黑灰产业活跃情况评价	23
图表 3.4-1: 对网络安全行业未来一年发展的趋势的评价	24
图表 3.4-2: 制约网络安全行业发展的主要障碍	25
图表 3.4-3: 各地从业人员对制约网络安全行业发展的主要障碍的看法 ...	26
图表 3.4-4: 当前网络安全技术人才数量评价	26
图表 3.4-5: 各地从业人员对当前网络安全技术人才数量评价	27
图表 4.1-1: 所在行业对等级保护工作指导现状	28
图表 4.1-2: 网络安全对单位重要性认识	29
图表 4.1-3: 所在单位网络安全状况的了解	29
图表 4.1-4: 所在单位网络安全管理状况满意度评价	30
图表 4.1-5: 所在单位网络安全管理需要改善的地方	31
图表 4.1-6: 所在单位网络安全保护专门机构设置情况	31
图表 4.1-7: 所在单位网络安全责任人落实情况	32
图表 4.1-8: 所在单位网络安全经费预算落实情况	33

图表 4.1-9: 对企业网络安全合规应遵循法规的认识	33
图表 4.1-10: 政府网络安全服务对行业帮助的有效性评价	34
图表 4.1-11: 从业人员网络安全培训情况	35
图表 4.1-12: 从业人员对网络安全“三化”概念的认识	35
图表 4.1-13: 从业人员对网络安全“六防”措施的认识	36
图表 4.1-14: 对网络安全等级保护制度 2.0 标准的了解	37
图表 4.1-15: 等保制度对产业、企业发展推动作用的评价	37
图表 4.1-16: 所在单位网络安全等级保护开展情况	38
图表 4.1-17: 所在单位发生网络安全事件情况	39
图表 4.1-18: 所在单位发生网络安全事件种类	39
图表 4.1-19: 单位网络安全应急预案完善度评价	40
图表 4.1-20: 对关键信息基础设施安全保护要求的认识	41
图表 4.1-21: 所在单位是否定期进行网络安全检查	41
图表 4.2-1: 对当前促进网络安全行业发展的政策环境的评价	43
图表 4.2-2: 当前促进网络安全产品与服务发展的政策环境评价比较	44
图表 4.2-3: 当前信息技术产业供应链安全问题的威胁	44
图表 4.2-4: 当前网络安全产品与服务的资费水平	45
图表 4.2-5: 不同保障水平与服务的资费水平评价对比	46
图表 4.2-6: 当前网络安全产品与服务存在的不足之处	46
图表 4.2-7: 对网络安全产品与服务实行等级评价管理的意见	47
图表 4.2-8: 当前网络安全技术人才数量评价	48
图表 4.2-9: 当前网络安全测评机构数量评价	48
图表 4.2-10: 对测评机构提供服务的需求	49
图表 4.2-11: 制约网络安全行业发展的主要障碍	50
图表 4.2-12: 网络安全行业未来一年发展的趋势评价	50
图表 4.2-13: 网络安全行业协会等社会组织服务情况	51
图表 4.3-1: 对新技术新应用的网络安全问题的关注度	52
图表 4.3-2: 从业人员 5G 网络使用率	53
图表 4.3-3: 各地从业人员 5G 网络使用率	53

图表 4.3-4: 对 5G 网络使用体验的评价.....	54
图表 4.3-5: 目前不使用 5G 网络的原因.....	55
图表 4.3-5: 对 5G 技术的顾虑.....	55
图表 4.3-6: 人工智能(AI)可以发挥优势的领域.....	56
图表 4.3-7: 目前人工智能应用的发展面临的阻力.....	57
图表 4.3-8: 对“AI 换脸”等“深度伪造”为代表的新技术新应用的想法.....	57
图表 4.3-9: 对区块链的了解程度.....	58
图表 4.3-10: 区块链未来发展趋势的看法.....	59
图表 4.3-11: 所在单位大数据技术应用情况.....	59
图表 4.3-12: 目前大数据技术应用存在的问题.....	60
图表 4.3-13: 体验过物联网应用的领域.....	61
图表 4.3-14: 物联网安全风险.....	61
图表 4.3-15: 数字政府和智慧城市的网络安全状况评价.....	62
图表 4.3-16: 数字政府和智慧城市中新技术的应用效果评价.....	63
图表 4.3-17: 加强新技术应用的网络安全保障的建议.....	63
图表 4.4-1: 所在单位网络安全科研经费预算情况.....	65
图表 4.4-2: 疫情冲击对本单位网络安全资金投入的影响.....	66
图表 4.4-3: 网络安全科研课题立项和管理方面的满意度.....	66
图表 4.4-4: 网络安全科研工作需要改善的地方.....	67
图表 4.4-5: 网络安全方面的科研成果转化满意度评价.....	68
图表 4.4-6: 网络安全科研成果转化感到不满意的地方.....	68
图表 4.4-7: 所在单位有关网络安全的课程开设情况.....	69
图表 4.4-8: 网络安全专业人才评价和队伍建设存在的问题.....	70

一、前言

随着网络信息社会发展，互联网已与人民群众日常生活密不可分。网络在提供各种生活便利和沟通便捷的同时，网络威胁也在增长：网络攻击、病毒传播、垃圾邮件等屡见不鲜；利用网络进行诈骗、盗窃、敲诈勒索、窃密等案件逐年上升，严重影响网络的正常秩序，损害网民权益；网上色情、暴力等不良和有害信息的传播，正在严重危害青少年的身心健康。如何加强网络安全社会治理、保障广大人民群众上网用网安全，日益成为社会广泛关注的重大问题。开展网络安全满意度调查，旨在进一步贯彻习近平总书记有关“要树立正确的网络安全观，坚持网络安全为人民、网络安全靠人民，坚持网络安全教育、技术、产业融合发展，坚持促进发展和依法管理相统一，坚持安全可控和开放创新并重，统筹推进网络安全工作，构筑起坚实的网络空间安全屏障。”等网络强国的重要思想，切实落实《网络安全法》及相关法律法规，增强网民的网络安全意识和防范能力，促进互联网企业履行社会责任，提升网民网络安全感和满意度，最大限度调动网民参与网络生态治理的自觉性和主动性，助力政府相关部门积极探索网络治理规律，提高综合治理的成效和水平。

网民网络安全感满意度调查的宗旨就是要坚持面向网民大众，目的是让大家有话可以说，让政府主管部门可以倾听和了解网络安全在网民中的感受、网民的诉求和存在的问题。同时也向广大网民宣传网络安全的相关政策、法律和知识。

为充分发挥网络安全社会组织在网络空间建设中的桥梁作用，切实履行网络社会组织的社会责任，全面提升社会组织服务国家及地方政府网络安全建设水平，促进全国网络安全事业的发展，从 2018 年开始由全国多家网络安全社会组织联合发起了每年一度的全国网民网络安全感满意度调查活动，调查活动及其报告引起社会巨大反响。

2020 年度全国网民网络安全感满意度调查活动在抗击新冠疫情取得阶段性胜利和国际形势跌宕起伏，复杂多变的背景下进行，具有特别的意义。本年度调查活动由全国 135 家网络安全行业协会及相关社会组织联合发起，公安部网络安全保卫局作为指导单位对活动给予了强有力的指导和支持。各有关部门、各级公安机关等也给予了大力的支持，各参与单位和企业、机构等密切配合，为活动的成功举行打下坚实的基础。

活动组委会在总结 2018、2019 年两届网民网络安全感满意度调查活动经验基础上，今年的调查活动在活动组织、品牌建设、推广发动、研究规划、问卷设计等方面进行了多项的创新和改进，取得显著的效果，活动影响力和问卷数量实现跨越式增长。

2020 年 6 月，以“网络安全为人民，网络安全靠人民”为活动主题的 2020 网民网络安全感满意度调查活动正式启动，7 月 22 日上午 9 时活动正式对外采集数据，全国各大网络平台同步开通线上采集通道，至 7 月 31 日 24 时结束。

本次调查活动问卷收回总量为 150.3168 万份，其中，公众网民版 124.3251 万份，网络从业人员版 25.9912 万份。经过数据清洗后，有效样本数据总数为 149.0304 万份，其中，公众网民版 123.1455 万份，网络从业人员版 25.8849 万份。另外，调查活动还收到网民对我国网络安全建设提出的意见和建议共 16.4347 万条。

调查问卷按访问对象不同分两类问卷：面向普通网民的公众版和面向网络行业从业人员的从业人员版问卷

公众版的调查问卷除了以共性问题为主的主问卷外，还根据内容主题的不同分了 8 个专题问卷，具体名称如下：

- 专题 1 问卷：网络安全法治社会建设专题
- 专题 2 问卷：遏制网络违法犯罪行为专题
- 专题 3 问卷：个人信息保护专题
- 专题 4 问卷：网络购物安全权益保护专题
- 专题 5 问卷：未成年人网络权益保护专题
- 专题 6 问卷：互联网平台监管与企业自律专题
- 专题 7 问卷：数字政府服务与治理能力提升专题
- 专题 8 问卷：新冠疫情的影响和应对专题

从业人员版的调查问卷除了以共性问题为主的主问卷外，还根据内容主题的不同分为 A 到 D 共 4 个专题问卷，具体名称如下：

- A 专题问卷：等级保护实施与企业合规专题
- B 专题问卷：行业发展与生态建设专题
- C 专题问卷：新技术应用与网络安全专题

D 专题问卷：科技创新与人才培养专题。

本报告第一章为概述；第二章为主要发现；第三章为基本情况，包括受调查网民的基本信息；第四章为安全感和共性问题分析，主要为调查问卷数据详细统计，包括网民整体网络安全感分析；第五章是专题分析，主要是公众版问卷专题 1 到专题 8 问卷和从业人员版专题 A 到专题问卷内容的详细统计结果。

本报告是基于 2020 年度网民网络安全感满意度调查活动收集回来的有效问卷数据，经过整理、统计、初步分析后编写形成的。本专题报告主要反映参与调查的网民群体特别是从业人员对网络安全相关行业发展状况、网络安全感和满意度的感受，揭示网络安全相关行业的发展的态势和趋势，以及网民的关注点和痛点，为有关各方提供参考。

网络安全感满意度调查



广东新兴国家网络安全和信息化发展研究院

二、主要发现

本次调查活动问卷收回总量为 150.3168 万份，其中，公众网民版 124.3251 万份，网络从业人员版 25.9912 万份。经过数据清洗后，有效样本数据总数为 149.0304 万份，其中，公众网民版 123.1455 万份，网络从业人员版 25.8849 万份。

经过对调查数据统计、初步分析后，有以下主要发现：

2.1 网络安全行业发展前景看好，政策环境有利行业发展

（1）虽然遭遇疫情冲击，但绝大多数的从业人员（接近八成的 79.42%）认为行业发展前景有较大的增长。

参与调查的从业人员对网络安全行业未来一年发展的趋势评价：36.99%认为明显增长，42.43%认为略有增长，即接近八成（79.42%）从业人员认为未来有增长。

（2）调查数据显示对网络安全领域市场发展持上涨看法的占绝大部分（88.65%）。显示从业人员对网络安全市场看法比较乐观。

（3）当前促进网络安全产品与服务发展的政策环境受到好评。21.93%从业人员认为非常好，39.54%认为好，33.84%认为一般，持肯定态度的占大部分（61.47%）。

2.2 网络安全面临挑战，供应链安全风险受到关注

（4）网络安全问题和网络安全事件仍呈较高发生率。

网络安全问题和网络安全事件呈较高发生率。43.42%的从业人员在工作中最常遇到的网络安全问题是安全隐患（硬件漏洞、代码漏洞、业务逻辑漏洞、弱口令、后门等），41.48%从业人员遇到恶意程序（勒索病毒、挖矿勒索、供应链木马、蠕虫病毒、僵尸网络等），恶意网络资源（恶意 IP 地址、恶意域名、恶意 URL、网络钓鱼等）遇到率为 39.70%，安全事件（主机受控、数据泄露、网页篡改、网络监听等）遇到率为 38.81%。

（5）信息技术产业供应链安全威胁受到关注，57.86%从业人员认为供应链安全威胁比较高和非常高。显示国际形势发展对信息技术产业供应链安全的威胁

更加突出，对产业的健康发展造成一定的影响。

2.3 打击网络犯罪任重道远，痛点多关注度高

（6）信息泄露、网络诈骗和网络骚扰是网络安全最突出的问题。77.31%的从业人员认为网络安全最突出或亟需治理的问题是信息泄露。网络诈骗、网络骚扰分别列 2、3 位，关注度达 65.58%和 62.01%。网络谣言与诽谤、网络赌博、网络色情、游戏沉迷关注度也比较高，分别为 46.75%、46.18%、44.14%、41.34%。数据显示信息保护、打击诈骗、网络欺凌、打击涉黄涉赌等是网民主要的痛点。

行业内遭受网络勒索病毒、木马等的入侵而导致经济上受损的时有发生，渗透率达到 53.81%（偶尔遇到和经常遇到），情况比较严重。

（7）参与调查的从业人员对互联网黑灰产业的活跃度变化的评价差别比较大，认为增加有 40.49%，其中认为明显增加的有 19.08%，略有增加有 21.41%。认为减少的也有 32.7%，而认为不了解也有 18.37%。

2.4 行业生态建设有待加强，服务体系建设受到关注

（8）调查显示当前网络安全产品与服务的资费水平评价为偏高：16.48%从业人员认为非常高，39.89%从业人员认为比较高，35.90%认为适中，持比较高和非常高看法的占大部分（56.37%）。显示网络安全行业产品和服务收费是比较高的。

（9）调查显示当前网络安全产品与服务存在问题主要为：1 创新能力不足（60.32%）、2 核心技术依赖进口（53.03%）、3 可靠性差（42.84%）、4 服务不到位（38.44%）、5 性能低（38.24%）。

（10）调查显示网络安全行业协会等社会组织服务提供了的大量服务，有的服务仍需要加大推广力度。其中 53.11%从业人员使用过技术培训服务，38.65%使用过继续教育服务，37.22%使用过资质认证服务，32.31%使用过政策宣贯服务，显示技术培训是覆盖率最高的服务，其它服务还有一定的提升空间。

2.5 企业安全管理措施有所加强，等级保护制度取得成效

（11）网络安全等级保护制度扎实推进，行业指导推进得到落实。78.13%的参与调查的从业人员所在行业出台了具体的指导意见，其中 41.80%从业人员所在行业有明确细致的指导意见，36.33%有较为简单指导意见。

参与调查的从业人员所在单位网络安全等级保护开展方面，58.48%从业人员所在单位做了信息系统定级备案，51.96%开展了信息系统安全建设整改，51.60%进行了信息系统安全测评，53.84%开展了网络安全自查，但仍有 10.24%从业人员所在单位没有进行过网络安全等级保护工作。

（12）调查显示从业人员对所在单位安全管理状况满意度评价较高，71.57%从业人员表示满意或非常满意，其中 45.28%从业人员表示满意，26.29%从业人员表示非常满意。

（13）企业网络安全管理措施得到进一步落实。69.20%从业人员所在单位设置了网络安全专门机构，74.97%从业人员所在单位落实了网络安全责任人，58.74%从业人员所在单位落实了网络安全经费预算。61.82%从业人员认为单位网络安全应急预案完善或较为完善。72.10%从业人员表示所在单位有定期进行网络安全检查。总体上网络安全管理有所改善，但还有一定的提升空间。

广东新兴国家网络安全和信息化发展研究院

2.6 网络安全人才建设有待加强，培训制度逐步落实

（14）从业人员认为制约网络安全行业发展的主要障碍排前 3 位是：1 人才 73.41%，2 技术 71.57%，3 资金 60.65%。

（15）有关网络安全专业人才评价和队伍建设方面的问题，关注度排在前 5 名的是：1 职称不完善、晋升渠道不畅（59%）、2 实训环境不足（55.82%）、3 继续教育流于形式（50.69%）、4 专业不对口（48%）、5 任职资格管理不完善（47.84%）。数据显示从业人员对网络安全专业人才职业发展和培养存在的问题比较关注。

(16) 参与调查的从业人员对当前网络安全技术人才数量评价呈持平的状态，认为一般最多，占 37.95%，认为比较充足的 22.64% 和认为有效缺乏的 22.31% 差不多，认为非常充足的 9.04% 和认为严重不足的 8.03% 差不多。技术人才问题不仅是数量问题，还有质量和结构的问题。

2.7 新技术应用登场，安全风险受到关注

(20) 从业人员对新技术的网络安全问题是比较关注。从关注度排列前 5 位为：5G 移动网络(73.64%)、大数据(62.30%)、人工智能(54.50%)、物联网(41.92%)、云计算(41.20%)。

5G 网络应用安全成为行业内关注热点，从业人员对 5G 技术的顾虑主要有：5G 比 4G 服务收费更高(68.91%)，5G 网络覆盖面小(59.74%)，担心 5G 技术不成熟出现网络错误或卡顿(33.85%)，担心 5G 网络不安全(25.72%)。

人工智能的技术成熟度、安全隐私保护问题等是从业人员关注的重点。从业人员认为目前人工智能应用发展面临的阻力主要有：1 技术有待成熟(75.46%)、2 安全隐私问题有待解决(67.24%)、3 应用普及难度大(57.08%)等。

(21) 网络安全产品服务需求大幅上涨，对网络产品和服务划分等级得到行业认可。行业内人员信心提高，88.65% 的从业人员认为当前网络安全行业市场需求上涨。大部分(58.29%) 从业人员对网络安全行业提供网络安全保障水平是比较认可的。

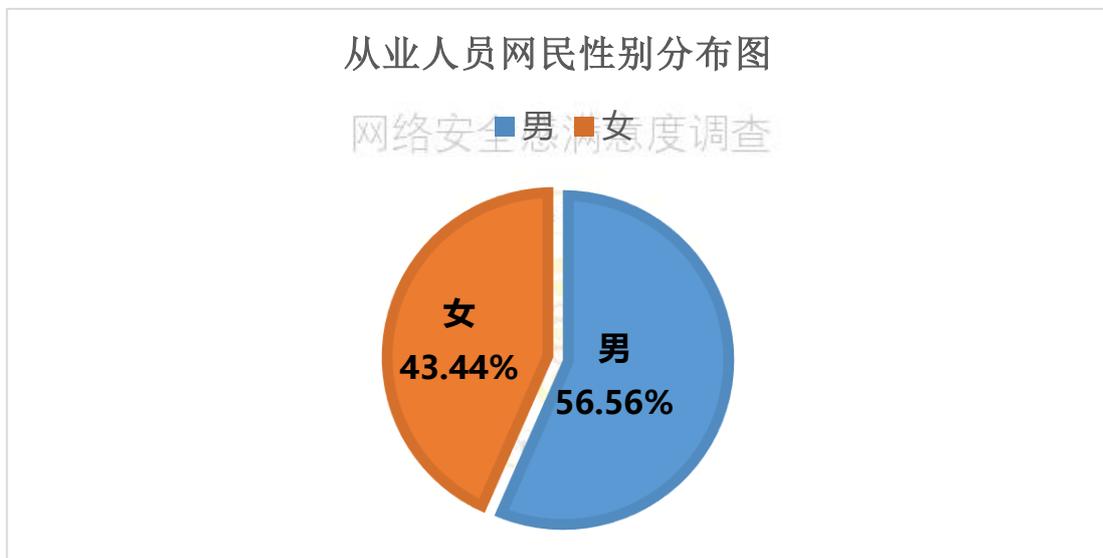
三、网络安全行业发展状况

3.1 从业人员状况

（1）性别分布

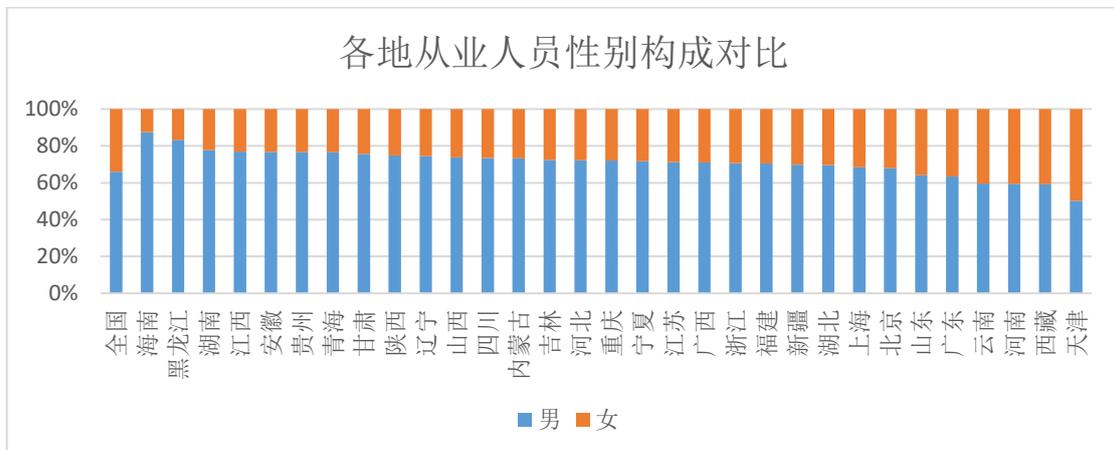
参与本次调查的从业人员网民中男性占 56.56%，女性网民占 43.44%。从数据上看从业人员中男性的比例稍高。

和去年相比，今年的数据更为均衡，参与调查的从业人员中男网民的占比有所下降，去年男网民占 70.21%，今年下降了 14 个百分点，达 56.56%；去年女性占 29.79%，今年上升了 14 个百分点，达到的 43.44%。今年的从业人员样本数量比去年增加很多，因此，数据分布较为平均。



图表 3.1-1：从业人员网民性别分布图

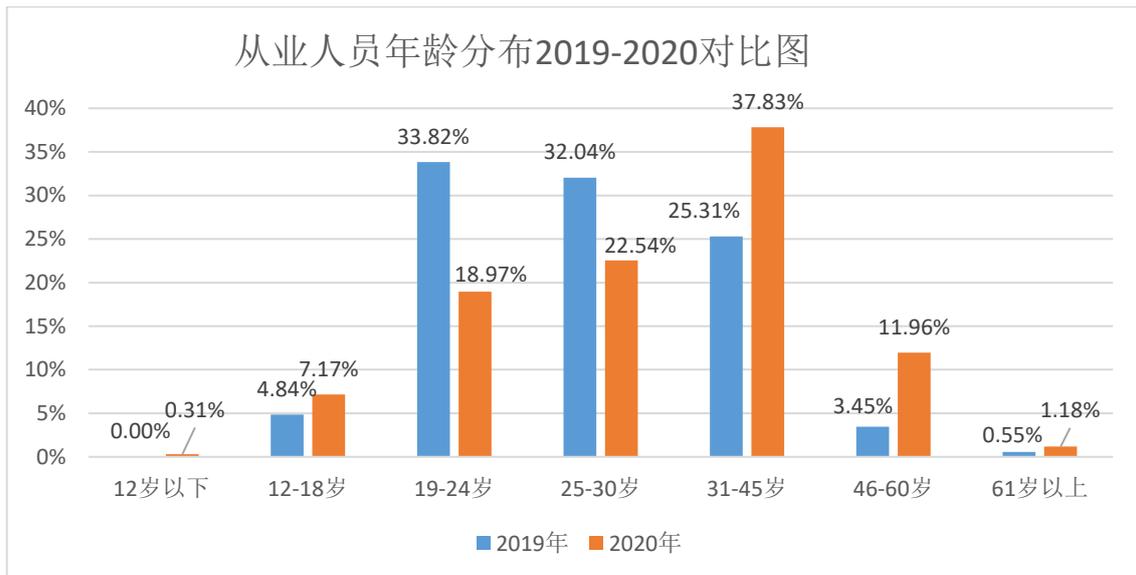
各地从业人员性别构成对比，除了天津的男女比例基本上比较均衡以外，其它地区的从业人员男性占大都在六成以上，呈男多女少的情况。



图表 3.1-2：各地从业人员网民性别分布对比

（2） 年龄分布

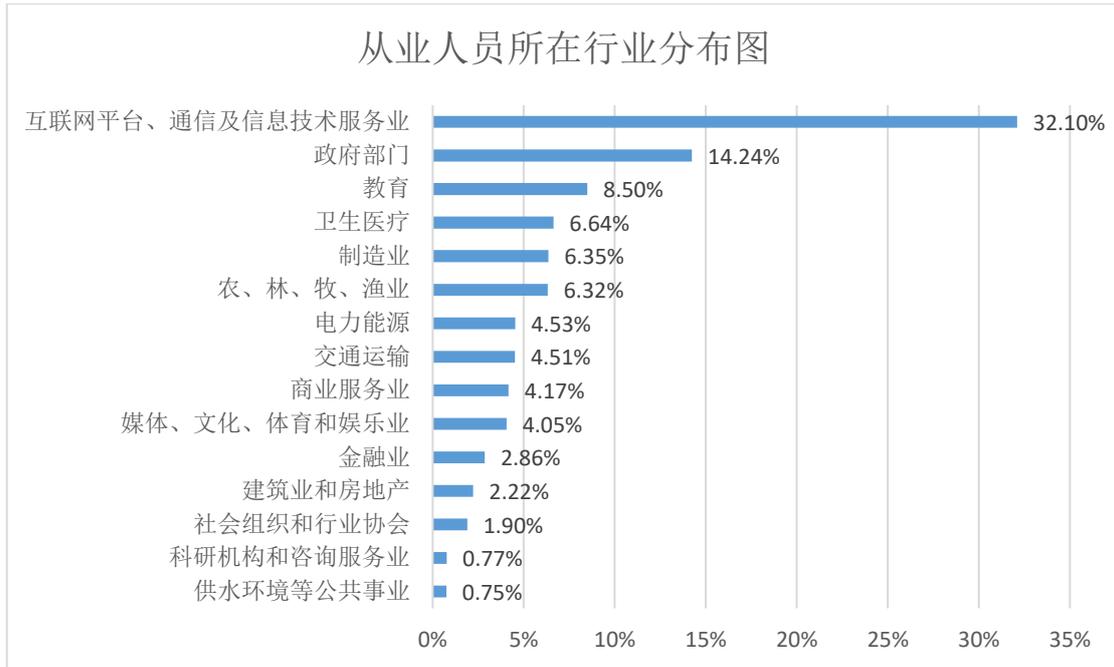
参与调查的从业人员网民中年轻人占大多数，其中，12 岁到 18 岁占 7.17%，19 岁到 24 岁占 18.97%，25 岁到 30 岁占 22.54%，31 岁到 45 岁占 37.83%，即 30 岁以下年轻人占约 49%。45 岁以下占 87%，从业人员年龄以中青年为主，其中 30 岁以下年轻人占差不多一半。



图表 3.1-3：从业人员网民年龄分布 2019-2020 对比图

（3） 行业分布

参加本专题网络安全从业人员主要分布在互联网平台、通信及信息技术服务业（占 32.10%）、政府部门（14.24%）、教育部门（8.50%）、卫生医疗（6.64%）等。

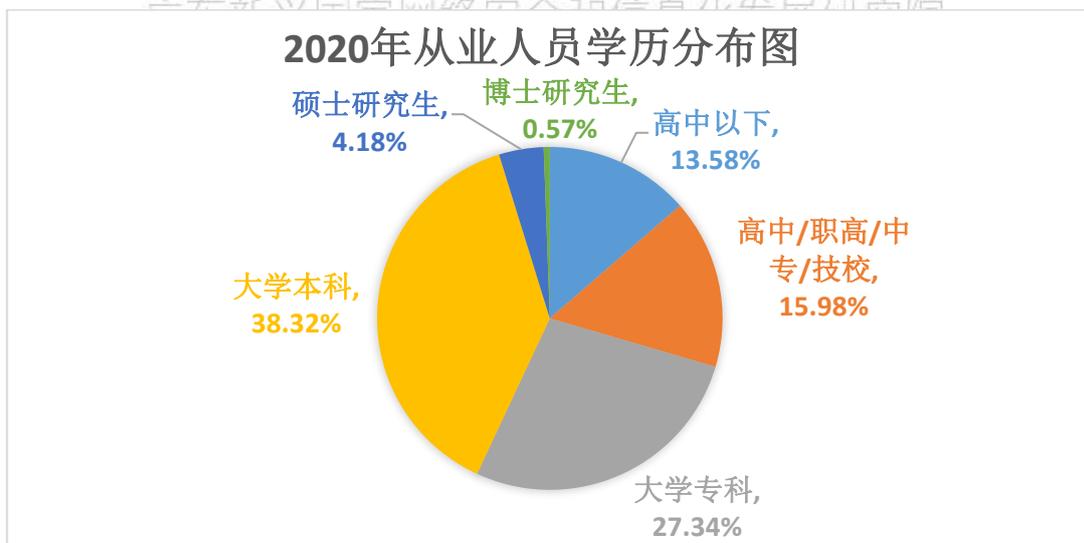


图表 3.1-4：从业人员所在行业的分布图

（图表数据来源：从业人员版等级保护实施与企业合规专题第 1 题：您单位所在的行业领域是？）

（4） 学历分布

参与调查的从业人员中大学本科学历人数最多，占 38.32%，其次是大专学历，占 27.32%。大专以上学历占 70.41%，在普通网民群体中受教育的程度相对不低，但在 IT 领域里学历水平不算高，大专等中低学历从业人员占比较高。



图表 3.1-5：从业人员学历分布图

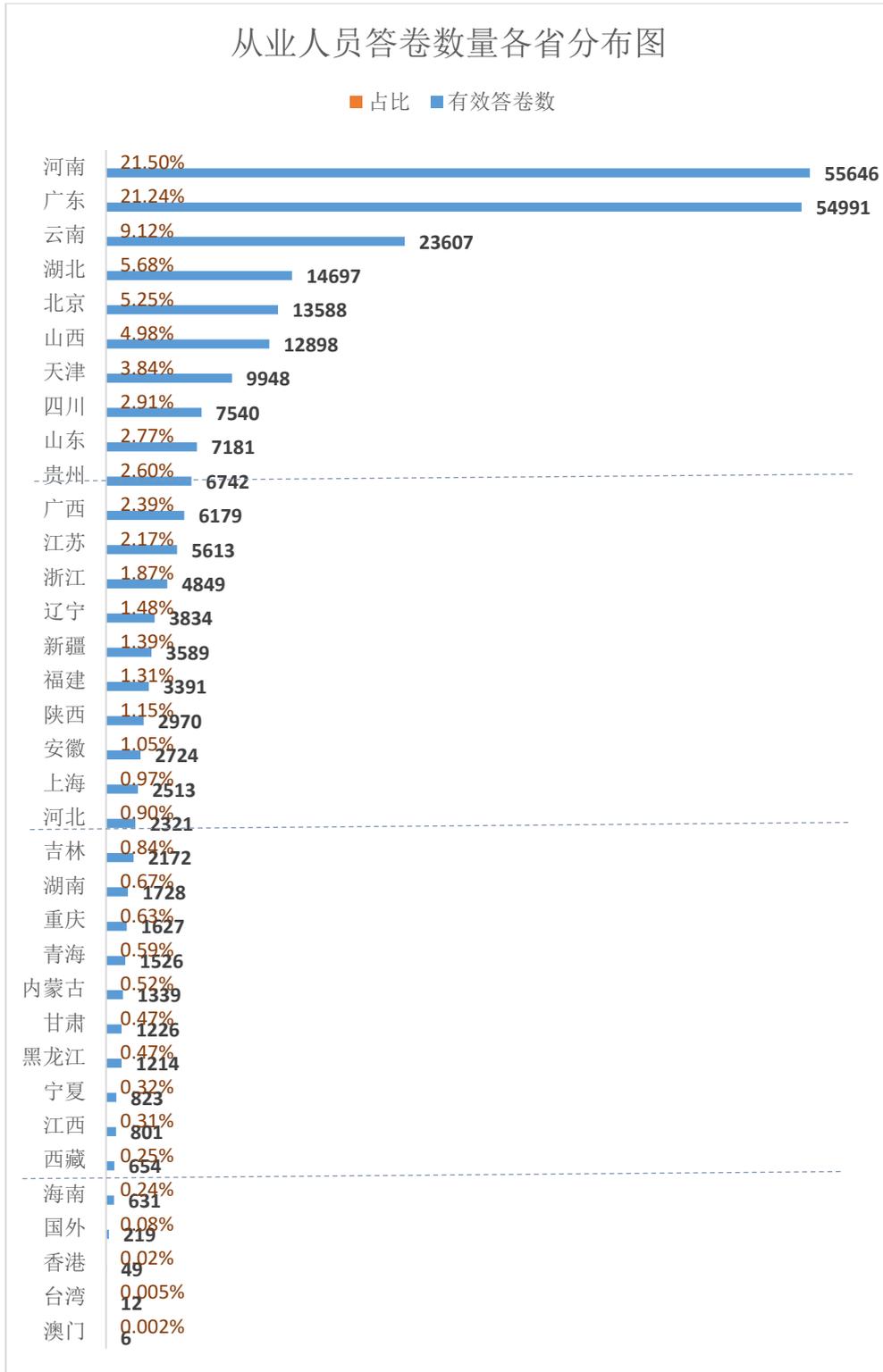
（5）地区分布

参与调查的从业人员网民来自全国各省、直辖市、自治区和港澳台地区等，其中河南、广东、云南、湖北、北京、山西、天津、四川、山东、贵州有效答卷数量排列前 10 位。各地区分布情况如下图：

网络安全感满意度调查



广东新兴国家网络安全和信息化发展研究院

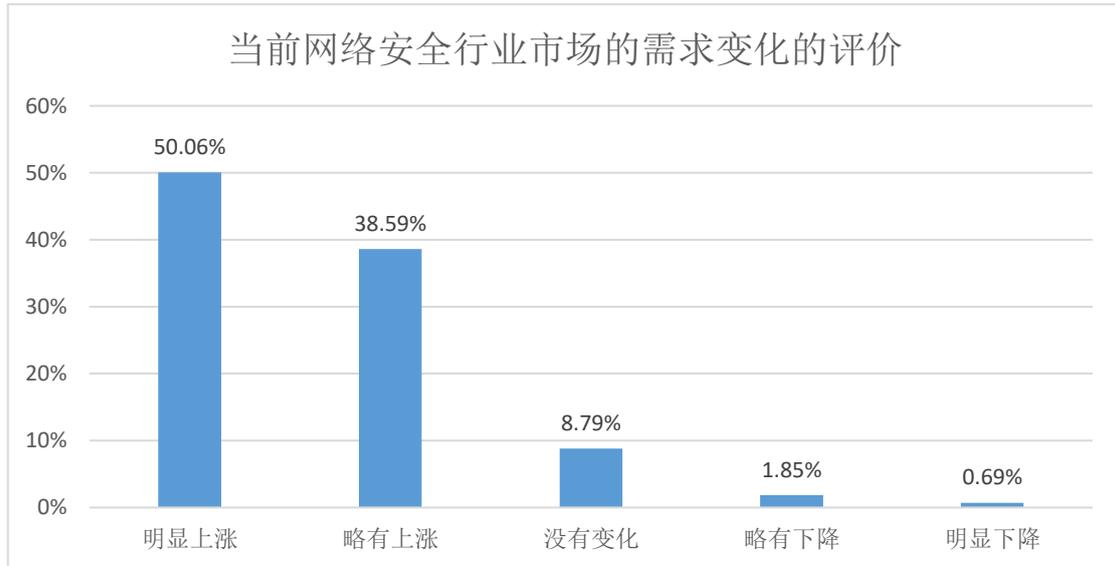


图表 3.1-6：从业人员答卷各省分布图

3.2 行业发展状况

（1）行业的市场需求变化

参与调查的从业人员对当前网络安全行业市场的需求变化评价为：50.06%从业人员认为明显上涨，38.59%从业人员认为略有上涨，8.79%认为没有变化，持上涨看法的占绝大部分（88.65%）。显示从业人员对网络安全市场看法比较乐观。



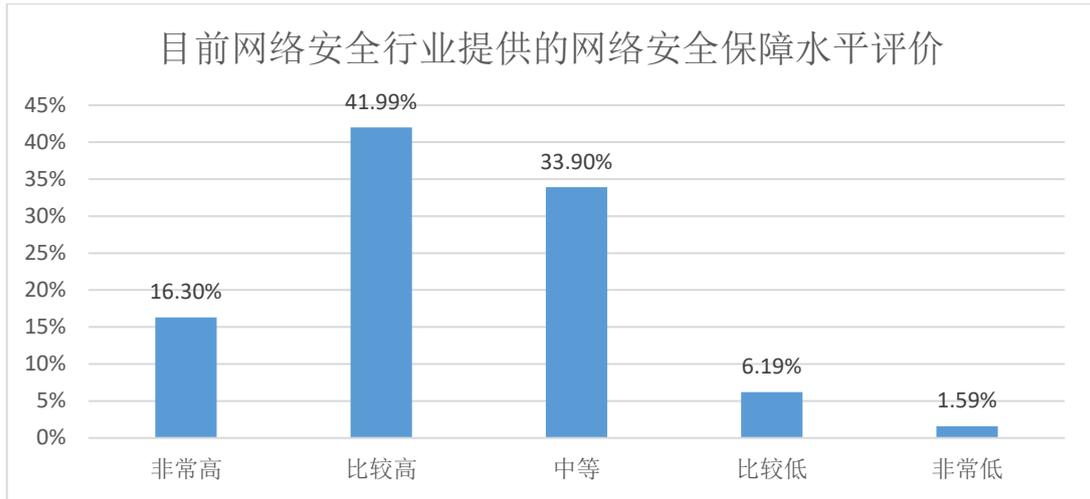
图表 3.2-1：从业人员对当前网络安全行业市场的需求变化的评价

（图表数据来源：从业人员版专题 B 第 2 题：相比以往，您认为当前网络安全行业市场的需求变化如何？）

广东新兴国家网络安全和信息化发展研究院

（2）行业安全保障水平

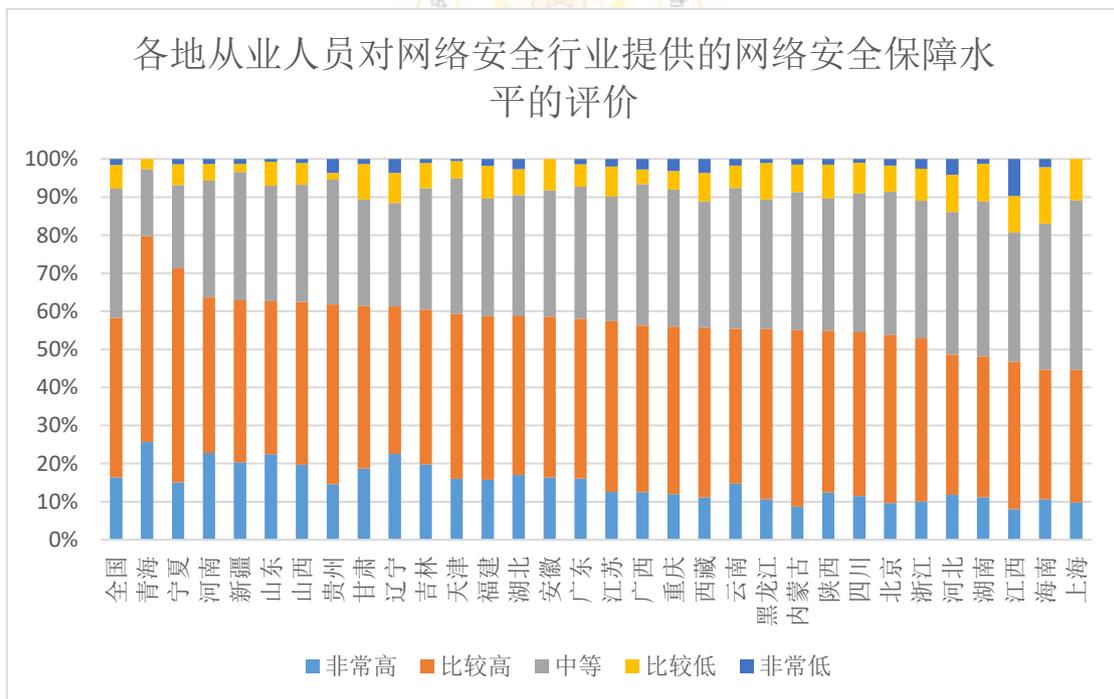
参与调查的从业人员对目前网络安全行业提供的网络安全保障水平评价为：16.30%从业人员认为非常高，41.99%从业人员认为比较高，33.90%认为中等，认为行业的网络安全保障水平比较高和非常高看法的占大部分（58.29%）。显示大部分从业人员对网络安全行业提供网络安全保障水平是比较认可的。



图表 3.2-2：目前网络安全行业提供的网络安全保障水平评价

（图表数据来源：从业人员版行业发展与生态建设专题第 3 题：据您了解目前网络安全行业提供的网络安全保障水平如何？）

各地从业人员对行业服务水平的评价青海、宁夏、河南、新疆、山东、山西、贵州、甘肃、辽宁、吉林等地从业人员的评价比较高，上海、海南、江西、湖南、河北等地评价相对靠后。

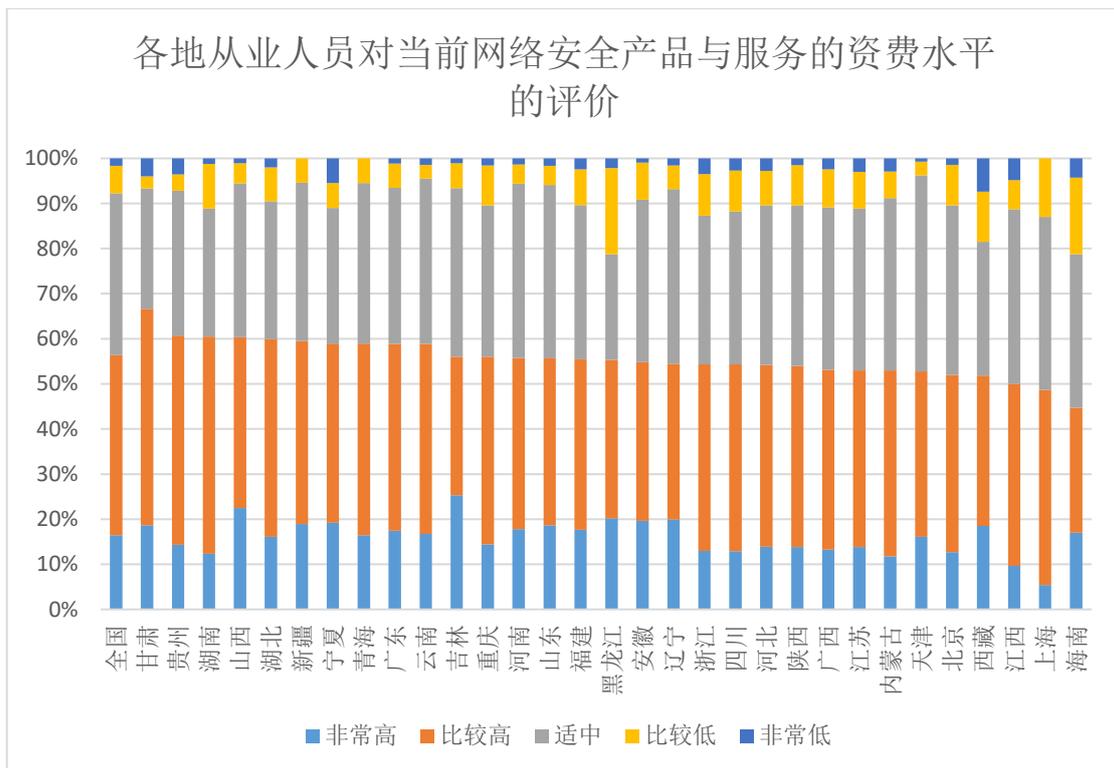


图表 3.2-3：各地从业人员对行业提供的网络安全保障水平的评价

(3) 行业服务资费水平

参与调查的从业人员对当前网络安全产品与服务的资费水平总体评价为：16.48%从业人员认为非常高，39.89%从业人员认为比较高，35.90%认为适中，持比较高和非常高看法的占大部分（56.37%）。显示网络安全行业产品和服务收费是比较高的。

按地区分布来看，甘肃、贵州、湖南、山西、湖北、新疆、宁夏、青海、广东、云南等地的从业人员有较高的比例认为资费水平偏高。主要是西北、西南地区。



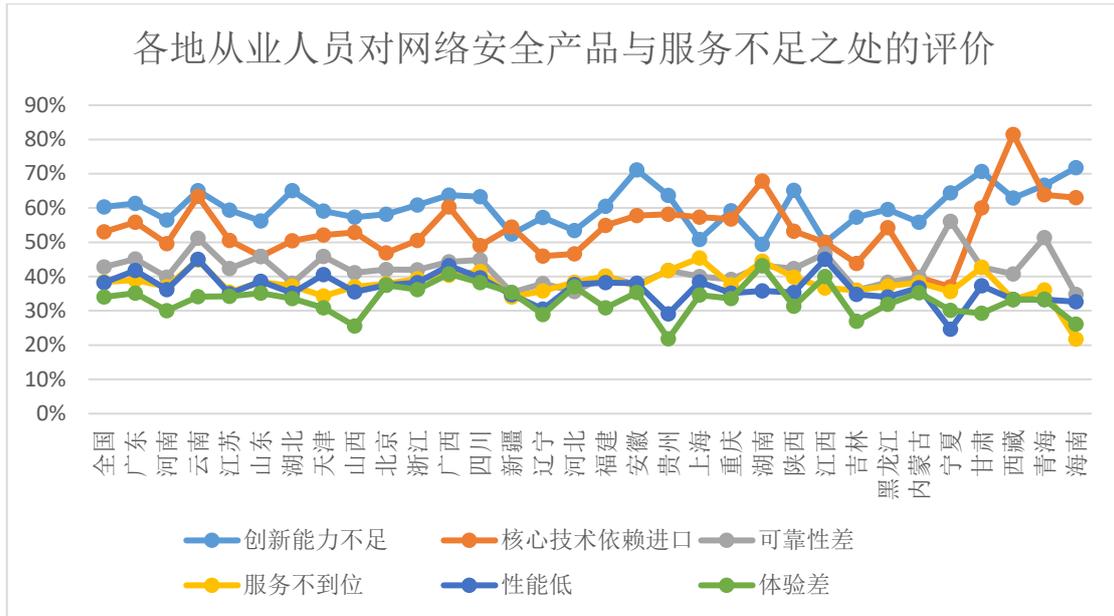
图表 3.2-4：各地从业人员对当前网络安全产品与服务的资费水平评价

（图表数据来源：从业人员版行业发展与生态建设专题第 5 题：您认为当前网络安全产品与服务的资费水平如何？）

（5）行业服务不足之处

参与调查的从业人员对当前网络安全产品与服务存在问题看法为：排前 5 位的为：1 创新能力不足（60.32%）、2 核心技术依赖进口（53.03%）、3 可靠性差（42.84%）、4 服务不到位（38.44%）、5 性能低（38.24%）。

从各地的数据看，大多数从业人员对核心技术依赖进口和创新能力不足比较关注，显示行业对供应链安全风险有较深刻的认识。



图表 3.2-5：当前网络安全产品与服务存在的不足之处

（图表数据来源：从业人员版行业发展与生态建设专题第 6 题：您认为当前网络安全产品与服务存在的不足之处是？）

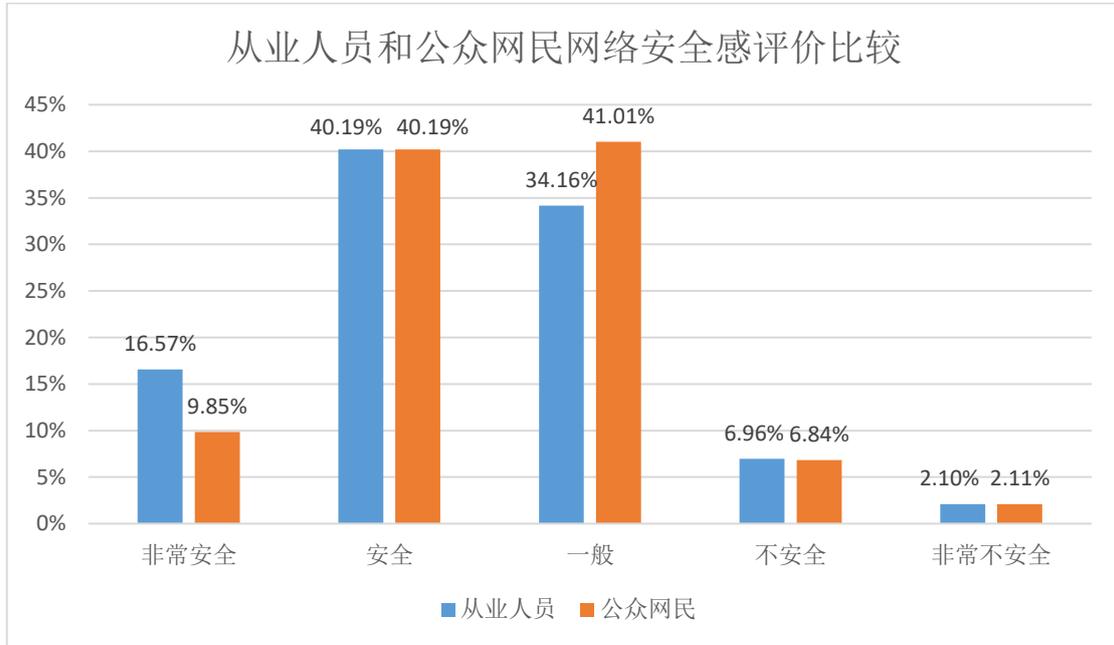


广东新兴国家网络安全和信息化发展研究院

3.3 网络安全态势

（1）从业人员安全感

数据显示从业人员持中间态度的比例比公众网民明显减少，相应地认为非常安全的比例比公众网民明显增加，其它评价分类比例基本一致。说明从业人员对网络的情况比较了解，网络安全感的感受也强烈一点。

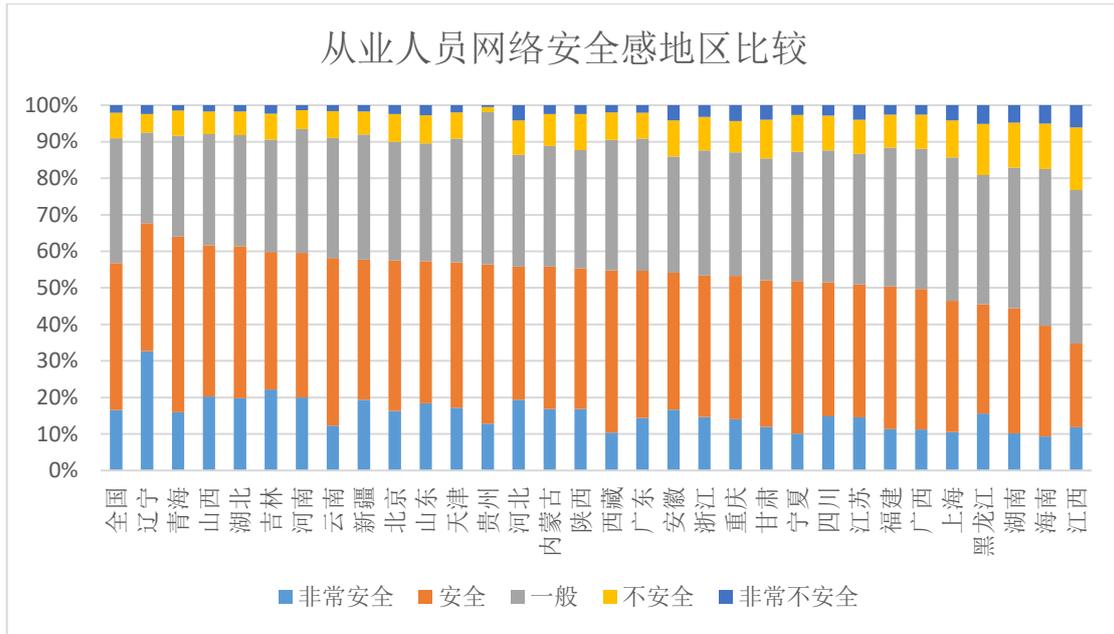


图表 3.3-1：从业人员和公众网民网络安全感评价比较

（图表数据来源：从业人员版主问卷第 6 题：您认为当前网络安全状况如何？）

1) 从业人员安全感地区差异比较

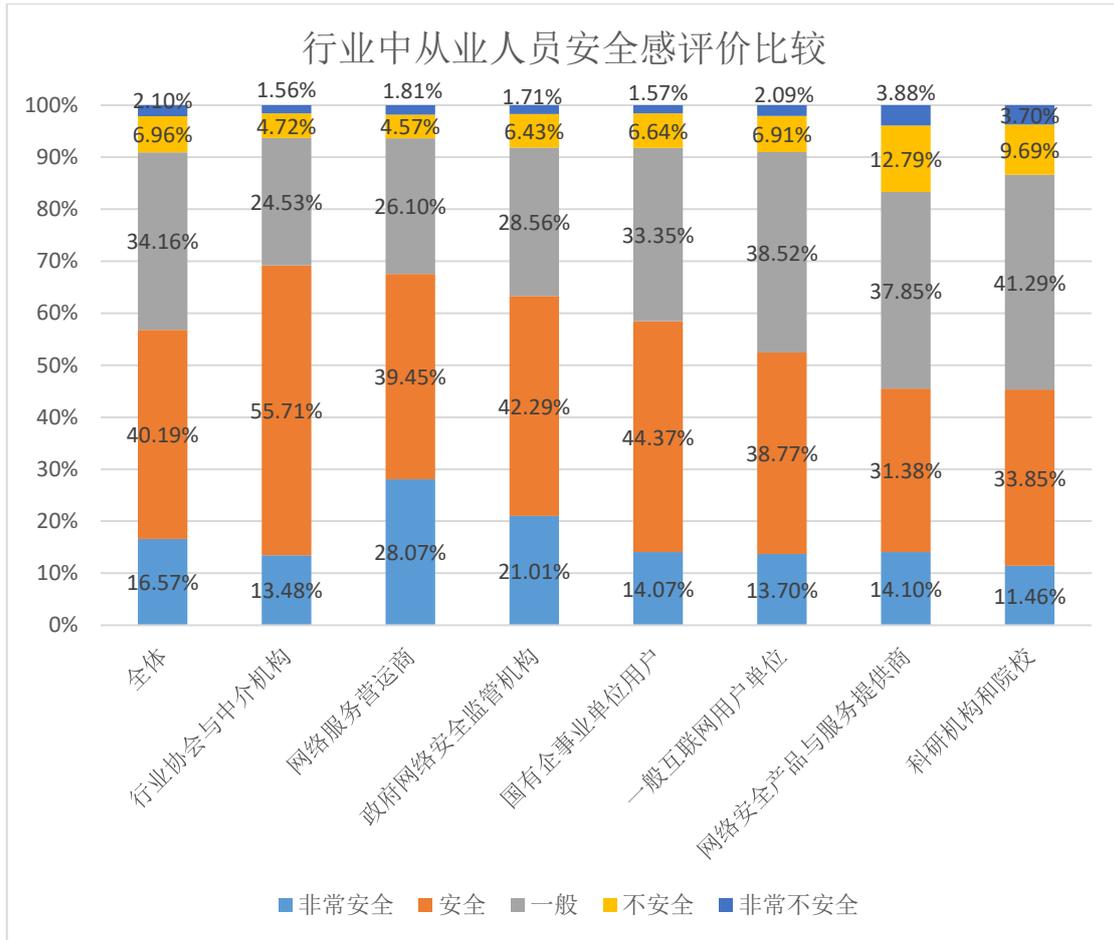
各省从业人员安全感比较，辽宁、青海、山西、湖北、吉林、河南等地区从业人员的安全感较高，认为非常安全和比较安全的比例超过六成。广西、上海、黑龙江、湖南、海南、江西等地从业人员安全感相对较低，认为非常安全和比较安全的比例少于五成。



图表 3.3-2：不同地区从业人员网络安全感评价比较

2) 不同行业的从业人员安全感差异比较

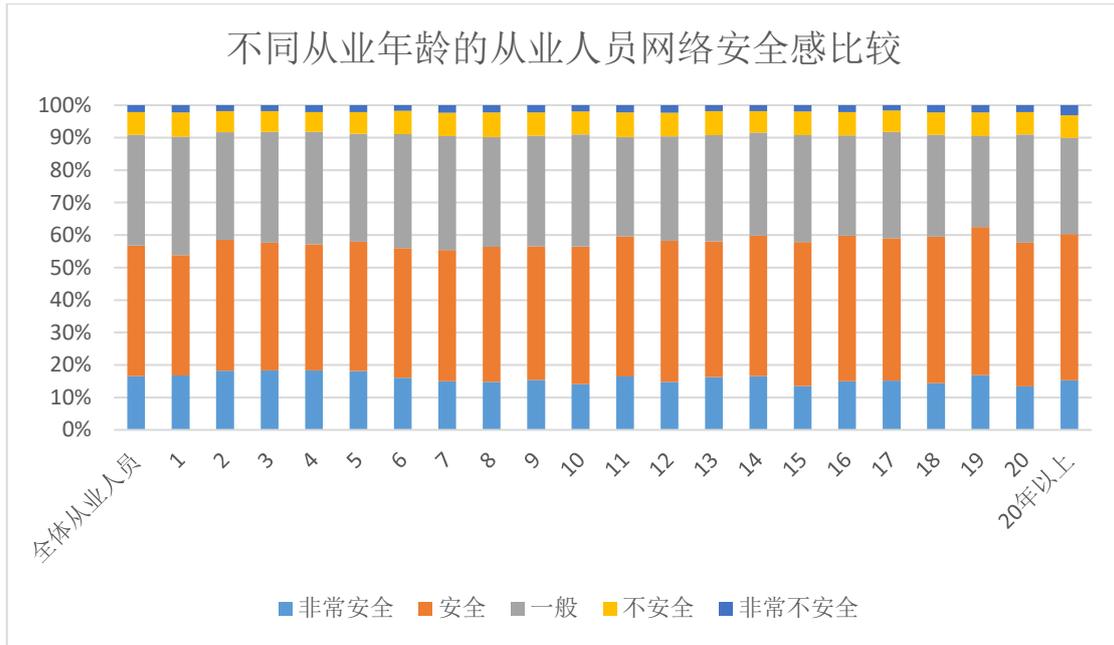
行业协会和中介机构的从业人员、网络服务营运商、政府网络安全监管机构的从业人员安全感相对较高，用户单位、网络安全产品与服务提供商、科研机构和院校的从业人员的安全感相对较低。



图表 3.3-3: 不同行业从业人员网络安全感评价比较

3) 不同从业年龄的从业人员网络安全感比较

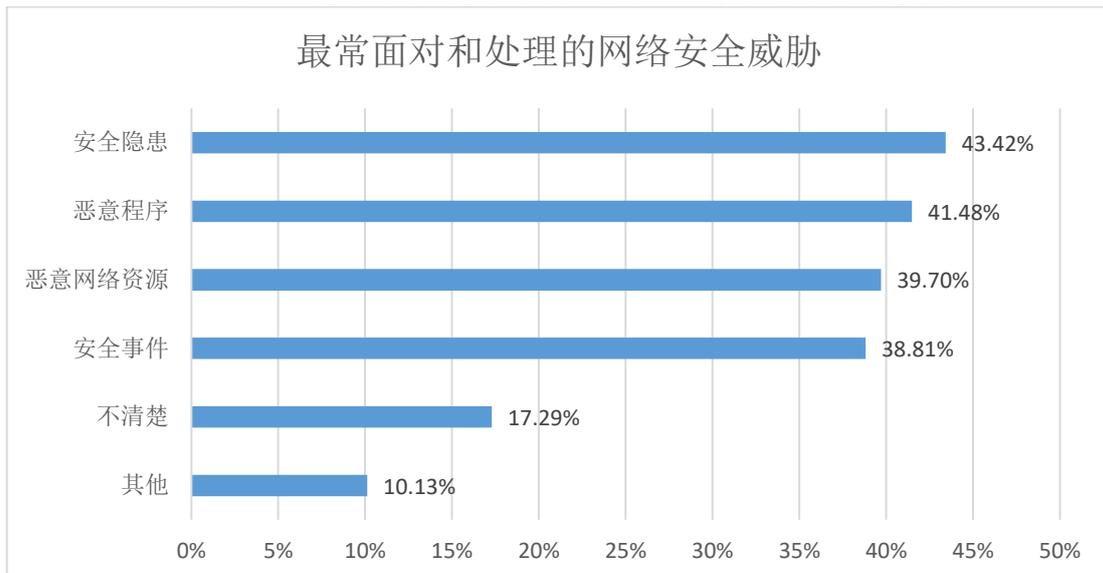
不同从业时间的从业人员安全感差别不大，相对地从业时间长的从业人员网络安全感比例略有上升。从业时间在 3-10 年之间的从业人员的网络安全感相对较低。



图表 3.3-4：不同从业年龄的从业人员网络安全感评价比较

(2) 从业人员在工作中常遇到的安全威胁

43.42%参与调查的从业人员在工作中最常遇到的网络安全问题是安全隐患（硬件漏洞、代码漏洞、业务逻辑漏洞、弱口令、后门等），41.48%从业人员遇到恶意程序（勒索病毒、挖矿勒索、供应链木马、蠕虫病毒、僵尸网络等），恶意网络资源（恶意 IP 地址、恶意域名、恶意 URL、网络钓鱼等）遇到率为 39.70%，安全事件（主机受控、数据泄露、网页篡改、网络监听等）遇到率为 38.81%。

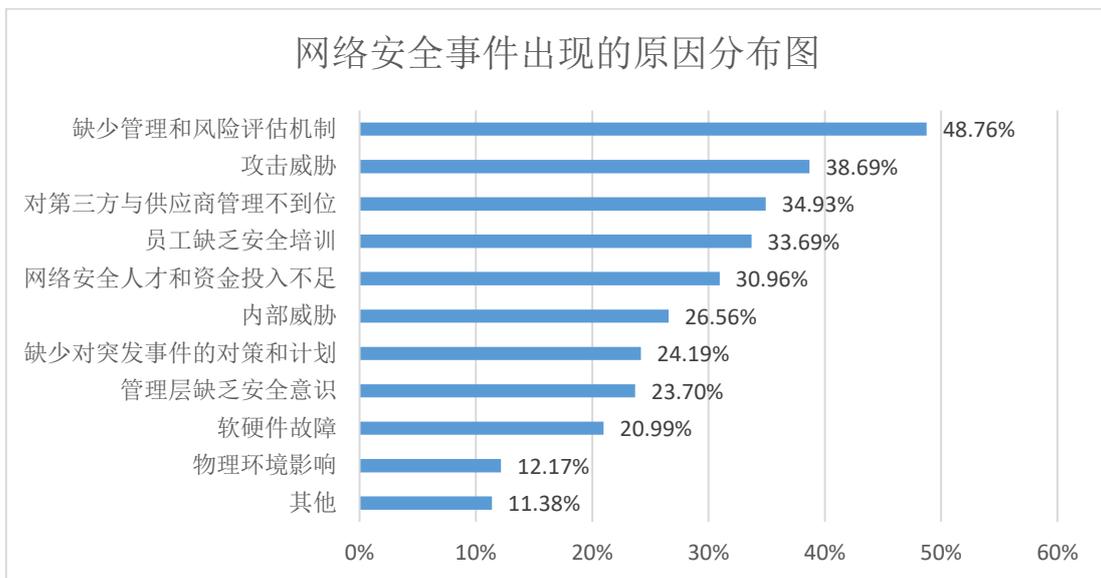


图表 3.3-6：在工作中最常面对的网络安全威胁

（图表数据来源：从业人员版主问卷第 8 题：您在工作中最常面对和处理的网络安全威胁是？（多选））

（3）网络安全事件频繁出现的原因

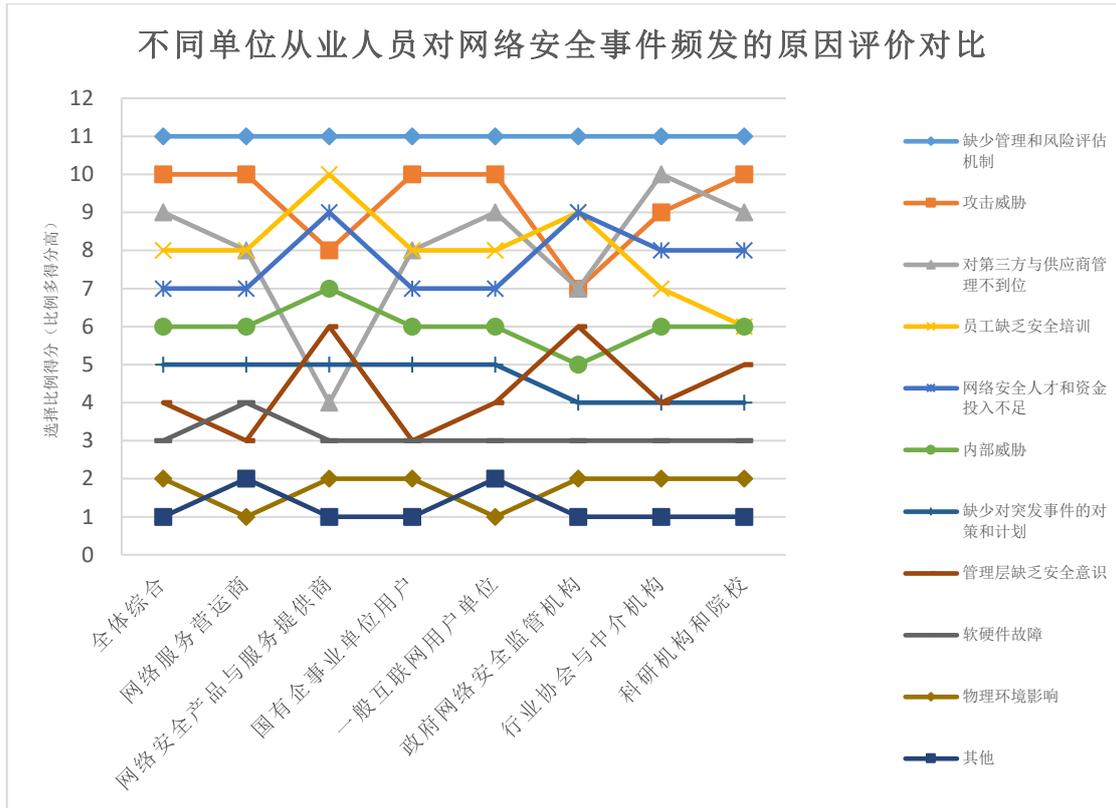
参与调查的从业人员认为网络安全事件频繁出现的原因排前五位是 1 缺少管理和风险评估机制，2 攻击威胁，3 对第三方与供应商管理不到位，4 员工缺乏安全培训，5 网络安全人才和资金投入不足，关注度分别为：48.76%、38.69%、34.93%、33.69%、30.96%；反映了管理、威胁、投入等方面是主要的原因。



图表 3.3-7：网络安全事件出现的原因

（图表数据来源：从业人员版主问卷第 9 题：您认为造成网络安全事件频繁出现的主要原因是？）

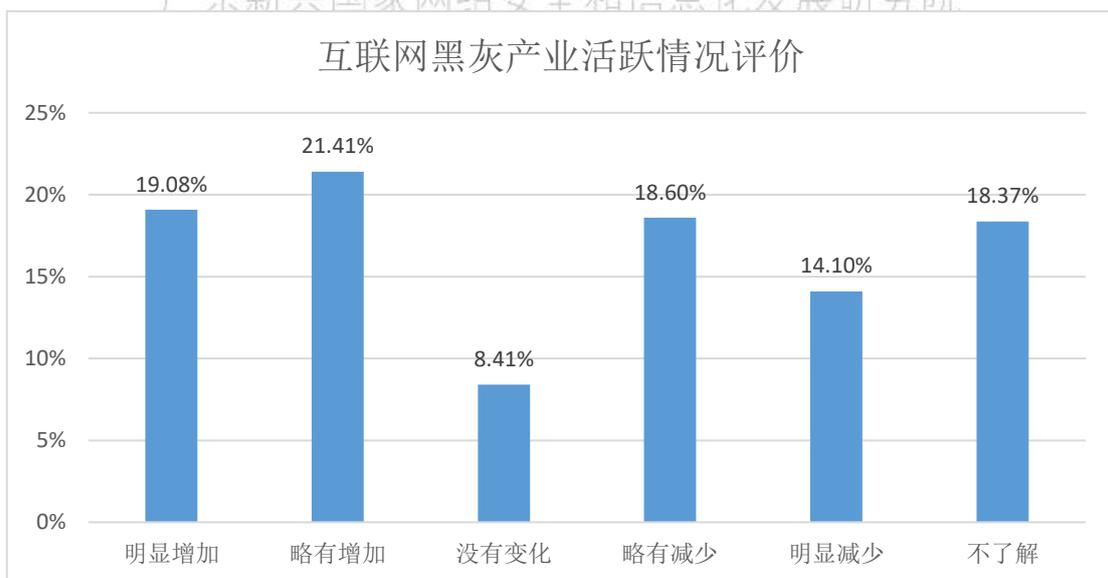
从不同单位从业人员的评价对比，除了网络安全产品与服务提供商、监管机构的选择跟其它各方不同以外，其它各方选择排列次序差别不大。服务供应商比较看重员工缺乏安全培训和人才资金投入不足等问题，认为管理层确认安全意识的比例较高。数据显示，不同单位站在用户、供应商的不同的立场对问题的看法不同。



图表 3.3-8: 不同单位对网络安全事件出现的原因的排列比较

(4) 互联网黑灰产业活跃情况

参与调查的从业人员对互联网黑灰产业的活跃度变化的评价差别比较大, 认为增加有 40.49%, 其中认为明显增加的有 19.08%, 略有增加有 21.41%。认为减少的也有 32.7%, 而认为不了解也有 18.37%。

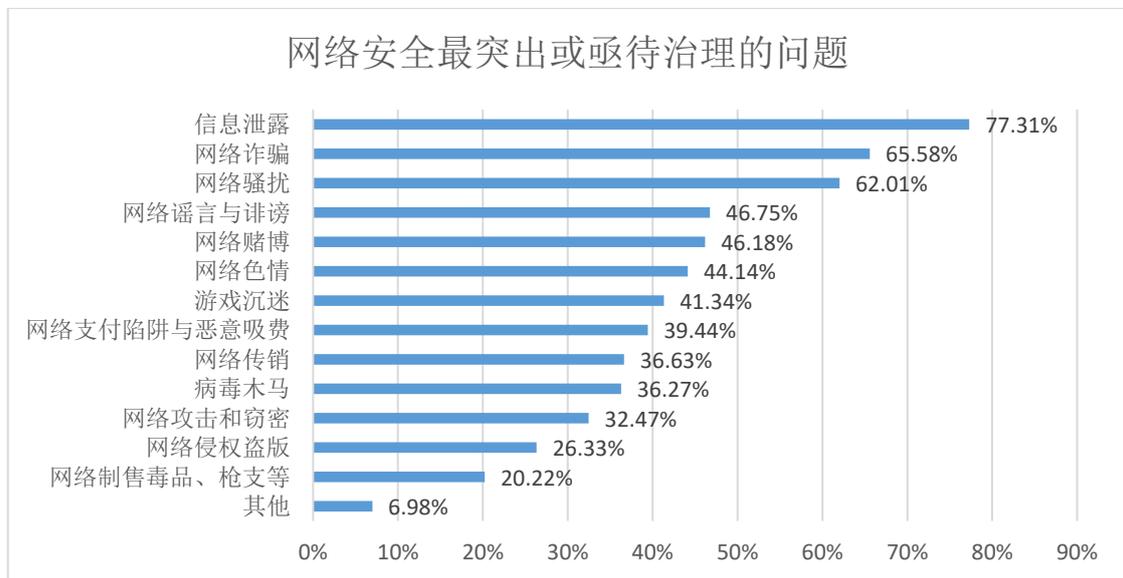


图表 3.3-9：互联网黑灰产业活跃情况评价

（图表数据来源：从业人员版主问卷第 10 题：您认为近年来网络数据、账号违法交易，网络色情等互联网黑灰产业的情况是？）

（5）网络安全突出问题

77.31%参与调查的从业人员认为网络安全最突出或亟需治理的问题是信息泄露。网络诈骗、网络骚扰分别列 2、3 位，关注度达 65.58%和 62.01%。网络谣言与诽谤、网络赌博、网络色情、游戏沉迷关注度也比较高，分别为 46.75%、46.18%、44.14%、41.34%。显示信息保护、打击诈骗、网络欺凌、打击涉黄涉赌等是主要的痛点。



图表 3.3-9：网络安全最突出或亟需治理的问题

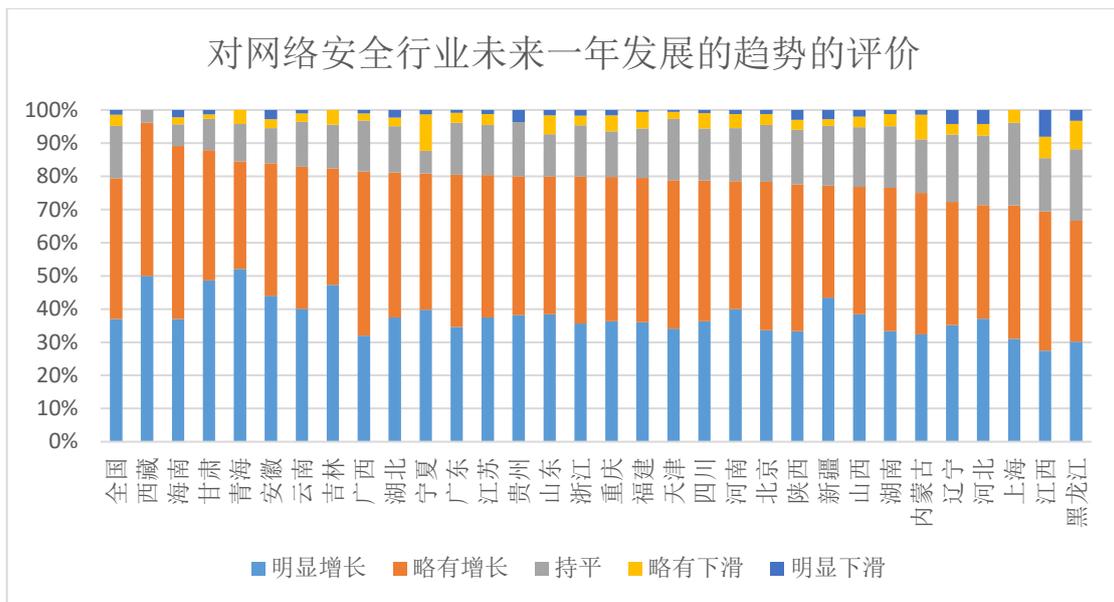
（图表数据来源：从业人员版主问卷第 14 题：您认为当前网络安全最突出或亟待治理的问题有哪些？）

3.4 行业发展前景

（1）未来发展趋势评价

参与调查的从业人员对网络安全行业未来一年发展的趋势评价：**36.99%**认为明显增长，**42.43%**认为略有增长，即接近八成（**79.42%**）从业人员认为未来有增长。

其中西藏、海南、甘肃、青海、安徽、云南、吉林、广西、湖北、宁夏、各地、江苏等地评价比较乐观，高于平均水平。

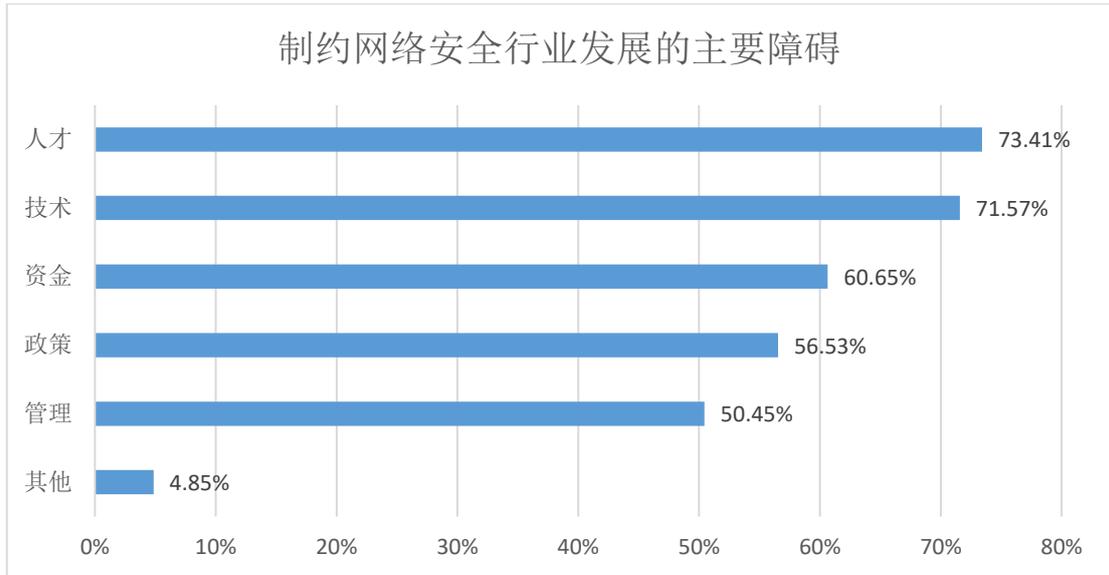


图表 3.4-1：对网络安全行业未来一年发展的趋势的评价

（图表数据来源：从业人员版行业发展与生态建设专题第 12 题：您认为网络安全行业未来一年发展的趋势如何？）

（2）制约行业发展的障碍

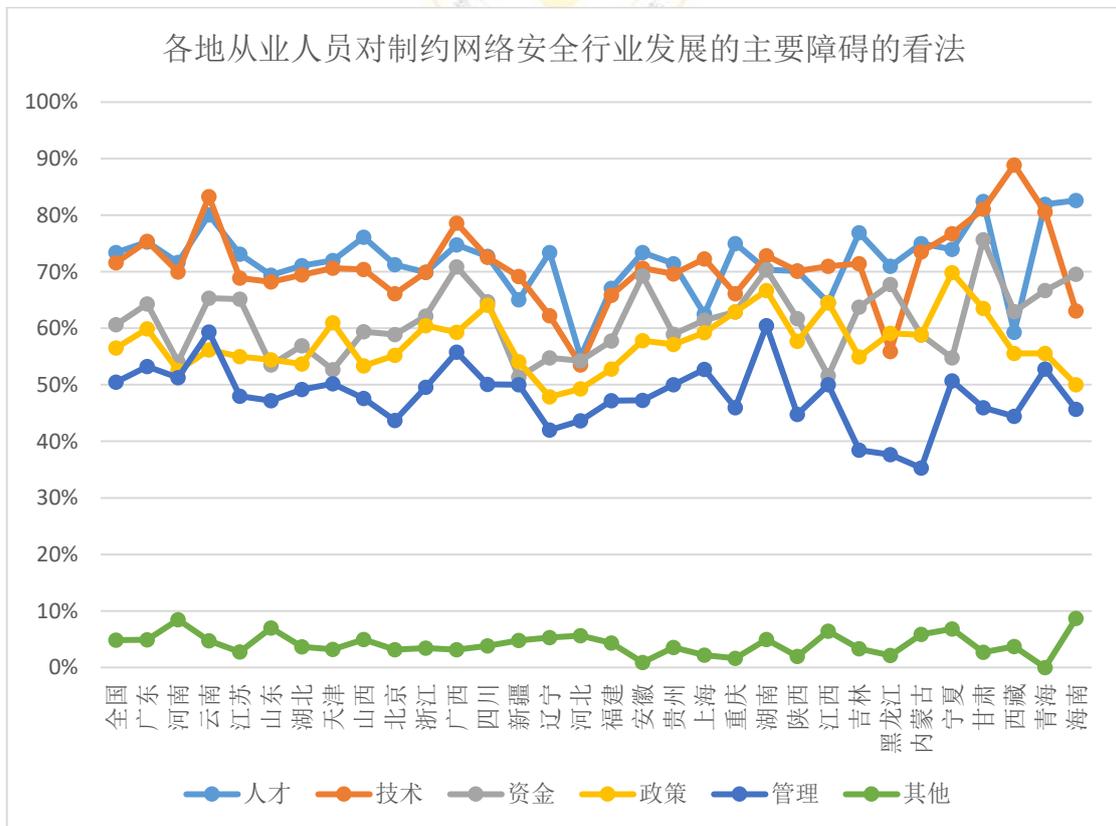
从业人员认为制约网络安全行业发展的主要障碍排前 3 位是：1 人才 73.41%，2 技术 71.57%，3 资金 60.65%。



图表 3.4-2：制约网络安全行业发展的主要障碍

（图表数据来源：从业人员版行业发展与生态建设专题第 11 题：您认为制约网络安全行业发展的主要障碍是什么？）

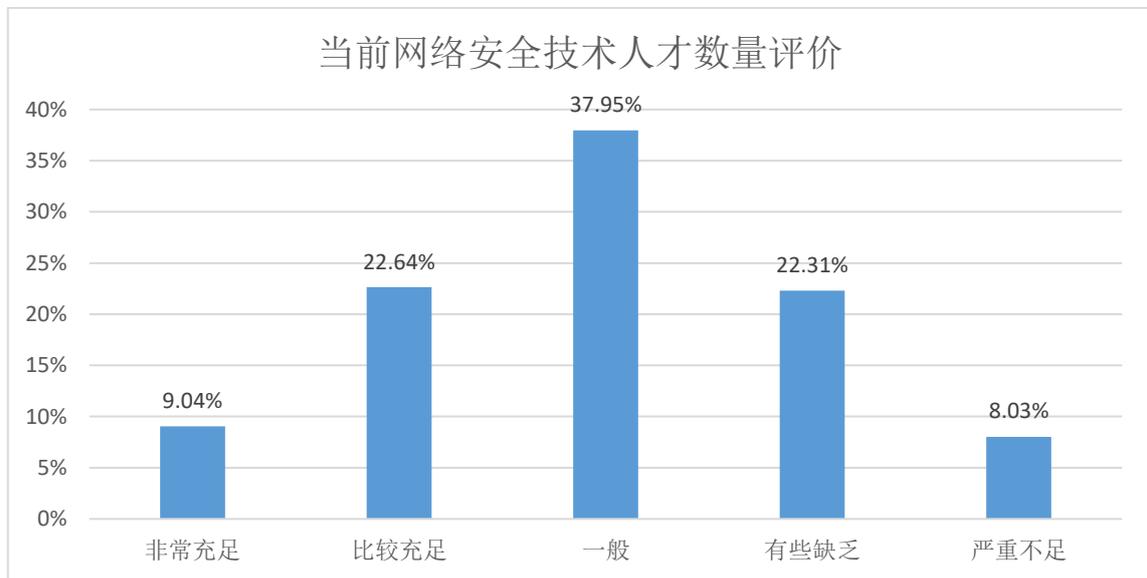
从各地数据对比显示除了西藏以外，全国对主要障碍排列次序都差不多。除了人才和技术，资金和政策这两对障碍内部位置有互换之外，其它的排列次序基本一样。



图表 3.4-3：各地从业人员对制约网络安全行业发展的主要障碍的看法
（图表数据来源：从业人员版行业发展与生态建设专题第 11 题：您认为制约网络安全行业发展的主要障碍是什么？）

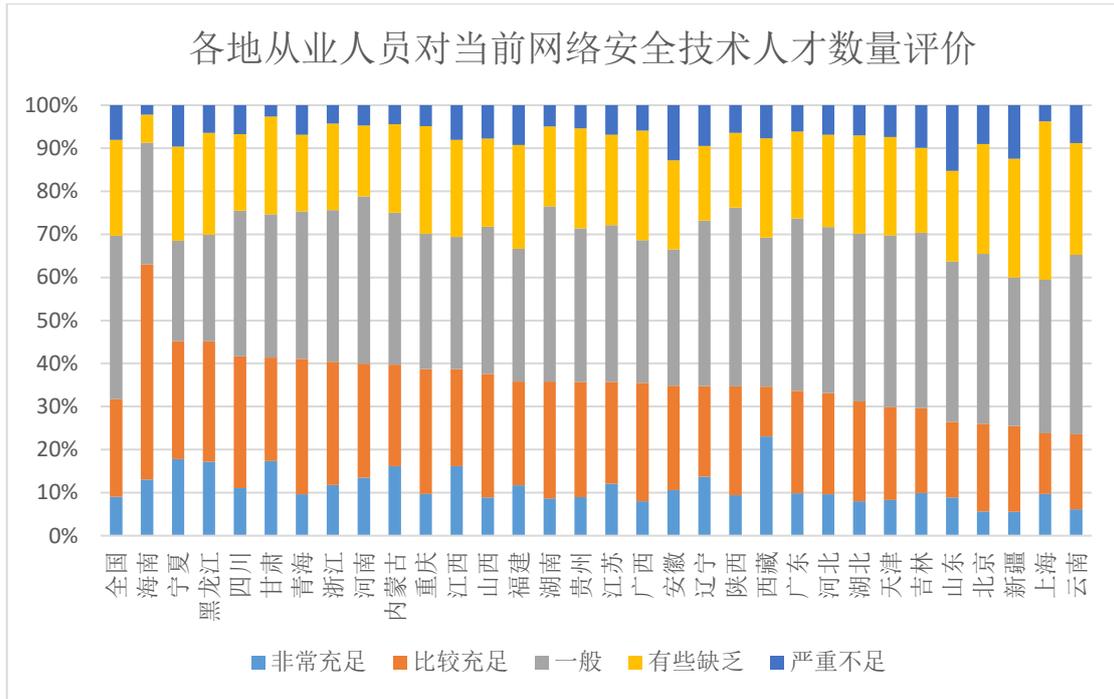
（4）行业技术人才数量

参与调查的从业人员对当前网络安全技术人才数量评价呈持平的状态，认为一般最多，占 37.95%，认为比较充足的 22.64%和认为有效缺乏的 22.31%差不多，认为非常充足的 9.04%和认为严重不足的 8.03%差不多。技术人才问题不仅是数量问题，还有质量和结构的问题。



图表 3.4-4：当前网络安全技术人才数量评价
（图表数据来源：从业人员版行业发展与生态建设专题第 8 题：您认为当前网络安全技术人才数量如何？）

各地从业人员的评价比较，云南、上海、新疆、北京等地评价较低，认为人才数量不足。海南、宁夏、黑龙江、四川、甘肃、青海、浙江、河南、内蒙古等地区认为比较充足的比例较多。



图表 3.4-5：各地从业人员对当前网络安全技术人才数量评价

（图表数据来源：从业人员版从业发展与生态建设专题问卷第 8 题：您认为当前网络安全技术人才数量如何？）



广东新兴国家网络安全和信息化发展研究院

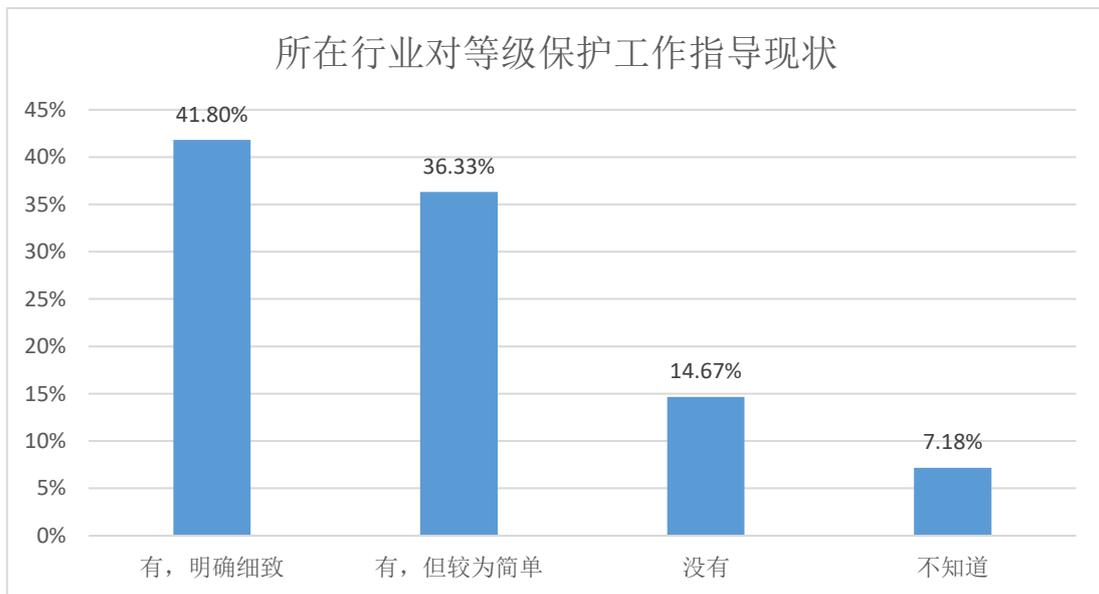
四、专题分析

4.1 等级保护实施与企业合规

参加本专题调查的从业人员数量为 15095 人。

（1）所在行业对等级保护工作指导

行业主管部门对等级保护工作的推进落实方面，78.13%的参与调查的从业人员所在行业出台了具体的指导意见，其中 41.80%从业人员所在行业有明确细致的指导意见，36.33%有较为简单指导意见。

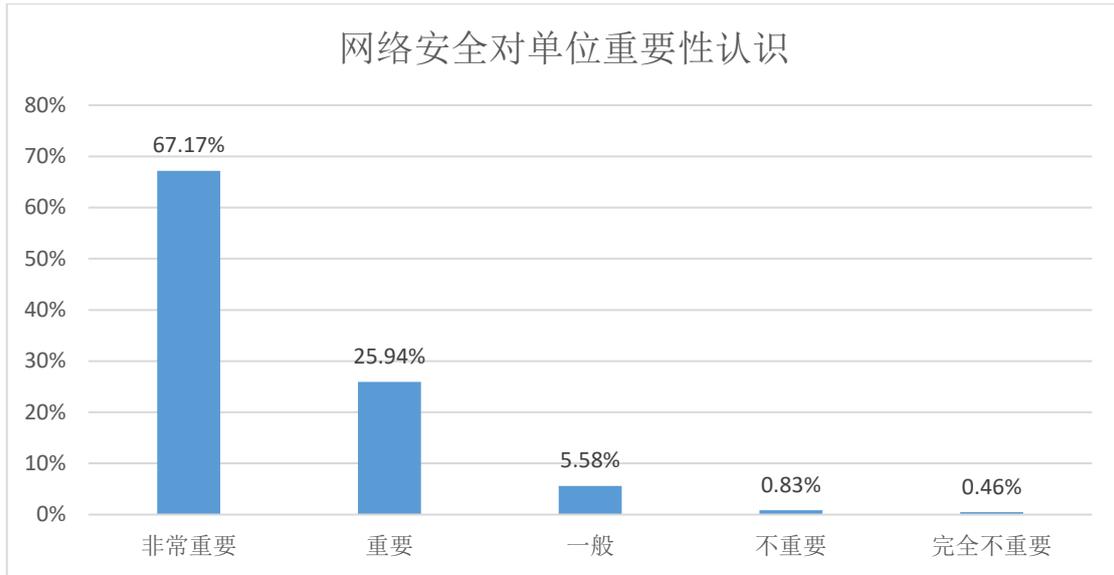


图表 4.1-1：所在行业对等级保护工作指导现状

（图表数据来源：从业人员版等级保护实施与企业合规专题第 2 题：您单位所在行业是否有明确的等级保护工作指导意见（系统定级、测评周期要求、安全建设和检查）？）

（2）网络安全对单位重要性认识

网络安全对单位的重要性认识方面，绝大部分（93.11%）参与调查的从业人员认为重要和非常重要，其中 67.17%从业人员认为非常重要，25.94%从业人员认为重要。

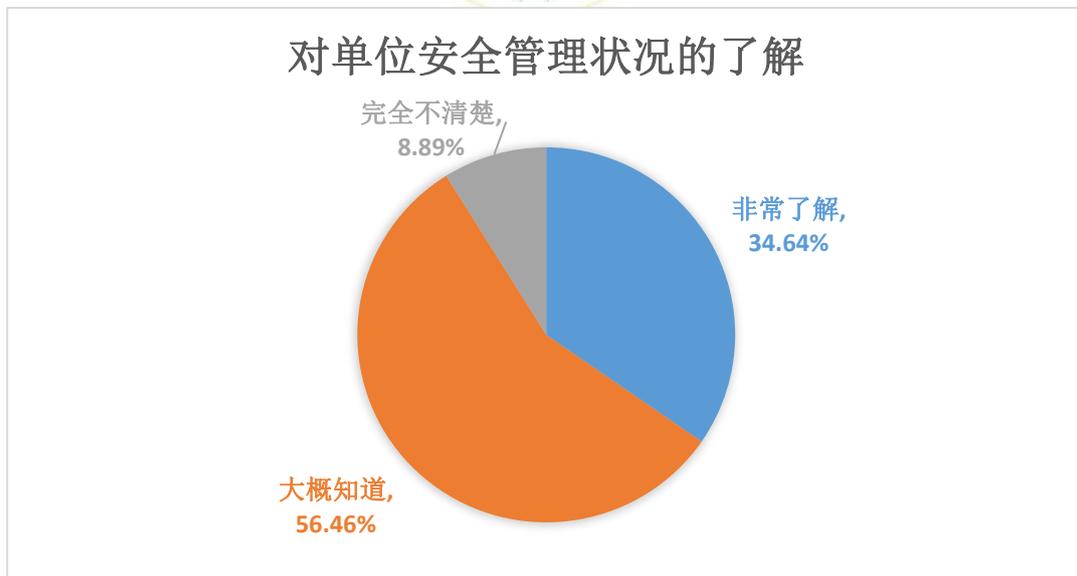


图表 4.1-2：网络安全对单位重要性认识

（图表数据来源：从业人员版等级保护实施与企业合规专题第 3 题：您认为网络安全对您所在单位来说重要吗？）

（3）所在单位安全状况

参与调查的从业人员对所在单位安全状况的了解方面，34.64%从业人员表示非常了解，56.46%从业人员表示大概知道，只有 8.89%从业人员表示完全不清楚。

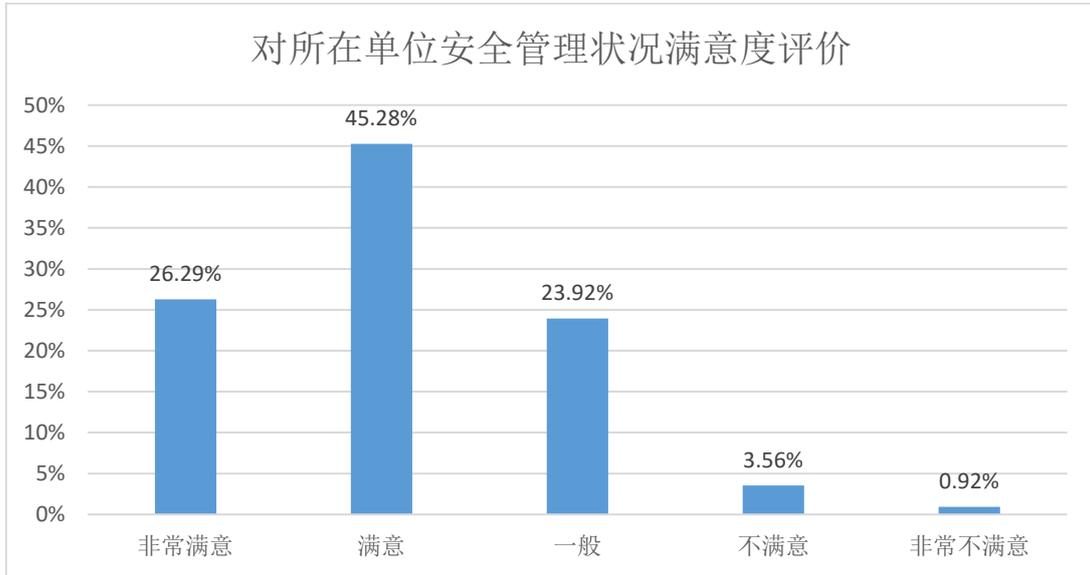


图表 4.1-3：所在单位网络安全状况的了解

（图表数据来源：从业人员版等级保护实施与企业合规专题第 4 题：您是否了解所在单位的网络安全现状？）

（3. 1）所在单位安全管理状况评价

参与调查的从业人员对所在单位安全管理状况满意度评价方面，71.57%从业人员表示满意或非常满意，其中 45.28%从业人员表示满意，26.29%从业人员表示非常满意。

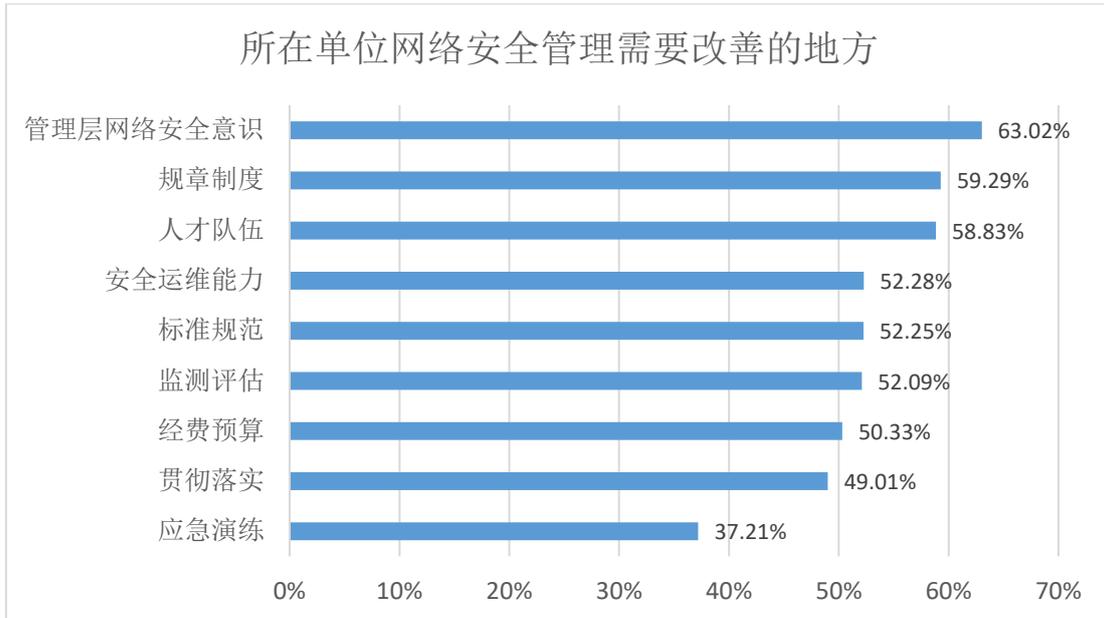


图表 4.1-4：所在单位网络安全管理状况满意度评价

（图表数据来源：从业人员版等级保护实施与企业合规专题第 4.1 题：您对所在单位的网络安全管理状况是否满意：）

（3. 2）所在单位安全管理存在问题

参与调查的从业人员对所在单位安全管理需要改善的地方主要方面，前五位分别是 1 管理层网络安全意识（63.02%）、2 规章制度（59.29%）、3 人才队伍（58.83%）、4 安全运维能力（52.28%）、标准规范（52.25%）。

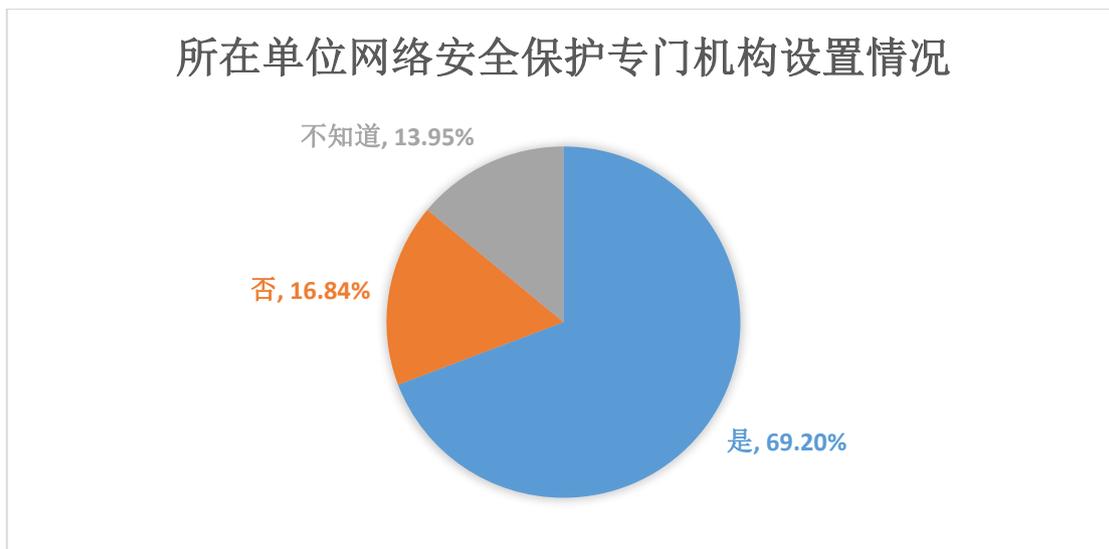


图表 4.1-5：所在单位网络安全管理需要改善的地方

（图表数据来源：从业人员版等级保护实施与企业合规专题第 4.2 题：您认为单位的网络安全管理在哪些方面需要改善？）

（4）网络安全保护专门机构设置

69.20%参与调查的从业人员所在单位设置了网络安全专门机构，16.84%的从业人员单位没有设置专门的网络安全保护机构。

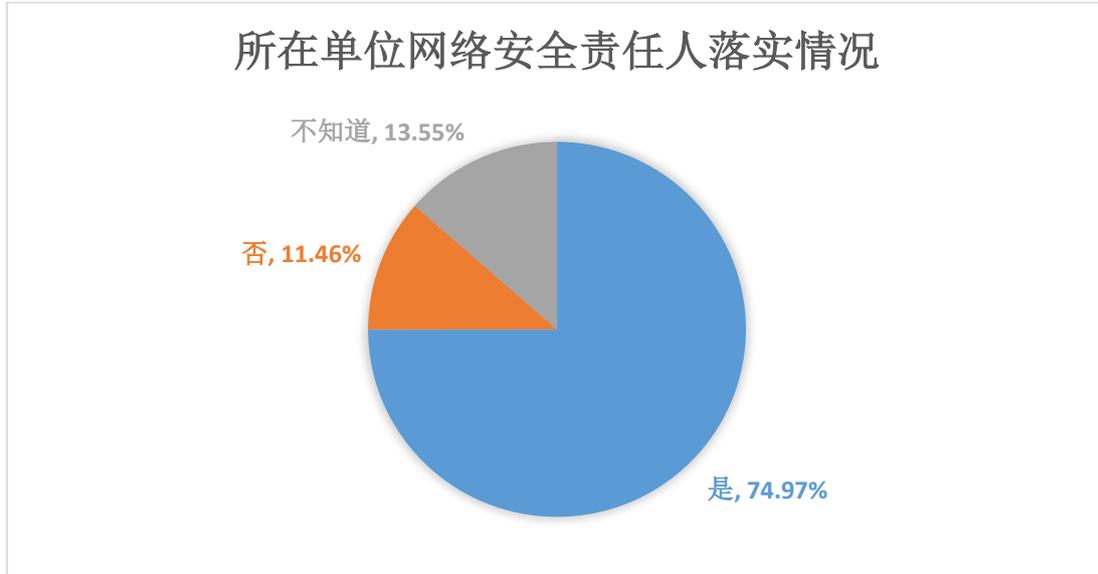


图表 4.1-6：所在单位网络安全保护专门机构设置情况

（图表数据来源：从业人员版等级保护实施与企业合规专题第 5 题：您所在单位是否有网络安全保护专门机构？）

（4. 1）单位网络安全责任人落实情况

74.97%参与调查的从业人员所在单位落实了网络安全责任人，11.46%的从业人员单位没有落实。

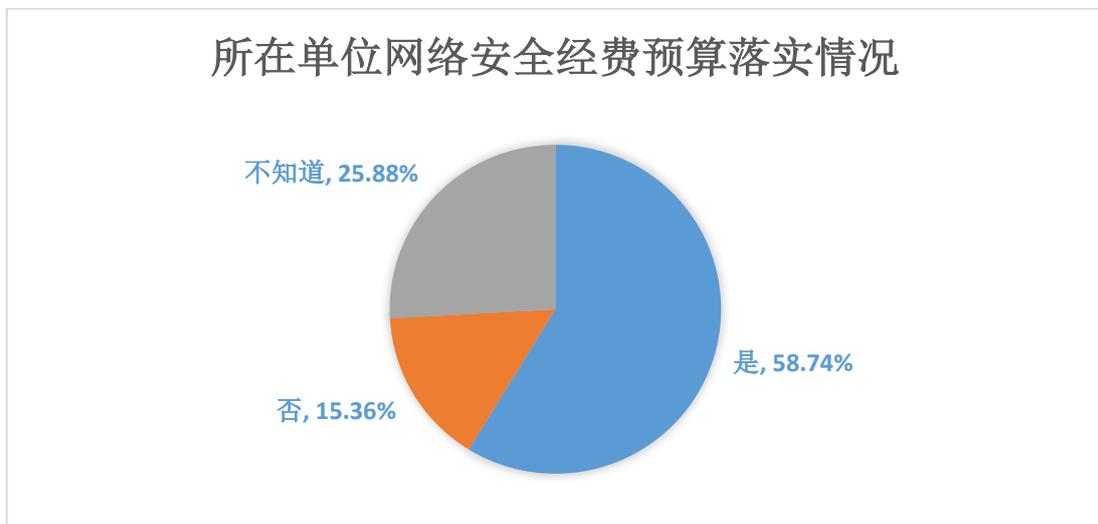


图表 4.1-7：所在单位网络安全责任人落实情况

（图表数据来源：从业人员版等级保护实施与企业合规专题第 5.1 题：您所在单位是否明确了网络安全责任人？）

（5）所在单位网络安全经费预算落实情况

58.74%参与调查的从业人员所在单位落实了网络安全经费预算，15.36%的从业人员单位没有落实。

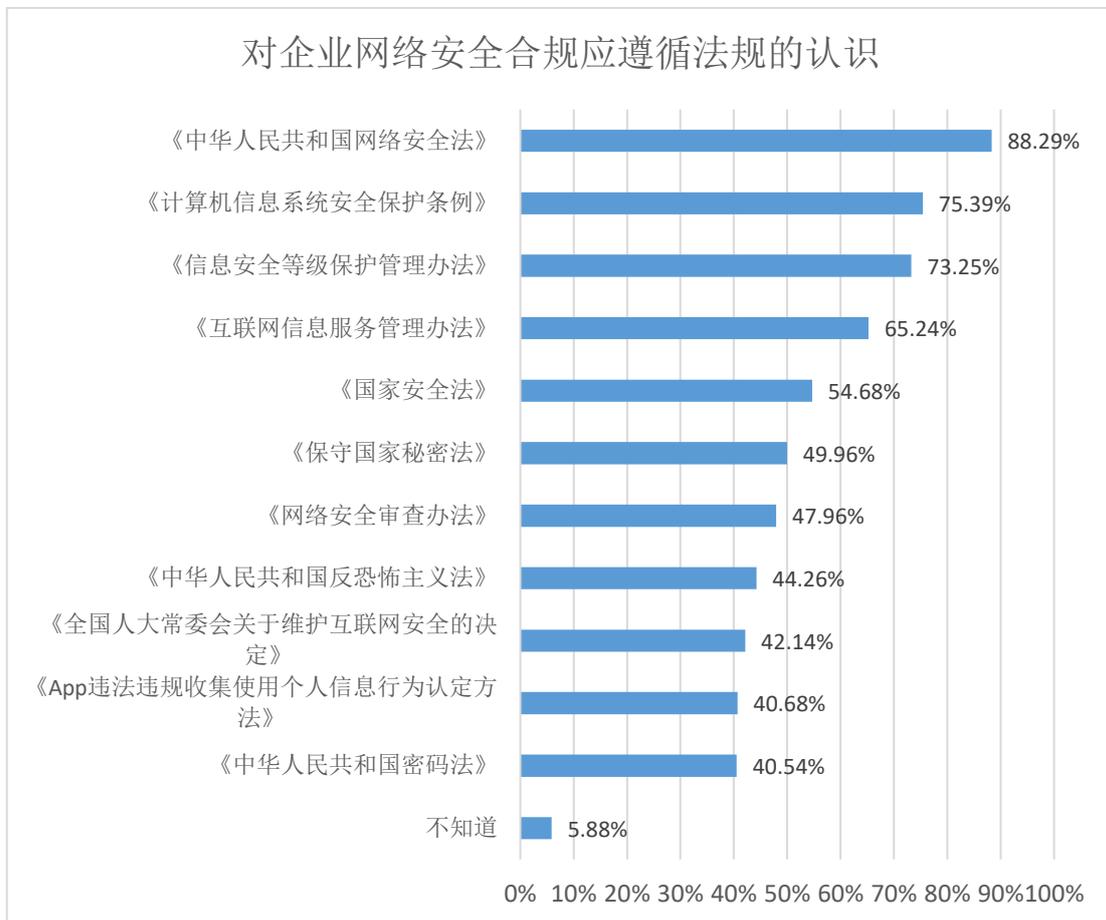


图表 4.1-8：所在单位网络安全经费预算落实情况

（图表数据来源：从业人员版等级保护实施与企业合规专题第 6 题：您所在单位是否有网络安全相关的经费预算？）

（6）对企业网络安全合规要求的认识

从业人员对企业网络安全合规要求认识有所提高，认为企业合规应遵循的法规认知度前 5 位分别为：1《中华人民共和国网络安全法》（88.29%）、2《计算机信息系统安全保护条例》（75.39%）、3《信息安全等级保护管理办法》（73.25%）、4《互联网信息服务管理办法》（65.24%）、5《国家安全法》（54.68%）。

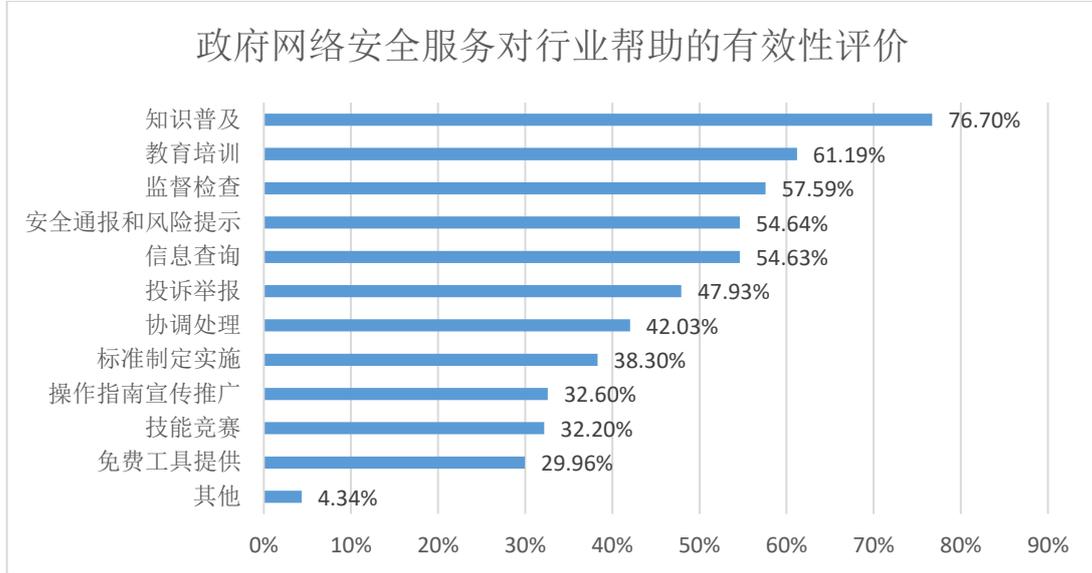


图表 4.1-9：对企业网络安全合规应遵循法规的认识

（图表数据来源：从业人员版等级保护实施与企业合规专题第 7 题：据您了解，您所在企业网络安全合规应遵循哪些要求？）

（7）政府部门提供的网络安全服务对行业的帮助

参与调查的从业人员对政府部门提供的网络安全服务对行业的帮助的有效性评价前 5 位分别为：1 知识普及（76.70%）、2 教育培训（61.19%）、3 监督检查（57.59%）、4 安全通报和风险提示（54.64%）、5 信息查询（54.63%）。大部分从业人员认为这些服务对行业有帮助。

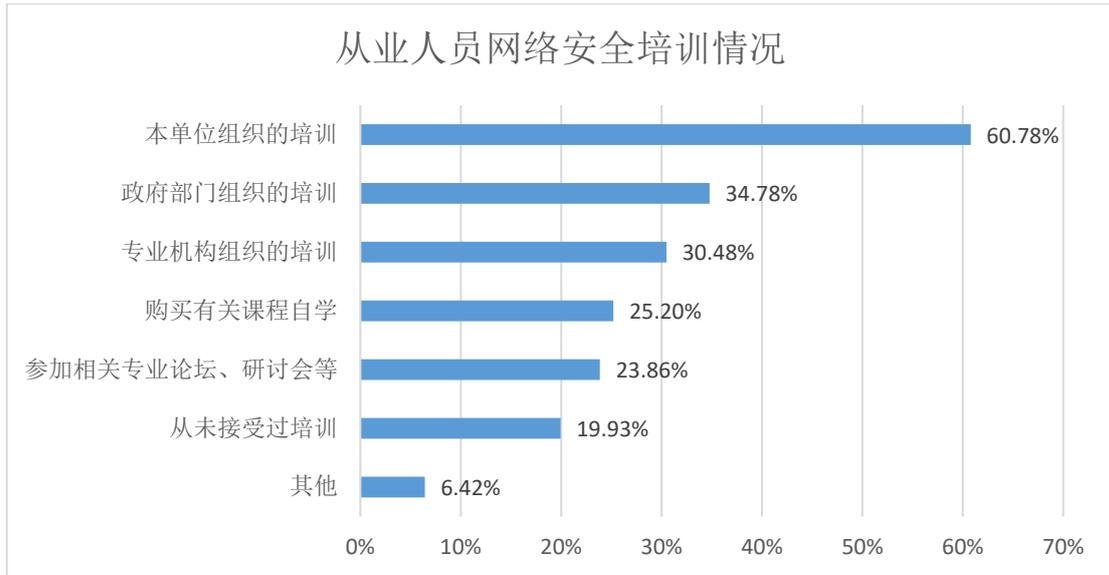


图表 4.1-10：政府网络安全服务对行业帮助的有效性评价

（图表数据来源：从业人员版等级保护实施与企业合规专题第 8 题：您认为政府部门提供的哪些网络安全服务对行业有较大帮助？）

（8）从业人员网络安全培训情况

参与调查的从业人员接受过网络安全培训最多前三位是本单位组织的培训（60.78%）、政府部门组织的培训（34.78%）、专业机构培训（30.48%）。但也有 19.93% 的从业人员从未接受过培训。

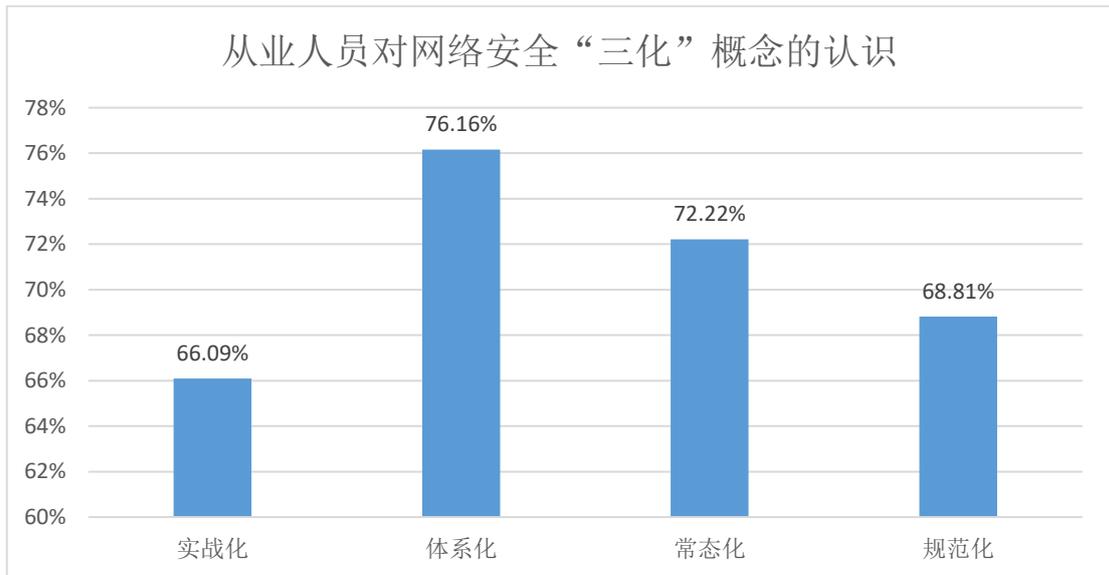


图表 4.1-11：从业人员网络安全培训情况

（图表数据来源：从业人员版等级保护实施与企业合规专题第 9 题：在过去的一年里，您接受过哪些网络安全培训？）

（8.1）对网络安全“三化”概念的认识

参与调查的从业人员对公安机关提出的网络安全“三化”认识度为体系化（76.16%）、常态化（72.22%）、实战化（66.09%）。选错规范化有 68.81%。显示相对比例的从业人员对网络安全“三化”概念的认识还比较模糊，有待进一步学习加深认识。

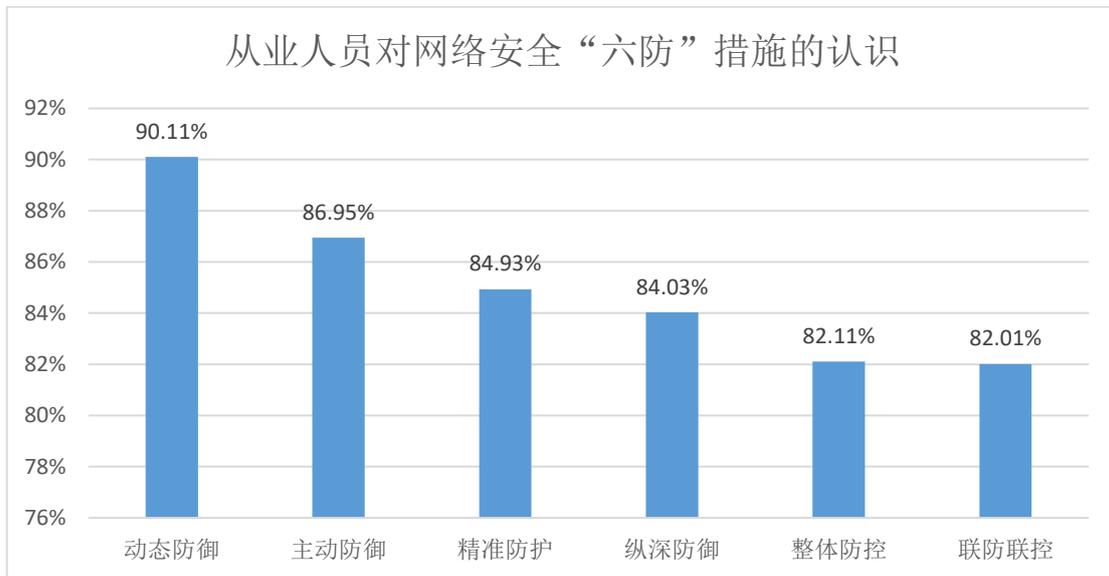


图表 4.1-12：从业人员对网络安全“三化”概念的认识

（图表数据来源：从业人员版等级保护实施与企业合规专题第 9.1 题：您知道公安机关提出的网络安全“三化”具体是指哪些方面？）

（8.2）对网络安全“六防”措施的认识

参与调查的从业人员对公安机关提出的网络安全“六防”措施的认识度为动态防御（90.11%）、主动防御（86.95%）、精准防护（84.93%）、纵深防御（84.03%）、整体防控（82.11%）、联防联控（82.01%）。显示大部分从业人员对网络安全“六防”措施的具体含义有一定的认识。

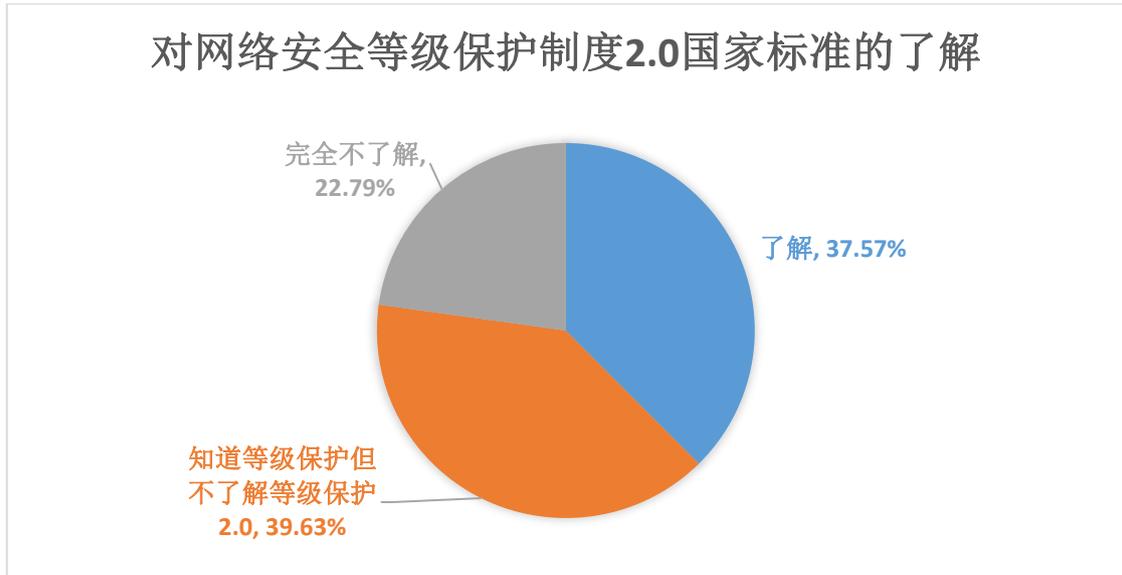


图表 4.1-13：从业人员对网络安全“六防”措施的认识

（图表数据来源：从业人员版等级保护实施与企业合规专题第 9.2 题：您知道公安机关提出的网络安全“六防”措施具体是什么？）

（9）网络安全等级保护制度的了解

参与调查的对网络安全等级保护制度了解方面，37.57%从业人员表示了解，39.63%从业人员表示知道等级保护，但不了解等级保护 2.0，完全不了解的占 22.79%。

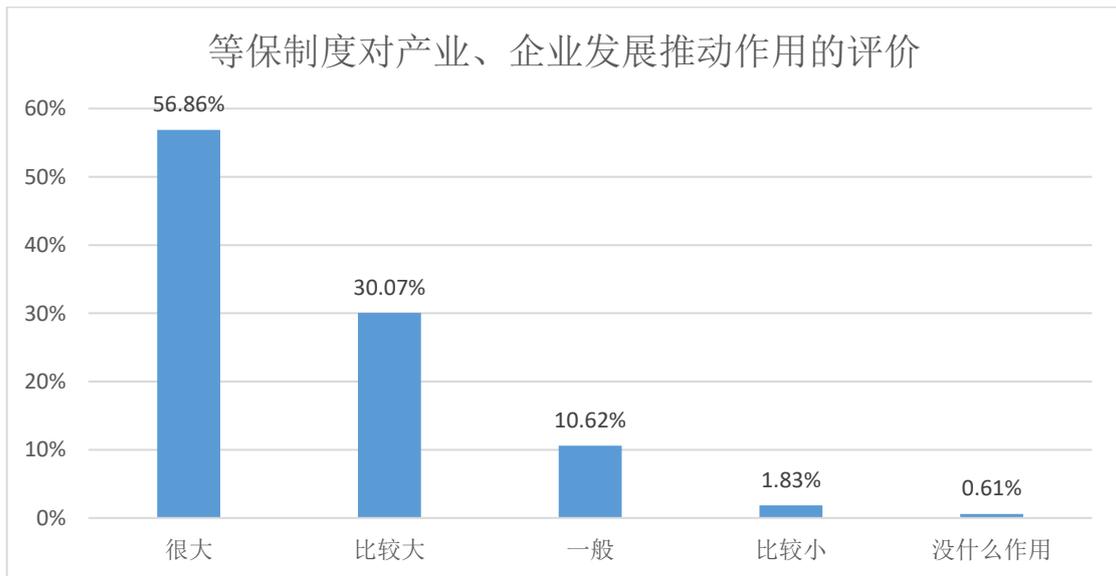


图表 4.1-14：对网络安全等级保护制度 2.0 标准的了解

（图表数据来源：从业人员版等级保护实施与企业合规专题第 10 题：您了解网络安全等级保护制度 2.0 国家标准的要求吗？）

（9.1）网络安全等级保护对产业、企业发展的推动作用

参与调查的网络安全等级保护对产业、企业发展的推动作用方面，56.86%从业人员表示作用很大，30.07%从业人员表示比较大，即 86.93%从业人员认为推动作用很大或比较大。



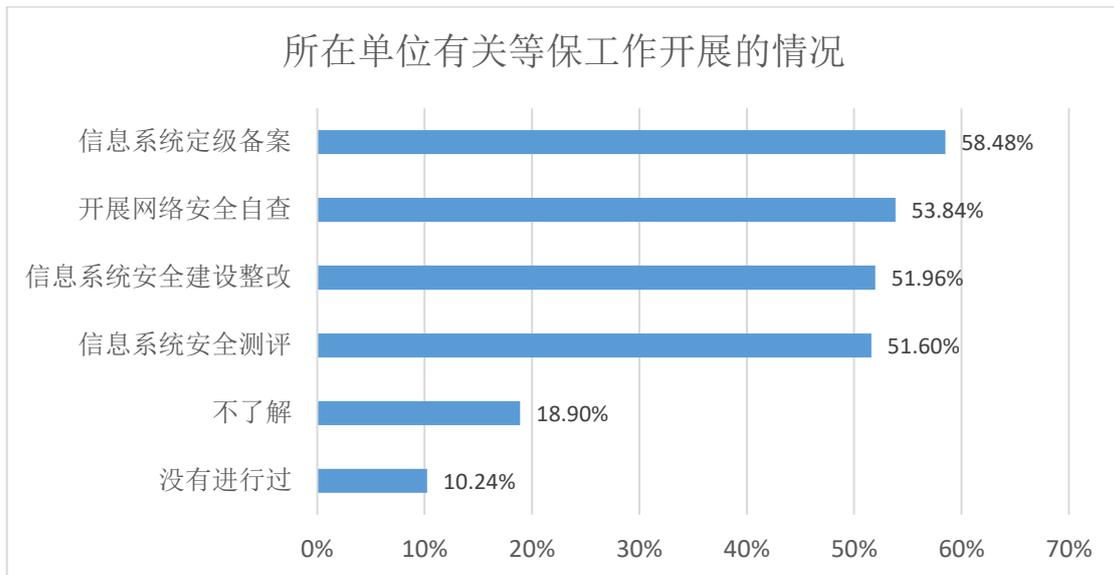
图表 4.1-15：等保制度对产业、企业发展推动作用的评价

（图表数据来源：从业人员版等级保护实施与企业合规专题第 10.1 题：您认为

网络安全等级保护对产业、企业发展的推动作用如何？）

（10）单位网络安全等级保护开展情况

参与调查的从业人员所在单位网络安全等级保护开展方面，58.48%从业人员所在单位做了信息系统定级备案，51.96%开展了信息系统安全建设整改，51.60%进行了信息系统安全测评，53.84%开展了网络安全自查，但仍有 10.24%从业人员所在单位没有进行过网络安全等级保护工作。

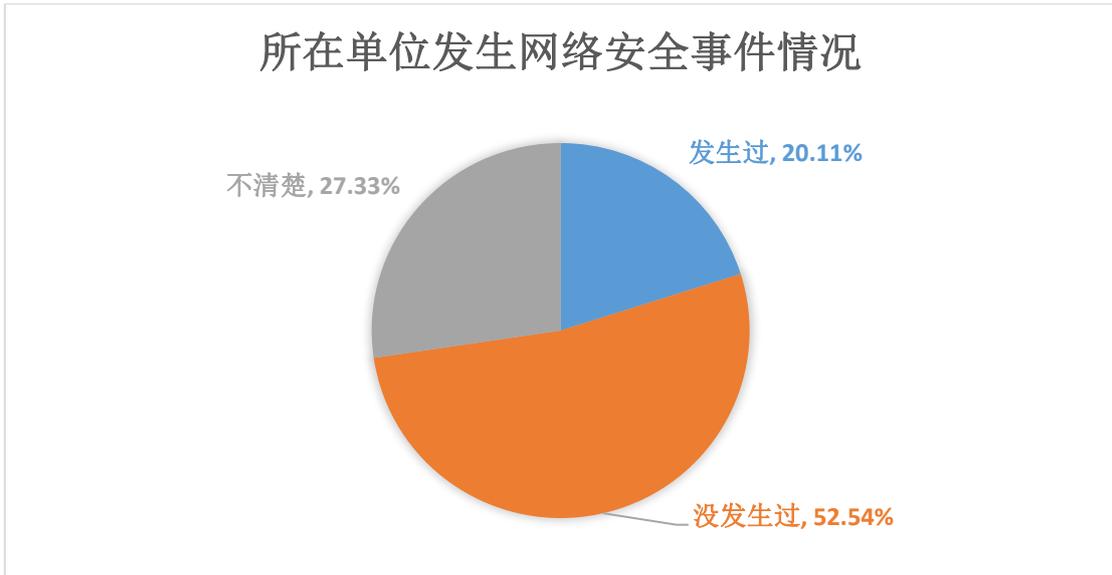


图表 4.1-16：所在单位网络安全等级保护开展情况

（图表数据来源：从业人员版等级保护实施与企业合规专题第 11 题：您所在单位是否进行过以下网络安全等级保护工作？）

（11）单位发生网络安全事件情况

从业人员所在单位发生网络安全事件方面，20.11%参与调查的从业人员所在单位发生过网络安全事件，52.54%没有发生过网络安全事件，还有 27.33%从业人员表示不清楚。

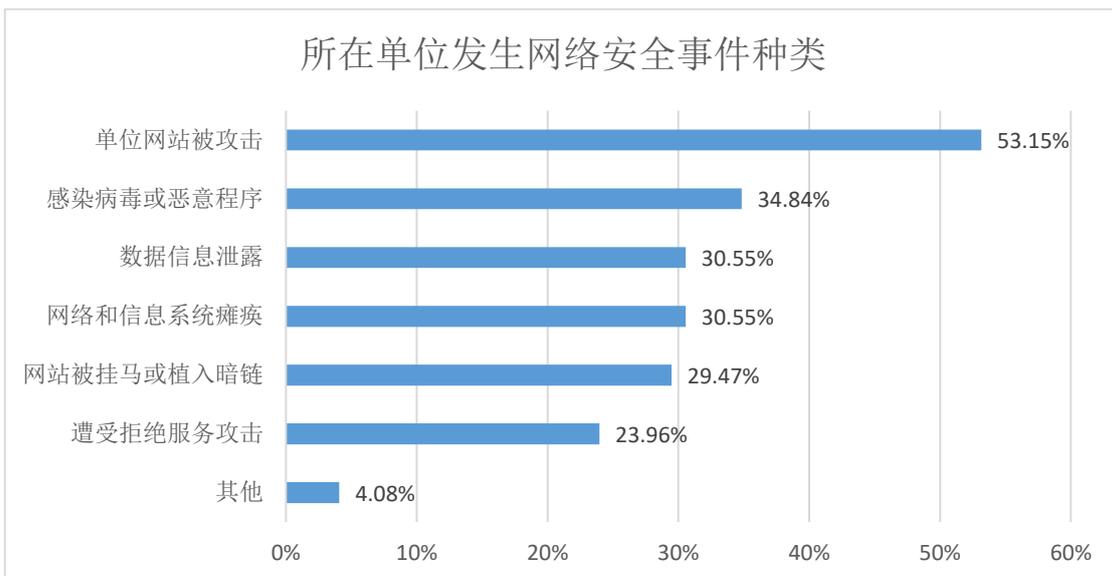


图表 4.1-17：所在单位发生网络安全事件情况

（图表数据来源：从业人员版等级保护实施与企业合规专题第 12 题：您所在单位发生过网络安全事件吗？）

（11. 1）单位发生网络安全事件种类

对所在单位发生的网络安全事件方面，在发生过安全事件的单位中 53.15% 参与调查的从业人员所在单位发生过单位网站被攻击，34.84% 从业人员单位发生过感染病毒或恶意程序，30.55% 发生过数据信息泄露、30.55% 发生过网络和信息系统瘫痪。

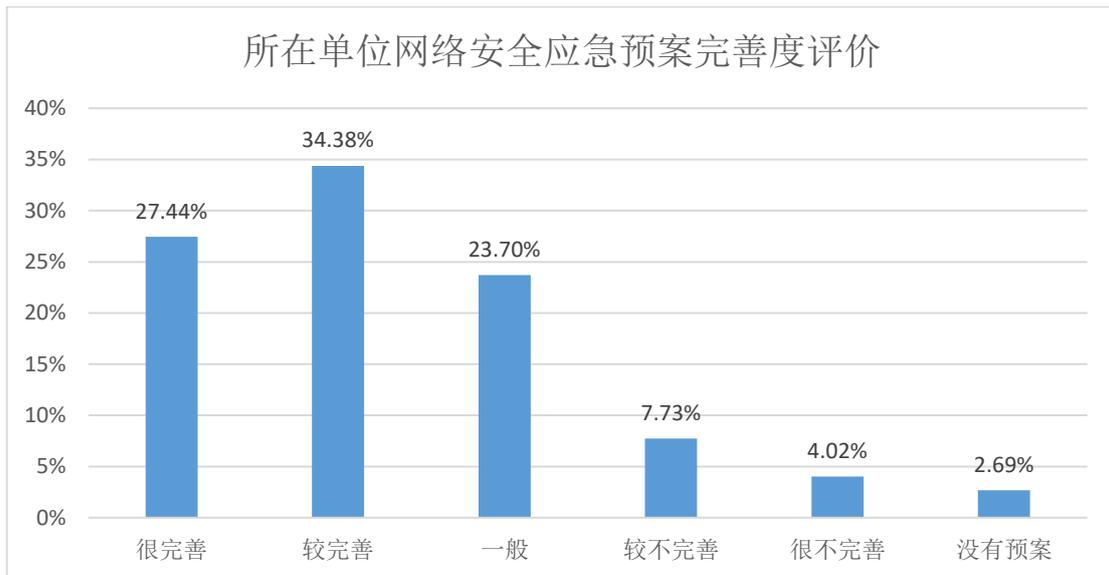


图表 4.1-18：所在单位发生网络安全事件种类

（图表数据来源：从业人员版等级保护实施与企业合规专题第 12.1 题：发生了什么事情？）（本题回答人数为 2861。）

（11. 2）单位网络安全应急预案完善度

对所在单位网络安全应急预案建设方面，27.44%参与调查的从业人员认为很完善，34.38%认为较完善、23.70%认为一般。即 61.82%从业人员认为单位网络安全应急预案完善或较为完善。

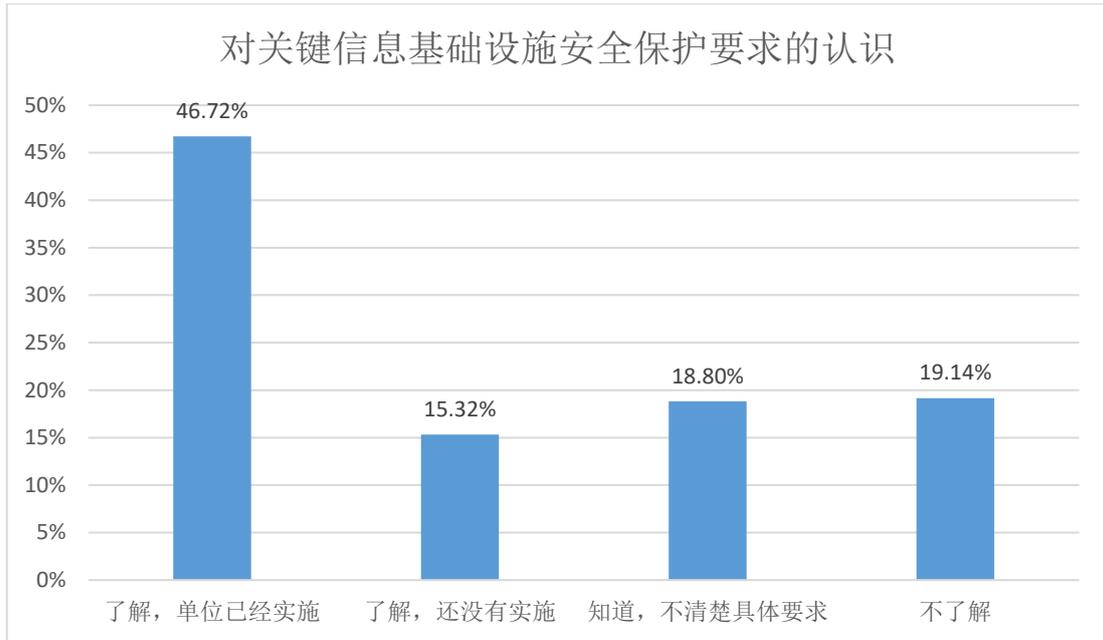


图表 4.1-19：单位网络安全应急预案完善度评价

（图表数据来源：从业人员版等级保护实施与企业合规专题第 12.2 题：您认为所在单位目前针对网络安全事件的应急预案是否完善？）（本题回答人数为 2861。）

（12）对关键信息基础设施保护要求的认识

对关键信息基础设施保护要求的认识方面，46.72%参与调查的从业人员认为了解而且单位已经实施，15.32%从业人员认为了解但还没有实施，18.80%认为知道但不清楚具体要求，19.69%认为不了解。显示关键信息基础设施保护已经被大部分从业人员（80.84%）了解，而且在部分从业人员（46.72%）所在单位已经实施实施，但仍有相当比例的从业人员（34.12%）还没有开始实施或不知到要求。显示关键信息基础设施保护要求的宣传取得良好的效果，但具体的实施规范和细则仍需要进一步细化和贯彻落实。

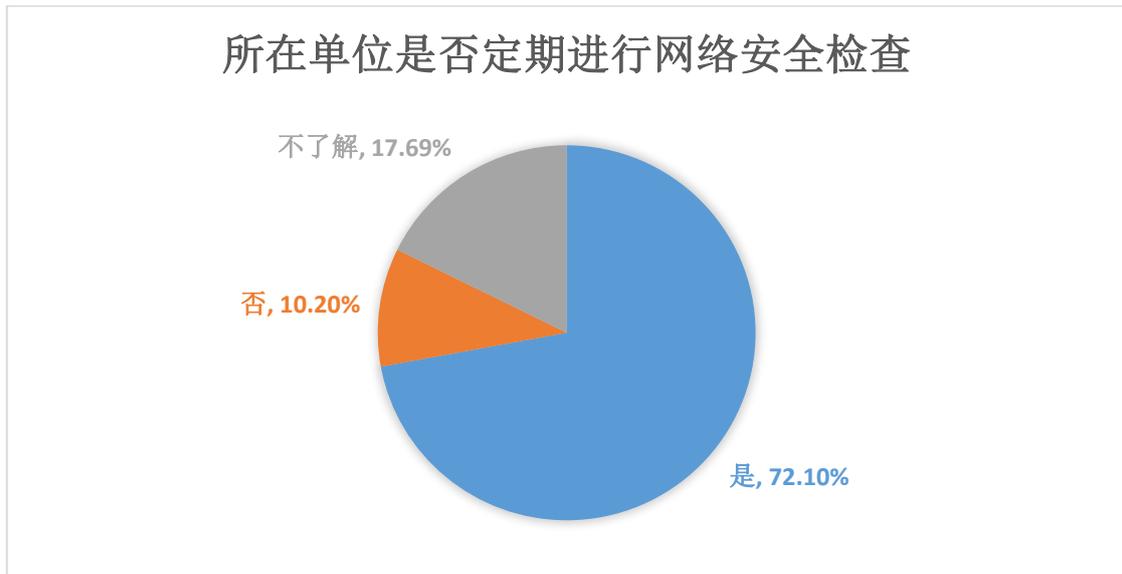


图表 4.1-20：对关键信息基础设施安全保护要求的认识

（图表数据来源：从业人员版等级保护实施与企业合规专题第 13 题：您对关键信息基础设施安全保护要求了解吗？）

（13）网络安全检查落实情况

对所在单位网络安全检查措施落实情况，72.10%参与调查的从业人员表示所在单位有定期进行网络安全检查，10.20%从业人员所在单位没有定期进行网络安全检查，17.69%表示不了解。



图表 4.1-21：所在单位是否定期进行网络安全检查

（图表数据来源：从业人员版等级保护实施与企业合规专题第 14 题：您所在单位是否定期对重要的信息系统/业务系统进行安全检查？）

网络安全感满意度调查



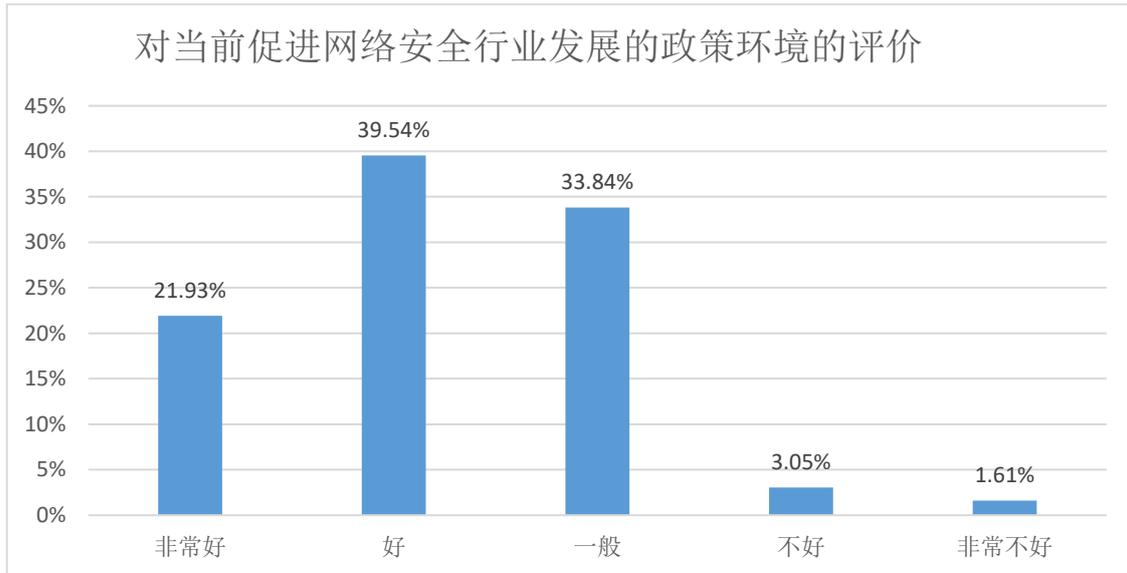
广东新兴国家网络安全和信息化发展研究院

4.2 行业发展与行业生态建设

参与本专题答题的从业人员数为 12913。

（1）行业发展的政策环境

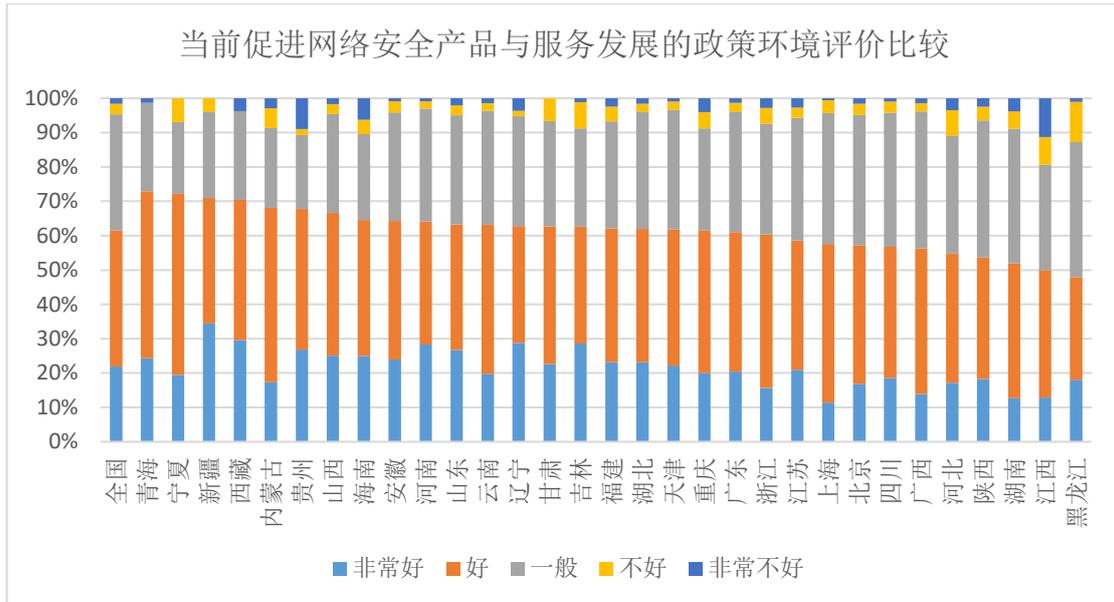
参与调查的从业人员对当前促进网络安全产品与服务发展的政策环境评价为：21.93%从业人员认为非常好，39.54%认为好，33.84%认为一般，持肯定态度的占大部分（61.47%）。但也有三分之一的从业人员评价不高。



图表 4.2-1：对当前促进网络安全行业发展的政策环境的评价

（图表数据来源：从业人员版行业发展与生态建设专题第 1 题：您认为当前促进网络安全产品与服务发展的政策环境如何？）

全国各地区比较，评价比较高的有青海、宁夏、新疆、内蒙古、贵州、山西等省，四川、广西、河北、陕西、湖南、江西和黑龙江的从业人员的评价较低。

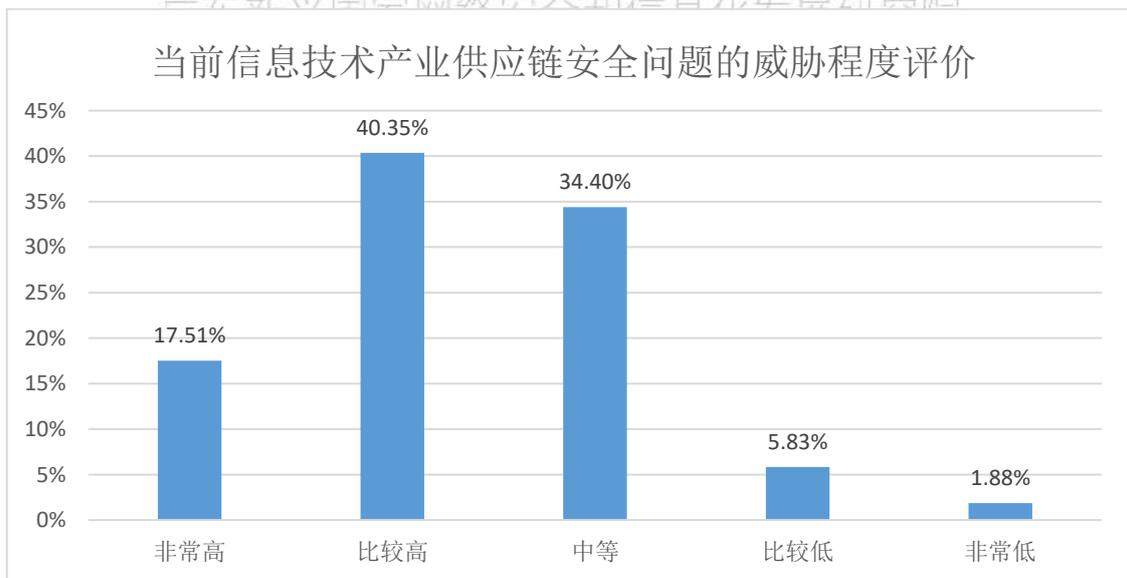


图表 4.2-2：当前促进网络安全产品与服务发展的政策环境评价比较

（图表数据来源：从业人员版行业发展与生态建设专题第 1 题：1.您认为当前促进网络安全产品与服务发展的政策环境如何？）

(2) 信息技术产业供应链安全威胁

参与调查的从业人员对信息技术产业供应链安全威胁评价为：17.51%从业人员认为威胁非常高，40.35%从业人员认为比较高，34.40%认为中等，持威胁比较高和非常高看法的占大部分（57.86%）。显示信息技术产业供应链安全的威胁是比较高的。

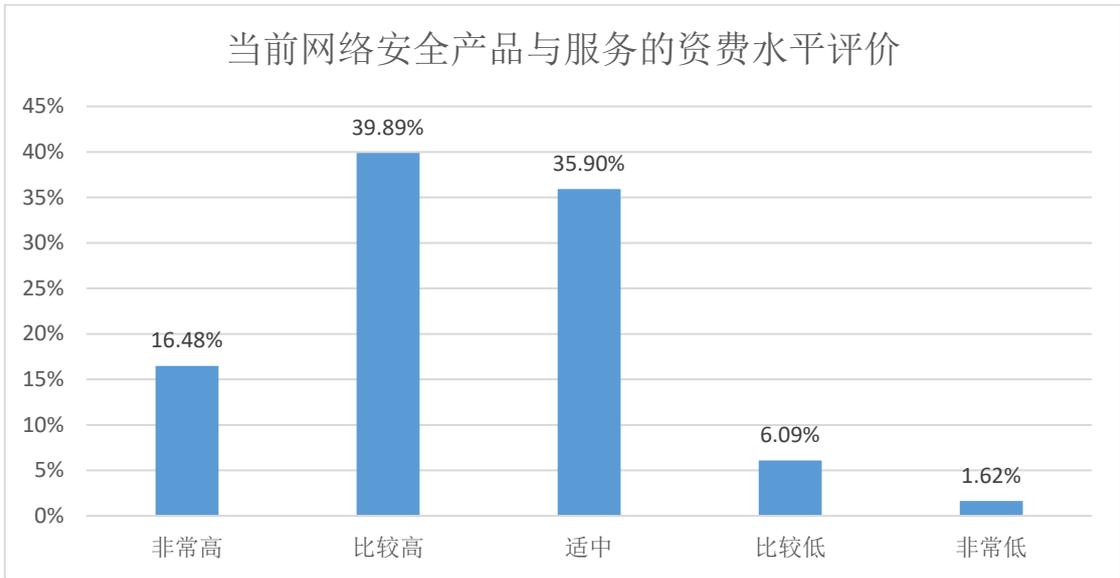


图表 4.2-3：当前信息技术产业供应链安全问题的威胁

（图表数据来源：从业人员版行业发展与生态建设专题第 4 题：您认为当前信息技术产业供应链安全问题的威胁如何？）

（5）当前网络安全产品与服务的资费水平

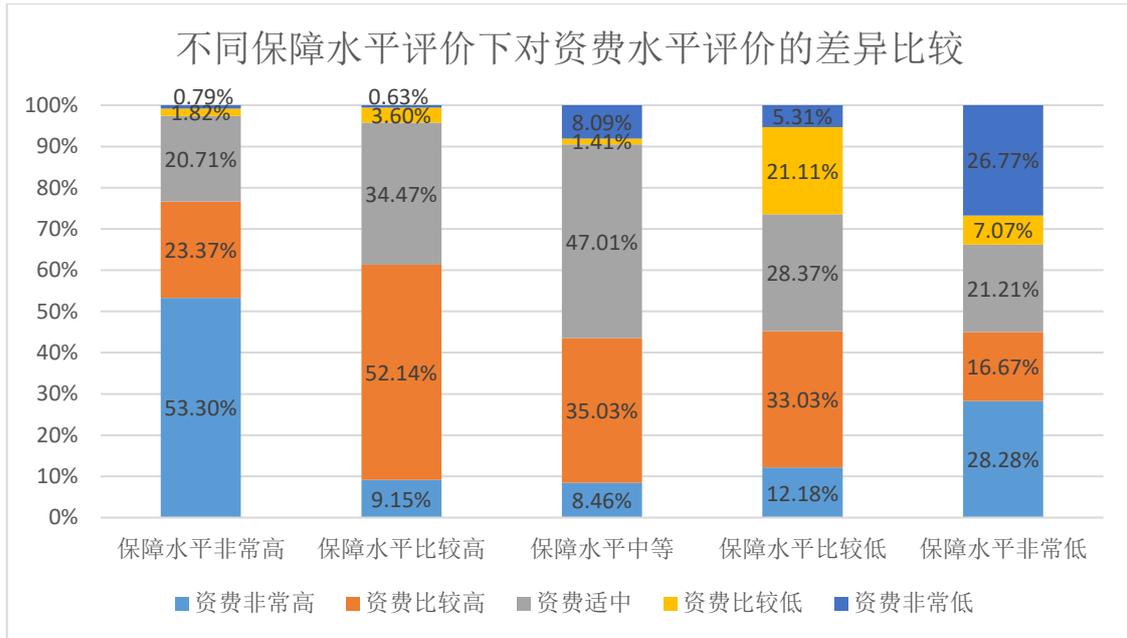
参与调查的从业人员对当前网络安全产品与服务的资费水平评价为：**16.48%**从业人员认为非常高，**39.89%**从业人员认为比较高，**35.90%**认为适中，持比较高和非常高看法的占大部分（**56.37%**）。显示网络安全行业产品和服务收费是比较高的。



图表 4.2-4：当前网络安全产品与服务的资费水平

（图表数据来源：从业人员版行业发展与生态建设专题第 5 题：您认为当前网络安全产品与服务的资费水平如何？）

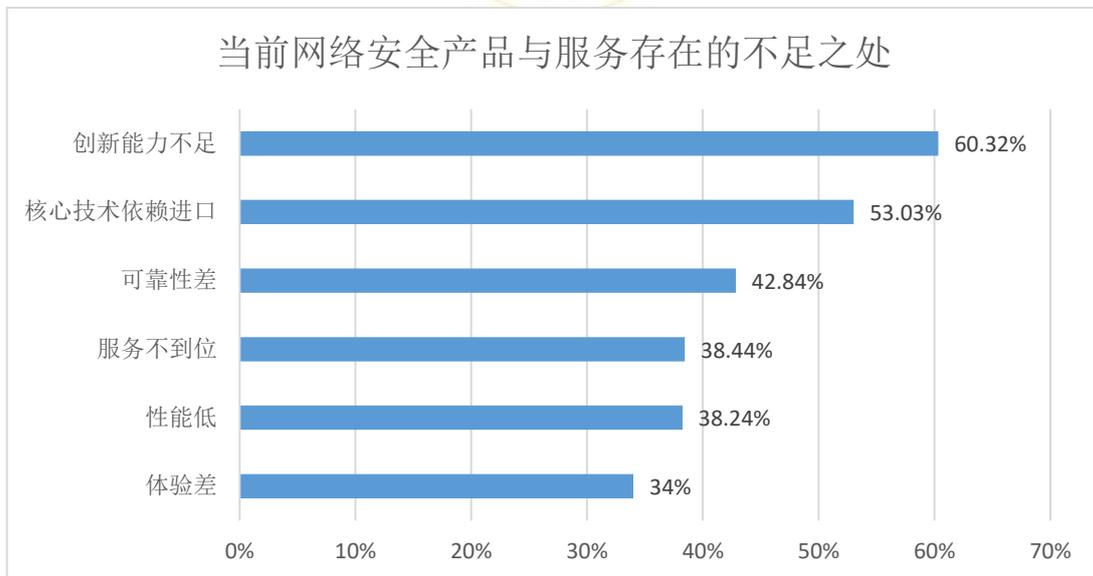
保障水平和资费高低有没有关系，从下图比较可以看出，认为保障水平非常高和比较高的从业人员中认为资费较高的人比例较高，而认为保障水平比较低的人群中认为资费水平低的比例较高。显示对服务水平满意的人通常对价格不满，对价格满意的人对服务水平不满意。能做到价廉物美的不多。



图表 4.2-5：不同保障水平与服务的资费水平评价对比

（6）当前网络安全产品与服务存在问题

参与调查的从业人员对当前网络安全产品与服务存在问题看法为：排前 5 位的为：1 创新能力不足（60.32%）、2 核心技术依赖进口（53.03%）、3 可靠性差（42.84%）、4 服务不到位（38.44%）、5 性能低（38.24%）。

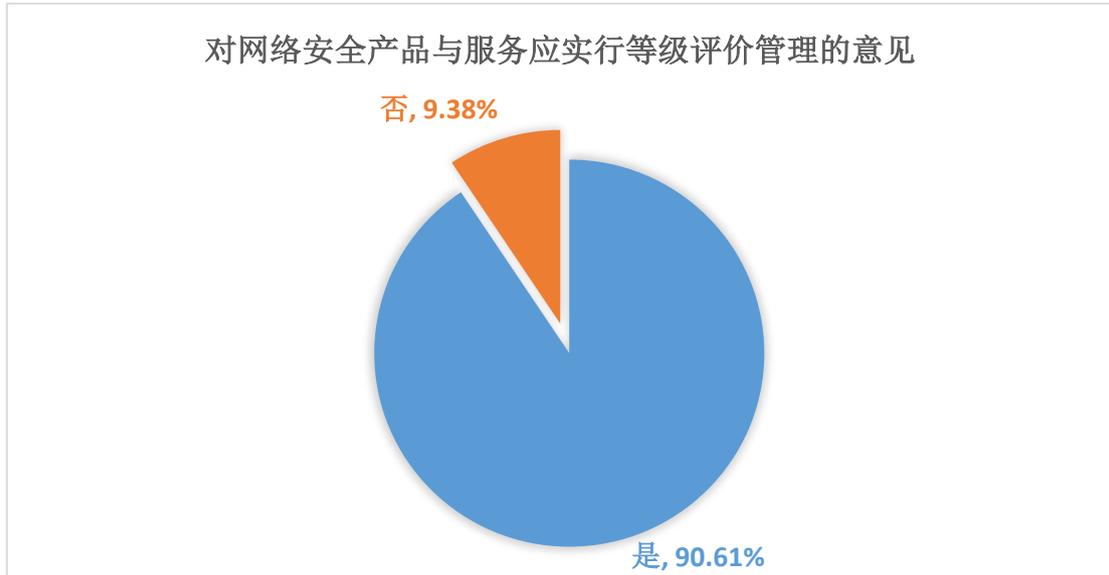


图表 4.2-6：当前网络安全产品与服务存在的不足之处

（图表数据来源：从业人员版行业发展与生态建设专题第 6 题：您认为当前网络安全产品与服务存在的不足之处是？）

（7）对当前网络安全产品与服务实行等级管理看法

参与调查的从业人员对当前网络安全产品与服务实行等级管理看法为：绝大部分 90.61%从业人员认为应该实行等级管理，小部分 9.38%认为不应实行等级管理。

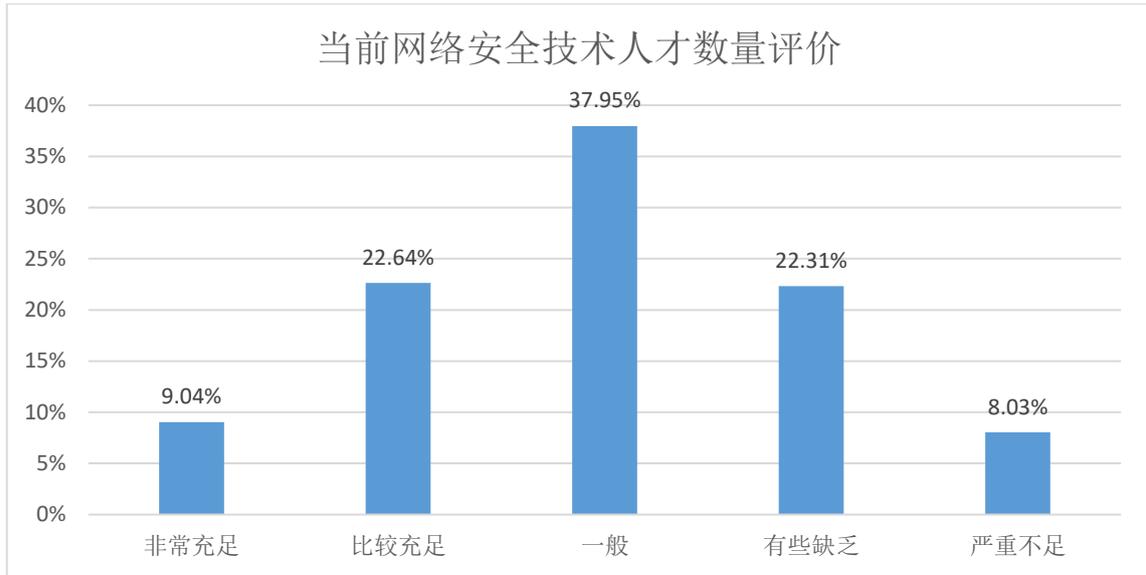


图表 4.2-7：对网络安全产品与服务实行等级评价管理的意见

（图表数据来源：从业人员版行业发展与生态建设专题第 7 题：您认为当前网络安全产品与服务是否应该实行等级评价管理？）

（8）当前网络安全技术人才数量评价

参与调查的从业人员对当前网络安全技术人才数量评价呈持平的状态，认为一般最多，占 37.95%，认为比较充足的 22.64%和认为有效缺乏的 22.31%差不多，认为非常充足的 9.04%和认为严重不足的 8.03%差不多。技术人才问题不仅是数量问题，还有质量和结构的问题。

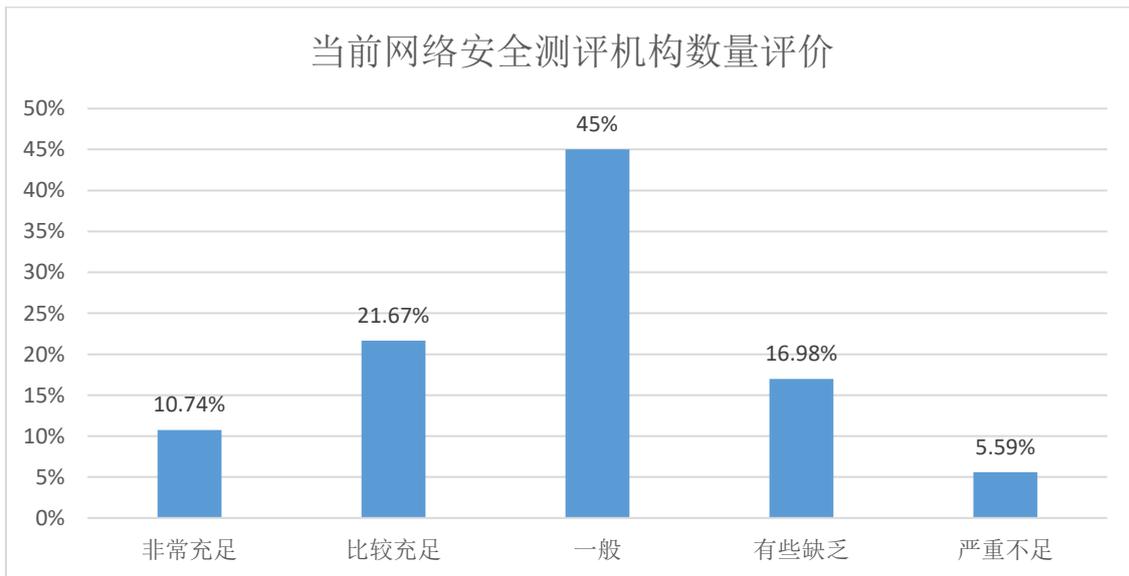


图表 4.2-8：当前网络安全技术人才数量评价

（图表数据来源：从业人员版行业发展与生态建设专题第 8 题：您认为当前网络安全技术人才数量如何？）

（9）当前网络安全测评机构数量评价

参与调查的从业人员中对当前网络安全测评机构数量评价方面，45%的从业人员网民认为数量一般。21.67%认为数量比较充足，16.98%认为有些缺乏，10.74%认为非常充足，5.59%认为严重不足。



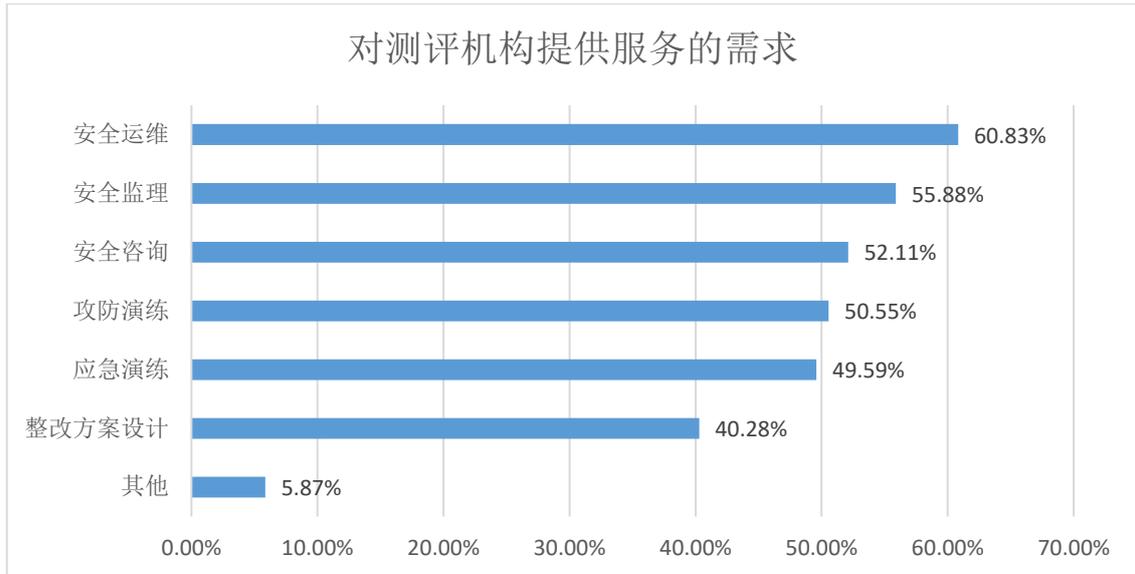
图表 4.2-9：当前网络安全测评机构数量评价

（图表数据来源：从业人员版行业发展与生态建设专题第 9 题：您认为当前网络

安全测评机构数量如何？）

（10）对测评机构提供服务的需求

参与调查的从业人员对测评机构提供服务的需求排前 5 位是：1 安全运维 60.83%，2 安全监理 55.88%，3 安全咨询 52.11%，4 攻防演练 50.55%，5 紧急演练 49.59%。



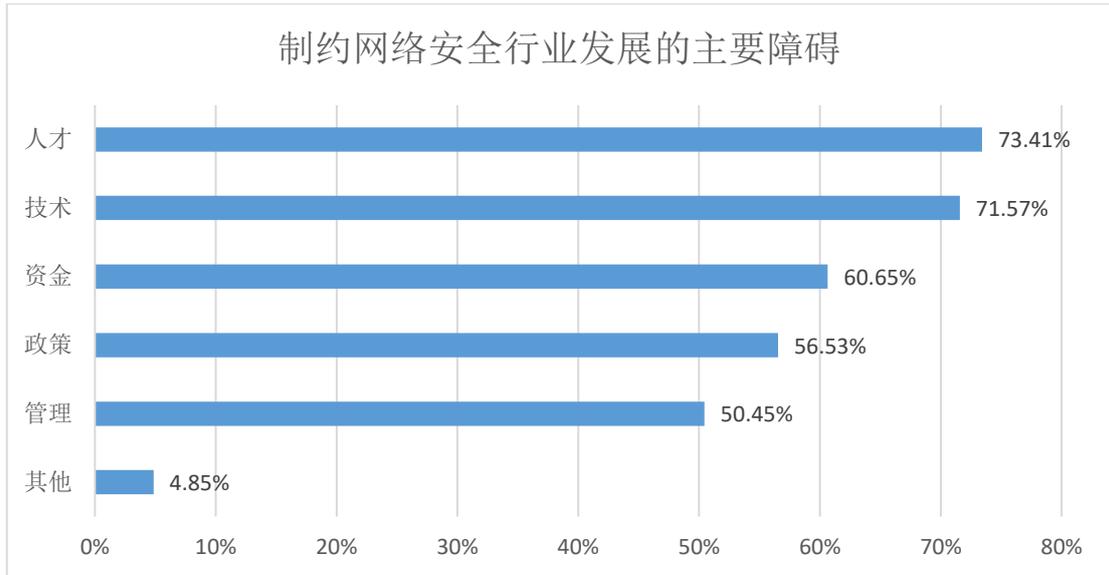
图表 4.2-10：对测评机构提供服务的需求

（图表数据来源：从业人员版行业发展与生态建设专题第 10 题：您所在单位还需要测评机构提供哪些服务？）

广东新兴国家网络安全和信息化发展研究院

（11）制约网络安全行业发展的主要障碍

从业人员制约网络安全行业发展的主要障碍排前 3 位是：1 人才 73.41%，2 技术 71.57%，3 资金 60.65%。

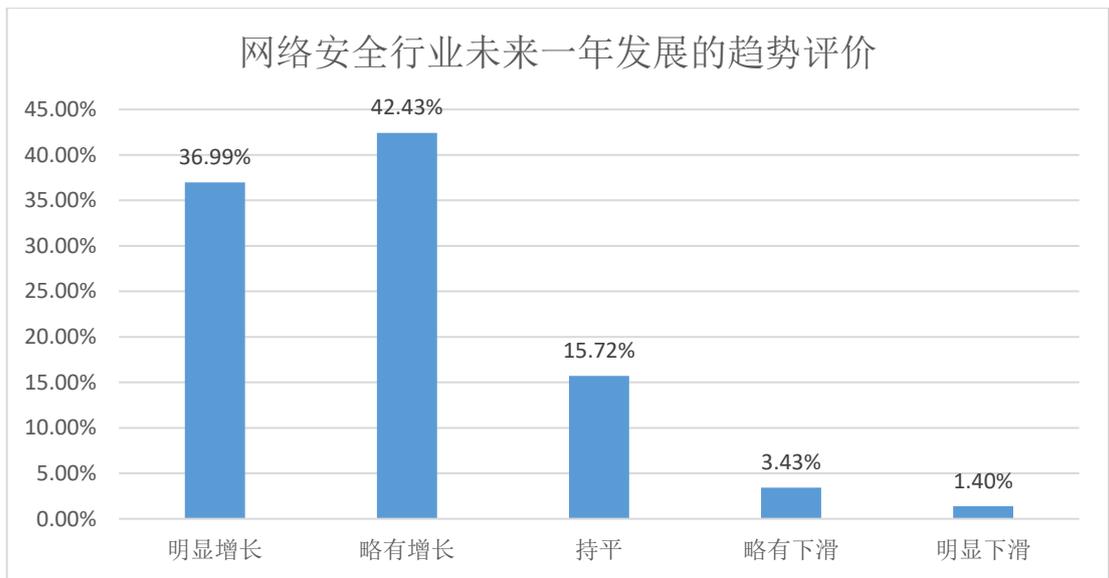


图表 4.2-11：制约网络安全行业发展的主要障碍

（图表数据来源：从业人员版行业发展与生态建设专题第 11 题：您认为制约网络安全行业发展的主要障碍是什么？）

（12）网络安全行业未来一年发展的趋势评价

参与调查的从业人员对网络安全行业未来一年发展的趋势评价：36.99%认为明显增长，42.43%认为略有增长，即接近八成（79.42%）从业人员认为未来有增长。



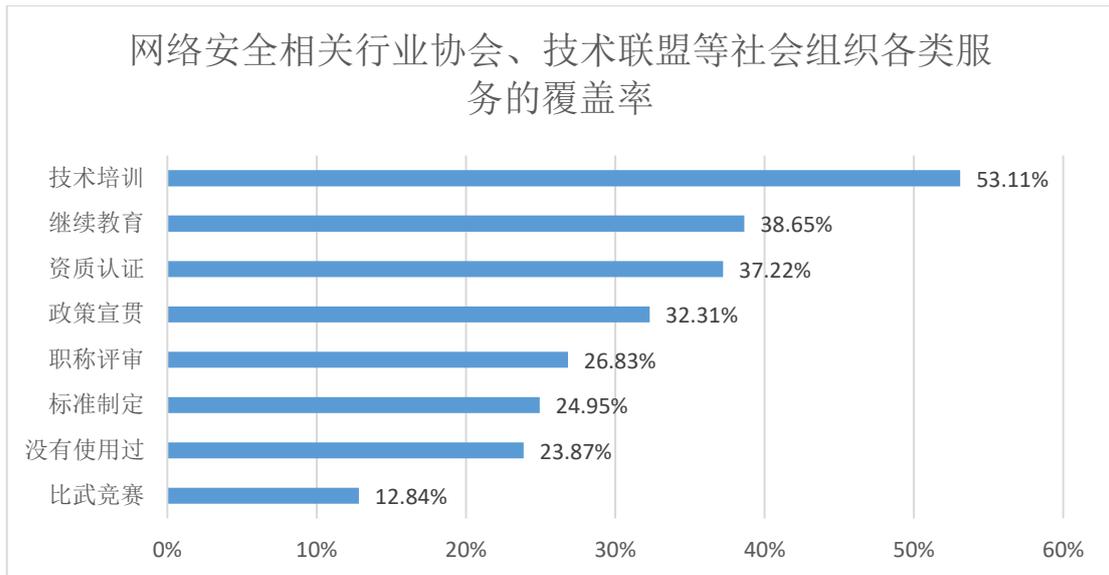
图表 4.2-12：网络安全行业未来一年发展的趋势评价

（图表数据来源：从业人员版行业发展与生态建设专题第 12 题：您认为网络安

全行业未来一年发展的趋势如何？）

（13）网络安全行业协会等社会组织服务情况

参与调查的从业人员对网络安全行业协会等社会组织服务情况评价：53.11%从业人员使用过技术培训服务，38.65%使用过继续教育服务，37.22%使用过资质认证服务，32.31%使用过政策宣贯服务，显示技术培训是覆盖率最高的服务，其它服务还有一定的提升空间。



图表 4.2-13：网络安全行业协会等社会组织服务情况

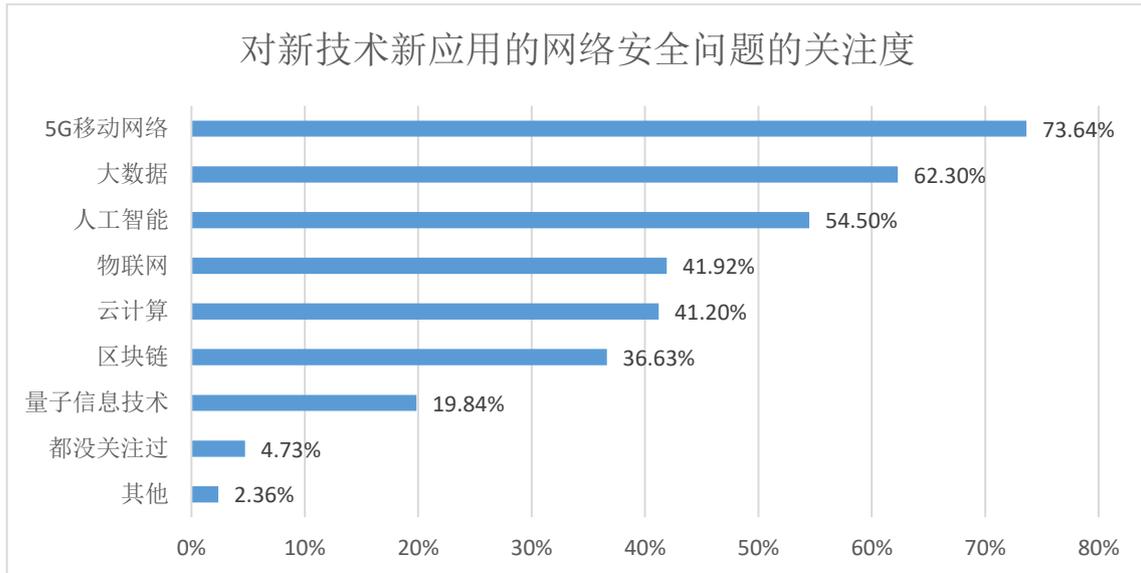
（图表数据来源：从业人员版行业发展与生态建设专题第 13 题：您使用过哪些由网络安全相关行业协会、技术联盟等社会组织提供的服务？）

4.3 新技术应用前景与制约因素

参与本专题答题的从业人员人数为 18663。

（1）对新技术新应用的网络安全问题的关注度

从业人员对新技术新应用的网络安全问题的关注度排列前 5 位为：5G 移动网络（73.64%）、大数据（62.30%）、人工智能（54.50%）、物联网（41.92%）、云计算（41.20%）。数据显示从业人员对新技术的网络安全问题是比较关注的。



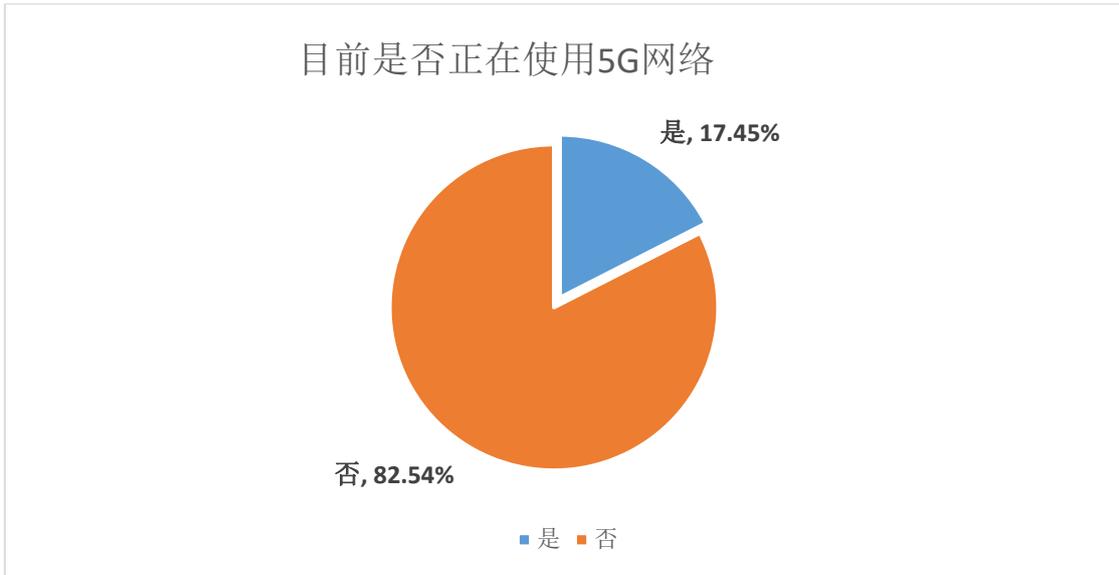
图表 4.3-1：对新技术新应用的网络安全问题的关注度

（图表数据来源：从业人员版新技术应用与网络安全专题第 1 题：您关注过以下哪项新技术新应用的网络安全问题？）

广东新兴国家网络安全和信息化发展研究院

（2）从业人员 5G 网络使用情况

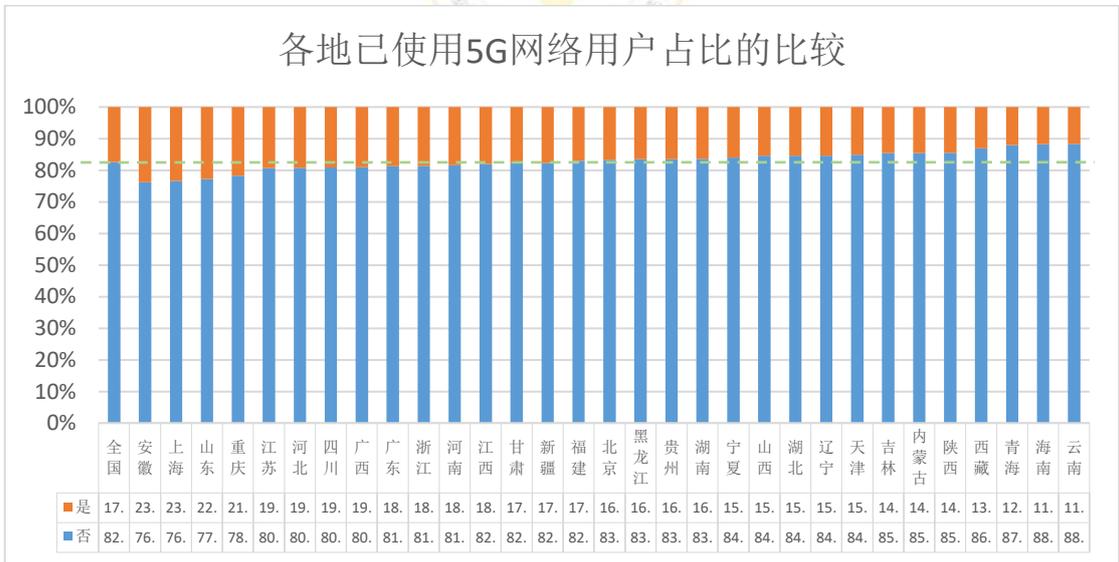
从业人员 5G 网络使用情况：17.45%从业人员已经使用 5G 网络，82.54%从业人员没有使用 5G 网络，显示 5G 网络应用刚起步，从业人员中使用率不算高。



图表 4.3-2：从业人员 5G 网络使用率

（图表数据来源：从业人员版新技术应用与网络安全专题第 2 题：您目前是否正在使用 5G 网络？）

5G 用户占比较高地区有：安徽、上海、山东、重庆、江苏、河北、四川、广西、广东、浙江等地，主要分布在东部和沿海。占比较低的有云南、海南、青海、西藏、陕西、内蒙古、吉林、天津、辽宁等地。主要分布在西南、东北和华北。

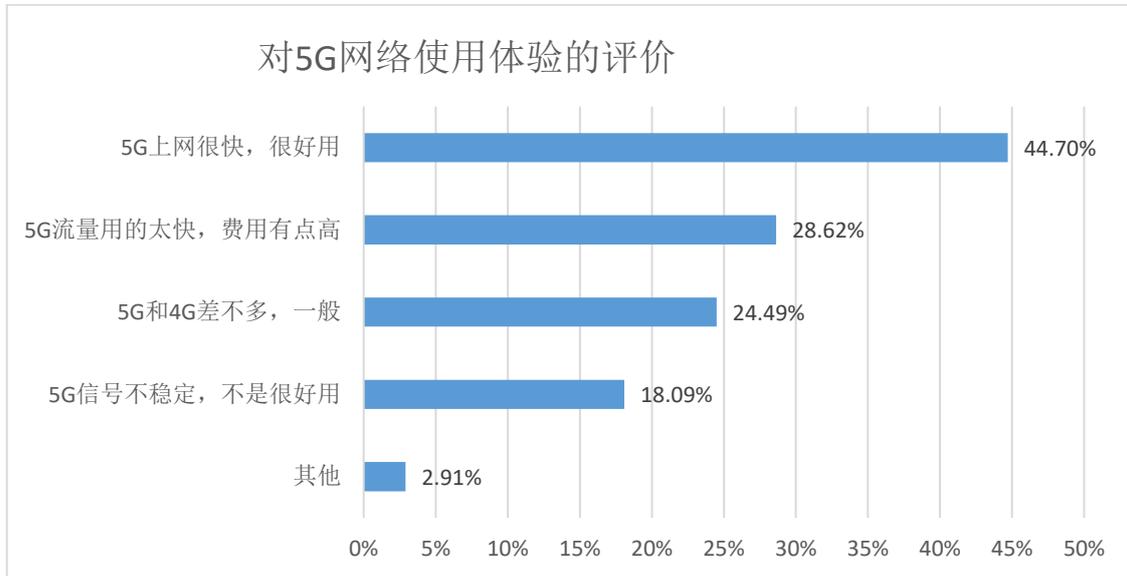


图表 4.3-3：各地从业人员 5G 网络使用率

(2. 1) 对 5G 网络使用体验的评价

参与调查的从业人员对 5G 网络使用体验评价：44.70%从业人员认为 5G 上

网很快很好用；28.62%从业人员认为 5G 流量用的太快，费用有点高；24.49%认为 5G 和 4G 差不多，感觉一般；还用 18.09%认为 5G 信号不稳定不是很好用。

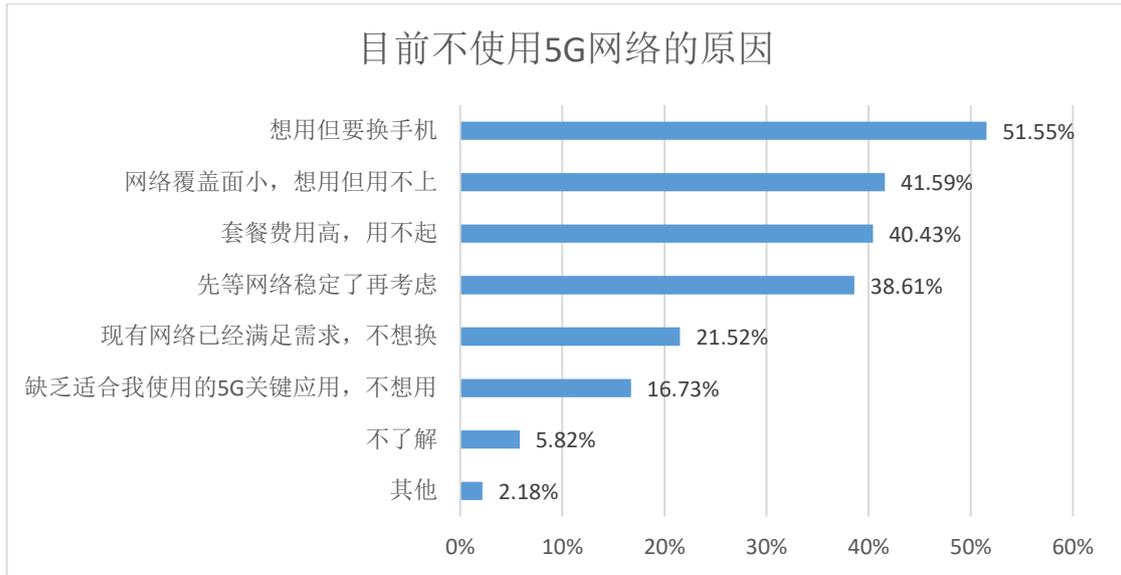


图表 4.3-4: 对 5G 网络使用体验的评价

（图表数据来源：从业人员版新技术应用与网络安全专题第 2.1 题：使用 5G 网络的感受是？）（本题是由使用过 5G 的人回答，答题人数 3711。）

（2.2）目前不使用 5G 网络的原因

目前不使用 5G 网络的原因排前 3 位为：1 想用但要换手机（51.55%）、2 网络覆盖面小想用但用不上（41.59%）、3 套餐费用高用不起（40.43%）；4 先等网络稳定了再考虑（38.61%）。数据显示手机终端、使用成本、网络质量等问题是参与调查的从业人员使用 5G 考虑的主要因素。

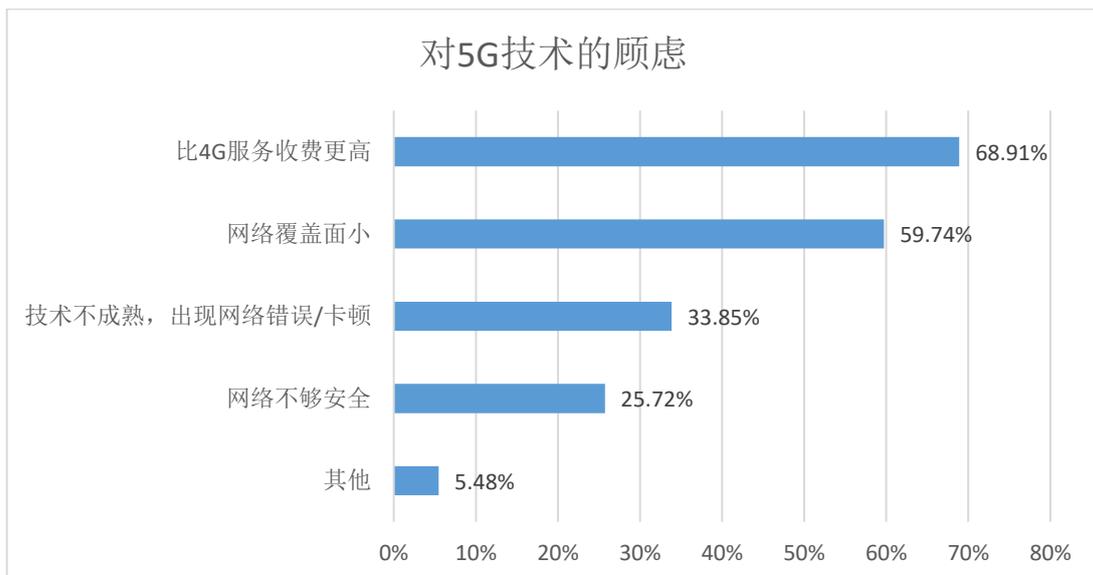


图表 4.3-5: 目前不使用 5G 网络的原因

（图表数据来源：从业人员版新技术应用与网络安全专题第 2.2 题：目前不使用 5G 网络的原因是？）

（3）对 5G 技术的顾虑

参与调查的从业人员对 5G 技术的顾虑主要有：1 比 4G 服务收费更高(68.91%)，2 网络覆盖面小（59.74%），3 技术不成熟出现网络错误或卡顿（33.85%），4 网络不安全（25.72%）。



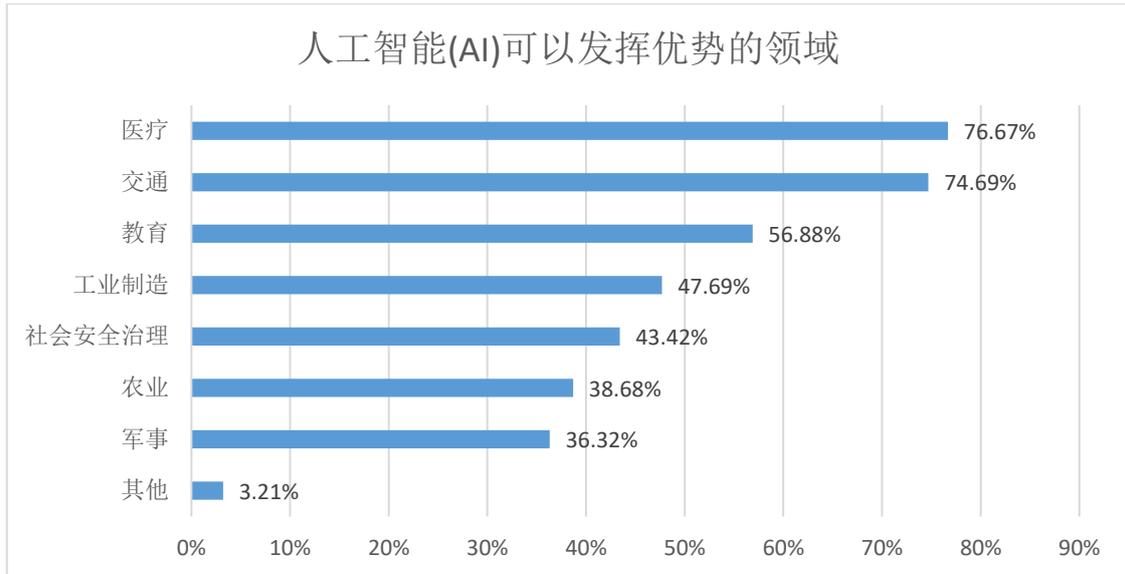
图表 4.3-6: 对 5G 技术的顾虑

（图表数据来源：从业人员版新技术应用与网络安全专题第 3 题：您对 5G 技术

存在哪些顾虑？）

（4）人工智能(AI)可以发挥优势的领域

参与调查的从业人员对人工智能(AI)可以发挥优势的领域认为：医疗（76.67%）、交通（74.69%）、教育（56.88%）、工业制造（47.69%）和社会安全治理（43.42%）等领域人工智能可以发挥优势。



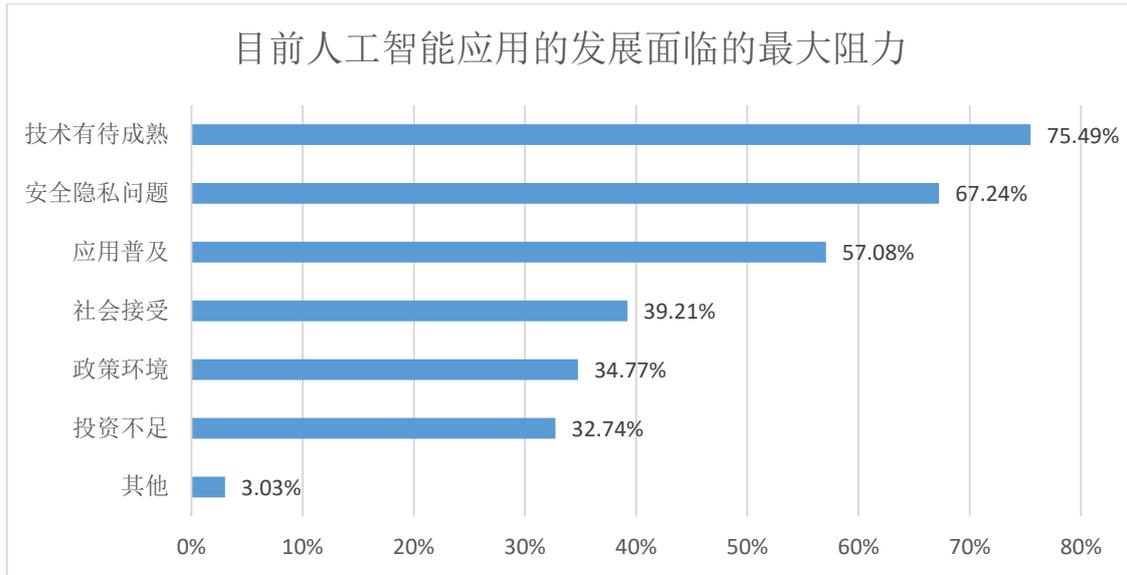
图表 4.3-7：人工智能(AI)可以发挥优势的领域

（图表数据来源：从业人员版新技术应用与网络安全专题第4题：您最期待人工智能(AI)在哪些领域发挥优势？）

广东新兴国家网络安全和信息化发展研究院

（5）目前人工智能应用发展面临的阻力

参与调查的从业人员对目前人工智能应用发展面临的阻力排前3位为：1 技术有待成熟（75.46%），2 安全隐私问题（67.24%），3 应用普及（57.08%），数据显示技术成熟度、安全隐私保护问题等是从业人员关注的重点。

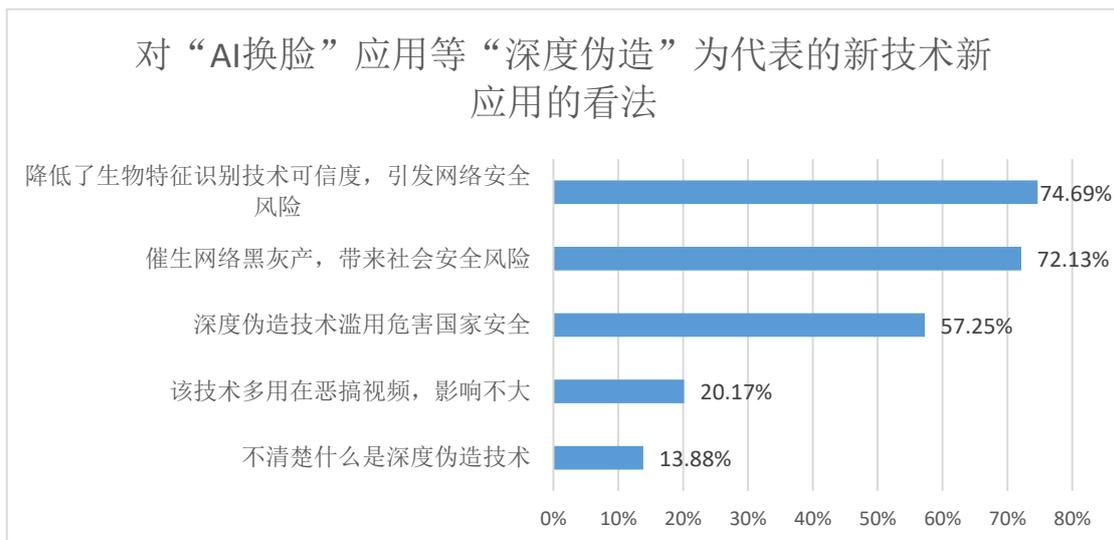


图表 4.3-8：目前人工智能应用的发展面临的最大阻力

（图表数据来源：从业人员版新技术应用与网络安全专题第 5 题：您认为目前人工智能应用的发展面临的最大阻力是？）

（6）对“AI 换脸”应用等“深度伪造”为代表的新技术新应用的想法

参与调查的从业人员对“AI 换脸”应用等“深度伪造”为代表的新技术新应用的想法排前 3 位为：1 减低了生物识别技术可信度（74.69%）、2 催生网络黑灰产业、带来社会风险（72.13%）、3 深度伪造技术滥用危害国家安全（57.25%）。数据显示从业人员对深度伪造技术是比较担心的。



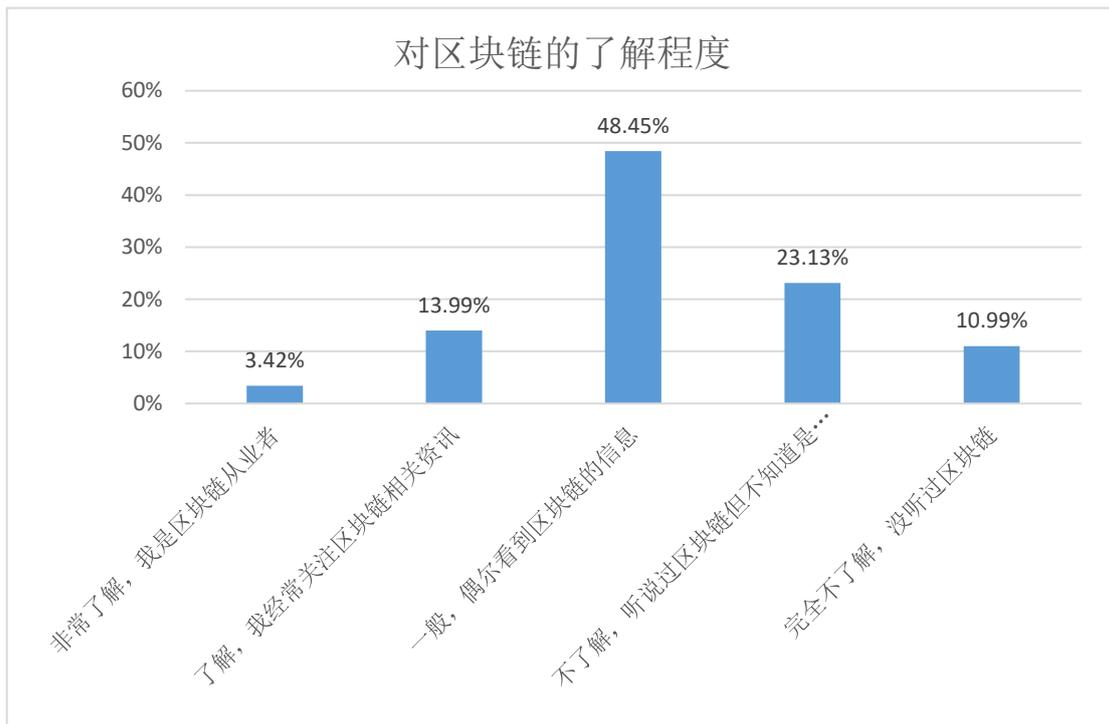
图表 4.3-9：对“AI 换脸”等“深度伪造”为代表的新技术新应用的想法

（图表数据来源：从业人员版新技术应用与网络安全专题第 6 题：近两年出现了

“AI 换脸”应用，您怎么看这种以“深度伪造”为代表的新技术新应用？）

（7）对区块链的认识

参与调查的从业人员对区块链的认识看法为：**48.45%**从业人员认为一般，偶尔看到区块链的信息；**23.13%**从业人员对区块链不了解，听说过；也有**10.99%**完全不了解。数据显示从业人员对区块链了解程度一般或不高。

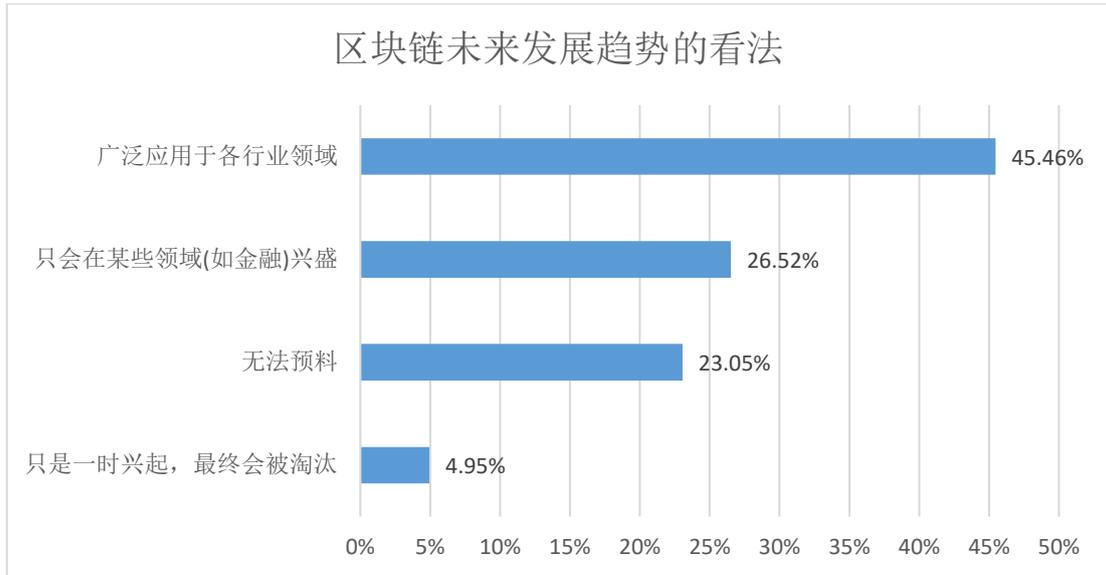


广东新兴国家网络安全和信息化发展研究院 图表 4.3-10：对区块链的了解程度

（图表数据来源：从业人员版新技术应用与网络安全专题第 7 题：对区块链，您了解多少？）

（8）区块链未来发展趋势

参与调查的从业人员对区块链未来发展趋势的看法：认为会广泛应用于各行业领域最多，占**45.46%**，认为只会在某些领域（金融）兴盛的占**22.64%**和认为无法预料的占**23.05%**，认为只是一时兴起，最终会被淘汰的**4.95%**。看好区块链发展的比例不低。

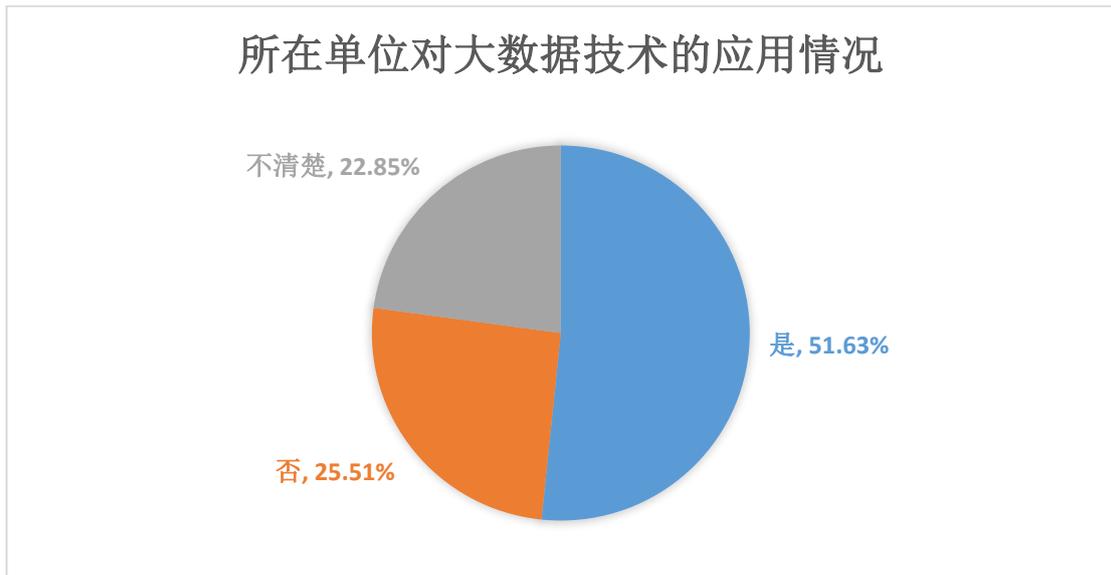


图表 4.3-11: 区块链未来发展趋势的看法

（图表数据来源：从业人员版新技术应用与网络安全专题第 8 题：您觉得区块链未来发展会如何？）

（9）所在单位对大数据技术应用情况

参与调查的从业人员所在单位对大数据技术的应用情况方面，51.63%的从业人员所在单位有应用了大数据技术；25.515%的从业人员所在单位没有应用大数据技术，22.85%表示不清楚。数据显示大数据开始在从业人员单位得到较广泛的应用。

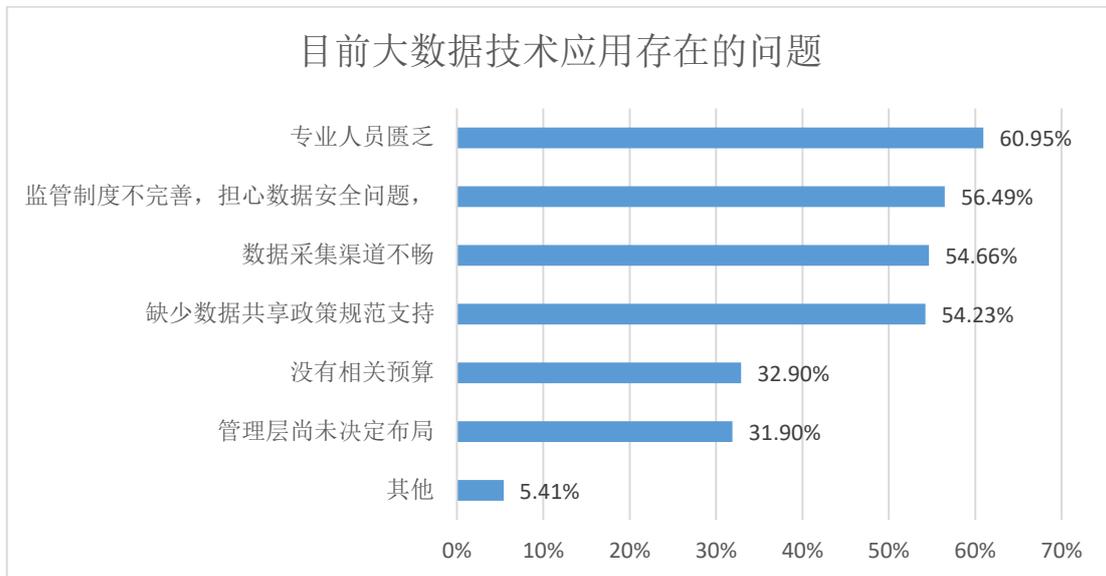


图表 4.3-12: 所在单位大数据技术应用情况

（图表数据来源：从业人员版新技术应用与网络安全专题第 9 题：您现所在单位是否应用了大数据技术？）

（10）目前大数据技术应用存在的问题

目前大数据技术应用存在的问题排前 5 位是：1 专业人员匮乏（关注度 60.83%），2 监管制度不完善（56.49%），3 数据采集渠道不畅（54.66%），4 缺少数据共享政策规范支持 54.23%，5 没有相关预算 32.90%。数据显示人才、制度、渠道、规范等问题是大家比较关注的。

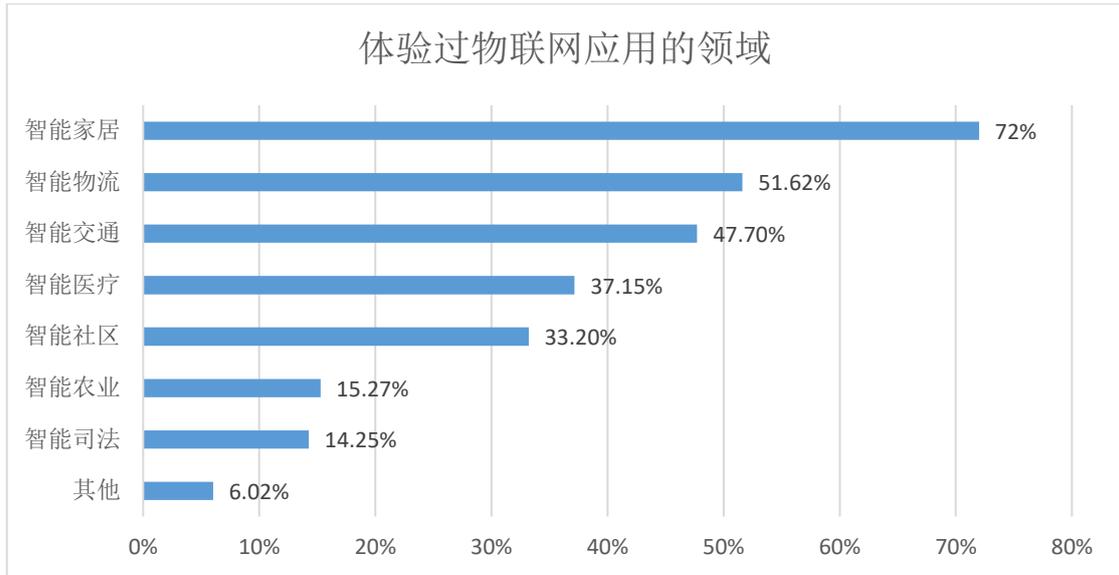


图表 4.3-13：目前大数据技术应用存在的问题

（图表数据来源：从业人员版新技术应用与网络安全专题第 10 题：您认为目前大数据技术应用上存在哪些问题？）

（11）对物联网的应用的感受

参与调查的从业人员对物联网应用的感受排前 3 位是：1 智能家居领域（关注度 72.%）2 智能物流（51.62%），3 智能交通（47.70%）。显示在智能家居、物流、交通等领域物联网技术应用比较广泛。

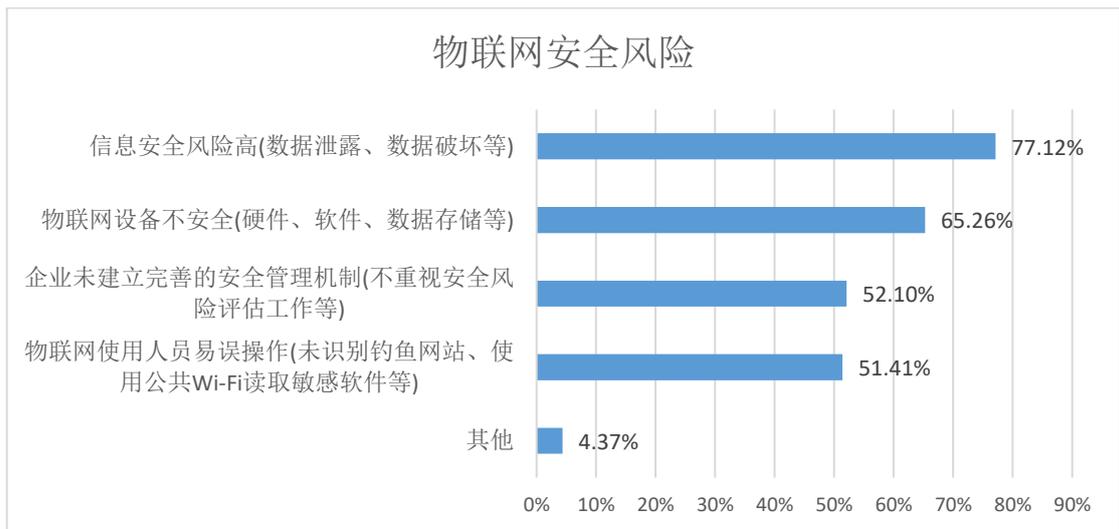


图表 4.3-14：体验过物联网应用的领域

（图表数据来源：从业人员版新技术应用与网络安全专题第 11 题：您在哪些领域体验过物联网的应用？）

（12）物联网安全风险认知

参与调查的从业人员对当下的物联网安全风险看法为：77.12%认为信息安全风险高，65.26%认为物联网设备不安全，52.10%认为企业未进阿里完善的安全管理机制，51.41%从业人员认为物联网使用人员易误操作。数据显示从业人员对物联网的安全风险是比较担心的。



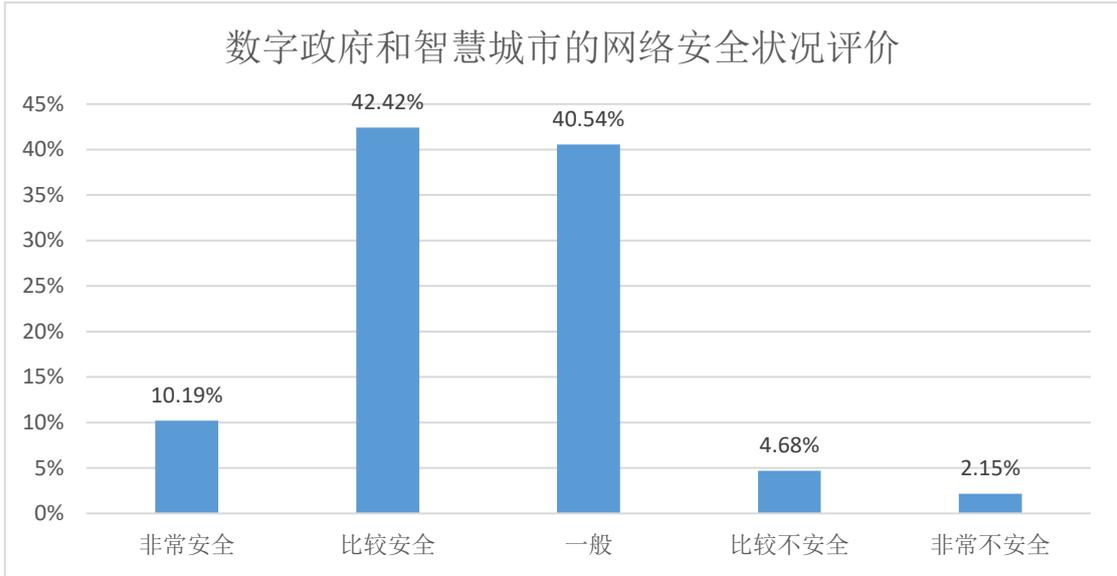
图表 4.3-15：物联网安全风险

（图表数据来源：从业人员版新技术应用与网络安全专题第 12 题：您认为当下

的物联网安全风险主要存在哪些方面？）

（13）数字政府和智慧城市的网络安全状况评价

参与调查的从业人员对数字政府和智慧城市的网络安全状况评价：**10.19%**从业人员认为非常安全，**42.42%**认为比较安全，**40.54%**认为一般。数据显示超过一半的从业人员认为数字政府和智慧城市的网络安全状况是比较安全的。

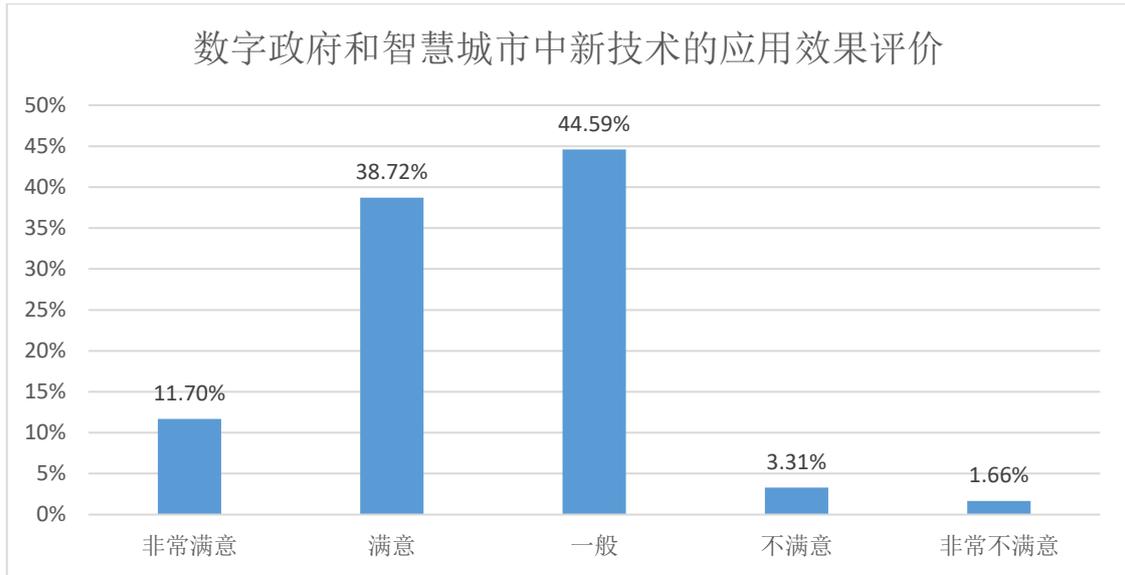


图表 4.3-16：数字政府和智慧城市的网络安全状况评价

（图表数据来源：从业人员版新技术应用与网络安全专题第 13 题：您对数字政府和智慧城市的网络安全状况评价？）

（14）数字政府和智慧城市中新技术的应用效果评价

从业人员对数字政府和智慧城市中新技术的应用效果评价：**11.70%**从业人员认为非常满意，**38.72%**认为满意，**44.59%**认为一般。数据显示超过一半的从业人员认为数字政府和智慧城市中新技术的应用效果是令人满意的。

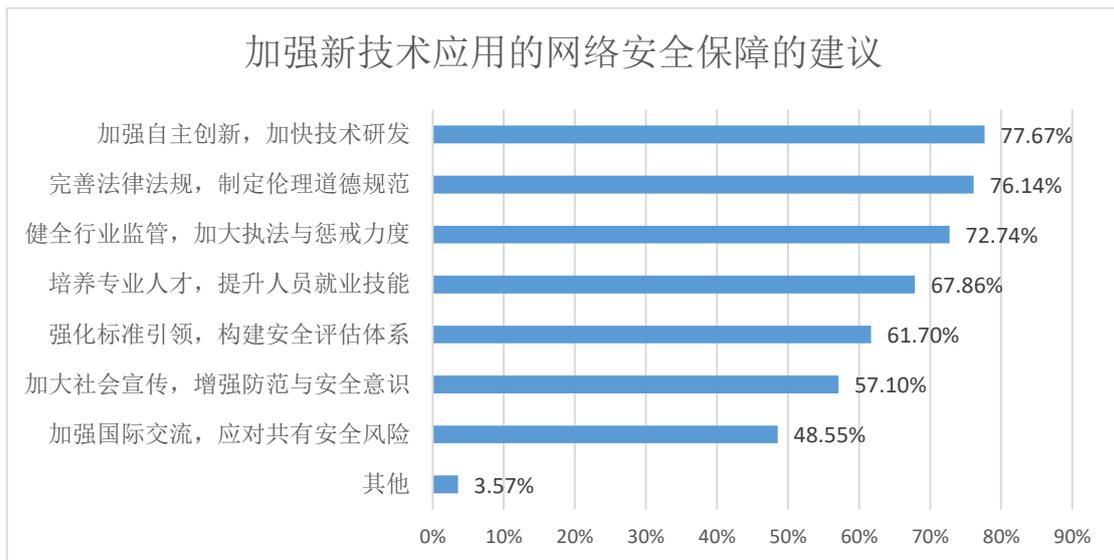


图表 4.3-17: 数字政府和智慧城市中新技术的应用效果评价

（图表数据来源：从业人员版新技术应用与网络安全专题第 14 题：您对数字政府和智慧城市中新技术的应用效果评价？）

（15）加强新技术应用的网络安全保障的建议

参与调查的从业人员对加强新技术应用的网络安全保障的建议排前 3 位的位：1 较强自主创新加快技术研发（认同率 77.67%）、2 完善法律法规（认同率 76.14%）、3 健全行业监管加大执法与惩戒力度（72.74%）。数据显示从业人员对加快自主创新、完善法规、坚强监管等方面比较关注。



图表 4.3-18: 加强新技术应用的网络安全保障的建议

（图表数据来源：从业人员版新技术应用与网络安全专题第 15 题：您对加强新技术应用的网络安全保障有哪些建议？）

网络安全感满意度调查



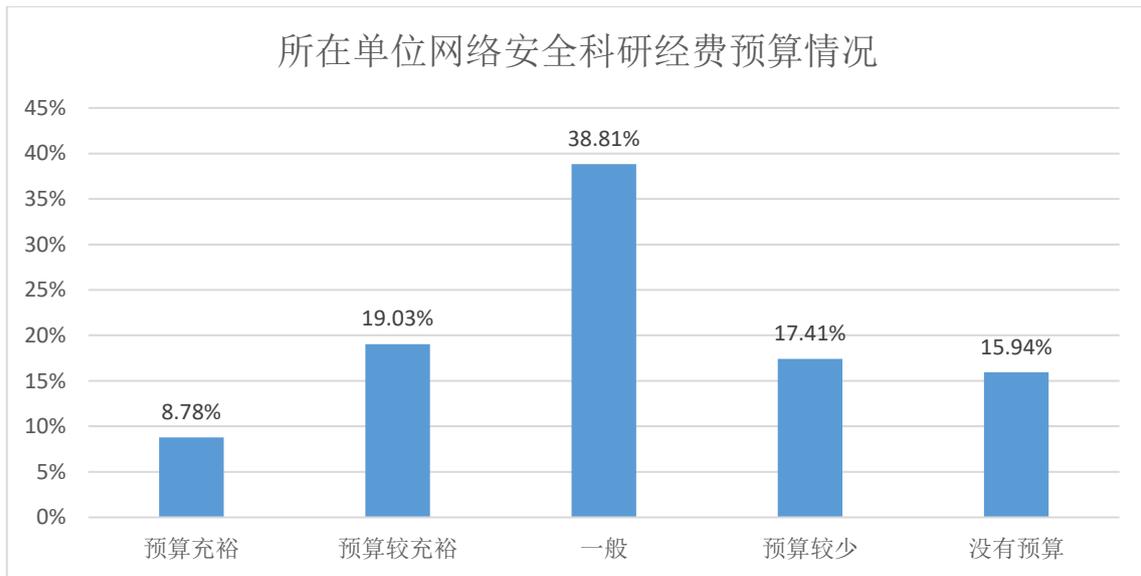
广东新兴国家网络安全和信息化发展研究院

4.4 科技创新与人才培养

参与本专题答题的从业人员人数为 1263。

（1）网络安全科研经费预算

在网络安全科研经费预算方面：8.78%参与调查的从业人员所在单位网络安全科研经费预算充裕，19.03%从业人员所在单位科研经费预算较充裕，38.81%科研经费预算一般，17.41%预算较少，15.94%没有预算。数据显示大部分（72.16%）从业人员所在单位网络安全科研经费一般或较少。

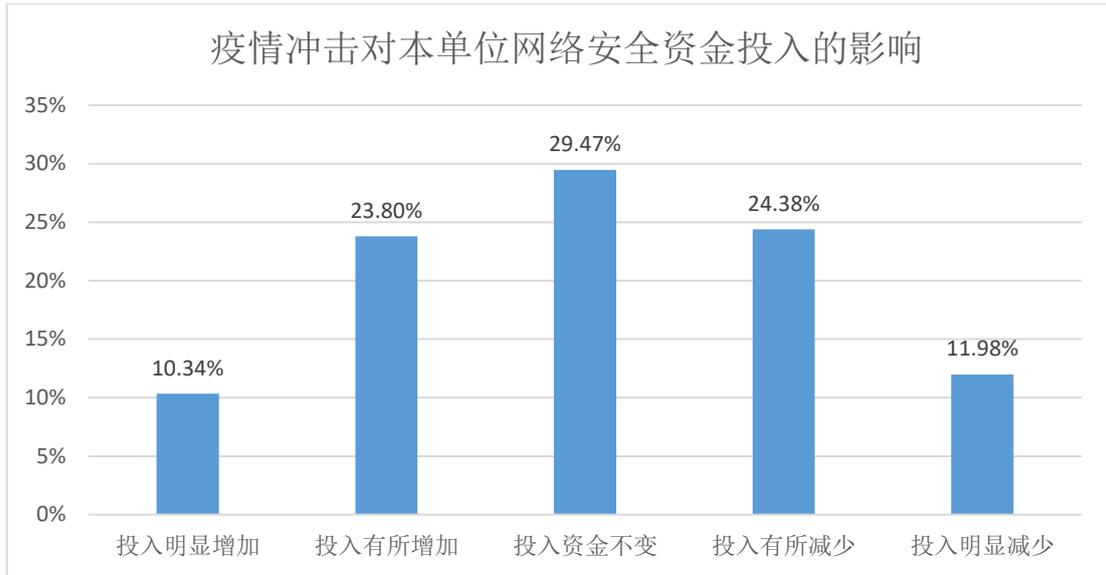


图表 4.4-1：所在单位网络安全科研经费预算情况

（图表数据来源：从业人员版科技创新与人才培养专题第 1 题：您所在单位在网络安全方面有没有专门的科研经费预算？）

（2）疫情对本单位网络安全方面的资金投入的影响

疫情对本单位网络安全方面的资金投入的影响方面：10.34%参与调查的从业人员所在单位网络安全投入明显增加，23.80%从业人员所在单位网络安全投入有所增加，29.47%投入资金不变，24.38%投入减少，11.98%投入明显减少。数据显示从业人员所在单位网络安全投入方面受到疫情的影响在总体上呈均衡态势，总的来说影响不大。

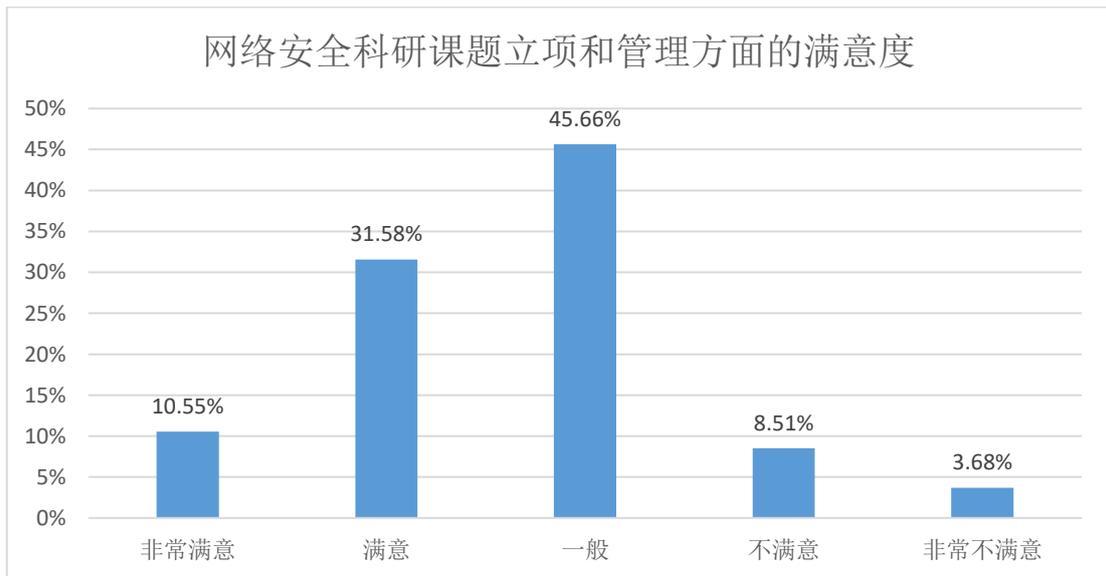


图表 4.4-2：疫情冲击对本单位网络安全资金投入的影响

（图表数据来源：从业人员版科技创新与人才培养专题第 2 题：全球疫情冲击带来的经济萎缩、收入减少对本单位网络安全方面的资金投入有什么影响？）

（3）网络安全科研课题立项和管理的评价

参与调查的从业人员对网络安全科研课题立项和管理方面的评价：10.55%表示非常满意，31.58%表示满意，45.66%表示一般，8.51%表示不满意，3.68%表示非常不满意。数据显示从业人员对科研课题立项和管理的评价中间偏好。



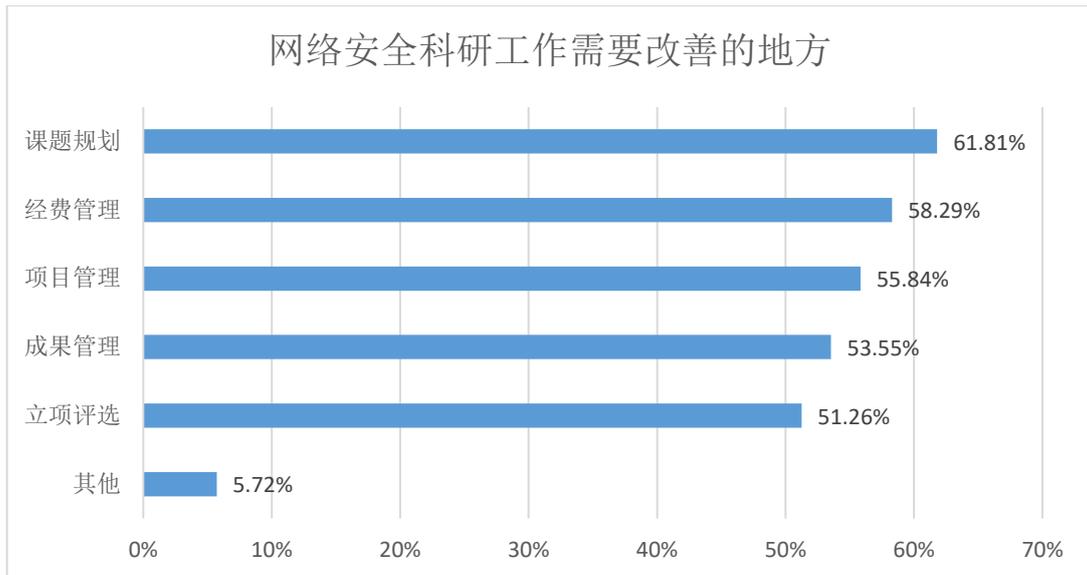
图表 4.4-3：网络安全科研课题立项和管理方面的满意度

（图表数据来源：从业人员版科技创新与人才培养专题第 3 题：您对网络安全科

研课题立项和管理方面的状况是否满意？）

（4）网络安全科研工作需要改善的地方

参与调查的从业人员对网络安全科研工作需要改善的地方的看法：1 课题规划（关注度 61.81%）、2 经费管理（关注度 58.29%）、3 项目管理（关注度 55.84%）。数据显示从业人员对科研工作不满意的地方主要在课题规划、经费管理、项目管理等方面。

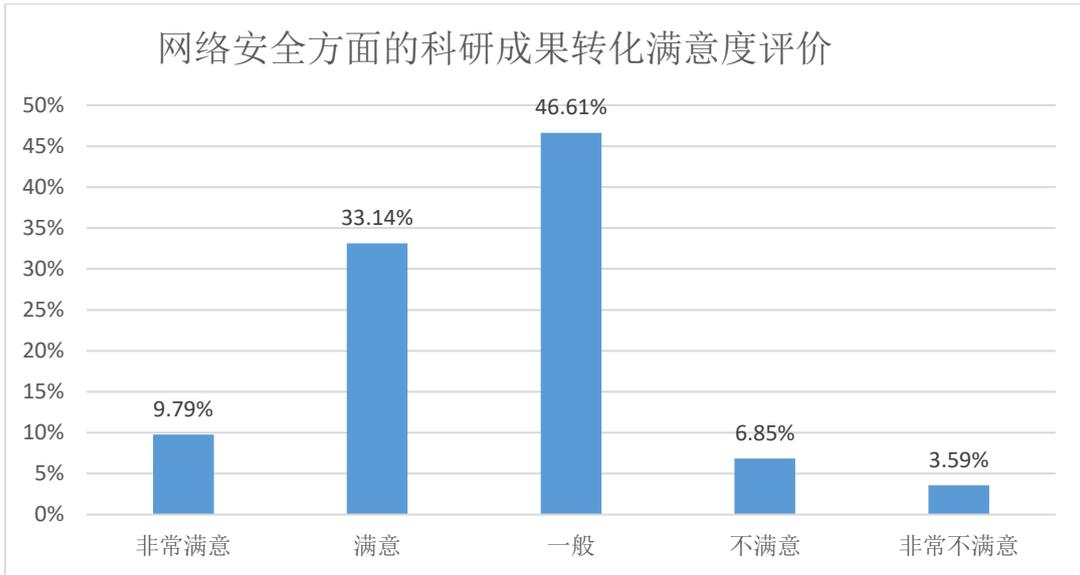


图表 4.4-4：网络安全科研工作需要改善的地方

（图表数据来源：从业人员版科技创新与人才培养专题第 4 题：您认为网络安全科研工作开展在哪些方面需要改善？）

（5）网络安全方面的科研成果转化状况

从业人员对网络安全方面的科研成果转化状况看法：9.79%从业人员认为非常满意、33.14%认为满意、46.61%认为一般、6.85%认为不满意、3.59%认为非常不满意。数据显示从业人员对科研成果转化评价中间或较好。

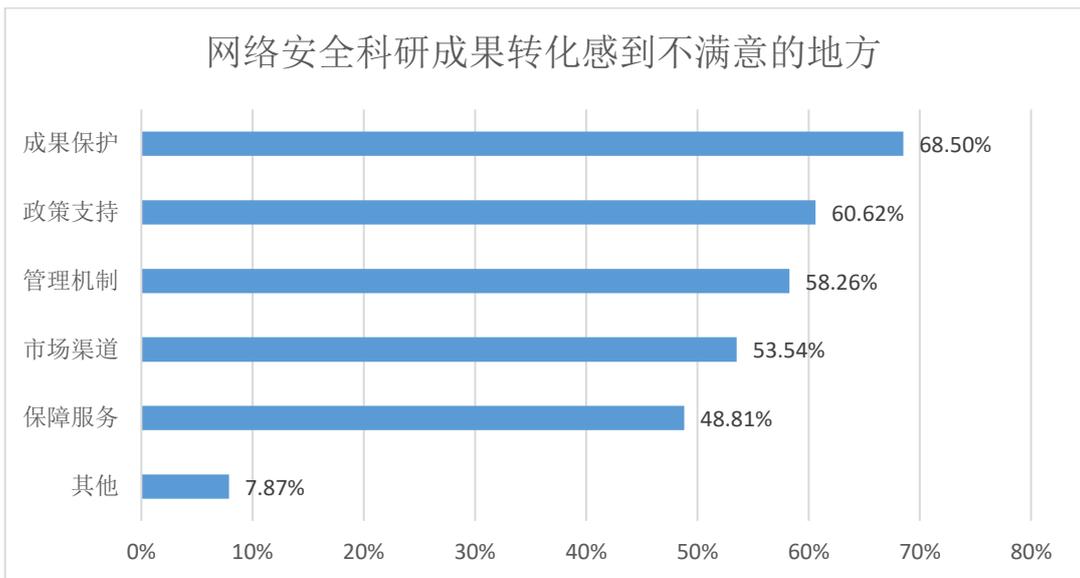


图表 4.4-5：网络安全方面的科研成果转化满意度评价

（图表数据来源：从业人员版科技创新与人才培养专题第 5 题：您对网络安全方面的科研成果转化状况是否满意？）

（5.1）网络安全方面的科研成果转化的问题

参与调查的从业人员对网络安全方面的科研成果转化存在问题的看法：**1 成果保护（关注度 68.50%）、2 政策支持（关注度 60.62%）、3 管理机制（关注度 58.26%）、4 市场渠道（关注度 53.54%）、5 保障服务（关注度 48.81%）。**数据显示从业人员认为成果保护、政策支持、管理机制等方面需要改善。

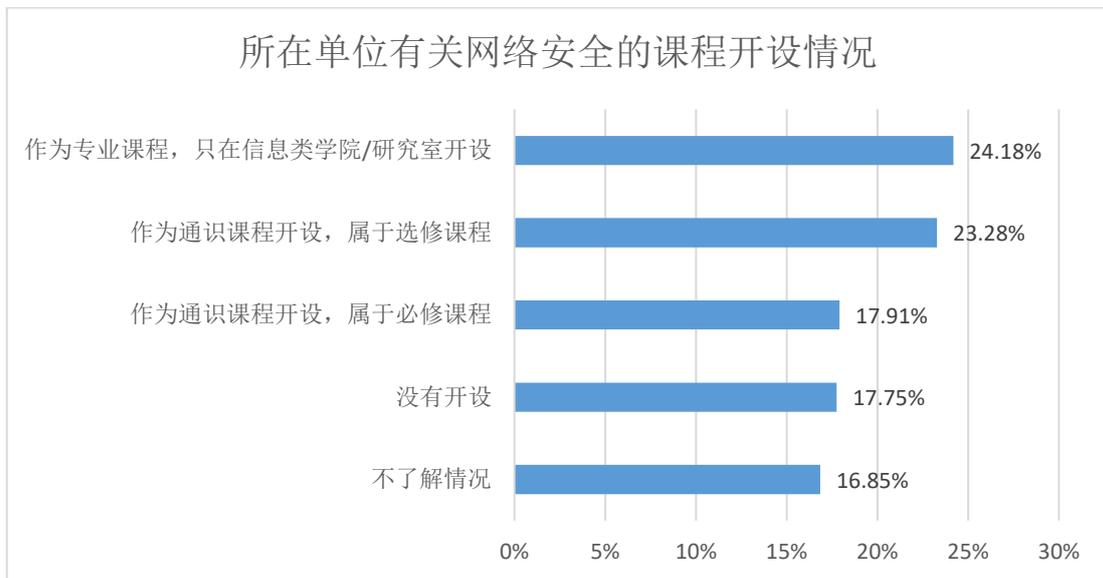


图表 4.4-6：网络安全科研成果转化感到不满意的地方

（图表数据来源：从业人员版科技创新与人才培养专题第 5.1 题：您对以下哪些方面感到不满意？）

（6）网络安全课程开设情况

参与调查的从业人员所在单位有关网络安全课程开设情况为：作为专业课程只在信息类学院开设最多（占比 24.18%）、作为通识课程开设，属于选修课程次之（占比 23.28%）、作为通识课程开设属于必修课程第三（占比 17.91%）、没有开设的第四（有 17.75%）。数据显示网络课程开设的比例一般，覆盖面不够广。

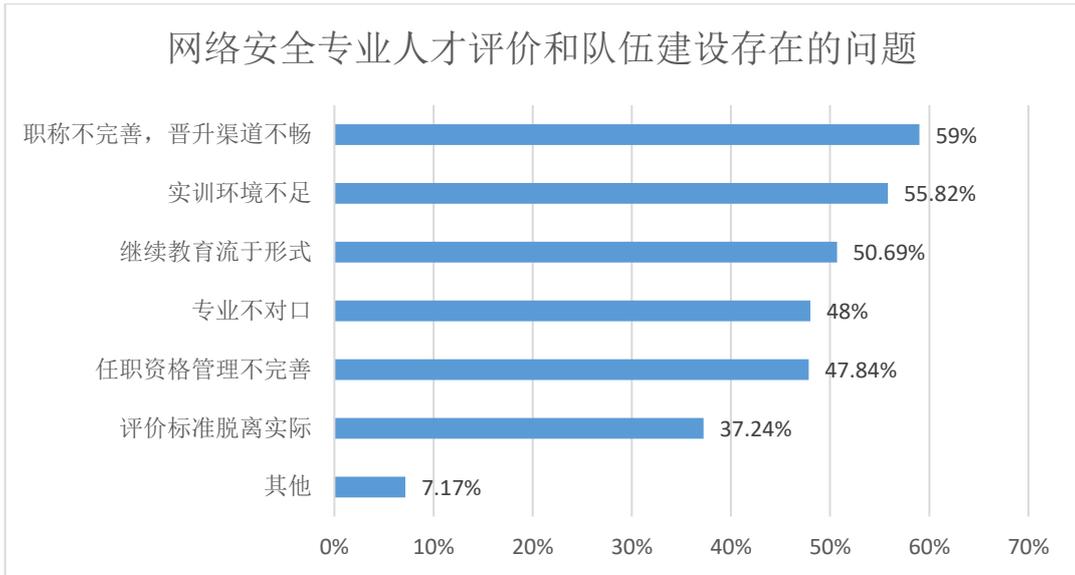


图表 4.4-7：所在单位有关网络安全的课程开设情况

（图表数据来源：从业人员版科技创新与人才培养专题第 6 题：您所在单位开设了关于网络安全的课程吗？）

（7）网络安全专业人才评价和队伍建设

有关网络安全专业人才评价和队伍建设方面的问题，关注度排在前 5 名的是：1 职称不完善、晋升渠道不畅（59%）、2 实训环境不足（55.82%）、3 继续教育流于形式（50.69%）、4 专业不对口（48%）、5 任职资格管理不完善（47.84%）。数据显示从业人员对网络安全专业人才职业发展和培养存在的问题比较关注。



图表 4.4-8：网络安全专业人才评价和队伍建设存在的问题

（图表数据来源：从业人员版科技创新与人才培养专题第 7 题：您认为网络安全专业人才评价和队伍建设方面存在哪些问题？）



广东新兴国家网络安全和信息化发展研究院

五、结论和展望

5.1 主要结论

本次网民网络安全感满意度调查是在总结去年满意度调查成功经验的基础上进行的，在许多方面包括问卷设计、组织发动、活动支持、数据服务等都有新的突破。在公安等有关主管部门大力支持下，在各组织单位共同努力下，调查活动取得良好效果，活动收回的问卷数量比去年有跨越式的增长，说明网络安全感满意度调查活动受到了网民极大的关注。从统计结果来看，本次问卷调查数据提供了丰富的信息，反映了广大网民对当前网络安全状况和治理效果的满意程度的评价，包括网民对热点问题的关注、对整体网络安全态势的感受、以及对政府监管、企业自律、行业发展、数字政府服务等方面的评价。另外，网民还提出了许多意见和建议，这些意见对政府有关部门加强网络空间治理，打造一个安全、清朗的网络空间有增添的调查的成果是丰富的。

概括起来，本次调查成果结合其它背景资料分析有以下主要结论：

（1）行业发展前景看好，网络安全领域成为热点

调查统计数据显示全国从业人员网民对网络安全行业发展前景看高，认为未来一年发展趋势是明显增长和略有增长的占了近八成（79.44%），其中认为明显增长占 37%，认为略有增长的占 42.44%。对行业发展的政策环境评价为非常好和好的共有 61.49%，超过六成，其中认为非常好的占 21.94%，认为好的占 39.55%。结合新基建、等级保护制度和关键信息基础设施保护制度的实施推动等利好因素分析，网络安全行业发展情景行业内普遍看好，网络安全领域在国际竞争加剧，国家利益面临重大安全挑战的背景下备受关注，网络安全领域成为热点，在国家治理和经济发展中发挥重要作用。

（2）疫情影响对行业冲击有限，市场需求增长前景看好

今年年初发生的新冠疫情给我国经济和民生造成很大的影响。出于疫情防控的需要，不得不采取的隔离措施使经济和社会停摆了一段时间，给不少的行业，特别是服务业造成较大的影响。与此同时人们工作和生活方式发生了较大的变化，网络化程度大大提升，各种业务和服务由线下转线上，远程办公、网上学习、视频会议等纷纷推出，网络平台企业、信息技术行业及时应变，推出针对线上渠道的各种网络应用服务，满足广大网民的需要。对于和线上服务密切相关的网络安

全领域的企业则是一次扩大市场的机会，可以说是危中有机，网络安全行业在应变中谋发展，一方面在抗击疫情过程中，网络安全领域的企业积极应对，上网、护网提供网络安全保障服务，另一方面，网络企业积极推出新应用和服务，满足线上业务的增长。因此，行业内受疫情的影响相对不算太严重。

政府推出的刺激经济的政策产生了良好的拉动作用。为了抵抗疫情冲击给经济带来的不良影响，政府推出了多种减税、投资等刺激经济的政策和措施，包括推出以新基建为重点的大规模基础设施建设，推动双循环，拉动消费等，在宏观层面上为扩大需求产生的明显的拉动作用，市场环境的转变，需求的启动，给网络安全领域的企业带来了更广阔的发展空间。

政府加强网络安全治理的措施有力推动了行业的发展。政府一方面加大了对智慧城市、智能管控平台的投入，提升政府现代化治理能力，刺激了相关技术和服务迅速推出利用网络、大数据、移动应用等信息技术的抗击疫情的新应用，如健康码、疫情通报、行程跟踪、医疗物资预约分发、远程医疗等。公安部门及有关管理部门加强了对网络空间的监管和对违法犯罪活动的打击，重点整治了网络诈骗、谣言传播等问题，有力地保障了网络空间的安全，调查数据也显示网民对政府采取的应对措施的效果评价是比较满意的。政府近年来加强智慧城市、智慧交通、平安城市等信息化建设大大地改善了信息化基础设施，为提升政府现代化治理能力，改善数字政府公共服务打下坚实的基础。可以说政府和网络行业在这次抗击疫情的斗争中接受了一次重大的考验，交出了一份令人较满意的答卷。

（3）网络安全形势严峻，病毒勒索等网络黑灰产业比较活跃

在信息社会的今天，网络空间更是各种势力争夺的主战场。当前国际风云变幻，针对我国的科技战、贸易战、颜色革命接连登场，各种敌对势力在或明或暗地在进行窥探和攻击。在持续高强度的安全威胁下，网络安全形势非常严峻。在信息技术的高速发展的背景下，网络犯罪呈现新的特点，正逐步向产业化、专业化、智能化、高隐蔽、高危害的方向发展，对网络安全防范和打击网络违法犯罪提出了新的挑战。调查数据显示当前网络暴力、恶意炒作、不良信息泛滥等问题比较突出，受到网民的关注，网络诈骗、网络黑灰产业等问题仍比较严重，打击网络犯罪任重道远。

（4）网络安全监管得到加强，企业合规自律水平有较大提升

网络安全等级保护制度和关键信息基础设施保护制度是我国网络安全保护体系建设中两大重要支柱。推行这几年来，以标准规范为指导，以定级、测评、监督为抓手，工作取得很大进展，网络信息系统安全的分级保护得到落实。关键信息基础设施保护工作也在进一步加强统筹协调、完善标准规范建设、理顺管理机制的过程中有序推进。通过落实网络安全等级保护和关键信息基础设施安全保护制度，强化了各单位的网络安全主体责任，推动了各单位落实网络安全建设和运维合规运作，促进了各单位网络安全管理水平提升，带动了网络安全产品与服务的发展，效果是明显的。

（5）供应链安全问题比较突出，自主创新带来新机遇

5G、物联网、大数据、人工智能、区块链等新技术的创新突破和推广应用，新基建、双循环等政策带动下，出现了许多新业态，形成经济发展的新动能，这也为信息技术行业带来许多新机遇，预示着一轮新的大发展，从业人员网民普遍对行业的发展持乐观的态度。另外一方面，从业人员网民也关注到新技术应用带来的网络安全风险问题，期望能同步考虑相关的网络安全保障措施。供应链安全问题也是一个受到网民的关注比较突出的问题，我国信息技术产业虽然发展很快，有的领域还取得了令人瞩目的成就，但总体上基础还比较薄弱，还存在关键技术、核心元器件、基础平台、产业生态等方面的短板，在科学研究，技术研发、人才培养等方面有待进一步完善和加强。

5.2 未来展望

（1）网络安全市场持续快速增长，新基建等领域成为热点

宏观上，后疫情时代，经济复苏和经济转型双线拉动，供给侧和需求侧改革共同发力，新基建、国产化替代、发展数字经济等措施加快形成新业态、新动能，对经济起了有力的推动作用。和新基建、信息技术密切相关的网络安全领域被认为具有良好的发展前景，已经成为市场的热点和投资的热点。新基建以投资拉动形成新需求，产生新动能。信息化基础设施是其中重要的组成部分，按照网络安全的要求信息安全要同步建设，必然刺激相关产品和服务市场的增长，数字化、网络化发展、创新驱动发展，新业态、新服务带来新机遇。云服务、新网络、数据中心的建设为中西部带来新的机遇，网络空间的一体化，地理区位的条件发生改变。数字经济成为中西部地区弯道超车的助推器。

网络安全领域层面，复杂多变的国际形势发展，国家面临着重大的安全挑战，网络安全领域要进一步加大力度进行保护。各级政府加强了政策引导，网络安全等级保护制度和关键信息基础设施保护制度的进一步贯彻推广，网络安全建设和基础设施建设同步规划、同步建设、同步投入使用的措施和要求，推动了网络安全领域的需求增长，为网络安全行业带来了前所未有的发展机遇。

（2）新技术加快更新换代，智能化与可信安全成为热点

5G、物联网、大数据、人工智能、区块链等新技术的创新突破和推广应用，新基建、双循环等政策带动下，新技术和传统行业的融合发展出现了许多新业态，形成经济发展的新动能，这也为信息技术和网络安全行业带来许多新机遇，预示着一轮新的大发展，从业人员网民普遍对行业的发展持乐观的态度。

在应用需求的驱动下，新技术不断迭代完善，可信技术、智能化技术、物联网技术等受到关注。网络安全等级保护和关键信息基础设施保护制度的推行和实施为网络安全行业的发展提供的巨大的推动力。网络安全等级保护 2.0 标准的推广给可信安全技术的快速发展起了重要的作用。大数据技术的应用结合丰富的应用场景，可以实现各种智能化应用，有的已经成为领先的技术。我国在传统积累包袱不重，在新技术推广方面有一定的优势，可以快速形成规模，实现弯道超车。

（3）服务体系逐步完善，质量为本品牌效应更突出

数字经济的发展为网络安全行业的快速发展提供了广阔的空间，经济转型中出现的新业态、新应用、新模式对网络安全提出了更高的要求，数字资产在不断累积和扩大，而网络安全风险仍层出不穷，如何提升服务能力，为数字经济发展保驾护航是网络安全行业共同面对的问题。

随着网络安全技术的产品和系统越来越复杂，网络安全行业的发展进入更专业、更高端的阶段。产品和技术的供应方的价值交付将更多地以服务为中心，竞争力更多地体现在服务能力、运营能力上。

网络安全领域将加快服务体系建设，通过整合行业资源，充分发挥咨询、产品、服务、测评、中介、培训等方面的作用，建立完善的服务机制，形成以服务质量为核心的竞争格局。网络安全是一个技术密集型的领域，质量为本，信誉度很重要，容易形成品牌效应，用户粘性比较强，拥有核心技术和服务能力的企业将取得更多的优势。网络安全行业的发展关键是人才。联合政、产、学、研、用

等各方面的力量，加强对人才的培养，加大网络安全科研的投入和成果转化的支持，提升网络安全行业技术水平。

（4）产业生态建设初具规模，形成中国特色的发展路径

随着网络空间治理的不断完善，网络安全行业面临新的发展机遇。国际政治风云变幻，大国之间冲突和对抗的加剧，国家安全面临严重挑战，特别是网络空间安全领域，安全风险更加突出。产业安全、供应链安全备受关注，随着国家加大对核心关键技术的研发投入，为实现自主可控打下坚实的基础。我国拥有足够规模的市场体量，有丰富的应用场景需求，有配套较齐全的产业体系，为行业发展和企业的发展提供了广阔的发展空间。

要利用市场规模和应用场景的优势，下大力气做好抓好核心技术的研发，提高关键技术、原材料、产品的自主可控程度，支持核心骨干企业，加强和完善产业生态建设，形成可持续发展的体系优势。展望未来，网络行业要以自主创新为手段，以标准规范为引领，根植本土，面向世界，积极开拓市场，打造中国方案、中国产品、中国标准。充分发挥行业协会、技术联盟等机构的作用，推动产业合作，资源共享，加快建设协调发展的产业生态。

广东新兴国家网络安全和信息化发展研究院

网络安全感满意度调查



广东新兴国家网络安全和信息化发展研究院

附件一：调查方法与数据样本情况

一、背景

为贯彻习近平总书记关于“网络安全为人民、网络安全靠人民”等网络强国的重要思想，进一步落实《网络安全法》及相关法律法规，增强网民的网络安全意识和防范能力，促进互联网企业履行社会责任意识和能力的提高，提升网民网络安全感和满意度，最大限度调动网民参与网络生态社会治理的自觉性和主动性，助力政府相关部门积极探索网络治理规律，提高网络治理成效，由公安部网络安全保卫局指导，全国 135 家网络安全行业协会及相关社会组织联合发起了 2020 网民网络安全感满意度调查活动。

二、目的

网民网络安全感满意度调查的宗旨就是要坚持面向网民大众，目的是让大家有话可以说，让政府主管部门可以倾听和了解网络安全在网民中的感受、网民的诉求和存在的问题。同时也向广大网民宣传网络安全的相关政策、法律和知识。

开展网民安全感满意度调查活动的具体目的有以下几点：

（1）通过广泛收集广大群众上网用网过程中对网络公共秩序、安全环境的真实感受和评价，科学反映我国网络治理成效和网络安全现状，为政府部门决策提供数据支持。为公安机关加强互联网安全监管和打击网络违法犯罪提供指引。

（2）通过发挥社会组织的桥梁作用，调动社会各方力量，广泛发动广大网络用户积极参与，齐心协力，贡献智慧，共建良好网络生态，共筑网络安全屏障。

（3）通过不断收集和积累网民网络安全感满意度数据，形成庞大的数据库，为满意度研究和各种数据分析挖掘研究提供数据基础，建立和优化网民网络安全感满意度评价模型，推动网民网络安全感满意的量化研究向前发展。

三、调查方式

（1）调查时间

2020 年 6 月，以“网络安全为人民，网络安全靠人民”为活动主题的 2020 网民网络安全感满意度调查活动正式启动。2020 年 7 月 22 日正式上线采集数据。到 2020 年 7 月 31 日 24 点结束采集。采集的时间段为 10 天。

（2）调查对象

本次调查对象分为两类：一类是普通网民，另外一类是网络行业从业人员。普通网民主要面向在中国境内有上网经验，熟悉中国互联网情况的互联网使用者。他们的意见主要体现互联网普通用户的感受。网络行业从业人员主要面向在网络行业工作人员，其工作单位或工作岗位和互联网有关，包括互联网企业、网络安全产品与服务的提供者、网络安全协会、政府主管部门、企事业单位、网络安全的学校和科研机构、一般的互联网用户等。网络行业从业人员对互联网的状态比较了解，是网络安全治理中主要的参与者、服务提供者和服务利用者。他们的意见体现了网络安全治理中关系密切的各类利益群体和专业人士的观点。

两类调查对象的意见的综合可以较为全面地反映各类网民的真实感受，为数据采集、分析提供坚实的基础。

（3）调查内容

本次网民网络安全感满意度调查内容丰富，以问卷的形式提出了 225 道题（小题），内容涵盖 2 个主问卷、12 大专题领域。调查问卷按访问对象不同分两类问卷：面向普通网民的公众版和面向网络行业从业人员的从业人员版问卷

公众版的调查问卷除了以共性问题为主的主问卷外，还根据内容主题的不同分了 8 个专题问卷，具体名称如下：

专题 1 问卷：网络安全法治社会建设专题

专题 2 问卷：遏制网络违法犯罪行为专题

专题 3 问卷：个人信息保护专题

专题 4 问卷：网络购物安全权益保护专题

专题 5 问卷：未成年人网络权益保护专题

专题 6 问卷：互联网平台监管与企业自律专题

专题 7 问卷：数字政府服务与治理能力提升专题

专题 8 问卷：新冠疫情的影响和应对专题

从业人员版的调查问卷除了以共性问题为主的主问卷外，还根据内容主题的不同分为 A 到 D 共 4 个专题问卷，具体名称如下：

A 专题问卷：等级保护实施与企业合规专题

B 专题问卷：行业发展与生态建设专题

C 专题问卷：新技术应用与网络安全专题

D 专题问卷：科技创新与人才培养专题。

本次调查问卷的设计以网络安全感满意指标体系为框架，以网民对网络安全的认知、需求、感受与评价为主线，针对相关政府主管部门、互联网企业、安全产品服务供应商、协会、科研机构、一般联网使用单位及网民自身在网络安全建设中的角色、职责、执行情况及其产生的效果设计调查问题。

除了一般的选择题外，问卷还设立了 11 道征求意见的填空题，以开放的形式让网民畅所欲言，以求充分收集网民的意见。

（4）调查形式

由于疫情防控需要，本次调查形式为线上方式。全国统一部署，各省分别组织落实，企业机构参与，网民自愿参加。

线上方式主要是依托在基于云平台问卷调查云服务，建立 2019 网民网络安全感满意调查服务门户和相应的网上问卷调查应用，同时支持两份公众版和从业人员版调查问卷的数据采集，提供手机和 PC 两个渠道，支持二维码扫描分享。利用组委会微信公众号和各合作单位以及支持单位的信息服务商门户进行推广，取得良好的效果。

（5）调查组织

指导单位公安部网络安全保卫局对调查活动给予了大力支持。领导高度重视，明确目标，指导把关，积极推动，狠抓落实，成效显著。

在指导单位的关心和指导下，为加强对调查活动的组织领导，活动发起单位组建了强有力的组织机构，机构分为领导小组、活动组委会（秘书处）和专家组等。

领导小组由指导单位公安部网络安全保卫局、各级有关主管部门，发起单位网安联主要领导组成，负责调查活动重大事项的决策。

活动组委会由各发起单位的主要领导组成，负责活动的组织工作，有关活动事项的组织实施。下设秘书处。秘书处负责日常办公事务处理和对外联系和活动的组织协调。活动组委会在总结 2018、2019 年两届网民网络安全感满意度调查活动经验基础上，今年的调查活动在活动组织、品牌建设、推广发动、研究规划、问卷设计等方面进行了多方面的创新和改进，取得显著的效果，活动影响力和问

卷数量实现跨越式增长。

专家组由国家及地方相关领域的专家、学者组成，负责审查及评价调查设计、调查过程的科学性、客观性和真实性。

活动的组织分为前期策划、问卷设计、组织发动、调查实施、数据分析与报告编制、成果发布与总结表彰等几个阶段。

各地发起单位和协会按照组委会的统一部署和要求开展工作，一是协调所在地互联网企业组织员工参与调查活动。最大限度地协调所在地互联网企业组织员工参与调查活动，确保调查活动有针对性、合理性、科学性地开展；二是组织协调所在地商业门户网站、新媒体网络平台、中央（地方）重点新闻门户网站等参与调查活动。充分发挥这些网络平台在本地影响力大、覆盖面广、粉丝量多的特点，通过一定的推广合作和激励机制，最大限度地吸引网民在线上参与调查，确保调查活动的广泛性、代表性；三是负责跟进本地样本量的完成情况，确保按量保质完成数据采集工作。

在领导小组、组委会、专家小组和各地参与发动单位的共同努力下，本次调查活动，按既定计划推进，采集了大量的网民数据，本次调查活动问卷收回总量为 150.3168 万份，其中，公众网民版 124.3251 万份，网络从业人员版 25.9912 万份。数据的采集量比上一年度幅度增长 6~7 倍，活动取得圆满成功。

四、调查数据的有效性

根据本次调查活动收集的数据情况来看有以下特点：

1) 调查数据总大

本次调查活动问卷收回总量为 150.3168 万份。经过数据清洗后，有效样本数据总数为 149.0304 万份，其中，公众网民版 123.1455 万份，网络从业人员版 25.8849 万份。另外，调查活动还收到网民对我国网络安全建设提出的意见和建议共 16.4347 万条。本次调查活动受到网民的热烈响应，参与人数多，采集的数据样本的规模大，样本数据的总体质量比较好。

2) 调查数据来源分布广泛

从调查数据来源来看，数据的分布广泛，全国 34 个省、直辖市、自治区（包括港澳台）400 多个地市（区）均有数据，其中 2 个省的数据量超过 20 万，21

个省数据量过万，31 个省的数量超过 1 千。

3) 调查数据分布比较均匀

从调查数据来源来看，数据的分布广泛，全国 400 多个地级市都有样本数据分布，反映本次样本分布比较均匀。

从以上分析，本次问卷调查数据的样本基本符合网民的分布的主要特性，具有较高的代表性。

网络安全感满意度调查



广东新兴国家网络安全和信息化发展研究院

附件二：调查报告致谢词

致谢

2020 年网民网络安全感满意度调查活动已顺利完成，在指导单位公安部网络安全保卫局大力指导和支持下，在参与各位的共同努力下调查活动取得圆满成功。调查活动结果经统计分析形成了本调查报告。调查报告的编制得到有关各方的指导和支持，报告编制组对有关参与各方的机构和人员表示衷心感谢。

感谢指导单位、发起单位、联合发起单位、组委会的组织指导（名单参看附件三、四）

感谢各牵头实施单位、承办单位、技术支撑单位的付出和贡献（名单参看附件四）

感谢新闻媒体、支持企业和机构的大力支持和配合（名单参看附件四）

感谢参与调查活动的各位专家、研究人员、技术人员和工作人员的辛勤劳动

感谢参与调查活动的公众网民和从业人员的积极参与

2020 年网民网络安全感满意度调查报告编制组
2020 年 9 月

附件三：调查活动指导单位、联合发起单位和组委会名单

（一）指导单位

公安部网络安全保卫局

（二）发起单位

网络安全感满意度调查

全国 135 家网络安全行业协会及相关社会组织（参看附件四）



（三）联合发起单位

北京大学

广东新兴国家网络安全和信息化发展研究院

中国互联网协会

中国电子技术标准化研究院

国家计算机病毒应急处理中心

（四）组委会

主任：

严 明 公安部第一、三研究所原所长

副主任：

谢毅平 广东新兴国家网络安全和信息化发展研究院院长
公安部科技信息化局原局长

袁旭阳 北京网络行业协会会长
公安部网络安全保卫局原副局长

陈 钟 北京大学网络和信息安全实验室主任

杨建军 中国电子技术标准化研究院副院长

陈建民 国家计算机病毒应急处理中心常务副主任

宋茂恩 中国互联网协会常务副秘书长

秘书长：

黄丽玲 全国信息网络安全协会联盟秘书长
广东省网络空间安全协会会长

副秘书长：

朱江霞 成都信息网络安全协会会长

胡俊涛 郑州市计算机网络安全协会秘书长

高 宁 广东新兴国家网络安全和信息化发展研究院总工

张 应 北京关键信息基础设施安全保护中心总工程师

郭守祥 北京网络空间安全协会副理事长

崔传桢 国家信息中心《信息安全研究》杂志执行主编

秘书长助理：

周贵招 全国信息网络安全协会联盟秘书长助理

林小博 北京网络空间安全协会秘书长助理

附件四：调查活动发起单位及支持单位名单（排名不分先后）

发 起 单 位

- | | |
|--------------------|----------------------|
| 1 北京网络行业协会 | 31 山东省信息网络安全协会 |
| 2 北京网络空间安全协会 | 32 福建省网络与信息安全产业发展促进会 |
| 3 中关村可信计算产业联盟 | 33 浙江省计算机系统安全协会 |
| 4 中关村网络安全与信息化产业联盟 | 34 河南省网络营销协会 |
| 5 中关村信息安全测评联盟 | 35 湖北省信息网络安全协会 |
| 6 北京关键信息基础设施安全保护中心 | 36 湖北省安全技术防范行业协会 |
| 7 上海市信息网络安全管理协会 | 37 湖南省网络空间安全协会 |
| 8 上海市信息安全行业协会 | 38 江西省网络空间安全协会 |
| 9 天津市网络文化行业协会 | 39 江苏省信息网络安全协会 |
| 10 天津市青少年网络协会 | 40 安徽省计算机网络与信息安全协会 |
| 11 天津市软件行业协会 | 41 广东省计算机信息网络安全协会 |
| 12 天津市互联网协会 | 42 广东省网络空间安全协会 |
| 13 天津市大数据协会 | 43 广东关键信息基础设施保护中心 |
| 14 重庆市信息安全协会 | 44 广东省电子政务协会 |
| 15 重庆计算机安全学会 | 45 广东软件行业协会 |
| 16 重庆信息安全产业技术创新联盟 | 46 广东省首席信息官协会 |
| 17 重庆市互联网界联合会 | 47 广东省版权保护联合会 |
| 18 河北省网络空间安全学会 | 48 广东省互联网协会 |
| 19 山西省信息网络安全协会 | 49 广东省信息消费协会 |
| 20 山西省互联网协会 | 50 广东省图书文化信息协会 |
| 21 吉林省信息网络安全协会 | 51 广东省物联网协会 |
| 22 吉林省信息技术应用协会 | 52 广州市网络安全产业促进会 |
| 23 吉林省电子信息行业联合会 | 53 广东省电子信息行业协会 |
| 24 吉林省计算机行业商会 | 54 海南省计算机学会 |
| 25 辽宁省信息网络安全协会 | 55 海南省网络安全协会 |
| 26 辽宁网络安全保障工作联盟 | 56 四川省计算机信息安全行业协会 |
| 27 黑龙江省网络安全协会 | 57 贵州省互联网上网服务行业协会 |
| 28 黑龙江省旅游产业发展促进会 | 58 云南省信息安全协会 |
| 29 黑龙江省虚拟现实科技学会 | 59 内蒙古自治区网络行业协会 |
| 30 陕西省信息网络安全协会 | 60 宁夏网络与信息安全行业协会 |

- | | |
|--------------------|----------------------|
| 61 广西网络安全协会 | 94 广州市信息基础协会 |
| 62 西藏互联网协会 | 95 广州华南信息安全测评中心 |
| 63 秦皇岛市信息网络安全协会（筹） | 96 深圳市计算机网络公共安全协会 |
| 64 长春市计算机信息网络安全协会 | 97 深圳市网络与信息安全行业协会 |
| 65 沈阳市网络安全协会 | 98 佛山市信息协会 |
| 66 大连市信息网络安全协会 | 99 揭阳网络空间安全协会 |
| 67 渭南市互联网协会 | 100 揭阳市信息技术和软件协会 |
| 68 榆林市网络安全协会 | 101 珠海市信息网络安全协会 |
| 69 商洛市信息网络安全协会 | 102 清远市网络安全协会 |
| 70 济宁市信息网络安全协会 | 103 茂名市计算机信息网络安全协会 |
| 71 青岛市计算机学会 | 104 茂名市网络文化协会 |
| 72 潍坊市网络空间安全协会 | 105 河源市计算机信息网络安全协会 |
| 73 曲阜市信息网络安全协会 | 106 惠州市计算机信息网络安全协会 |
| 74 聊城市网络空间安全协会 | 107 韶关市计算机信息网络安全协会 |
| 75 郑州市网络安全协会 | 108 东莞市信息技术联合会 |
| 76 杭州市网络安全协会 | 109 肇庆市计算机学会 |
| 77 宁波市计算机信息网络安全协会 | 110 汕尾市计算机学会 |
| 78 金华市信息安全协会 | 111 成都信息网络安全协会 |
| 79 金华市信息产业协会 | 112 成都安全可靠信息技术联合会 |
| 80 金华市网商协会 | 113 成都市大数据协会 |
| 81 丽水市信息网络安全协会 | 114 成都物联网产业发展联盟 |
| 82 温州市软件行业协会 | 115 贵阳市信息网络安全协会 |
| 83 洛阳市信息网络安全协会 | 116 贵阳市大数据产业协会 |
| 84 南昌市网络信息安全协会 | 117 曲靖市计算机信息网络安全协会 |
| 85 南昌市互联网创业协会 | 118 玉溪市网络安全协会 |
| 86 扬州市信息网络安全协会 | 119 包头市计算机公共网络安全协会 |
| 87 连云港市计算机信息网络安全协会 | 120 通辽市信息网络安全协会 |
| 88 南通市信息网络安全协会 | 121 南宁市信息网络安全协会 |
| 89 泰州市信息网络安全协会 | 122 网络安全（天津）检测中心 |
| 90 苏州市互联网协会 | 123 青海省网络与信息安全信息通报中心 |
| 91 湘潭市计算机学会 | 124 石河子大学信息科学技术学院 |
| 92 长沙市开福区网络安全协会 | 125 宁夏大学信息工程学院 |
| 93 广州市信息网络安全协会 | 126 重庆信息安全产业研究院 |

- | | |
|-------------------------|---------------------|
| 127 甘肃烽侦网络安全研究院 | 131 江西中证电子数据司法鉴定中心 |
| 128 广东新兴国家网络安全和信息化发展研究院 | 132 四川大学信息安全研究所 |
| 129 广东省现代社会评价科学研究院 | 133 中国计算机学会计算机安全专委会 |
| 130 广东中证声像资料司法鉴定所 | 134 中国联合国采购促进会网信分会 |
| | 135 中国化管理协会网络文化工作委员 |

网络安全感满意度调查



广东新兴国家网络安全和信息化发展研究院

牵头实施单位

全国信息网络安全协会联盟（网安联）

承办单位

广东新兴国家网络安全和信息化发展研究院

技术支撑单位

北京关键信息基础设施安全保护中心

广东关键信息基础设施保护中心

长沙冉星信息科技有限公司（问卷星）

广东中证声像资料司法鉴定所

广州华南信息安全测评中心

部分新闻媒体

参与调查活动的中央及各地方媒体、平台，包括且不限于：

中央电视台《社会与法》频道 《光明日报》

《信息安全与通信保密》 《南方都市报》

《中国信息安全》 人民网

《信息网络安全》 中国网

《信息安全研究》 未来网

《警察技术》 环球网

《经济》 中青在线

《经济参考报》 光明网

《中国财经论坛》 金羊网

《中青报》

部分支持企业和机构

腾讯	哔哩哔哩
阿里巴巴	UC
百度	滴滴
网之易	嘀嗒出行
今日头条	UU 跑腿
抖音	天盈九州
火山小视频	贝壳找房
新浪	房天下
新浪微博	Q 房网
京东	一起住好房
美团	瓜子二手车
拼多多	酷溜网
顺丰速运	珍爱网
苏宁易购	完美世界
魅族	一点资讯
YY 直播	优贝在线
虎牙直播	智联招聘
斗鱼直播	奇虎 360
花椒直播	绿盟
么么直播	亚信安全
快手直播	奇安信
映客直播	安恒
陌陌直播	任子行
酷狗	天融信
迅雷	新华三
TT 语音	圣博润
Hello 语音	炫音网络
荔枝 FM	友迪资讯
vivo	远光软件
oppo	国网思极网安科技（北京）有限公司
金山 WPS	合肥天帷信息安全技术技术有限公司
搜狐	辽宁浪潮创新信息技术有限公司
爱奇艺	深圳市易图资讯股份有限公司

深圳市中手游网络科技有限公司	北京小唱科技有限公司
广州艾媒数聚信息咨询股份有限公司	北京和讯在线信息咨询服务有限公司
韶关家园传媒有限公司	北京光宇在线科技有限责任公司
广东米果传媒有限公司	北京球秘科技有限公司
茂名市群英网络有限公司	北京卓越晨星科技有限公司
广东力通网络科技有限公司	北京白鹭世纪科技股份有限公司
广州九尾信息科技有限公司	北京邦得鼎盛科技有限公司
东莞市阳光网络信息有限公司	北京智启蓝墨信息技术有限公司
有米科技股份有限公司	北京瓦力网络科技有限公司
全通教育集团（广东）股份有限公司	北京文网亿联科技有限公司
广东能龙教育股份有限公司	北京中润互联信息技术有限公司
中山市读书郎电子有限公司	北京思享时光科技有限公司
东方财富信息股份有限公司	盐城市鹤鸣亭传媒股份有限公司
上海基分文化传播有限公司	常州大学常州信息工程学院
上海寻梦信息技术有限公司	常州经开区今创集团
上海喜马拉雅网络科技有限公司	江苏翠起信息科技有限公司
万达信息股份有限公司	四川安洵信息技术有限公司
上海观安信息技术股份有限公司	四川麻辣社区网络传媒有限公司
行吟信息科技（上海）有限公司	成都思维世纪科技有限责任公司
上海浦东软件平台有限公司	北京智游网安科技有限公司
上海纽盾科技股份有限公司	成都创信华通信息技术有限公司
上海阅文信息技术有限公司	成都西维数码科技有限公司
波克科技股份有限公司	成都市锐信安信息安全技术有限公司
上海景域文化传播有限公司	成都安美勤信息技术股份有限公司
上海星艾网络科技有限公司	成都吉胜科技有限责任公司
上海霆懋科技服务有限公司	亚信科技（成都）有限公司
上海东方网股份有限公司	成都卫士通信息产业股份有限公司
上海安阖在创信息科技有限公司	内蒙古信元网络安全技术股份有限公司
上海兴动实业有限公司	黑龙江安信与诚科技开发有限公司
上海谋乐网络科技有限公司	黑龙江亿林网络股份有限公司
上海驭胜信息技术有限公司	哈尔滨安天科技集团股份有限公司
上海御盾信息科技有限公司	哈尔滨蓝易科技有限公司
上海成蹊信息科技有限公司	哈尔滨创新远航科技有限公司
杭州米络科技有限公司	武汉市多比特信息科技有限公司

武汉楚天优游网络科技有限公司	晋信安科技有限公司
湖北盛天网络技术股份有限公司	因弗美讯科技有限公司
安域等保测评公司	上海交通大学党委宣传部
贵阳金峰星际网络科技有限公司	天津市教育委员会
贵州盛世合元科技发展有限公司	宿迁市教育局
贵州数博谷信息技术有限责任公司	无锡市卫生健康委员会
贵阳宏图科技有限公司	内蒙古税务局
大连海川云天信息科技有限公司	国家计算机网络应急技术处理协调中心上海
中冶葫芦岛有色金属集团有限公司	分中心
海城金航网络科技有限公司	上海市网络技术综合应用研究所
浪潮创新科技股份有限公司	上海计算机软件技术开发中心
辽宁北方实验室有限公司	中国民航大学信息安全测评中心
重庆智多信息发展有限公司	广东警官学院
重庆跃动网络技术有限公司	广东轻工业职业技术学院
重庆猪八戒网络有限公司	广东金融学院
南省鼎信信息安全等级测评有限公司	广州大学研究院
上海云辰信息科技有限公司	广州医科大学
珠海网博信息科技股份有限公司	广东药科大学
江苏国瑞信安科技有限公司	广州大学
浙江佰安信息科技有限公司	江苏科技大学
杭州世平信息科技有限公司	江苏大学
湖南红网新媒体集团有限公司	宿迁学院
福建国科信息科技有限公司	江苏省宿迁中学
福州物联网开放实验室有限公司	建湖高级中学
福州闽盾网络与信息安全测评技术有限公司	建湖县第二中学
中科锐眼（天津）科技有限公司	西华大学
清众鑫科技有限公司	吉利学院
大同市利伟科技有限公司	电子科技大学成都学院
大同市华立科技有限责任公司	普宁职业技术学校
山西联创电子信息技术有限公司	揭阳职业技术学院
山西晋城无烟煤矿业集团有限责任公司	潮汕职业技术学院
山西兰花科技创业股份有限公司	中国电信广州分公司
晋城市天狐网络信息有限公司	中国移动广东广州分公司
中创慧安科技有限公司	中国联通广州市分公司

中国电信股份有限公司揭阳分公司	广州珠江实业集团
中国移动通信集团广东有限公司揭阳分公司	广州医药集团
中国联合网络通信有限公司揭阳分公司	广州市第一人民医院
中国联通郑州分公司	广州市第八人民医院
无锡移动	广州市第十二人民医院
宿迁移动	广州市红十字会医院
宿迁电信	中山大学附属第一医院
广东电网公司	中山大学附属第三医院
广州供电局有限公司	中山大学附属肿瘤医院
内蒙古电力集团公司	中山大学孙逸仙纪念医院
中国人民银行宿迁分行	广东药科大学附属第一医院
云南曲靖交通集团有限公司	曲靖市第一人民医院
中国铁路昆明局集团有限公司曲靖站	曲靖市第二人民医院
中国铁路昆明局集团有限公司曲靖北站	广州广电传媒集团
内蒙古公路交通投资发展有限公司	陕西网
广州地铁集团有限公司	群众新闻网
广州市公共交通集团有限公司	爱建湖网
广州港集团有限公司	山西市场导报（媒体）
广汽集团	中山市中山网传媒有限公司
广州燃气集团	深圳新闻网传媒股份有限公司
广州石化	广东足球协会
广州工业发展集团	福建省电子商务协会

广东新兴国家网络安全和信息化发展研究院