2022
广东省数字政府网络安全指数
评估报告

广东省“数字政府”改革建设工作领导小组办公室

2023 年 1 月

组织单位：

广东省“数字政府”改革建设工作领导小组办公室

编写单位：

工业和信息化部电子第五研究所、深信服科技股份有限公司、奇安信科技集团股份有限公司、数字广东网络建设有限公司、广东省网络安全应急响应中心（网络安全 110）、三六零数字安全科技集团有限公司、安天科技集团股份有限公司、公安部第三研究所、广州赛宝认证中心服务有限公司

参编人员：（按姓氏笔画排序）

叶滨、刘丕群、刘启超、李尧、李炜、杨鹏飞、吴寒、沈玉龙、张报明、张浏骅、罗奇伟、金楠、钟世敏、洪延青、贺高戈、耿光刚、高尚省、高智伟、郭勇、唐玉鑫、常晓宇、曾磊、董博、詹林献、雷刚

前　言

加强数字政府建设是引领和驱动数字经济发展的重要动力，是加快数字社会建设步伐的必然要求，是建设网络强国、数字中国的基础性和先导性工程，是推进国家治理体系和治理能力现代化的重要举措。习近平总书记在党的二十大报告中深刻指出，国家安全是民族复兴的根基，社会稳定是国家强盛的前提，强调必须坚定不移贯彻总体国家安全观，把维护国家安全贯穿于党和国家工作各方面全过程，确保国家安全和社会稳定。总书记以马克思主义政治家强烈的忧患意识和历史担当，提出“没有网络安全就没有国家安全；过不了互联网这一关，就过不了长期执政这一关”。习近平总书记关于网络安全的系列重要论述，高屋建瓴、博大精深，为新时代做好数字政府网络安全工作指明了前进方向、提供了根本遵循。

近年，广东省在全国率先启动数字政府改革建设，不断提升数据治理、运营能力和公共数据开发应用水平，优化全省政务信息化体制机制。省级政府一体化政务服务能力在连续三年取得全国第一名的基础上，持续保持全国领先水平，稳居前列。一是以粤省事、粤商通、粤政易为代表的“粤系列”政务服务平台社会和经济成效显著，其中粤省事累计注册实名用户数超过 1.8 亿，粤商通注册用户超过 1341 万，粤

政易注册用户超过253万；二是首创首席数据官制度，强化跨部门、跨层级、跨领域统筹协同机制，并在6个省直部门以及10个地市先行先试；三是首创数据流通交易全周期服务，并在南沙成立广州数据交易所；四是率先推出全国首批数据经纪人名单，以电力、金融领域龙头企业为实验田，探索数据要素流通新模式。

随着数字政府改革建设不断深入，数据流通交易规模快速增长，安全漏洞、数据泄露、网络诈骗、勒索病毒等网络安全威胁日益凸显，有组织、有目的的网络攻击形势愈加明显，为网络安全防护工作带来更多挑战，数字政府面临的网络安全形势愈加严峻复杂。

为贯彻落实党的二十大报告中关于“坚持以新安全格局保障新发展格局”的战略部署，落实国务院《关于加强数字政府建设的指导意见》中提出“构建数字政府全方位安全保障体系”的有关要求，广东省“数字政府”改革建设工作领导小组办公室牵头组织，工业和信息化部电子第五研究所具体负责，深信服、奇安信、数字广东、广东省网络安全应急响应中心、三六零、安天、公安部三所、赛宝认证等单位共同参与，开展了2022年度广东省数字政府网络安全指数评估工作。

本报告是广东省“数字政府”改革建设工作领导小组办公室组织编写的第3部反映广东省数字政府网络安全体系建设状况的研究报告。报告以调查评估数据为基础，梳理分析当前广东省各地市数字政府网络安全的安全现状、存在问题

和工作亮点，推动、指引各地市持续加强网络安全体系建设，推动全省数字政府网络安全工作迈上新台阶、实现新跃升。

本次评估工作得到了广东省委网信办、广东省公安厅、广东省通信管理局的大力支持。在此，衷心感谢各地市政务服务数据管理局、各地市直部门对评估工作的参与和支持，感谢三六零集团、安天集团提供省域网络安全大数据，感谢暨南大学、北京理工大学、西安电子科技大学、国家计算机网络应急技术处理协调中心广东分中心、北京永信至诚科技股份有限公司等单位专家对本报告的帮助以及提出的宝贵意见。

目 录

图目录

表目录

第一章 评估概况

一、评估背景

当今世界正经历百年未有之大变局，国际国内复杂严峻形势与当前新型冠状病毒感染防控工作交织叠加，网络安全风险正在向其他传统安全和非传统安全风险渗透、传递、转化和叠加，网络安全已成为总体国家安全观不可或缺的组成部分。

党的二十大报告指出，要“以新安全格局保障新发展格局”“完善重点领域安全保障体系和重要专项协调指挥体系”。国务院印发的《关于加强数字政府建设的指导意见》指出，要“全面强化数字政府安全管理责任，落实安全管理制度，加快关键核心技术攻关，加强关键信息基础设施安全保障，强化安全防护技术应用，切实筑牢数字政府建设安全防线”。《中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要》指出，要“加强网络安全风险评估和审查，提升网络安全威胁发现、监测预警、应急指挥、攻击溯源能力”。为贯彻落实党中央、国务院关于网络安全的相关要求，省“数字政府”改革建设工作领导小组办公室根据数字政府网络安全指数指标体系（以下简称“指标体系”），组织开展了2022年度数字政府网络安全指数评估工作。

二、评估对象

广东省21个地级市（以下简称“各地市”，如表1-1所示）。

表1-1 广东省21个地级市名称

1	广州	12	中山
2	深圳	13	江门
3	珠海	14	阳江
4	汕头	15	湛江
5	佛山	16	茂名
6	韶关	17	肇庆
7	河源	18	清远
8	梅州	19	潮州
9	惠州	20	揭阳
10	汕尾	21	云浮
11	东莞		

三、评估原则

（一）科学导向。本次评估按照《国务院关于加强数字政府建设的指导意见》提出的“强化安全管理责任、落实安全制度要求、提升安全保障能力、提高自主可控水平”有关要求，通过建立建全指标体系全面评价各地市数字政府网络安全水平，引导、鼓励各地市持续加强网络安全体系建设，推动全省数字政府网络安全工作迈上新台阶、实现新跃升。

（二）数据客观。本次评估依托数字政府建设运营单位掌握的数字政府安全运营数据、网络安全监管部门掌握的数

字政府安全监管数据、安全调研数据、网络安全厂商及互联网公司掌握的省域网络安全大数据、“粤盾-2022”数字政府实战攻防演练结果数据等，采用定量与定性相结合的分析方法，对全省各地市数字政府网络安全管理、安全建设、安全运营、安全效果等四个方面进行评价，客观科学地反映我省各地市数字政府网络安全整体防护水平。

（三）注重实效。本次评估从提升数字政府网络安全防护能力的目标出发，注重数字政府网络安全管理、建设、运营的实际成效，帮助各地市全面掌握当前数字政府安全现状，发现存在的问题，找到解决的方案，形成“执行-评估-反馈-改进”的闭环管理模式。

（四）能力评价。本次评估对各地市数字政府网络安全总体能力进行成熟度分级，成熟度从高至低依次为优化级（S）、完善级（A）、稳健级（B）、受控级（C）、启动级（D）等五个级别。各能力成熟度等级定义见附录。

四、评估过程

2022 年 3 月，广东省“数字政府”改革建设工作领导小组办公室牵头成立评估工作组，制定了 2022 年安全指数评估工作方案。为实现数字政府网络安全指数评估工作整体的规范化和标准化。4 月，广东省政务服务数据管理局联合研究院所、高校、安全厂商等 11 家单位共同编制《广东省数字政府网络安全指数评估实施指南》，帮助评估对象了解广东省数字政府网络安全指数的评估方法和流程，为广东省各地市开展本地化安全指数评估提供参考。7 月至 11 月，评估

工作组采集、处理、分析评估数据，形成安全指数评估结果。

（一）建立指标体系

本年度广东省数字政府网络安全指数评估工作在参照《广东省数字政府网络安全指数指标体系》标准的基础上，重点围绕安全管理、安全建设、安全运营、安全效果 4 个方面，建立面向 21 个地市的评估指标体系，引导各地市有重点地提升数字政府网络安全防护能力。

2022 年度广东省数字政府网络安全指数指标体系共包含 4 项一级指标，24 项二级指标，103 项评估要点，与 2021 年保持一致。

图1-1 广东省数字政府网络安全指数评估模型

安全管理指标用于评价地区数字政府网络安全管理措施是否充分、适宜，主要包含安全战略规划、安全标准规范、安全管理组织、人员安全管理、安全投入以及供应链安全管理 6 个方面。主要从安全规划和管理制度的制定及落实着手，通过强化安全意识，明确安全责任，加大安全投入，使各地市各部门有规可循，从而强化管理、形成闭环。

安全建设指标用于评价地区数字政府网络安全技术措

施是否完备，包含网络安全等级保护、关键信息基础设施保护、数据安全保护、个人信息保护、密码应用以及安全服务支撑体系 6 个方面。主要从注重定级备案和等级测评、重点保护关键信息基础设施和数据安全方面着手，通过聚焦法律法规热点，抓合规、促落实，建立既强调全面又突出重点的技术防护体系。

安全运营指标用于评价数字政府网络安全保障体系在运行过程中的风险识别、安全监测及应急处置等能力，包含信息资产管理、日常安全运维、安全监测、应急处置、安全检查、安全审计、业务连续性保障、安全协同 8 个方面。重点通过摸清资产底数，及时发现风险隐患，采取相应的处置措施，形成联防联控的强大合力，确保数字政府网络安全防护体系稳定运行。

安全效果指标用于评价地区数字政府网络安全保障体系的实际运行效果，包含网络环境安全、安全漏洞、安全事件及专项工作 4 个方面。侧重从结果的角度进行评价，通过安全大数据、安全运营监管数据以及攻防实战演练，反映数字政府安全管理、安全建设及安全运营等方面工作实施效果。

（二）实施指数评估

2022 年 7 月至 11 月，评估工作组对全省 21 个地市数字政府网络安全管理、建设、运营、效果等方面进行了调研，采集了 21 个地市涉及人员、机构、制度、经费、系统以及安全运行维护、省域网络安全大数据、安全应急与通报、“粤盾-2022”数字政府实战攻防演练结果等相关数据约 6.8 万项。

10 月下旬开始，依据评估指标和评估模型，对采集数据进行了全方位分析，形成了安全指数评估结果。

五、数据采集

（一）数据采集对象

本报告的数据采集对象涵盖全省 21 个地市的市直部门，如表 1-2 所示，涉及各地市政务云平台、大数据中心、政府官网及重要政务应用等。数据来源主要为:

（1）数字政府安全运营数据;

（2）网络安全监管部门监管数据;

（3）安全调研数据;

（4）省域网络安全大数据;

（5）“粤盾-2022”广东省数字政府网络安全攻防演练结果。

表1-2 数字政府网络安全评估数据采集的地市市直部门名称

市政府办公厅(室)	市财政局	市交通运输局	市国有资产管理委员会
市发展和改革委(局)	市人力资源和社会保障局	市水务局	市市场监督管理局
市教育局	市自然资源局	市农业农村局	市统计局
市科技创新局	市生态环境局	市商务局	市金融工作局
市工业和信息化局	市医疗保障局	市文化广电旅游体育局	市信访局
市交通运输局	市城市管理和综合执法局	市卫生健康局	市林业和园林局

市公安局	市政务服务数据管理局	市退役军人事务局	……
市民政局	市审计局	市应急管理局	
市司法局	市住房和城乡建设局	市宗教事务局	

（二）数据采集周期

本次评估所采集的数据覆盖周期为：2021 年 11 月至 2022 年 10 月。

第二章 评估结果

一、总体情况

（一）总体指数排名

2022 年广东省数字政府网络安全指数为百分制。其中，安全管理、安全建设、安全运营、安全效果 4 个一级指标分别占 25%、20%、25%、30%。各地市一级指标指数、总体指数及总体排名如表 2-1 所示。

表2-1 广东省地市数字政府网络安全指数得分及排名

地市名称	安全管理指数	安全建设指数	安全运营指数	安全效果指数	总体指数	总体排名
广州	75.74	66.78	82.07	84.95	78.29	2
深圳	90.43	86.32	87.16	78.80	85.30	1
珠海	67.54	62.69	69.49	88.32	73.29	6
汕头	65.14	43.06	64.67	66.33	60.96	11
佛山	64.97	72.05	77.61	84.90	75.53	5
韶关	59.05	35.28	54.55	58.63	53.04	18
湛江	59.66	35.73	54.92	80.78	60.02	12
肇庆	74.52	56.25	80.12	71.88	71.47	9
江门	70.60	52.54	69.98	88.67	72.25	7
茂名	52.39	36.87	59.57	59.31	53.16	17

惠州	78.28	64.38	65.71	92.58	76.65	3
梅州	64.29	55.89	60.61	50.18	57.46	15
汕尾	61.04	52.11	57.12	58.47	57.51	14
河源	56.76	41.36	57.79	69.05	57.63	13
阳江	48.17	29.39	60.82	53.63	49.21	21
清远	50.98	48.01	50.22	53.71	51.01	20
东莞	78.11	62.54	81.30	78.10	75.79	4
中山	63.43	63.02	79.94	78.56	72.02	8
潮州	59.01	40.59	53.98	53.72	52.48	19
揭阳	50.41	47.19	56.61	56.94	53.28	16
云浮	58.24	43.51	67.39	71.83	61.66	10

广东省各地市数字政府网络安全总体指数排名如图 2-1 所示。全省平均值为 64.19，9 个地市超过平均值，占比 42.86%。其中，**深圳市**以总体指数得分 85.30 居全省榜首，**广州市、惠州市、东莞市、佛山市**分列第 2 至 5 名，总体指数得分分别为 78.29、76.65、75.79、75.53，各地安全指数均有一定提升。**惠州市**网络安全指数首次进入前三，惠州市委、市政府领导多次指示批示，强调做好数字政府网络安全工作；分管市领导多次带队检查网络安全工作，现场指导攻防演练活动；同时，惠州在“粤盾-2022”攻防演练表现出色，取得第一名的好成绩。**湛江市**和**揭阳市**相比 2021 年进步较大，其中，湛江市从第 19 名进步至第 12 名，揭阳市从第 21 名进步至第 16 名。2022 年，湛江和揭阳重视数字政府网络安全工作，分管市领导多次主持召开安全指数评估专题调度会，网络安

全工作取得了较好成效，在“粤盾-2022”攻防演练中排名明显提升。

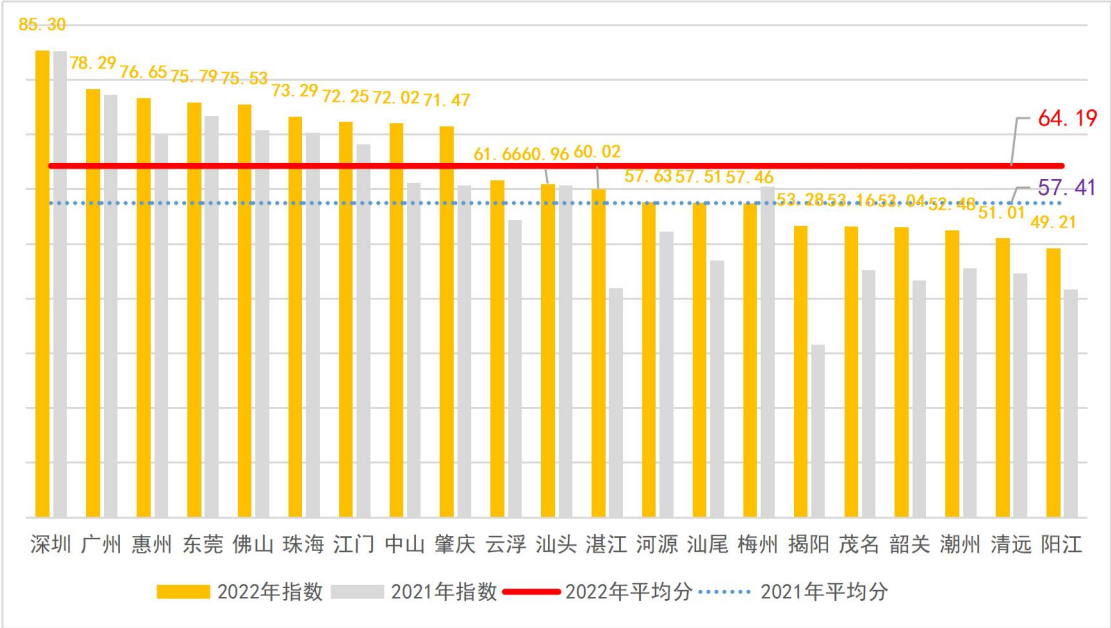

图2-1 广东省各地市数字政府网络安全指数排名

（二）能力水平分布

从安全指数评估结果来看，仍未有地市能够达到**优化级（S）**的水平。总体指数处于**完善级**（A）的有**深圳市，**占比为 4.76%。深圳市数字政府已形成良好的制度、人员、技术等集成应用，并能够通过定性和定量测量跟踪管控措施的实施效果，持续完善管控措施，初步实现综合防御。总体指数处于**稳健级**（B）的有**广州、惠州、东莞、佛山** 4 个地市，占比为 19.05%。这 4 个地市数字政府已形成符合实际的制度规范及配套技术支撑，且组织内外部有较好的协作，初步实现主动防御。总体指数处于**受控级**（C）的有**珠海、江门、中山、肇庆、云浮、汕头、湛江** 7 个地市，占比为 33.33%。这 7 个地市数字政府已建立了基本的制度规范及配套技术措施，但落地执行还不到位，安全效果不稳定。总体指数处于

启动级（D）的有**河源、汕尾、梅州、揭阳、茂名、韶关、潮州、清远、阳江** 9 个地市，占比为 42.86%。这 9 个地市数字政府尚处于管理制度、技术措施和运营体系的初步构建阶段，没有形成稳定的能力。**惠州、东莞、佛山** 3 个地市由受控级（C）升至为稳健级（B），**云浮、湛江** 2 个地市由启动级（D）升至为受控级（C）。

表2-2 广东省地市数字政府网络安全能力分布

优化级（S）	完善级（A）	稳健级（B）	受控级（C）	启动级（D）
	深圳	广州 惠州 东莞 佛山	珠海 江门 中山 肇庆 云浮 汕头 湛江	河源 汕尾 梅州 揭阳 茂名 韶关 潮州 清远 阳江

（三）总体指数分析

2021 年与 2022 年的数字政府网络安全指数一级指标对比情况如图 2-2 所示，2022 年全省数字政府网络安全指数 4 个一级指标均有所提升：一是**安全管理指数小幅增加**，各地市在安全指数工作开展过程中相继出台或制定相应的规划或制度，管理制度相对而言越来越完善，但在供应链安全管理方面还有较大提升空间。二是**安全建设指数进步明显**，虽

然仍为四项一级指标中得分最低的一项，但各地市在2022年纷纷开展数据安全保护探索工作，加大信息系统等级保护备案和测评工作力度，取得了较好的效果。三是**安全运营指数表现良好**，大部分地市加强日常安全运维，监测预警和应急处置机制更加完善，但资产清单还不够清晰，安全审计与业务连续性保障仍需持续改进。四是**安全效果指数稳步提升**，各地市纷纷开展本地区攻防演练活动，并且在“粤盾-2022”攻防演练中，大部分地市整体防御水平与往年相比明显提升。

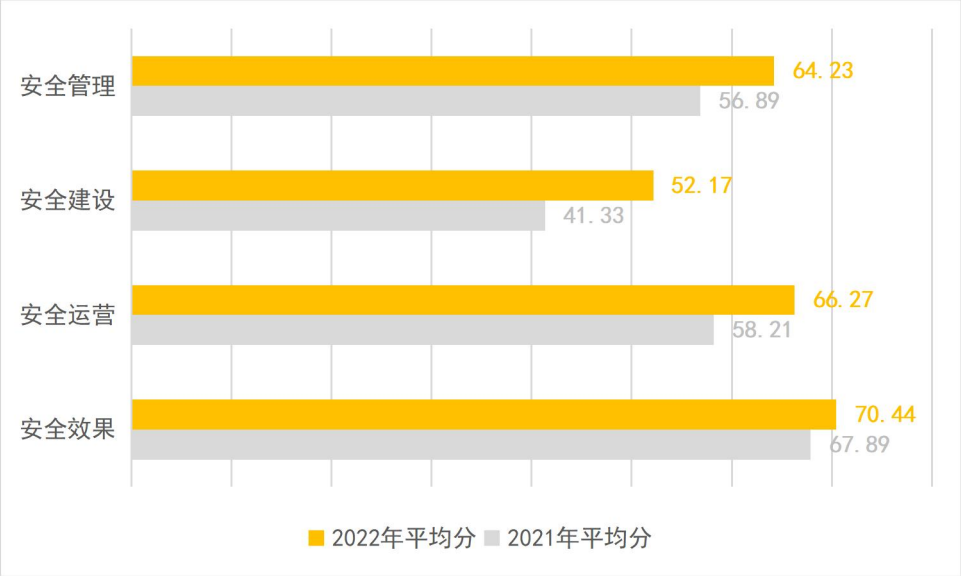

图2-2 数字政府网络安全指数一级指标对比

二、工作成效和存在问题

（一）工作成效

随着政府数字化、智能化的快速发展，网络安全已成为事关国家安全和国家发展的重大战略问题。在网络安全指数评估工作稳步推进的三年中，以网络安全筑牢数字政府改革发展的根基已成为普遍共识。各地市加快开展数字政府网络安全防护体系建设，同时积极探索数字政府网络安全工作的

新思路和新机制，数字政府网络安全取得了良好的发展成效。

一是管理机制日益完善，安全意识明显提升。各地纷纷制定数字政府网络安全相关的战略规划和管理制度，大部分市直部门建立网络安全领导小组，拥有专职的网络安全管理人员。目前，12 个地市发布了电子政务外网网络安全管理办法，部分地市编制了安全指数工作方案或成立安全指数提升工作领导小组，通过指数的引领作用有重点的开展数字政府网络安全工作。此外，2022 年各地市参加数字政府网络安全线上培训人数由 9767 增加至 18927（增涨了 93.79%），通过考试的人数由 8078 增加至 18631（增涨了 130.64%），人员安全意识得到明显提升。

二是安全建设逐步强化，等保工作加快推进。各地市积极开展等级保护、数据安全等相关工作，有条件的地市探索开展重要信息系统保护、个人信息保护和密码应用等工作。尤其在网络安全等级保护方面，市直部门的等保定级备案率较 2021 年翻了一番，等保测评比例也有小幅增长。目前已有 15 个地市探索开展数据分类分级工作，14 个地市探索制定重要数据具体目录，对下一步开展数据安全保护工作奠定了良好的基础。

三是运营能力持续优化，风险防范能力加强。全省各地市持续加强日常安全运维，及时与省平台共享相关运行运维数据，并持续优化网络安全技术体系，部分地市建立了安全监控、事件研判分析、威胁应急处置等安全监测治理闭环管理机制，多部门联合开展网络安全攻防演练、教育培训、安

全宣传等活动，进一步坚实了网络安全“人防”“技防”双防线。

四是攻防演练效果良好，安全漏洞修复及时。“粤盾-2022”攻防演练中，发现并通报了284个网络安全隐患，比2021年、2020年分别减少了71.1%、28.3%，弱口令、一令通行、已知历史漏洞未修复等低级错误发生率大幅减少。有的地市分管市领导专门到地市演练指挥部坐镇指挥；有的地市网信、公安、政数等部门联合行动，集中开展分析研判、监测预警和应急处置工作，与往年相比大部分地市整体防御水平提升明显，体现了广东省数字政府网络安全保障水平的不断提高。

（二）存在问题

数字政府网络安全经过近两年强化和提升，虽然取得了一定的效果和成绩，但是整体网络安全工作仍然存在一些问题，需继续加强能力提升。

一是安全管理制度还不够落地落细落实。随着各地市对网络安全的重视程度不断提高，数字政府网络安全规划及管理制度不断完善，目前大部分地市均制定了数字政府网络安全规划及配套管理办法，但责任不到位、制度未落实仍然是目前亟需改善的现状，安全防护措施层面距离制度规范中提到的安全要求和防护级别仍有较大的差距。如不到30%的市直部门开展安全考核工作，仅有22.82%市直部门与供应商人员签订保密协议，大部分地市对供应链安全管理的认识还不足，未能有效开展供应链风险评估和定期对供应商服务进行安全监控和审计。

二是数据安全建设仍需要加强统筹推进。数字政府的数据资产类型呈多样化，数据载体分布广、数据源众多，这些都给数据识别和分类分级造成困难。目前，已有部分地市探索开展数据分类分级工作，但数据分类分级的科学性和有效性尚未得到实践验证，使得数据安全保护对象不明确，数据安全保护要求不清晰，进而影响数据安全风险评估的有效开展。因此，数据分类分级是数据安全建设工作的当务之急，应加快推动自上而下的数据分类分级安全保护制度建设，结合各地市重要数据特点和安全保护需求，抓住关键风险点对数据进行准确识别。

三是资产底数梳理还不够全面准确清晰。随着广东数字政府迈入 2.0 阶段，数字政府网络空间资产呈指数级增长态势，特别是云上云下资产复杂交织、类型众多。目前，虽然已有不少地市市直部门梳理并建立了信息资产清单，但部分地市市直部门，仍存在资产清单管理不到位、责任归属不明，资产防护强度和范围均存在疏漏的问题。“自身家底”还有待进一步梳理摸清，资产底数准确性、资产清单完整性有待进一步完善，资产漏洞风险排查手段和能力有待持续提升。如在“粤盾-2022”攻防演练中，有近 1/3 的重点靶标存在临时替换靶标、更换所属单位或 IP 地址、无法访问等问题。

四是综合防护水平仍需要巩固完善提升。总体而言，大部分地市的综合防护和纵深防御能力应用还不够深入。只有少数地区已建设配套密码应用支撑能力并开展商用密码应用安全性评估、明确个人信息保护职责并建设相应保障措施。

部分地市虽有一定的应对网络威胁的能力，但对区域划分、边界隔离、终端防护、监测预警等技术防护手段的综合应用不充分，对网络战级别的实战能力仍显著不足，面对 APT、零日漏洞的发现能力弱，整体联防联控、网络对抗反制能力和极限生存能力仍处于初级阶段。

第三章 安全管理指数

一、总体分析

如图 3-1 所示，在安全管理的二级指标中，安全战略规划指数的平均值为 78.29，10 个地市超过平均值，占比 47.62%；安全标准规范指数平均值为 65.77，11 个地市超过平均值，占比 52.38%；安全管理组织指数的平均值为 63.52，10 个地市超过平均值，占比 47.62%；人员安全管理指数的平均值为 57.12，9 个地市超过平均值，占比 42.86 %；安全投入指数的平均值为 70.18，11 个地市超过平均值，占比 52.38%；供应链安全管理指数的平均值为 48.45，8 个地市超过平均值，占比 38.10%。

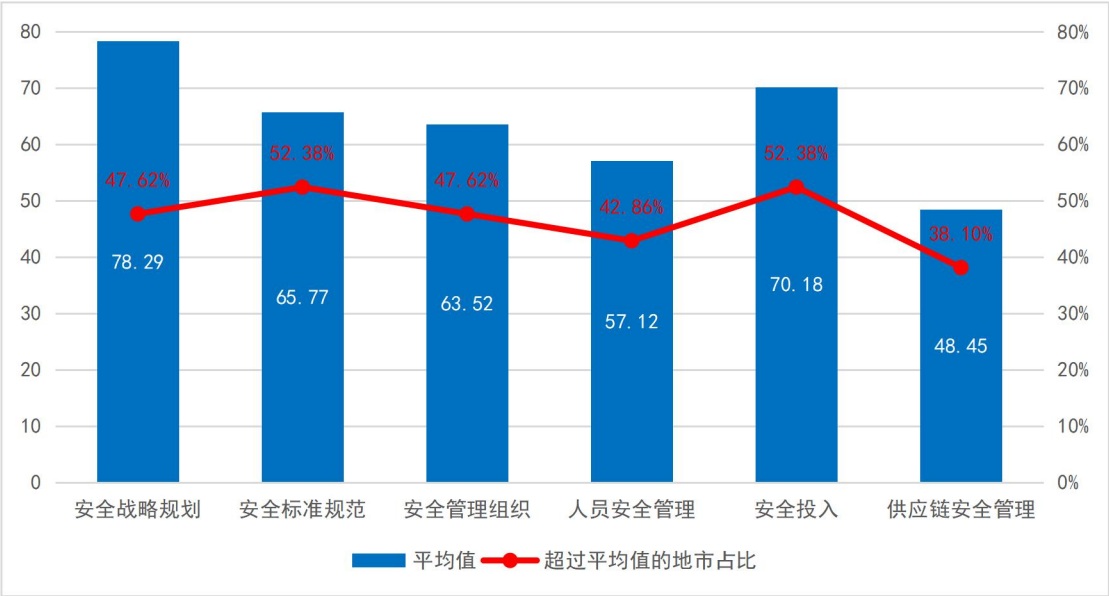

图3-1 安全管理二级指标指数平均值分析

与 2021 年相比，全省数字政府网络安全管理工作取得进一步成效，主要表现在：**一是**编制数字政府网络安全战略规划的地市由 18 个增加至 21 个；**二是**编制数字政府网络安全管理办法的地市由 13 个增加至 18 个；**三是**地市政务服务数据管理部门组织开展的安全意识、技能教育和培训的次数由 31 次增加至 57 次；**四是**参加省政务服务数据管理局组织的网络安全意识、管理、技能培训的人次由 9767 增加至 18927，通过考试的人次由 8078 增加至 18631，考试合格率由 82.71%增加至 98.44%；**五是**明确供应商安全职责的市直部门数量占比由 36.17%增加至 57.88%。

如图 3-2 所示，全省 21 个地市安全管理指数的平均值为 64.23，10 个地市超过平均值。其中，网络安全管理指数处于**完善级（A）**的有深圳市，占比为 4.76%；网络安全管理指数处于**稳健级（B）**的有惠州、东莞、广州 3 个地市，占比 14.29%；网络安全管理指数处于**受控级（C）**的有肇庆、江门、珠海、汕头、佛山、梅州、中山、汕尾 8 个地市，占比 38.10%；网络安全管理指数处于**启动级（D）**的为其余 9 个地市，占比 42.86%。

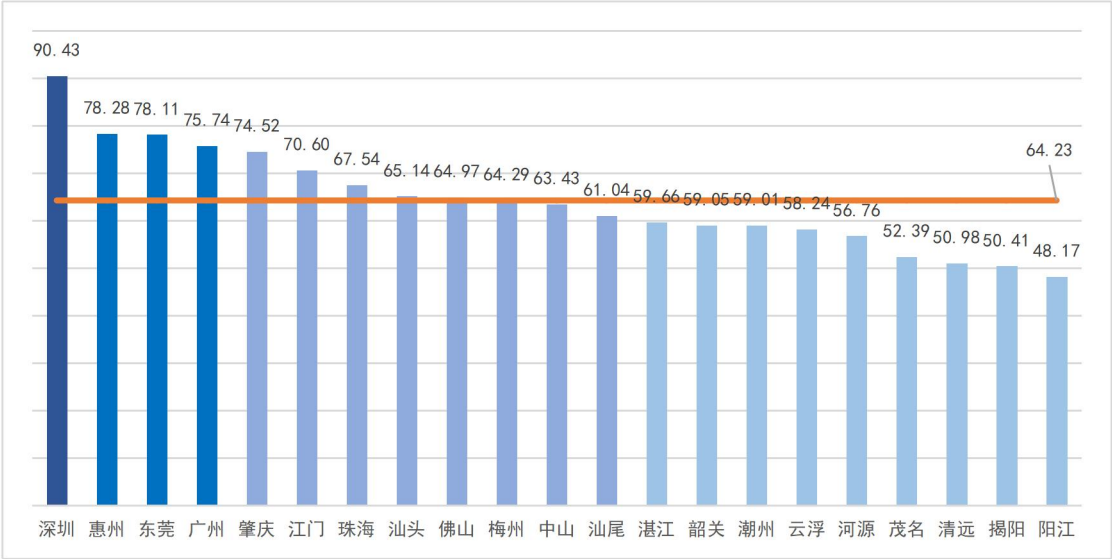

图3-2 广东省数字政府安全管理指数排名

分析发现，**深圳**等表现良好的地市制定了地区数字政府网络安全总体规划、指引或规范等，统筹开展本地区的网络安全工作。同时，大部分市直部门建立了较为完善的网络安全管理制度，成立了网络安全领导小组，注重提升安全意识，强化人员安全管理，加大了安全投入。

表现不太理想的地市网络安全管理工作仍有差距。**一是**顶层设计依旧不完善，仍有 10 个地市未编制网络安全规划的具体实施方案，未印发地市级政务外网网络安全指引；**二是**安全管理责任落实不到位，11 个地市超过 70%的市直部门未成立数据安全领导小组，11 个地市超过 50%的市直部门未制定网络安全工作责任制实施细则，4 个地市近 70%的市直部门没有专职安全管理人员；**三是**人员安全管理依旧不足，13 个地市超过 70%的市直部门未开展人员考核及奖惩工作，18 个地市超过 60%的市直部门未落实与供应商人员签订保密协议，9 个地市超过 60%的市直部门未对供应商人员开展安全教育培训；**四是**供应链安全管理水平较低，仍有 15 个

地市超过 70%的市直部门未开展供应链网络安全风险评估，9 个地市超过 50%的市直部门未明确供应商安全职责，13 个地市超过 70%的市直部门未开展供应商监控和评价。

二、分指数分析

（一）安全战略规划

安全战略规划指数主要评价网络安全战略方针、战略目标的明确程度和网络安全规划制定及实施情况。2022 年重点关注是否制定网络安全总体规划以及配套的实施方案。

如图 3-3 所示，全省 21 个地市安全战略规划指数平均值为 78.29，10 个地市超过平均值。其中，珠海、湛江、肇庆、惠州、梅州、阳江、东莞、潮州、深圳、江门 10 个地市明确了本地区数字政府网络安全的总体目标，编制了网络安全规划文件，部分制定了网络安全规划配套的实施方案，表现良好；揭阳、广州、汕头、韶关、汕尾、河源、中山 7 个地市表现中等；其余地市表现不太理想。

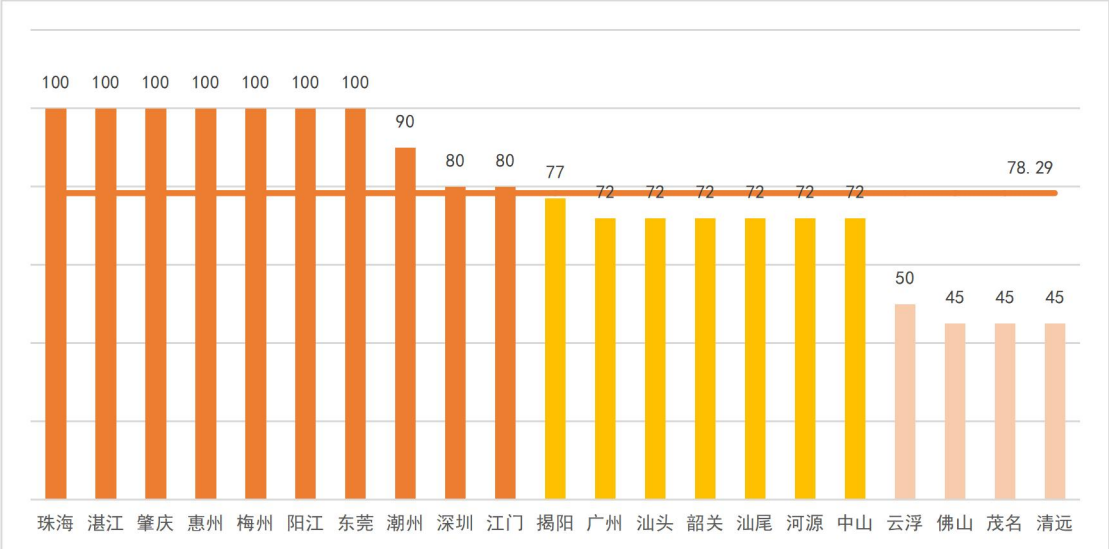

图3-3 广东省数字政府安全战略规划指数排名

各地市良好实践主要表现在：一是**深圳、珠海、湛江、肇庆、江门、惠州、梅州、阳江、东莞、潮州**编制了地市数字政府网络安全规划、行动计划、工作方案等，明确了网络安全总体目标和工作任务。二是**珠海、湛江、肇庆、惠州、梅州、阳江、东莞**制定了网络安全规划配套的实施方案，明确了数字政府网络安全各项工作的阶段任务、分工及时间节点等，确保网络安全各项工作有序推进和顺利实施。

各地市可参考以下建议开展安全战略规划与实施工作：**一是**根据地区数字政府网络安全现状，明确网络安全战略目标，制定并发布网络安全战略或规划，并为规划实施提供必要的资源保障；**二是**跟踪检查网络安全战略落实情况，对实施情况进行评估，同时对网络安全现状与战略目标进行对比，根据存在的差距对工作任务进行优先级排序，并提供必要的资源和资金保障，推动战略有效落地实施；**三是**进一步梳理地区数字政府建设和网络安全现状，根据数字政府改革建设和网络安全体系建设等方面的需求，定期进行网络安全规划的修订。

（二）安全标准规范

安全标准规范指数主要评价地区数字政府网络安全指引及标准规范制定情况，部门数字政府网络安全管理制度制定情况。2022年重点关注是否发布地区数字政府网络安全标准规范，以及市直部门是否建立并发布体系化的网络安全管理制度。

如图3-4所示，全省21个地市安全标准规范指数的平均值

为65.77，11个地市超过平均值。其中，深圳、汕头、惠州、珠海、肇庆5个地市发布了地区级数字政府网络安全行业指引或标准规范，并且地市政务服务数据管理部门指导、督促各市直部门建立了较完善的网络安全管理制度，表现良好；中山、东莞、广州、韶关、河源、云浮、江门、茂名、潮州、梅州、湛江11个地市表现中等；其余地市表现不太理想。

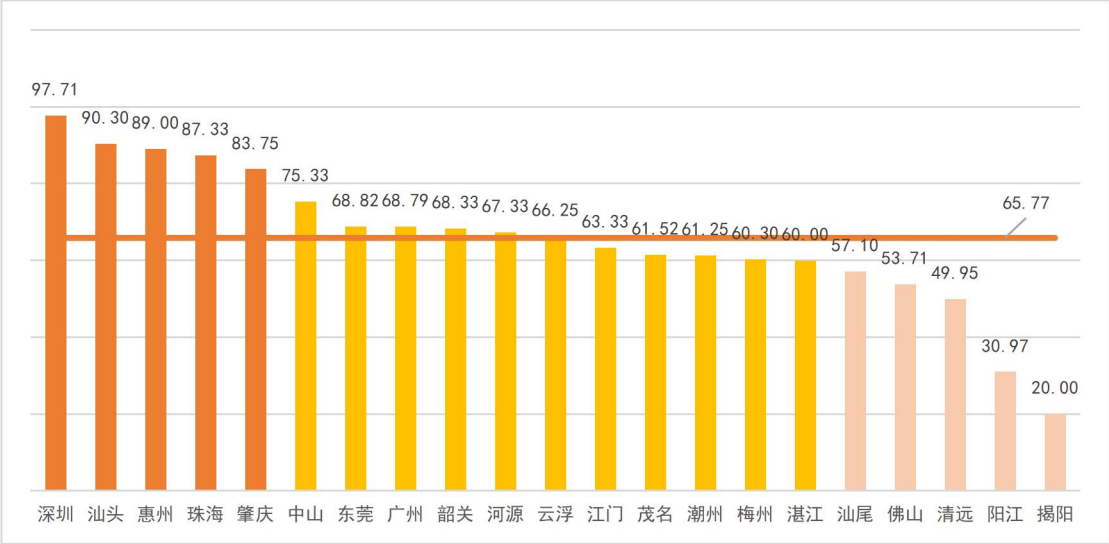

图3-4 广东省数字政府安全标准规范指数排名

各地市良好实践主要表现在：一是**深圳**参考《广东省数字政府网络安全指数指标体系》，融合供应链安全、数据安全和涉疫系统安全等，编制了《深圳市党政机关网络安全指数指标》，为全市各单位提供网络安全建设指导。二是**珠海**发布了《数字政府网络安全防护指南》，指导各部门高效精准地开展网络安全工作。

各地市可参考以下建议开展标准规范制定工作：**一是**充分落实国家、广东省网络安全相关法律法规、标准规范等，制定地市级网络安全指引或标准规范，完善地区网络安全管理机制；**二是**各部门依照网络安全相关法律法规、标准规范

要求，结合网络安全管理现状，建立由安全策略、管理规范、操作手册、记录表单等构成的数字政府四级安全管理制度体系；**三是**严格落实各项管理制度要求，依照要求开展网络安全各项工作，同时，通过定期的风险评估、监督检查、安全审计等，检查各项制度实施情况，确保安全工作合规开展。

（三）安全管理组织

安全管理组织指数主要评价网络安全管理组织的健全性，数据安全负责人和管理机构明确程度，数字政府相关参与方网络安全工作责任的明晰程度，部门内部业务处（科）室与安全管理处（科）室的安全职责分工的明晰程度，网络安全管理人员配备情况，网络安全管理人员职责分工明确程度以及网络安全专家队伍和智库机构的建设情况等方面。2022 年重点关注地区是否明确数字政府相关参与方网络安全工作责任，市直部门是否明确相关部门与人员的安全责任与分工。

如图 3-5 所示，全省 21 个地市安全管理组织指数的平均值为 63.52，10 个地市超过平均值。其中，深圳、肇庆、惠州 3 个地市明确了数字政府相关参与方的网络安全工作责任，地区大部分市直部门成立了网络安全领导小组，明确了相关部门以及安全管理人员的职责，表现良好；广州、东莞、茂名、江门、汕头、云浮、河源、佛山、清远 9 个地市表现中等；其余地市表现不太理想。

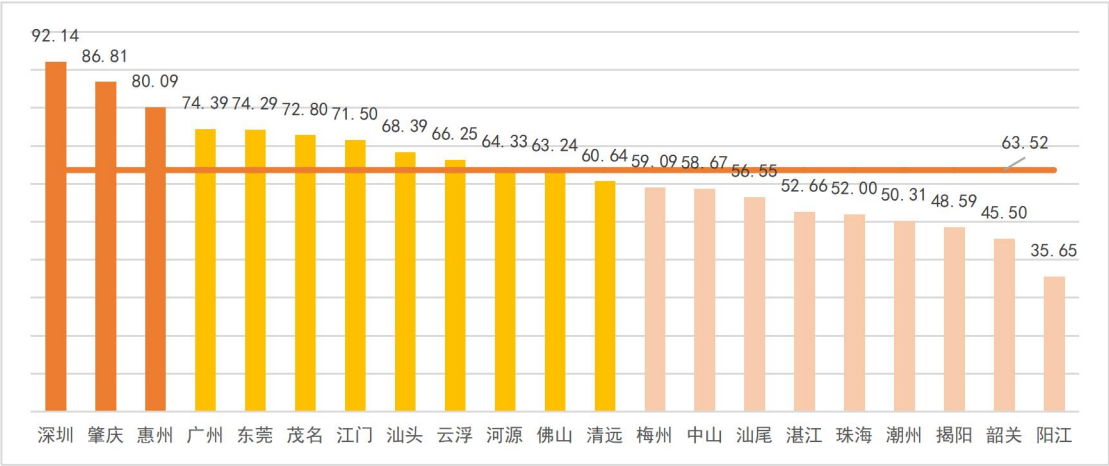

图3-5 广东省数字政府安全管理组织指数排名

各地市良好实践主要表现在：一是**广州、深圳、汕头、湛江、肇庆、江门、茂名、惠州、梅州、河源、东莞、中山、潮州**均通过印发地市级电子政务外网网络安全相关文件，明确了数字政府相关参与方的网络安全工作职责。二是**深圳**超过90%的市直部门成立了网络安全领导小组，拥有专职安全管理人员。三是**梅州**组建了数字政府网络信息安全专家库，聘任领域专家学者、领军人才等，为信息安全工作提供决策咨询和技术支撑。

各地市可参考以下建议开展安全管理组织建设工作：**一是**各地应将数字政府相关参与方的网络安全责任及分工文件化、制度化，确保政务外网、政务大数据中心及政务云相关参与方责任边界清晰；**二是**各部门通过建立网络安全、数据安全领导小组，建立权责明确且内部沟通顺畅的网络安全管理组织，确保网络安全各项工作顺利开展；**三是**参照省级数字政府网络安全工作责任要求，贯彻落实网络安全工作责任制实施细则，明确和落实各部门党组领导班子和领导干部网络安全工作责任；**四是**设置足够多的网络安全专、兼职岗

位，明确岗位职责、任职要求等，持续推动网络安全队伍建设；**五是**邀请在数字政府、网络安全领域具有一定影响力的专家、学者、专业技术人才等，组建数字政府网络安全专家委员会，对数字政府网络安全体系建设中的重大决策及问题，提供决策咨询支撑。

（四）人员安全管理

人员安全管理指数主要评价安全意识、安全技能教育、培训和宣传工作开展情况，安全考核与奖惩工作开展情况，供应商人员的背景调查、保密协议签订、安全培训教育等安全管理情况。2022年重点关注参加省政务服务数据管理部门组织的网络安全培训的学习及效果评价情况，市直部门是否开展安全考核与奖惩、供应商人员安全管理工作。

如图3-6所示，全省21个地市人员安全管理指数的平均值为57.12，9个地市超过平均值。其中，深圳注重安全意识教育和技能培训，持续开展人员（含供应商人员）安全管理，强化了网络安全考核与奖惩，表现良好；广州、惠州、佛山、梅州、云浮、东莞、中山7个地市表现中等；其余地市表现不太理想。

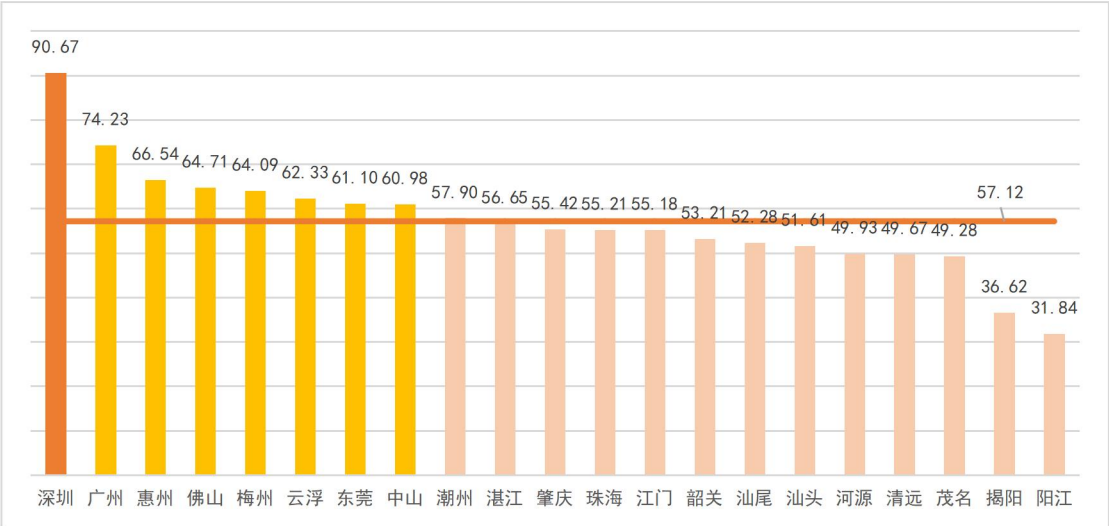

图3-6 广东省数字政府人员安全管理指数排名

各地市良好实践主要表现在：一是大力加强网络安全意识教育和技能培训，在2022年全省数字政府网络安全意识及技能线上培训中，**广州、深圳、珠海、佛山、韶关、肇庆、江门、惠州、梅州、汕尾、河源、东莞、中山、潮州、揭阳、云浮**整体考试合格率超过98%。特别是**广州、深圳、梅州、河源**等地市政务服务数据管理部门组织有力，各市直部门和人员培训参与度高、覆盖面广，培训效果好。此外，**梅州市**还建成了全省首个网络安全主题公园，在全市开展网络安全宣传活动，营造了良好的网络安全氛围。二是强化人员安全管理，如**珠海**市政府办公室牵头汇总各部门网络安全联系人，形成全市各部门网络安全人员库。

各地市可参考以下建议开展人员安全管理工作：**一是**完善人员安全教育和培训制度，充分利用数字政府课堂、广东省网络培训学院等积极开展线上线下网络安全教育和宣传活动，积极组织各部门参加省政务服务数据管理局组织的网络安全意识和技能培训，将人员在省培训中的考试参加率和

通过率纳入部门考核；**二是**进一步明确网络安全人员安全工作考核的原则、内容、组织形式以及问责机制等，夯实不同岗位人员安全责任；**三是**建立供应商人员管理机制，确保与供应商服务人员签订保密协议，定期对供应商人员开展网络安全教育与意识培训，明确供应商人员安全职责，避免人因导致的网络安全问题。

（五）安全投入

安全投入指数主要评价数字政府新建信息化项目的网络安全预算情况，以及安全日常运维、教育培训、安全防护加固、风险评估、升级运维、应急处置等网络安全保障工作经费落实情况。2022 年重点关注新建政务信息化项目网络安全建设投资占比，以及年度网络安全预算经费的落实情况。

如图 3-7 所示，全省 21 个地市安全投入指数的平均值为 70.18，11 个地市超过平均值。其中，深圳、广州、东莞、佛山 4 个地市比较注重网络安全经费投入，表现良好；江门、肇庆、惠州、珠海、汕尾、汕头、中山、揭阳、韶关、梅州、潮州 11 个地市表现中等；其余地市表现不太理想。

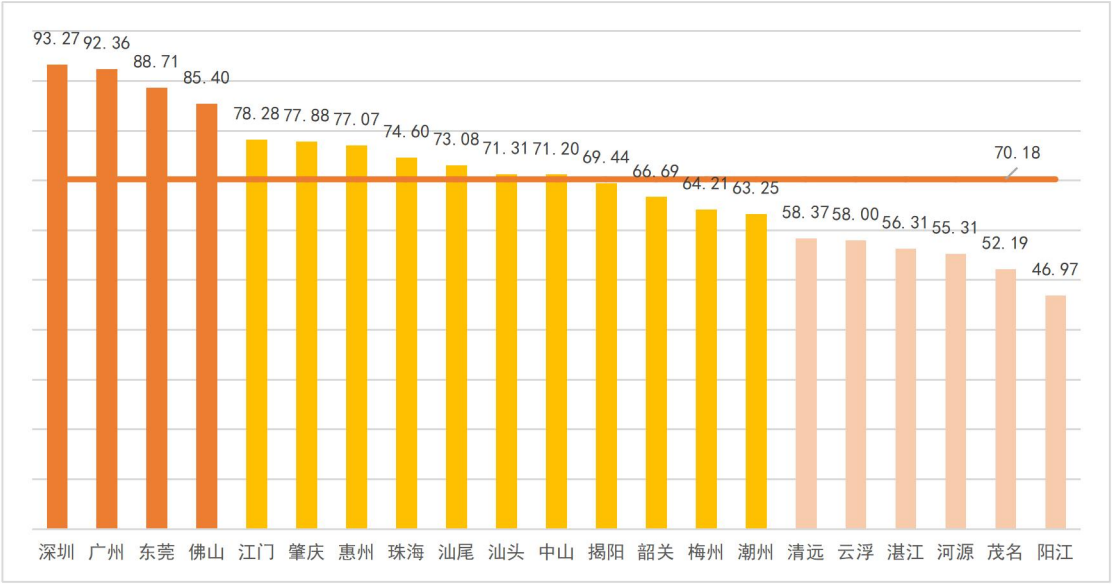

图3-7 广东省数字政府安全投入指数排名

各地市良好实践主要表现在：一是**深圳**深化网络安全立项审批管理改革，由市政务服务数据管理局统筹网络安全预算支出，要求新建信息化项目网络安全投入占比不低于5%。二是**东莞**将“新建信息化项目的网络安全投入占比不低于5%”的要求纳入网络安全工作责任制考核中，网络安全建设投入占比连续四年超过11%。

各地市可参考以下建议开展安全投入工作：**一是**加大数字政府网络安全建设资金支持力度，落实国家、省关于网络安全建设经费的要求，确保网络安全投入占全部信息化投入的比例不少于5%的最低要求；**二是**加大对安全日常运维、安全教育培训、安全防护加固、安全风险评估和应急处置等服务资金保障。

（六）供应链安全管理

供应链安全管理指数主要评价供应链风险评估开展情况，采购的产品和服务是否符合国家相关安全规定，供应商

安全职责是否明确，供应商服务安全监控和审计机制建立及执行情况，供应商的安全评价机制建立及执行情况。2022 年重点关注是否开展供应链风险评估，是否明确供应商安全职责。

如图 3-8 所示，全省 21 个地市供应链安全管理指数的平均值为 48.45，8 个地市超过平均值。其中，深圳开展了供应链安全管理和供应商管理的良好实践和探索，表现良好；江门、东莞、惠州、佛山、广州 5 个地市表现中等；其他地市表现不太理想。

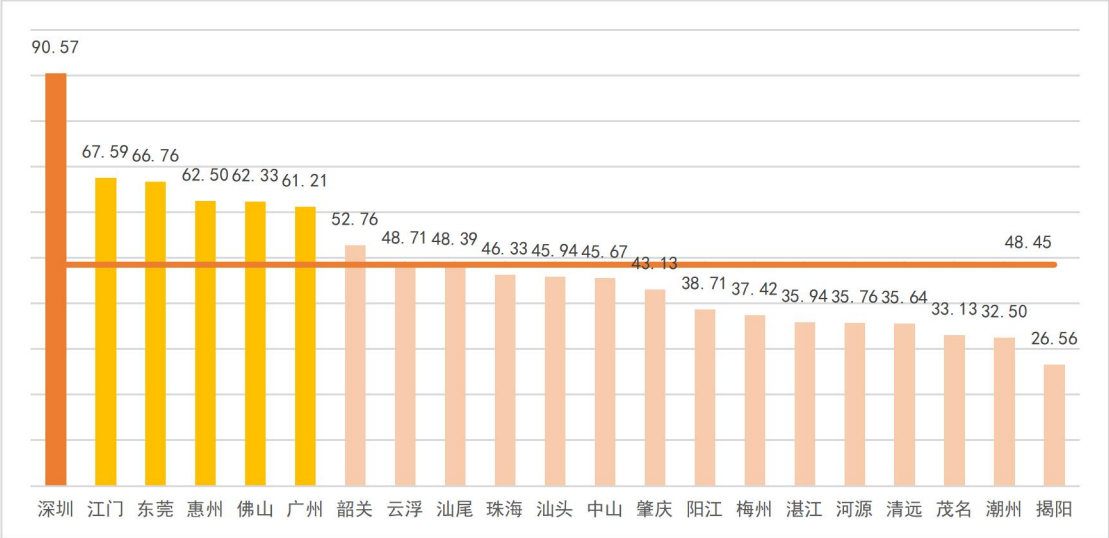

图3-8 广东省数字政府供应链安全管理指数排名

各地市良好实践主要表现在：一是**深圳**通过编制《深圳市数字政府供应链安全管理办法》，加强对地市数字政府供应链安全管理的统筹推进，为各部门提供统一的标准规范。二是**江门**市政务服务数据管理局联合各主管、监管部门要求各部门建立外包或委托服务安全管理机制，与受托方签订保密协议，压实服务供应商安全责任。

各地市可参考以下建议开展供应链安全管理工作：**一是**

组织专题研究市级政务信息化项目供应链安全管理工作，推动制定地区数字政府服务供应商安全管理要求指南，指导各部门约束服务供应商行为安全合规；**二是**推动各部门加强服务供应商安全管理力度，加强服务供应商合同条款的约束，明确服务供应商应承担的相关网络安全责任，推动服务供应商加强人员、源代码、资产管理、日常运维等安全管理；**三是**加强供应商监督管理及跟踪评价，通过背景审查、资质认定、定期审计等，确保供应商履行网络安全保障义务与责任。

第四章 安全建设指数

一、总体分析

如图 4-1 所示，在安全建设的二级指标中，网络安全等级保护指数的平均值为 67.23，8 个地市超过平均值，占比 38.10%；关键信息基础设施保护指数的平均值为 49.23，9 个地市超过平均值，占比 42.86%；数据安全保护指数的平均值为 39.22，12 个地市超过平均值，占比为 57.14%；个人信息保护指数的平均值为 41.39，8 个地市超过平均值，占比 38.10%；密码应用指数的平均值为 46.97，14 个地市超过平均值，占比 66.67%；安全服务支撑体系指数的平均值为 51.06，10 个地市超过平均值，占比 47.62%。

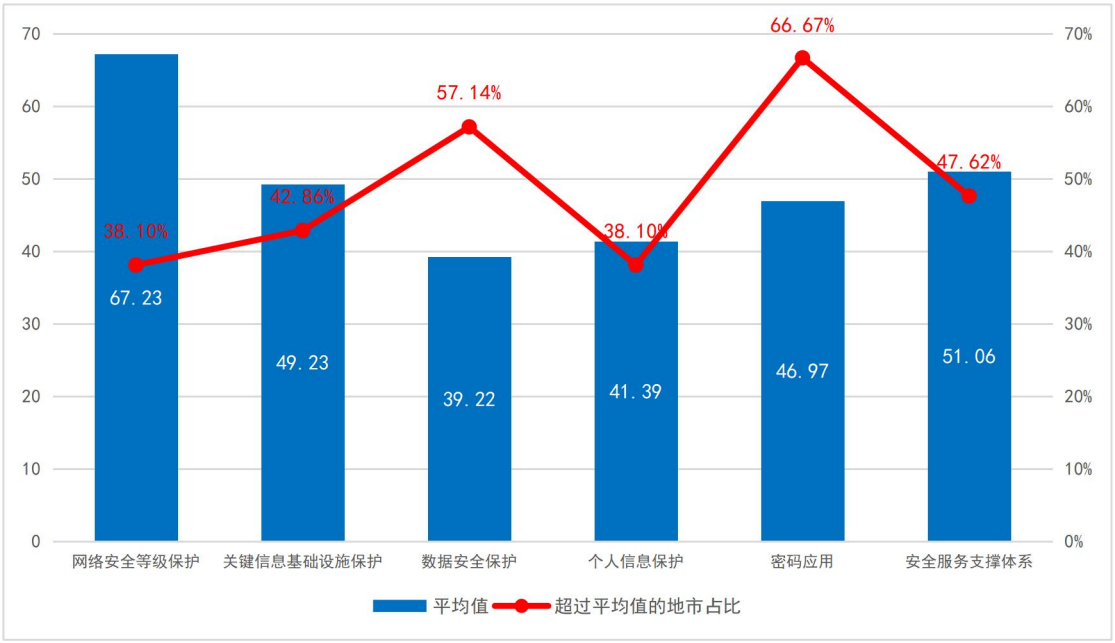

图4-1 安全建设二级指标指数平均值分析

与 2021 年相比，全省数字政府网络安全建设工作取得较大进展，主要表现在：**一是**政务信息系统等级保护定级备案率由 2021 年的 30.28%增加至 60.16%，定期测评率由 2021 年的 46.61%增加至 49.80%，在备案率大幅增长的情况下，测评率仍有小幅提升；**二是**全省有 15 个地市探索开展政务数据分类分级，14 个地市探索建立重要数据具体目录；**三是**明确个人信息保护责任部门的市直部门由 15.40%增加至 35.89%；**四是**全省探索建设政务云配套密码应用保障能力的地市由 12 个增加至 19 个。

如图 4-2 所示，全省 21 个地市安全建设指数的平均值为 52.17，10 个地市得分超过平均值。其中，网络安全建设指数处于**完善级（A）**的有深圳市，占比为 4.76%；网络安全建设指数处于**受控级（C）**的有佛山、广州、惠州、中山、珠海、东莞 6 个地市，占比 28.57%；网络安全建设指数处于**启动级（D）**的为其余 14 个地市，占比 66.67%。

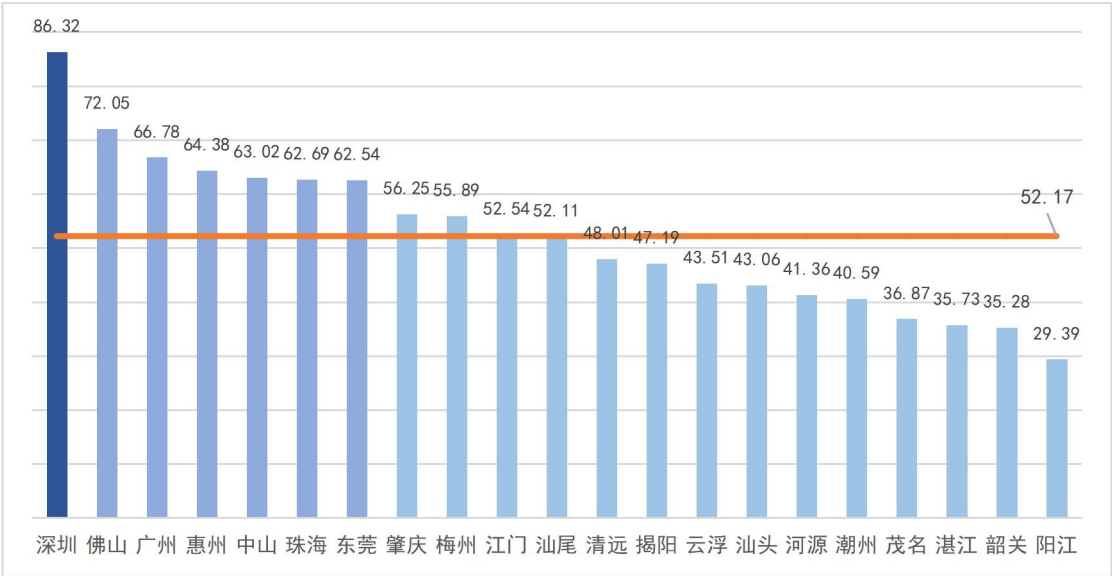

图4-2 广东省数字政府安全建设指数排名

分析发现，**深圳**等表现相对较好的地市等级保护定级备

案率和定期测评率较高，探索开展了数据分类分级防护，明确了数据安全和个人信息保护职责，初步开展了密码资源池建设和密码改造，拥有比较完善的服务支撑体系。

表现不太理想的地市安全建设工作亟待加强。一**是**等级保护技术要求仍需进一步落实，7 个地市超过 70%的市直部门未落实政务外网分区防御、内外部逻辑隔离防护要求；**二是**数据保护工作有待深入，12 个地市建设数据加密、脱敏、防泄漏、数字水印技术手段的市直部门不足 30%；**三是**个人信息保护仍处于起步阶段，12 个地市超过 70%的市直部门未明确个人信息保护的责任部门，20 个地市开展个人信息安全影响评估的市直部门数量不足 10%；**四是**密码应用工作有待开展，只有少数地市建成政务云配套的密码应用保障能力并应用；**五是**安全服务支撑体系有待完善，13 个地市超过 50%的市直部门尚未有完善的网络安全咨询、设计、集成、运维等服务体系。

二、分指数分析

（一）网络安全等级保护

网络安全等级保护指数主要评价政务信息系统等级保护定级备案情况、等级保护测评及整改情况、政务信息系统上线前安全测评以及政务外网分区防御、内部逻辑隔离、互联网出口安全管控等安全技术要求落实情况。2022 年重点关注政务信息系统定级备案及定期测评情况。

如图 4-3 所示，全省 21 个地市网络安全等级保护指数的平均值为 67.23，8 个地市超过平均值。其中，深圳、佛山、

中山 3 个地市重视网络安全等级保护工作，积极主动开展等级保护备案和定期测评，并落实相关安全技术要求，表现良好；惠州、肇庆、潮州、珠海、江门、清远、湛江、韶关、广州、梅州、汕头、东莞、云浮 13 个地市表现中等；其余地市表现不太理想。

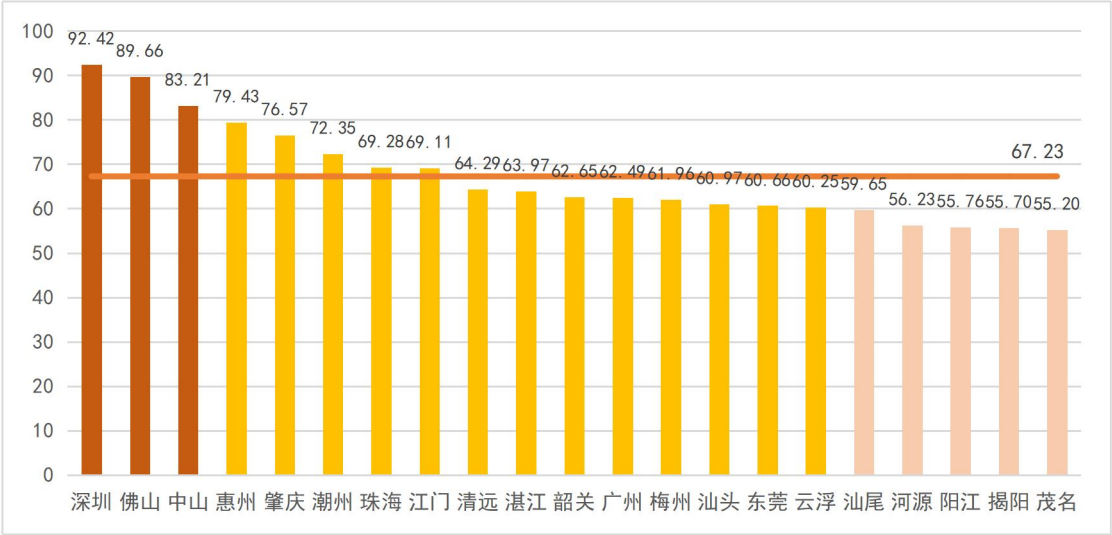

图4-3 广东省数字政府网络安全等级保护指数排名

各地市良好实践主要表现在：一是**深圳、佛山**加强网络安全等级保护工作和经费保障，督促各单位落实等级保护建设要求。在 2022 年全省政务系统等保定级备案率为 60.16%，定期测评率为 29.96%的情况下，深圳、佛山定级备案率和定期测评率均大幅超过全省平均水平。二是**中山**开展政务信息化项目统一等保测评，实现政务信息系统统筹规划合规检查和网络安全测评。

各地市可参考以下建议持续深化网络安全等级保护工作：**一是**扩大等级保护工作覆盖面，按照国家、省相关法规标准要求，加强政务信息系统定级备案，积极落实相关安全技术防护措施，定期开展测评；**二是**按照标准要求，等保二

级及以上系统定期进行等保测评，并根据测评结果和意见建议，开展整改加固和检查优化，提升安全防护能力；**三是**严格按照要求，落实政务信息系统必须开展上线前安全测评。

（二）关键信息基础设施保护

关键信息基础设施保护指数主要评价关键信息基础设施清单建立情况，关键信息基础设施边界防护技术、访问控制、容灾备份建设等重要安全技术要求落实情况。2022 年重点关注是否探索开展本行业重要政务信息系统认定及安全保护工作。

如图 4-4 所示，全省 21 个地市关键信息基础设施保护指数的平均值为 49.23，9 个地市超过平均值。其中，广州、佛山、东莞、深圳、江门 6 个地市表现中等；其余地市表现不太理想。关键信息基础设施保护工作整体有较大提升空间，广州、深圳、佛山、江门和东莞参照国家关键信息基础设施保护相关法规标准探索开展了重要政务信息系统保护工作。

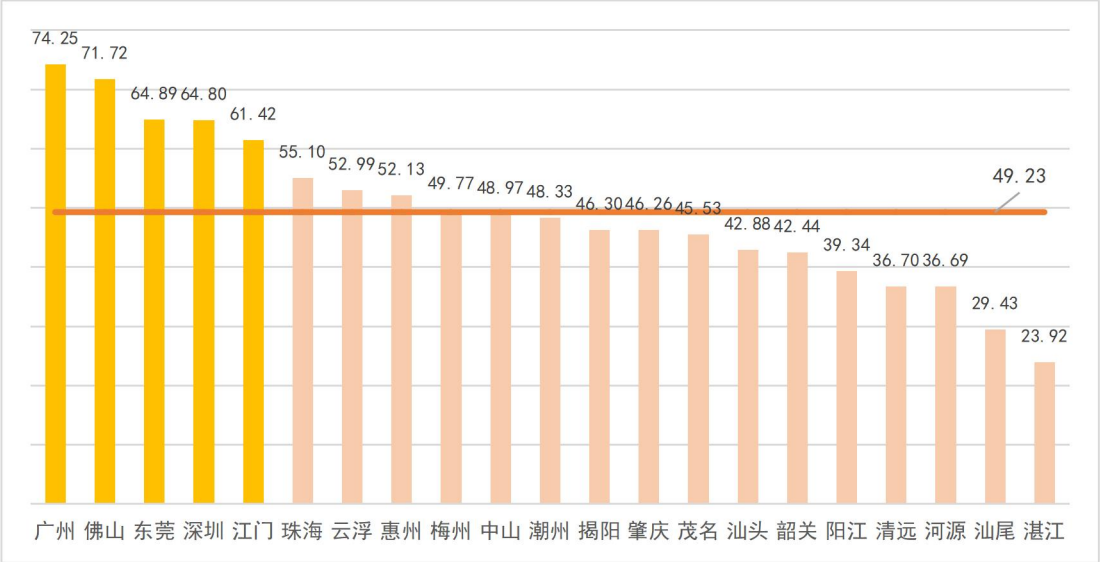

图4-4 广东省数字政府关键信息基础设施保护指数排名

建议各地市参考以下实践持续探索开展重要政务信息

系统安全保护工作：**一是**参照《关键信息基础设施安全保护条例》《信息安全技术 关键信息基础设施安全保护要求》，开展重要政务信息系统的调研与摸排，探索开展重要政务信息系统识别和认定工作，梳理重要政务信息系统清单；**二是**从分析识别、安全防护、监测评估、监测预警、主动防御以及事件处置等方面，明确重要政务信息系统保护要求，采取必要措施保护重要政务信息系统业务连续运行；**三是**网信、公安、政数等部门联合开展重要政务信息系统监督检查，督促各项安全保护措施落地落实，切实加强重要政务信息系统安全保护。

（三）数据安全保护

数据安全保护指数主要评价数据分类分级标准规范的建立及执行情况、重要数据目录准确性和完整性情况、重要数据安全技术要求建设情况、全流程数据安全管理制度建设情况、数据安全风险评估开展情况、政务数据开放共享管理机制建设情况、重要政务数据安全开发管理机制建设情况、重要数据的出境安全管理制度落实情况。2022 年重点关注是否对数据探索进行分类分级，是否建设数据安全技术防护措施。

如图 4-5 所示，全省 21 个地市数据安全保护指数的平均值为 39.22，12 个地市超过平均值。其中，深圳探索开展了政务数据分类分级，建设了部分数据安全管理制度和数据加密、脱敏、防泄漏等技术手段，表现良好；广州表现中等；其余地市表现不太理想。数据安全保护工作仍有很大的提升

空间。

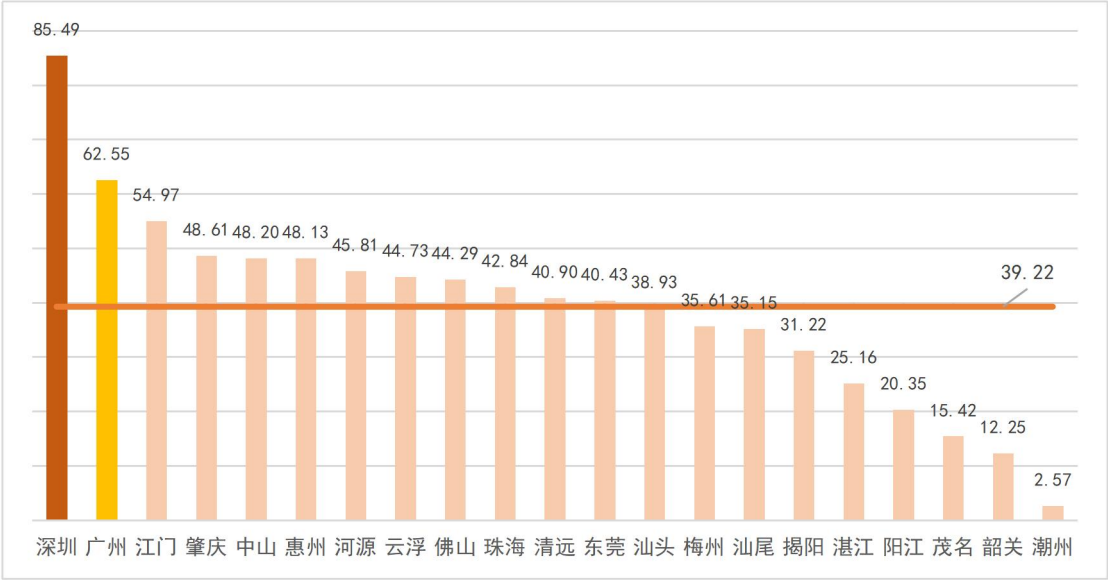

图4-5 广东省数字政府数据安全保护指数排名

各地市良好实践主要表现在：一是**深圳**编制印发《公共数据安全要求》及配套实施指南，指导开展数据全生命周期安全建设；打造涵盖数据脱敏溯源、泄露防护、风险监测、安全审计、密钥管理、数据库安全运维等功能的数据安全与大数据平台，推动数据安全能力平台化、服务化；开展全市党政机关数据安全自查专项行动，为全市各单位数据安全建设提供指导。二是**东莞**建成政务数据大脑，部署数据完整性检测、存储加密、备份恢复等防护措施，开展数据全生命周期安全防护治理。

各地市可参考以下建议开展数据安全保护工作：**一是**参照国家和广东省相关要求，编制地区政务数据分类分级指南，明确不同类别、不同级别数据的安全保护要求，建立数据目录清单，摸清数据资产底数，组织开展数据分类分级保护工作；**二是**利用数据安全工作协调机制的统筹优势，督导各部门建立健全数据安全领导机构，明确数据安全责任部门和责

任人，强化各单位数据安全意识；**三是**围绕数据生存周期全过程，建立全流程数据安全管理制度，推动重要数据部署和应用数据安全技术手段，提升各部门数据安全管理和防护能力。

（四）个人信息保护

个人信息保护指数主要评价个人信息保护的责任部门与负责人明确情况、个人信息处理的合规情况、个人信息安全影响评估开展情况、个人信息共享、传输、存储等机制建设情况、个人信息存储的安全情况。2022 年重点关注是否明确个人信息保护的责任部门与负责人，是否开展个人信息安全影响评估，个人信息存储、传输是否采取安全措施。

如图 4-6 所示，全省 21 个地市个人信息保护指数的平均值为 41.39，8 个地市超过平均值。其中，深圳各市直部门初步明确了个人信息保护职责，开展了个人信息安全影响评估，并配套了相应管理和技术措施，表现良好；中山、肇庆、广州表现中等；其余地市表现不太理想。

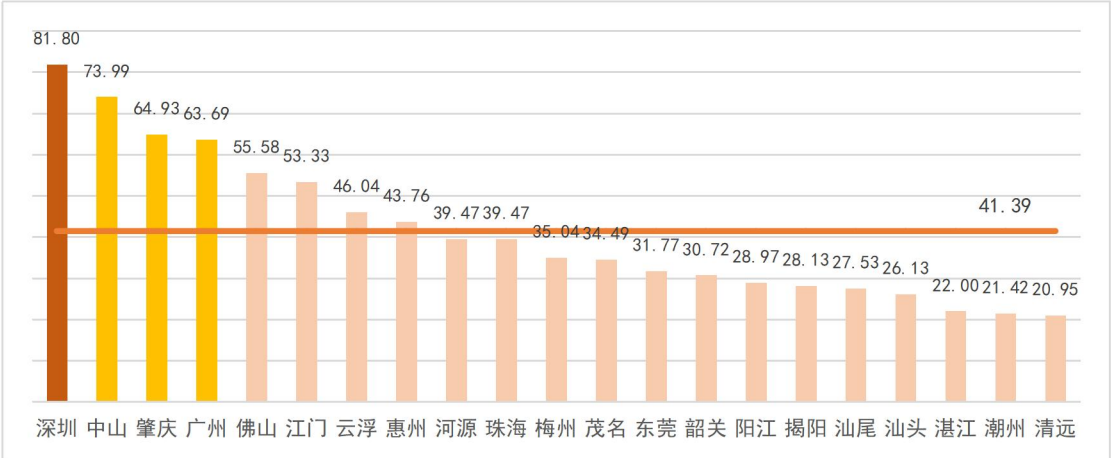

图4-6 广东省数字政府个人信息保护指数排名

各地市良好实践主要表现在：**深圳**制定《个人信息安全

规范基本要求》，要求上线运行的涉疫系统需满足个人信息保护有关要求，建立疫情防控数据统筹共享工作机制，要求各区各部门使用疫情防控数据时，需提供个人信息安全规范差距分析报告。同时，自 2019 年开始，定期开展政务类 APP 个人信息安全影响评估，提升政务类 APP 个人信息保护风险防范与应急处置能力。

各地市可参考以下建议开展个人信息保护工作：**一是**按照《个人信息保护法》《信息安全技术个人信息安全规范》等法律标准要求，明确个人信息保护的部门和岗位职责，建立健全个人信息保护的制度流程，定期开展个人信息保护内部培训，加强内部从业人员个人信息保护意识和能力；**二是**对政府网站、APP 等信息系统进行个人信息安全影响排查和评估，根据评估结果开展整改加固；**三是**通过个人信息去标识化、加密、访问控制等技术手段，防止个人信息泄露、篡改、丢失。

（五）密码应用

密码应用指数主要评价密码应用保障能力建设、新建政务信息系统密码应用、存量系统进行密码应用改造、密码应用安全性评估开展等情况。2022 年重点关注地区是否建设密码资源池，以及新建信息系统是否开展密码应用。

如图 4-7 所示，全省 21 个地市密码应用指数的平均值为 46.97，14 个地市超过平均值。其中，珠海、中山、韶关、东莞、肇庆、佛山 6 个地市，表现中等；其余地市表现不太理想。

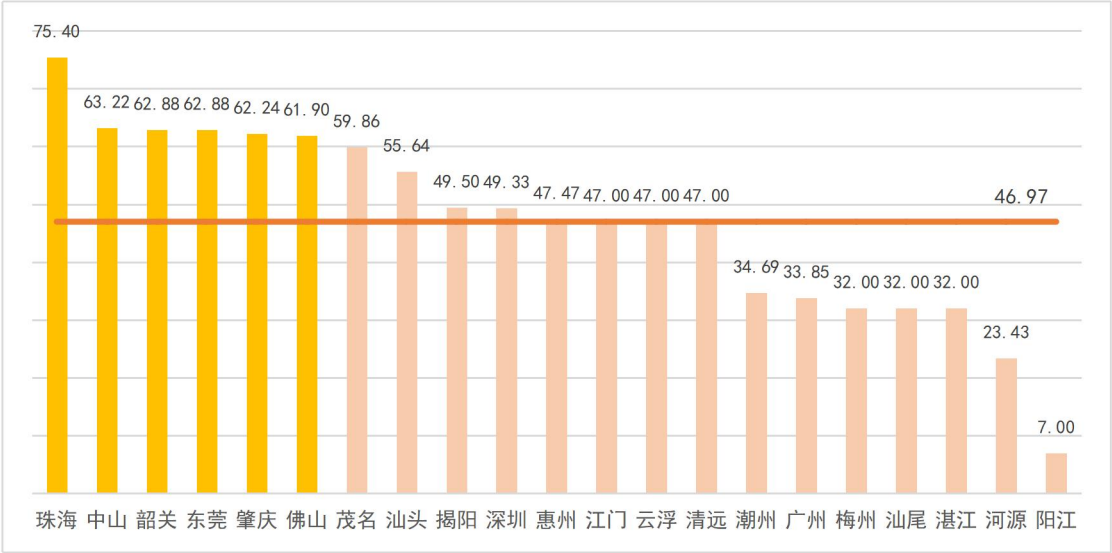

图4-7 广东省数字政府密码应用指数排名

各地市良好实践主要表现在：一是**珠海、佛山、韶关、肇庆、茂名、东莞、中山**均初步建成了政务云平台配套的密码资源池，为市直各部门提供相关密码支撑服务能力，并有部分系统开展了密码应用安全性评估工作。二是**珠海**印发《关于定期开展密码应用安全性评估的通知》《珠海市市级政务信息化项目商用密码应用工作指引》，初步建立了政务信息化项目密码应用管理机制。

各地市可参考以下建议开展密码应用工作：**一是**联合密码管理部门，明确数字政府密码应用支撑服务相关单位的职责分工，编制印发政务信息化项目密码应用改造工作指引、密码应用支撑服务对接规范等标准规范，指导各部门规范开展密码应用工作；**二是**商请财政部门，确定密码应用支撑服务采购模式；积极协调云服务提供方等单位加快密码资源池建设，建立健全密码应用支撑服务体系；**三是**组织开展政务信息化项目密码应用改造培训，组织项目承建方、密码厂商、密码测评机构等做好密码应用方案咨询、建设、改造、安全

性评估、测评等支撑工作，加快推进政务信息系统的密码应用建设、改造和对接工作。

（六）安全服务支撑体系

安全服务支撑体系指数主要评价网络安全咨询、设计、集成、运维、测试、风险评估（含等保、密评等）、应急处置、攻防演练等安全服务提供商/安全服务资源池的完善程度以及数字政府网络安全产业协同、合作情况。2022 年重点关注安全服务资源池的完善程度以及数字政府网络安全产业协同情况。

如图 4-8 所示，全省 21 个地市安全服务支撑体系指数的平均值为 51.06，10 个地市超过平均值。其中，深圳、东莞、佛山 3 个地市建立了相对较为完善的安全服务支撑体系，表现良好；广州、珠海、梅州、惠州、汕尾 5 个地市表现中等；其余地市表现不太理想。

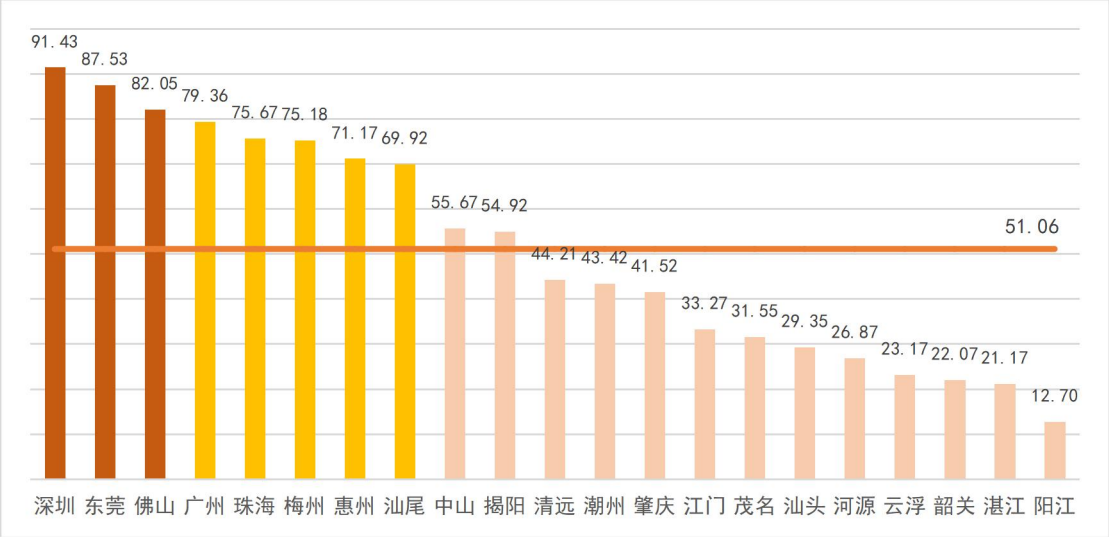

图4-8 广东省数字政府安全服务支撑体系指数排名

各地市良好实践主要表现在：一是**深圳、东莞、惠州、清远**等地市建立了数字政府网络安全行业协会、教育基地，

重点针对数字政府网络安全开展技术研究、实践探索与教育培训等，提升了地区网络安全服务支撑能力。二是深圳组建了由在编人员组成的实战攻防队伍，丰富了网络安全攻防人才梯队。

各地市可参考以下建议完善安全服务支撑体系工作：一是组建本地化、专业化安全服务团队，重点围绕设计集成、运营运维、测试评估、应急处置等基本支撑服务，集中行业优势资源，完善安全支撑服务体系；二是充分利用国家、省市、产业联盟、协会等资源，建立产业完整的安全生态；三是加强产业链上下游企业与用户单位在技术、市场、人才等方面的合作，推动相关信息共享、技术交流、联合攻关，促进数字政府网络安全产业资源高效利用。

第五章 安全运营指数

一、总体分析

如图 5-1 所示，在安全运营的二级指标中，信息资产管理指数的平均值为 49.12，12 个地市超过平均值，占比 57.14%；日常安全运维指数的平均值为 75.18，8 个地市超过平均值，占比 38.10%；安全监测指数的平均值为 43.69，11 个地市超过平均值，占比 52.38%；应急处置指数的平均值为 64.29，12 个地市超过平均值，占比 57.14%；安全检查指数的平均值为 45.11，9 个地市超过平均值，占比 42.86%；安全审计指数的平均值为 42.44，9 个地市超过平均值，占比 42.86%；业务连续性保障指数的平均值为 44.12，10 个地市超过平均值，占比 47.62%；安全协同指数的平均值为 89.71，10 个地市超过平均值，占比 47.62%。

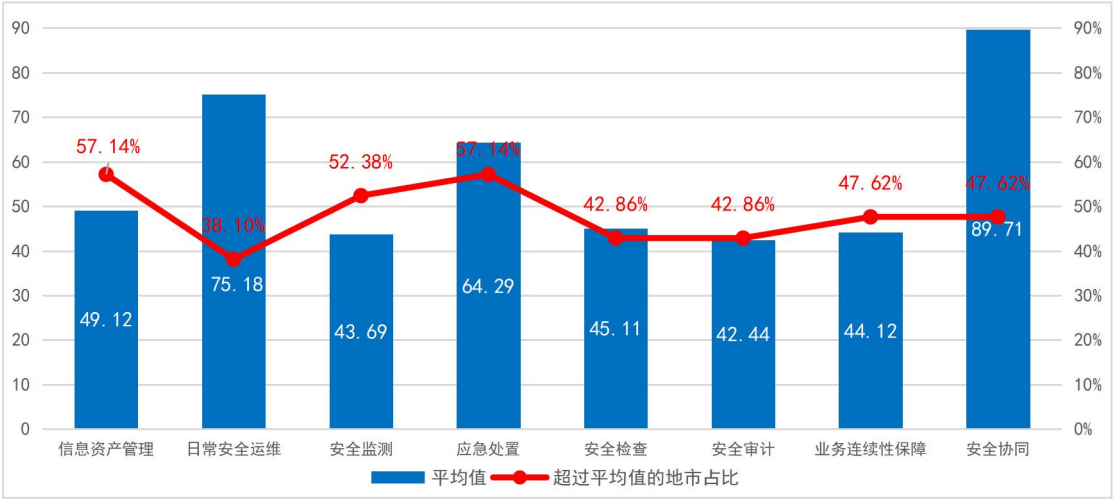

图5-1 安全运营二级指标指数平均值分析

与 2021 年相比，全省数字政府网络安全运营工作继续保持稳中向好的态势，主要表现在：**一是**指定专人负责系统日常巡检、权限管理和变更管理的市直部门数量占比分别由 26.16%、20.48%、18.24%增加至 51.71%、47.39%、43.37%；**二是**实现日志集中管理并妥善保存 6 个月的市直部门数量占比由 29.75%增加至 43.67%；**三是**全省已有超过 75%的市直部门制定了网络安全应急预案，超过 40%的市直部门组织开展了应急演练；**四是**定期对日志进行审计分析的市直部门数量占比由 23.47%增加至 50.00%。

如图 5-2 所示，全省 21 个地市安全运营指数的平均值为 66.27，9 个地市超过平均值。其中，网络安全运营指数处于**完善级（A）**的有深圳市，占比为 4.76%；网络安全运营指数处于**稳健级（B）**的有广州、东莞、肇庆、中山、佛山 5 个地市，占比 23.81%；网络安全运营指数处于**受控级（C）**的有江门、珠海、云浮、惠州、汕头、阳江、梅州 7 个地市，占比 33.33%；网络安全运营指数处于**启动级（D）**的为其余 8 个地市，占比 38.10%。

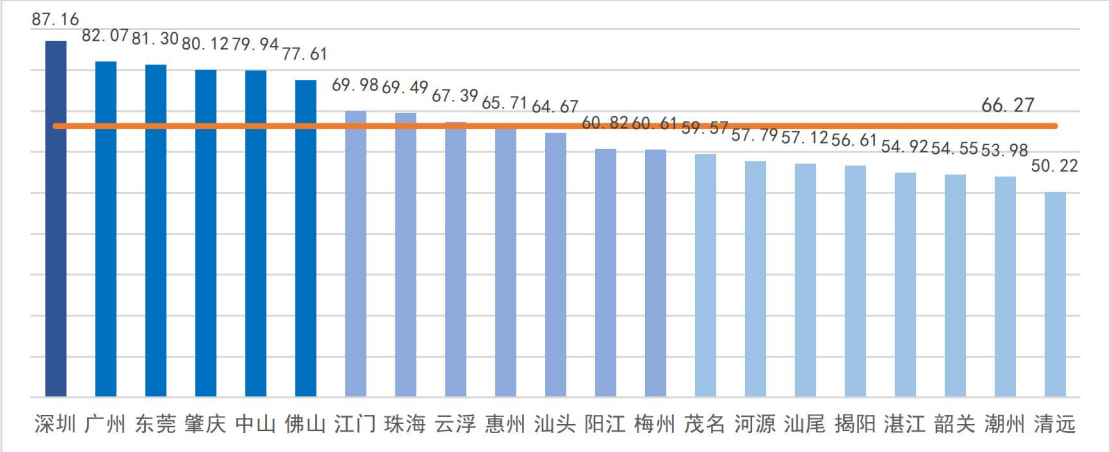

图5-2 广东省数字政府安全运营指数排名

分析发现，**深圳、广州、东莞、肇庆**等表现相对较好的地市大部分市直部门能够较为清晰地掌握资产底数，指定专人负责系统权限管理、变更管理，具备较为完善的安全监测与应急能力，制定了网络安全应急预案并定期开展演练和培训，形成了较为完善的安全事件通报及处置机制，定期开展安全风险评估并及时整改风险隐患，建立了安全审计机制并定期对日志进行审计分析，具有较好的业务连续性保障能力。

表现不太理想的地市安全运营能力有待全面提升。**一是**关键信息资产底数不清、责任不明，11 个地市超过 30%的市直部门未建立政务信息系统清单，未明确系统安全责任人；**二是**安全监测能力不成体系，9 个地市超过 60%的市直部门不具备完善的威胁监测、异常行为监测、失陷监测、网站防篡改能力，16 个地市超过 70%的市直部门未开展数据安全风险监测，11 个地市超过 60%的市直部门未开展主机入侵监测；**三是**安全检查工作开展不足，9 个地市超过 50%的市直部门未开展网络安全风险评估，11 个地市超过 50%的市直部门未开展网络安全基线核查、漏洞扫描和渗透测试工作；**四是**安全审计工作开展不足，9 个地市超过 60%的市直部门未建立审计机制，未定期审计安全策略和安全制度执行情况；**五是**业务连续性保障能力较低，10 个地市超过 60%的市直部门未开展数据、系统备份，并开展备份数据有效性测试，16 个地市超过 70%的市直部门未开展灾难恢复培训及灾难恢复测试等工作。

二、分指数分析

（一）信息资产管理

信息资产管理指数主要评价政务信息系统清单内容的准确性、完整性以及政务信息系统服务端口清单的准确性等方面。2022 年重点关注是否建立了准确、完整的政务信息系统和服务端口清单。

如图 5-3 所示，全省 21 个地市信息资产管理指数的平均值为 49.12，12 个地市超过平均值。其中，深圳、东莞各市直部门建立了比较完整、准确的政务信息系统资产和服务端口清单，表现良好；中山、肇庆、广州、揭阳、江门 5 个地市，表现中等；其余地市表现不太理想。

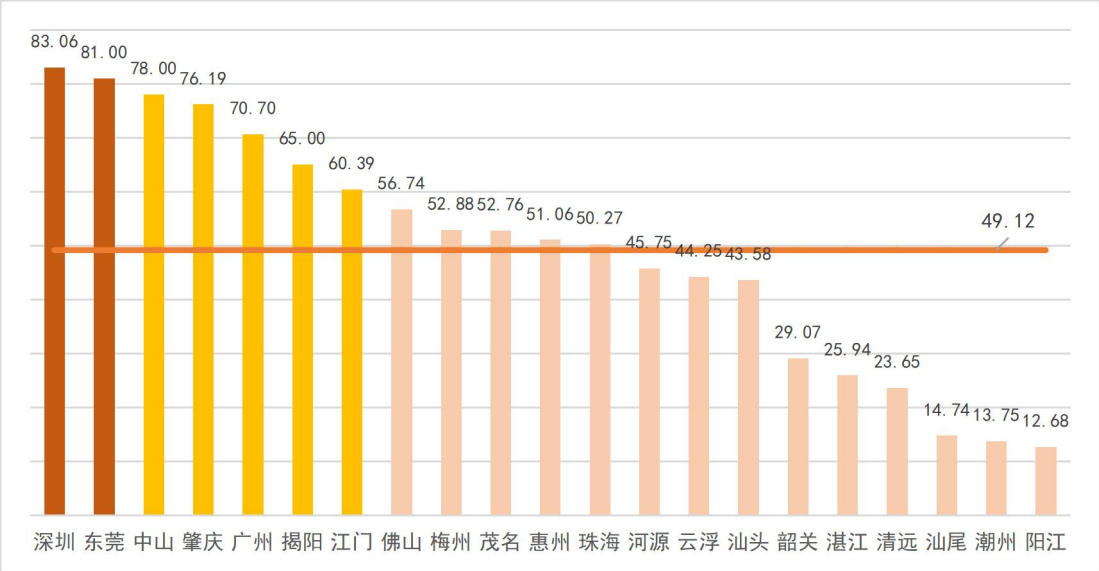

图5-3 广东省数字政府信息资产管理指数排名

各地市良好实践主要表现在：一是**珠海、肇庆、揭阳**等地市采用自主上报和技术手段检测相结合的方式，组织开展资产盘点工作，强化地区政务信息资产管理。二是**东莞**使用智能化安全运维管理平台，为各部门提供统一的信息资产管理平台，共登记 1.5 万余条资产信息。

各地市可参考以下建议开展信息资产管理工作：**一是**进一步压实各部门的网络安全工作主体责任，确保每个系统、每台设备都做到底数清、情况明、责任到人；**二是**组织各部门开展应用系统、IP 地址、网络域名、硬件设施等信息资产摸查，指导各部门梳理和建立信息资产台账，形成覆盖多部门的地市政务领域信息资产清单；**三是**加强信息资产状态核查，清理漏洞长期不修复、资源长期空闲、系统长期不运维的“僵尸”应用系统，下线已被新系统替代或不再使用的老旧系统，清理非本单位 IP 地址和非本单位域名的政务系统，定期核查信息资产台账，持续更新优化信息资产清单。

（二）日常安全运维

日常安全运维指数主要评价系统日常运维开展、日志集中管理情况，网络安全运营中心（SOC）建设及与省平台级联对接情况。2022 年重点关注是否定期开展网络安全巡检，网络安全运营中心建设及与省级平台对接情况。

如图 5-4 所示，全省 21 个地市日常安全运维指数的平均值为 75.18，8 个地市超过平均值。其中，东莞、深圳、肇庆、广州、中山、佛山 6 个地市建立了安全运维管理制度和操作流程，加强了安全运维人员培训，有效开展了日常安全运维工作，表现良好；其余地市表现中等。

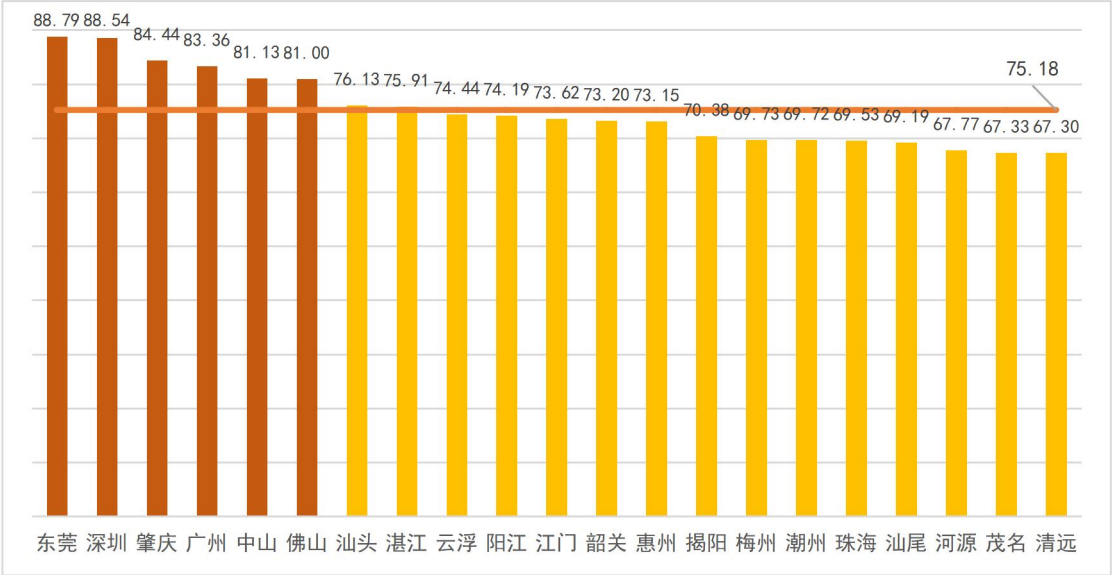

图5-4 广东省数字政府日常安全运维指数排名

各地市良好实践主要表现在：一是**广州、深圳、东莞、中山**等建立了 7*24 小时政务外网网络安全运维团队，支撑政务外网网络安全运营。二是**广州、中山**建成了市级数字政府运营中心，对电子政务外网、政务云平台等关键信息基础设施实行统一运维。三是**珠海、江门、东莞、中山、云浮**等在开展网络安全日常运维的基础上，定期发布网络安全运营报告。

各地市可参考以下建议开展日常安全运维工作：**一是**完善健全政务信息系统安全运维制度与规范，明确各部门和服务提供商职责，重点加强安全设备告警处置、策略有效性优化、规则库升级等工作；**二是**建设地区级数字政府网络和数据安全运营中心，持续完善网络和数据安全运营平台建设，建立智能化、一体化的安全运营体系，为各部门提供必要的技术服务保障支持；**三是**完成地区网络和数据安全运营平台与省平台对接，同步网络和数据安全的运维、监测数据，实现省市网络安全协同。

（三）安全监测

安全监测指数主要评价全流量威胁监测分析开展情况、异常行为监测开展情况、失陷监测开展情况、威胁情报分析开展情况、欺骗防御开展情况、网站防篡改开展情况、数据安全风险监测开展情况、主机入侵检测开展情况、办公终端安全监测开展情况、政务外网非法无线接入点监测开展情况。2022 年重点关注是否开展全流量威胁监测分析、异常行为监测、失陷监测、数据安全风险监测。

如图 5-5 所示，全省 21 个地市安全监测指数的平均值为 43.69，11 个地市超过平均值。其中，东莞、广州、深圳、云浮、佛山、肇庆、潮州 7 个地市表现中等；其余地市表现不太理想。安全监测工作整体仍有待进一步加强。

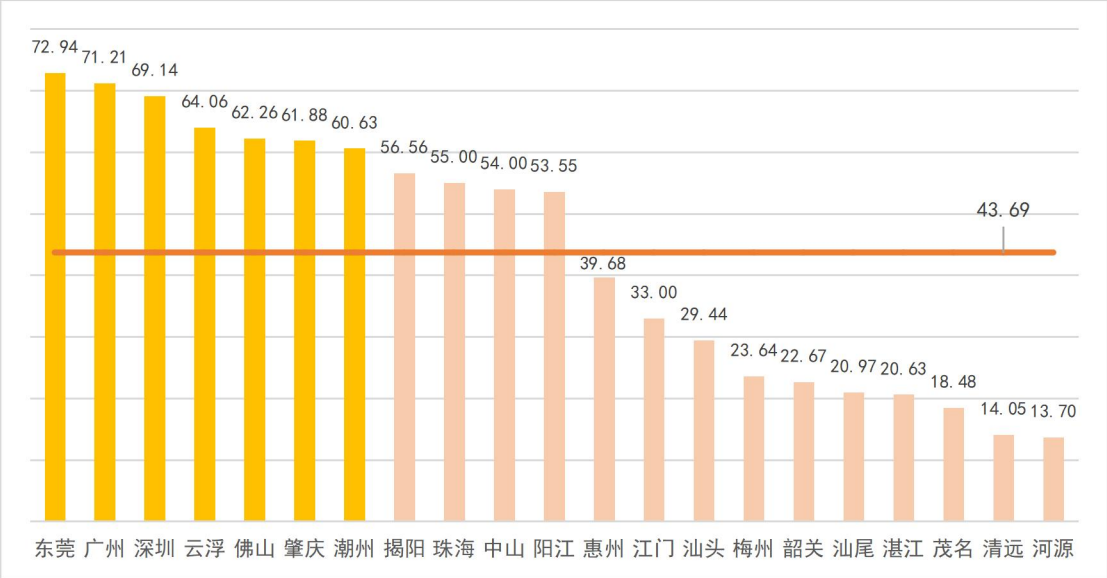

图5-5 广东省数字政府安全监测指数排名

各地市良好实践主要表现在：一是深圳建立市级网络安全态势感知和应急处置平台，并对接国家信息安全漏洞共享平台，与国家互联网应急中心形成联动共享机制；市级态势

感知平台完成与典型单位及试点单位对接，实现对重点行业、重点领域网络安全态势感知与通报预警。二是东莞建设网络安全态势感知平台，提升系统漏洞、网络安全、全网流量、深度安全、僵木蠕毒的态势感知能力；部署安装服务器主机安全系统，为主机提供实时入侵监测。

各地市可参考以下建议持续推进安全监测工作：一是建设地市级网络安全态势感知平台，开展面向威胁与攻击的扩展威胁监测响应能力建设，构建以资产发展为中心的态势感知能力；二是重点强化数据和应用访问过程中异常行为和数据泄露的风险监测，加强互联网、暗网有关安全威胁情报、重要网络攻击事件情报、新型网络病毒攻击情报和网络攻击窃密事件情报的收集、分析；三是完成地市态势感知平台与重点行业、重点领域以及各部门网络安全态势感知平台对接工作，充分整合各方安全监管能力，形成网络安全攻防态势统一感知和协同处置工作机制；四是加强监测告警的分析溯源能力，通过告警聚合、攻击向量关联等手段辅助分析研判，定位真实攻击，溯源攻击者，报送监管和主管部门。

（四）应急处置

应急处置指数主要评价网络安全应急预案管理情况、数据安全应急预案管理情况、个人信息安全事件应急预案管理情况、安全事件报告情况、安全事件处置情况、安全事件调查评估情况。2022 年重点关注是否制定网络安全应急预案并定期开展演练，是否建立网络安全事件应急处置、调查评估、溯源分析及整改加固机制。

如图 5-6 所示，全省 21 个地市应急处置指数的平均值为 64.29，12 个地市超过平均值。其中，中山、江门、深圳、广州、肇庆 5 个地市制定了网络安全应急响应与处置相关管理制度及办法，形成了安全应急响应与处置机制，表现良好；佛山、云浮、河源、汕头、东莞、珠海、惠州、梅州、阳江、茂名 10 个地市表现中等；其余地市表现不太理想。

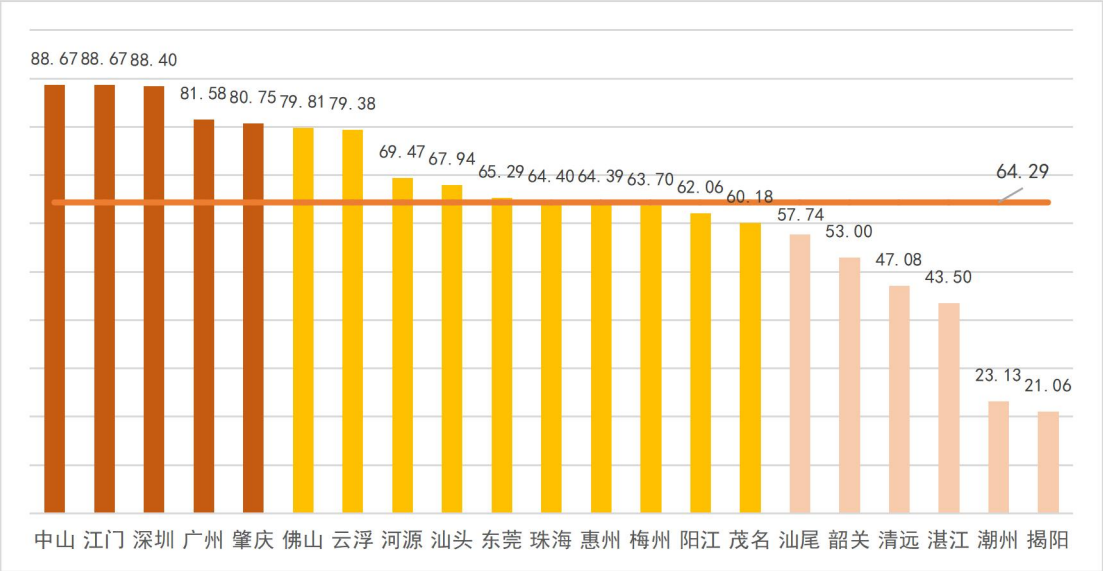

图5-6 广东省数字政府应急处置指数排名

各地市良好实践主要表现在：一是**深圳**印发《深圳市数字政府网络安全和数据安全事件应急预案》，建立安全事件应急响应制度，构建安全应急处置规范体系；依托网络安全态势感知和应急处置平台，完善网络与数据安全突发事件应急工作体系。二是**江门**印发《江门市电子政务外网网络与信息安全事件应急预案》，形成安全应急响应与处置机制；建成地市级网络安全 110 分中心，构建地市级网络安全应急支撑体系。三是**中山**多次组织安全模拟演练活动，提高安全事件的应急处置和响应能力；安全运维中心每天在粤政易群发送有关单位的终端病毒、弱口令和高危漏洞告警，并跟踪复

核各单位的处置情况。

各地市可参考以下建议不断优化应急处置工作：**一是**完善数字政府网络安全应急预案，建立健全数据安全和个人信息安全应急处置机制，定期开展培训和演练；**二是**强化应急处置能力，完善集安全事件发现、应急响应与处置恢复为一体的快速应急响应联动机制，规范应急处置流程，明确责任分工、技术保障、信息报送等重点任务，提高应急响应速度；**三是**做好极限生存准备，确保在发生勒索病毒攻击事件等极端情况下，采取极限生存保障模式，快速有效地开展系统和数据恢复工作。

（五）安全检查

安全检查指标主要评价全面风险评估开展情况、安全基线核查执行情况、漏洞扫描开展情况、渗透测试开展情况、系统代码审计开展情况、安全漏洞隐患整改情况、应用系统开源组件安全检测开展情况。2022 年重点关注是否开展全面风险评估、安全基线核查、漏洞扫描以及渗透测试。

如图 5-7 所示，全省 21 个地市安全检查指数的平均值为 45.11，9 个地市超过平均值。其中，东莞、佛山、广州、深圳 4 个地市持续开展了风险评估、安全基线核查、漏洞扫描等工作，及时修复了安全隐患，强化了风险防范能力，表现良好；肇庆表现中等；其余地市表现不太理想。

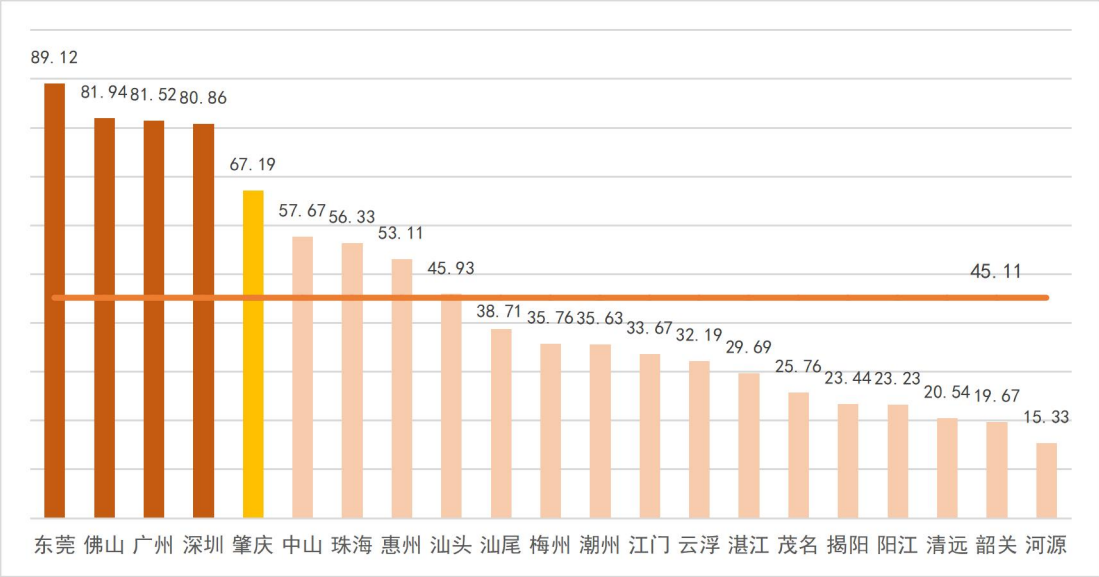

图5-7 广东省数字政府安全检查指数排名

各地市良好实践主要表现在：一是**深圳**建设了市党政机关网络安全众测系统，建设全市统一的安全漏洞库及安全测试人员库，组织安全专家对全市党政机关系统进行安全测试，排查修复漏洞隐患。二是**珠海**市政务服务数据管理局每季度组织技术团队对政务外网和重要业务系统进行全面安全检查，及时修复系统漏洞。

各地市可参考以下建议开展安全检查工作：一**是**制定网络和数据安全风险防范指引，指导、监督加强系统风险评估、弱口令排查、漏洞隐患发现和修复、安全基线配置等自查加固工作；**二是**建立常态化的安全检查工作机制，组织专业团队，定期开展网络安全风险评估、基线核查、漏洞扫描、渗透测试等网络安全检查评估工作，并根据网络安全检查情况及时进行整改和加固提升。

（六）安全审计

安全审计指标主要评价安全审计制度及审计计划的制定及执行情况、安全审计人员配备情况、安全策略及安全制

度执行审查开展情况、日志审计开展情况。2022 年重点关注是否形成了安全审计机制，是否开展日志审计。

如图 5-8 所示，全省 21 个地市安全审计指数的平均值为 42.44，9 个地市超过平均值。其中，东莞、深圳 2 个地市大部分市直部门建立了安全审计制度并定期开展日志审计分析，表现良好；广州、肇庆、汕尾、佛山、中山 5 个地市表现中等；其余地市表现不太理想。

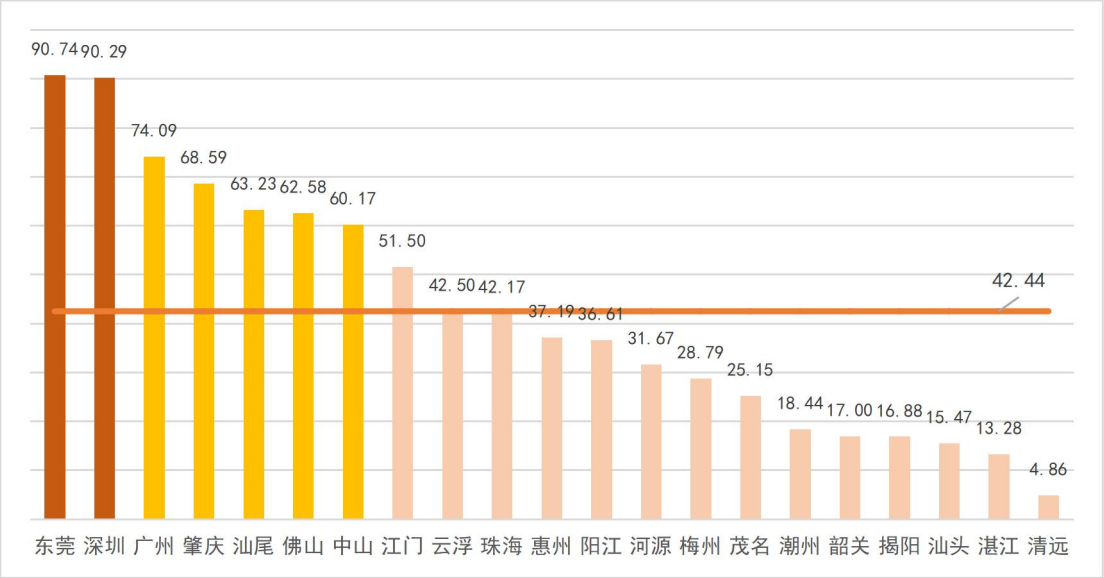

图5-8 广东省数字政府安全审计指数排名

各地市良好实践主要表现在：一是**深圳**超过 80%的市直部门制定了网络安全审计管理制度，组织开展了网络安全策略和安全制度执行情况审查，并定期对日志进行审计。二是**东莞**建成了安全体系日志审计平台，统一接入政务外网安全设备日志，提升日志审计溯源能力。

建议各地市参考以下建议开展安全审计工作：**一是**建立健全数字政府网络安全审计机制，明确审计责任人；**二是**定期组织专业化团队对外部监管要求、安全策略及安全制度执行情况开展审计，强化日志审计分析和人员行为审计，并形

成审计报告；**三是**深化审计成果运用，探索实现重要安全审计事项的自动化审计能力。

（七）业务连续性保障

业务连续性保障指数主要评价数据备份及恢复测试情况、业务影响分析开展情况、灾难恢复培训及灾难恢复测试开展情况。2022 年重点关注是否开展业务影响分析、数据备份和恢复测试。

如图 5-9 所示，全省 21 个地市业务连续性保障指数的平均值为 44.12，10 个地市超过平均值。其中，深圳、广州 2 个地市大部分市直部门定期开展业务影响分析、重要数据备份和恢复测试，强化了重点时期的网络安全保障，表现良好；中山、肇庆、东莞、佛山、珠海 5 个地市表现中等；其余地市表现不太理想。

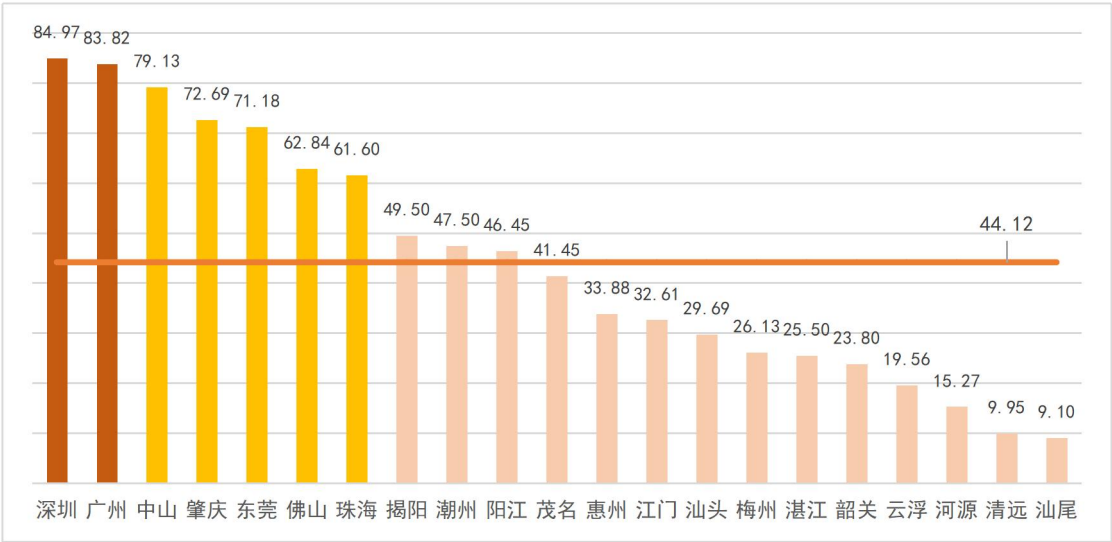

图5-9 广东省数字政府业务连续性保障指数排名

各地市良好实践主要表现在：一是**广州、深圳**超过 80%的市直部门对重要数据、系统执行了备份，并对备份数据开展了有效性测试。二是**肇庆**在政务云肇庆节点增加容灾备份

功能，对重要系统的重要数据提供备份服务。三是东莞举办全市范围灾难恢复培训，组织开展了政务信息系统业务影响分析。

各地市可参考以下建议开展业务连续性保障工作：一是根据数据、系统重要性制定备份策略，定期开展数据备份及恢复测试，提升业务连续性保障能力；二是加强业务影响分析，确定关键资产，分析关键资产的威胁，评估资产威胁概率及对业务的影响，制定业务连续性计划，选择合适的风险应对措施；三是强化容灾备份体系建设，对重要的业务系统同步开展冗余、双活等灾备系统建设，持续提升本地、异地备份服务能力，督促各部门开展灾难恢复培训及灾难恢复测试，降低系统故障和数据丢失风险。

（八）安全协同

安全协同指数主要评价与网信、公安等监管机构之间的沟通合作情况，与上级政务服务数据管理部门安全管理工作的配合程度，向上级政务服务数据管理部门报告安全事件是否及时、全面，向上级政务服务数据管理部门上报安全监测数据是否及时、准确。2022 年重点关注是否与网信、公安等监管机构之间建立沟通机制，是否配合上级政务服务数据管理部门开展安全管理工作，是否及时上报安全事件和安全监测数据。

如图 5-10 所示，全省 21 个地市安全协同指数的平均值为 89.71，10 个地市超过平均值。21 个地市政务服务数据管理部门与省政务服务数据管理部门建立了良好的安全协同

机制，地市各主管、监管部门之间建立了良好的沟通联络机制，整体表现良好。

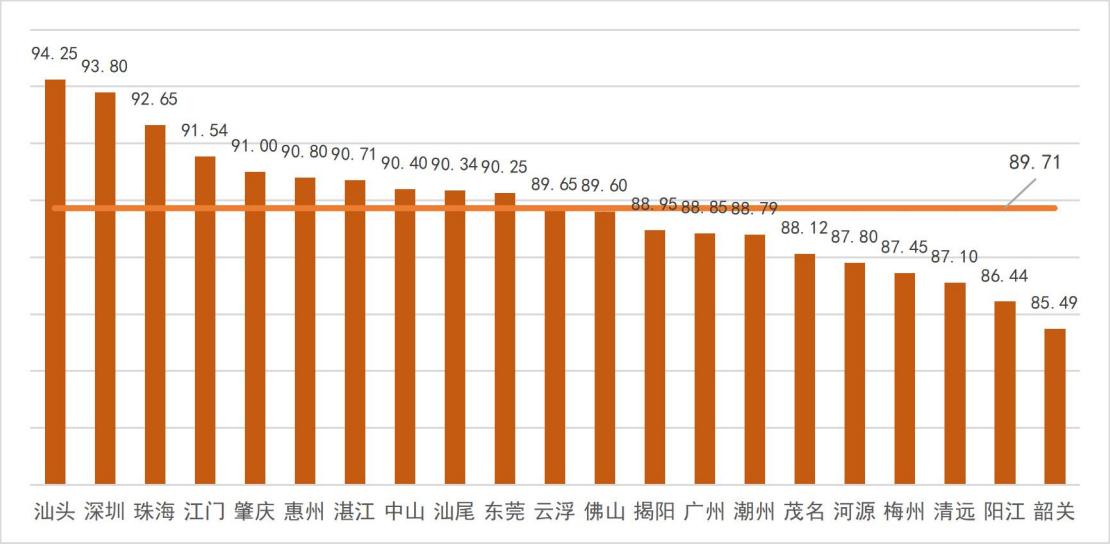

图5-10 广东省数字政府安全协同指数排名

各地市良好实践主要表现在：一是各地市政务服务数据管理部门在组织数字政府网络安全演练活动中与网信、公安等安全监管部门建立了协同联动机制。二是积极配合省政务服务数据管理部门各项工作，主动上报安全运维、监测数据等，基本实现了网络安全信息共享、通报预警以及联防联控能力。三是**珠海、江门、东莞、中山、云浮**等市主动上报地市网络安全运维报告。

各地市可参考以下建议开展安全协同工作：**一是**进一步发挥网信、密码、保密、工信、公安、政数等部门联动工作机制的作用，不定期组织工作调度协调会，常态化开展联合通报、联合检查、应急演练、攻防演练等工作，进一步增强网络安全信息共享以及联防联控能力；**二是**各部门态势感知平台与同级和上级网信、公安、政务服务数据管理部门平台

对接，实现监测数据和信息共享，形成条块结合、纵横联通、协同联动的综合防控大格局。

第六章 安全效果指数

一、总体分析

如图 6-1 所示，在安全效果的二级指标中，网络安全环境指数的平均值为 86.69，10 个地市超过平均值，占比 47.62%；安全漏洞指数的平均值为 95.24，16 个地市得分超过平均值，占比 76.19%；安全事件指数的平均值为 94.05，14 个地市得分超过平均值，占比 66.67%；专项工作指数的平均值为 56.08，11 个地市超过平均值，占比 52.38%。

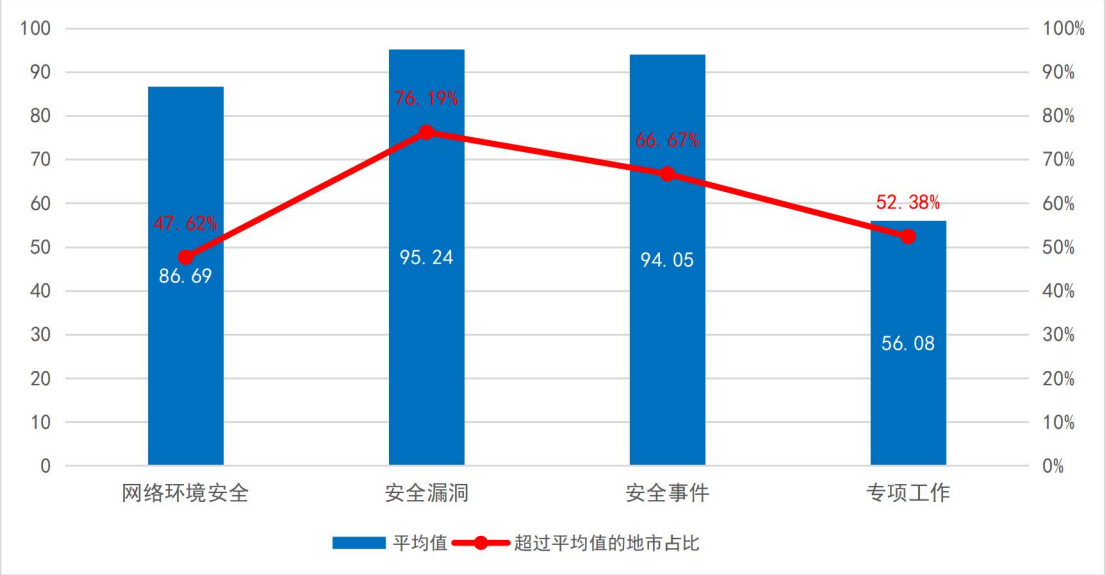

图6-1 安全效果二级指标指数平均值分析

安全效果方面，通过“粤盾-2022”攻防演练发现，全省的网络安全水平与去年相比有进一步的提升，全省电子政务系统具备更好的监测预警、应急响应与处置能力，数字政府网络安全治理体系进一步健全，安全保障水平进一步强化。

如图 6-2 所示，全省 21 个地市数字政府网络安全效果指数的平均值为 70.44，11 个地市超过平均值。其中，网络安全效果指数处于**完善级（A）**的有惠州、江门、珠海 3 个地市，占比为 14.29%；网络安全效果指数处于**稳健级（B）**的有广州、佛山、湛江、深圳、中山、东莞 6 个地市，占比 28.57%；网络安全效果指数处于**受控级（C）**的有肇庆、云浮、河源、汕头 4 个地市，占比 19.05%；网络安全效果指数处于**启动级（D）**的为其余 8 个地市，占比 38.10%。

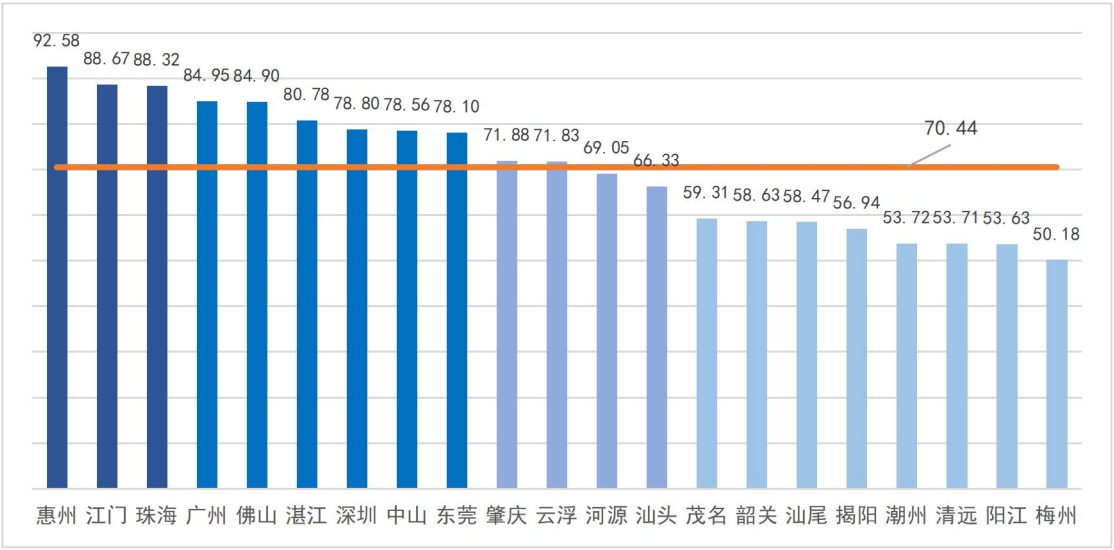

图6-2 广东省数字政府安全效果指数排名

网络安全效果指数排名与网络安全管理、网络安全建设、网络安全运营指数的排名基本一致，且安全效果指数与二级指标专项工作指数保持高度一致，主要原因是专项工作指标数据主要基于“粤盾-2022”广东省数字政府网络安全攻防演练的结果，且权重较大，导致网络安全效果指数与攻防演练结果高度相关。

总结发现，“粤盾-2022”广东省数字政府网络安全攻防演练期间，有的地市分管市领导专门到地市演练指挥部坐镇

指挥；有的地市网信、公安、政数等部门联合行动，集中开展分析研判、监测预警和应急处置工作；有的地方克服疫情防控吃紧、持续高温、区域停电等诸多问题，坚持 24 小时不间断值守，积极应对各类网络攻击手段；特别是江门、湛江、云浮、揭阳 4 个地市的整体防御水平与往年相比明显提升。准备充分，积极防守的地市都取得了较好的专项工作甚至安全效果指数得分。

其中，表现相对较好的地市如惠州市，**一是**组建了应对“粤盾-2022”攻防演练工作专班，制定了演练防守实施方案；**二是**网信、政数、公安部门等部门成立演练组织指挥机构，督导检查各项准备工作落实，全程组织演练防护行动；**三是**开展持续 3 个月的政务外网专项清网护网行动，开展为期半年的应对境外黑客渗透攻击专项整治，开展为期 1 个月的全市网络安全检查，提前发现并整改隐患；**四是**开展“惠盾-2022”网络安全攻防演练，为参与“粤盾-2022”攻防演练预热、积累经验；**五是**组织开展为期 2 周 4 班次的全市网络安全人员培训，提升人员防守意识和技能；**六是**组织专业的防守队伍，实行 5*24 小时不间断防护值守，取得了较好防守效果。

二、分指数分析

（一）网络环境安全

网络环境安全指数主要评价地区桌面终端被非法控制情况，桌面终端中木马、病毒情况，移动终端被非法控制情况，移动终端中木马、病毒情况，办公场所无线 AP 弱口令、被挟持情况，政务信息系统互联网高危端口暴露情况。2022

年重点关注移动终端、桌面终端中病毒、木马或者失陷情况。

如图 6-3 所示，全省 21 个地市网络环境安全指数的平均值为 86.69，10 个地市超过平均值。21 个地市得分均超过 80，整体表现良好。

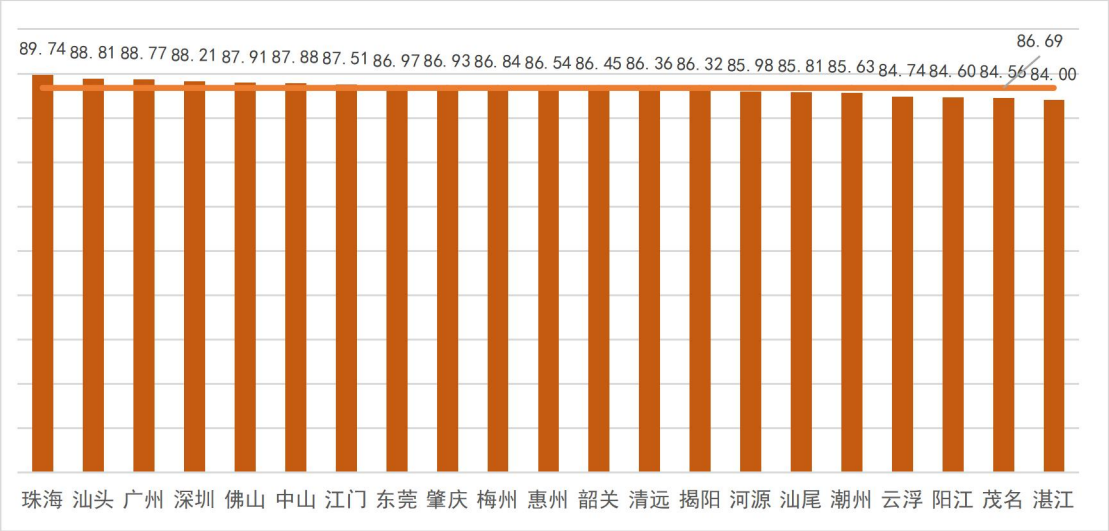

图6-3 广东省数字政府网络环境安全指数排名

从统计结果来看，广东省遭受的病毒木马前五位分别是virus.Synaptics、trojan.Tiggre、adware.AdLoad、packed.Black、virus.Ramnit。其中 virus.Synaptics 是一种感染型病毒，能够联网下载更新、接受远程指令控制计算机、监听键盘，通过邮件回传计算机的敏感信息及屏幕截图。trojan.Tiggre 是一种木马程序，通常会伪装成游戏辅助、系统工具等软件，会在启动伪装程序的同时窃取敏感数据、在系统中植入后门、下载其他恶意程序、控制连接的移动设备等。adware.AdLoad 是一种广告软件，通过与其他软件捆绑入侵用户计算机，随后联网下载其他广告程序，并且可能会不定期弹出广告。packed.Black 是一种加壳的程序，经过 Themida 工具加壳保护编译后的代码，使得代码难以分析和检测，并且能够检测

运行环境，拒绝调试和在虚拟环境中运行。virus.Ramnit 是一种感染型病毒，会窃取敏感信息，还可能充当后门并与服务器通信，允许远程攻击者访问受感染的计算机。

（二）安全漏洞

安全漏洞指数主要评价地区数字政府中危及以上安全漏洞情况，中危及以上漏洞数与地区系统总数比例。2022 年重点关注“粤盾-2022”数字政府网络安全攻防演练发现并通报的安全漏洞及时修复情况。

如图 6-4 所示，全省 21 个地市安全漏洞指数的平均值为 95.24，16 个地市超过平均值。21 个地市均修复了“粤盾-2022”数字政府网络安全攻防演练发现并通报的安全漏洞，表现良好。但个别地市由于系统覆盖广、漏洞数量多等原因，导致漏洞修复不够及时。

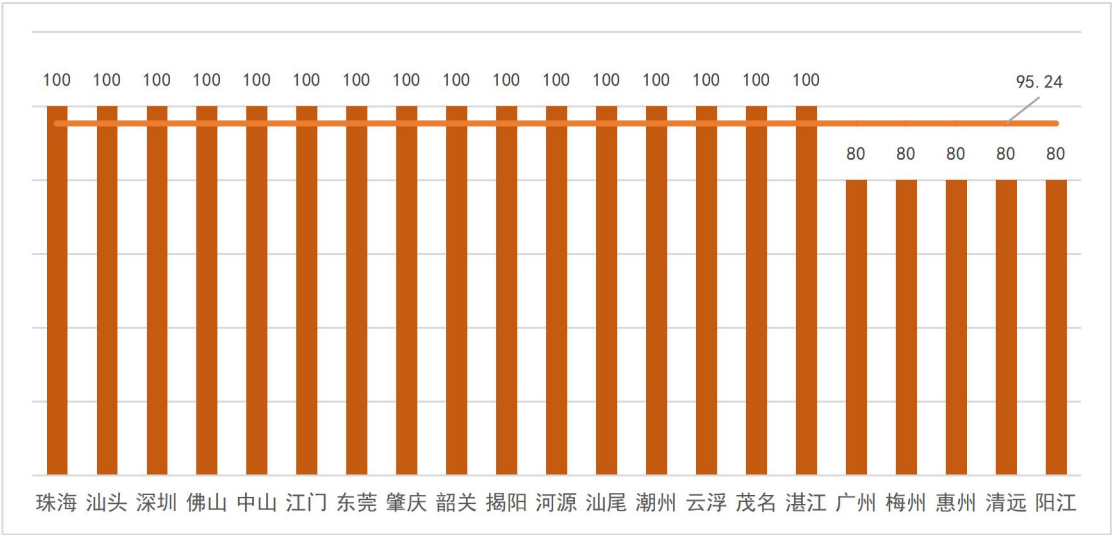

图6-4 广东省数字政府安全漏洞指数排名

分析发现，“粤盾-2022”通报的漏洞数量占比前五名分别是后台弱口令、社工钓鱼、文件上传、堡垒机漏洞和反序列化攻击。其中，弱口令漏洞被破解利用，攻击者可随意登

录，造成获取权限、非法控制、严重信息泄露等；社工钓鱼漏洞可被利用获取权限，执行任意操作，导致严重信息泄露；文件上传漏洞可被利用获取权限，造成非法控制，任意命令执行，重要数据、文件增删改查；堡垒机漏洞可被直接利用对堡垒机进行攻击，获取管理员权限，突破防护边界，获取服务器、数据库以及安全设备等权限；反序列化攻击漏洞可被利用攻击网站，获取管理员权限，执行任意系统命令。

建议各地市**一是**要强化漏洞监测，通过定期开展漏洞扫描、渗透测试等，及时发现设备和系统中存在的各种漏洞；**二是**要实现漏洞闭环管理，重点针对监管部门、粤盾攻防演练、地市攻防演练等发现并通报的重大安全漏洞问题，及时采取防护措施，清除相关安全隐患，确保漏洞态势处于可控范围内，提高整体安全性。

（三）安全事件

安全事件指数主要评价特别重大网络安全事件发生情况，重大网络安全事件发生情况，较大网络安全事件发生情况，以及一般网络安全事件发生情况。2022 年重点关注网络安全事件被监管部门通报情况。

如图 6-5 所示，全省 21 个地市安全事件指数的平均值为 94.05，14 个地市超过平均值。其中，珠海、汕头、深圳、中山、江门、东莞、韶关、揭阳、汕尾、茂名、广州、惠州、清远、阳江、佛山、河源、潮州、云浮、湛江 19 个地市表现良好；梅州、肇庆 2 个地市表现中等。

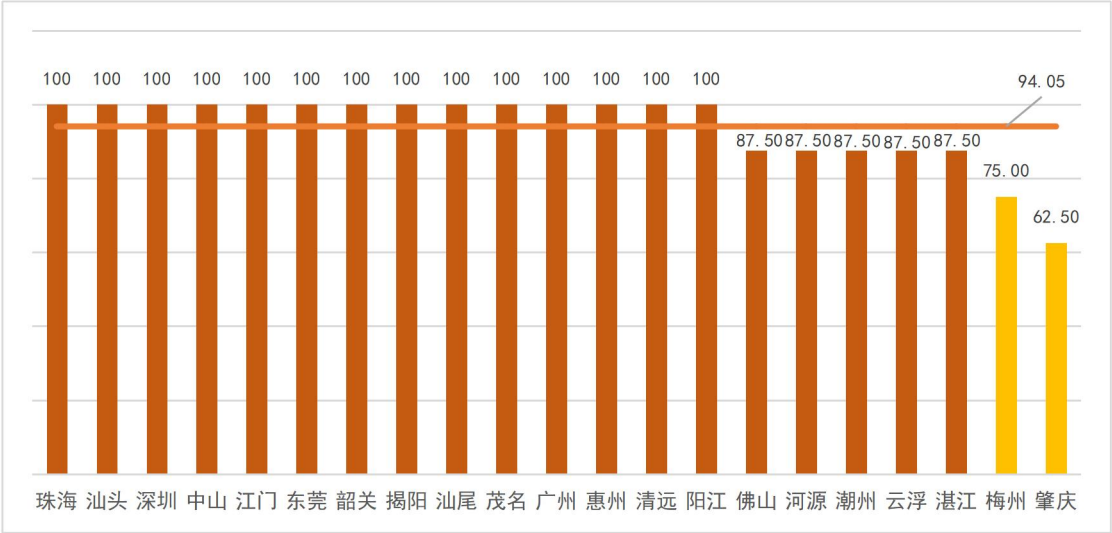

图6-5 广东省数字政府安全事件指数排名

分析发现，各地市被监管部门通报的网络安全事件主要是由僵尸木马、弱口令、钓鱼攻击三类问题引发。建议各地市坚持预防为主，预防与应急相结合，“谁主管谁负责、谁运行谁负责”的原则，**一是**强化安全事件应急与处置日常管理，通过常态化演练、宣传和培训，提高事件防范意识和技能，提升网络安全事件应对能力。**二是**明确各主管、监管部门及各部门各单位的职责，建立健全跨部门联动处置机制，充分发挥各方面力量共同做好网络安全事件的预防和处置工作。**三是**明确安全事件预警分级机制，统筹组织开展本地区网络安全事件监测，认真研判监测内容，及时发布预警信息。**四是**网络安全事件发生后，立即启动应急预案，实施处置，组织研判并及时报送信息；针对特别重大网络安全事件组织有关部门和专家进行调查处理和总结评估，提出处理意见和改进措施并按程序上报。

（四）专项工作

专项工作指数主要评价地市在实战攻防演练中的情况，省级安全检查中的情况，获得国家、省级网络安全竞赛、能力认证、试点示范工程等奖励、荣誉情况，以及履行网络安全监督检查职能的工作成效。2022 年重点关注“粤盾-2022”数字政府网络安全攻防演练结果以及地市组织攻防演练活动情况和成效。

如图 6-6 所示，全省 21 个地市数字政府专项工作指数的平均值为 56.08，11 个地市超过平均值。其中，惠州、江门、珠海、广州、佛山 5 个地市表现良好；湛江、深圳、中山、东莞、肇庆 5 个地市表现中等；其余地市表现不太理想。

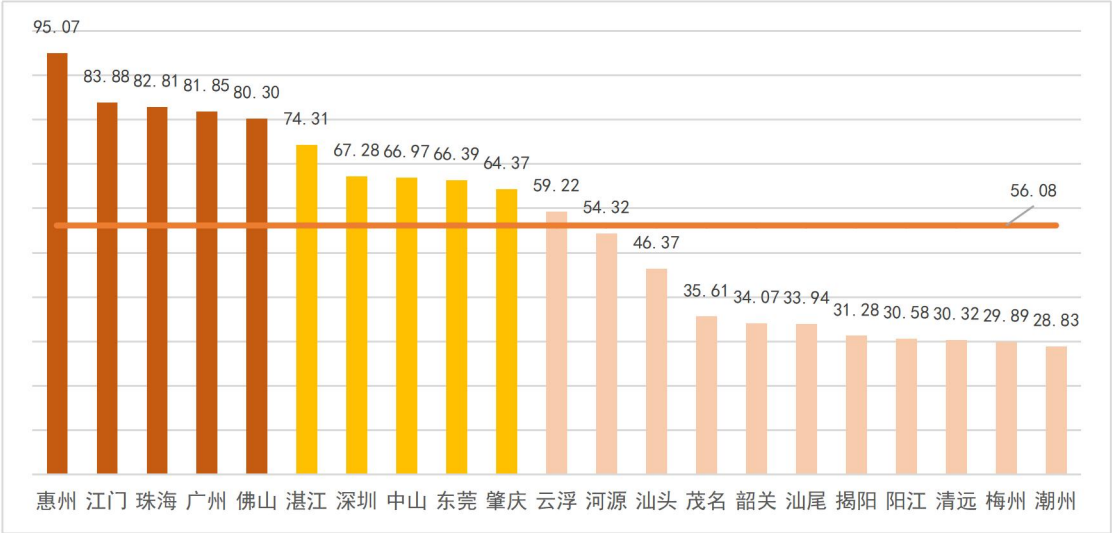

图6-6 广东省数字政府专项工作结果指数排名

通过对粤盾演练战果分析，发现各地市网络安全意识明显增强，监测预警应急处置机制更为完善，省数字政府整体网络安全防护水平有了质的提升。但仍有一些问题危害极大，可能构成重大网络安全和数据安全隐患，具体表现为：

一是弱口令和大量历史高危漏洞未修复。据统计，2020、2021、2022 年粤盾实战演练各地各部门弱口令问题占比分别为 67%、54%、41%。可以看出，2022 年虽有较大进步，但依然是演练发现的问题中占比最大的。这些问题不仅涉及普通用户账号，也涉及管理员账号。从地市来看，此类问题可造成 2 个政务云平台、4 个大数据中心、200 余台主机、78 个数据库、8 台文件服务器被控制，涉及 1400 多万业务数据、268 万条个人信息。同时，演练中发现一些系统仍存在 Shiro、Log4j、Weblogic 等框架上的已知高危漏洞。

二是关键系统和设备资产不清、责任不明。各地市报名参加本次演练的重点靶标约 120 个。在实战演练进入倒计时阶段，部分单位才临时提出变更，其中 34 个靶标系统要求替换、3 个系统要求更换所属单位或地址、且有 3 个系统无法访问，占重点靶标总数的 1/3。反映出部分单位存在资产清单管理不到位、责任归属不明的问题。一旦涉及的信息资产被黑客攻击后，将会出现无法及时监测预警、无人应急处置的情况，可能会导致攻击危害扩大、安全事件升级。

三是网络安全技术建设投入少，综合应用不充分。演练发现，由于前期各地市长期存在“重建设轻安全”的情况，安全投入严重不足、历史欠账多，对区域划分、边界隔离、终端防护、监测预警、密码应用等技术防护手段的综合应用不充分，攻击者利用各种手段，突破边界进入内部网络后，可任意横向和纵向渗透攻击造成更大范围的破坏。

四是供应链管理点多面广、形态复杂多样。演练发现，

供应链攻击比例逐年提高，已成网络安全管理重大风险来源。部分供应商运维特权账号管理不严，信息泄露被钓鱼攻击植入木马，导致系统被控制；部分供应商将源代码存放在互联网或公共技术论坛，易被攻击者获取并分析出漏洞，导致系统权限被控；供应商为维护方便，将多个业务系统、VPN 的账号和口令设置成一样或使用密码本记录系统账号和口令，攻击者成功控制一个系统就等于控制了一堆系统；部分供应商为运维方便，绕过安全隔离措施直接访问政务外网，造成政务外网安全防护形同虚设。

第七章 思路与建议

一、工作思路

党的二十大报告，首次把国家安全作为报告独立的一部分作了系统阐述，对党和政府在当前统筹好发展和安全两件大事具有重要指导作用。随着经济社会加速向网络化、数字化、智能化转型，网络安全已成为构筑新优势、领先新赛道的基础和前提，也是数字政府高质量发展的核心动力。面对层出不穷、愈加复杂的网络病毒攻击，全面筑牢网络安全防护网、保障数字政府网络安全变得十分必要、极其迫切。

面对新机遇和新挑战，安全指数作为数字政府稳定、安全、高质量发展的重要工具，把“看不见、摸不着”的网络安全防护能力转化为具体可量化考核的评价指标，有效地督促各地市提高数字政府安全治理能力，打造“实战化、体系化、常态化”的数字政府网络安全防护能力，为政务应用安全运行和政务数据安全保护提供有力保障。下一步，安全指数工作将从以下四个方面继续深入开展:

一是在“标准化”引领中强化决策支撑效果。加快广东省数字政府网络安全指数指标体系、实施指南等标准的制定，推动安全指数评估工作规范化开展，发挥安全指数标准在提高各地市数字政府网络安全政策科学性、确保网络安全措施实施有效性方面的积极作用，为实现更高质量、更有效率、

更加公平、更可持续的数字政府网络安全建设提供战略支撑。

二是在“常态化”监测中增加可信数据来源。围绕安全管理、安全建设、安全运营、安全效果等4个一级指标、24个二级指标，研究可自动取数或常态化监测的重点指标，增加可信数据来源，建立健全按周期计算指数的方法，提升安全指数的准确性、及时性和全面性。

三是在“动态化”调整中引导安全工作开展。根据国家及广东省数字政府改革建设工作重点，以及最新法律法规和国家标准等，不断调整和完善安全指数的评估重点和评估要点，提高指数的针对性和实效性，引导各地市各部门有目标、有重点的开展安全工作。

四是在“具体化”践行中推进指数深化转化。开展网络安全指数解读和能力提升培训，指导地市开展本地区数字政府网络安全指数评估，加强对各地市安全指数工作推进情况的实时监测和总结归纳，推广典型做法和优秀实践，适时开展省直单位安全指数研究。

二、工作建议

为应对更加复杂、更加隐蔽、更加专业的网络威胁攻击，必须坚持以习近平新时代中国特色社会主义思想为指导，深入贯彻落实党的二十大精神，全面贯彻国家总体安全观，以新安全格局保障新发展格局，在广东省数字政府网络安全指标体系的框架下，借助评估工作的引导及促进作用，坚持系统谋划与重点突破，聚焦网络安全薄弱领域，通过“固优势、抓重点、补短板、强弱项”，有效防范化解各类网络安全问

题，全面提升广东省数字政府网络安全防护能力和保障水平，为实现网络强国战略目标助力奋进。

（一）抓“自身建设”，完善数字政府安全保障体系

一是强化网络安全管理责任。建议各地市按照职责分工，统筹做好数字政府网络安全工作，落实主体责任和监督责任，构建全方位、多层级、一体化安全防护体系，形成跨地区、跨部门、跨层级的协同联动机制。同时，建议各地市定期召开工作调度会，分析问题，部署任务，推动各级部门落实安全防护和安全管理各项措施。

二是强化考核评价与教育培训。建议各地政务服务数据管理部门完善数字政府网络安全、数据安全考核评价体系，研究制定考核具体内容、方法、程序，加强考核结果应用。加强网络安全教育训练和人才培养，建立完善网络安全人才发现、选拔、使用机制，组织关键岗位人员参加网络安全执业资格考试、职称评审或技能鉴定，不断提高业务水平。

三是强化供应链安全风险管理。建议各地市建立健全供应商安全评价机制、政务信息化项目供应链安全管理工作指引，通过安全检查、安全审查等多种手段加强供应链安全管理。定期开展供应链安全风险评估，识别供应链各环节存在的安全风险，制定应对及防范措施，并定期对供应商信息化服务安全进行监控和审计。

（二）抓“重点环节”，赋能数字政府建设发展动力

一是加强分区分域安全管理。建议各地市加大网络安全建设投入，加强网络和数据的分区分域管理、收紧互联网出

口，依据业务系统重要性合理划分不同的网络安全区域。按照最小化原则强化网络边界安全隔离控制措施，建立网络策略开通审批机制，严格控制网络访问权限。加强办公网络、开发测试网络、业务生产网络以及不同安全等级业务系统的隔离和防护。

二是加强数据安全管理建设。建议各地市加快推进首席数据官制度和推广工作，明确首席数据官作为网络和数据安全责任人，并明确相应责任机构，统筹负责本级政府或本部门数据安全保障工作，建立健全数据安全审计制度、数据全生命周期安全管理制度、数据安全事件应急处理机制、数据分类分级管理等，完善数据安全技术体系。

三是推动电子政务密码应用。建议各地市在重要信息系统建立时要统筹好密码应用，规范电子印章、电子文件、电子证照和移动政务办公中的密码应用。加强政务网络、政务云、政务大数据中心等资源共享中的密码保护，提升密码技术在各方面保护的作用。

（三）抓“融合优化”，提高数字政府运营保障水平

一是全面清理僵尸系统。建议各地市加强应用系统、IP地址、网络域名、硬件设施等信息资产摸查，梳理和建立信息资产台账。清理存在漏洞长期不修复、资源长期空闲、系统长期不运维的“僵尸”应用系统，下线已被新系统替代或不再使用的老旧系统，清理非本单位IP地址和非本单位域名的政务系统。

二是实现一体化安全运营。建议各地网络和数据安全运

营平台要完成与省平台对接，同步网络和数据安全的预报、预警、预演，并视情做好预案启动，做到及时发现问题、风险“动态清零”，实现主动防、早发现、快处置。

三是加强网络攻击监测和处置。建议各地市加强电子政务网络骨干网节点的网络流量监测，加强自建专网（专区）、本地局域网的网络病毒攻击监测和处置。对接入各类专网（专区）的网络流量要进行监测分析，及时发现感染网络病毒进行攻击传播的风险，督促相关部门完成风险处置。

（四）抓“综合防控”，提升数字政府整体防护效果

一是常态化开展攻防演练。建议各地市通过“实兵、实网、实战”的常态化数字政府网络安全攻防演练，排查各级政务信息系统的安全风险隐患，检验各地市的网络和数据安全防护水平。充分运用攻防演练成果应用，完成相关问题的风险整改闭环，举一反三，提升整体防护能力。

二是做好漏洞闭环管理。建议各地市持续组织专业安全力量对数字政府一体化政务服务平台等重点系统开展网络安全风险排查、漏洞扫描、渗透测试等工作，开展常态化的网络和数据安全风险排查整改及加固。同时，全面开展弱口令和已知高危漏洞排查，及时清除相关安全隐患。

三是提升极限生存能力。建议各地市坚持底线思维，制定应急预案并定期开展应急演练，确保在发生勒索病毒攻击事件等极端情况下，做好极限生存准备，采取极限生存保障模式，快速有效地开展系统和数据恢复工作。

附录：数字政府网络安全能力成熟度定义

成熟度级别	分数范围（X）	定义
优化级（S）	X≥95	为业界最高水平，效果得到了充分验证。能够主动地改善流程，运用新技术，实现网络安全工作的持续优化。
完善级（A）	85≤X<95	已形成良好的制度、人员、技术等集成应用，并能够通过定性和定量测量跟踪管控措施的实施效果，持续完善管控措施，初步实现综合防御。
稳健级（B）	75≤X<85	已形成符合实际的制度规范及配套技术支撑，且组织内外部有较好的协作，初步实现主动防御。
受控级（C）	60≤X<75	已建立了基本的制度规范及配套技术措施，但落地执行还不到位，安全效果不稳定。
启动级（D）	X<60	尚处于管理制度、技术措施和运营体系的初步构建阶段，没有形成稳定的能力。