2020北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE

实战化安全运行视角下的医卫行业安全风险

奇安信行业安全研究中心 主任 裴智勇

目录

01 实战化安全运行能力

什么是实战化安全运行能力建设

实战化安全运行能力建设

立足于业务架构衍生出安全架构的组织体系建设解决方案。通过识别业务架构中支撑生产运行的业务驱动力、组织构成和组织行为，以此为基础推动支撑安全运行组织建设的对等设计。

安全运营

着重于运行体系的评价、决策方案建设，通过运行过程记录、数据采集与指标设计，实现安全运行水平的评价，并促成安全运行决策。

安全运维

着重于运行体系的流程、规程方案建设，通过一系列操作步骤与规范、保障预案，实现安全运行过程的质量控制。

实战化安全运行视角下的安全风险

漏洞

潜在安全风险

处罚

与合规运行

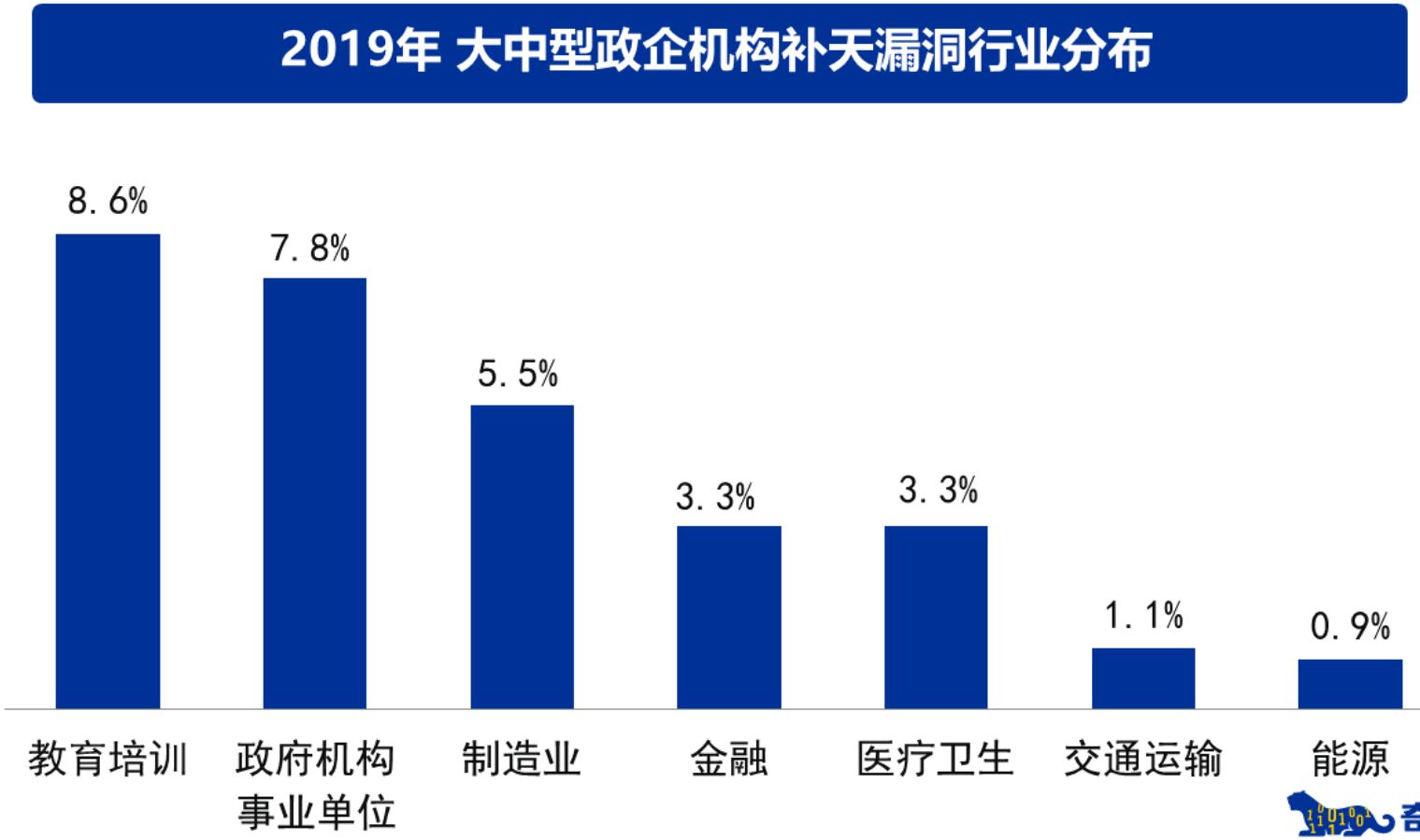
事故

预警与响应

02 安全漏洞报告

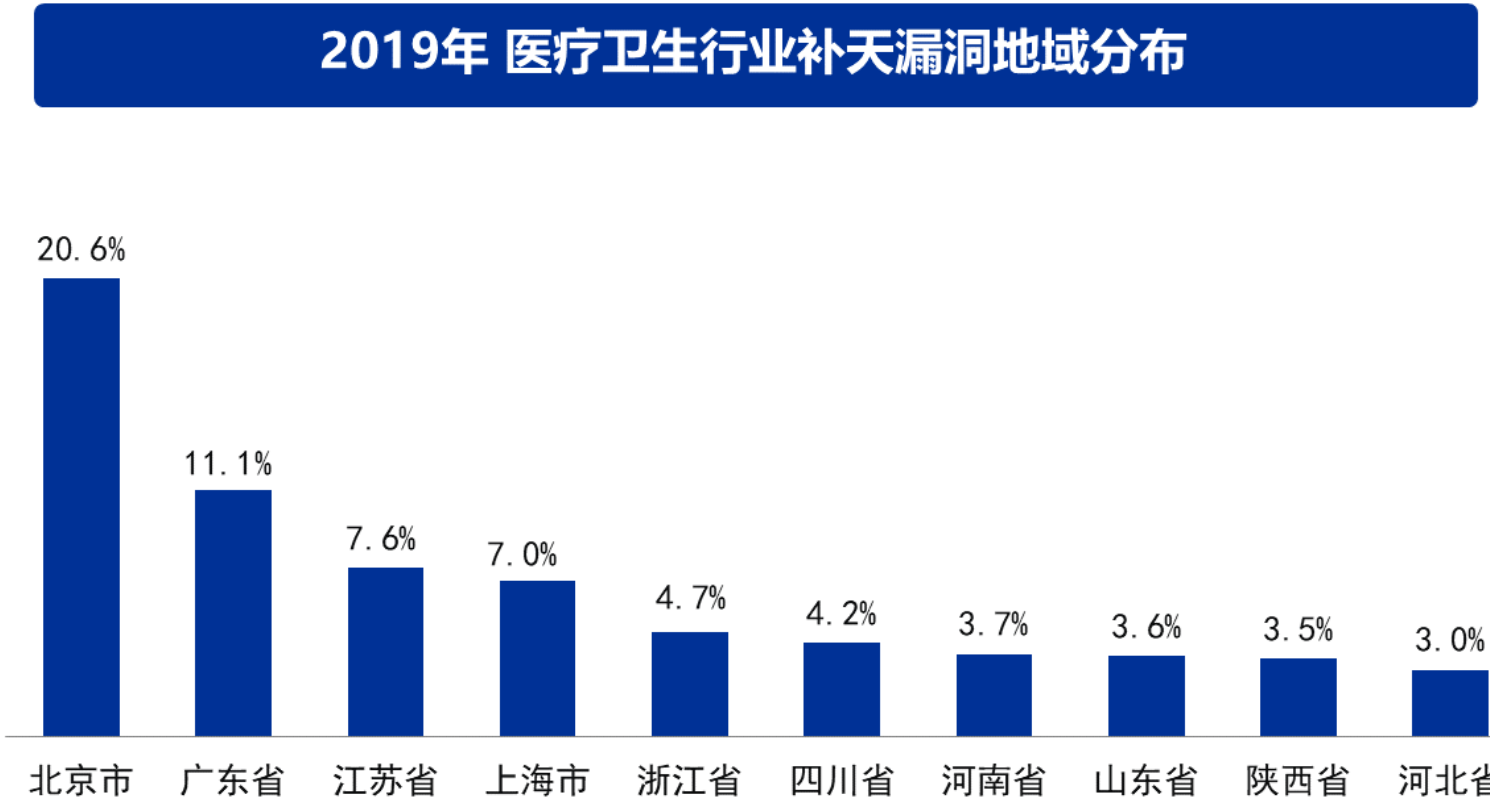
医卫行业安全漏洞情况

2019年1-12月，补天漏洞响应平台共收录全国医疗卫生行业相关网站的安全漏洞2237个。占全国漏洞的3.3%。



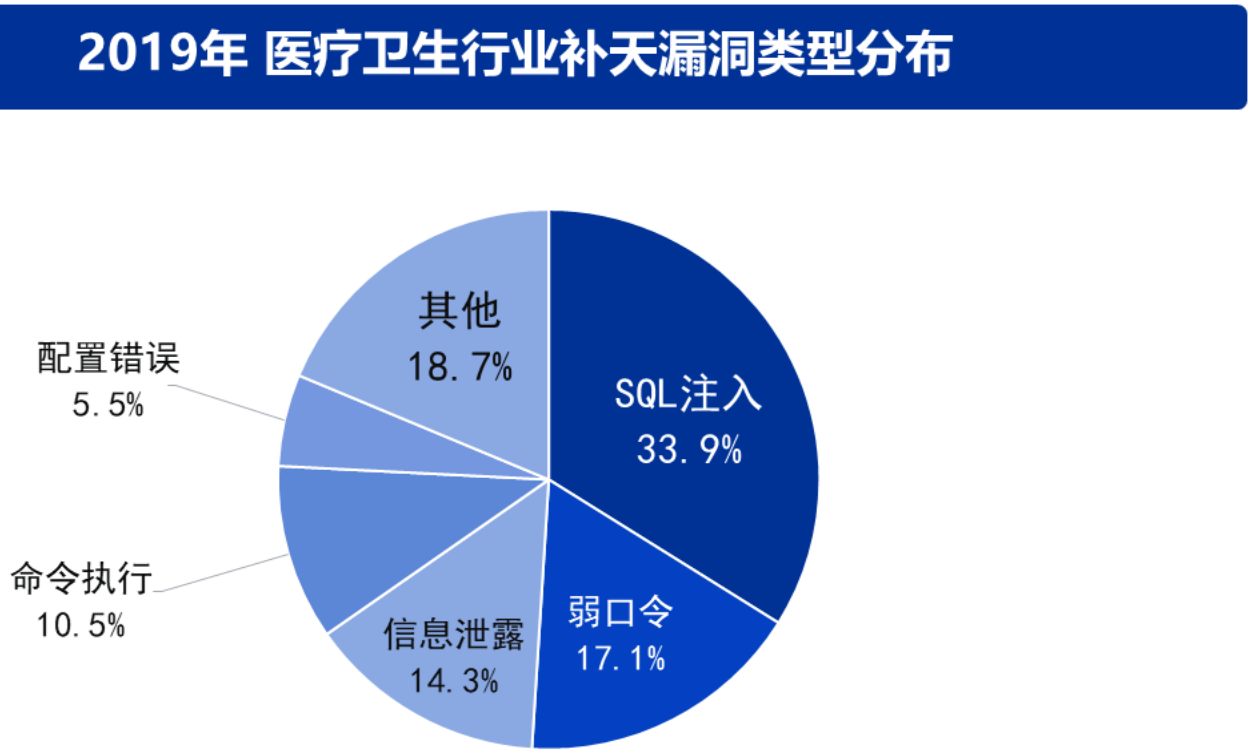
医卫行业安全漏洞情况

补天漏洞响应平台收录的医疗卫生机构安全漏洞中，北京地区占两成。



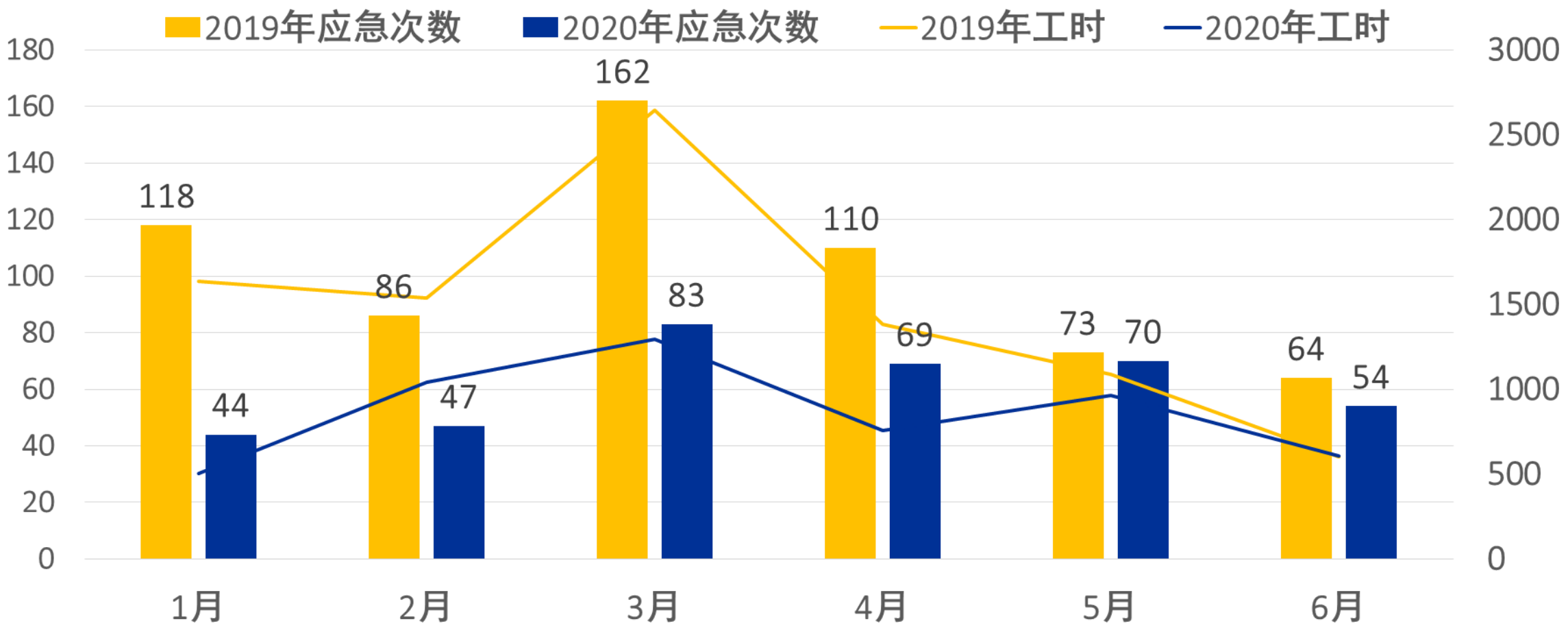
医卫行业安全漏洞情况

弱口令（1731%）、配置错误（5.5%）等低级漏洞仍然普遍存在。



03 事故应急响应

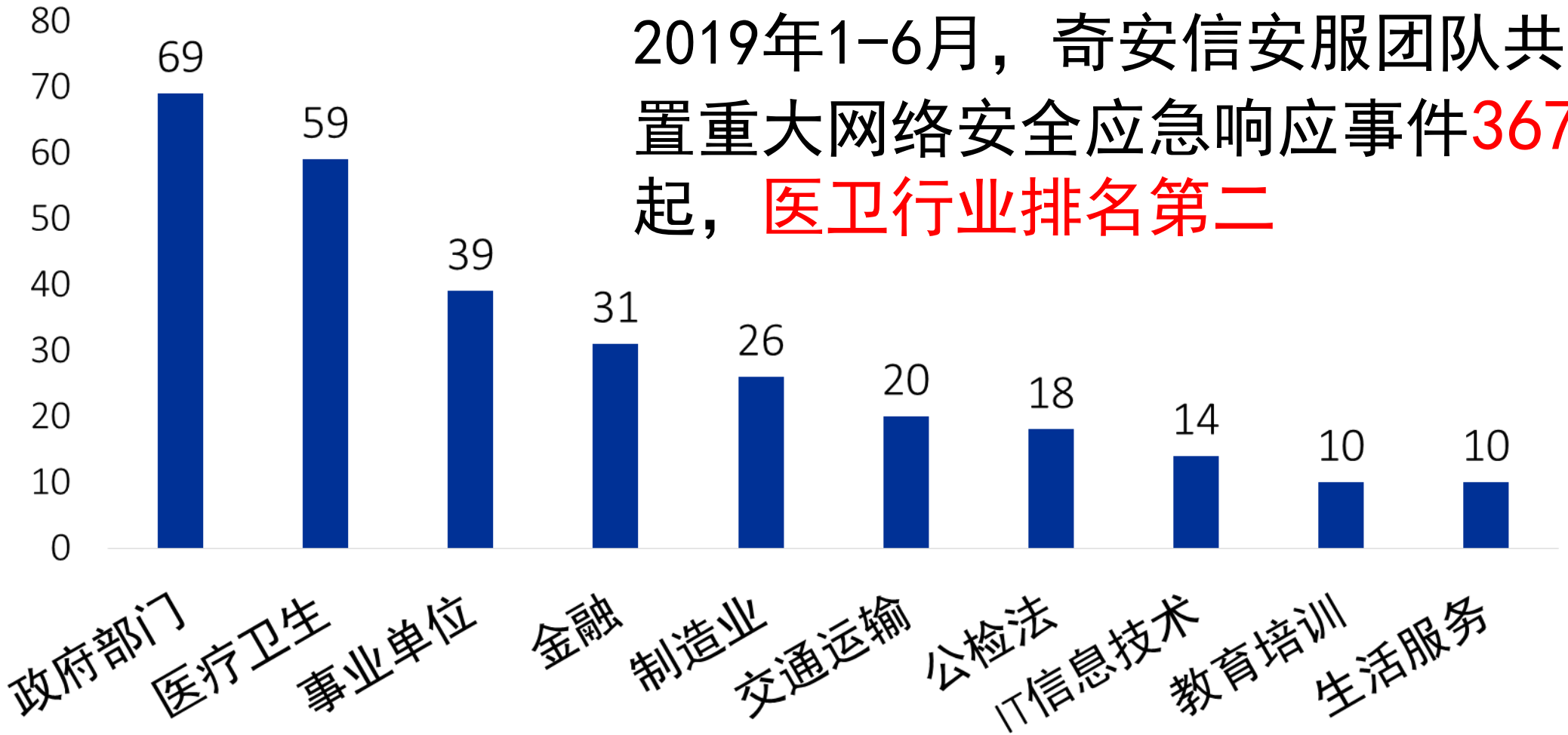
2020年上半年应急响应服务整体走势



2020年1-6月奇安信安服团队供收到应急响应求助367起，同比下降40.1%

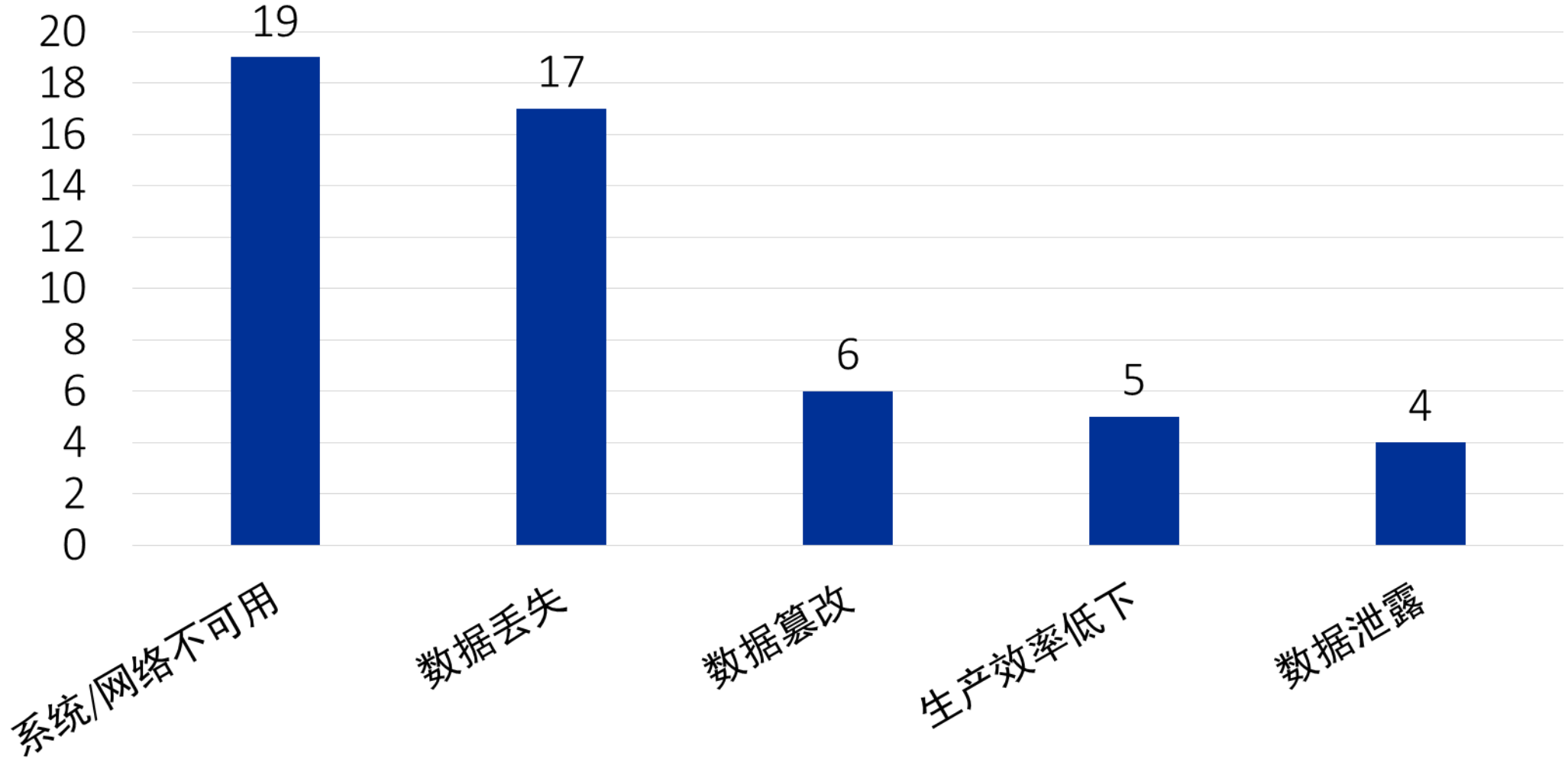
1、疫情影响，生产活动半暂停状态　　2、2019年3月份，永恒之蓝下载器木马爆发

应急响应行业分布



2019年1-6月，奇安信安服团队共处置重大网络安全应急响应事件367起，医卫行业排名第二

医疗卫生行业遭受攻击影响TOP5



2020年1-6月数据

某市医药公司OA系统失陷，造成数据泄露

发病症状

2020.3中旬，某医药公司

OA系统失陷

服务器出口地址被外连

初诊情况

对外攻击IP为该公司内网OA系统出口地址

服务器存在任意写入文件漏洞，发现木马文件

发现两个Webshell后门

病因诊断

服务器开启远程登陆端口

攻击者登陆端口，写入漏洞，执行命令、上传木马

攻击者利用恶意程序发起外联，进行数据传输

治疗方案

修复漏洞

关闭远程3389等危险端口，加强设备权限管理

更新病毒库，防火墙加入相关策略，禁止服务器主动发起外联

某省三甲医院感染Crysis勒索病毒事件

发病症状

2020.2月，某省三甲医院多台服务器文件被勒索病毒加密

业务无法进行

初诊情况

主机服务器感染Crysis勒索病毒

防病毒软件授权到期

发现两个webshell后门

病因诊断

一台服务器对外开放远程桌面服务

管理员密码弱口令，多台服务器被爆破

防病毒软件长期无运维

治疗方案

修改弱口令

更新防病毒软件授权

开启放爆破功能，禁用危险端口

建立安全灾备预案

应急响应典型事故

某三甲医院业务瘫痪8小时，损失800多万

疫情爆发

2019. 3，某三甲医院网络时断时续

终端无法链接网络

医院系统瘫痪

初诊情况

终端老旧且未打补丁

终端没有安全防护

大量办公终端感染蠕虫病毒

病因诊断

终端老旧且没有任何防护

用带毒的U盘随意传输资料。

所有信息都储存在终端上

治疗方案

更换老旧设备并安装企业级杀软

全网扫毒

分区进行端口、IP级别的隔离

重要文件定期进行非本地备份

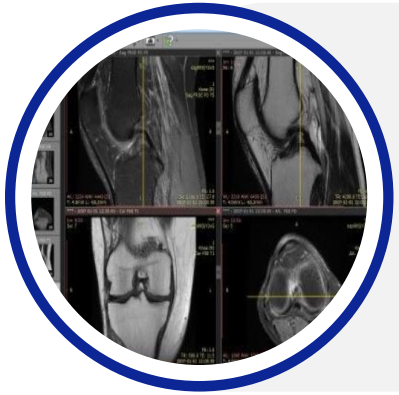
全球医卫大事概览

新加坡150万病患资料被盗，相关机构被罚100万

时间：2019年1月

瑞典六年间约270万医疗通话记录泄露

时间：2019年2月



11.9亿份敏感医疗图像在公网暴露，包含美国军方人员信息

时间：2019年11月

美国110家养老院系统遭入侵，黑客勒索1400万美元比特币

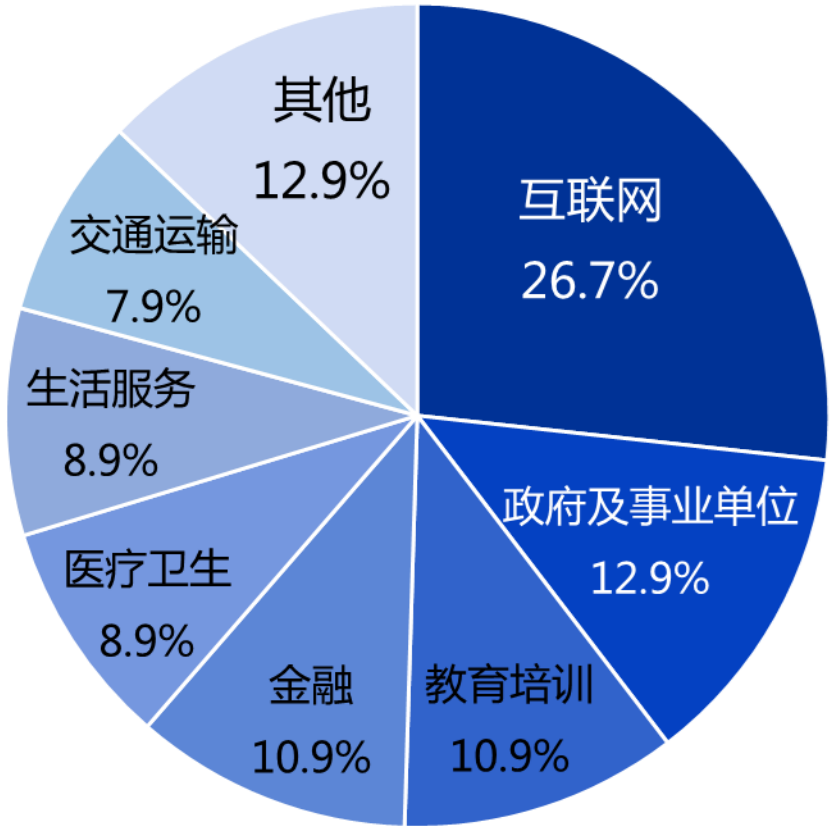
时间：2019年11月

相关资讯整理自安全内参

04 行政执法案例

总体情况——行业分布

2019年至今《安全内参》共收录网络安全行政执法具体案例1026起



统计显示，在1026起执法案例中：

互联网行业的网络安全事件数量最多，占26.7%

医疗卫生行业排名第五，占比8.9%。

医疗卫生行业典型执法案例分析综述

建设运维管理疏失

- 未按等保标准建设
- 违反相关法规侵犯用户隐私
- 内鬼

黑客攻击

- 漏洞未及时处理
- 遭受勒索攻击

医院不符合等保要求被查处

案件回顾：

2019年6月，某市公安局网安支队在开展网络安全**执法检查**过程中发现，该市一医院未制定内部安全管理制度和操作规程、未采取监测、记录网络运行状态、网络安全事件的技术措施，未按照规定留存相关的网络日志且在网络正式联通的30日内未到公安机关进行备案。依据《中华人民共和国计算机信息系统安全保护条例》第二十条、《中华人民共和国网络安全法》第五十九条之规定。给予责令改正并行政警告处罚。

违法/犯罪主体	政企机构
违法/犯罪性质	建设运维管理疏失
所属行业	医疗卫生
影响范围	政企机构利益
关键词	医院、未备案、不符合国家标准
触犯法条	《中华人民共和国计算机信息系统安全保护条例》第二十条、《网络安全法》第五十九条
机构责任	不履行安全保护义务

建设运维管理疏失

某医疗科技公司收集用户隐私被处罚案

案件回顾：

2019年11月，接公安部**通报线索**，一款求医问药类APP应用疑似存在侵害个人信息行为。经查，某事一医疗科技公司运营的该款APP应用，在安装过程和首次使用未明示用户隐私协议。警方依据《网络安全法》第41条、第64条规定，对该公司予以警告，对直接负责的主管人员予以罚款1万元，责令限期整改。

违法/犯罪主体	政企机构
违法/犯罪性质	建设运维管理疏失
所属行业	医疗卫生、互联网
影响范围	**公众利益**
关键词	医疗、APP、未明示用户隐私权益
触犯法条	《网络安全法》第41条、第64条
机构责任	不履行安全保护义务

建设运维管理疏失

宁夏某医院两护士贩卖产妇和新生儿信息被刑拘案

案件回顾：

2019年4月，某市公安局下属地区网安大队成功**侦破**一起侵犯公民个人信息案。经调查为母婴摄影店提供信息的“上线”是该市某医院的两名护士。网安大队随后将贩卖公民个人信息的关某、张某成功抓获，二人对利用职务便利，获取产妇及新生儿信息贩卖给周某并从中获利的犯罪事实供认不讳。关某、张某已被依法刑事拘留，对周某予以行政处罚。

违法/犯罪主体	内部人员
违法/犯罪性质	建设运维管理疏失
所属行业	医疗卫生
影响范围	政企机构利益、**公众利益**
关键词	医院、内鬼、非法出售他人信息
触犯法条	《网络安全法》第四十四条、第四十五条
机构责任	公开资料未明确

建设运维管理疏失

某医院遭恶意重复挂号影响正常使用案

案件回顾：

2019年3月，某地警方接**报警**称，某三甲医院在线挂号系统疑似遭攻击导致运行缓慢。经查，嫌疑人冯某为预约挂号方便，利用其发现的该医院挂号系统漏洞，制作软件在挂号系统后台重复无效“挂号”、“退号”近29万次，一定程度上影响了预约挂号系统正常运行和患者网上预约体验感。警方依据《网络安全法》第27条、第63条规定，对冯某予以行政拘留3日。

违法/犯罪主体	个人黑客
违法/犯罪性质	外部入侵
所属行业	医疗卫生
影响范围	政企机构利益、**公众利益**
关键词	挂号系统被破坏、漏洞
触犯法条	《网络安全法》第27条、第63条
机构责任	公开资料未明确

黑客攻击

某地医院遭勒索病毒攻击业务停摆被处罚案

案件回顾：

2019年1月，某地公安局接到报警，称辖区某医院服务器被黑客攻击植入勒索病毒，医院业务全面“停摆”。该公安机关立即开展刑事侦查，同时启动“一案双查”工作机制对医院存在的网络安全管理问题开展行政调查。经民警调查，发现该医院未按照网络安全等级保护制度的要求履行安全保护义务，医院后台系统、医院网站等放置在同一服务器中，未采取防范网络攻击的技术措施及重要数据备份措施。公安局网安支队依据《网络安全法》第二十一条、第五十九条规定，对该医院予以一万元罚款，对直接负责的主管人员予以五千元罚款。

违法/犯罪主体	个人黑客、政企机构
违法/犯罪性质	外部入侵
所属行业	医疗卫生
影响范围	政企机构利益、**公众利益**
关键词	不符合等保标准、勒索病毒、业务停摆
触犯法条	《网络安全法》第二十一条、第五十九条
机构责任	不履行安全保护义务

黑客攻击

05 安全建议

十大工程，五大任务

十大工程

- 新一代身份安全
- 重构企业级网络纵深防御
- 数字化终端及接入环境安全
- 面向云的数据中心安全防护
- 面向大数据应用的数据安全防护
- 面向实战化的全局态势感知体系
- 面向资产/漏洞/配置/补丁的系统安全
- 工业生产网安全防护
- 内部威胁防控体系
- 密码专项

五大任务

- 实战化安全运行能力建设
- 应用安全能力支撑
- 安全人员能力支撑
- 物联网安全能力支撑
- 业务安全能力支撑

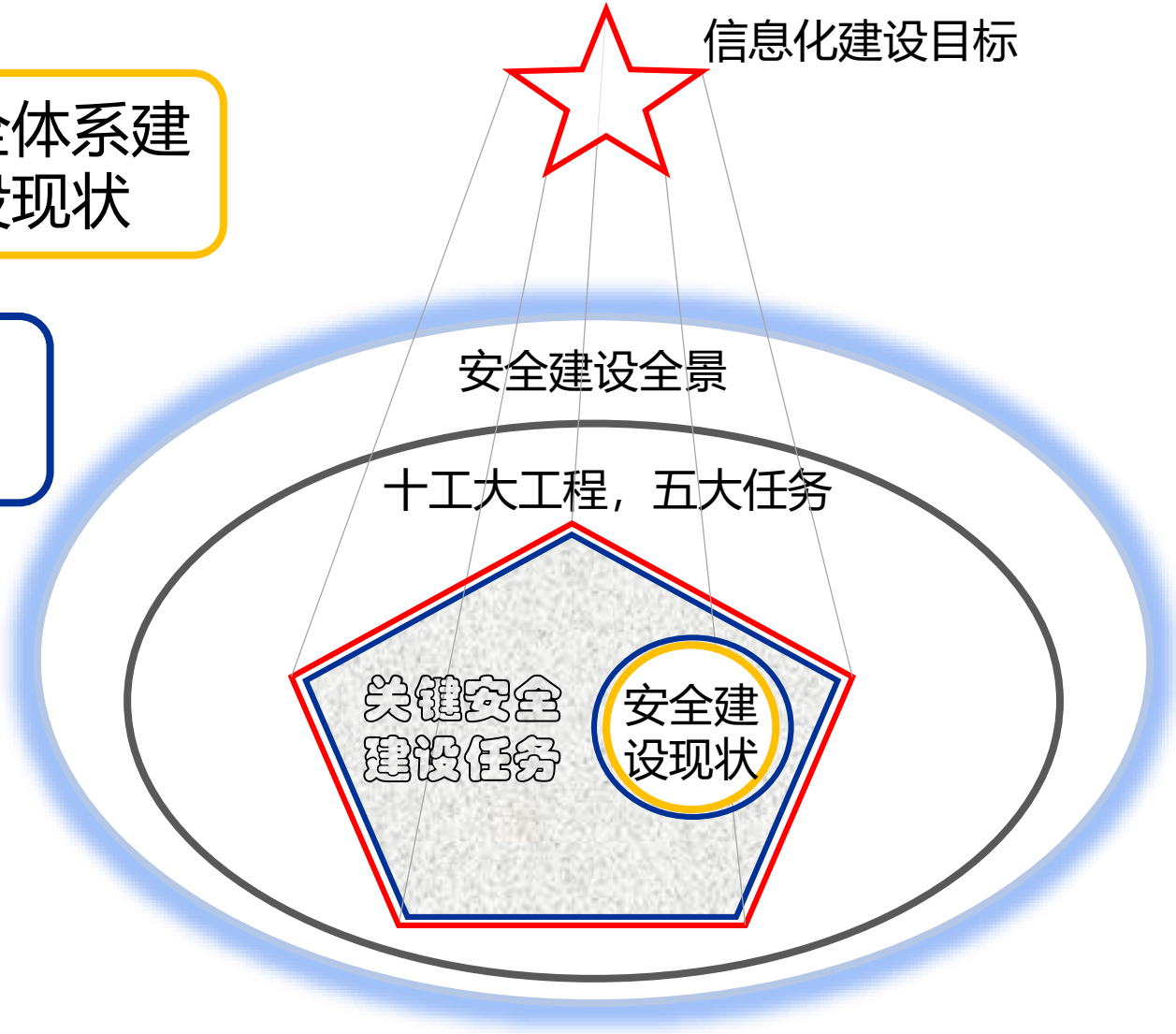
甲方视角、信息化视角、全景视角

网络安全规划建设的“超级公式”

信息化规划范围 ⊙ 十大工程五大任务 - 安全体系建设现状

= 关键安全建设任务（协同联动、整体运行）

如果没有“十大工程，五大任务”，我们该如何排查网络安全的建设盲点？运气 or 经验？




2020北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE
THANKS
全球网络安全 倾听北京声音

医院网络安全管理模式的思考

刘敏超

解放军总医院 信息中心 主任

2020北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE

医院网络安全管理模式的思考

解放军总医院信息中心 主任 刘敏超

当前的挑战和未来变化

信息化生态环境的演变：从封闭走向开放

- 传统局域网生态环境转向“互联网+”生态环境

医院信息安全管理面临的挑战

- 医院业务的内涵与开展方式在迅速变化
- 医院应用的信息技术在快速演化
- 信息产业蓬勃发展导致对医院信息化的虹吸效应

未来变化：全开放全连接

- 深度融合与连接：产学研医联动，全球通力合作
- 底层支撑不可知不可控：运营商的5G、多云…

新技术带来的挑战

+ 大平台、大共享、大数据
+ 互联网+公共卫生、医疗、医保、医药
+ 物联网、云计算、5G、AI

新技术促进了医院新业务模式的发展

但新的威胁又该如何应对呢?

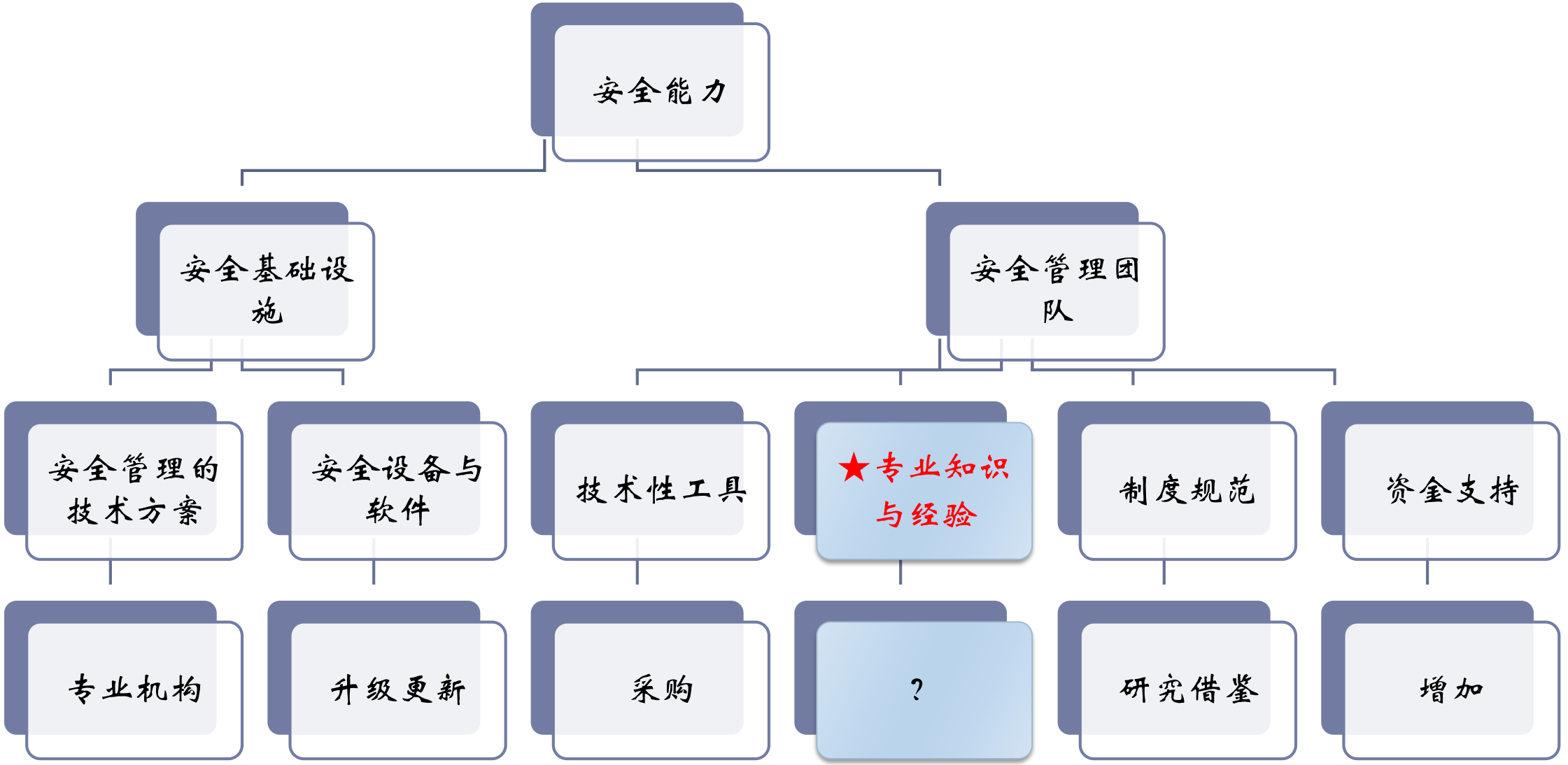
医院网络安全管理的特点

- 医院网络安全管理的特征
  - 全局性
  - 持续性
  - 安全风险的隐蔽性
  - 动态性
  - 实时性
  - 专业性
  - 攻防不等对性
  - 基础条件的局限性

故障点	机房	弱电间	服务器及存储硬件，网络硬件	网络故障或终端故障
故障现象及原因	停电、空调停运、漏水、失火、自然（或人为）破坏	停电、空调停运、漏水、失火、自然（或人为）破坏	损坏、被盗、故障、性能不满足要求	性能突然下降、死机、网络中断、黑客攻击、**病毒攻击**
措施	Z专业化机房建设；机房监控；机房巡视；门禁	UPS；备份；巡视；属地化管理等	硬件备份；加密；巡视与监控；数据备份；网络配置备份；厂商支持；定期升级硬件	规划业务负载；冗余链路；**升级病毒库；**网络技术人员进修；厂商支持；**终端管理；移动介质管理；漏洞扫描；恶意代码监测；**
故障点	数据库	核心业务数据	业务应用系统	人工操作
故障现象及原因	性能下降、宕机、用户数限制	损坏、丢失、存储满	性能下降、严重bug	误删除、大查询导致核心服务能力下降
措施	业务分布式配置 剥离非核心业务 实时监控 定期调优	定期备份与恢复 控制软件研发质量 管控第三方软件研发	第三方厂商准入管理 管控第三方软件研发	加强技术培训；严格操作规程； 加强权限管理； 研发与生产环境隔离；

- 医院网络安全管理的核心目标
  - 持续提升安全管理能力。
  - 医院网络安全管理不是面对一个具体问题寻求解决方案或者完成一项具体的信息化任务，而是要帮助医院适应一个复杂多变、未知但充满风险的环境。

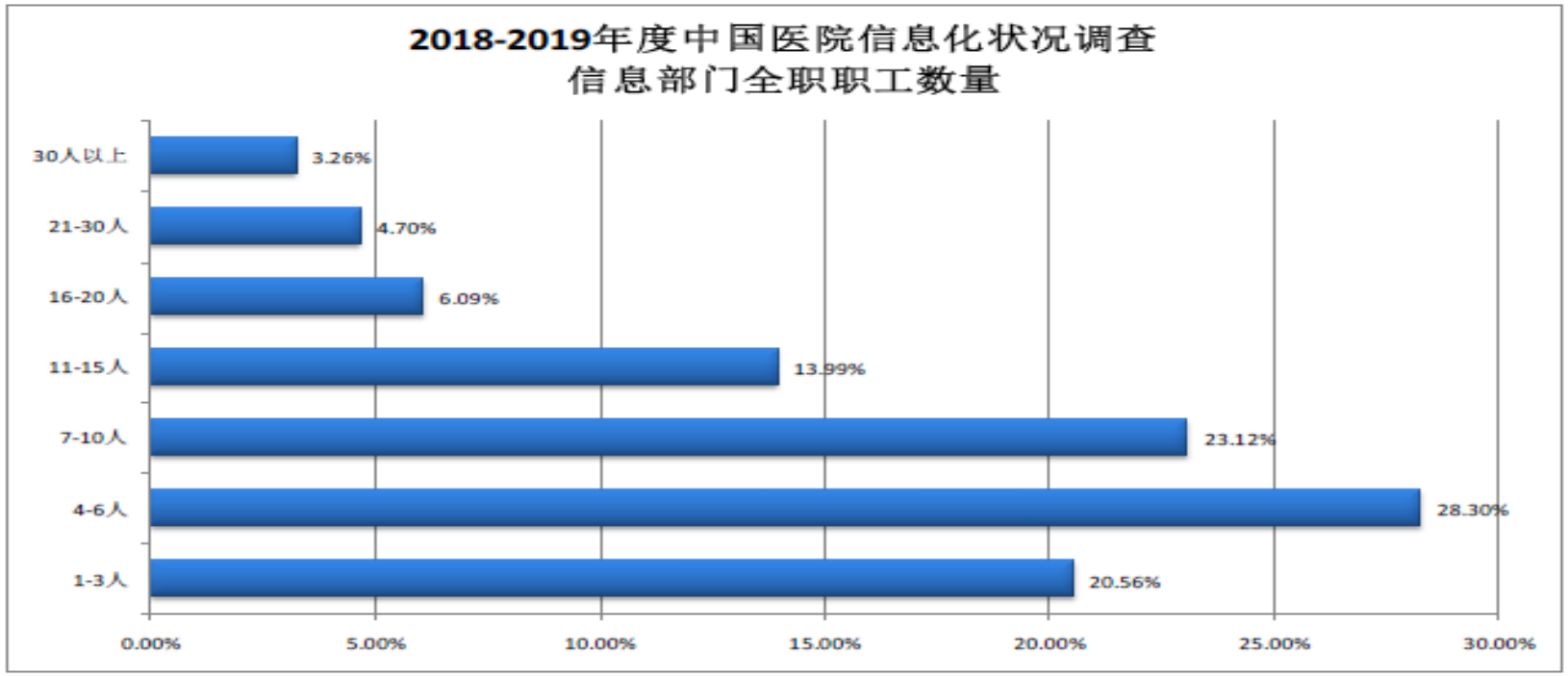
网络安全管理就是安全能力建设



医院网络安全能力不足


安全运营人员
数量不足
分析响应人员
能力不足
攻防渗透人员
培养成本
基础结构安全
强身健体
ARCHITECTURE
纵深防御
纵深防御
PASSIVE DEFENSE
积极防御
监测响应
ACTIVE DEFENSE
威胁情报
掌握敌情
INTELLIGENCE
进攻反制
先发制人
OFFENSE
人员需求

医院信息化团队现状



摘要

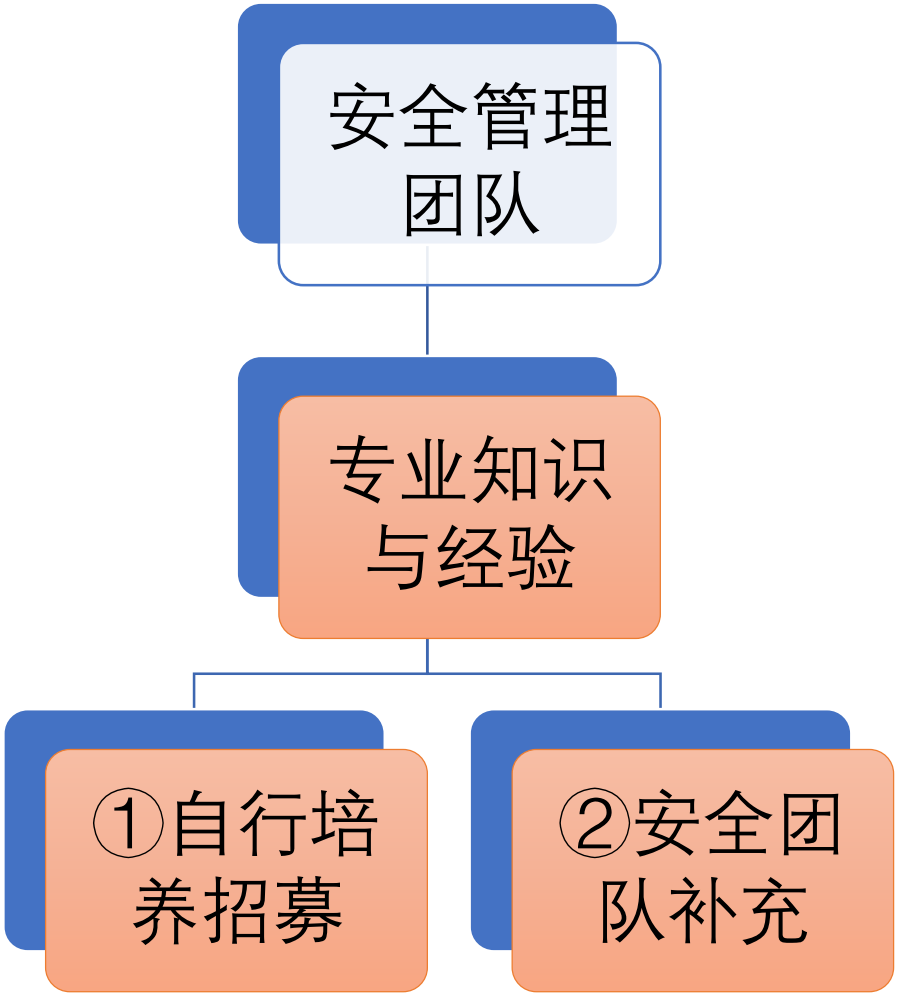
2018-2019 年度参与调查医院样本总量为 1909，通过筛查去除本指标不合格样本数据后以总样本 1873 为基数进行汇总。参与调查的医院其信息部门全职职工平均为 9.16 人，比去年的 9.52 略有降低。大部分参与调查医院信息部门的职工数量集中分布在 10 人以下，占样本总量的 65.40%。平均每一个信息化部门全职职工管理床位 97.24 个，与去年的 99.62 个床位相比略有降低，每位信息职工负责床位数呈逐年降低态势。

描述

对本次调查中关于信息化部门全职职工数量的 1873 个有效数据进行分析可见，参与调查的医院其信息部门全职职工平均为 9.52 人，比去年的 9.92 略有降低。详见参看下面分层数据。全职职工总人数 4~6 人居多，占样本总量 25.08%(79 家)。总体来看，职工数量集中分布在 10 人以下，所占样本量达 65.40%。而大于 10 人的医院数量较少，仅占 34.60%。详细数据见图 1.3.3_1，表 1.3.3_1。

数据来源于CHIMA中国医院信息化现状调查2018-2019年度医院信息技术负责人调研报告

医院安全管理的几种思路



- **思路1：自行培养招募**
  - 组建完善的安全管理技术队伍
  - 负责医院网络安全规划、指导与评估
  - 负责安全管理工作的执行
- **思路2：院外安全团队作为补充**
  - 维持精简安全管理技术队伍
  - 负责安全管理工作的执行
- **思路3：外包安全管理团队**
  - 无自有技术团队，仅有协调人员
  - 院外安全管理团队常驻技术力量
- **思路4：网络安全服务全外包**
  - ？未来


2020北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE
THANKS
全球网络安全 倾听北京声音