



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

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

◦ 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

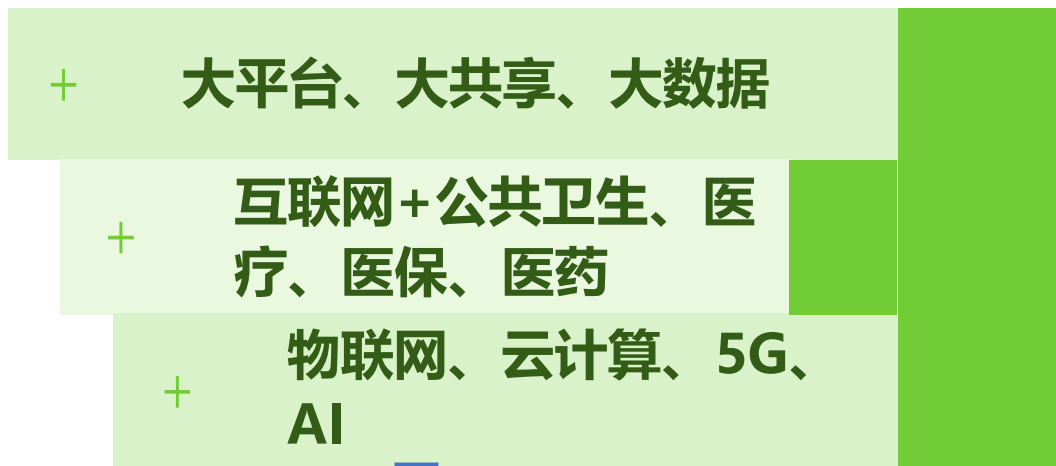
- 深度融合与连接：产学研医联动，全球通力合作
- 底层支撑不可知不可控：运营商的5G、多云…



新技术带来的挑战



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



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

• 医院网络安全管理的核心目标

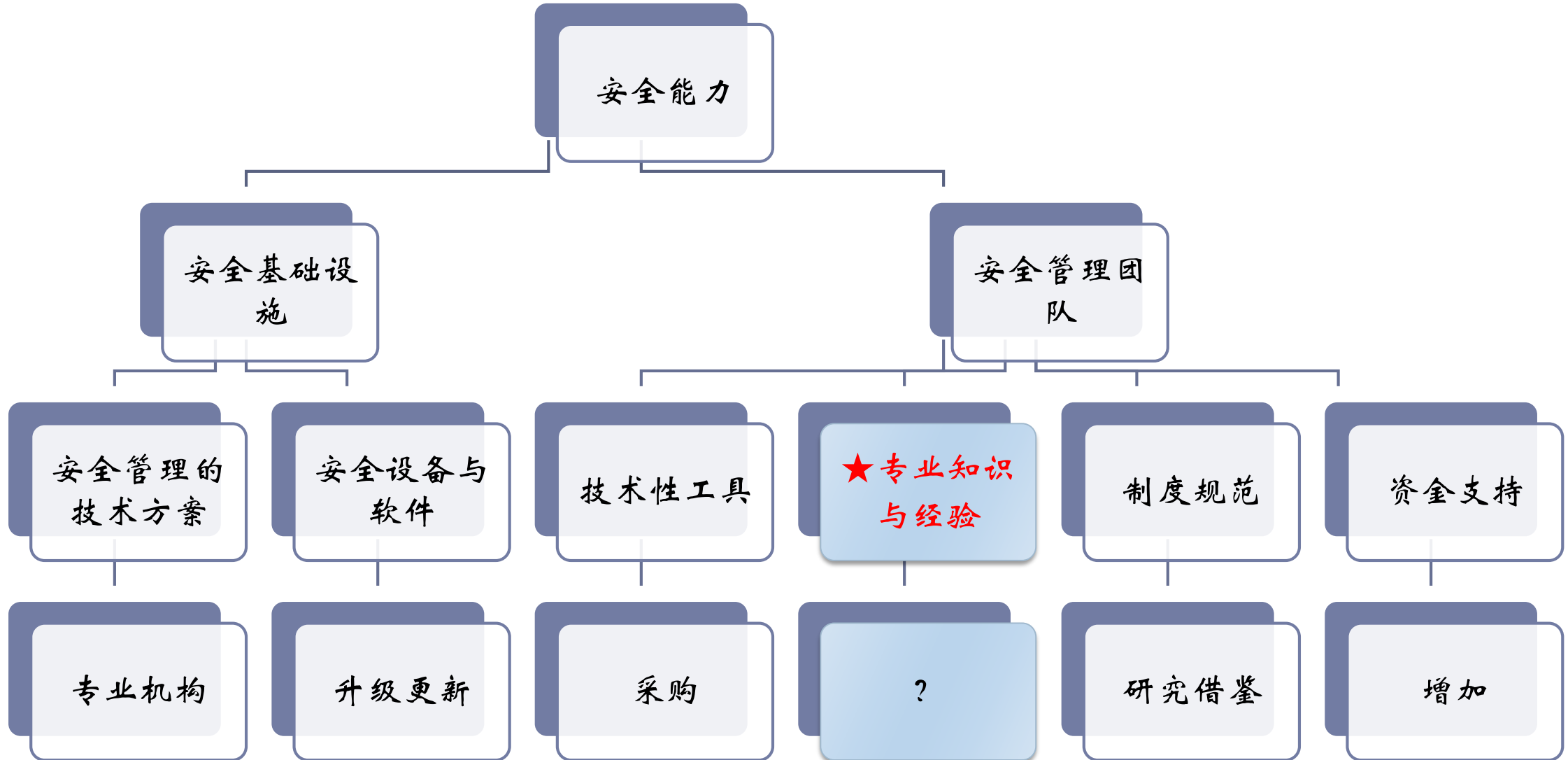
- 持续提升安全管理能力。
- 医院网络安全管理不是面对一个具体问题寻求解决方案或者完成一项具体的信息化任务，而是要帮助医院适应一个复杂多变、未知但充满风险的环境。

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；

网络安全管理就是安全能力建设



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



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

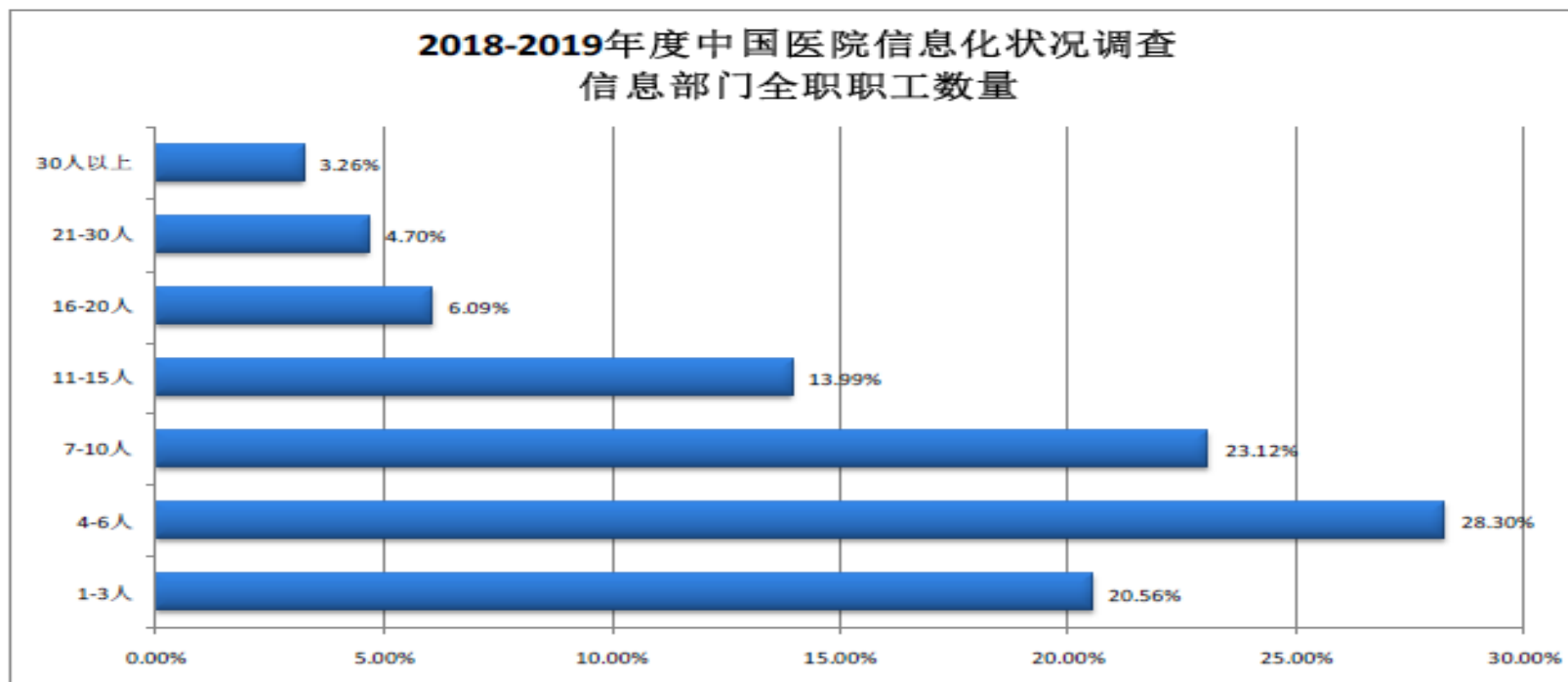
INTELLIGENCE

进攻反制

先发制人

OFFENSE

人员需求

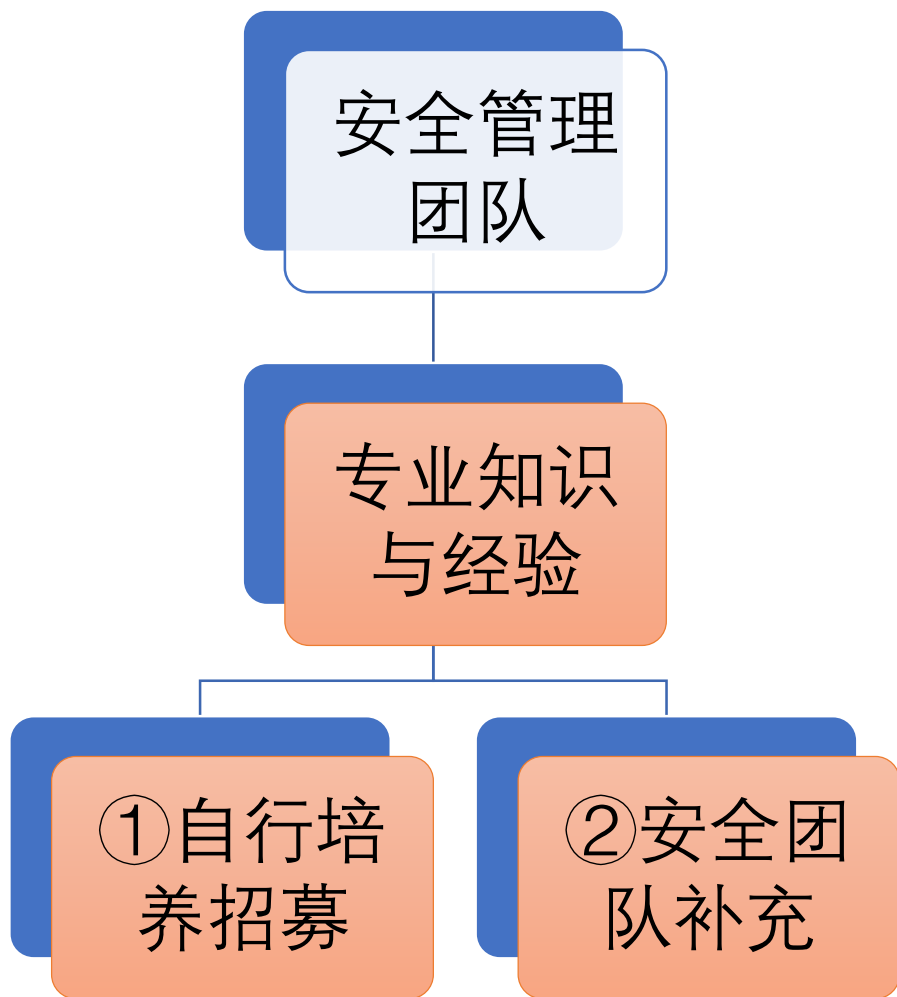


摘要

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。



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