医疗行业安全指数报告

(2018 年 8 月)

出品单位:

目录

一、概述

医疗服务信息化是国际发展的趋势。也是我国医疗改革的的重要内容和必由之路，随着信息技术的快速发展，越来越多的企业和医疗机构加入到医疗信息化的建设浪潮中。

互联网医疗火热背后，医疗信息安全问题如影随形。近年来，针对医院的勒索、挖矿、医疗信息泄露等医疗行业的信息安全事件层出不穷，医院信息系统已经成为了不法黑客的重点攻击对象之一。

本报告由腾讯智慧安全研究发布，中国医院协会信息管理专业委员会（CHIMA）提供医疗行业信息化状况调查报告，双方基于大数据对医疗行业安全状况进行了客观、量化的评估，深入分析了医疗行业的典型安全威胁以及所面临

的潜在安全风险，并尝试引导性的进行行业安全治理、规避潜在的安全风险，提升安全管理水平。

报告以安全大数据及第三方授权或公开的信息和数据为基础，结合抽样分析/调查报告等方法，经综合整理、分析得出。其主要选取了信息化程度高，管理水平强的大中型医院和指标数据作为参考对象，涵盖 956 家三级甲等医院、7 家第三方医疗服务平台，包括 92 个授权网站、79 个患者 APP（安卓版）等外部网络资产。另外本报告还参考了由中国医院协会信息管理专业委员会（CHIMA）发布的《2017-2018 年度中国医院信息化状况调查报告》（以下简称《调查报告》）。

自《中华人民共和国网络安全法》颁布，在卫健委指导下，全国医院信息安全建设水平不断提升。从指数总体来看，全国医疗行业指数值处于良好水平（759 分）。

然而，2018 年至今，我国医疗体系遭受攻击的频率呈明显上升趋势，医疗信息安全环境并不乐观。黑客入侵攻击、信息泄露等安全问题对医院等公共机构的威胁仍不容忽视。

从安全指数所指向的问题来看，医疗行业信息安全建设意识薄弱，核心数据缺乏有效的安全防护。问题主要表现为：

- 网络空间资产端口开放较多，隐患大，如开放远程登录服务的比例高达 50%；
- 外网电脑的安全风险较多，可能会给不法访问者以可乘之机；
- 线上服务平台及第三方医疗服务平台脆弱性会提升医疗数据泄露的风险；

- 医疗行业已经成为勒索病毒攻击的主要目标，医疗业务连续性受到挑战。

二、安全指数情况

2.1 安全指数评估

安全指数说明

本报告联合团队基于安全大数据、人工智能分析技术和威胁实时感知能力，从多个安全维度和安全特征，对医疗行业整体安全态势进行了全面、客观的威胁分析和脆弱性评估，并在全面风险量化分析的基础上汇总得到了“腾讯智慧安全指数”。

安全指数以多个不同维度的安全问题评估为基础，在安全问题评估的基础上分别汇集到相应的安全域，对各个安全域进行加权汇总，得到了企业安全指数。然后按照行业属性，对企业安全指数求均值即可得到行业互联网安全指数。

安全指数以客观安全数据为依据的特性，使其一定程度上能够反映行业安全趋势，具有先导性、预测性。进一步地，利用该安全指数，可对相关行业进行安全状况差距对比、安全问题洞察等。更多关于安全指数的定义和计算的详情，见附录。

安全指数是介于 0~1000 区间内，数值越高，其安全状况越好、风险水平越低。不同指数区间，反应的响应安全状况如下表所示。

指数值	含义
0~499	较差
500~699	一般
700~899	良好
900~1000	优秀

表 2_1_1 指数的含义映射表

安全指数态势

除港澳台以外的各省市、自治区具体数据来看，北京市、上海市、吉林省、重庆市、山东省的安全指数排名最高，安全指数均高于 770，排名靠后的几个省（市）安全指数值均低于 750 分

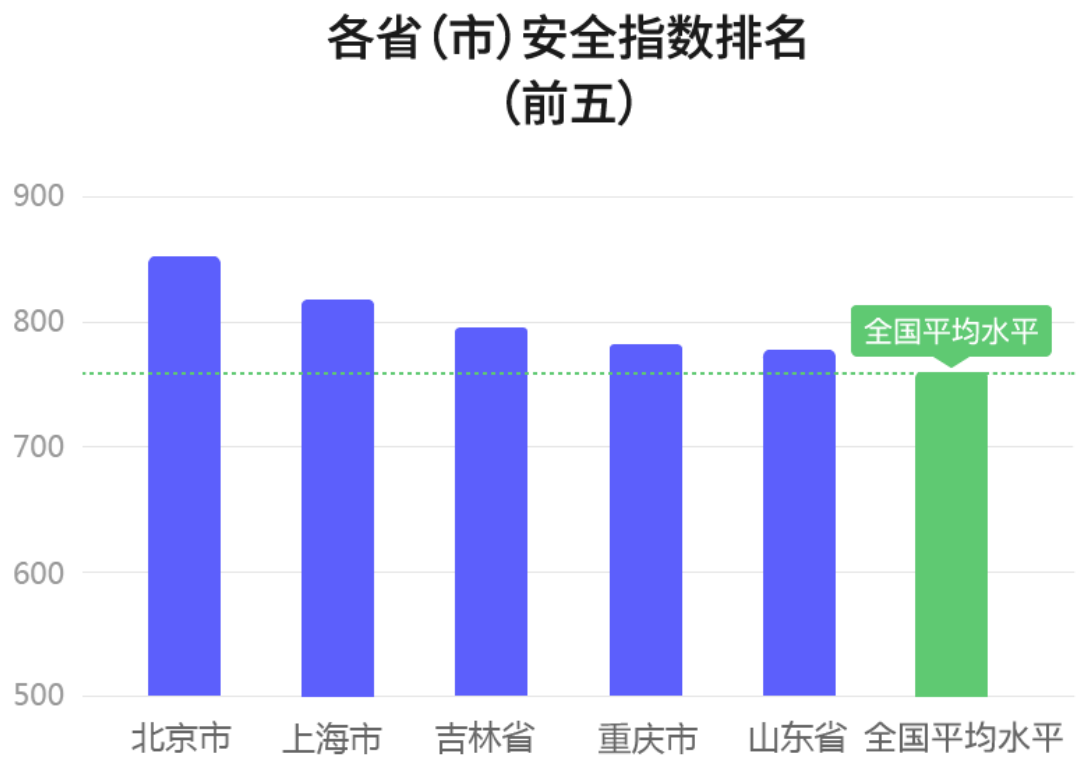

图 2_1_1：各省（市）安全指数排名（前五）

以国内（除港澳台以外）各医院的维度来看， 医院安全指数的分布如下：

●..22%的医院安全指数处于优秀水平；

●..38%的医院安全指数处于良好水平，

●..39%的医院安全指数处于一般水平；

●..1%的医院安全指数处于较差水平。

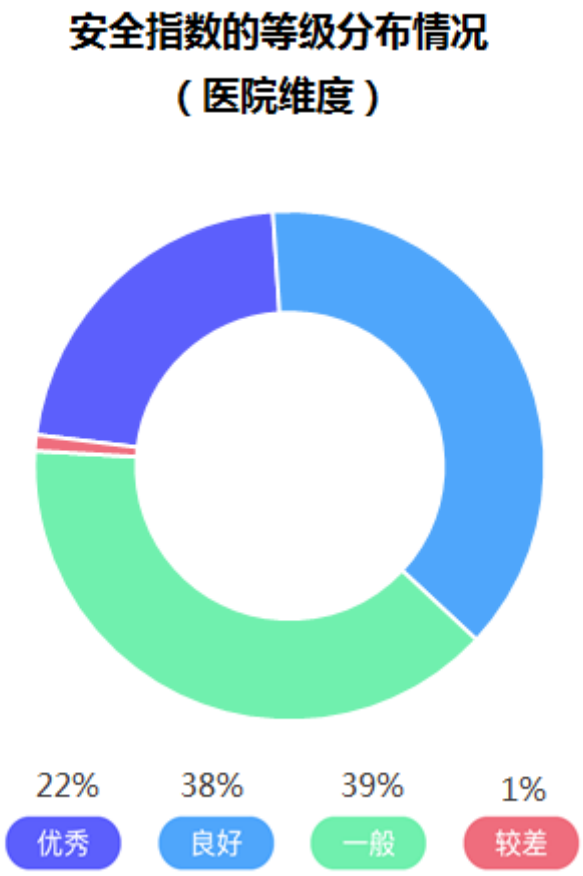

图 2_1_2：安全指数的等级分布情况（医院维度）

目前医疗行业面临的问题主要集中在主机安全、应用安全和网络安全。如图 2_1_3 所示，其安全指数值越低，风险越高。

图 2_1_3：医疗行业网络安全指数情况(除港澳台以外)

2.2 安全措施采用情况

安全措施采用情况，引用了由中国医院协会信息管理专业委员会（CHIMA）发布的《2017-2018 年度中国医院信息化状况调查报告》中的调查数据，该调查报告共收到反馈的调查报告 535 份，其中有效答卷 484 份，分别对应 484 家相互独立，没有重复与关联的医院。484 家医院占到全国医院总数的 1.8

0%。样本覆盖除香港特别行政区、澳门特别行政区以及台湾省以外的 29 个行政区。数据详情可参阅《2017-2018 年度中国医院信息化状况调查报告》。

医院实施等级保护情况

从调查数据来看，有 36.16%的医院通过了等级保护测评。经济发达地区实施等级保护工作的比例高于中等发达地区和经济欠发达地区。

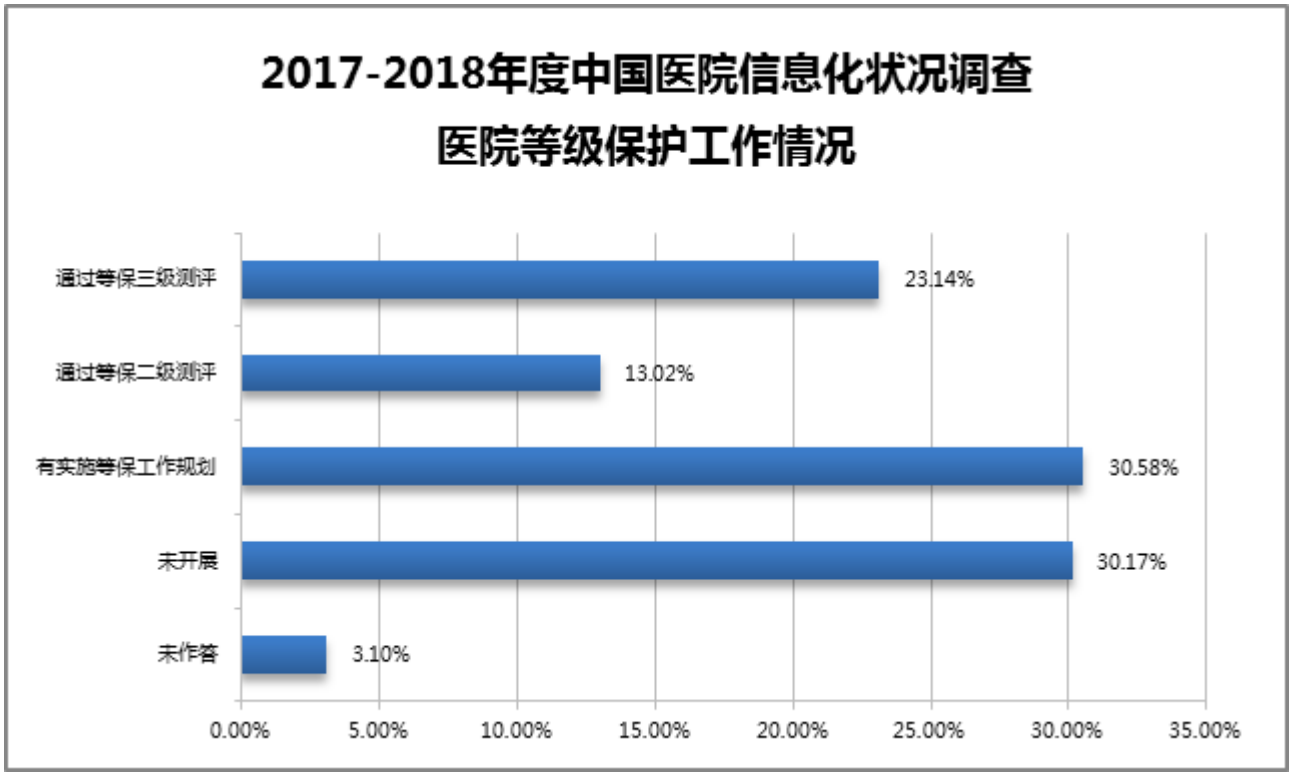

图 2_2_1：医院等级保护工作情况

系统安全措施采用情况

对参与调查关于医院采用的操作系统级安全措施的有效数据分析可见，网络版反病毒软件的采用率仍高居首位，比例为 71.07%。排在第二位到第五位的分别是桌面管理软件 46.49%、软件防火墙 38.22%、系统镜像快速恢复 26.45%、单机版反病毒软件 24.79%。

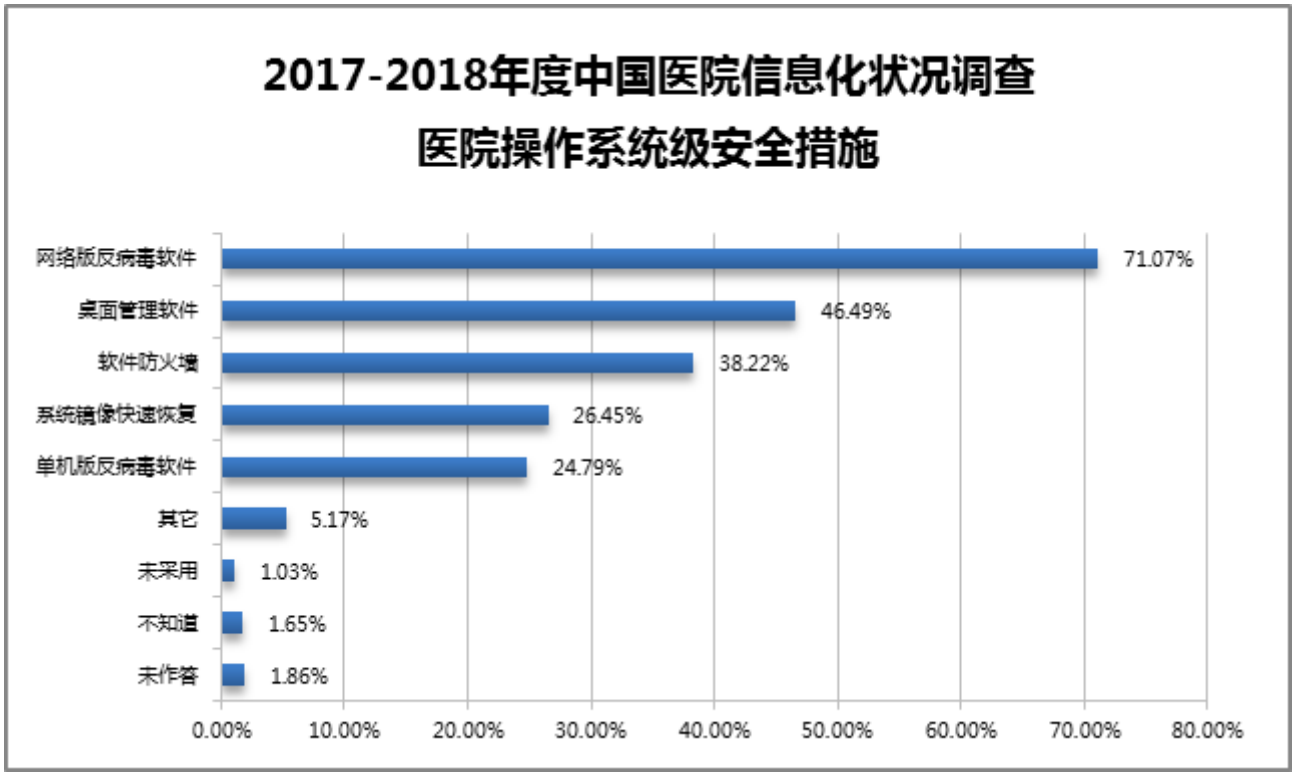

图 2_2_2：医院采用的操作系统级安全措施

对调查关于医院采用的信息系统体系结构安全措施的有效数据分析可见，主要应用服务器双机热备的医院比例仍然最高，达到 72.31%，其次是服务器集群，采用率达为 48.55%，位于第三位的服务器冷备机采用率为 26.45%。

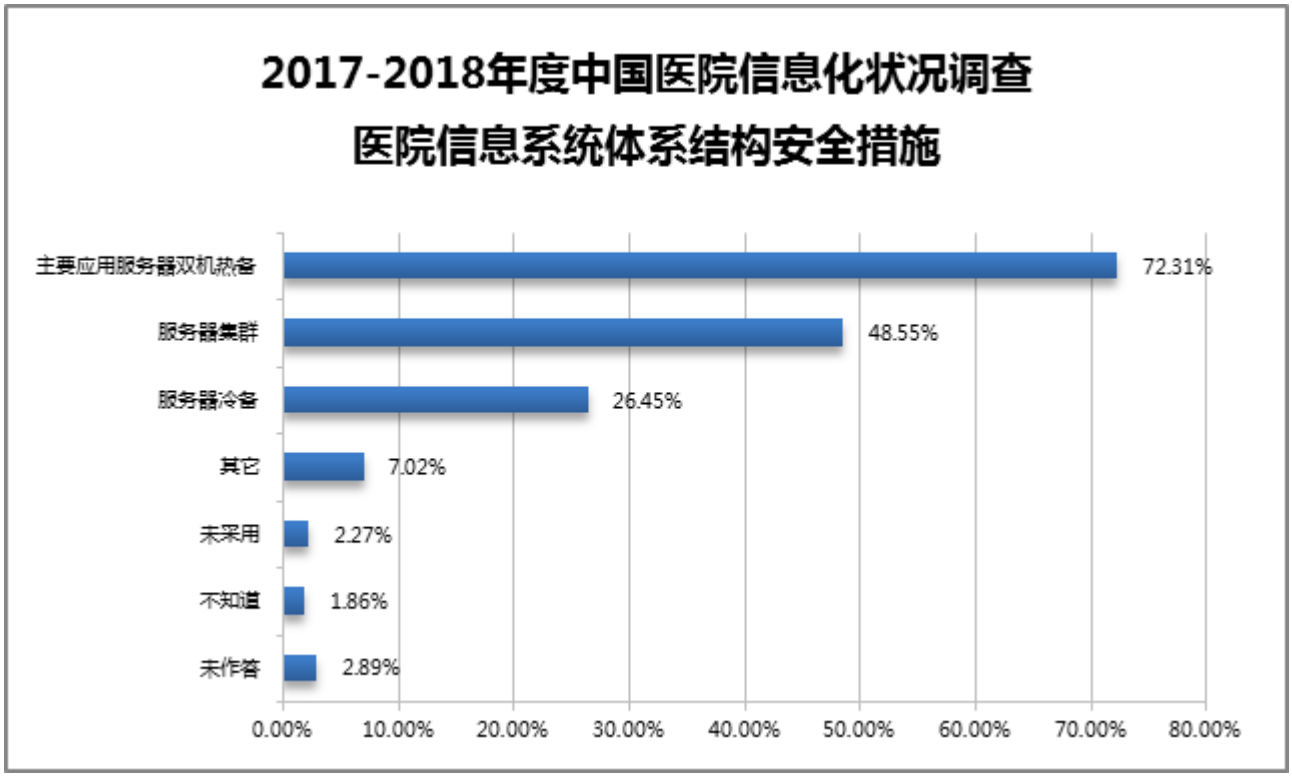

图 2_2_3：医院信息系统体系结构安全措施

数据安全措施采用情况

从调查中医院采用的各种数据安全措施分析看，数据灾备、数据库镜像备份、数据冷备份和数据离线存储仍然是医院主要的数据安全措施。

对调查关于医院采用的数据安全措施的有效数据分析可见，排在第一位和第二位的是数据灾备和数据库镜像备份，比例接近半数分别为 49.79%和 49.17%，排在第三位至第七位的分别是数据冷备份、数据离线存储、集中存储异地镜像备份、数据库行为审计和身份认证，采用率分别为 41.74%、40.91%、22.11%、20.66%和 13.43%。

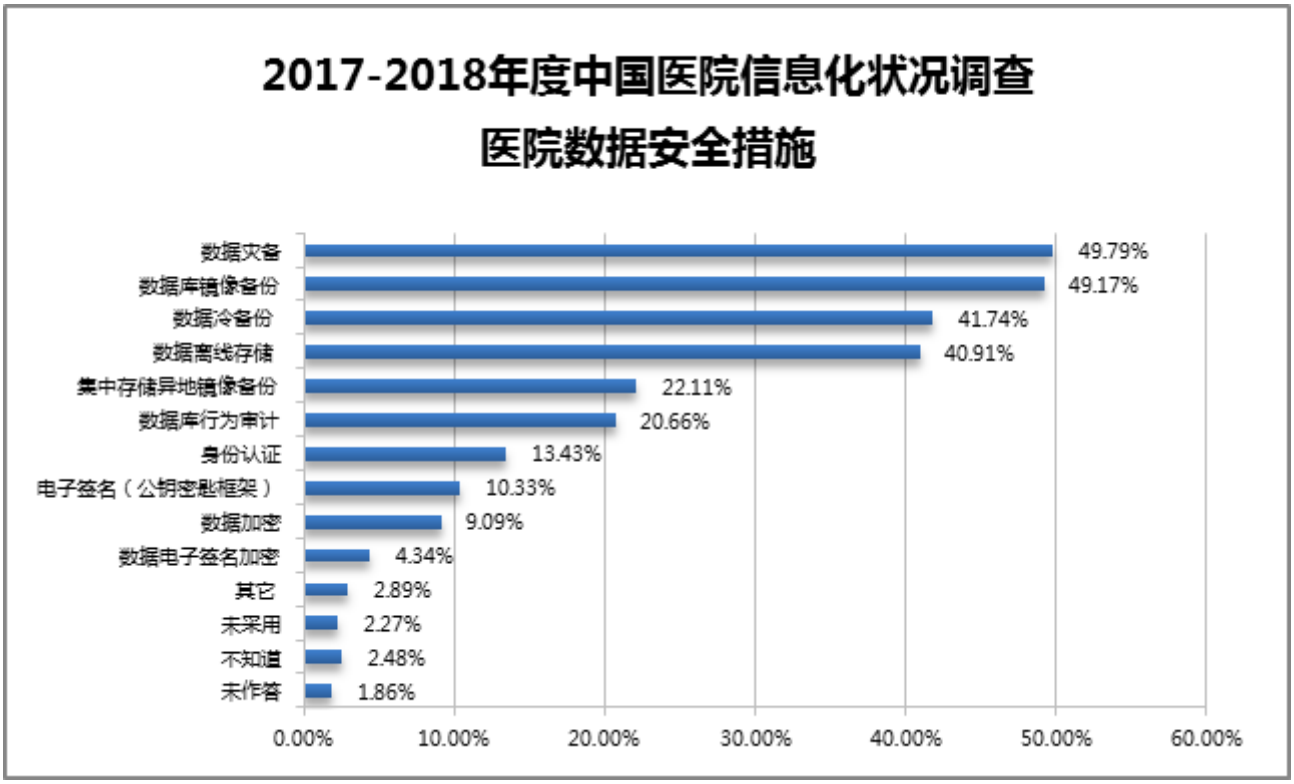

图 2_2_4：医院数据安全措施

网络安全设备和隔离网络情况

现阶段我国医院采用的网络安全措施中，防火墙设备的采用率高居首位。不同级别医院在应用各种网络安全设备方面均具有极显著性差异。

对参与此次调查的医院采用的网络安全设备类别分析可见，采用率位列前六的分别是防火墙、VPN 设备、物理隔离设备、网闸设备、入侵检测设备和防毒墙，比例均超过 20%，其中采用防火墙的医院比例达到 82.02%，远远高于其它设备，说明防火墙是多数医院首选的网络安全措施。

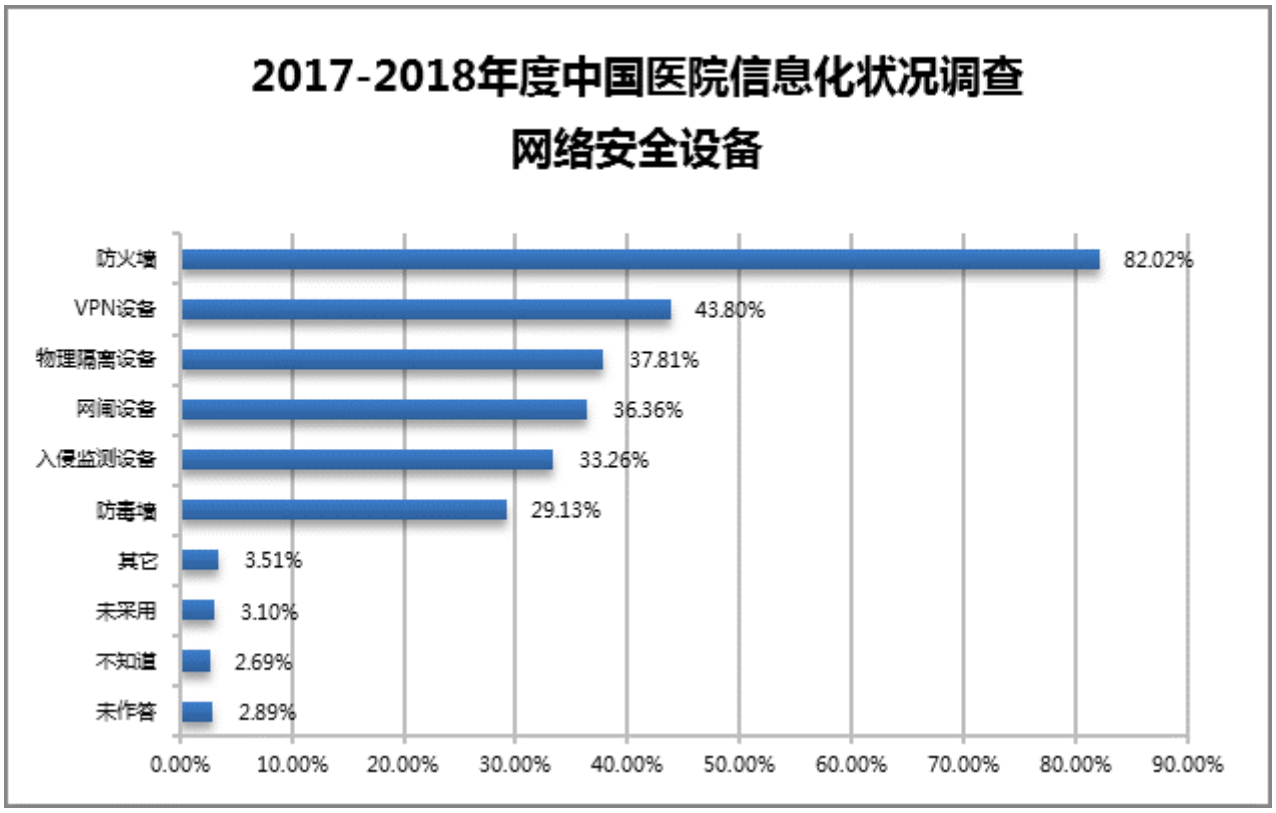

图 2_2_5：医院采用的网络安全设备

在参与调查的医院中，大部分医院拥有独立并物理隔离的网络，网络数量多于 1 个的医院已超过半数，达 54.55%；绝大多数医院的网络主干带宽达到百兆及百兆以上，占总样本量的 86.98%；

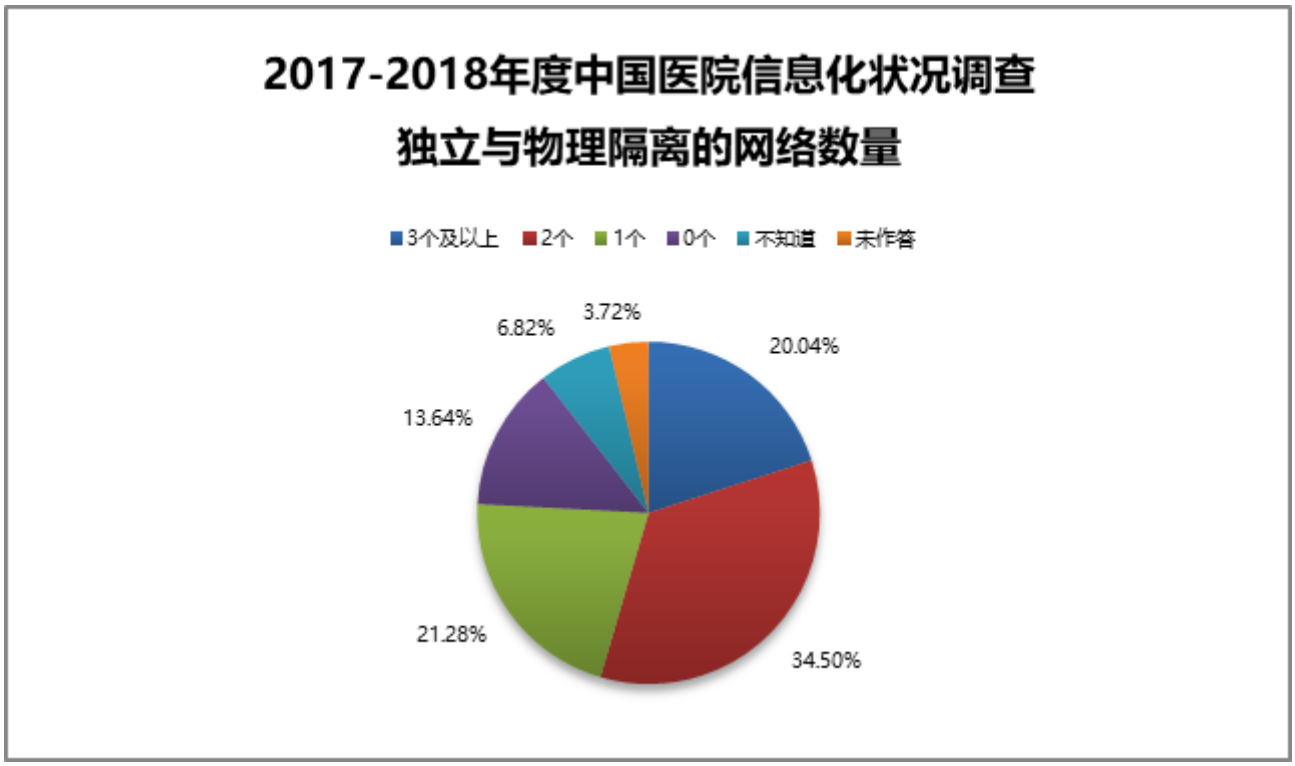

图 2_2_6：独立而且物理隔离的网络数量

三、风险详细分析

3.1 医疗行业成黑客攻击重要目标

数据的经济价值驱使不法分子铤而走险

由于医院等机构的特殊性，患者预约信息、检查检验信息、就诊信息、医学数据等医疗信息都是属于需要紧急使用的信息，一旦这些数据被加密勒索，就会造成很大的影响，医院会想尽办法尽快恢复数据。

以美国互联网黑市的信息售价为参考，数据丰富的医疗信息的价值是信用卡信息的 10 倍。欺诈者利用这些精准信息可以进行电信诈骗、虚假医疗广告营销等违法活动。这些具有较高商业价值的诊疗信息，受到黑色产业链的觊觎。

利用外网资产的弱点进行攻击

外网资产的安全关乎内网的安全。黑客一般通过攻击外网服务器和办公网电脑系统实现对内网的攻击和数据的窃取。

通过攻击外网服务器获取外网服务器的权限，继而利用成功入侵的外网服务器作为跳板，攻击内网其他服务器。

另外一方面，通过钓鱼、挂马等社工攻击的方式，实现对办公电脑的控制或数据洗劫，从而获取进入内网的入口信息（帐号、密码等），或者直接对有价值的办公网系统实施勒索等破坏性攻击。

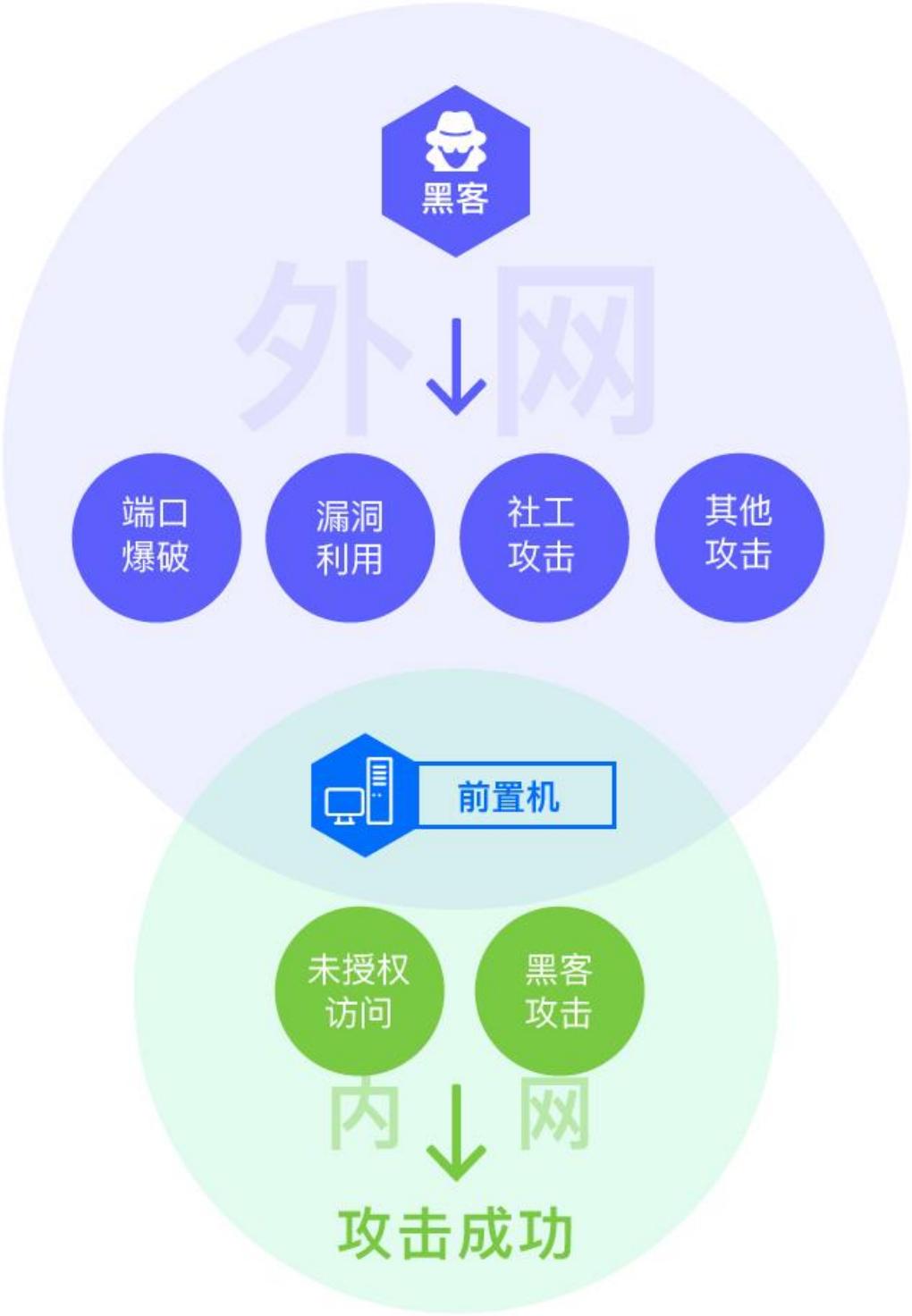

图 3_1_1：黑客攻击/入侵内网示意图

3.2 主机安全隐患较高

网络空间资产端口开放较多，隐患大

基于第三方网络空间资产测绘，国内仍有多家三甲医院的 Web 网站和出口 IP 的资产存在较高的安全隐患。

我们在空间测绘的结果中筛选出最近几年黑客攻击事件中出现频率较高的端口，发现全国有不少医疗单位仍然开放着这些高危端口。3306 端口、3389 端口的开放比例（分别为：3.43%和 1.41%）明显高于国内全网相应端口的开放比例（分别为 1.38%和 1.01%）。此外，还有较大比重的邮件服务、数据库服务等端口暴露在公网上。

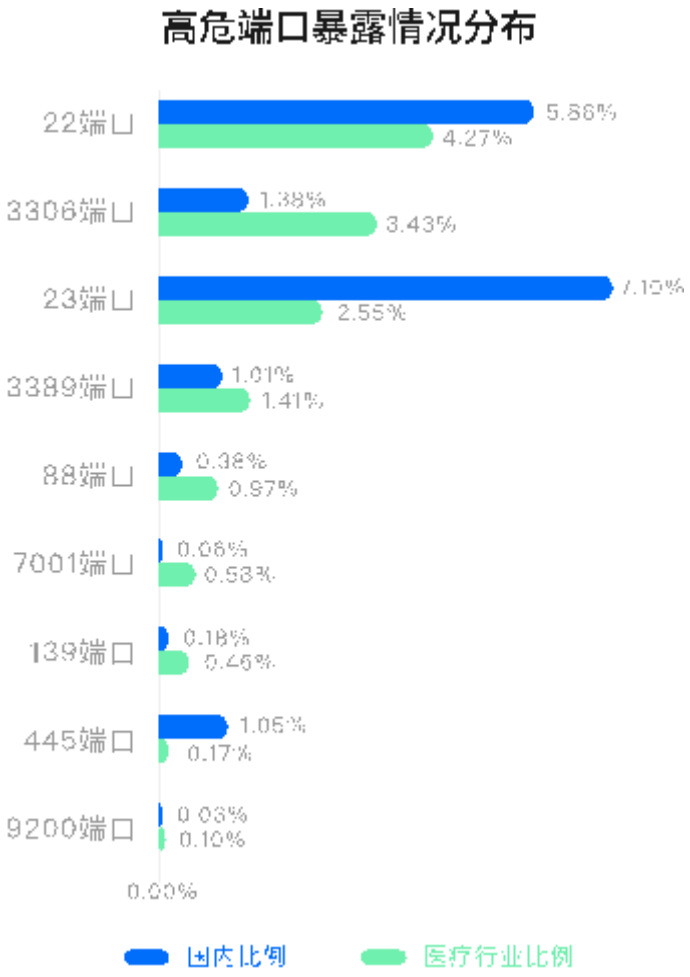

图 3_2_1：高危端口暴露情况

数据库是几乎所有黑客都觊觎的东西，所以数据库系统直接暴露在外网是非常危险的行为，而使用默认端口的数据库暴露在外网会极大减低黑客攻击的难度，增加被攻击的风险。

根据测绘结果统计分析，全国医疗行业的数据库端口开放最多的是 3306 端口，超出其他数据端口的开放，详细状况如下：

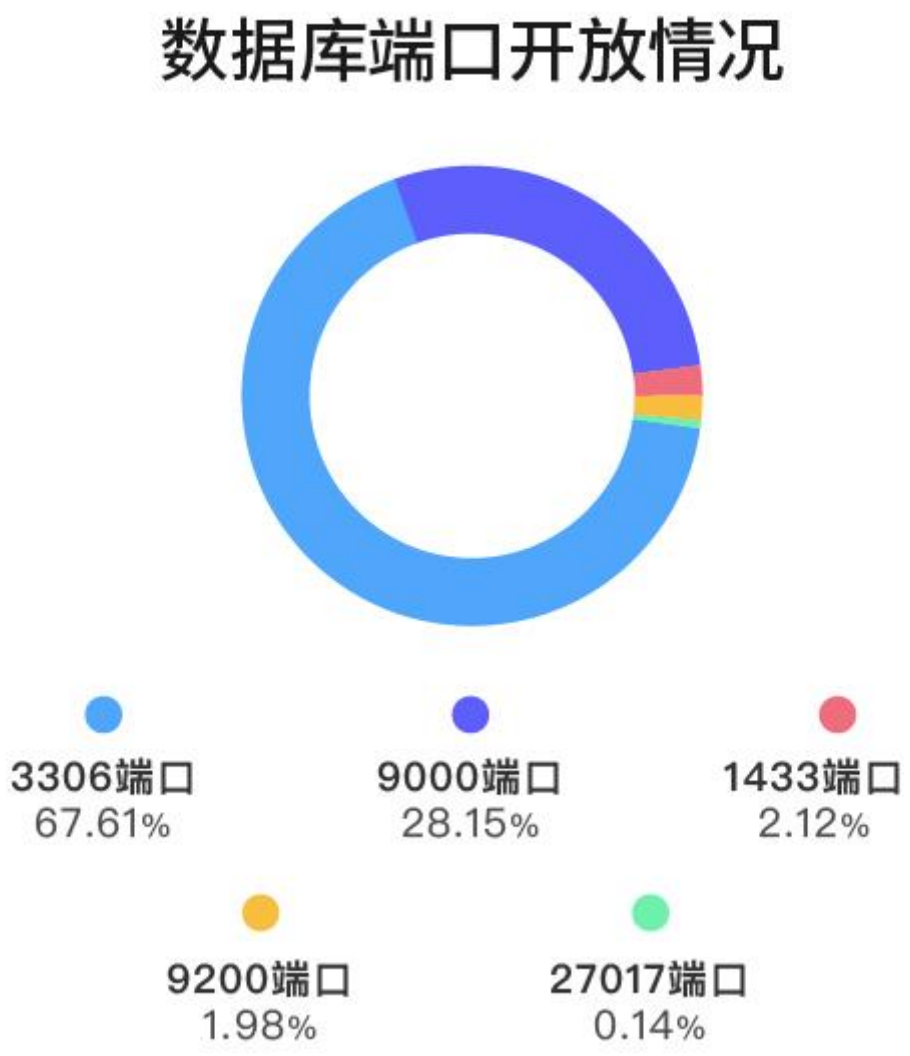

图 3_2_2：数据库端口开放情况

数据库攻击者，除了窃取数据信息（拖库）之外，还可能针对数据库的数据实施经济勒索攻击。攻击者先将数据库进行备份，然后利用远程命令删除数据库从而实施勒索。

最典型的勒索攻击莫过于 2017 年 5 月份爆发的 WannaCry，该病毒会对公网随机 IP 地址的 445 端口进行扫描感染。

根据测绘结果分析，仍有部分省份的医疗机构开放了 445 端口。如果这些服务器没有打上相应的补丁，那么仍然存在被勒索病毒攻击的风险。即便是打上了补丁，也仍然需要面对勒索病毒变种的攻击。

外网电脑存在较多风险

基于对腾讯智慧安全终端产品的防护数据的分析得出如下结论

医院环境中，30%的电脑系统存在待修复的高危漏洞，与全网环境的情况一致；

12%的医院有外网电脑曾被入侵并植入挖矿木马；

15%的医院有外网电脑存在勒索病毒的破坏行为。

图 3_2_3：外网电脑存在的主要风险

3.3 应用安全脆弱性凸显

随着互联网+医疗的发展，越来越多的医院借助 WEB、患者 APP、第三方医疗服务平台等形式，提供网上预约挂号、网上缴费、网上查询报告等多项线上医疗服务。更便利的是，第三方医疗服务平台还可同时为多家医院提供线上挂号预约、体检预约以及医生咨询等服务。

抽样统计发现，全国大中型医院中，有 87.4%的医院提供线上服务，73%的医院提供线上预约挂号服务，51.7%的医院提供线上缴费服务，56.4%的医院提供线上检验化验报告查询服务。超过半数的大型医院提供了较成熟的线上医疗服务。

从《2017-2018 年度中国医院信息化状况调查报告》的门急诊管理信息系统实施状况的调查统计数据可以看到，三级医院的患者 APP、第三方平台服务实施率分别在 11.79%和 10.65%。

但线上医疗服务带来了新的漏洞风险和数据泄露风险。

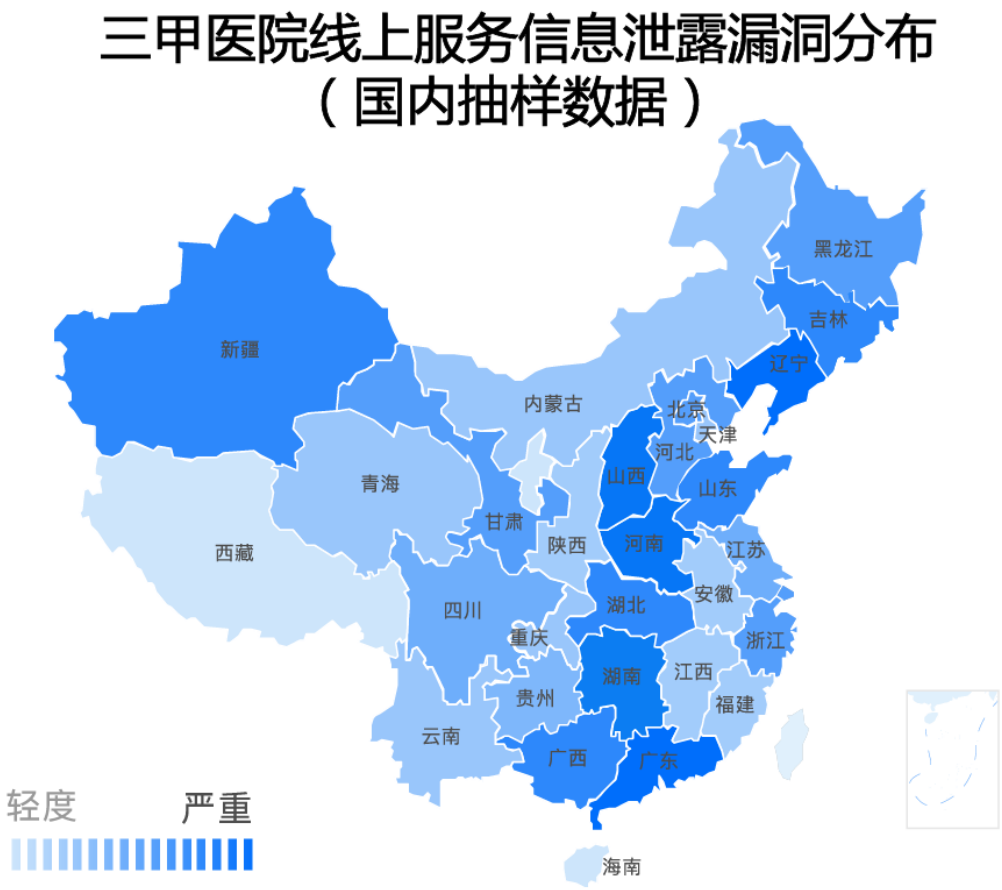

图 3_3_1：三甲医院线上服务信息泄露漏洞分布（国内抽样数据）

患者 APP（Android）存在较多漏洞

基于对国内患者 APP 的抽样调查分析，80%左右的患者 APP 存在漏洞，其中有 67%的患者 APP 存在可利用的高危漏洞。

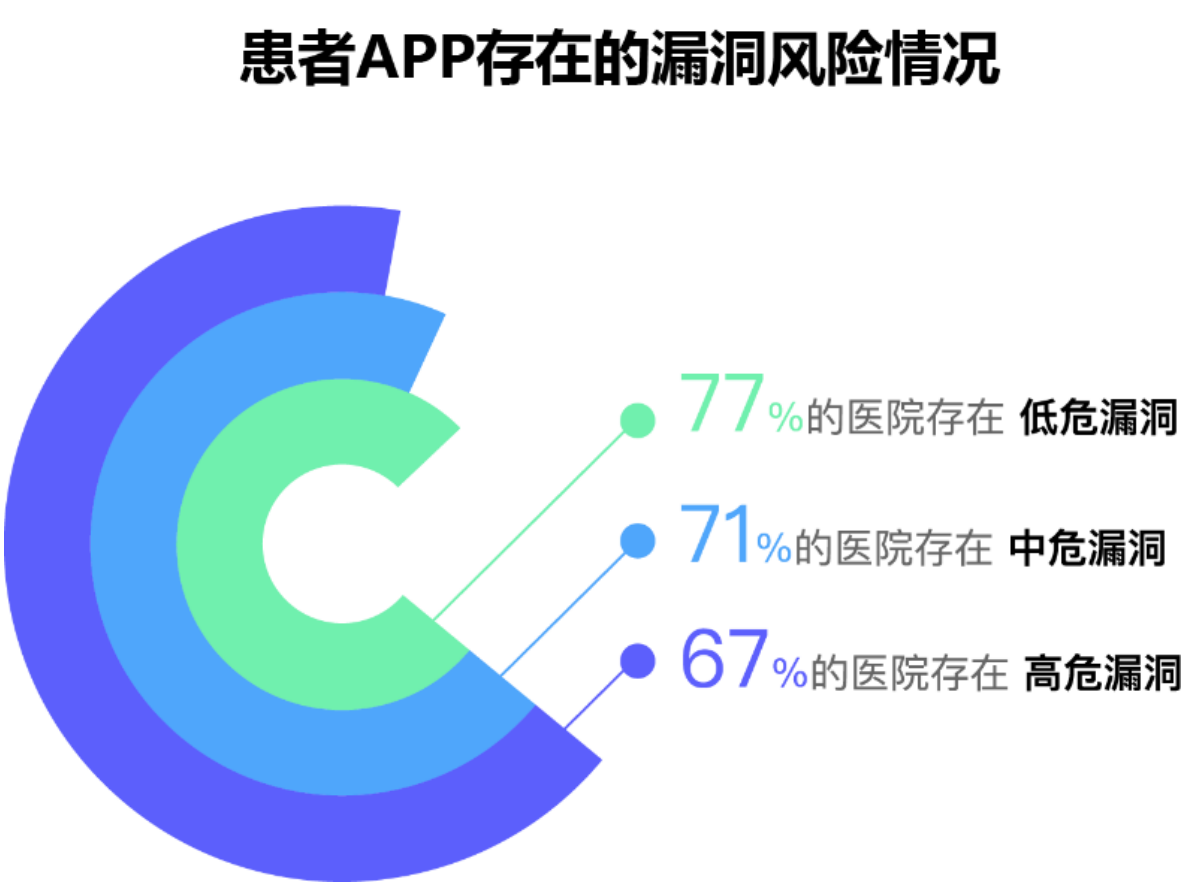

图 3_3_2：医院安卓应用软件存在的漏洞风险情况

高危漏洞主要为以下 5 个漏洞

WebView 组件系统隐藏接口未移除漏洞

Android 主机名\证书弱校验风险

Webview 绕过证书校验漏洞

Android HTTPS 中间人劫持漏洞

WebView File 域同源策略绕过漏洞

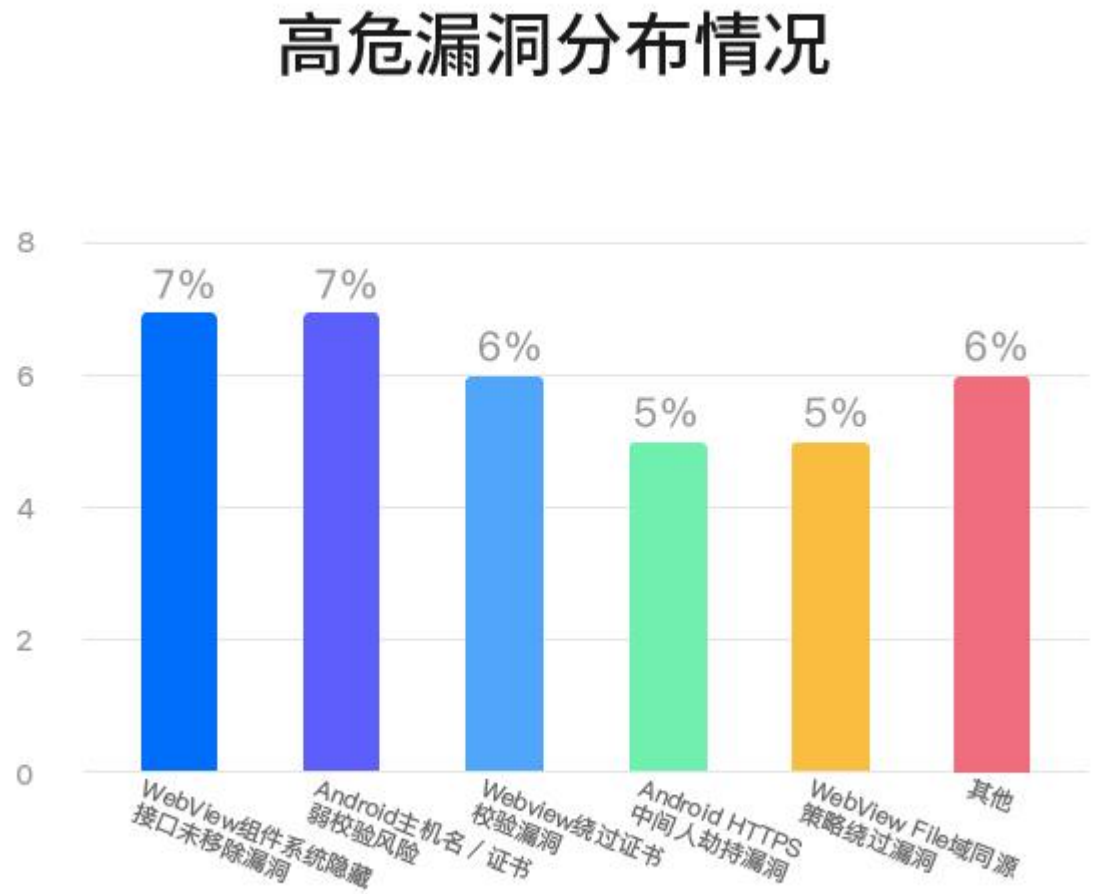

图 3_3_3：医院安卓应用软件存在的高危漏洞情况

第三方医疗服务平台安全值得关注

第三方医疗服务平台多存在严重的信息泄露风险，包括登录绕过、未授权访问、平等越权等问题，可能导致大量患者的姓名、手机号、身份证、以及就诊记录、化验检验报告等多项敏感信息泄露。

今年 7 月安全团队在日常守护全网用户信息安全工作过程中，发现某健康医疗平台存在多个漏洞。经过初步验证，漏洞有可能泄露使用过线上医疗服务

产品的用户的个人信息、挂号信息，以及绑定医疗卡用户的就诊信息、检查报告等。

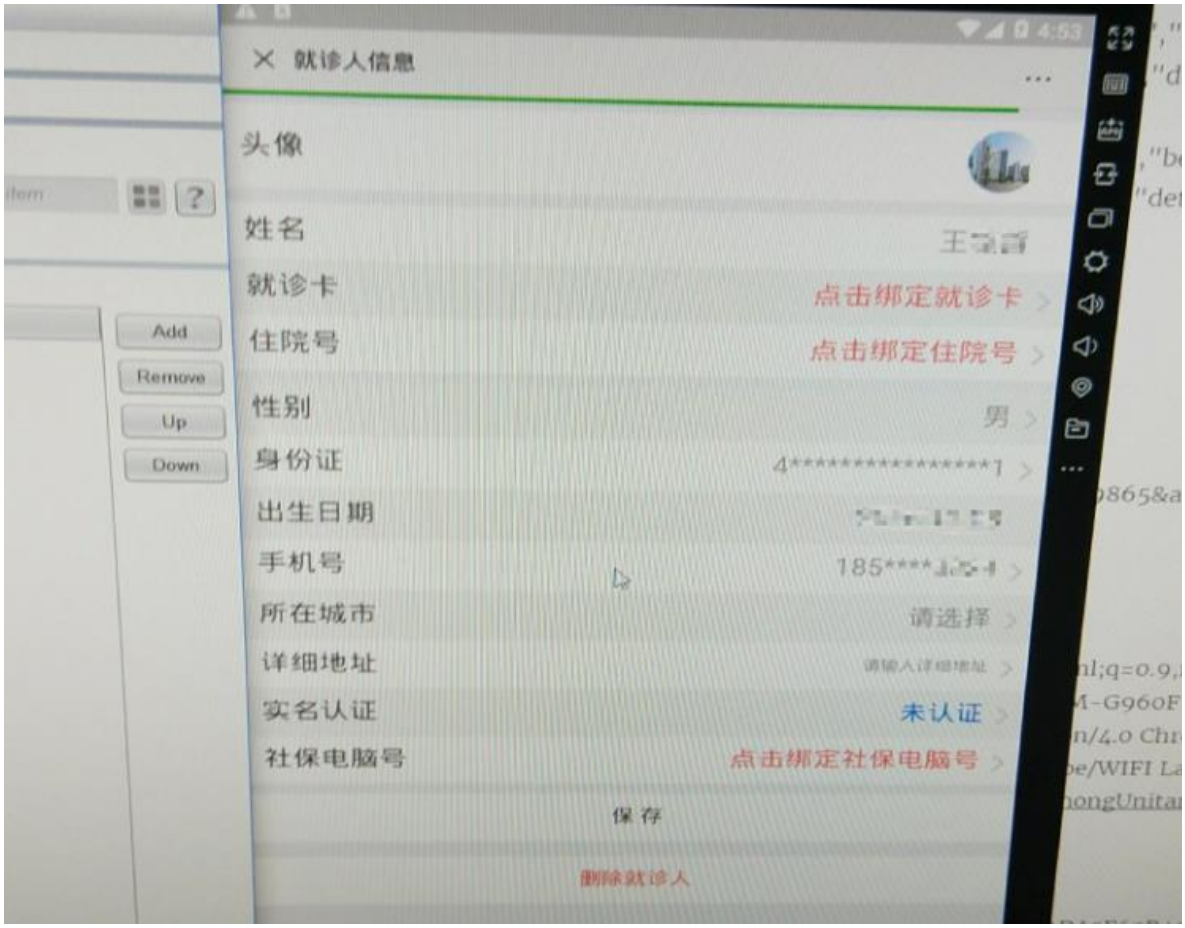

图 3_3_4：某第三方健康医疗平台越权登录演示图

3.4 网络安全面临严峻的威胁

2017 年以来，医疗行业已成为攻击者实施勒索的最主要目标，有 29%的勒索软件的攻击目标是各类医疗相关机构。除勒索外，医疗业务资源被黑客滥用于挖矿，亦会破坏企业内部 IT 环境、数据中心的正常运行秩序以及关键应用的交付，同样使得业务连续性遭受极大安全威胁。勒索、挖矿已经成为影响医疗业务连续性的主要威胁。

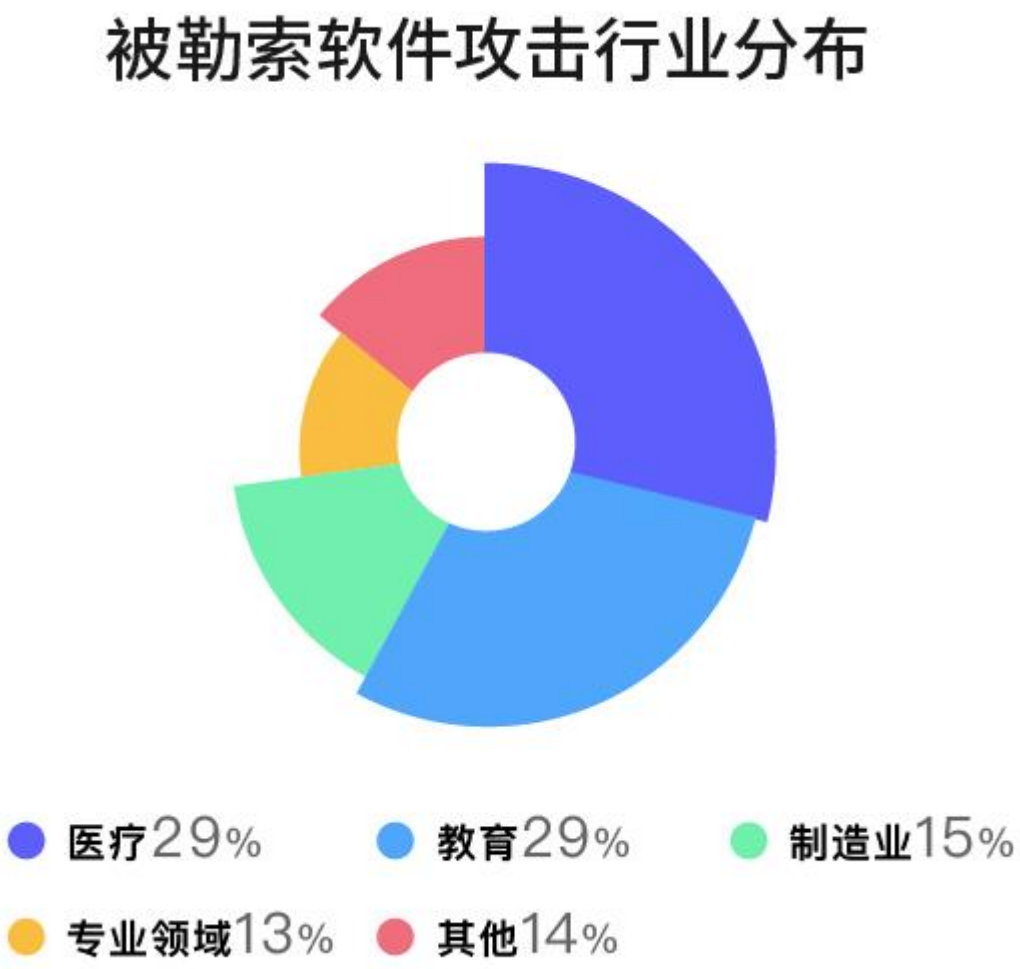

图 3_4_1：被勒索软件攻击行业分布

湖南某医院 GlobeImposter 勒索病毒事件

2018 刚过完年，国内两家省级医院就遭到了黑客攻击，致使其服务器感染 GlobeImposter 勒索病毒，致其系统瘫痪，同时数据库文件被加密破坏，直接影响了正常就医秩序。

湖北某医院遭撒旦（Satan）勒索病毒袭击事件

https://mp.weixin.qq.com/s/E8naBacDKTnK8bIoVJdAyA

安全团队接到湖北某医院反馈，其内部多台服务器遭遇勒索病毒攻击，所有数据类文件都被加密，加密后文件名被修改成“[dbger@protonmail.com]+原

始文件名+.dbger”。安全团队分析发现，入侵该医院服务器的是撒旦（Satan）勒索病毒的最新变种。

国内多家三甲医院服务器遭暴力入侵

https://mp.weixin.qq.com/s/WG__6dwac_bPcoWLf925lg

7 月份国内多家三甲医院服务器被黑客入侵，攻击者暴力破解医院服务器的远程登录服务之后种植多种挖矿木马以攫取经济利益。

3.5 医疗信息泄露问题不可小觑

过去几年，美国医疗服务信息化行业得到了长足的发展，同时，医疗数据泄露事件也呈逐年上升趋势。2015 年地下黑市大约有 1.1 亿条医疗记录需要出售，几乎占据了全美国一半的医疗数据。2017 年媒体报道的医疗数据泄露事件就达到 350 多起。

从美国医疗数据泄露的来源来看，除了内部人员窃取/丢失数据等内因外，更多的是来自外部的黑客渗透入侵、未授权访问/接口暴露等网络攻击威胁。

1、 近年来，由黑客渗透入侵导致的数据泄露事件增速越来越快，已经跃升为第一因素；
2、 由于服务器配置不当、漏洞等因素造成的未授权访问问题也呈增速发展；
3、 内部人员窃取或丢失数据造成的数据泄露问题，近几年来逐渐减少。

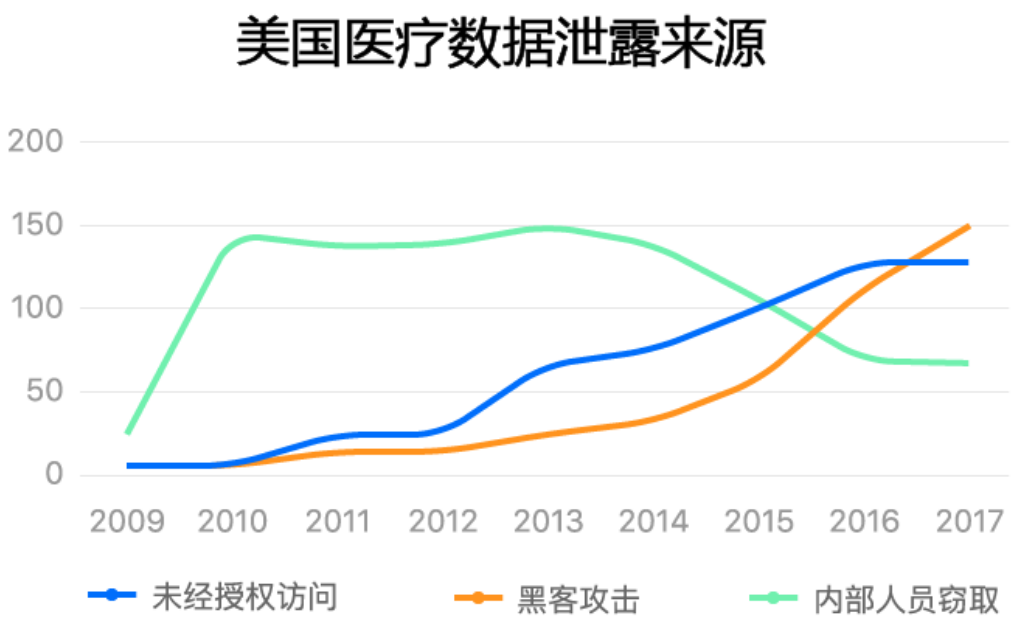

图 3_4_2：美国医疗数据泄露来源

2017 年 9 月《法制日报》曾报道国内某医院的服务信息系统遭受黑客入侵，致超过 7 亿条公民信息遭泄露，8000 余万条公民信息被贩卖。

纵观全球，黑客攻击造成的的医疗信息泄露事件仍然频发。仅在 2018 年过去的几个月中，单次泄露数据大于 500 条的数据泄露事件就发生了数百起，几乎每个月都会发生 3 到 4 起重大医疗数据泄露事件。如：

2018 年 7 月，新加坡政府健康数据库遭黑客攻击，包括总理李显龙在内的 150 万患者数据泄露；

同月，UnityPoint Health 遭网络钓鱼攻击，140 万患者记录泄露。

2018国外医疗安全事件

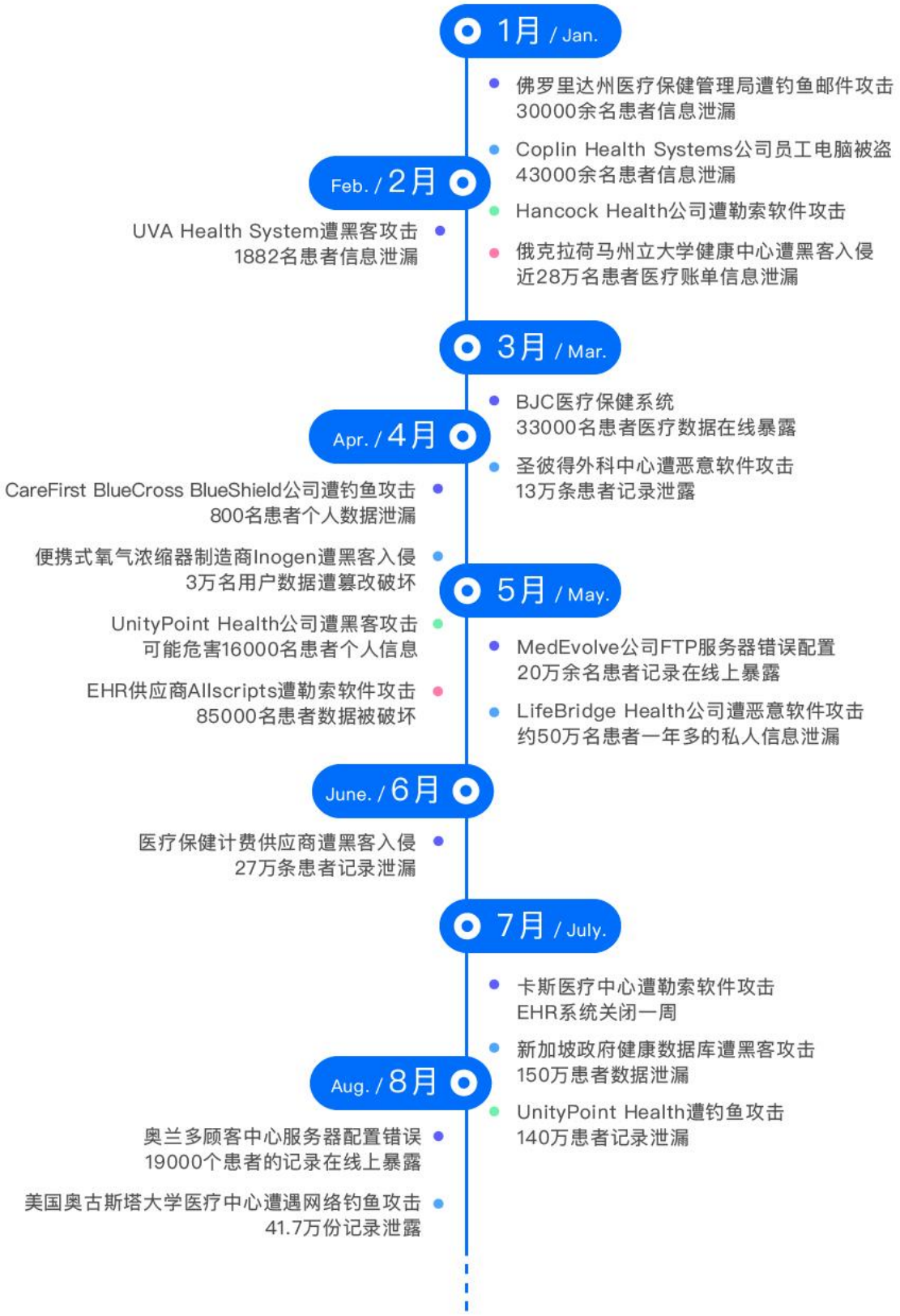

图 3_4_3：2018 国外医疗信息安全事件

四、结语

本报告研究认为，数字经济时代，安全是所有 0 前面的 1。伴随“互联网+医疗健康”推进，医疗企业和机构所面临的网络信息安全风险也被成倍放大，提升安全风险防范意识，加强信息安全体系建设，才能有效保障和驱动医疗信息化的良性发展。

当前，我国医疗信息化建设正在提速，而医疗信息安全建设保障工作也得到了行业普遍关注和重视；解决医疗信息安全相关威胁和挑战，需要继续加强在医疗信息安全领域的投入、建立系统化的安全保障体系：

- 对当前医疗信息化安全系统进行全面体检，定位安全问题，排除安全隐患；
- 选择专业的医疗安全解决方案，建设安全防御体系，降低网络信息安全风险；
- 加强医疗网络信息安全技术团队培训，全面提升安全防御意识和团队素养；
- 定期进行网络信息安全检查及安全防御演练，提升重大威胁应急响应能力；
- 建立面向行业的应急响应协同机制，及时预警联防共治，携手应对网络风险。

五、附录

5.1 指数说明

指数构成

医疗行业安全指数体系由“企业安全指数”和“行业互联网安全指数”两部分构成。

企业安全指数

企业安全指数是一个基础性的综合指数，由覆盖企业安全状况的五大安全域的构成，包括：网络安全、主机安全、应用安全、业务安全、数据和隐私安全。

将用于量化描述每个域的安全状况的值定义为单一指数。基于五个域的单一指数，得到最终的企业安全指数。

行业互联网安全指数

行业互联网安全指数一个汇总结果，是所属企业或机构的企业安全指数的平均值。

其它

基于监管区域或行政管理级别，行业互联网安全指数可按照辖区内的企业安全指数计算相应的区域性行业互联网安全指数。如全国性的行业互联网安全指数、省(市)级行业互联网安全指数等。

数据维度

用于计算企业安全指数的安全问题数据，主要来源于：

- 外部威胁信息：对外部开放互联网情报、暗网情报等进行主动收集和进一步的智能分析，得到企业、行业相关的安全问题；

- 主动监测得到的企业互联网资产、业务等的威胁情况和脆弱性信息：通过直接或间接的方式对互联网资产进行探测、持续监控，进一步的关联到行业、企业，形成对企业安全问题状况分析；
- 企业内部的威胁事件和脆弱性：基于互联网流量、日志以及安全设施数据等，结合威胁情报感知到的企业内部发生的安全问题。

安全问题覆盖

用于进行企业安全状况评估数据全面覆盖五大安全域，包含映射在 43 安全维度的 106 项问题，并支持扩充。

网络安全

基于网络流量、外部威胁情报等数据观测到的与企业安全相关的恶意性网络活动问题。如对企业业务进行的各类型网络攻击的风险，企业访问恶意 IP 的威胁，企业回调僵尸网络基础设施的威胁，企业对外发起攻击的威胁等。

主机安全

基于客户端数据和外部情报数据，识别到的企业或机构的主机上存在的安全问题。例如，主机存在高危漏洞、对外开放高危端口、发现恶意软件、业务被勒索、遭受 APT 攻击等安全问题。

应用安全

基于网络数据、外部情报等，识别到的的应用安全问题。例如。使用存在高危漏洞的组件，web 应用、移动 App 等存在漏洞，未使用安全的通信方式等。

业务安全

基于外部情报、网络数据分析等方式，识别到自身业务或对外提供的服务中的安全问题。例如，存在仿冒网站，身份验证缺失，网站被篡改、挂马等安全问题。

隐私与数据安全

基于对外部情报、社区内容的跟踪分析，识别到与企业、机构相关的数据类安全问题。例如，自身的业务数据、凭据的泄露和交易，用户隐私数据的泄露和交易。

计算方法

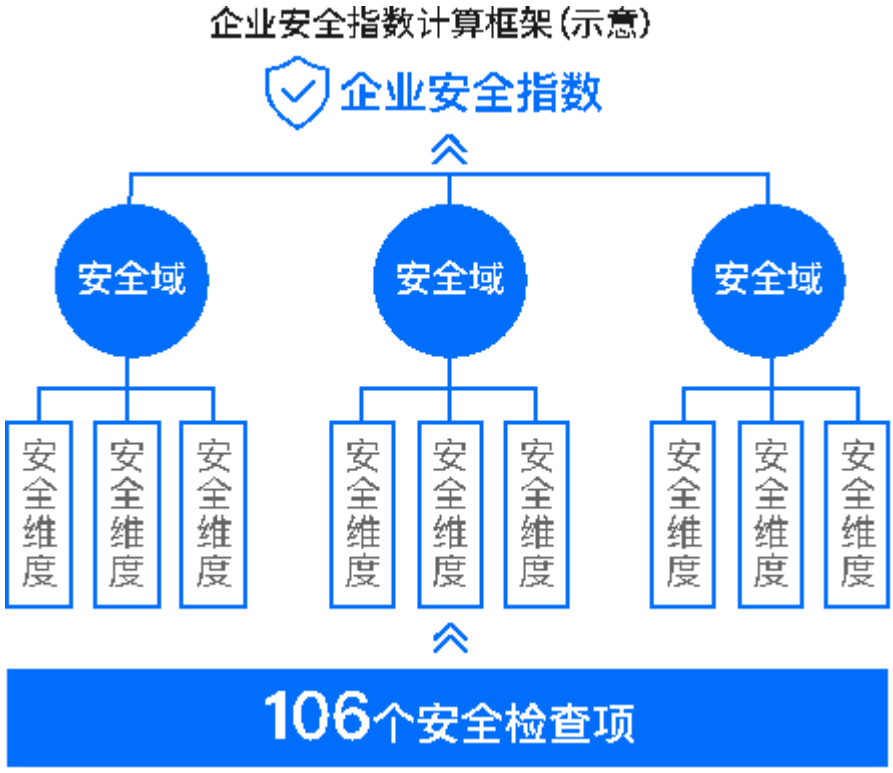

图 5_1_1：企业安全指数计算框架（示意图）

1. 计算预定义安全检查项的基础损失$base_Loss$

$$base\_Loss = Risk * Severity * Asset * Confidence$$

其中$Risk, Severity, Asset, Confidence$为专家对一个安全检查项评估出的指标：

- $Risk$ 风险类型：脆弱性/威胁事件，取值分别为 1 或 2
- $Severity$ 严重性：取值 1-5
- $Asset$ 资产、业务的重要性：取值 1-5
- $Confidence$ 安全问题的准确识别能力：取值 1-5

2. 基于企业在安全检查项的发生频次，计算安全检查项损失$Bbase_Loss$

$$Bbase\_Loss = f(C) * base\_Loss$$

其中C表示企业在该安全检查项的发生频次，$f(C)$为基于安全检查项定义的对其发生频次的映射函数：

$$f(C) = \begin{cases} C, C \le T+1 \\ T + \log(C-T), C > T+1 \end{cases}$$

3. 根据安全检查项的所属安全维度，计算企业在各安全维度的安全值$BDim_Score$

$$BDim\_Score_j = \max(0, 1000 - \sum_{i \in set_j} \alpha_i * Bbase\_Loss_i)$$

其中$BDim_Score_j$表示第 j 各安全维度的得分，$Bbase_Loss_i$表示第 i 各安全检查项损失，set_j表示第 j 各安全维度包含的安全检查项的下标集合，α_i表示第 i 各安全检查项在第 j 各安全维度中的重要性。

4. 基于安全维度得分，计算得到各安全域的安全值$BDomain_Score$

$$BDomain\_Score_k = \sum_{j \in dset_k} \beta_j * BDim\_Score_j$$

其中$BDomain_Score_k$为第 k 各安全域的得分，$BDim_Score_j$表示第 j 各安全维度的得分，$dset_k$表示第 k 各安全域包含的安全维度的下标集合，β_j表示第 j 个安全维度在第 k 各安全域中的权重。

5. 由各安全域的安全值得到企业安全值$Score$

$$Score = \sum_k \omega_k * BDomain\_Score_k$$

其中$BDomain_Score_k$为第 k 各安全域的安全值，ω_k为对安全维度数量设置的域权重。

6. 由企业安全值得到企业安全指数$Security_Index$

$$Security\_Index = g(Security\_Score, factor)$$

其中$Score$为企业的安全值，$g(Score)$为依据该医院的信息化指数等数据，对企业安全值的映射函数。

5.2 报告说明

本报告的内容，包括但不限于描述性信息、数据、图表、分析性内容、结论、建议，均是以腾讯安全大数据及第三方授权或公开的信息和数据为基础，结合抽样分析\调查报告等方法，经综合整理、编辑得出。囿于信息及手段的局限性，本报告研究团队无法保证本报告的内容具有绝对客观性和准确性。本报告内容仅代表腾讯于本报告作出时的单方观点，仅供参考使用。