网络安全风险评估

中国医学科学院阜外医院：韩作为

目录

CONTENTS

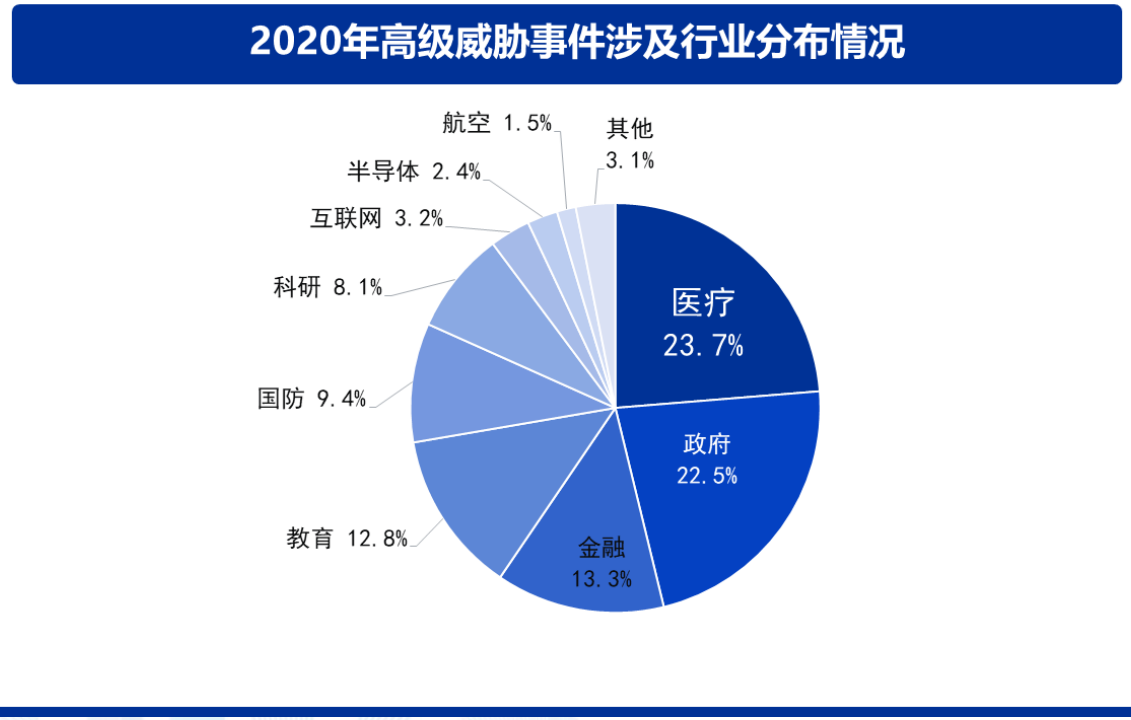
contents

2021 CHINC China Hospital Information Network Conference

01

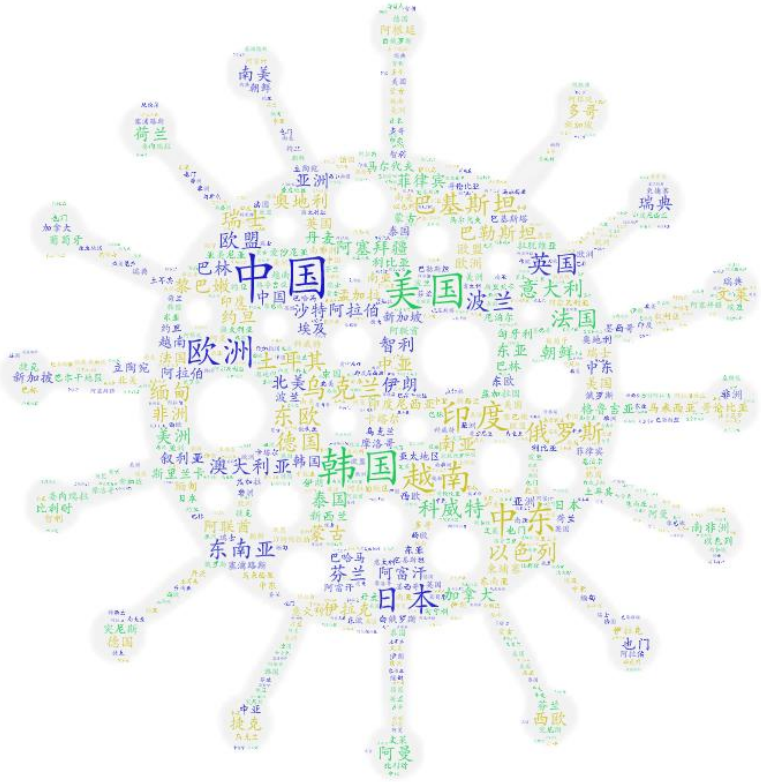
医疗卫生行业网络安全形势

医卫行业成为全球网络攻击的主要目标



2020年，针对
疾控与防疫机构
病毒研究机构
疫苗研发机构
医学研究机构
的高级威胁活动持续不断

中国成为全球网络攻击活动首要目标



开源情报提及率最高的五个受害国家：**中国7.4%**，韩国6.6%，美国4.9%，巴基斯坦3.2%，印度3.2%

开源情报提及率最高的五个APT组织：**Lazarus10.3%**，Kimsuky7.8%，海莲花5.4%，Darkhotel4.8%，蔓灵花3.2%

疫情相关词汇成为年度网络攻击诱饵文件热词

医疗行业网络安全事件

新型冠状病毒大流行以来，各国都将研发疫苗提升成为科研领域的最优先事项。围绕着疫苗研发数据的信息安全问题日渐凸显，自年中以来已有多起针对疫苗研发数据的安全事件发生

7月 新冠疫苗竞赛爆发“冷战” 俄罗斯被指通过黑客窃取研发信息

10月 美国一医疗技术公司负责研发新冠疫苗，遭黑客攻击，数据被封锁

11月 微软监测到三场针对新冠病毒疫苗的黑客行动

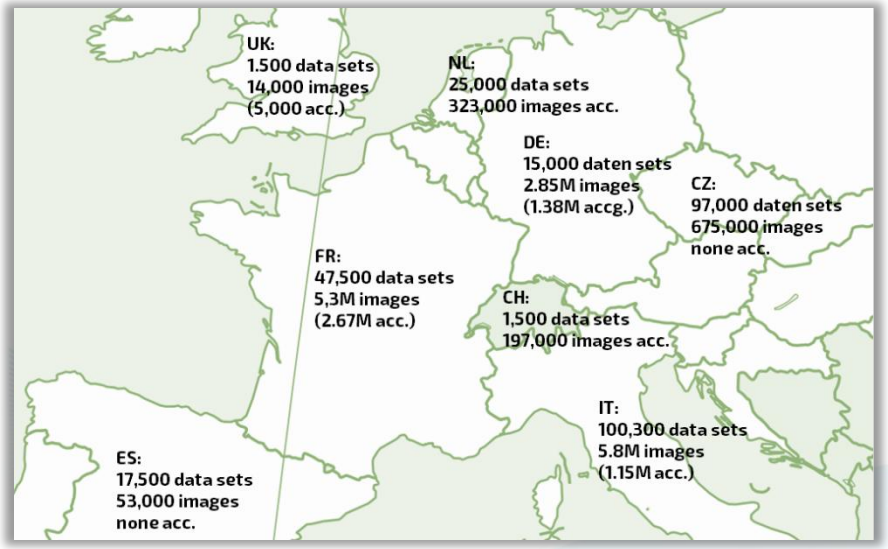
12月 IBM安全研究人员表示，黑客攻击新冠病毒疫苗的供应链

网络安全事件总是紧追公共卫生热点

医疗行业网络安全事件

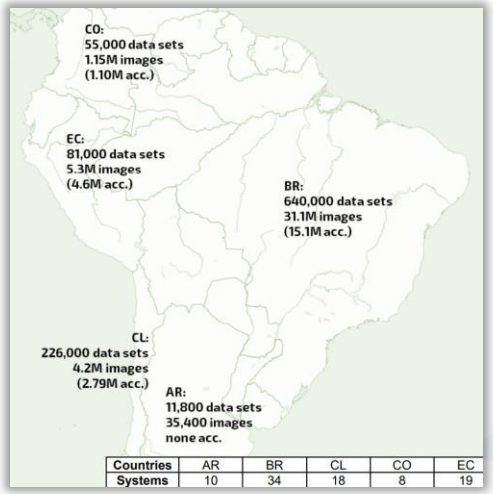
全球 7.37 亿医疗数据泄露，涉及 2000 多万人，波及 52 国

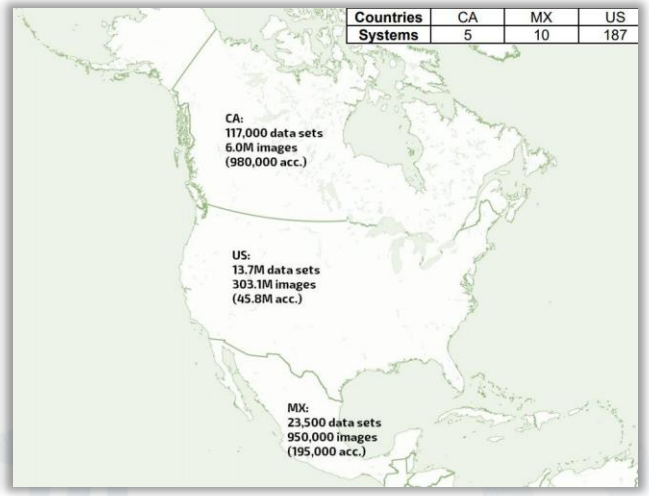
据外媒 Securityaffairs 报道，德国漏洞分析和管理公司 Greenbone Networks 的专家发现，600 个未受保护的服务器暴露于互联网，这些服务器包含大量医疗放射图像其中，有超过 7.37 亿个放射图像，涉及 2000 多万人，影响到 52 个国家的患者。

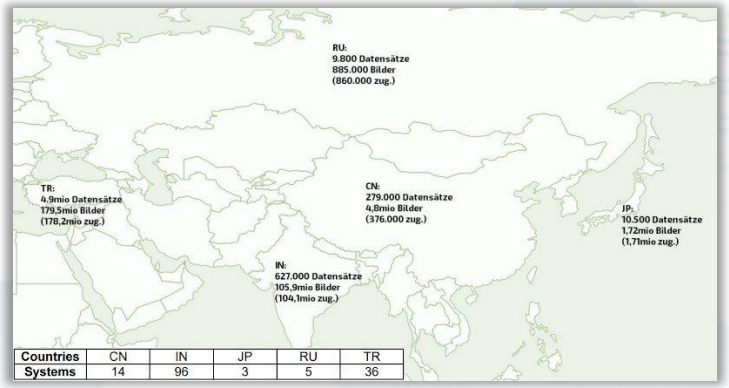


在欧洲，意大利受影响的系统数量最多，有 10 个，它也是泄露医疗信息数量最多的国家，有 10.03 万数据集，580 万医疗射图像

在北美，数量最多未受保护的 PACS 系统是在美国，同时它也是数据集暴露最多的国家，有 1370 万数据集，超过 3 亿张医学图像，暴露的机器系统是 187

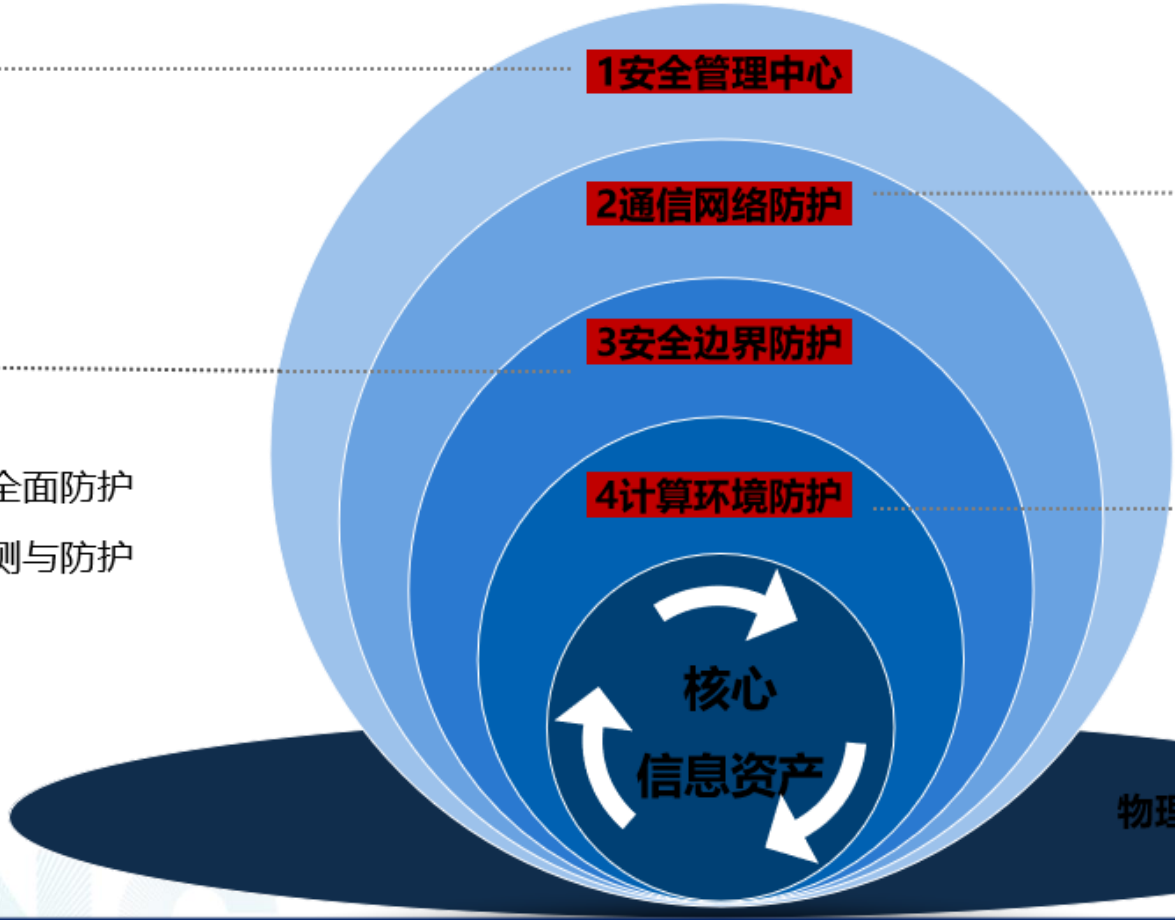






在亚洲，数量最多的开放式机器是在印度，但是土耳其泄露的数据记录（490 万）和医学放射图像（490 万）确是处于领先地位

网络安全防护体系



■安全管理中心

- 统一管理
- 集中审计
- 安全态势感知

■边界安全防护

- 边界已知威胁全面防护
- 新型威胁的检测与防护

■通信网络安全防护

- 传输信息加密
- 可信接入保护

■计算环境安全防护

- 主机安全
- 应用安全
- 数据安全

建设“一个中心”管理下的“三重防护”体系

面临的问题及困惑

- 到底应该优先解决什么问题？
- 如何应对未知的威胁？
- 付出与收益不成比例？
  真的是越安全越好吗？
- 每年都有投入资金做安全
  但这么多年下来到底效果如何？

怎么处理上述问题及疑惑？——风险评估

2021 CHINC China Hospital Information Network Conference

02

网络安全风险评估通识

如何理解风险评估

风　险

悲剧里面挖出来的学问

风险评估

直观、明确感受风险

信息安全风险评估，是对信息资产所面临的威胁、存在的弱点、造成的影响，以及三者综合作用所带来的风险的可能性评估

网络安全风险评估的发展

20世纪30年代

风险评估起源

美国保险公司

20世纪50年代

系统安全风险评估

电子、航空、铁路、公路、
原子能、汽车等领域

1976年

风险评估术语形成

美国国家环保局首次颁布
“致癌物风险评估准则”

2005年

ISO 27000系列

ISO 27001 ISO27002等
信息安全管理体系

2007年

中国

GB/T 20984
《信息安全风险评估规范》

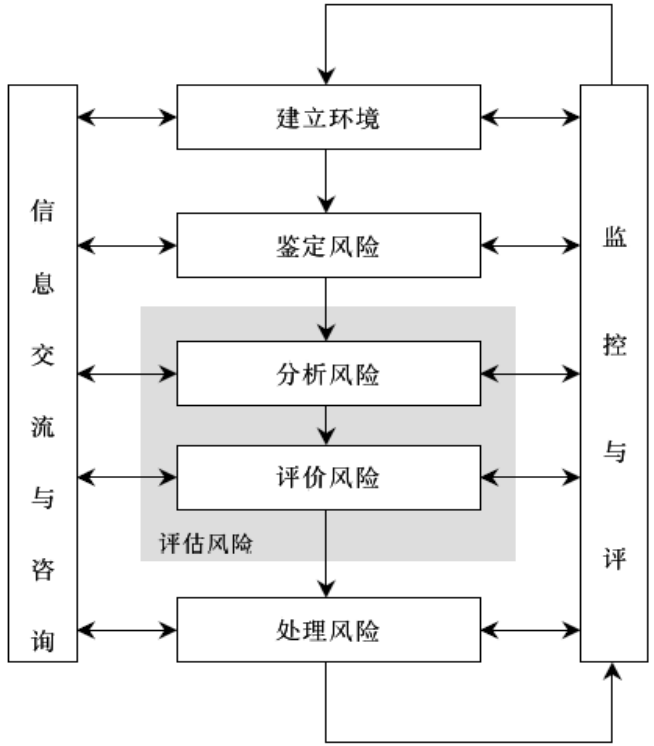
风险管理与风险评估

01.学术定义上

风险评估是风险管理的一个子集……

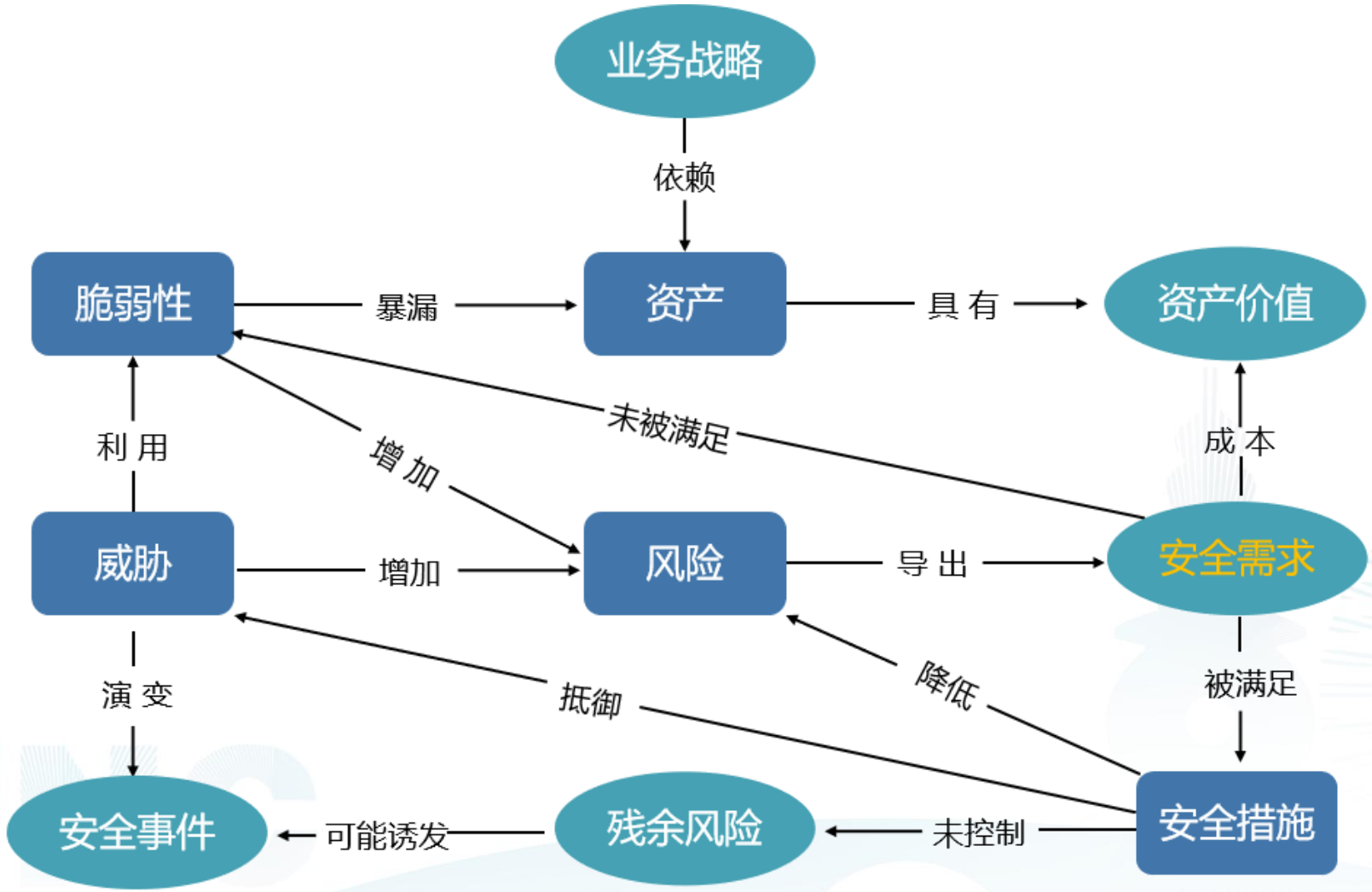
02.实践中

风险评估项目基本包含风险管理各个流程……



风险管理 = 风险识别 + 风险控制 + 风险监测

风险评估模型



@20984《规范》P3

风险评估相关术语

资 产 任何对企业拥有价值东西

脆弱性 可被威胁利用的弱点

可能性 发生几率或频率

威 胁 安全事件发生的潜在原因

风 险 威胁利用弱点带来损害的可能性

影 响 后果

安全措施 控制措施或对策

残余风险 在实施安全措施之后仍然存在的风险

资产 威胁 脆弱性

资 产 —— 鸡 蛋

脆弱性 —— 缝

威 胁 —— 苍 蝇

网络安全风险评估参考标准

标 准

包括国内外标准及最佳实践……

- 《信息安全风险评估规范》GB/T20984-2007
- 《信息安全风险评估实施指南》GB/T31509-2015
- 《信息安全风险管理指南》ISO/IEC 27005
- 《信息安全风险管理要求》ISO/IEC 31000
- 等级保护标准簇等
- 行业主管机关的要求和制度

国际常见的安全体系

在信息科技不断创新和高速发展的同时，信息科技管理所面临的问题也日益明显，为此国际上推出了诸多针对不同信息科技管理方面的体系和标准，用以帮助企业提高自身的信息科技整体素质、管理意识和管理水平。国际上较为常见和使用的信息科技管理体系包含以下几类

安全标准	关键点				特点
ISO27001	PDCA模型	14个 安全控制域	113个 安全控制措施		■ **基于PDCA**信息安全管理 ■ 信息**安全风险管理**
COBIT	COBIT 体系结构	4个控制域	34个信息技术过程控制		■ 用于**安全治理** ■ 安全全生命周期管理等
ITIL	6个模块	5个生命周期：战略、设计、转换、**运营**、改进			■ 企业的IT服务**管理**实践标准 ■ 用于IT**流程管理和服务管理**
ISF SoGP	8大领域：可恢复性、意识、风险评估、合规、信息安全评估、供应链管理、制度标准及规范、安全灾备				■ **安全风险管理**的实践集合 ■ 安全**管理** 和**技术落实要求**
信息保障技术框架IATF	4个技术框架焦点域：网络和基础设施，区域边界、计算环境和支撑性基础设施				■ 焦点域特有的**安全需求** ■ 相应的**技术**措施
NIST 系列文档	安全管理标准	安全技术标准			■ 系列安全技术标准，包含风险评估，新兴技术标准等
TOGAF	业务 架构	应用 架构	数据 架构	技术 架构	■ 国际最佳实践企业**系统架构** ■ 企业级IT架构建设**安全控制**

■ 各标准尽管侧重点不同，但原则上有以下共通之处：

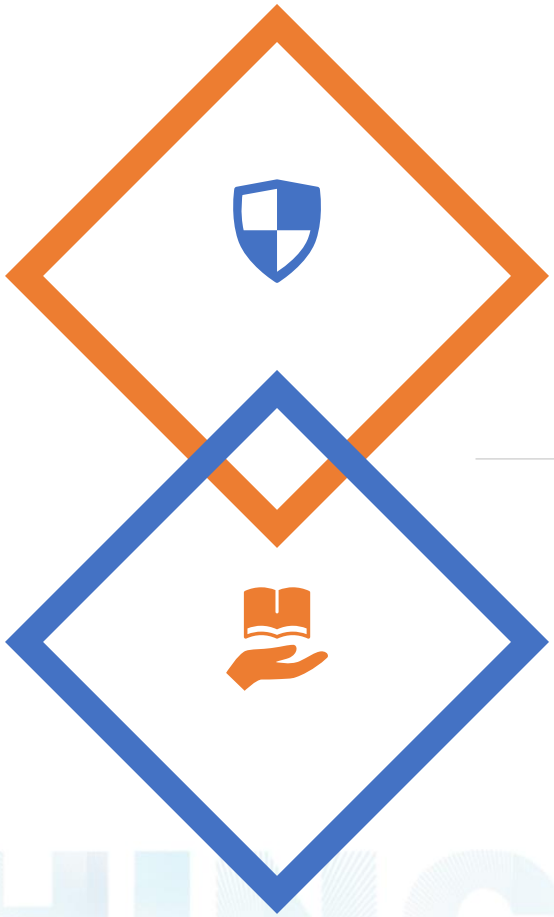
以**信息安全风险**为切入点，为组织如何管理信息安全风险提供指导。

提供有关**安全管理及控制**的操作实践及指引。

涵盖**管理、技术、运营**（流程）等相关内容。

■ 各标准阐述的安全管理范围及建议的操作实践本身基本无冲突

风险评估分类



定性/定量

定性分析

依据资产价值、威胁、脆弱性、控制措施

忽略事件发生的概率……

定量分析

威胁事件发生的概率和可能造成的损失

量化分析……

基于知识/模型

基于知识的评估

依照经验、专家……

基于模型的评估

合理抽象形成模型、数据分析……

基于资产的定性的风险评估

定量评估

ALE：Annual Risk Expectancy 年预期损失

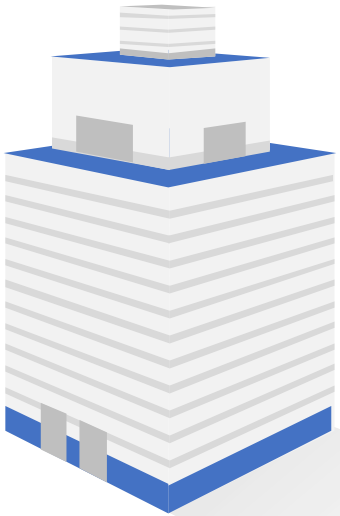
- ARO 年发生率
- SLE 单一风险预期损失

ALE=SLE*ARO

- 一个组织的网络设备资产价值为100000元，一场意外火灾使其损坏了价值的25%
- 那么，火灾的单一风险预期损失SLE=100000*25%=25000元
- 按照经验统计，这种火灾每5年发生一次，那么年发生次数ARO=1/5=0.2
- 因此，ALE=SLE*ARO=25000*0.2=5000元

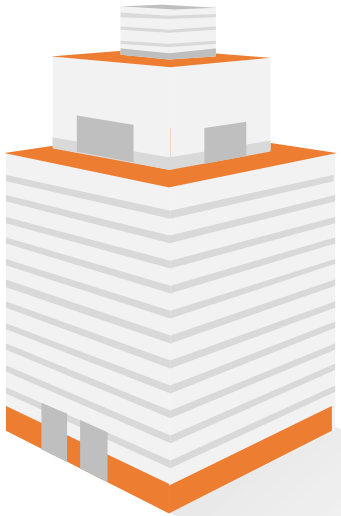
定性评估

定量方法在实际工作中可操作性较差,一般风险计算多采用**定性计算**



定性评估计算过程

- 将资产、威胁、脆弱性量化（等级化）赋值
- 选用计算方法计算（相乘法或矩阵法）



定性评估实质

- 反应面临风险的大小的准确排序
- 确定风险的性质（无关紧要、可接受、待观察、不可接受）
- 不是风险计算值本身的准确性

风险评估的目的和意义

企业网络安全现状

网络系统安全风险永远存在，不断变化，不能消除

只有适度安全才是最合适

需要对信息系统定期检测（类似人健康体检）

风险评估适用于信息系统检测

风险评估的作用

准确了解当前信息系统及网络的安全现状

明确安全建设需求，合理规划安全投入

给领导在信息安全方面决策提供支撑和依据

提高员工安全意识，培养内部安全人才

03

风险评估全流程

风险评估全流程

- 风险评估全流程
- 项目前期准备
- 资产识别与赋值
- 脆弱性识别与赋值
- 威胁识别与赋值
- 已有的安全措施确认
- 风险计划与处置建议

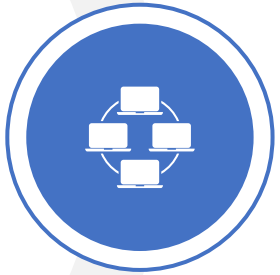
风险要点

资 产

对组织具有价值的信息或资源
是安全策略保护的对象

脆弱性

可能被威胁所利用的资产或若
干资产的薄弱环节



业务系统风险

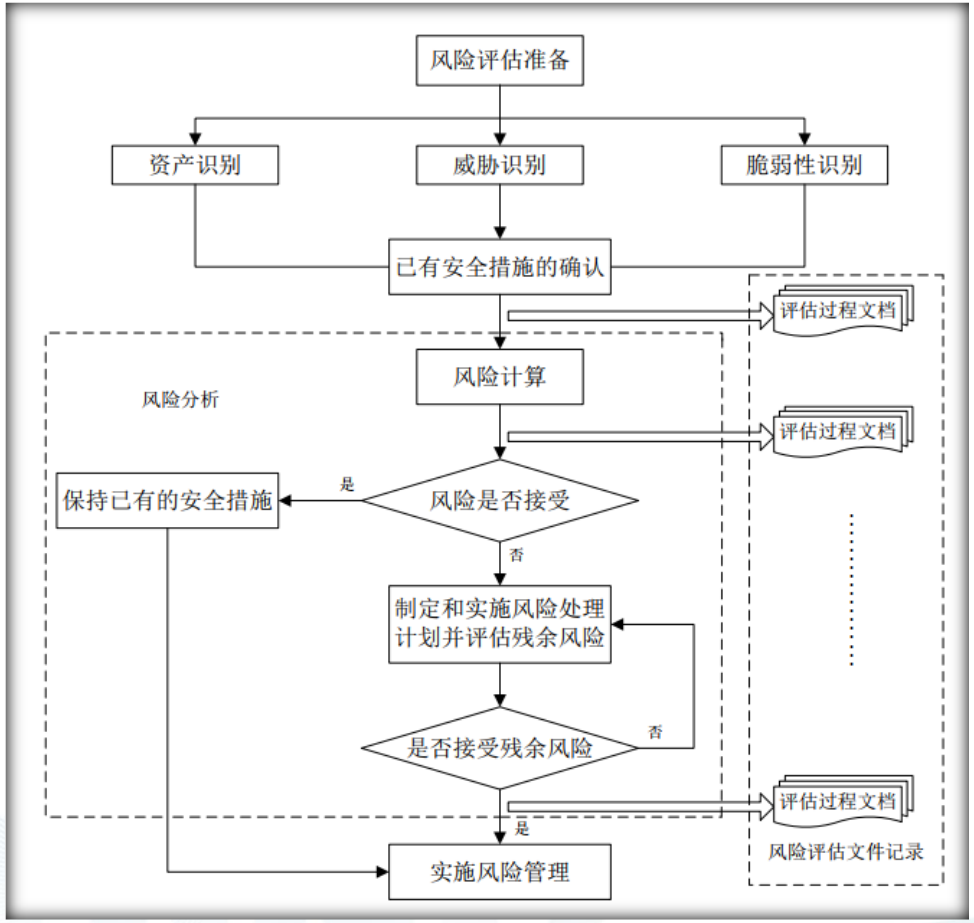
安全措施

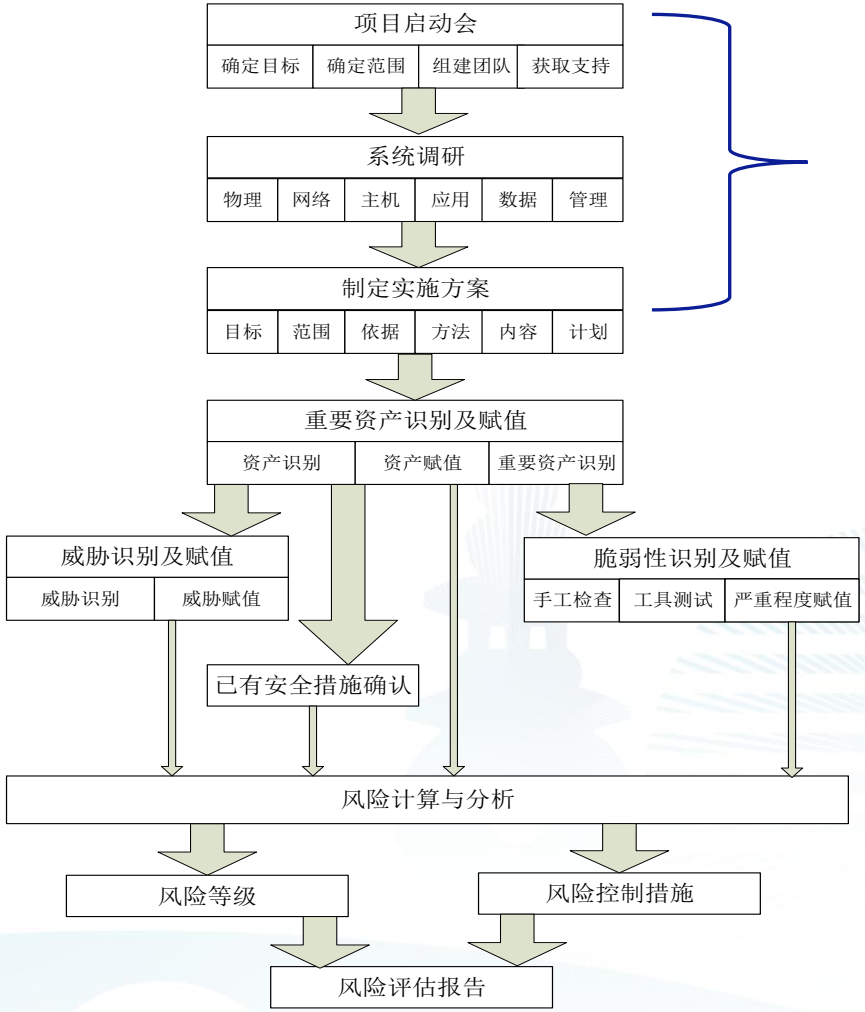
保护资产、抵御威胁、减少脆弱性
降低安全事件的影响，以及打击信息犯
罪而实施的各种措施、制度和机制

威 胁

可能导致对系统或组织危害的
不希望事故潜在的起因

风险评估全流程





确定目标

风险评估贯穿于信息系统生命周期

各阶段中风险评估实施的内容、对象、安全需求不同

确定被评估系统的生命周期阶段

- 业务战略
- 安全目标

- 设计方案
- 安全功能

- 实施风险
- 功能验证

- 资产、威胁、脆弱性
- 已有的安全措施

- 废弃资产
- 残留信息

确定范围

结合评估目标

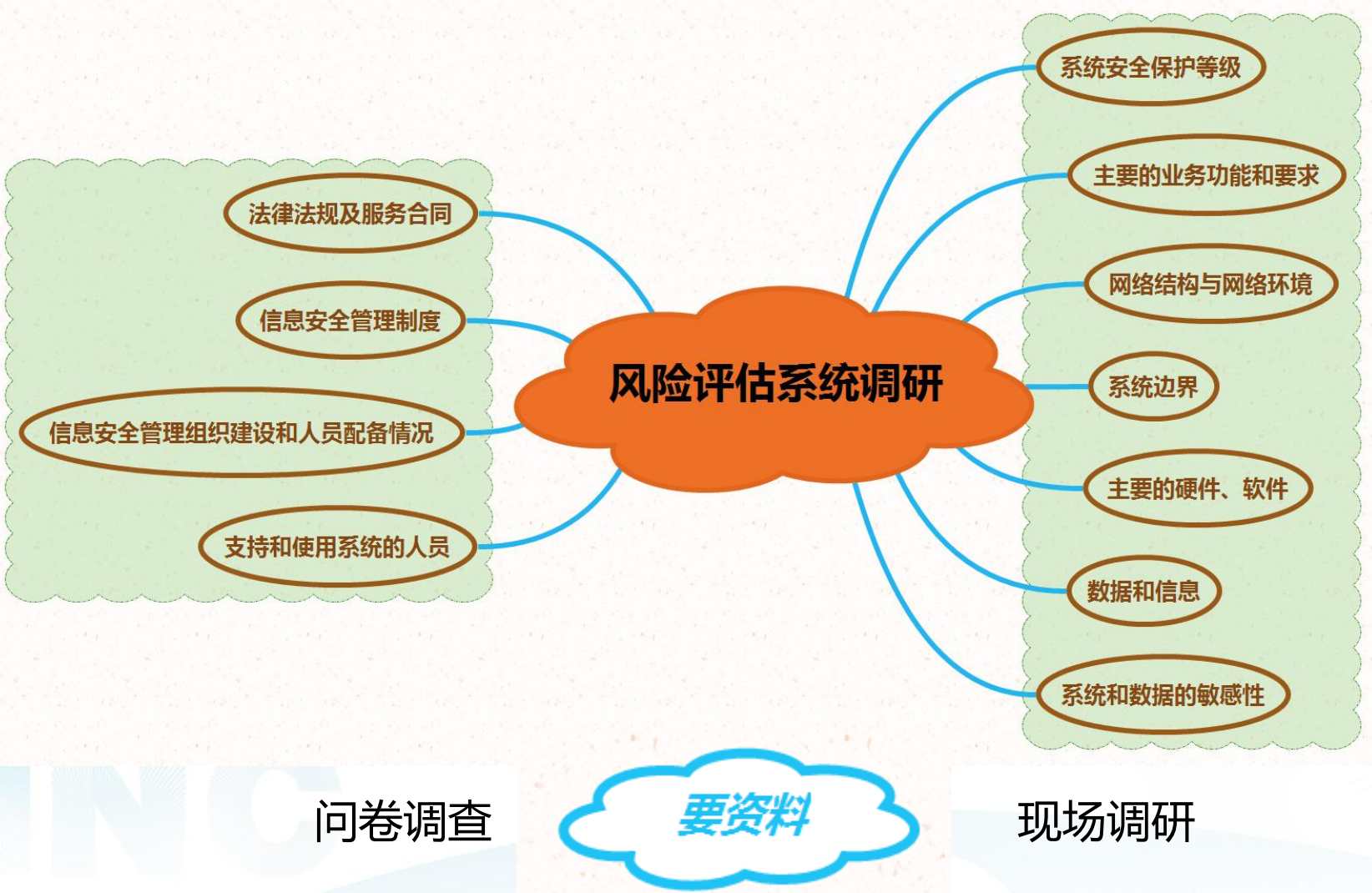
组织的实际信息系统情况

- 组织的全部信息资源
- 独立的信息系统
- 关键业务流程

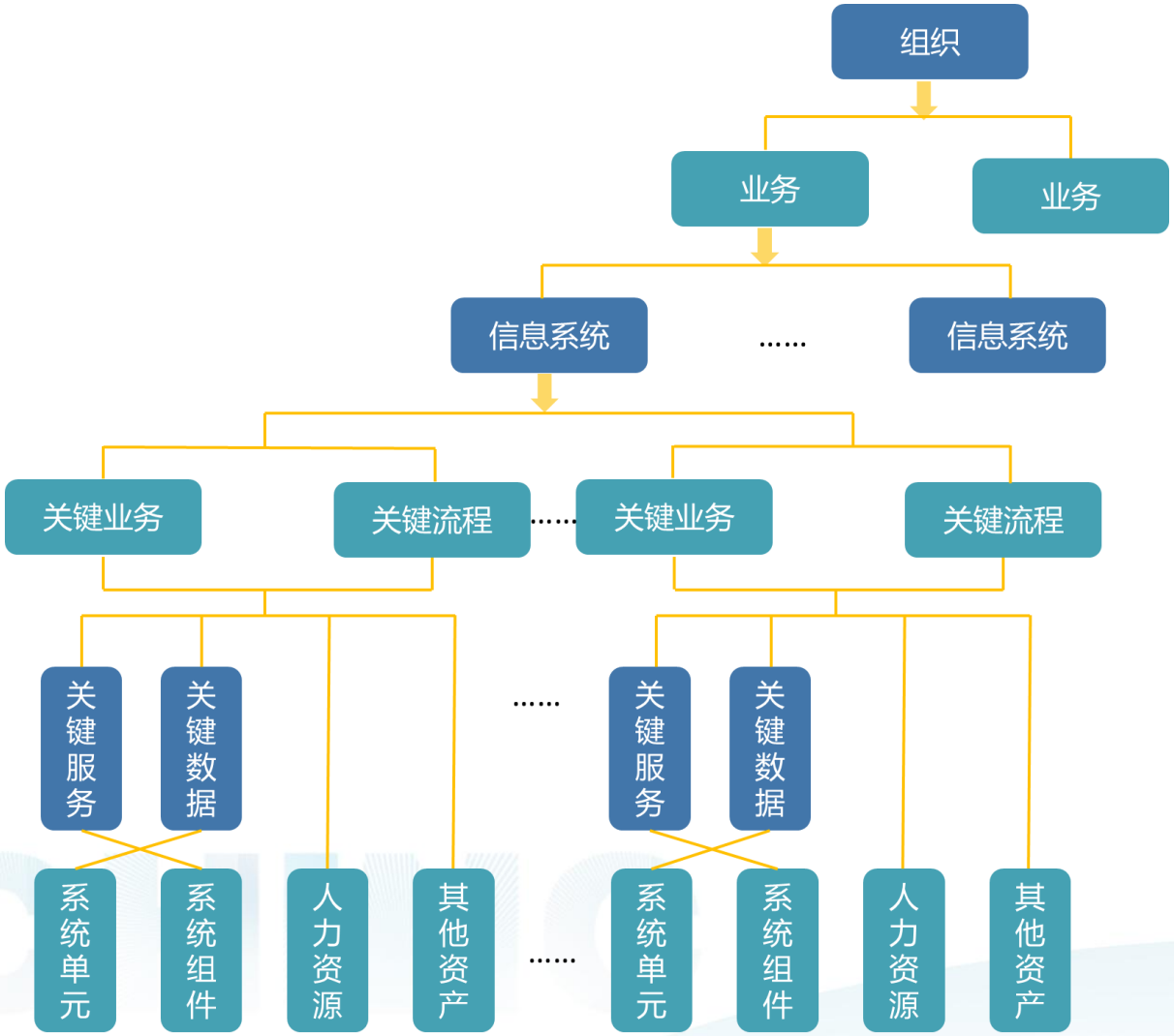
边界划分原则

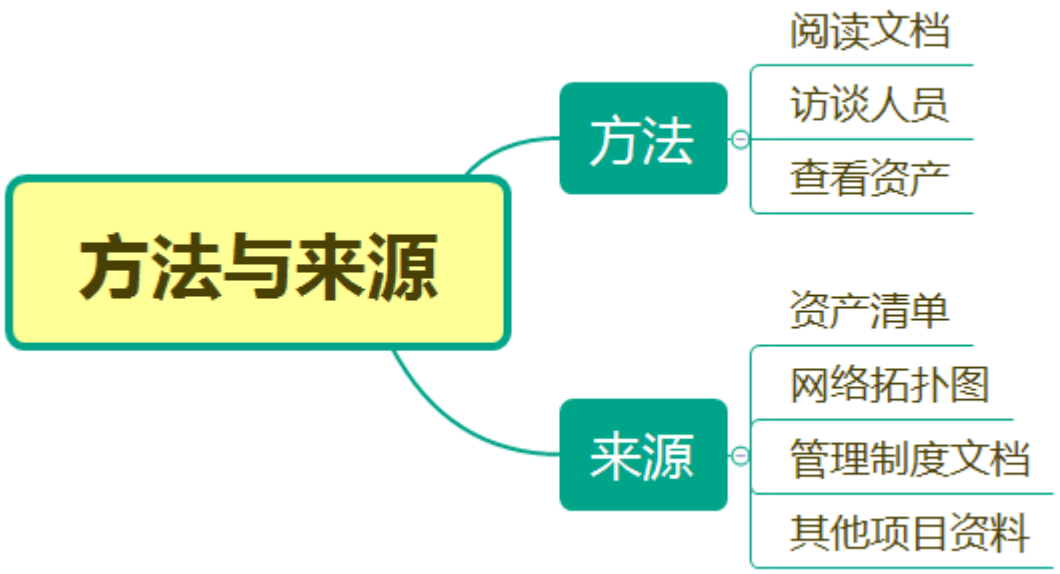
1. 业务系统的逻辑边界
2. 网络及设备载体边界
3. 物理环境边界
4. 组织管理权限边界

系统调研


风险评估系统调研
法律法规及服务合同
信息安全管理制度
信息安全管理组织建设和人员配备情况
支持和使用系统的人员
系统安全保护等级
主要的业务功能和要求
网络结构与网络环境
系统边界
主要的硬件、软件
数据和信息
系统和数据的敏感性
要资料
问卷调查
现场调研

资产识别步骤和方法


组织
业务
业务
信息系统
.....
信息系统
关键业务
关键流程
.....
关键业务
关键流程
关键服务
关键数据
.....
关键服务
关键数据
系统单元
系统组件
人力资源
其他资产
.....
系统单元
系统组件
人力资源
其他资产


方法与来源
方法
阅读文档
访谈人员
查看资产
来源
资产清单
网络拓扑图
管理制度文档
其他项目资料

资产识别--七层模型


管理层
管理策略、管理机构、管理人员
业务层
HIS
电子病历
LIS
PACS
OA
数据层
结构化数据
非结构化数据
分散科研数据
管理数据
应用层
C/S软件
B/S 软件
移动端软件
通用软件
主机层
操作系统、主机设备
操作系统、主机设备
网络层
网络设备
安全设备
物理层
机房和通信链路

资产赋值

安全保障等级	机密性-C	完整性-I	可用性-A
5 很高	包含组织最重要的秘密，关系未来发展的前途命运，对组织根本利益有着决定性的影响，如果泄露会造成灾难性的损害	完整性价值非常关键，未经授权的修改或破坏会对组织造成重大的或无法接受的影响，对业务冲击重大，并可能造成严重的业务中断，难以弥补	可用性价值非常高， 合法使用者对信息及信息系统的可用度达到年度99.9%以上， 或系统不允许中断
4 高	包组织的重要秘密，其泄露会使组织的安全和利益受到损害	完整性价值较高，未经授权的修改或破坏会对组织造成重大影响，对业务冲击严重，较难弥补	可用性价值较高， 合法使用者对信息及信息系统的可用度达到每天90%以上，或系统允许中断时间小于10分钟
3 中等	组织的一般性秘密，其泄露会使组织的安全和利益受到损害	完整性价值中等， 未经授权的修改或破坏会对组织造成影响， 对业务冲击明显，但可以弥补	可用性价值中等， 合法使用者对信息及信息系统的可用度在正常工作时间达到70%以上， 或系统允许中断时间小于30分钟
2 低	仅能在组织内部或在组织某一部门内部公开的信息，向外扩散有可能对组织的利益造成轻微损害	完整性价值较低， 未经授权的修改或破坏会对组织造成轻微影响， 对业务冲击轻微，容易弥补	可用性价值较低， 合法使用者对信息及信息系统的可用度在正常工作时间达到25%以上， 或系统允许中断时间小于60分钟
1 很低	可对社会公开的信息，公用的信息处理设备和系统资源等	完整性价值非常低， 未经授权的修改或破坏对组织造成的影响可以忽略， 对业务冲击可以忽略	可用性价值可以忽略， 合法使用者对信息及信息系统的可用度在正常工作时间低于25%

资产价值计算

$$k = \text{Round1}\{\text{Log}_2\{[\alpha \times 2^C + \beta \times 2^I + \gamma \times 2^A]\}\}$$

根据资产机密性、完整性和可用性的不同等级对其赋值进行**加权计算**

加权法

综合评定法

K=Max（C,I,V）

选择对资产机密性、完整性和可用性**最为重要**的一个属性的赋值等级

脆弱性识别—最重要的环节

威胁利用资产的脆弱性，才可能造成伤害

尽可能的消减资产的脆弱性，阻止或消减威胁造成的影响

脆弱性的特点

隐蔽性

- 有些脆弱性只有在一定条件和环境下才能显现

安全措施本身脆弱性

- 不正确的、起不到应有作用的或
- 没有正确实施的安全措施本身就可能是一个脆弱性

脆弱性识别方法

脆弱性赋值

对资产的损害程度

技术实现的难易程度

脆弱性的流行程度

等级	标识	定义
5	很高	如果被威胁利用，将对资产造成完全损害
4	高	如果被威胁利用，将对资产造成重大损害
3	中	如果被威胁利用，将对资产造成一般损害
2	低	如果被威胁利用，将对资产造成较小损害
1	很低	如果被威胁利用，将对资产造成的损害可以忽略

威胁识别

威胁来源

01.环境因素

断电、静电、自然灾害、意外事故……

02.人为因素

恶意人员故意破坏、非恶意人员缺乏责任心……

威胁分类

01.软硬件故障

硬件设备故障、应用软件及数据库故障……

02.管理不到位

安全管理不规范、或者管理混乱……

11. 抵赖

不承认所做的操作和交易……

威胁赋值

等级	标识	定义
5	很高	出现的频率很高（或>=1次/周）；或在大多数情况下几乎不可避免；或可以证实经常发生过
4	高	出现的频率较高（或>=1次/月）；或在大多数情况下可能会发生；或可以证实多次发生过
3	中	出现的频率中等（或>1次/半年）；或在某种情况下可能会发生；或被证实曾经发生过
2	低	出现的频率较小；或一般不太可能发生；或没有证实发生过
1	很低	威胁几乎不可能发生，仅可能在非常罕见和例外的情况下发生

在实际的风险评估中

威胁频率的判断应在评估准备阶段根据历史统计或行业判断予以确定

需要在准备阶段得到评估方的认可

威胁种类赋值列表

编号	威胁种类	描述	威胁子类	常规发生可能性	常规破坏程度	威胁值
T1	物理环境影响	对信息系统正常运行造成影响的物理环境问题和自然灾害	断电、静电、灰尘、潮湿、温度、鼠蚁虫害、电磁干扰、洪灾、火灾、地震等	低	低	1
T2	软硬件故障	对业务实施或系统运行产生影响的设备硬件故障、通讯链路中断、系统本身或软件缺陷等问题	设备硬件故障、传输设备故障、存储媒体故障、系统软件故障、应用软件故障、数据库软件故障、开发环境故障等	低	高	3
T3	无作为或操作失误	应该执行而没有执行相应的操作，或无意执行了错误的操作	维护错误、操作失误等	低	中	2
T4	恶意代码	故意在计算机系统上执行恶意任务的程序代码	病毒、特洛伊木马、蠕虫、陷门、间谍软件、窃听软件等	中	高	4
T5	越权或滥用	通过采用一些措施，超越自己的权限访问了本来无权访问的资源，或者滥用自己的权限，做出破坏信息系统的行为	非授权访问网络资源、非授权访问系统资源、滥用权限非正常修改系统配置或数据、滥用权限泄露秘密信息等	高	高	5
T6	物理攻击	通过物理的接触造成对软件、硬件、数据的破坏	物理接触、物理破坏、盗窃等	低	高	3
T7	网络攻击	利用工具和技术通过网络对信息系统进行攻击和入侵	网络探测和信息采集、漏洞探测、嗅探（账号、口令、权限等）、用户身份伪造和欺骗、用户或业务数据的窃取和破坏、系统运行的控制和破坏等	高	高	5
T8	泄密	信息泄露给不应了解的他人	内部信息泄露、外部信息泄露等	高	高	5
T9	篡改	非法修改信息，破坏信息的完整性使系统的安全性降低或信息不可用	篡改网络配置信息、篡改系统配置信息、篡改安全配置信息、篡改用户身份信息或业务数据信息等	高	高	5
T10	抵赖	不承认收到的信息和所作的操作和交易	原发抵赖、接收抵赖、第三方抵赖等	低	中	2
T11	管理不到位	安全管理无法落实或不到位，从而破坏信息系统正常有序运行	管理制度和策略不完善、管理规程缺失、职责不明确、监督控管机制不健全等	高	中	4

已有的安全措施确认

03.安全性价比

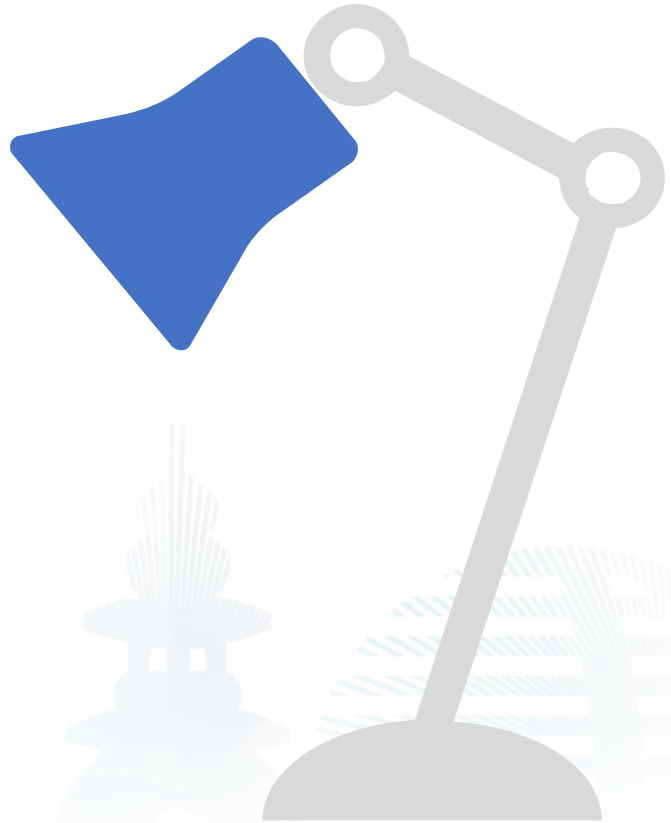
- 通过保留安全措施及修正安全措施达到提升信息安全投入性价比

02.修正安全措施

- 对不适当的安全措施进行取消或修正，用更合适的措施替代

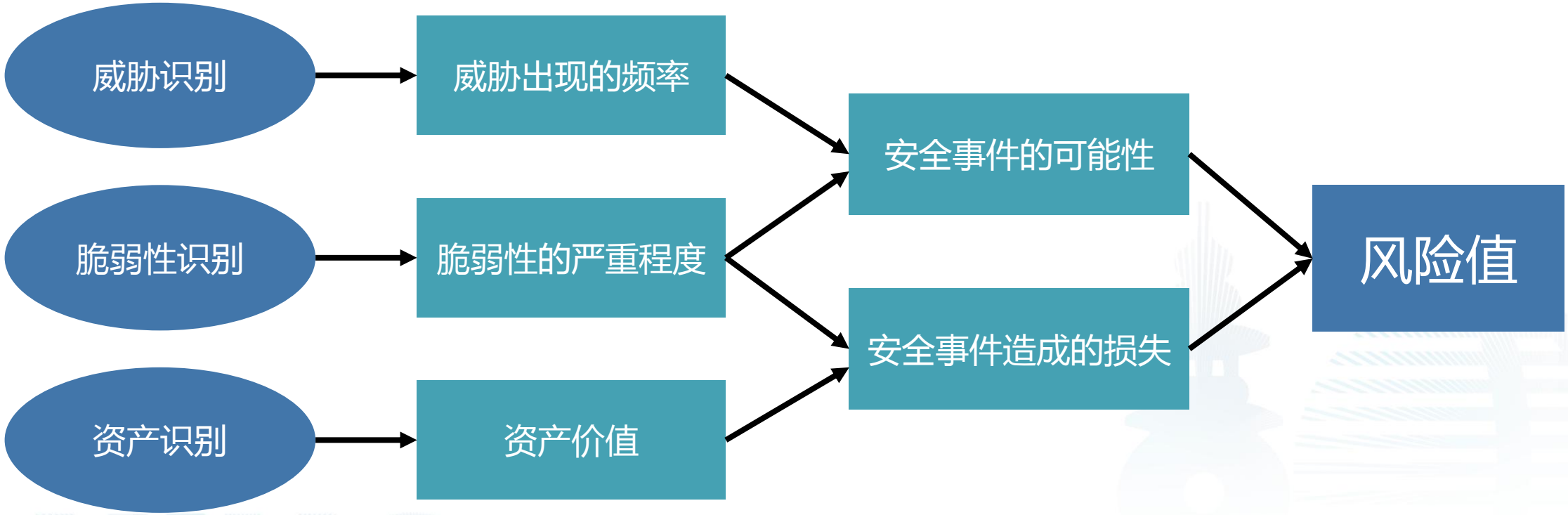
01.保留安全措施

- 有效的安全措施继续保留，避免不必要的工作和费用



已有安全措施确认与脆弱性识别存在一定的联系

风险分析模型


威胁识别
脆弱性识别
资产识别
威胁出现的频率
脆弱性的严重程度
资产价值
安全事件的可能性
安全事件造成的损失
风险值

风险计算的方法

相乘法 R=A*V*T

计算安全事件发生可能性

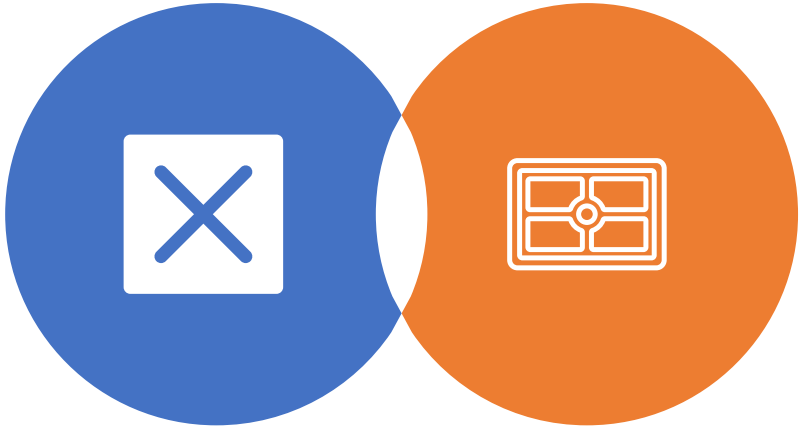
$$\text{安全事件发生可能性}=\sqrt{\text{脆弱性严重程度}\times\text{威胁发生频率}}$$

计算安全事件的损失

$$\text{安全事件的损失}=\sqrt{\text{资产价值}\times\text{脆弱性严重程度}}$$

计算安全事件风险值

$$\text{安全事件风险值}=\sqrt{\text{安全事件发生可能性}\times\text{安全事件的损失}}$$



矩阵法

构造一个二维矩阵

形成安全事件的可能性与安全事件造成的损失之间的二维关系

参见20984附录A

风险计算

序号	关键系统单元	资产名称(测试对象编号)	脆弱性描述	威胁编号	已有安全措施	威胁发生率 T	脆弱性程度 V	资产价值 A	风险值 $\sqrt{T*V}*\sqrt{A*V}$	风险等级
2	门户网站数据库服务器	SDJT-FWQ-02	数据库管理用户身份鉴别信息未具有不易被冒用的特点，口令未有复杂度要求并定期更换；	T5：越权或滥用 T9：篡改	禁止远程登录维护	1	3	5	7	2
			未采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别。	T5：越权或滥用 T9：篡改	禁止远程登录维护	1	2	5	4	1
			安全审计： 审计范围未覆盖到服务器上的每个数据库用户； 审计内容未包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件； 审计记录未包括事件的日期、时间、类型、主体标识、客体标识和结果等； 未能够根据记录数据进行分析，并生成审计报表；； 未保护审计进程，避免受到未预期的中断； 未保护审计记录，避免受到未预期的删除、修改或覆盖等。	T10：抵赖	无	3	3	5	12	3
			安全漏洞： Oracle 2007 年 1 月更新修复多个安全漏洞 Oracle 2007 年 4 月更新修复多个安全漏洞 Oracle 2007 年 7 月更新修复多个安全漏洞 Oracle 2007 年 10 月更新修复多个安全漏洞 Oracle 2008 年 1 月更新修复多个安全漏洞	T4：恶意代码 T5：越权或滥用 T7：网络攻击 T9：篡改	在防火墙中进行严格的访问控制策略	2	5	5	16	4

风险值的相对性

结 果

风 险 值 R 是 相 对 概 念

一个信息系统中多个子系统
风险值大小的比较是相对的

相对性

方 法

不同风险计算方法的归一性

不同风险计算方法对同一对
象风险值计算是相对一致的

风险处置建议

降 低 采取保护措施

转 移 外包

接 受 接受风险可能带来的结果

规 避 通过不使用面临风险的资产来避免风险

04

风险评估的总结和展望

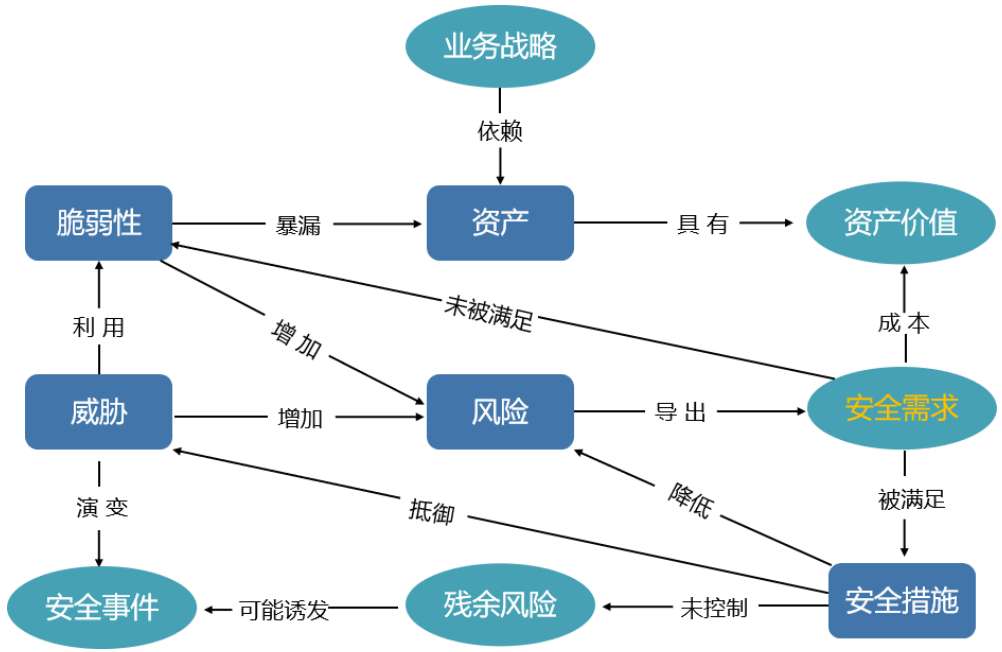
风险评估专业性向普及性转变

标准的普及与实践方法的推广
风险评估的思想已经深入人心

风险评估变成了非常基础的必要功能
融入信息安全与风险管理的方方面面

就像电视剧「士兵突击」中的钢七连一样，它的职能并没有消失，只是不再需要单独存在，变成了一种基础必备的素质，融入进每个战斗单元

风险评估的方法由复杂向简化转变



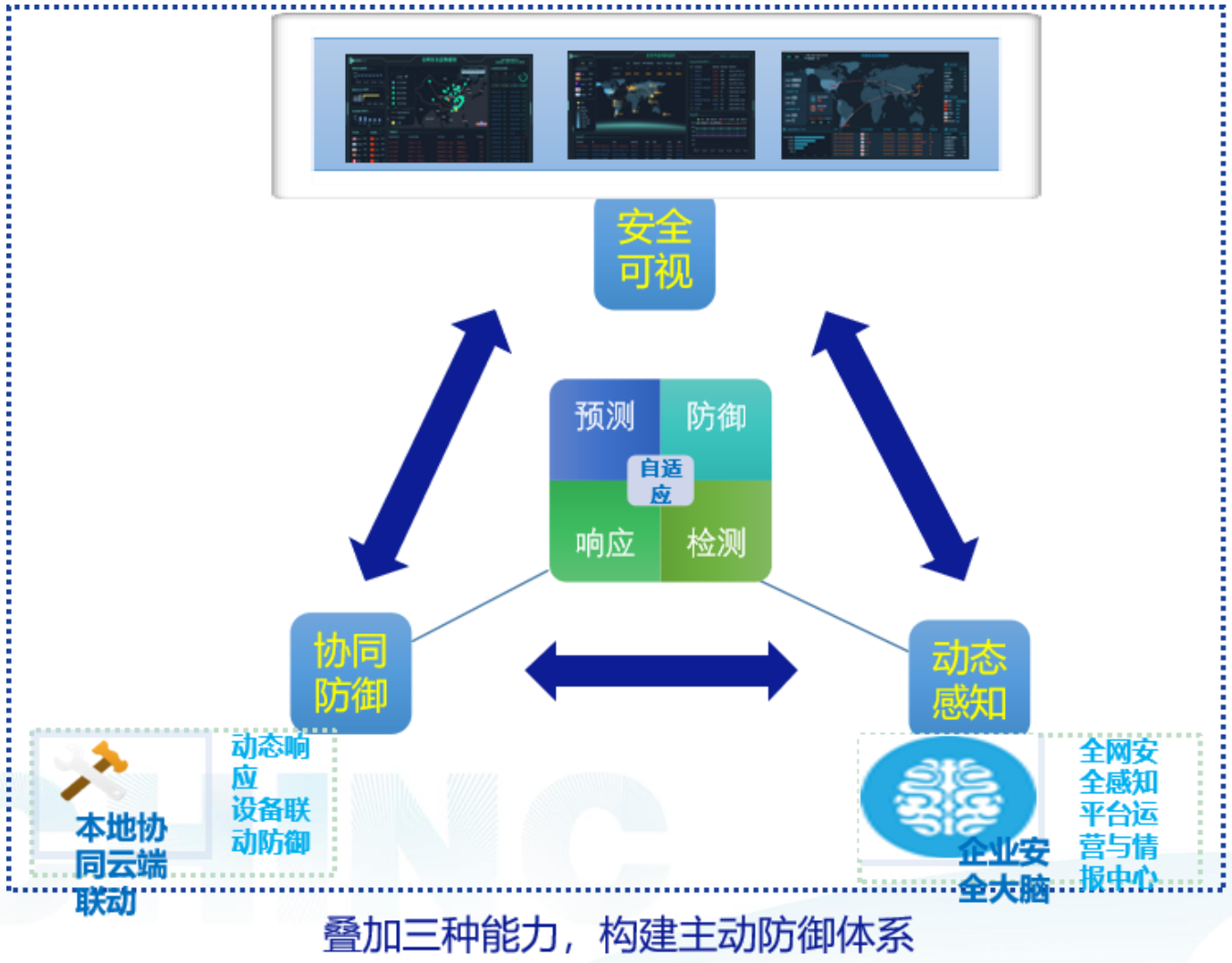
风险要素模型

风险构成包含资产威胁和弱点
三个要素缺一都无法构成风险

当前风险评估的方法与形式并是重点能够抓住风险并以成本有效的方式解决掉风险是根本

- **基于资产风险评估**
- **定性安全评估**
- **基于流程安全评估**

风险评估的方法由复杂向简化转变



叠加三种能力，构建主动防御体系

通过安全平台将风险评估进行实时、在线处置，将周期性任务转向持续安全运营

风险动态监测把威胁评估从线下搬到线上，通过安全事件管理平台形成安全威胁在线分析

谢谢观看！

中国医学科学院阜外医院：韩作为