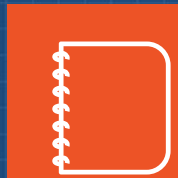


卫生医疗
信息安全交流

翟建军

2014年10月

提纲

信息安全整体态势

信息安全管理的新趋势

信息安全管理的几点建议

中国卫生信息化发展的阶段

第一阶段

2003年以前

- 处于起步阶段
- 以挂号、诊疗等流程电子化为主
- 呈单个系统、小范围应用的特点

第二阶段

2003年~2009年

- 公共卫生信息化建设的快速发展期
- 建立了传染病与突发公共卫生事件网络直报系统
- 逐步建立卫生应急指挥、卫生统计、妇幼保健、新农合等业务系统

第三阶段

2009年深化医改以来

- 卫生信息化全面快速发展期
- 各地探索建立区域信息平台，以电子健康档案为核心，实现区域内医疗卫生机构互联互通、信息共享，逐步实现医疗卫生业务协同。
- 医院建立以电子病历为基础的挂号、收费、治疗一体化的医院管理信息系统，优化医疗服务流程。
- 大力发展远程医疗，促进优质医疗资源纵向延伸，通过多种方式方便居民看病就医。

建设区域信息平台，实现业务协同、信息共享

◆ 以电子健康档案为基础，互联互通、信息共享，业务协同

人口健康数据的汇聚对信息安全带来极大威胁

- 收集渠道更加广泛（网络几乎覆盖全国各级各类医疗卫生机构，可穿戴设备）
- 信息更全面，数据的关联性更强（以人为中心，贯穿生命全过程）
- 信息广泛共享、互联（攻击入口很多）
- 对数据的挖掘分析可为我所用，也可为恶意甚至敌对势力所用（“棱镜门”）

医院信息系统

区域信息平台

国家信息平台

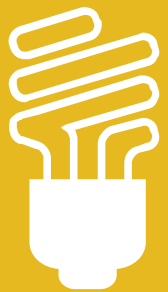
数据的变化趋势

疾病诊疗信息 → 电子健康档案 → 大数据分析

威胁的变化趋势

个人隐私数据 → 敏感数据 → 情报--机密

安信天行



一、整体态势

1、我国网络遭受外部攻击持续增加

被控制网站

2011年 1万多

2013年 6万多

被控制主机

2011年 800万

2013年 1000多万

钓鱼-境外注册

2011年 60%

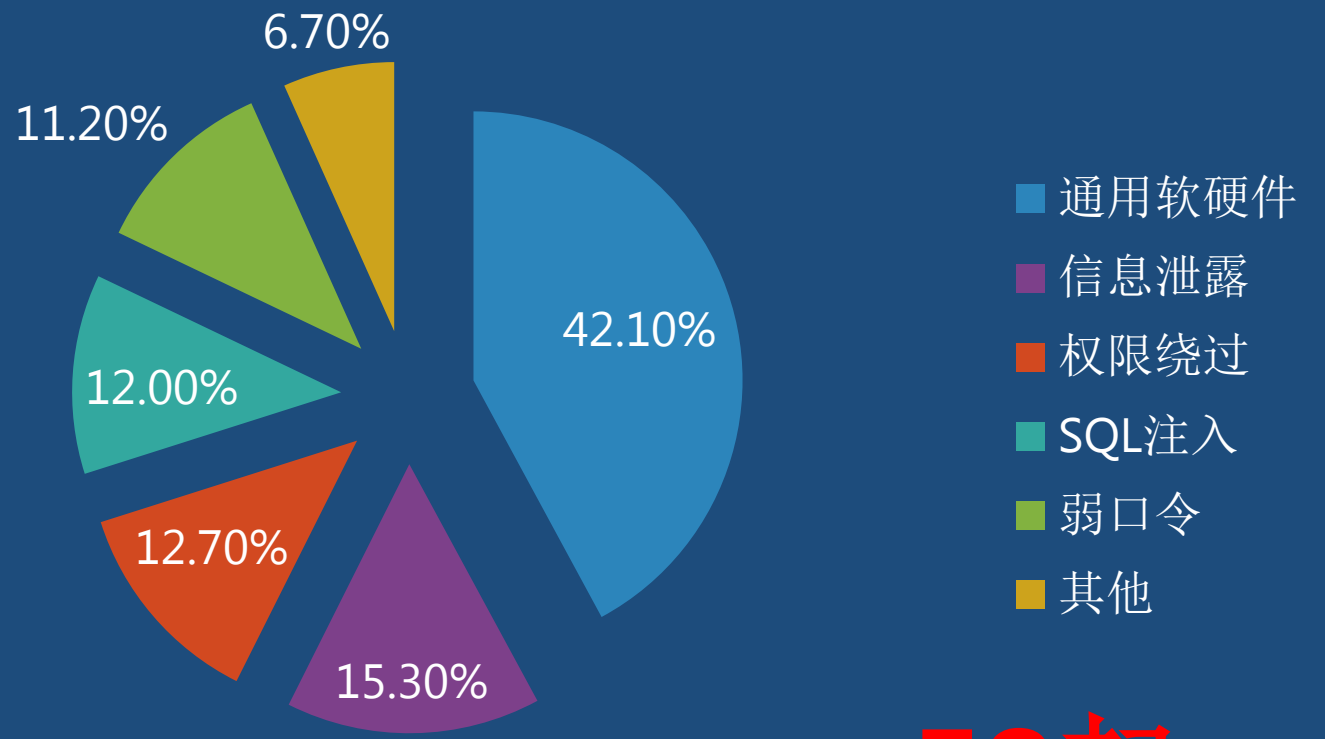
2013年 90.2%

政府网站重灾区

（日美韩）

2、基础设施安全薄弱

2013电信风险事件518起，较2012年增长一倍

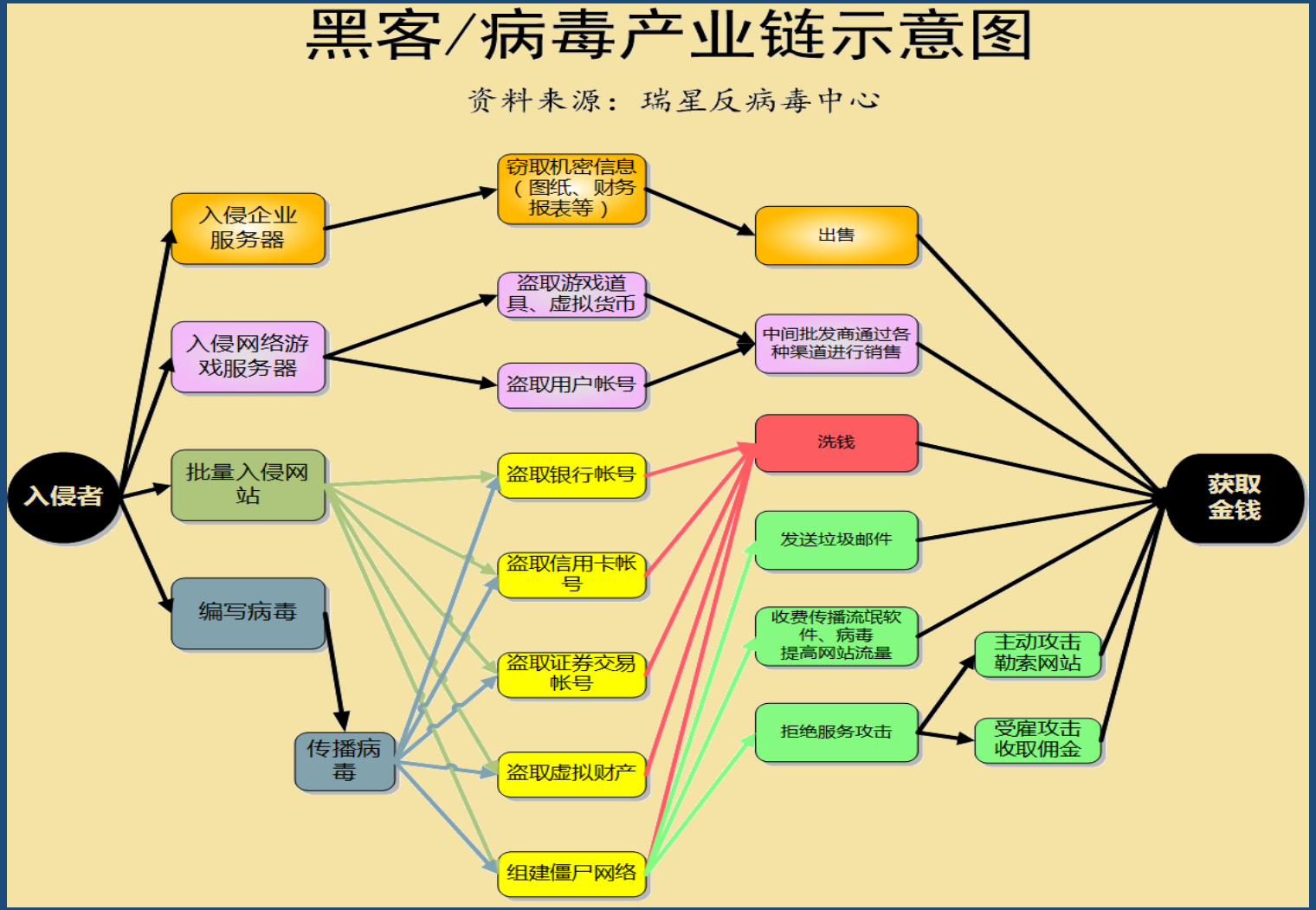


.CN域名系统攻击持续，2013年大约58起

谁将是下一个受害者？


其他重要信息系统
网络管理中心
重要网站
……
财政
金融
工商
税务
……
经济信息系统
公用通信
广播电视传输
……
基础信息系统
重点
信息系统
国家科研
海关
审计
教育
交通运输
社会保障
能源
国防工业
……
国家事务处理系统

3、地下产业猖獗



集团化、
产业化的趋势

网络黑金进入“渠道为王”时代

4、个人信息安全威胁上升

企业邮箱　政府邮箱　个人邮箱

登录帐户和密码被窃取后

最直接和常见的损失

帐号余额被盗

当前余额不足

垃圾病毒邮件

充作水军帐户

骚扰电话短信

破解注册邮箱

1、直接登录邮箱，查看邮件；
2、根据特点，设计针对性的密码表。

根据来往邮件
1、分析网络行为；
2、分析人际关系
3、

份

相册被入侵

XXJ主角

网购信息泄露，财产损失

亲朋好友受到牵连

哥们，手头有点紧，速汇钱！

更多服务影响
股票、财务、银行卡、健康、子女、父母等

5. 移动设备安全成为新目标

安卓平台恶意程序数量爆发式增长，99.5%针对安卓平台

4.1 韩八百万手机用户信息泄露 两名嫌疑人被捕

2012 年 07 月 30 日 09:13　　来源：新京报

据新华社电 韩国电信公司 29 日承认，企业 800 多万手机用户的个人信息遭电脑“黑客”窃取，警方当天逮捕两名嫌疑人。

这家韩国第二大移动通信运营商说，本月早些时候发现遭黑客攻击迹象，随后向警方报案。调查发现，一些黑客今年 2 月起窃取手机用户信息，包括用户姓名、手机号码和家庭住址，继而转卖给一些电话销售机构。

韩国联合通讯社报道，两名嫌疑人中包括一名供职首都首尔一家信息技术企业的前高级程序员。两人获利至少 10 亿韩元(约合 88 万美元)。另有 7 人因购买信息用于电话销售，由警方登记备案。

一名韩国电信发言人告诉法新社记者，这家企业手机用户大约 1700 万，超过一半、即 870 万用户信息泄露。韩国电信公司 29 日向用户致歉。

6. 保密形势严峻

- 新保密法10年修订
- 保密检查全面展开
- 分保工作全面展开

国家安全

经济目的性

个人威胁

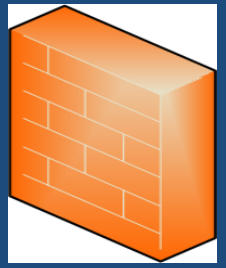
基础设施

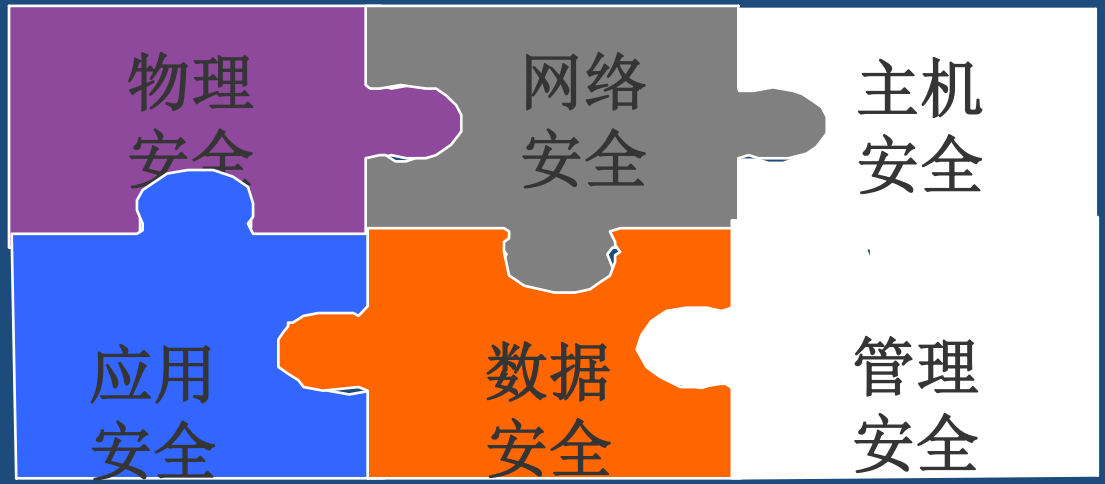
终端设备

保密形势

安信天行

二、信息安全管理的新趋势





我们是不是忽视了什么？或者说欠缺了点什么？

2、业务信息系统安全稳定的运行

本位回归

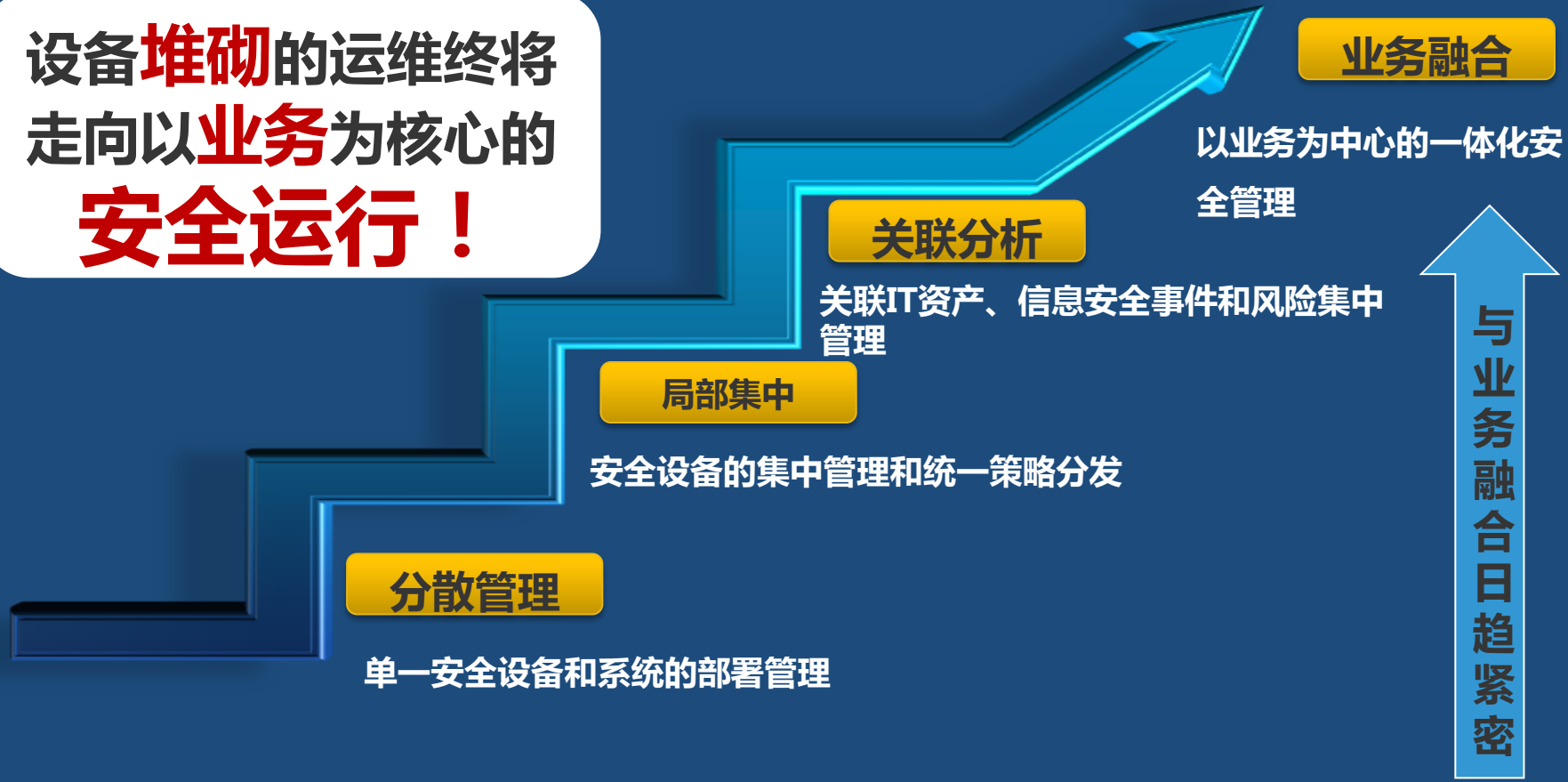
物理 网络 系统

应用 业务

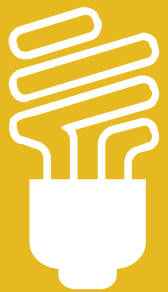
管理安全 ……

安全运行管理的关注点—业务

设备**堆砌**的运维终将走向以**业务**为核心的**安全运行！**

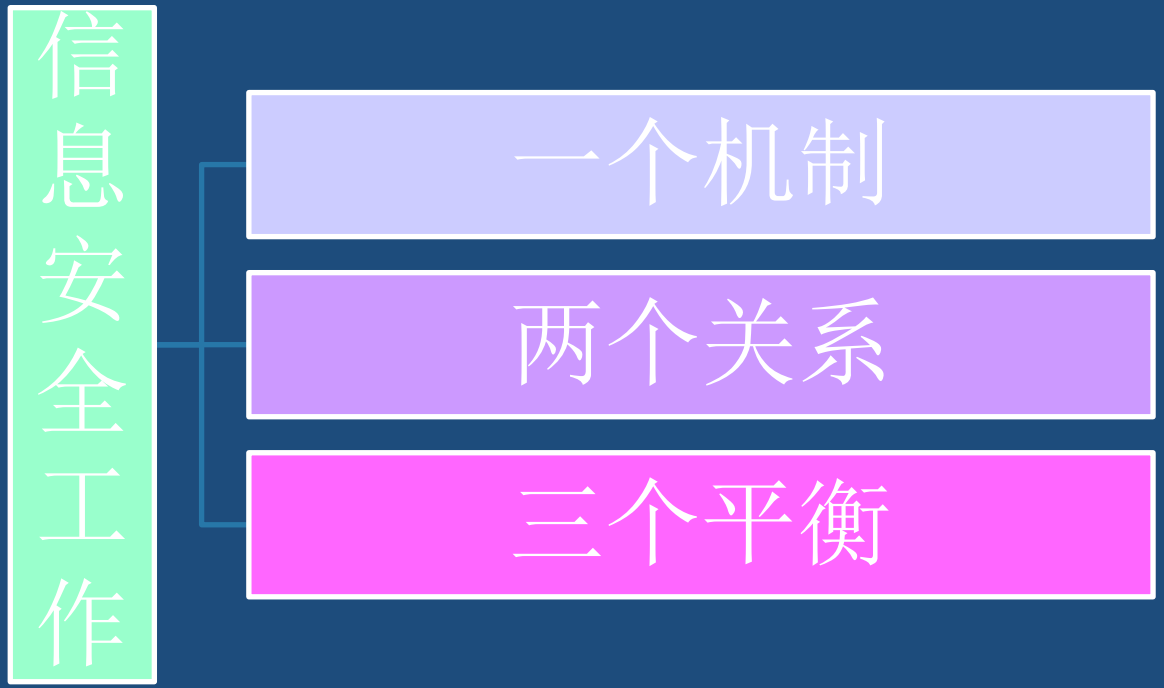


安信天行

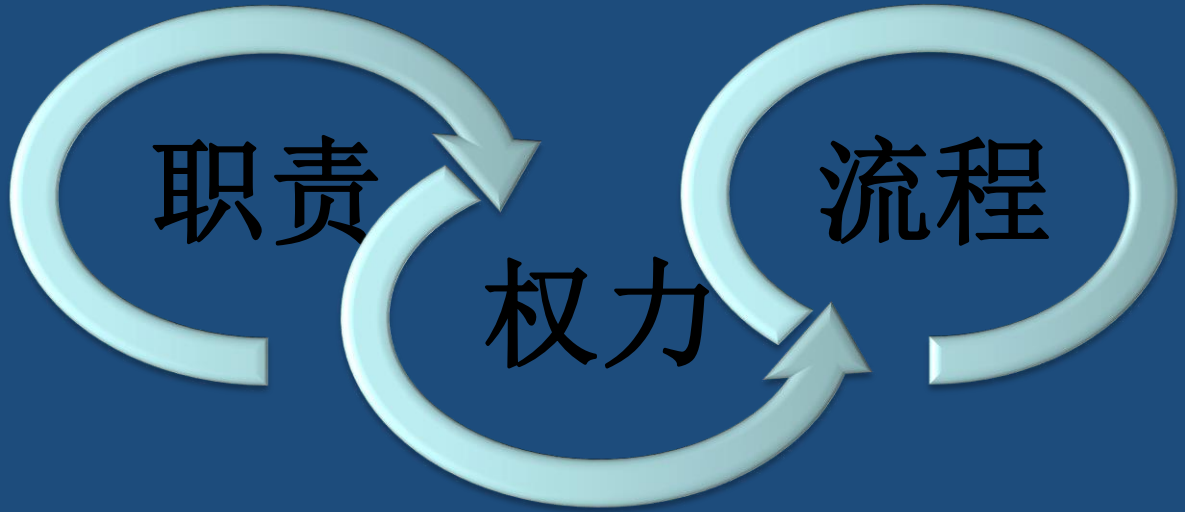


三、信息安全管理的几点建议

如何做好信息安全工作



一个机制：管理机制/工作机制



两个关系

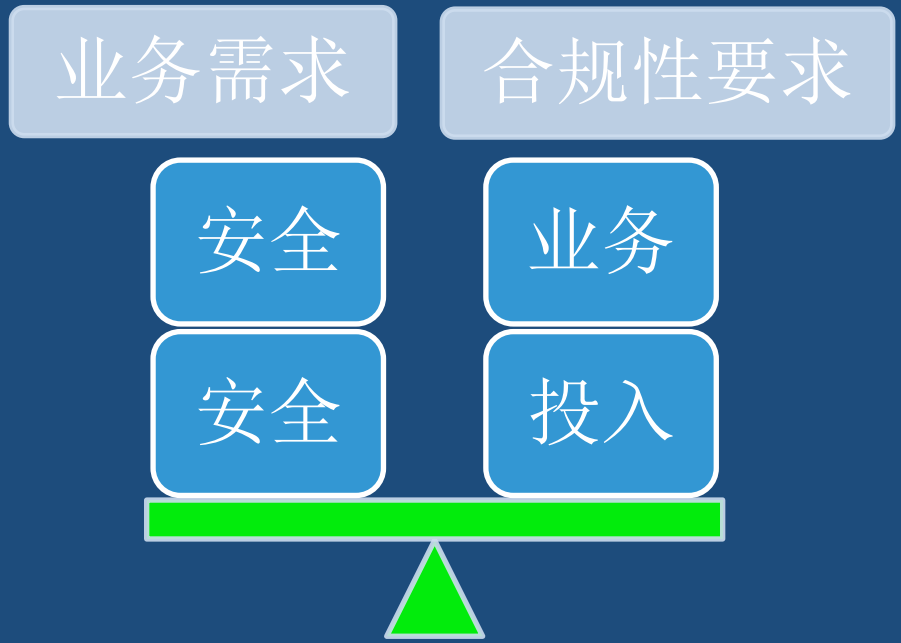
信息安全与信息化的关系

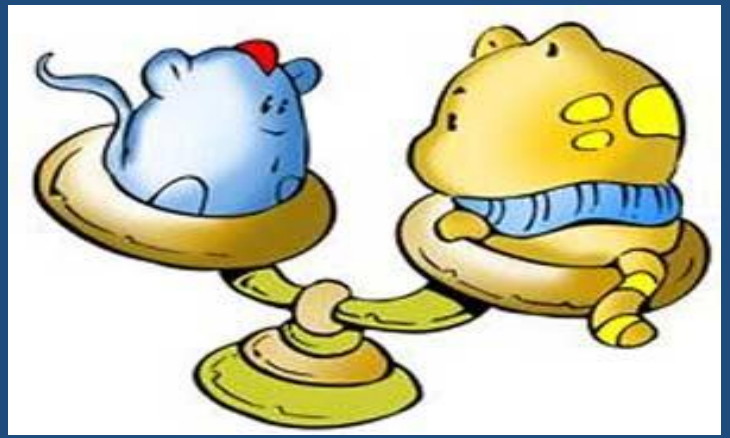
1. 信息安全是信息化是否成熟的标志
2. 信息安全是信息化应用有效开展的基础
3. 信息安全是业务正常、可靠运行的保证

安全处与其他部门的关系

三个平衡

信息安全---寻求平衡的过程





做好安全工作的几点建议

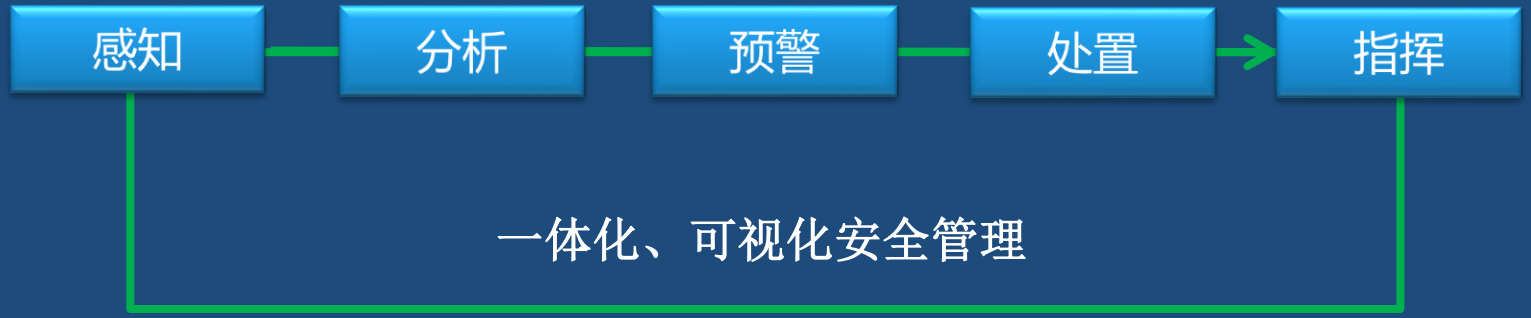
1、了解单位的信息安全目标是什么？

- 保护我们的秘密与敏感信息、保障业务安全稳定的运转；
- 确保法规遵循；
- 使我们的关联单位（包含上下级单位）满意，让他们确信他们的数据在我们这边是安全可信的；

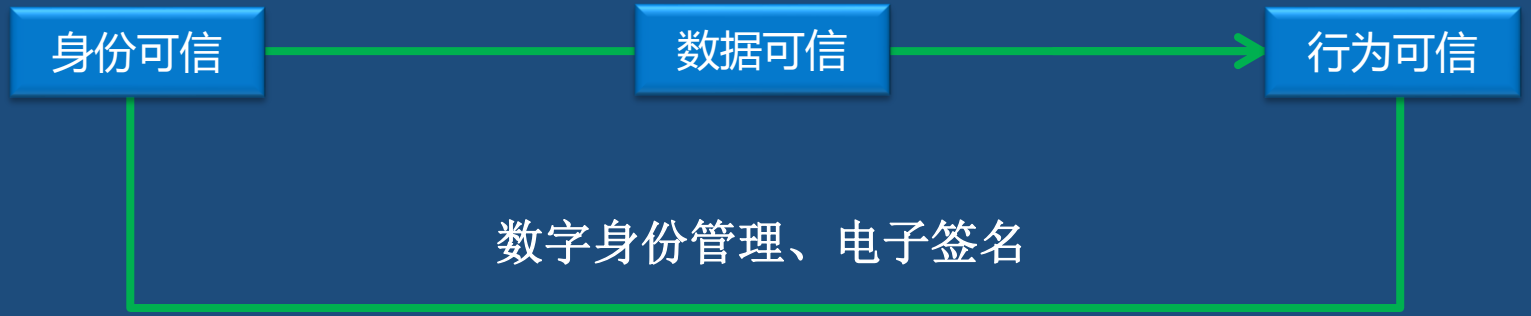
2、争取单位最高领导支持

3、将信息安全做成单位业务流程中的一部分

- 构建人口健康系统统一指挥、协同有序的安全管理体系



- 构建人口健康信息全生命周期的网络信任体系



4、将安全保障工作融合到系统建设过程中

系统建设前	• 咨询活动：分析业务系统的安全属性 • 安全设计：结合等保思想开展安全设计
系统建设中	• 安全植入：在当前安全平台中的安全植入
系统上线前	• 检测：代码安全检测、安全测试、脆弱性检测 • 加固优化：应用、系统等加固与优化
系统正式运行	• 整合：新系统整合到现有服务的范围内 • 计划与执行：制定调整整体服务计划，植入到原有运维体系中

5、让每个人每个部门都清楚信息安全与他们的关系；

将信息安全与

他们自身的发

展…关联起来

信息安全与我们之间的关系

个人

单位

国家

- 工作效率
- 个人财富
- 个人前途
- 个人自由

6、充分了解各个业务环节中安全因素

7、对内部安全问题要引起足够重视；

内在风险

外联监控；

资源管控；

8、合理应用业务安全需求，但不能影响效率，安全要与业务紧密结合，建立在保障业务发展的基础上重点防御，避免防护过度

9、尽可能的让信息安全实现对用户的便利性

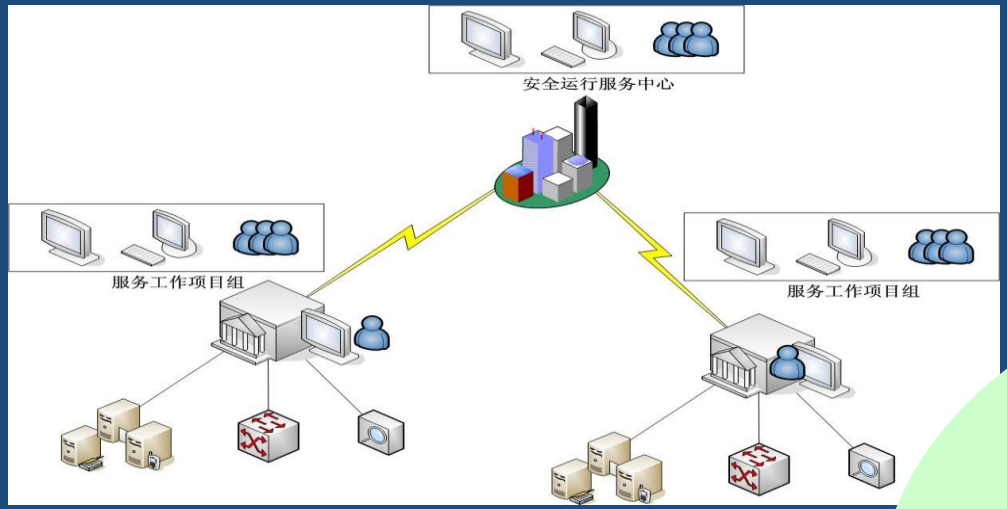
10、建立威慑力量；

审计追踪

11、强化培训

- 安全意识培训
- 安全技术培训
- 安全管理培训
- 安全制度培训

12、统筹利用社会资源



政府业务系统

一线队伍

BJCA总部专业团队待命

BJCA实验室

资深专家

BJCA总部专业团队

我们致力于

让信息安全变得简单，并可管理!

微信订阅号

新浪微博

翟建军
邮箱：zhaijianjun@bjca.org.cn
电话：010-58045886