网络安全架构设计过程中如何处理数据安全与用户隐私保护之间的关系

王艳辉　　360集团隐私审核总监

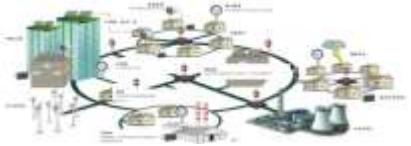
ISC 互联网安全大会 中国·北京
Internet Security Conference 2018 Beijing·China

目录

一、挑战

一、挑战

智慧城市



智能电网

智能家居

万物互联

车联网

智能工厂&制造

联网的可穿戴设备

一、挑战

一、挑战

美国千万公务员信息泄露：受害者尚未接到通知

金融界 2015-07-15 22:24:00

北京时间7月15日消息，美国政府官员周二表示，尽管两个月前相关部门就已发现，美国政府2150万雇员的个人信息在黑客攻击中泄露，但政府官方尚未通知任何受影响的个人。

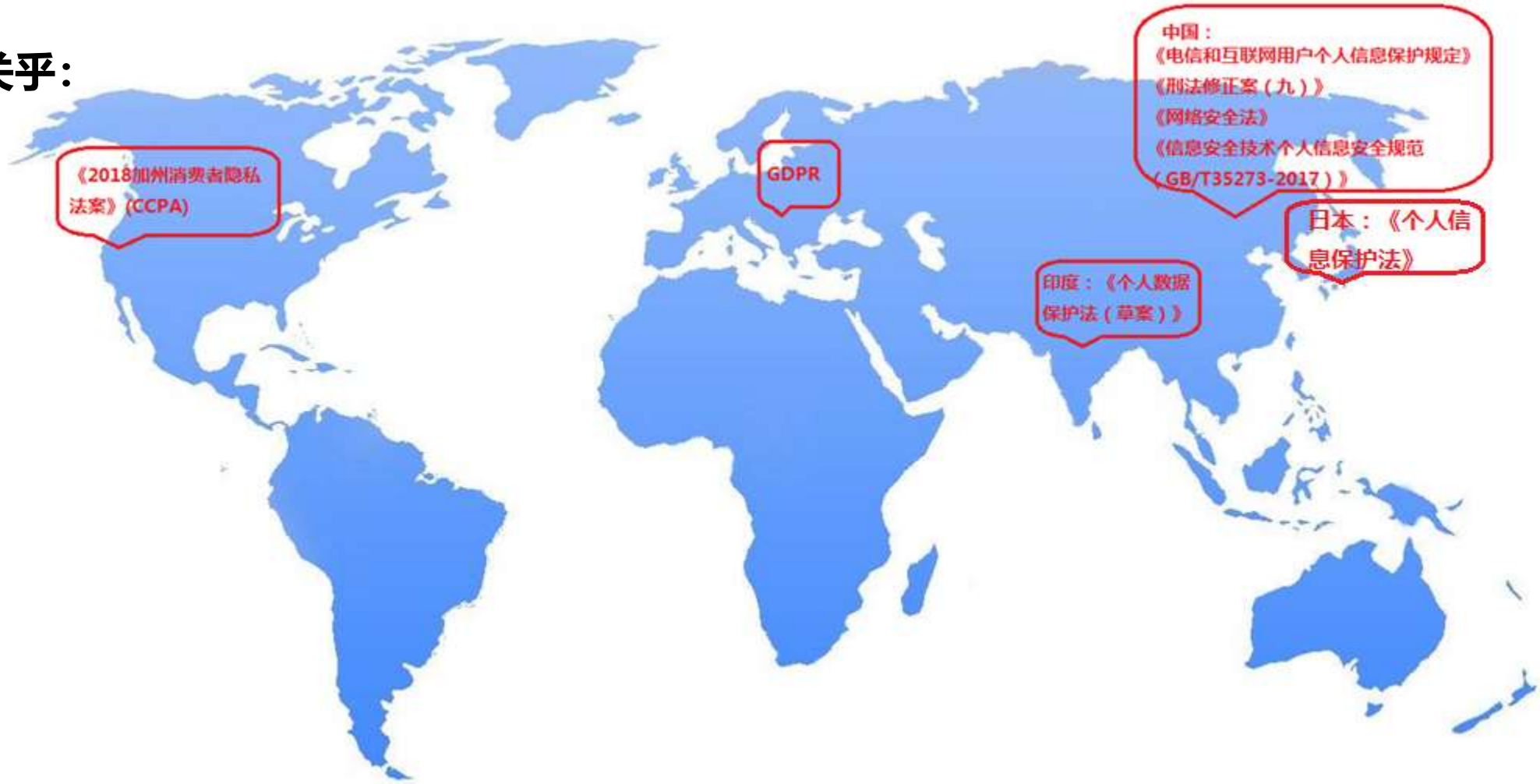
路透社援引美国多个政府部门消息人士的说法称，负责管理这些数据的美国人事管理局正在与其他部门共同设立系统，以通知受影响的个人。美国人事管理局一名官员表示，由于数据本身很复杂，而许多政府雇员会在多个部门之间流动，因此确定一种合适的通知机制需要几周时间。

这名官员表示，美国政府正尝试设立统一的系统，而不是让不同部门分别发布通知。预计美国人事管理局将聘请承包商负责此事，不过目前招标尚未开始。

一、挑战

用户个人信息关乎：

- 人身安全
- 社会安全
- 国家安全



一、挑战

大数据与隐私保护之间的平衡：

数据滥用

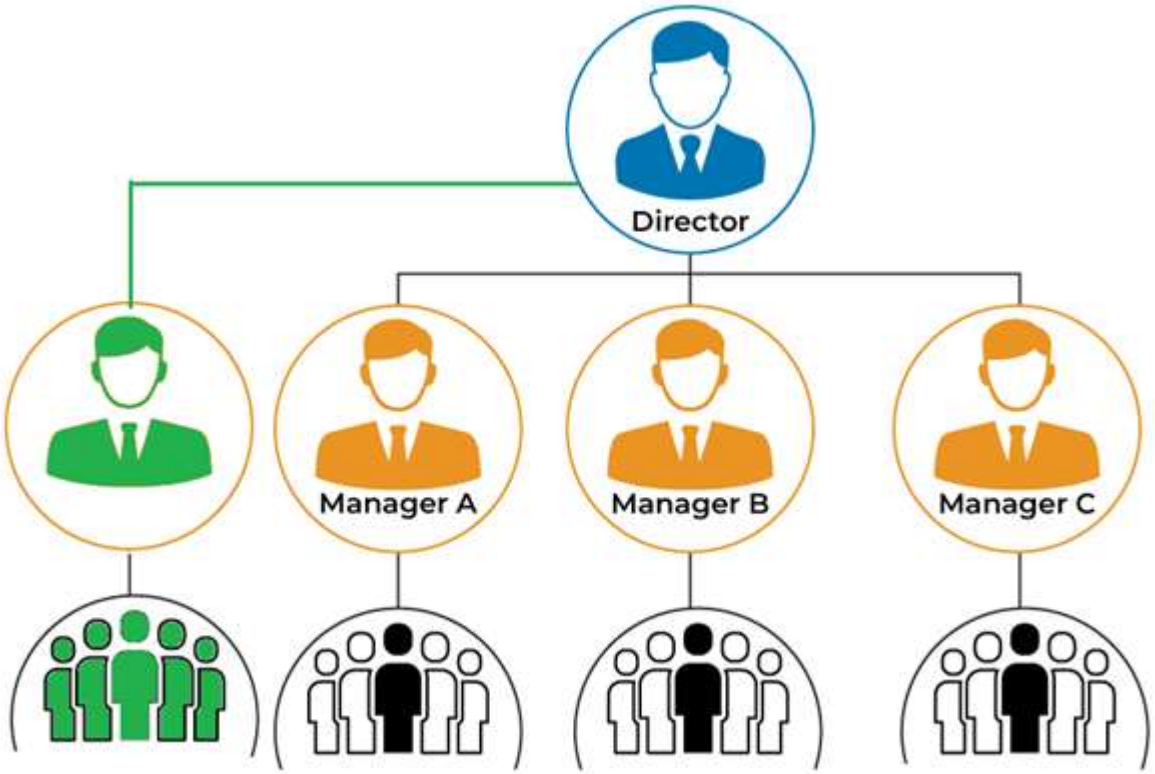
数据泄露

二、有效的组织架构

二、有效的组织架构

企业发展：

- 追求利润，重视大数据开发利用
- 惩罚力度轻，轻视个人信息保护



推动个人信息保护，保证大数据产业的健康发展，保证个人信息安全：

- **改变现有组织架构，建立自上而下管理机制**

二、有效的组织架构

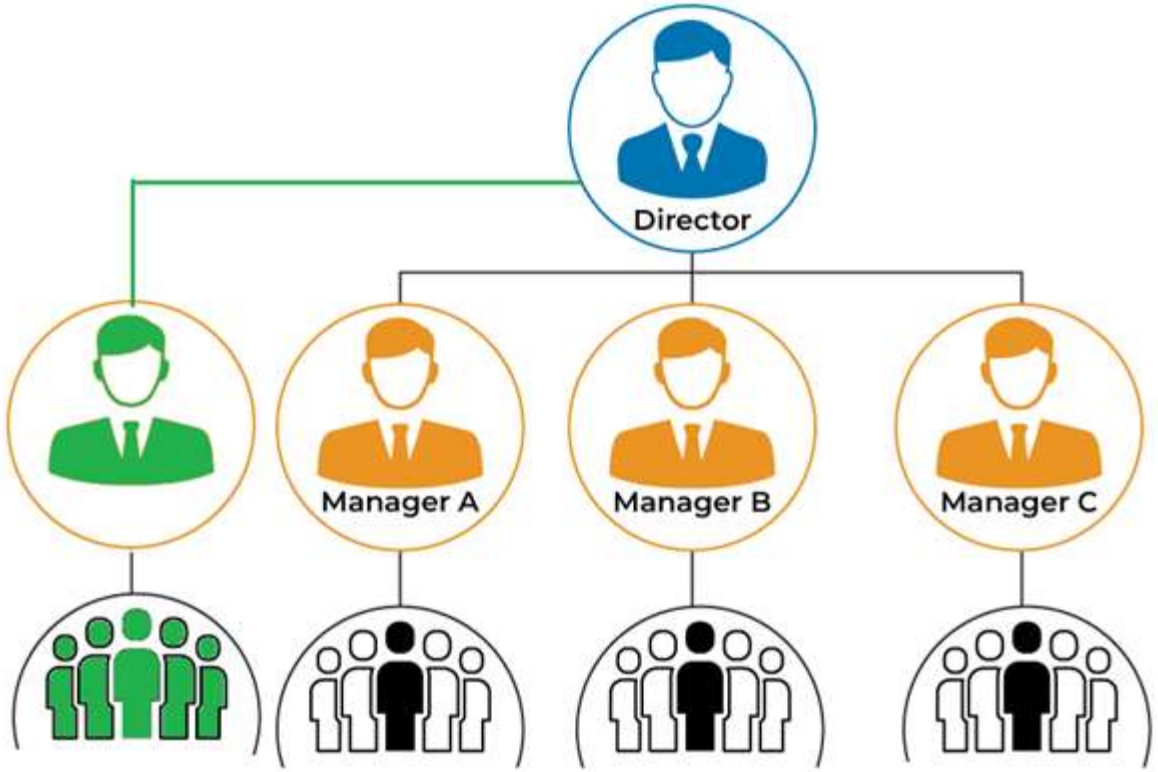
首席隐私官？ 数据保护官（DPO)? 数据安全官?

- 直属于公司CEO管理，拥有用户数据最高决策权和监督权
- 有很强的执行力和推动力
- 将个人信息保护纳入信息安全管理范畴
- 决策个人数据在企业内外的流动，并监管
- 了解国内外法律法规、推动各个业务、各部门个人信息体系保护建设
- 制定适合企业发展的流程、制度
- 了解企业所有业务，从产品设计初期介入，可以对业务say no
- 了解网络安全
- 了解互联网技术实现
- … …

二、有效的组织架构

一个CPO+一个隐私部门+：

1. 法务 +
2. 信息安全部 +
3. 大数据中心 +
4. OPS +
5. 业务部门



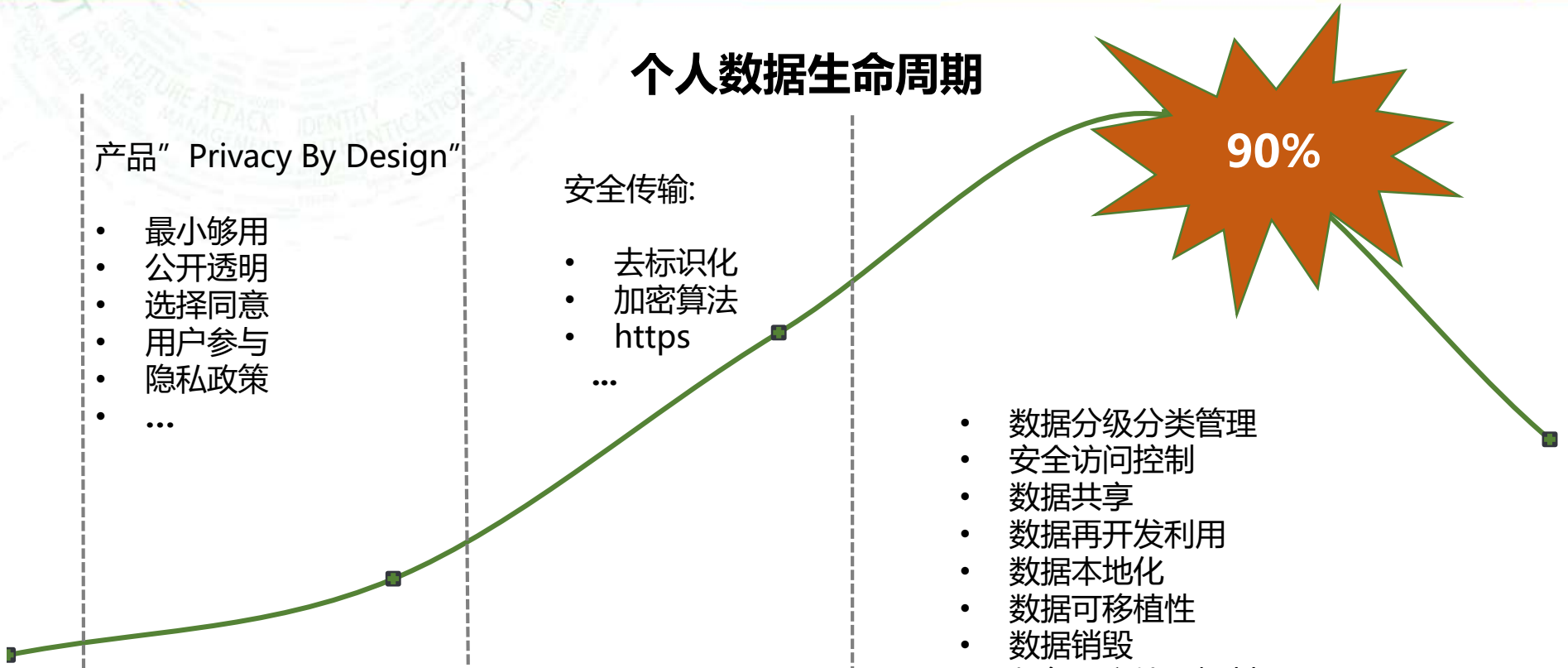
职责：

1. 研究相关法律法规
2. 制定内部相关流程
3. 加强信息安全技术手段
4. 对业务功能进行决策
5. 隐私政策
6. 一切与个人信息保护相关的事宜

三、安全架构设计

三、安全架构设计

个人数据生命周期



产品”Privacy By Design”

- 最小够用
- 公开透明
- 选择同意
- 用户参与
- 隐私政策
- …

安全传输:

- 去标识化
- 加密算法
- https

…

- 数据分级分类管理
- 安全访问控制
- 数据共享
- 数据再开发利用
- 数据本地化
- 数据可移植性
- 数据销毁
- 紧急预案处理机制
- …

Before Collecting

Collecting

After Collecting

三、安全架构设计

收集前：

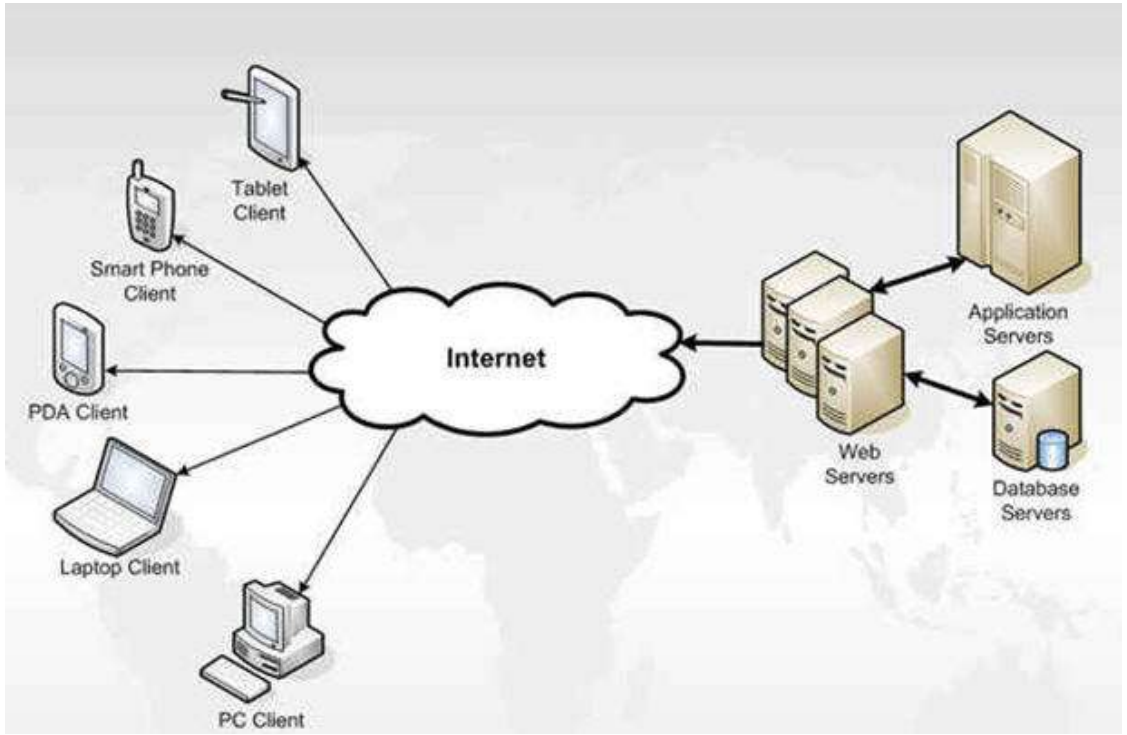
（1） 隐私政策

（2） Privacy By Design

- 不该看的不看
- 不该传的不传
- 不该存的不存
- 不该用的不用
- 一切行为必须明示、尊重用户的知情权和选择权
- 必须经过用户许可

（3）软件的安全防护

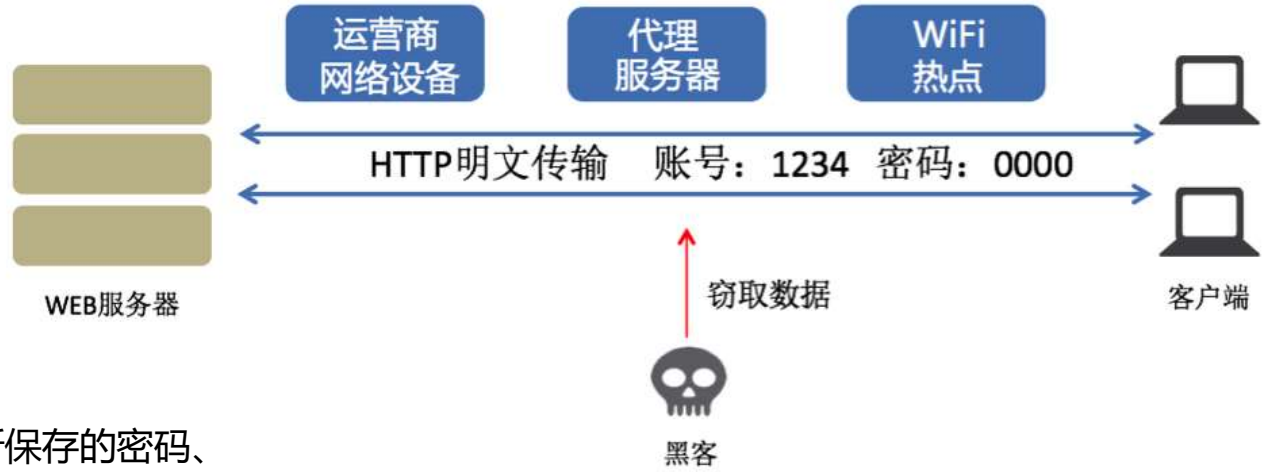
防篡改，防逆向，防窃取，加固



三、安全架构设计

收集中：保证传输过程的安全

- 加密算法
- https
- 去标识化，匿名化
- password非明文存储
- Android Webview SSL 自签名安全校验，避免浏览器所保存的密码、Cookie、收藏夹以及历史记录等敏感信息被恶意盗用，从而造成个人信息被泄露。
- … …



三、安全架构设计

收集后

收集内容与约定的一致，或自查自身业务收集的用户个人信息

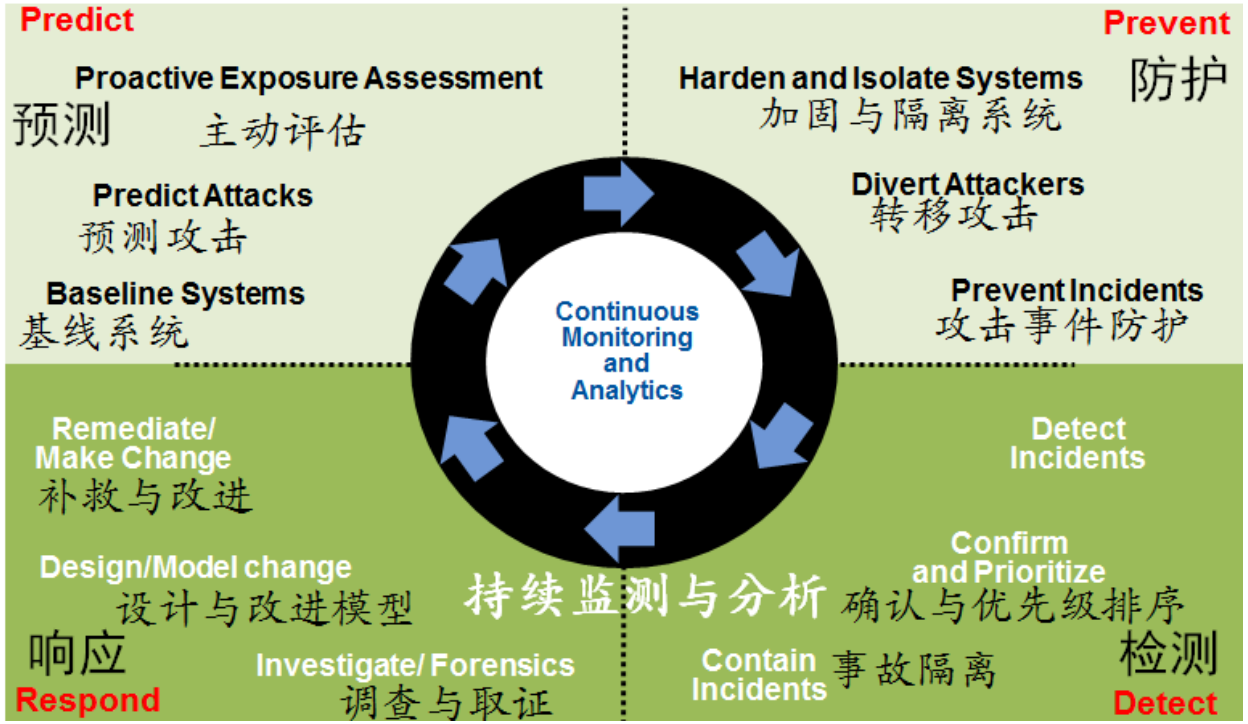
- 抓包
- 旁路监听：20w通信模型、发现100多个异常通信模型
- 日志分析

访问控制监控

- 系统管理员、信息安全管理员、隐私审核人员三权分立、互相监督、互相监管。
- 异常访问检测

服务器加固

- 服务器漏洞检测与补丁
- 开源系统漏洞检测与补丁
- 定制化开发
- APT攻击检测
- ……



三、安全架构设计

收集后

防批量访问、导出

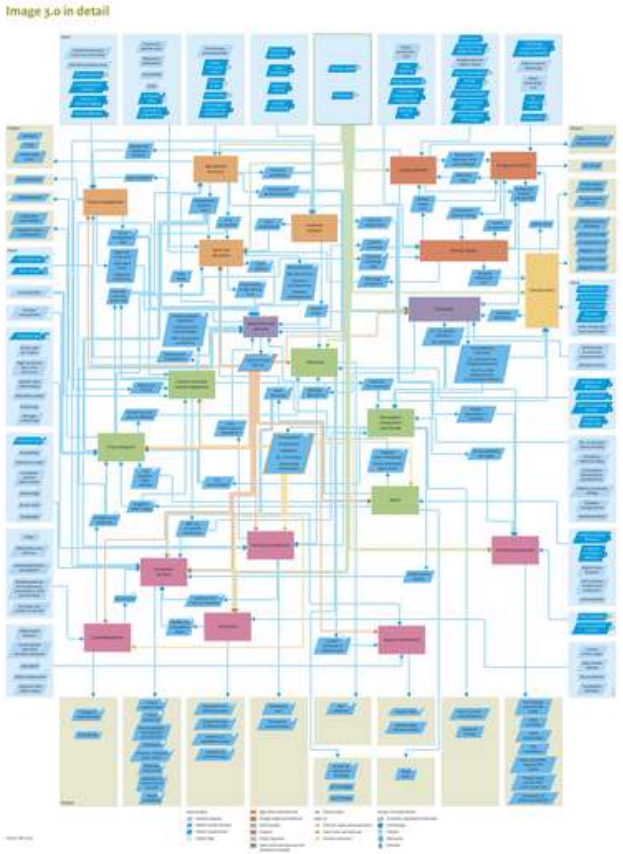
- 客服系统、不显示号码、通过平台一个一个操作
- 堡垒机

分级分类管理

- 建立公司级的数据血缘关系管理，目录级别->内容级别
- 统一对外合作接口监控管理
- 删除与销毁

数据共享

- 内部共享：原始数据不共享，清晰业务模式，模型后脱敏数据
- 外部合作：原始数据不共享，清晰合作目的，合同约束，接口提供，接口访问异常检测



三、安全架构设计

紧急预案处理

- “防不住”已成共识
- 自动化是王道
- 应急响应即服务

四、仍待解决的问题

四、仍待解决的问题

跨境问题

- 很多国家立法限制个人数据跨境转移
- 本地化vs全球化，例如：社交数据、电商

不同国家的法律冲突

- 企业在不同的国家有不同的数据管理标准?

网络安全标准

- 没有统一的安全标准
- 鉴定机构，时效性

数据真正的融合

- 企业外数据流动、真的能融合吗?

四、仍待解决的问题

个人信息的使用和流动，一定会促进大数据产业的发展，一定会促进科技的进步，社会的发展。同时，作为个人信息使用者不能忽视对个人信息的保护。当个人信息保护与数据使用者利益发生冲突时，必须保证个人信息的安全优先。

ISC 2018
ISC互联网安全大会

360互联网安全中心

谢 谢！

ISC 互联网安全大会 中国 · 北京
Internet Security Conference 2018 Beijing · China