OWASP

Open Web Application Security Project

金融云隐私挑战与应对

演讲者：陈绍良　　普华永道

个人介绍

陈绍良先生，普华永道风险管理资深专家

拥有超过十二年的风险管理从业经历

其在信息安全、信息科技治理及服务管理

内部控制及合规性检查，商业连续性管理等领域能力突出

业内知名的金融行业风险管理专家

参与国内外金融机构的风险管理体系建设

对于交易风险控制有着独到见解

同时信息安全领域有着丰富的实践经验

带领团队多次高质量地完成项目实施

主要服务于金融、互联网、运营商领域

目录

提醒：

我在讲解PPT时，如有任何问题，您可以举手示意。

同时我已将需要讨论的问题在PPT中列出。

金融云隐私的定义和分类

一组统计数据

来自普华永道的2017全球信息安全调查报告

63%企业表示进行IT云计算化，其中**32%**金融企业进行IT云计算化。

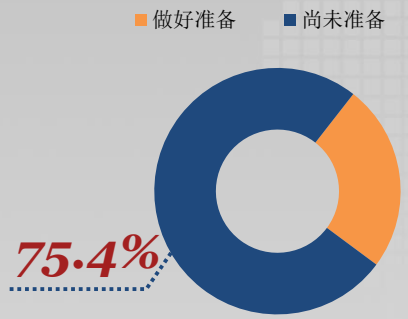
未来12个月中，关于隐私这方面的行动如下：

38%的企业计划进行要进行员工隐私培训和教育
36%的企业计划制定隐私保护的策略
32%的企业计划进行隐私评估
31%的企业计划制定隐私事件响应

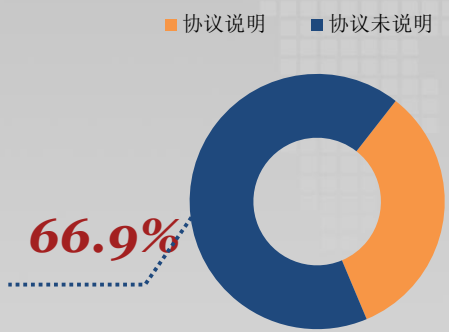
数据来源：www.pwccn.com

一组统计数据

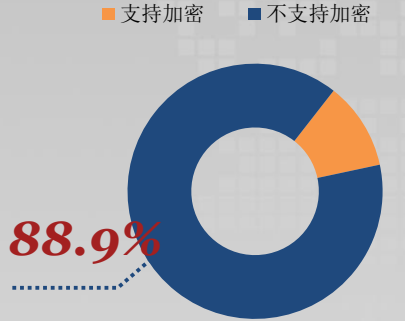
统计显示全球**75.4%**基于云的应用没有准备好如何应对欧盟的通用数据保护条例(GDPR)，另一种叫法为一般数据保护条例



统计显示**66.9%**的云服务没有在服务协议说明用户对于数据的拥有权



统计显示**88.9%**的云服务不支持静态数据加密



数据来源：resources.netskope.com

隐私的关注

- 隐私关注

  《中华人民共和国网络安全法》2017年6月1日
  《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》
  《中华人民共和国民法总则》2017年10月1日 隐私权力

  网络安全法提及的个人信息保护工作是同样关注个人数据及隐私保护

  IAPP组织认为：“Data privacy is focused on the use and governance of personal data”

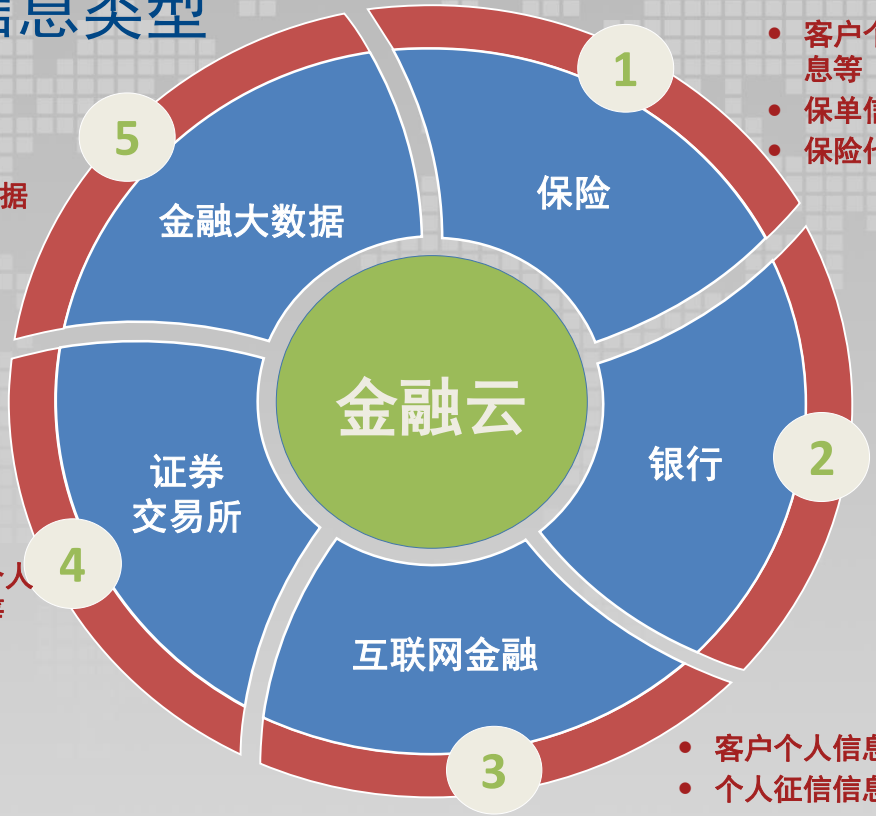
- 云隐私是什么

  各种形式的云+隐私相关的各类数据及信息

- 金融云隐私是什么

  金融类企业+使用各种形式的云+金融企业不被罚+供应商不被投诉+隐私相关的各类数据及信息

金融隐私信息类型



- 客户个人信息，如：个人身份信息等
- 保单信息
- 保险代理人信息

- 客户个人信息，如：个人身份信息等
- 客户的交易数据
- 客户贷款信息
- 银行卡信息
- 个人征信信息

- 客户个人信息，如：客户理财信息等
- 个人征信信息

- 客户个人信息，如：个人身份信息、收入情况等
- 客户的交易数据

- 来自第三方的数据
- 自身采集的

隐私保护与个人信息保护

共同点

目标一致：两者都以保护数据为目标。

防护方式：两者可以采用相同的防护措施

保护组织：同一保护组织

处罚程度：目前中国及国外对于隐私这块的法律处罚是严厉的

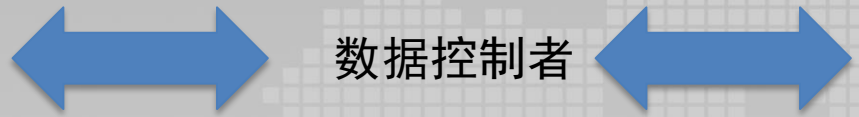
不同点

范围不同：个人信息范筹更大。个人信息是反应人的生物特性和社会特性的信息。

权属上：隐私更强调个人的信息不被其他人知晓，个人信息更强调个人对信息的控制。

保护角度：隐私更强调信息及数据隐秘性。个人信息更强调防泄露，防滥用，防诈骗。

隐私数据保护角色及定义



定义：法律所定义的个人及组织
角色：个人敏感数据及隐私数据

定义：数据实际控制者，此处表达更多为组织
角色：如传统银行，Fintech

定义：从事数据处理者
云服务提供商，如AWS，Azure阿里等

备注：此处角色的认定还是要依据各国的法律具体规定

问题

金融云数据的特点？（5分钟讨论）

金融云隐私数据的特点

- 用户的姓名
- 家庭住址
- 通信方式
- 通信录，通信记录
- 婚姻情况
- 消费习惯
- 精确的地理信息

- 关键核心信息
- 对人身安全起着重要的影响作用

- 公有云，私有云，混合云，社区云
- CSP本土供应商、CSP海外供应商
- 数据本地存储、数据跨境存储

- 处理难度大
- 定位难
- 协调部门多
- 直面社会信任危机
- 企业信誉挽回难度大

- 用户全球化
- 合规标准的全球化
- 数据分布的全球化
- 管理的全球化
- 应对危机的全球化

金融企业隐私保护的驱动力

法律层面的惩治也日趋严厉，国内加强这块的立法和管理

社会层面，广大人民群众对于隐私保护的呼声日益强烈

金融关联的基础设施已成为网络安全法中的关键基础设施.

隐私保护的能力也是一家企业的重要的竞争力

全球趋势，特别是中国走出去的企业越来越多，海外监管严厉

隐私保护遵从的法律和标准

遵从国家法律

- 《中华人民共和国刑法》
- 《中华人民共和国网络安全法》
- 《全国人大常委会关于加强网络信息保护的决定》
- 《电信和互联网用户个人信息保护规定》
- 《信息安全技术公共及商用服务信息系统个人信息保护指南》
- 《中华人民共和国侵权责任法》
- ……

遵从监管机构的要求

- 《中国人民银行关于银行业金 融机构做好个人金融信息保护工作的通知》（银发[2011]17 号）
- 《金融行业信息系统信息安全等级保护实施指引(JR/T 0071-2012）》
- 关于加强银行卡敏感信息安全管理 防范终端机具改装的倡议书
- ……

遵从他国的法律（如境外业务，海外上市）

- 欧盟：
《一般数据保护条例》EU GDPR
- 美国：
《 隐私法案》、 《电子通讯隐私法案》、 《电脑匹配与隐私权法》

遵从国际标准的要求

- 支付卡行业数据安全标准（PCI DSS）
- ISO/IEC 29100《隐私保护框架》
- ISO/IEC29101《隐私体系框架》
- ISO/IEC 29190《隐私能力评估模型》

欧洲GDPR数据保护条例的重要突破-走出去的企业

重要特点

– 欧盟1995年《数据保护指令》的适用范围采取的是属地主义，即要求机构的成立地、或进行个人数据处理活动的设备位于欧盟境内。而GDPR则实现了从属地主义扩展至属人主义的突破——无论是何种行业或领域，只要在向欧盟境内个人提供产品或服务过程中涉及了个人数据的处理，该类数据处理行为都将落入GDPR的适用范围。例如：任何网站甚至手机软件（APP）只要能够被欧盟境内的个人所访问和使用，产品或服务使用的语言是英语或者特定的欧盟成员国语言、产品标识的价格为欧元，都可以被理解为该产品、服务的目标用户包括欧盟境内用户，从而需要适用《条例》。此外，GDPR也在监管方式、数据处理要求、数据主体权利、数据控制者和处理者的责任承担、数据跨境传输机制、监管与救济等方面，实现了显著的进步与发展。

- 适用提示
  - 中国云计算企业
  - 中国对境外用户提供服务的企业
  - 跨境电商
  - 大数据分析

- 主体权利
  - 知情权
  - 访问权
  - 反对权
  - 个人数据携带权
  - 被遗忘权（删除权）

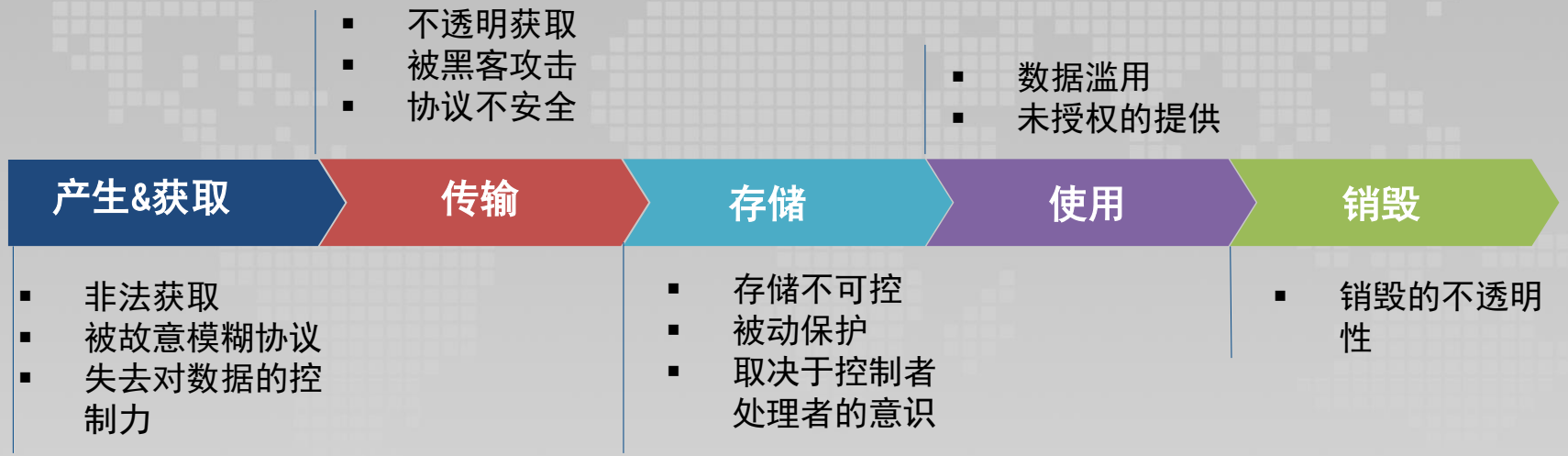
欧洲GDPR数据保护条例的重要突破-适用中国企业

- 云客户（具体使用者）关注点
  - 在GDPR定义为数据控制者
  - 基本原因要遵循
  - 风险评估
  - 签订责任明确的合同，合同签订的关注点
  - 数据主体所有者是否在欧盟境内
  - 确保透明度，目的，用途
  - 删除数据

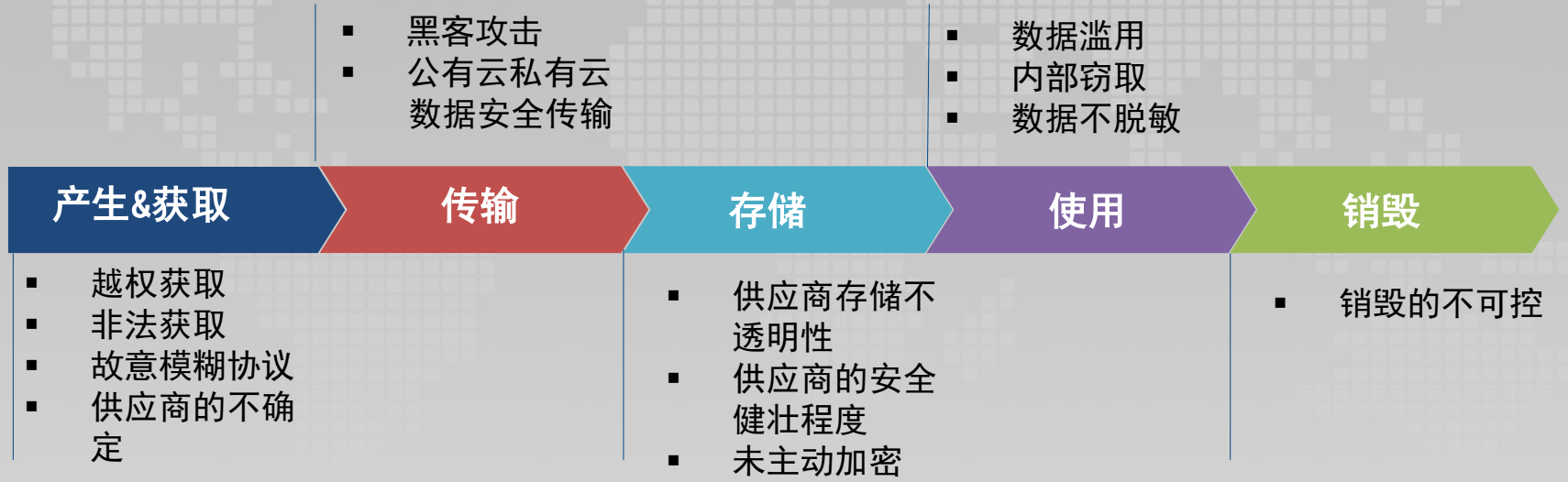
- 云服务提供商
  - 基本原则
  - 要针对云客户提供符合欧盟的数据保护措施
  - 不同服务类型，提供不同服务
  - 确保透明度，目的，用途
  - 删除数据

金融云隐私主要风险分析

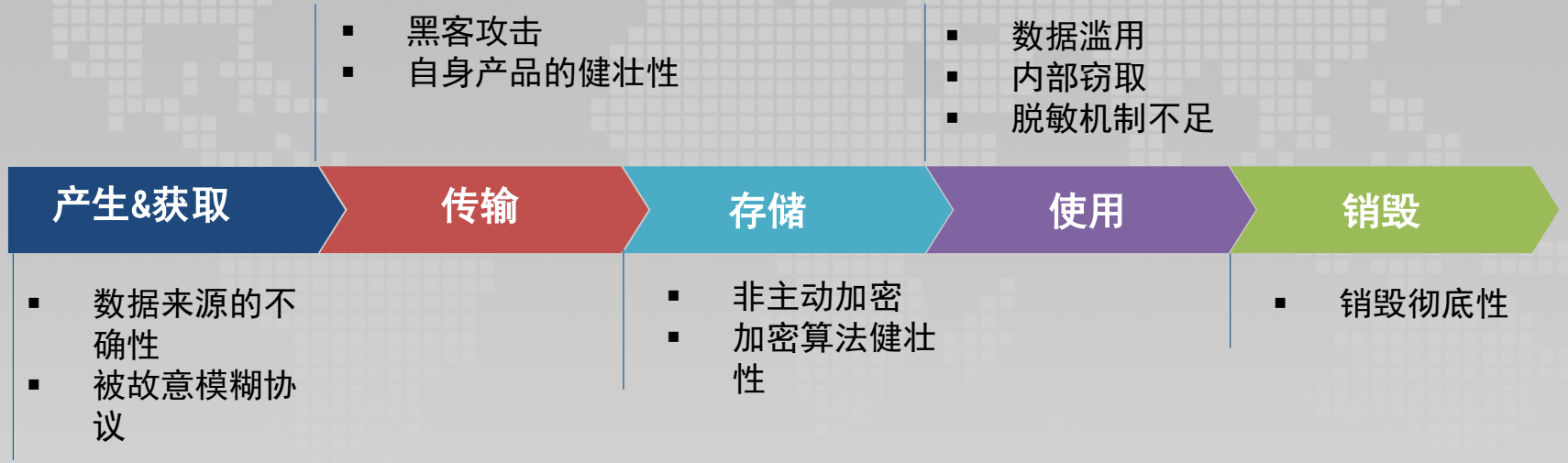
主要风险分析–数据主体（以个人为例）



主要风险分析–数据控制者



主要风险分析–处理者


黑客攻击
自身产品的健壮性
数据滥用
内部窃取
脱敏机制不足
产生&获取
传输
存储
使用
销毁
数据来源的不确性
被故意模糊协议
非主动加密
加密算法健壮性
销毁彻底性

问题

数据泄露事件发生带来企业损失？（10分钟讨论）

隐私泄露产生的成本估算

- 影响人数
  - 实际影响的人数，以实际泄露的人数比对数据库里的名单
- 处理时间
  - 单个人员核实时间 （以小时为单位）
  - 每个人员法律咨询服务时间（以小时为单位）
  - 单个受影响人员的（以小时为单位）
  - 其他交互时间（以小时为单位）

这个估算表近期推出，请关注微信公众号。

单个人员处理成本

法律人员（投入时间）

网络人员（投入时间）

安全高管（投入时间）

额外成本

品牌宣传费

取证与调查费

其他不可避免的成本，

客户丢失成本

影响客户数量

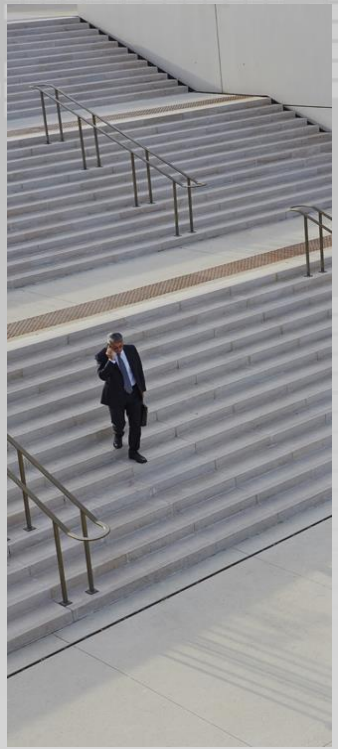
平均每个客户消费

金融云隐私的应对之道

问题

构建什么样的保护体系，从什么方面入手？（15分钟讨论）

金融云隐私整体保护框架



治理

- 以数据隐私项目推动建设
- 加强数据隐私意识
- 执行数据隐私认证
- 执行数据隐私度量
- 内部数据隐私审核，评估和评级

策略

- 建立数据隐私政策
- 完成数据隐私分类
- 整合数据隐私政策
- 隐私与信息生命周期管理
- 管理隐私订阅服务
- 隐私合规遵从
- 平衡隐私合规和员工监控

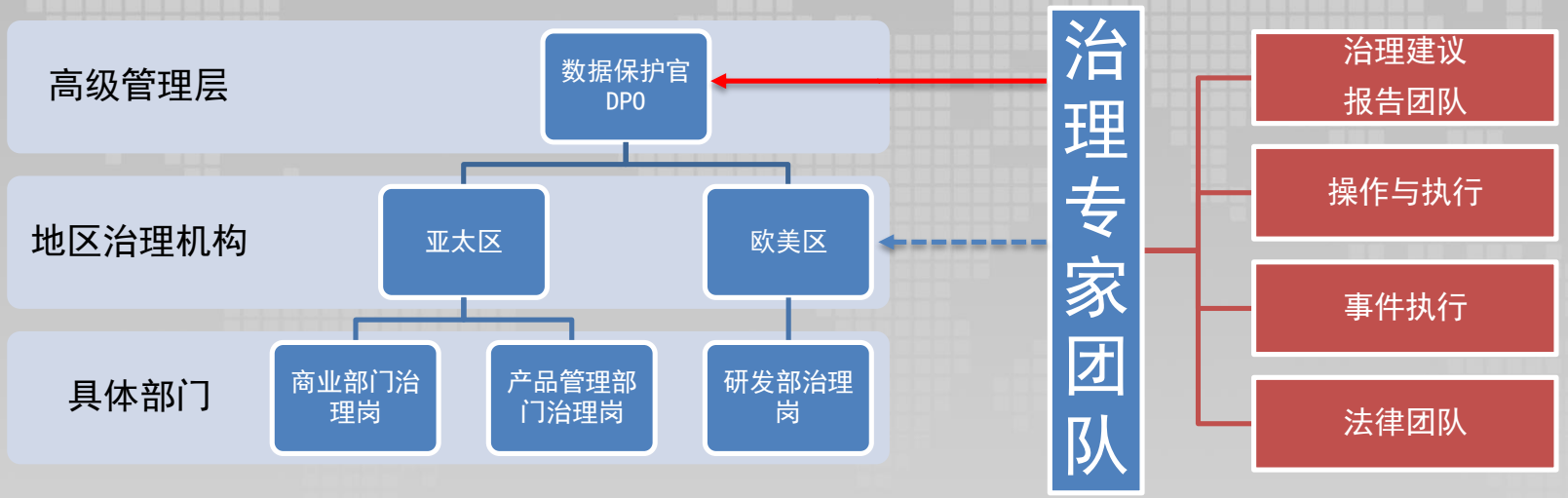
业务流程

- 执行隐私风险评估
- 执行运营管理过程
- 隐私保护团队建立
- 回应数据相关请求
- 保护跨境数据
- 管理第三方供应商关系
- 管理数据泄露风险
- 用户数据遗忘权执行

技术

- 实施隐私增强技术
- 保护移动环境中的个人信息
- 实施安全可靠的数据挖掘
- 安全的元数据存储管理
- 使用强加密和脱敏技术
- 访问控制
- 渗透测试
- 人工智能
- 机器学习
- 技术管控平台

治理-构建隐私保护的组织体系-团队架构



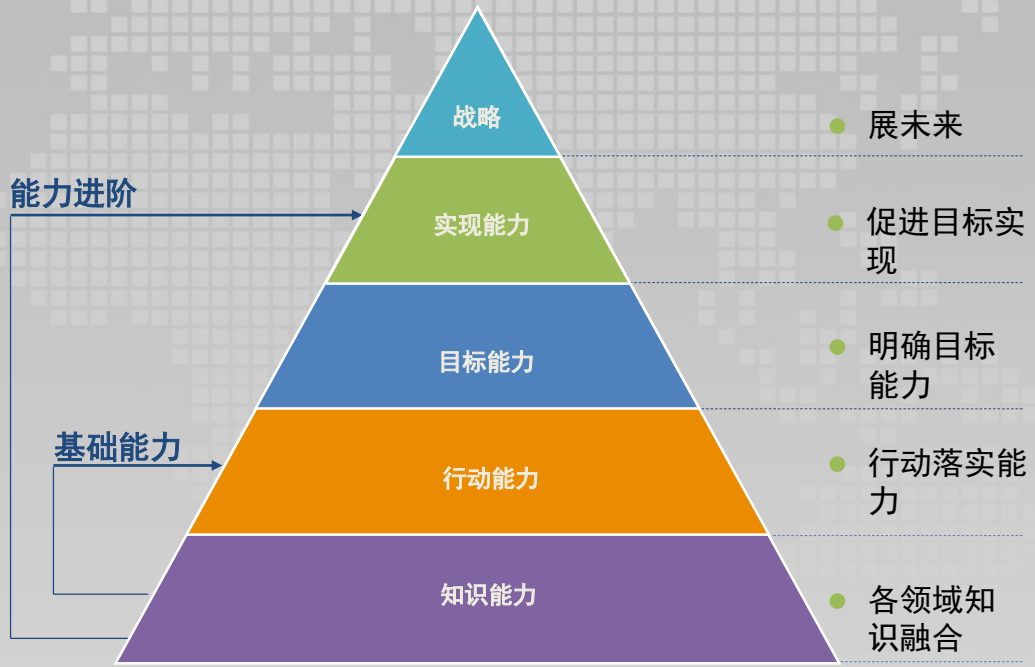
我个人认为 DPO定义可以扩大为数据及隐私保护官

治理-DPO能力体系

- DPO数据保护官
- DPO对我国企业来说是一个新兴的职位，但未来的重要程度不可忽视。

- 企业的管理层未来应对各类数据安全及隐私保护的挑战，非常有必要设立这个职位。

- 特别是对于已经开展和即将开展跨境业务的企业，是必须要纳入公司职级体系中的。



治理-构建隐私保护的梯次防线

第一防线

操作与控制

- 具体执行
- 切实感知
- 隐私评估

第二防线

制定管理

- 制定策略
- 管理汇报
- 评估合理

第三防线

内部审计

- 独立分析
- 独立评估
- 对外联系

治理-构建隐私保护的组织体系-职责划分

防线	部门	职责
一道防线	业务部门	制定具体本部门隐私合规流程 职责 隐私定义 隐私评估
一道防线	技术部门	技术架构 技术实现
二道防线	隐私合规部	隐私合规 策略制定 框架评估 框架调整
二道防线	安全及风险管理	提供物理安全 网络安全 应用安全 数据安全 保障 管理安全管理标准 隐私威胁建模 安全调查 取证
二道防线	风险管理委员	隐私保护宏观策略的制定与颁布 报告隐私主管部门
二道防线	法律部门	提供隐私保护的法律支持
三道防线	内部审计委员会	牵头隐私保护内部审计工作 制定隐私保护内部审计工作的内容 范围 方法
三道防线	内审部门	隐私保护评审工作 监督实施

策略—包括范围建议

- **收集哪些数据**
  - 人际关系网络（ 如IM，或交友类软件）
  - 设备信息，如IMEI等
  - 来自第三方或关联公司的信息
- **如何使用这些数据**
  - 提供、完善用户体验，广告服务等
- **这些数据如何被分享**
  - 网站使用、第三方使用、广告，推广等
- **如何管理和删除这些信息**
  - 如何保存，删除数据，用户可以采取的删除方式
- **如何管理和删除这些信息**
  - 如何保存，删除数据，用户可以采取的删除方式
- **如何应对法律的要求**
  - 适用何国何地法律
  - 有无美国，欧盟地区的法律条款的要求
- 运营的方式
  - 全球数据管理方式
  - 全球数据移动方式

策略实践—隐私保护的原则

1 明确个人信息收集的目的	6 个人信息的准确性.
2 个人信息的来源明确	7 个人信息使用的核查.
3 收集什么样的个人信息及收集渠道	8 对于第三方核查的必要
4 安全的存储个人信息	9 最小化使用个人信息
5 分权限的访问个人信息	10 减小个人信息泄露的可能性

问题

如何评估一家云供应商的隐私保护能力?
（10分钟讨论）

流程—供应商隐私保护能力评估模型

网络安全防护能力
- 是否有独立安全团队
- 是否有独立研发的安全产品
- 是否发生过大的安全事件
- 安全事件响应速度

数据加密能力
- 采用的加密算法，是国际通用的，还是中国标准的
- 数据加密处理的便捷性
- 数据加密采取的机制，是非对称加密，还是对称加密

数据透明处理能力
- 数据使用说明
- 数据分析使用说明
- 是否公布数据的去向
- 是否说明数据销毁情况
- 是否与第三方分享

数据脱敏能力
- 抗解密能力
- 防重复能力
- 脱敏数据可使用
- 脱敏算法的可靠性
- 脱敏数据不可恢复性

数据审计能力
- 云客户数据使用审计
- 云服务数据审计记录
- 数据迁移审计能力

认证情况
- 等级保护
- C-STAR认证
- ISO27000系列认证
- 跨境隐私规则（CBPR），FedRAMP认证 TRUSTe认证

问题

如何处理隐私泄露事件？（10分钟讨论）

流程—隐私泄露处理流程（供参考）

注意：国外对于数据泄露通知是有区别的

- 内部事务处理团队持续跟进事件情况，如漏洞修复，与客户沟通情况
- 确认内部和外部处理完毕，通过正式渠道向外公布。

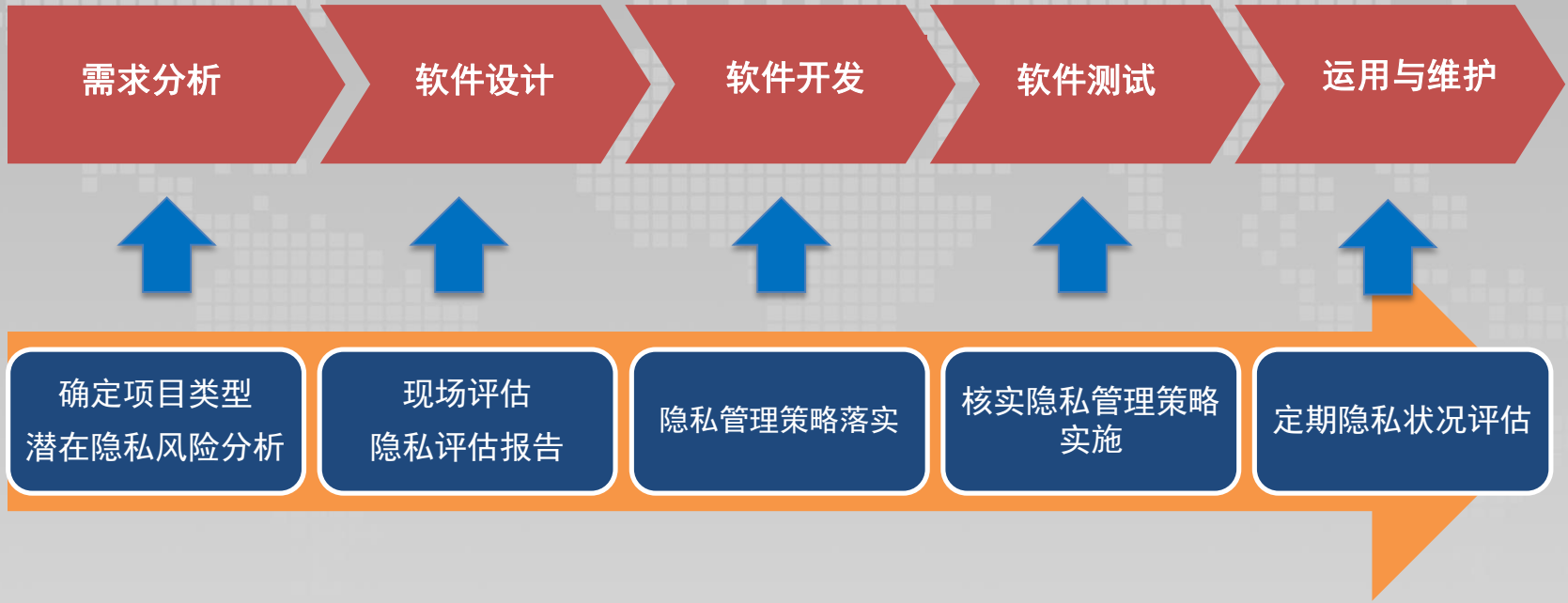
- 确认事件的真实性
- 内部沟通确认
- 知会相关责任人和关键领导

- 通过网站、邮件、微信、短信等渠道对外公布消息
- 同时启动对外服务渠道，与客户就隐私泄露问题进行沟通

- 召集关联业务领导和成员
- 召集公司法务人员
- 召开内部正式会议
- 与公安等司法机构沟通
- 与司法取证机构沟通
- 寻求外部法律和技术支持

- 确认对外发布的内容
- 确认对外发布的渠道
- 考虑外部安全资源的介入，进行相应的安全防护

流程—隐私评估在软件开发生命周期中的实践



问题

隐私评估报告的结构及阶段（10分钟讨论）

流程—隐私影响评估检查项-APP（示例）

技术漏洞	• 是否关键页面存在钓鱼劫持风险，导致用户信息泄露 • 是否本地存储用户名和口令 • 是否存在SQL，XSS, CSRF漏洞，导致数据泄露
功能使用	• 权限的合理性 • 权限分配表 • 权限的梳理检查 • 权限滥用导致隐私数据泄露
网络通信	• 网络通信协议的可靠性和安全性 • 是否使用如HTTPS的通信协议 • 是否进行二次加密通信 • ……
数据合规	• 使用国家，是否存在海外国家用户 • 服务器是否部署在海外国家 • 是否上传银行卡号、身份证号等 • ……

未来可形成APP隐私保护的检查表，指导可落地工作

技术—隐私保护技术的实施建议

- 网络层面
  - 加密通道是必须的，如 SSL
  - 客户端和服务端

- 服务器端
  - 审计是必要的，不管是云客户及云服务提供商
  - 如有必要，可以增加数据加密网关或软件，
  - 如果应用加密软件，一定要将加密过程写在应用中，要进代码封装，要能抵抗反编译

- 数据库
  - 开启数据库软件本身的加密功能是必须的。
  - 确保数据库的版本是足够健壮的，必要的补丁还是升级的
  - 数据库的审计和必要动作拦截是必须的
  - 云客户可能考虑自行使用高强度的加密方法，如PGP(Pretty Good Privacy)，IBE算法(Identity-based encryption)，目前基于物联网和云计算研究比较多，解决PKI中的身份证书的管理问题

技术—隐私保护技术的实施建议（续）

- 大数据分析
  - 大数据分析及预测是基于对个人隐私的保护
  - 隐私及敏感数据一定要进行足够强度的隐私算法，防止数据还源

- 关键提示
  - 加密：加密只是隐私数据防护&个人信息保护的一环，需要整体的DLP方案相配套，这是云客户及云服务商双方努力的
  - 前瞻：保持隐私数据技术的前瞻性
  - 访问控制：建立基于角色，对象的信息访问机制，对于进行数据严格授权访问