RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012

THE GREAT CIPHER

MIGHTIER THAN THE SWORD

伟大的密码胜于利剑

识别、评估和保护信息资产

Branden Williams 和 Jason Rader
RSA Security

RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012

专题会议 ID：SM-1002
专题会议分类：中级

我们如何估算信息的价值？

数据与金钱

- 一方面，我们有一些数据

- 另一方面，我们有大量金钱

转换率是什么？

- 10 位数据 = 10 RMS？
- 1 GB = £1,000？
- 1 个字节 = 2 位？

- 此转换率位于何处？ 如何使用它？
  - 不存在！
  - 有太多因素影响它的全球映射。

信息分类情况如何？

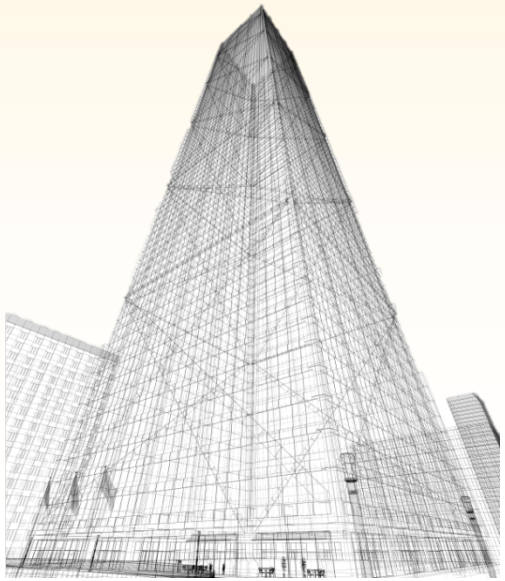
信息分类情况如何？

- 典型的分类系统存在问题
  - 缺少定义（这类信息由什么构成？）
  - 以及自动化（教系统如何处理）
  - 不处理个人数据价值（需要保险存储？）

从数学角度看情况如何？

- 信息分类并不能真正解决成本/收益/风险问题
  - 让外部价值 = 回报 * $\log_{10}$（角色数）
  - 让可靠性 = 历史上计算价值的能力
    - 数量 > 0 且 ≤ 1
    - 低可靠性会导致保护成本较高
- 在保护方面花费的资金 ∝ $\frac{\text{外部价值}}{\text{可靠性}}$
- 必须考虑内部价值！

我们需要一个新模型



- 最少的模型要求：
  - 按价值对信息分组
    - 对于我
    - 对于竞争对手/军方
    - 仅当信息丢失时
  - 解决随时间推移的信息价值
    - 信息价值随时间的推移不断变化
    - 通常会发生折旧，有些信息比其他信息折旧更快一些
  - 反映角色数和动机
  - 反映基于回报的动机的变化
    - 市场力量会动态改变这一点
    - 大型数据存储比小型数据存储更具吸引力

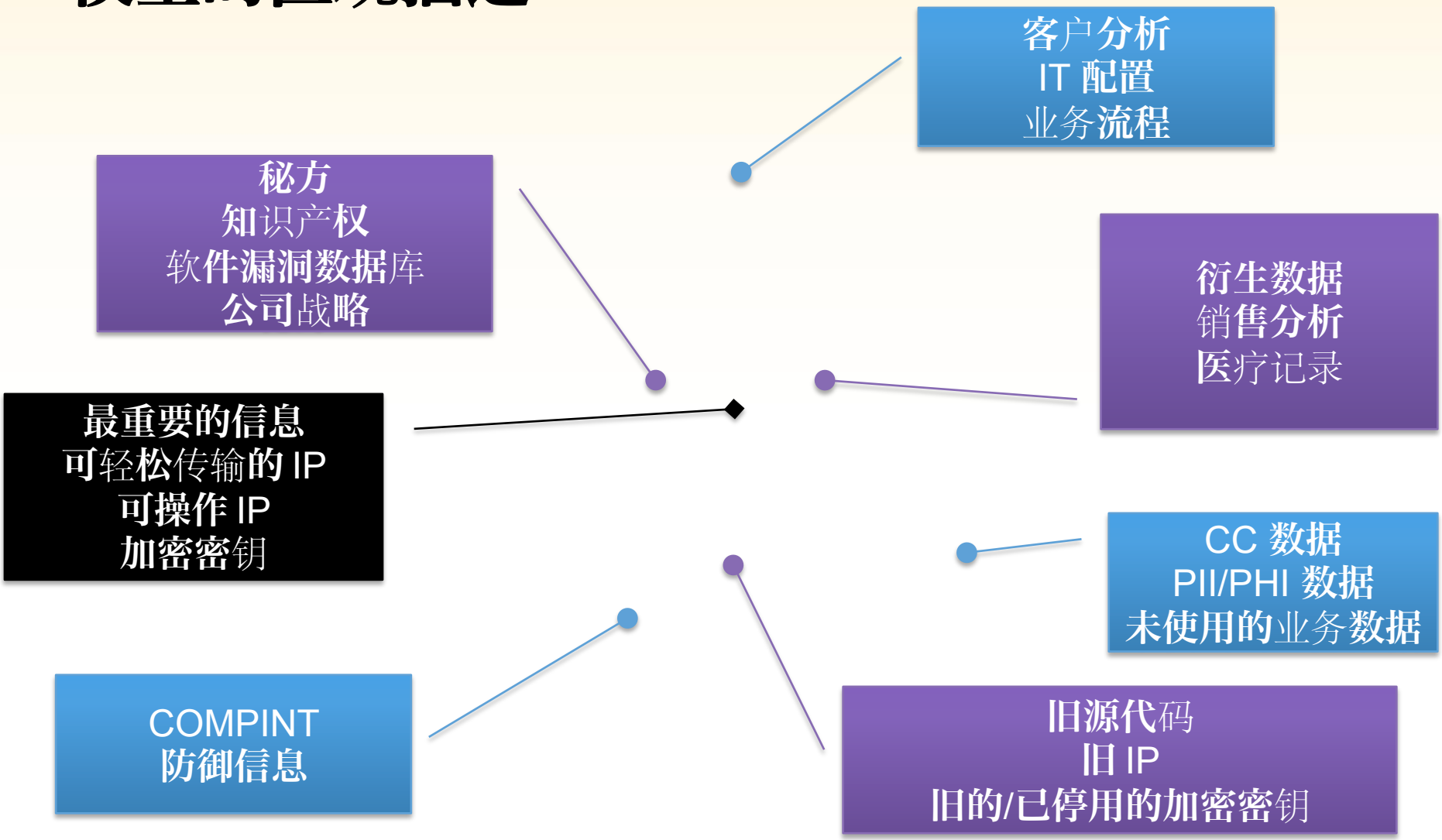
模型需要非常简单

- 无行业术语
- 无需字典
- 无大量页面

并且灵活

- 必须能够随着价值的变化而调整
- 必须依赖准确的输入
  - 角色数
  - 数据盗窃的预期回报
  - 外围环境防御的强度
  - 使用该数据的业务流程数
  - 数据激增量
  - 考虑回报变化时的数据量
- 必须能够影响安全状况

模型的直观描述


客户分析
IT 配置
业务流程
秘方
知识产权
软件漏洞数据库
公司战略
衍生数据
销售分析
医疗记录
最重要的信息
可轻松传输的 IP
可操作 IP
加密密钥
CC 数据
PII/PHI 数据
未使用的业务数据
COMPINT
防御信息
旧源代码
旧 IP
旧的/已停用的加密密钥

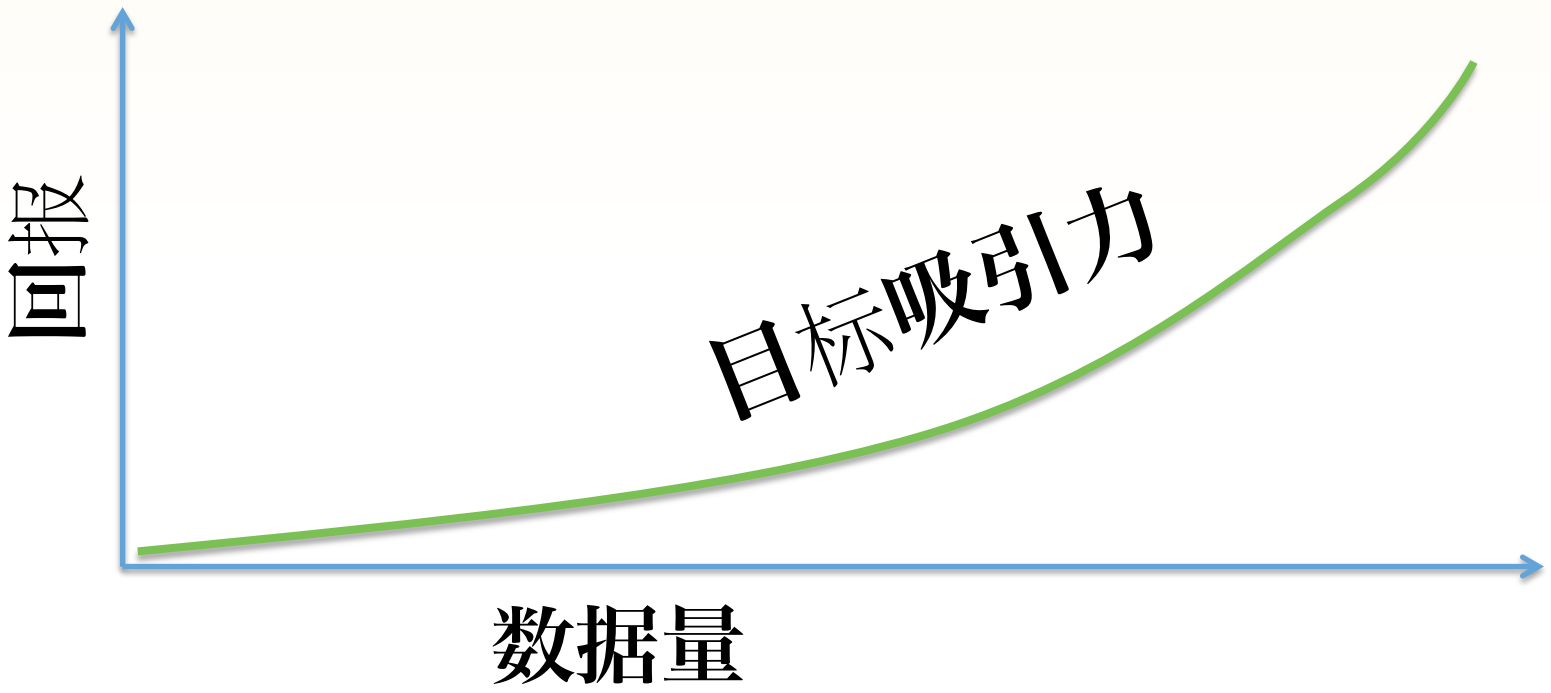
模型

对您有价值	对竞争对手有价值	丢失时有价值	示例	违规可能性	业务影响	操作
1	50	2.3B*	潜在角色数			
Y	N	N	客户分析 IT 配置 业务流程	低	A/I	受保护，但未进行保险存储
Y	Y	N	知识产权 秘方 软件漏洞数据库 公司战略	中	C–延迟风险 A/I 即时	保护（保险存储）
N	Y	Y？	旧源代码 旧 IP（从中派生新 IP） 旧的加密密钥	中	C/I	C：销毁 I：安全归档

模型（第 2 部分）

对您有价值	对竞争对手有价值	丢失时有价值	示例	违规可能性	业务影响	操作
1	50	2.3B*	潜在角色数			
N	N	Y	信用卡号码 PII/PHI 未使用的业务数据	高（角色数）	C	外包 销毁 模糊处理
Y	N	Y	安全 数据分析（收入） 医疗记录 高手客户 专用算法 财务数字	低（高影响）	C	保护 IP（保险存储） 安全的数据
Y	Y	Y	最重要的信息 可轻松传输的 IP	高		保护（保险存储）

大量数据的相关性



抗击数据增长的风险

- 减少数据存储
  - 截断
  - 降低价值的选项（令牌）
  - 销毁
- 减小有效大小
  - 100 万条记录 / 10 个密钥 = 10 万条记录！
  - 多个算法

如何应用模型

- 查看您的企业控制的数据种类
  - 尝试定义它是什么，然后将其与模型关联
  - 务必找到未使用的信息
  - 了解数据的流动和增长
- 在允许的位置添加值
  - 评估信息价值是个人行为
  - 使用您自己的数据
  - 不要依赖外部源来定义数据价值
- 记住置信度因数！
- 根据模型执行操作！

联系信息：

- Branden R. Williams
  - Branden.williams@rsa.com
- Jason Rader
  - Jason.rader@rsa.com

谢谢大家！

RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012