# 企业数据安全理念

蒋鲁宁

2018-01-12

技高一筹 HIGH-TECH FOR TECH HIGH

以人工智能 护数据资产

# 概述

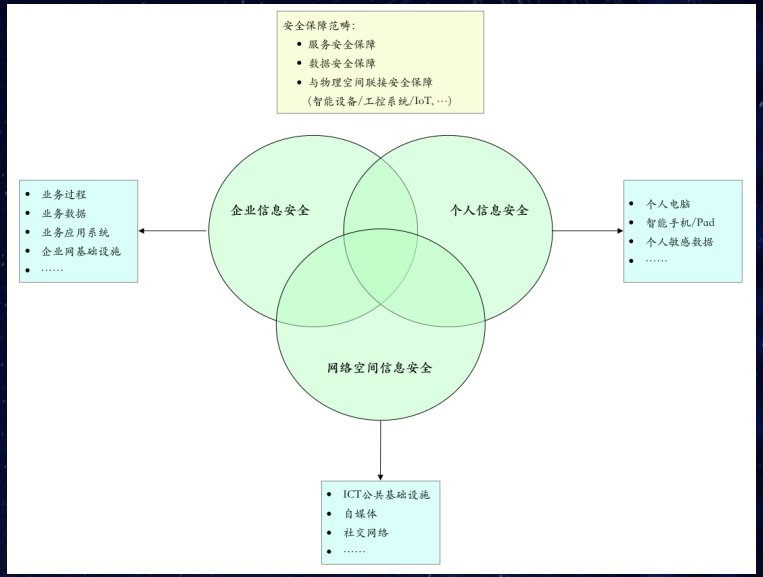
- 过去十多年作为企业网安全架构师，参与了许多数据安全体系的设计，这些项目涉及的：
  - 企业规模从几百人到几十万人
  - 项目规模从几十万到几千万人民币
  - 业务性质从传统行业到IT行业和互联网行业
- 比较过去这些年的项目，企业数据安全没有发生变化的仅有两点：
  1. “势态持续变化”的规律没有变，例如：
     - 企业数据在变：规模、种类、产生率、重要性、…
     - 企业ICT技术在变：云计算、大数据、BYOD、开源软件、 …
     - 企业面临的威胁在变：靶向攻击、内部威胁、勒索病毒、…
  2. “业务驱动的安全”的原则没有变，例如：
     - 企业的价值链决定了安全体系架构
     - 业务的重要程度决定投资和优先级
     - 对业务发展的作用决定了安全的绩效
- 基于上述项目的经历，分享一些企业数据安全理念，这些理念运用企业数据安全管理上，不无裨益。

# 变化对企业数据安全的影响

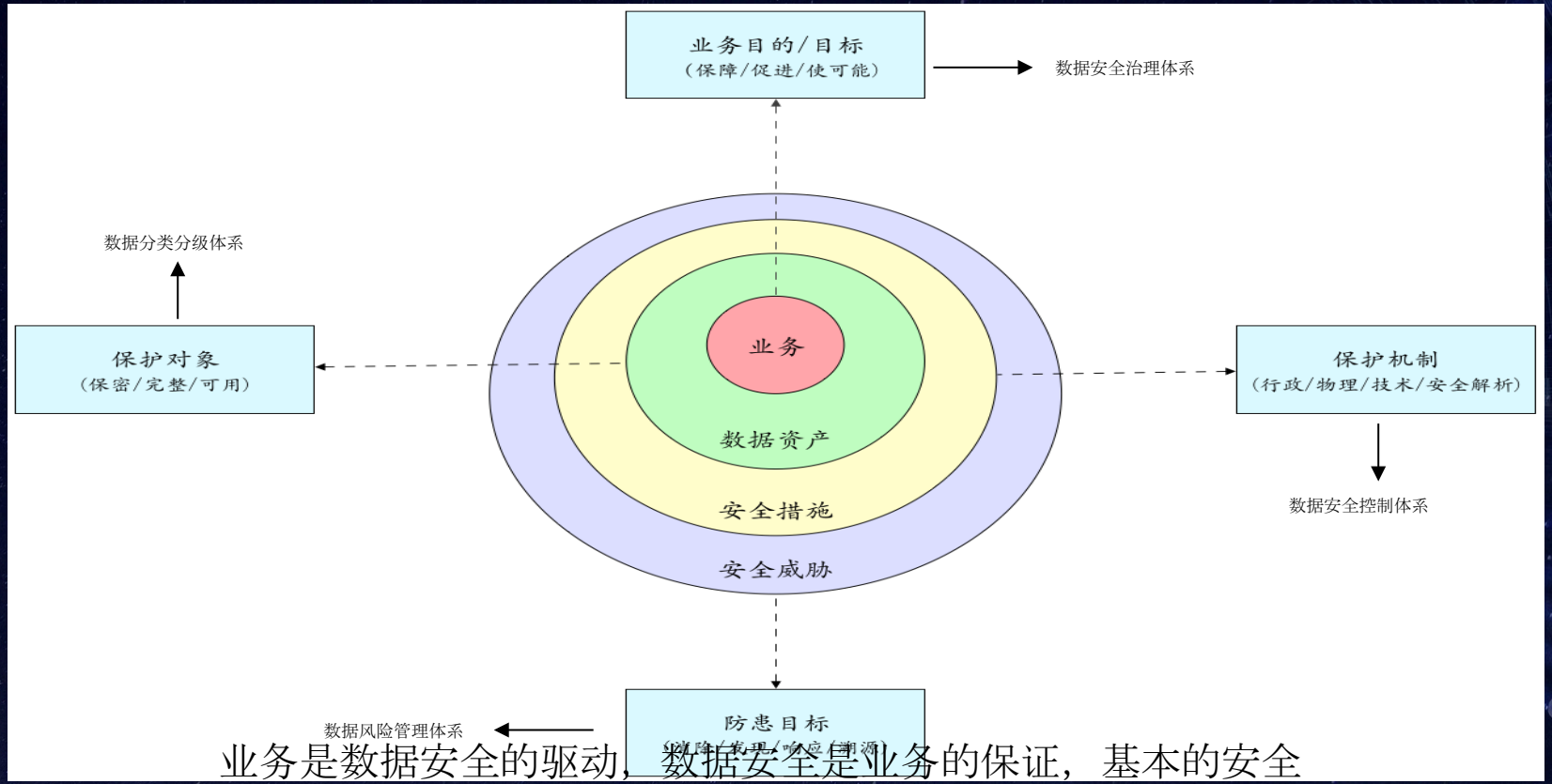
- 早期业界DLP的基于内容感知和统一策略的数据外发审计，通过对数据内容的审计来确定是否违规。随后DLP产品也纳入到安全控制产品，用于检测数据盗取的外发。
- 近些年来，企业信息安全态势发生了极大变化，例如相关于DLP而言：
  - D：从数据(Data)变化到数据资产(Data Asset)，这意味着：
    - 业务价值和财务价值
    - 应最大程度共享
    - 过去的安全控制不适用
  - L：从数据的泄漏(Leak)到数据的损失(Loss)
    - 边界的外泄越来越难审计
    - 数据资产成为恶意分子的主要觊觎对象
    - 内部威胁(包括内部恶意员工和侵入到内部的恶意分子)更能造成数据损失。
  - P: 从预防(Prevention)到保护(Protection)
    - 技术上完全的预防已不可能
    - 即使可能也很难承担高昂的成本
    - 更多的投入侧重到治理和监测
- 基于数据科学的安全解析(如BDSA)，逐渐发展为安全技术的核心，如NTA、UEBA和EDR等。这些新型的安全控制既能够发现已知威胁，也能够发现未知威胁。

# 业务驱动：企业与数据安全

- 企业(Enterprise)
  - 狭义的“企业”含义是从事商业活动的组织，包括制造、开采、建设、运输、销售和服务等。
  - 广义的“企业”是受一个统一治理体系管控，具有明确管辖边界的组织（例如政府机构、军队和商业组织），特别是对企业内的信息有自主的管辖权。
- 企业网数据安全
  - 企业网：一个组织安全策略可管辖范围的计算机网络资源，包括网络设备和入网设备/系统以及网络中的各种形态的数据。
  - 企业网安全：包括对企业网基础设施安全应用系统、数据和相关业务流程的安全保障、如对企业网资源的访问控制、与互联网网连接的边界控制等。
  - 企业信息安全：包括防止企业敏感信息外泄、数据完整性的维系和数据可用性的保证，覆盖了企业所有信息。
  - 企业网数据安全：覆盖全部企业网的信息安全，是企业信息安全的组成部分。
  - 企业网数据资产安全：以数据为中心的(Data-Centric)，提供企业业务最大程度共享下的企业数据安全。

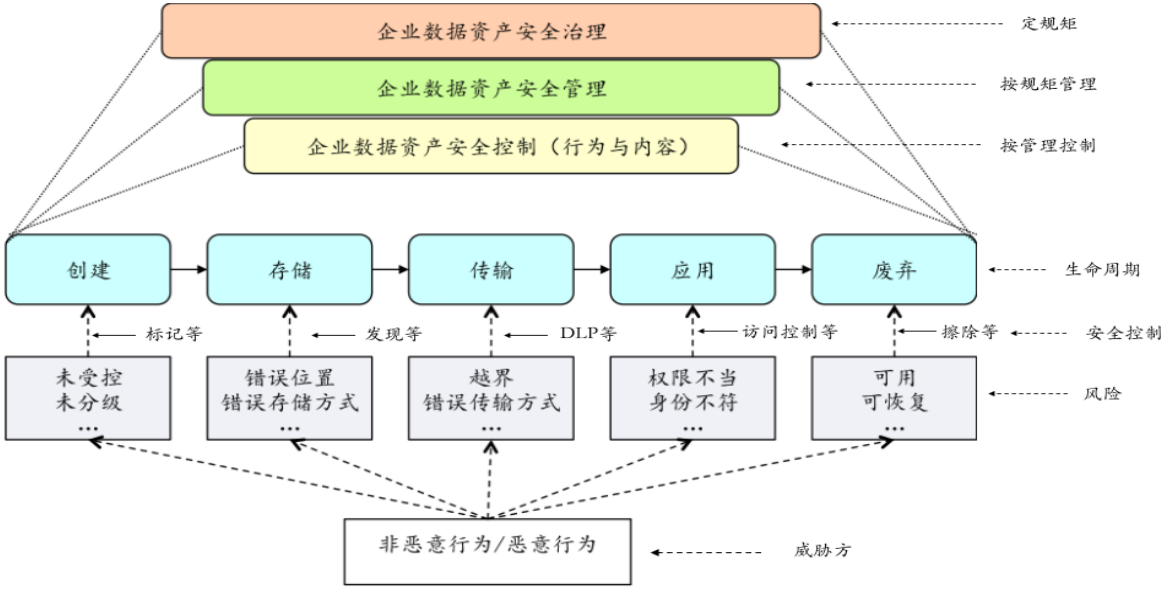


# 业务驱动：企业数据安全逻辑




业务是数据安全的驱动，数据安全是业务的保证，基本的安全逻辑没有变化，但业务目的/目标、保护对象、保护机制和防患目标随

# 业务驱动：企业数据安全框架




企业数据安全框架的实施难度取决于数据生命周期的复杂程度，例如跨越多个业务域、多种数据类别和多种计算环境要比简单业务、单一结构数据和数据仅在存储在本地具有更多的挑战。

# 小结

- 随着ICT技术的发展，数据将逐渐成为企业的核心资产之一，企业数据的安全也将意味着企业的安全。
- 在过去多年的项目实践中认识到，随着企业数据变得日益重要，受到的安全威胁也与日俱增。
- 业务驱动的安全业界很早就倡导的安全最佳实践，但由于业务域的多样性，与安全域重叠有限，因此往往由安全人员负责设计安全体系面临着极大挑战。
- 新理念、新方法、新技术能够提升企业数据安全的有效性，但最终的有效性必须是相对业务而言的。

# Thanks.