数字化安全

安全技术解析及隐私保护治理

主讲老师：李福东

【课程背景】

数字化时代，以物联网、大数据、人工智能为核心的新一代信息技术，在推动社会化生产力提升和组织变革的同时，引发了越来越严重的安全问题。

2022 年 2 月，某科技公司、王某某等人因窃取 2.1 亿条简历数据，涉嫌侵犯公民个人信息罪，被告单位被判处罚金人民币 4000 万元，王某某被判处有期徒刑 7 年、罚金人民币 1000 万元；

3 月份，BlackMoon 僵尸网络在国内已感染数百万终端；4 月初，国内某上市公司邮箱遭入侵，被骗 2000 余万元；5 月初，俄罗斯胜利日期间，黑客攻击俄在线电视显示反战信息。

上述安全事件频发，对信息安全管理提出了越来越大的挑战，为了有效地支持数字经济的平稳健康与快速发展，非常有必要掌握信息安全相关知识，构建数字化安全管理能力。

然而，数字化安全管理与治理决不能“头疼医头，脚疼医脚”，“按下葫芦起了瓢”，需要全面、系统地进行谋划、规划、设计，实现“规划、建设、运维、运营、评价、改进”的一体化管理。

为此，本课程首先学习数字化安全管控体系的构建方法，横向维度采用分阶段方式构建安全管理体系，纵向维度采用分层方式构建安全管理体系，以便最大限度地消除安全隐患，防患于未然。

接着，本课程从产品安全、网络安全、数据安全、隐私安全的视角，对数字化安全管理进行全面而深入的解析，最终掌握数字化安全管理、安全治理、隐私保护等方面的方法与技术，并通过政府、金融、能源、教育、电信、医疗、交通、互联网等行业的企业安全治理案例，让学员掌握从方案设计、安全运营、隐私与合规治理等全流程的方法与技术。

【课程收益】

- 深刻理解信息安全的价值作用和本质内涵；
- 系统化掌握安全技术体系构建方法；
- 掌握产品安全及各层次安全管理方法；
- 掌握数据安全治理与管理的方法；
- 掌握隐私安全与防护的方法。

【课程特色】生活化、场景化；启发式教学、激发创新灵感

【课程对象】安全方案架构师、产品经理、运维人员、法务与合规治理人员、中高层

【课程时间】1 天（6 小时/天）

【课程大纲】

一、 夯实基础——信息安全入门

1、信息安全的价值和作用

- 全球典型安全事件一览
- 无法回避的信息安全问题

2、信息安全的本质和内涵

- 信息安全的定义
- 信息安全的分类
- 信息安全 CIA 三要素

3、从三层架构看信息安全

- 从系统架构到信息安全
- 三层架构模型解析

案例：某社交巨头、某银行

二、寻踪觅迹——产品安全管理

1、用户认证安全

- 口令保护方法
- 生物特征数据保护方法
- 后台之间身份认证方法

2、授权与访问控制

- 授权的原则和方式
- 典型的授权风险
- 授权与 AC 的关系

3、安全审计

- 审计的目的和内容
- 操作日志的管理

4、资产保护与业务安全

- 资产保护的类型与方法
- 业务逻辑漏洞的避免

案例：某银行、某互联网企业

三、未雨绸缪——构建安全技术体系

1、信息安全技术体系架构

- 横向 5A 分段管理
- 纵向 4L 分层管理

2、网络与通信层安全

- 通信网络安全威胁

- 主要网络攻击技术
- 网络安全防护技术

3、设备和主机层安全

- 安全架构 5A 在 3L 的关注点
- 搭建自动化运维平台

4、应用和数据层安全

- 安全架构 5A 在 4L 的关注点
- 数据库实例安全访问原则
- 客户端数据安全

案例：某政府部门、某电信运营商

四、绝对控制——数据安全治理

1、数据安全治理与管理

- 治理与管理的区别和联系
- 数据安全治理三要素
- 数据安全管理政策体系

2、数据安全管理三大职能

- 安全项目管理
- 安全运营管理
- 合规与风险管理

3、数据安全风险成熟度分析

- 风险识别或评估
- 风险度量或成熟度分析
- 风险处置与收敛跟踪
- 风险运营工具和技术

案例： 某互联网公司、某电信运营商

五、以人为本——隐私保护与合规遵从

1、隐私保护合规治理知识基础

- 隐私保护与数据安全
- 数据控制与数据处理
- 法律法规与政策文件修订

2、通用数据保护条例 GDPR（欧盟）

- 个人数据处理六项原则
- 个人数据处理法律依据（6 个）
- 隐私治理基本原则（10 项）

3、个人信息安全规范（中国）

- 个人信息和个人敏感信息
- 个人信息安全基本原则（6 个）
- 个人信息生命周期管理（5 段）
- 个人信息保护核心原则（6 项）

4、GRC 与隐私保护治理

- GRC 三要素解析
- 隐私保护治理方法与流程
- 隐私保护能力成熟度评估

案例：某金融企业、某工业企业