第二章 人员安全和风险管理概念

2.1 促进人员安全策略

- 职责分离: 把关键的、重要的和敏感工作任务分配给若干不同的管理员或高级执行者，防止共谋
- 工作职责:最小特权原则
- 岗位轮换:提供知识冗余，减少伪造、数据更改、偷窃、阴谋破坏和信息滥用的风险，还提供同级审计，防止共谋

2.1.1 筛选候选人

筛选方法:

1. 背景调查
2. 社交网络账户复审

2.1.2雇佣协议和策略

- 雇佣协议
- 保密协议

2.1.3 解雇员工的流程

2.1.4 供应商、顾问和承包商控制

SLA:服务级别协议

2.1.5 合规性

合规是符合或遵守规则、策略、法规、标准或要求的行为

2.1.6 隐私

2.2安全治理

- 安全治理是支持、定义和指导组织安全工作相关的实践合集
- 第三方治理: 由法律、法规、行业标准、合同义务或许可要求规定的监督

2.3理解和应用风险管理概念

2.3.1风险术语

- 资产: 环境中应该加以保护的任何事物
- 资产估值: 根据实际的成本和非货币性支出作为资产分配的货币价值
- 威胁:任何可能发生的、为组织或某些特定资产带来所不希望的或不想要结果的事情
- 脆弱性:资产中的弱点或防护措施/对策的缺乏被称为脆弱性
- 暴露:由于威胁而容易造成资产损失，暴露并不意味实施的威胁实际发生，仅仅是指如果存在脆弱性并且威胁可以利用脆弱性
- 风险:某种威胁利用脆弱性并导致资产损害的可能性 风险 =威胁 * 脆弱性，安全的整体目标是消除脆弱性和延长威胁主体和威胁时间危机资金安全，从而避免风险称成为现实
- 防护措施： 消除脆弱性或对付一种或多种特定威胁的任何方法
- 攻击: 发生安全机制被威胁主体绕过或阻扰的事情
- 总结：风险概念之间的关系

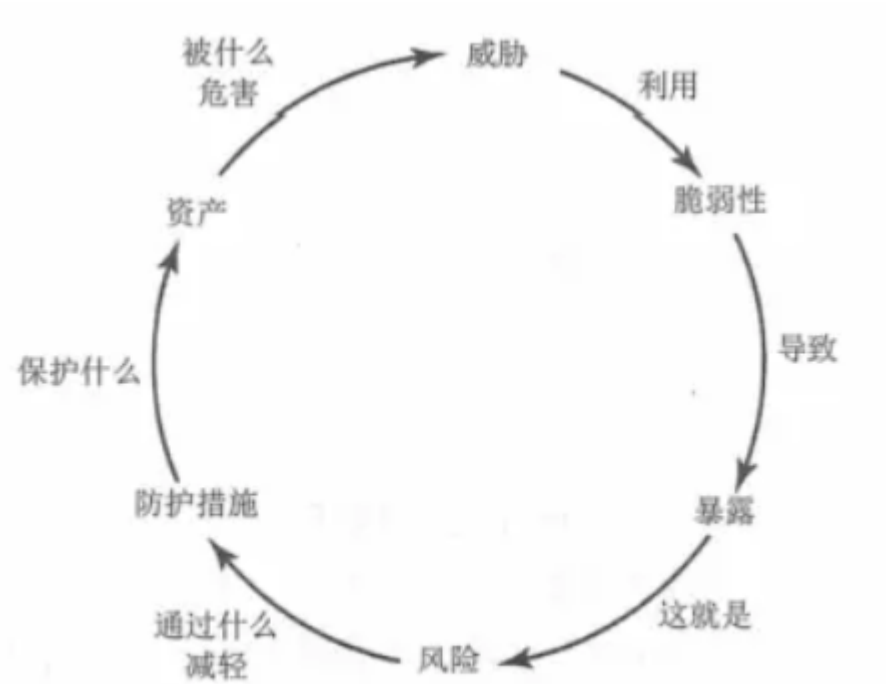

图 2.4　风险的元素

2.3.2 识别威胁和脆弱性

IT的威胁不仅限于IT源

2.3.3 风险评估/分析

定量的风险分析

1. 暴露因子(EF)： 特定资产被已实施的风险损坏所造成损失的百分比

2. 单一损失期望(SLE):特定资产的单个已实施风险相关联的成本 SLE = 资产价值(AV) * 暴露因子(EF)
3. 年发生占比（ARO）:特定威胁或风险在一年内将会发生的预计频率
4. 年度损失期望（ALE）:对某种特定资产，所有已实施的威胁每年可能造成的损失成本 ALE = SLE * ARO
5. 计算使用防护措施时的年损失期望
6. 计算防护措施成本（ALE1-ALE2）- ACS
    - ALE1:对某个资产与威胁组合不采取对策的ALE
    - ALE2：针对某个资产与威胁组合采取对策的ALE
    - ACS：防护措施的年度成本

定性的风险分析

- 场景，对单个主要威胁的书面描述
- Delphi技术:简单的匿名反馈和响应过程

2.3.4 风险分配/接受

- 风险消减：消除脆弱性或组织威胁的防护措施的实施
- 风险转让：把风险带来的损失转嫁给另一个实体或组织
- 风险接受：统一接受风险发生所造成的结果和损失
- 风险拒绝：否认风险存在以及希望风险永远不会发生
- 总风险计算公式：威胁 * 脆弱 * 资产价值 = 总风险
- 剩余风险计算公式：总风险 - 控制间隙 = 剩余风险

2.3.5 对策的选择和评估

风险管理范围内选择对策主要依赖成本/效益分析

2.3.6 实施

- 技术性控制：采用技术控制风险
- 技术控制示例：认证、加密、受限端口、访问控制列表、协议、防火墙、路由器、入侵检测系统、阀值系统
- 行政管理性控制：依照组织的安全管理策略和其他安全规范或需求而定义的策略与过程
- 物理性控制：部署物理屏障，物理性访问控制可以防止对系统或设施某部分的直接访问

2.3.7 控制类型

- 威慑：为了阻吓违反安全策略的情况

- 预防：阻止不受欢迎的未授权活动的发生
- 检测：发现不受欢迎的或未授权的活动
- 补偿：向其他现有的访问控制提供各种选项
- 纠正：发现不受欢迎或未授权的操作后，将系统还原至正常的状态
- 恢复：比纠错性访问控制更高级，如备份还原、系统镜像、集群
- 指令：指示、限制或控制主体的活动，从而强制或鼓励主体遵从安全策略

2.3.8 监控和测量

- 安全控制提空的益处应该是可以测量和度量的

2.3.9 资产评估

2.3.10 持续改进

- 安全性总在不断变化

2.3.11 风险框架

- 分类 对信息系统和基于影响分析做过处理、存储和传输的信息信息进行分类
- 选择 基于安全分类选择初始化基线、安全基线
- 实施 实施安全控制并描述如何在信息系统和操作环境中部署操作
- 评估 使用恰当的评估步骤评估安全系统
- 授权
- 监控 不间断的监控信息系统的安全控制

2.4 建立和管理信息安全教育、培训和意识

- 培养安全意识的目标是将安全放在首位并且让用户意识到这点

2.5 管理安全功能

- 安全必须符合成本效益原则
- 安全必须可度量