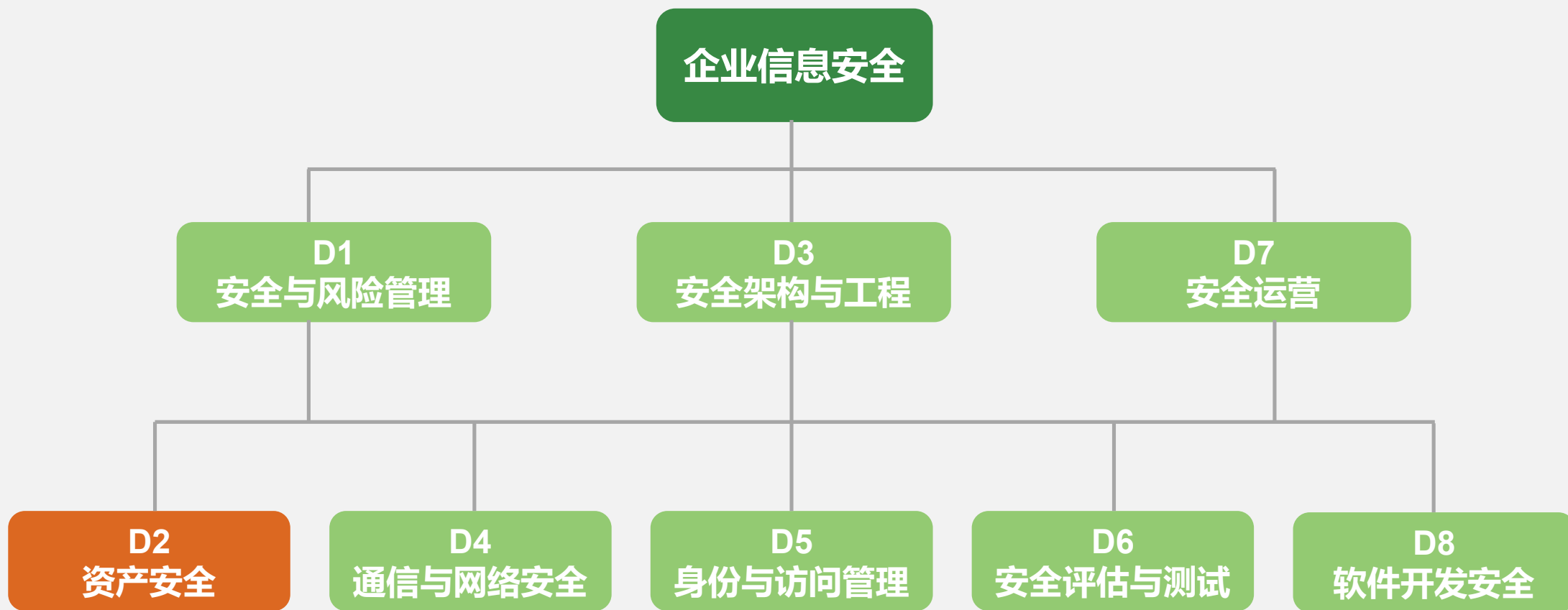


铭学在线课堂-CISSP认证

D2-资产安全

知识架构



CBK学习目标

- 熟悉和掌握信息和资产分类的概念和方法
- 熟悉涉及信息、系统、业务过程中的数据所有权和责任相关问题
- 掌握如何保护隐私的概念和方法
- 掌握如何选择和实施恰当的数据安全控制措施
- 理解数据的处理要求



本章知识架构



| 本节内容

1.1 信息资产安全基本概念

- A、数据相关概念
- B、信息资产生命周期及安全

数据治理

- 数据治理的概念包括内部或外部正确、持续处理数据的人员、流程和IT组织
- 数据治理委员会负责监督数据策略，并概述了不同职能利益相关方的角色和职责
- 组织应使用一些指导原则来建立其数据治理模型，这些原则包括：
 - ✓ 建立责任
 - ✓ 为组织提供最佳支持的计划
 - ✓ 有效获取
 - ✓ 必要时确保性能
 - ✓ 确保符合规则
 - ✓ 确保尊重人为因素

数据策略

- 数据管理必须遵循一套广泛适用于组织的原则和程序
- 完善的数据策略可以指导组织仅仅收集所需的信息、确保这些信息安全，并且在不需要的时候安全的销毁它们。
- 完善的数据策略可指导组织在如何解决影响数据安全时，如何实践
- 定义明确的数据策略可以为管理层在制定数据质量、格式、访问和保留有关实践和标准时提供指导

数据质量

- 质量保证（QA）和 质量控制（QC）
 - ✓ QA解决了问题：“数据是否符合目的？”
 - ✓ QC解决了以下问题：“数据可以使用吗？”
- 良好的数据质量实践需要减少的常规错误类型：
 - ✓ 记账错误
 - ✓ 遗漏错误

数据文档化

- 数据文档的组成部分一般包括：数据怎么样创建、数据的结构和内容、以及对数据所执行的任何操作
- 数据文档的目标如下：
 - ✓ 数据寿命和重用
 - ✓ 数据用户应该了解数据的内容、上下文和限制
 - ✓ 更容易在组织内发现数据
 - ✓ 数据互操作性和数据交换

数据模式

- 数据模式指的是：如何定义数据架构的蓝图
- 这是一个很大的概念，仅限在资产安全方面，数据模式是数据组织的元素
- 例如：有关安全控制（例如加密、访问和授权级别以及处置计划）的决定将由数据模式告知

信息生命周期

- 在宏观层面上，我们可以将信息分为四个阶段：



获取

首先

- 组织只会通过从其他地方复制或者从头开始创建，这两种方式中的一种来获取信息

最后

- 我们必须应用一些策略性的控制。

然后

- 在获取信息之后，和在它可以使用之前，我们有必要采取的一些步骤使之有价值。

使用

- 从安全角度来看，在信息生命周期中的这一阶段，确保其机密性、完整性和可用性是最大的挑战。

机密性：

- 它将被具有必要访问级别的各种用户所读取

可用性

- 你要保持信息的可用性，而且只有正确的人以被授权的方式才能修改它

完整性：

- 由于信息被使用，我们必须确保其内部一致性
- 一致性也是一个策略和法规遵从性的问题

存档

- 不再被经常使用的事实可能意味着如果我们不予以适当的控制，未授权或意外的对其访问和更改就可能会在很长的一段时间都不被发现
- 在决定哪些备份需要被保护以及如何进行时，参考我们的风险评估是很重要的
- 保留数据多长时间的问题



处置

- 每个组织都迟早不得不面临数据处置的问题。这通常是，但不总是，意味着数据的销毁
- 数据是否真正的被销毁
- 数据是否被正确的销毁



| 本节内容

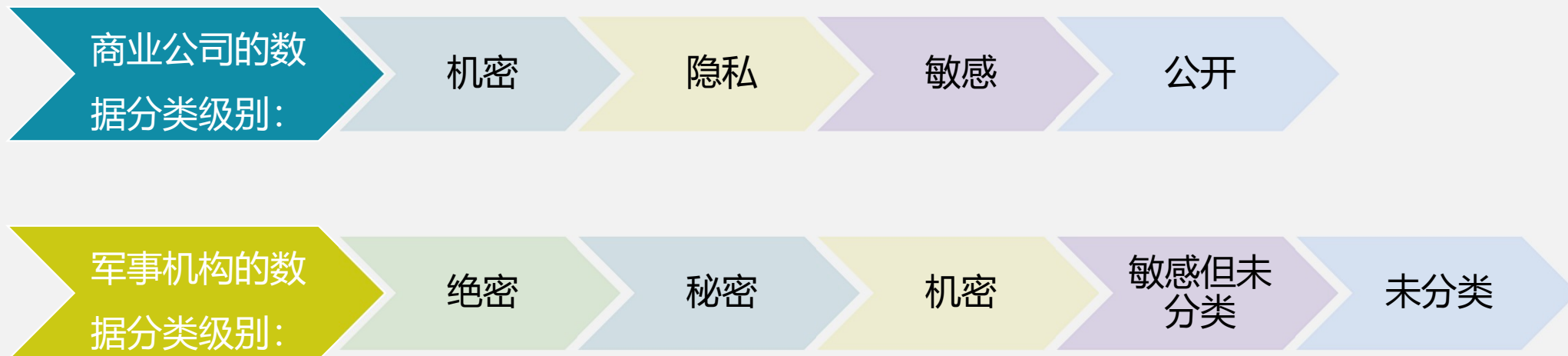
1.2 信息分类分级

- A、信息分类分级概述
- B、信息分类分级的级别
- C、信息分类分级的原则和控制
- D、信息分类分级计划步骤

信息分类分级概述

- 信息分类的目的都是为了**量化一个组织**如果丢失了信息后可能承受多少**的损失**；
- 信息的**关键性**，源自信息一旦**丢失后**给组织**基本业务流程**带来的影响；
- 一旦根据敏感程度对**信息分类**，公司就能够决定保护各种信息所需要的**安全控制**；
- 数据分类有助于保证以成本**最为低廉的方式**保护数据；
- 每种分类都应当**具有单独的处理要求和措施**，以便说明如何访问、使用和销毁数据。

信息分类分级的级别



不要走极端而提出大量的分类方法

每种分类都应唯一且区别于其他分类，同时不能有任何重叠

信息分类分级的原则和控制

组织机构可能用于决定信息
敏感度的一些准则参数：

数据的用途

数据的价值

数据的寿命

数据泄漏可能导致的损失级别

数据被修改或出现讹误可能导致的损失级别

保护数据的法律、法规或合约责任

数据对安全的影响

谁能够访问这些数据


由谁维护这些数据

谁能够重造这些数据

如果数据不可用或出现讹误，那么造成的机会损失有多少

信息分类分级计划步骤

- 正确分类计划的必要步骤：



定义分类级别。

指定确定如何分类数据的准则。

任命负责为数据分类的数据所有者。

任命负责维护数据及其安全级别的数据看管员。

制订每种分类级别所需的安全控制或保护机制。

记录上述分类问题的例外情况。

说明可用于将信息保管转交给其他数据所有者的方法。

建立一个定期审查信息分类和所有权的措施。向数据看管员通报任何变更。

指明信息解密措施。

将这些问题综合为安全意识计划，让所有员工都了解如何处理不同分类级别的数据。

| 本节内容

1.3 信息资产安全相关的角色和责任

- A、高级管理层
- B、数据所有者、数据监管者、系统所有者、数据管理员
- C、安全管理员、审计员
- D、其他人员：主管、变更分析员、数据分析员、用户

高级管理层

- 高级管理层（Executive Management）持续对组织负有**最终责任**
 - ✓ 制定**长远规划、业务目标和目的**
 - ✓ 确保组织在信息安全方面采取适当的**应尽注意和应尽责任**



数据所有者、数据监管者、系统所有者、数据管理员

- 数据所有者(Data Owner)通常是一名管理人员，他负责管理某个业务部门，**对特定信息子集的保护和应用负最终责任**
- 数据监管者(Data Custodian)负责数据的保护与维护工作。这个角色通常由IT或安全部门员工担任
- 系统所有者 (System Owner) 负责一个或多个系统，每个系统可能保存并处理由不同数据所有者拥有的数据。这个角色必须确保系统的脆弱性得到正确评估，并且向应急响应团队和数据所有者报告所有的系统脆弱性。
- 数据管理员 (Data Administrator) 根据 “最小特权” 原则和 “知其所需” 原则分配权限，仅授予用户工作所需的权限

安全管理员、审计员

- 安全管理员（Security Administrator）负责实施和维护企业内具体的安全网络设备和软件；安全管理员必须确保为用户授予的访问权限支持公司策略和数据所有者的指示。
- 审计员（Supervisor）的目标是确保组织机构遵循了自己制定的策略和适用的法律法规。组织可以拥有内部审计员和/或外部审计员。外部审计员往往代表法律机构，确保组织符合法规要求。



其他人员：主管、变更分析员、数据分析员、用户

- 主管（Supervisor）这一角色，也称为用户管理者，其最终负责所有用户活动和由这些用户所创建和拥有的任何资产
- 变更控制分析员（Change Control Analyst）负责批准或否决变更网络、系统或软件的请求。这个角色必须确保变更不会引入任何脆弱性，并保证对变更进行适当测试，使其得以顺利实施
- 数据分析员（Data Analyst）负责保证以最佳方式存储数据，从而为需要访问和应用数据的公司与个人提供最大的便利
- 用户（User）有义务遵守操作安全措施，从而保证数据对其他人的机密性、完整性和可用性



本章知识架构



| 本节内容

2.1 适当的数据保留

- A、数据保留策略
- B、电子发现协议 (e-Discovery)

制定保留策略

- 每个数据保留策略的核心是解决三个基本问题：

我们保存什么数据？

我们保存这些数据
多长时间？

我们在哪里保存
这些数据？

我们如何保留

为了使保留的数据有用，它必须能被及时访问到的，我们需要考虑以下方法：

分类法

分级

标准化

索引

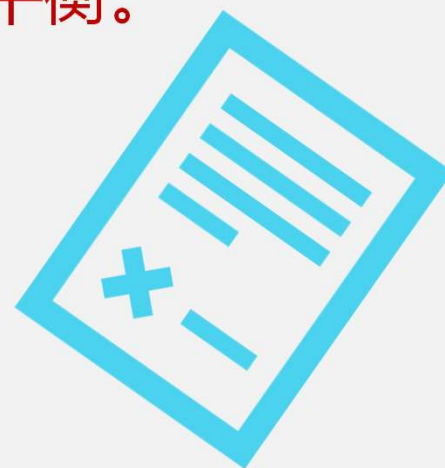
我们保留多长时间

- 当前有大量法定的和监管的保留时长要求，以下是一些一般性准则：

数据类型	一般保留期限
业务文档（如会议记录）	7年
发票	5年
应付与应收账款	7年
人力资源文件	7年（离职员工）或3年（未雇佣的候选人）
法律通信	永久

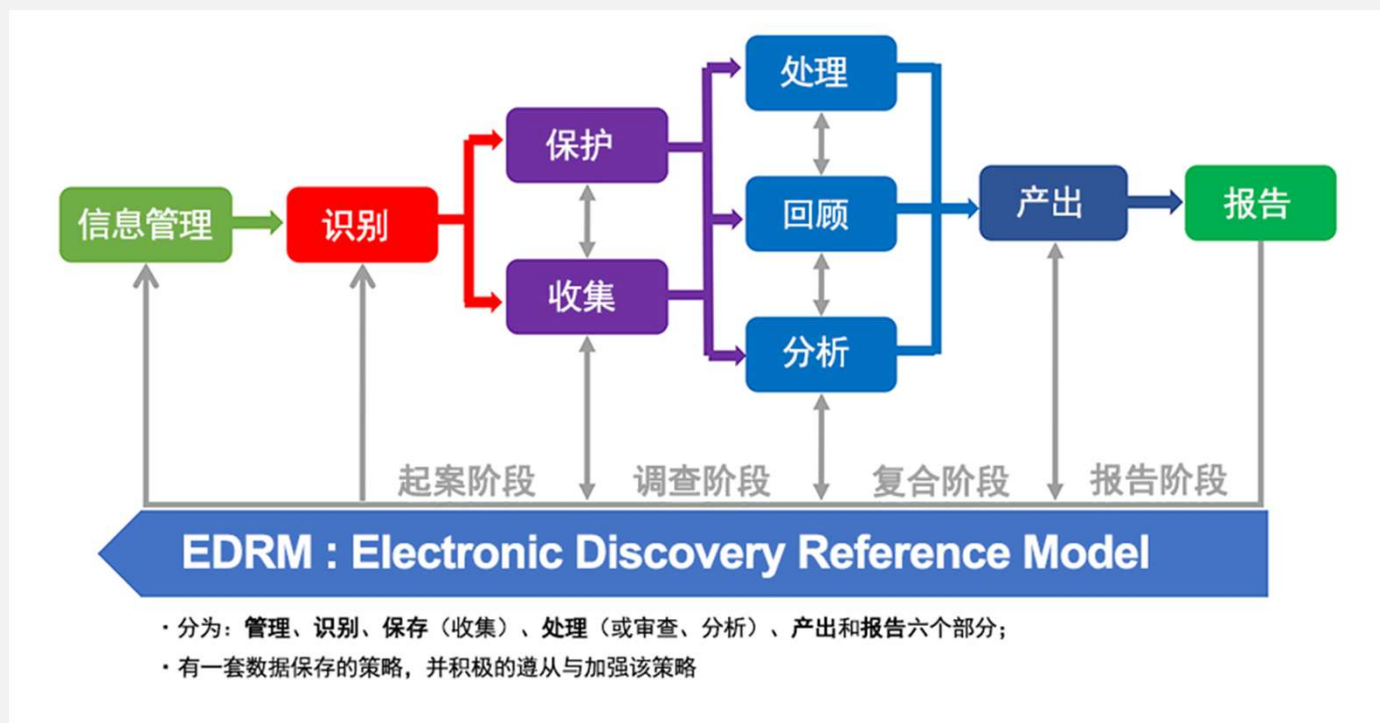
我们保留数据需要注意什么

- 除了前面列出的类别，还有许多其他记录是我们想保留的；
- 同样，**法律顾问必须参与这一进程**，以确保所有法律义务能得到满足；
- 保留数据的决定必须是**谨慎、具体和可执行的**；
- 最大的挑战之一：**业务需求与员工或客户隐私之间的平衡。**



电子发现

- 电子存储信息的发现（ESI）或称电子发现是**被法院或外部律师所制定的**，与法律程序有关的所有ESI的过程。



电子发现参考模型（EDRM）

| 本节内容

2.2 保护隐私数据

- A、隐私数据所有者和处理者
- B、隐私数据收集
- C、隐私数据的处置

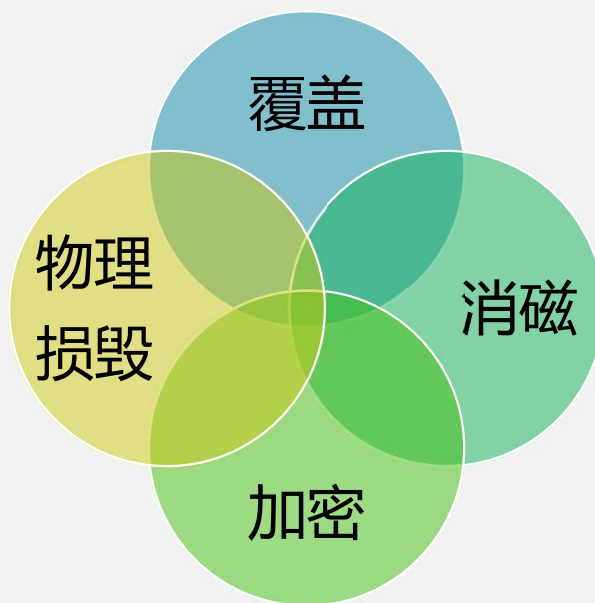
隐私数据的所有者和处理者们

- 所有者的一个责任就是数据分类和批准披露的请求
- 所有者间接或直接决定谁可以访问特定的数据
- 数据处理者通常由保护（或危及）数据隐私的用户组成
- 对于处理者在隐私保护方面的关键是培训和审计



数据残留

- 为了应对数据残留，**识别**那些用于确保隐私或敏感数据被正确移除的过程是很重要的。
- 一般来说，**有四种方法可消除数据的残留**：



数据残留

- 相关术语：
 - ✓ 擦除 (Erasing)
 - ✓ 消除 (Clearing)
 - ✓ 清除 (Purging)
 - ✓ 解除分类 (Declassification)
 - ✓ 净化 (Sanitization)
 - ✓ 消磁 (Degaussing)
 - ✓ 销毁 (Destruction)



隐私数据收集

- 你必须了解与你的组织存储或使用其数据的所在地相关的特定隐私法律；
- 组织收集的个人信息类型以及其生命周期的考虑因素也必须是有明确的书面策略；
- 在编写策略时，你需要回答以下问题：
 - ✓ 收集个人的什么数据？（例如姓名，网站访问，电子邮件信息等）？
 - ✓ 为什么我们收集这些数据，以及我们如何使用它们（例如，提供服务，以确保安全）？
 - ✓ 我们与谁共享此数据（例如，第三方提供商，执法机构）？
 - ✓ 谁拥有收集的数据（例如，主体，组织）？
 - ✓ 这些数据的主体（例如，选择退出，限制）有什么权利？
 - ✓ 什么时候销毁这些数据（例如，五年后，从不）？
 - ✓ 有什么具体的法律或法规与这些数据相关？



| 本节内容

2.3 确保恰当的数据安全控制

- A、数据安全控制
- B、介质控制和管理
- C、保护其他资产

数据安全控制

选择使用哪些控制来减少信息风险，不仅取决于分配给该信息的价值，还取决于该信息动态特点。一般来说，数据存在三种状态：

- ✓ 静止的数据
- ✓ 运动中的数据
- ✓ 使用中的数据

介质控制

- 介质和设备**需要各种控制**，以确保不会危及其上的数据的完整性、机密性和可用性；
- 介质和设备包括电子(磁盘、CD/DVD、磁带、诸如USB盘之类的闪存等)和非电子(纸质)的信息形；
- 介质应该被清楚地**标记和做记录**，其完整性应该被验证；
- 当**不再需要时其存储的数据应该被正确地擦除**；
- 对电子介质擦除有**净化、清除和破坏**等方法；
- 其他类型的信息(如纸质文件、缩影胶片和缩微平片)也需要进行安全处理、**“垃圾搜索”** 是指搜索家庭或公司的垃圾箱

介质管理

- 无论是在介质库中或者由其他系统及个人管理，介质管理都应包括以下属性和任务：

追踪(审计日志记录)

有效实现访问控制

追踪(本地或异地)备份
版本的数量和位置

对介质变更的历史记
录归档

确保环境条件不会危
及介质的安全

确保介质的完整性

定期清查介质

执行安全处置活动

标记内部和外部标签

保护其他资产



保护移动设备



保护纸质记录



保护保险箱



| 本节内容

2.4 数据泄露

- A、常见的数据泄漏原因
- B、数据泄漏防护（DLP）

数据泄露的一些原因

转移信息不恰当

残余数据

笔记本电脑或介质丢失、被盗

意识培训不足



数据泄漏防护（DLP）

- 数据泄漏防护（DLP）包括组织为防止未经授权的外部各方访问敏感数据而采取的各种行动。该定义包括：
 - ✓ 数据必须被认为是敏感的
 - ✓ DLP关系到外部各方
 - ✓ 外部访问我们的敏感数据必须是未经授权的
- DLP的真正挑战涉及到我们组织的整体观
- DLP的**不仅仅是一个技术问题**



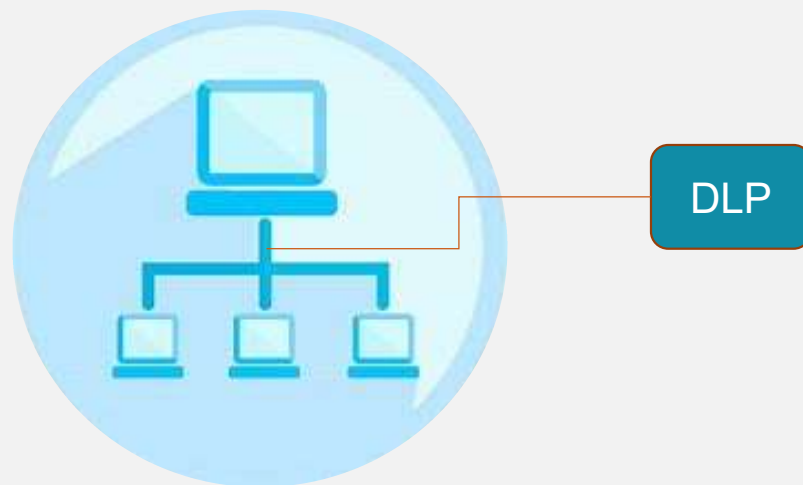
数据泄漏防护（DLP）

- 数据泄漏防护（DLP）关键要素包括：
 - ✓ 数据清单
 - ✓ 数据流
 - ✓ 数据保护策略
 - ✓ 实现，测试和调优



网络DLP

- 网络DLP（NDLP）是对运动中的数据应用数据保护策略
- NDLP产品通常是一些实施部署在组织的网络周边的设备



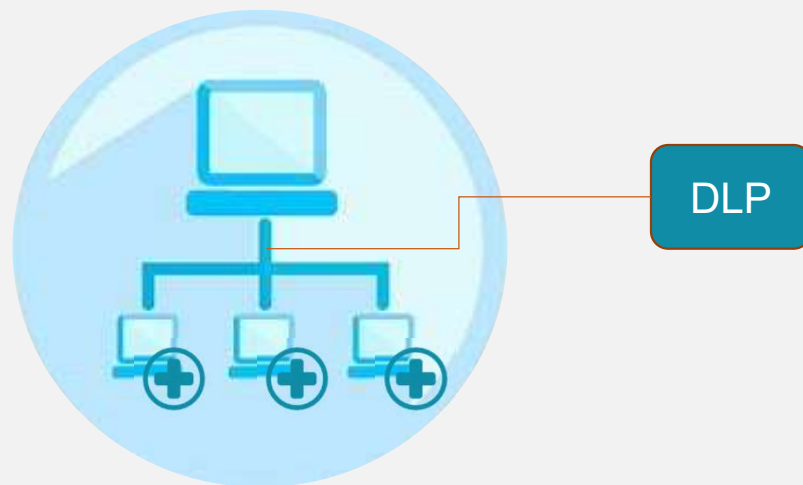
端点DLP

- 端点DLP（EDLP）是对静态的数据和使用中的数据应用保护策略。
- EDLP被部署在每个受保护的端点上以软件形式运行。



混合DLP

- DLP的另一种方法是在整个企业中部署NDLP和EDLP
- 这种方法是最昂贵和最复杂的
- 它提供了最好的安全覆盖



THANK YOU
感谢聆听



✧ | 以科学方法推动IT新职业发展