DAMA-DMBOK

数据管理知识体系指南CDGA/CDGP认证

第7章 数据安全（完整课程视频请扫描二维码）

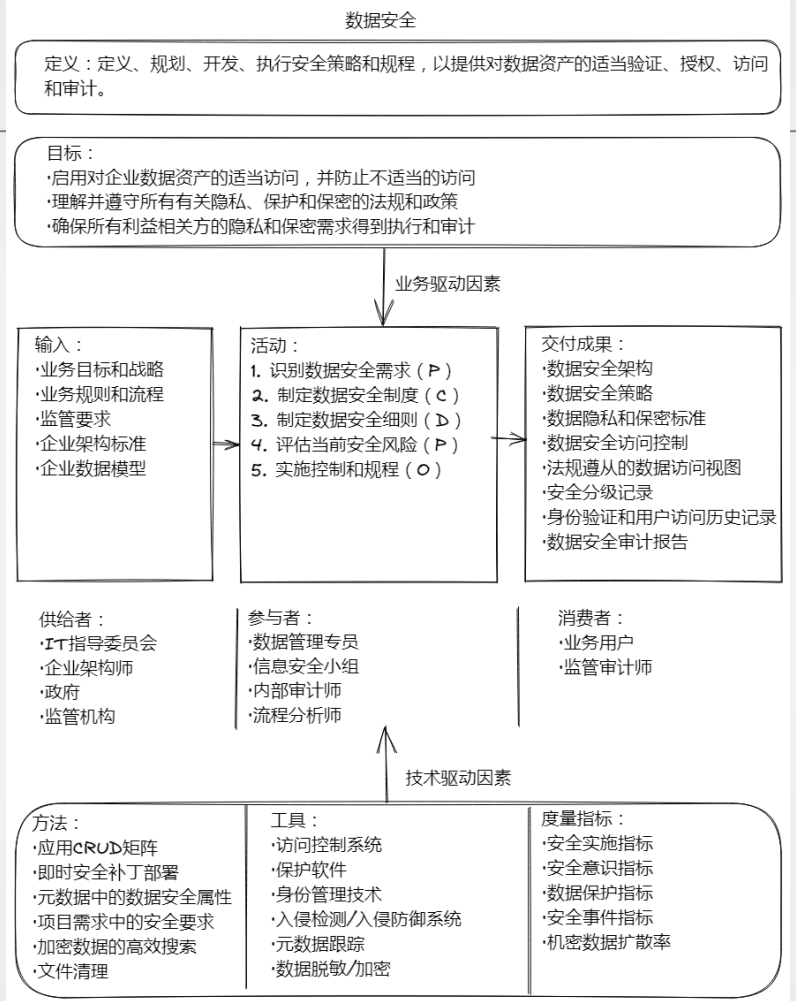
第7章 数据安全/Contents

01

引言

数据安全的定义、业务驱动因素、目标和原则、基本概念

数据安全的语境图



（P）计划　（C）控制　（D）开发　（O）运营

语境关系图：数据治理和管理职责

数据安全的定义

数据安全包括安全策略和过程的规划、建立与执行，为数据和信息资产提供正确的身份验证、授权、访问和审计。

要求来自以下方面：

（1）利益相关方
（2）政府法规
（3）特定业务关注点
（4）合法访问需求
（5）合同义务

业务驱动因素

1、降低风险

对组织数据进行分类分级的整个流程：

1）识别敏感数据资产并分类分级
2）在企业中查找敏感数据
3）确定保护每项资产的方法
4）识别信息与业务流程如何交互

2、业务增长

3、安全性作为资产

目标和原则

目标：

1）支持适当访问并防止对企业数据资产的不当访问
2）支持对隐私、保护和保密制度、法规的遵从
3）确保满足利益相关方对隐私和保密的要求

原则：

1）协同合作
2）企业统筹
3）主动管理
4）明确责任
5）元数据驱动
6）减少接触以降低风险

1、脆弱性

是系统中容易遭受攻击的弱点或缺陷，本质上是组织防御中的漏洞。某些脆弱性称为漏洞敞口。

2、威胁

是一种可能对组织采取的潜在进攻行动。威胁包括发送到组织感染病毒的电子邮件、使网络服务器不看重负以致无法执行业务（拒绝服务攻击）的进程，以及对已知漏洞的利用等。

存在威胁的地方也称为攻击面

3、风险

风险既指损失的可能性，也指构成潜在损失的事物或条件。

可以从以下几方面计算风险：

1）威胁发生的概率及其可能的频率

2）每次威胁事件可能造成的损害类型和规模，包括声誉损害。

3）损害对收入或业务运营的影响

4）发生损害后的修复成本

5）预防威胁的成本，包括漏洞修复手段

6）攻击者可能的目标或意图

4、风险分类：

1）关键风险数据：

由于个人信息具有很高的直接财务价值，因此内部和外部各方可能会费尽心思寻求未经授权使用这些信息。滥用关键风险数据不仅会上海个人，还会导致公司遭受重大处罚，增加挽留客户、员工的成本以及损害公司品牌与声誉，从而对公司造成财务损害。

2）高风险数据

高风险数据为公司提供竞争优势，具有潜在的直接财务价值，往往被主动寻求未经授权使用。

损害可能导致法律风险、监管处罚以及品牌和声誉受损

3）中等风险数据

对几乎没有实际价值的公司非公开信息，未经授权可能会对公司产生负面影响

5、数据安全组织

首席信息安全官（CISO）

任何情况下，数据管理者都要参与数据安全工作。

代表各方利益的是哪个角色？CDO？首席数据官？

6、安全过程

（1）4A1E

1）访问（Access）

2）审计（Audit）

3）验证（Authentication）

4）授权（Authorization）

5）权限（Entitlement）

（2）监控

主动监控：检测机制。系统应包括检测意外事件（包括潜在的安全违规）的监视控制。包含机密信息的应主动、实时监控。

被动监控：评价机制。是通过系统定期捕获系统快照，并将趋势与基准或其他标准进行比较，跟踪随时发生的变化。

7、数据完整性

在安全性方面，数据完整性（Data Integrity）是一个整体状态要求，以免于遭受不当增删改所造成的影响。

萨班斯法案主要涉及对如何创建和编辑财务信息的规则进行识别，以保护财务信息的完整性。

最有名的数据安全法律/个人隐私法律是哪部？注意题目是问哪一部还是哪几部？

8、加密

加密（Encryption）是将纯文本转换为复杂代码，以隐藏特权信息、验证传送完整性或验证发送者身份的过程。

（1）哈希：Hash将任意长度数据转换为固定长度数据表示。即使知道所使用的的确切算法和应用顺序，也无法解密出原始数据。通常用于对传送完整性或身份的验证。常见的哈希算法有MDS和SHA

（2）对称：对称加密使用一个密钥来加解密数据。发送方和接收方都必须具有读取原始数据的密钥。可以逐个字符加密数据（如在传送中），也可对数据块加密。

常见的私钥算法包括数据加密标准（DES）、三重DES（3DES）、高级加密标准（AES）和国际数据加密算法（IDEA）。DES可被多种手段攻击；Cyphers Twofish算法和Serpent算法也被视为安全算法。

（3）非对称

在非对称加密中，发送方和接收方使用不同的密钥。发送方使用公开提供的公钥进行加密，接收方使用私钥解密显示原始数据。当许多数据源只需将受保护的信息发送给少数接收方（如将数据提交到清算交易所）时，这种加密方法非常有用。

非对称加密算法包括RSA加密算法和Diffie-Hell-man密钥交换协议等。PGP是一个免费的公钥加密应用程序。

9、混淆或脱敏

可通过混淆处理（变模糊或不准确）或脱敏（删除、打乱或以其他方式更改数据的外观等）的方式来降低数据可用性，同时避免丢失数据的含义或数据与其他数据集的关系。

脱敏分为两种类型：

（1）静态数据脱敏：永久且不可逆转地更改数据。不会在生产环境使用。

1）不落地脱敏：当在数据源和目标环境之间移动需要脱敏或混淆处理时，会采用不落地脱敏。不会留下中间文件或带有未脱敏数据的数据库，不落地方式很安全。遇到问题可以重新运行脱敏过程。

2）落地脱敏：当数据源和目标相同时，可使用落地脱敏。从数据源中读取未脱敏数据，进行脱敏操作后直接覆盖原始数据。假定当前位置不应该保留敏感数据，在移动至不安全位置之前就应该进行脱敏，存在一定风险，进程失败则很难还原为可用格式。

（2）动态数据脱敏： 是在不更改基础数据的情况下，在最终用户或系统中改变数据的外观。

（3）脱敏方法

1）替换： 将字符或整数值替换为查找或标准模式中的字符或整数值。

2）混排

3）时空变异：日期前后移动若干天，小到足以保留趋势

4）数值变异：应用一个随机因素，重要到使他无法识别

5）取消或删除

6）随机选择：部分或全部数据元素替换为随机字符或一系列单个字符

7）加密技术

8）表达式脱敏：将所有值更改为一个表达式的结果。

9）键值脱敏： 指定的脱敏算法/进程结果必须是唯一可重复的，用于数据库键值字段脱敏。这种类型脱敏对用于测试需要保持数据在组织范围内的完整性极为重要。

10、网络安全术语

（1）后门：是指计算机系统或应用程序的忽略隐藏入口。

（2）机器人或僵尸：是已被恶意黑客使用特洛伊木马、病毒、网络钓鱼或下载受感染文件接管的工作站。

（3）Cookie：是网站在计算机硬盘上安放的小型数据文件，用于识别老用户并分析其偏好。Cookie用于互联网电子商务。

（4）防火墙：防火墙是过滤网络流量的软件和硬件，用于保护单个计算机或整个网络免受未经授权的访问和免遭企图对系统的攻击。

（5）周界：Perimeter，是指组织环境与外部系统之间的边界。通常将防火墙部署在所有内部和外部环境之间。

（6）DMZ：De-Militarized Zone，非军事区，指组织边缘或外围区域。在DMZ和组织之间设有防火墙，DMZ环境与互联网之间始终设有防火墙。DMZ环境用于传递或临时储存在组织之间移动的数据。

（7）超级用户账户：超级用户账户是具有系统管理员或超级用户访问权限的账户，仅在紧急情况下使用。这些账户的凭据保存要求具有高度安全性，只有在紧急情况下才能通过适当的文件和批准发布，并在短时间内到期。

（8）键盘记录器：是一种攻击软件，对键盘上键入的所有击键进行记录，然后发送到互联网上的其他地方。

（9）渗透测试：在渗透测试（Penetration Testing）中，来自组织本身或从外部安全公司聘任的“白帽”黑客试图从外部侵入系统，正如恶意黑客一样，试图识别系统漏洞。通过渗透测试发现的漏洞应该在应用程序正式发布之前予以解决。

（10）虚拟专用网络：使用不安全的互联网创建进入组织环境的安全路径或“隧道”，隧道是高度加密的。VPN允许用户和内部网络之间通信，通过使用多重身份验证元素连接到组织环境外围的防火墙，VPN对所有传送数据进行加密。

11、数据安全类型

（1）设施安全

是抵御恶意行为人员的第一道防线，设施上至少应具有一个锁定能力的数据中心，其访问权限仅限于授权员工。

（2）设备安全，标准包括：

1）使用移动设备连接的访问策略

2）在便携式设备上存储数据

3）符合记录管理策略的设备数据擦除和处置

4）反恶意软件和加密软件安装

5）安全漏洞的意识

（3）凭据安全

1）身份管理系统

2）电子邮件系统的用户ID标准

3）密码标准

4）多因素识别

（4）电子通信安全

基本概念——12、数据安全制约因素

保密和监管的主要区别是要求来源不同，保密要求来自内部，监管来自外部定义。另外区别是任何数据集只能有一个密级，其密级是基于最敏感的数据项设立；然而监管分类是附加的，单个数据集可能根据多个监管类别限制数据，应执行每种法规类别所需的所有操作以及保密要求。

1）保密等级

机密或私密

机密信息仅在“需要知道”的基础上共享

2）监管要求

监管信息在“允许知道”的基础上共享。

基本概念——12、数据安全制约因素

（1）机密数据

1）对普通受众公开

2）仅内部使用（Internal Use Only）

3）机密（Confidential）

若无恰当的保密协议或类似内容，不得在组织以外共享。

4）受限机密（Restricted Confidential）

要求个人通过许可才能获得资格，仅限于特定需要知道的个人。

5）绝密（Registered Confidential）

信息机密程度非常高，任何信息访问者都必须签署一份法律协议才能访问数据，并承担保密责任。

（2）监管限制的数据

1）法规系列举例

①个人身份信息（PII）

也称为个人隐私信息PPI，包括任何可以识别个人或一组人的信息。

②财务敏感数据

③医疗敏感数据/个人健康信息（PHI）

④教育记录

2）行业法规或基于合同的法规

①支付卡行业数据安全标准（PCI-DSS）

②竞争优势或商业机密

③合同限制

13、系统安全风险

识别风险的第一步是确定敏感数据的存储位置以及这些数据需要哪些保护，还需确定系统的固有风险。

（1）滥用特权：解决权限过大的方案是查询级访问控制

（2）滥用合法特权：故意和无意滥用，　　部分解决滥用合法特权的方案是数据库访问控制

（3）未经授权的特权升级：防止特权升级漏洞：将传统入侵防护系统（IPS）和查询级访问控制入侵防护相结合。

（4）服务账户或共享账户滥用

1）服务账户：便利性在于可自定义对进程的增强访问，如果用于其他目的，则无法跟踪到特定的用户或管理员。　　服务账户的使用限制为特定系统上的特定命令或任务，需要文档和批转才能分发凭据。考虑每次使用时分配新密码。

2）共享账户：默认不应使用共享账户

（5）平台入侵攻击

定期软件升级（补丁）

入侵防御系统IPS

入侵检测系统IDS

（6）注入漏洞：在SQL注入攻击中，攻击者将未经授权的数据库语句插入（或注入）到易受攻击的SQL数据通道中，如存储过程和WEB应用程序的输入空间。 通常作为合法命令执行，攻击者可以不受限制地访问整个数据库。

（7）默认密码

（8）备份数据滥用：备份数据库加密

14、黑客行为/黑客

15、网络钓鱼/社工威胁

通常涉及直接通信（无论是当面、通过电话，还是通过互联网），旨在诱使有权访问受保护数据的人提供该信息（或信息访问途径）给拟用于犯罪或恶意目的人。

社会工程是指恶意黑客试图诱骗人们提供信息或访问信息的方法。

网络钓鱼是指通过电话、即时消息或电子邮件诱惑使接收方在不知情的情况下提供有价值的信息或个人隐私。通常，这些呼叫似乎来自合法来源。

16、恶意软件

（1）广告软件：从互联网下载至计算机的间谍软件

（2）间谍软件：是指未经同意而潜入计算机以跟踪在线活动的任何软件程序

（3）特洛伊木马：伪装或嵌入合法软件

（4）病毒：是一种计算机程序，它将自身附加到可执行文件或易受攻击的应用程序上，能造成从让人讨厌到极具破坏性的后果。

（5）蠕虫：一种自己可以在网络中进行复制和传播的程序

（6）恶意软件来源

1）即时消息

2）社交网

3）垃圾邮件，排除模式包括：

①已知的垃圾邮件传送域

②抄送或密送的地址超出限量

③电子邮件正文只有一个超链接的图

④特定文本字符串或单

拒绝服务攻击是哪种？

02

活动

识别需求、制定制度、定义细则、评估风险、实施控制

识别数据安全需求

数据安全活动包括确定需求、评估当前环境的差距或风险、实施安全工具与流程以及审核数据安全措施，以确保其有效。

1、识别数据安全需求

（1）业务需求

（2）监管要求

1）支付卡行业安全标准PCI DSS

2）欧盟的巴塞尔协议II

3）客户信息保护的FTC（联邦贸易委员会）标准（美国）

2、制定数据安全制度

1）企业安全制度

员工访问设施和其他资产的全局策略、电子邮件标准和策略、基于职位或职务的安全访问级别以及安全漏洞报告策略。

2）IT安全制度

目录结构标准、密码策略和身份管理框架

3）数据安全制度

单个应用程序、数据库角色、用户组和信息敏感性的类别。

3、定义数据安全细则

1、定义数据保密等级： 一般用途到绝密

2、定义数据监管类别

安全分级和监管分类的一项关键原则是，大多数信息可以聚合，从而使其具有更高或更低的敏感性。

分类分级的工作成果是一组经正式批准的安全分级和监管类别，以及从中央存储库中获得此类元数据的流程，以便业务和技术员工了解他们所处理、传送和授权信息的敏感性。

3、定义安全角色

方法有两种：网格（从数据开始）或层次结构（从用户开始）

（1）角色分配矩阵

基于数据机密性、法规和用户功能，矩阵可用于映射数据的访问角色。

（2）角色分配层次结构

在工作组或业务单元级别构建组定义。在层次结构中组织这些角色，以便子角色进一步限制父角色的权限。

4、评估当前安全风险

1）存储或传送的数据敏感性
2）保护数据的要求
3）现有的安全保护措施

实施控制和规程

控制和规程至少应涵盖：

1）用户如何获取和终止对系统和应用程序的访问权限
2）如何为用户分配角色并从角色中去除
3）如何监控权限级别
4）如何处理和监控访问变更请求
5）如何根据机密性和适用法规对数据进行分类
6）检测到数据泄露后如何处理

实施控制和规程

（1）分配密级

（2）分配监管类别

（3）管理和维护数据安全

1）控制数据可用性/以数据为中心的安全性

管理用户权限，以及对在技术上基于权限的访问控制的结构（数据脱敏、视图创建）等。

2）监控用户身份验证和访问行为

1）监管风险

2）检测和恢复风险

3）管理和审计职责风险

4）依赖于不适当的本地审计工具的风险

基于网络的审计设备的优点：

1）高性能

在线运行，对数据库影响很小

2）职责分离

独立于DBA运行，将审计职责与管理职责分开

3）精细事务跟踪

支持高欺诈检测、取证和恢复。日志包括源应用程序名称、完整查询文本、查询响应属性、源操作系统、时间和源名称等详细信息。

（4）管理安全制度遵从性

1）管理法规遵从性

①衡量授权细则和程序的合规性

②确保所有数据需求都是可衡量的，因此也是可审计的

③使用标准工具和流程保护存储和运行中的受监督数据

④发现潜在不合规问题以及存在违反法规遵从性的情况时，使用上报程序和通知机制。

2）审计数据安全和合规活动

①评估制度和细则，确保明确定义合规控制并满足法规要求

②分析实施程序和用户授权实践，确保符合监管目标、制度、细则和预期结果。

③评估授权标准和规程是否充分且符合技术要求

④当发现存在违规或潜在违规时，评估所要执行的上报程序和通知机制。

⑤审查外包和外部供应商合同、数据共享协议以及合规义务，确保业务合作伙伴履行义务及组织履行其保护受监管数据的法律义务。

⑥评估组织内安全实践成熟度，并向高级管理层和其他利益相关方报告“监管合规状态”

⑦推荐的合规制度变革和运营合规改进。

03

工具和方法

杀毒软件、HTTPS、身份管理、防火墙、元数据跟踪、脱敏加密
GRUD、补丁部署、安全属性、安全要求、加密搜索、文件清理

数据安全的工具

1、杀毒软件/安全软件
2、HTTPS
3、身份管理技术
4、入侵侦测和入侵防御软件
5、防火墙（防御）
6、元数据跟踪

有助于组织对敏感数据的移动进行跟踪，存在风险：外部代理可从与文档关联的元数据中检测出内部信息。

7、数据脱敏/加密

限制敏感数据的移动

1、应用角色GRUD矩阵

数据-流程矩阵，数据-角色关系矩阵，有助于映射数据访问需求，并指导数据安全色组、参数和权限定义。CRUD-创建、移动、更新、删除；CRUDE-执行

2、即时安全补丁部署

3、元数据中的数据安全属性

元数据存储库对于确保企业数据模型在跨业务流程使用中的完整性和一致性至关重要。

4、项目需求中的安全要求

分析阶段详细确定数据和应用程序安全要求。还可用于选择适当的供应商/采购软件包

5、加密数据的高效搜索

减少需要解密数据量的方法之一是采用相同的加密方法来加密搜索条件（如字符串），然后用密文去查找匹配项

6、文件清理

文件清理是在文件共享之前从中清理元数据（如历史变更记录跟踪）的过程。文件清理降低了注释中的机密信息可能被共享的风险。特别在合同中。

04 实施指南

GRUD、安全补丁部署、数据安全属性、安全要求、加密搜索、文件清理

1、就绪评估/风险评估

组织可通过以下方式提高合规性：

1）培训
2）制度的一致性
3）衡量安全性的收益
4）为供应商设置安全要求
5）增强紧迫感
6）持续沟通

2、组织与文化变革

3、用户数据授权的可见性

4、外包世界中的数据安全

1）服务水平协议（SLA） 安全责任可以外包吗
2）外包合同中的有限责任条款
3）合同中的审计权条款
4）明确界定违反合同义务的后果
5）来自服务提供商的定期数据安全报告
6）对供应商系统活动进行独立监控
7）定期且彻底的数据安全审核
8）与服务提供商的持续沟通
9）如果供应商位于另一国家/地区并发生争议时，应了解合同法中的法律差异。

CRUD（创建 读取 更新 删除）矩阵映射跨业务流程、应用程序、角色和组织的数据职责，以跟踪数据转换、血缘关系和监管链。执行业务决策或应用程序功能（如批准审查、批准订单）的能力必须包含在矩阵中

RACI（负责、批注、咨询、通知）矩阵：可成为合同协议和数据安全制度的一部分。通过定义责任矩阵在参与外包的各方之间确立明确的问责制和所有权，从而支持总体数据安全制度及其实施。

5、云环境中的数据安全

共担责任、定义数据监管链以及定义所有权和托管权尤为重要。

05

数据安全治理

安全治理和度量指标

1、 数据安全和企业架构

安全架构涉及：

1）用于管理数据安全的工具
2）数据加密标准和机制
3）外部供应商和承包商的数据访问指南
4）通过互联网的数据传送协议
5）文档要求
6）远程访问标准
7）安全漏洞事件报告规程

安全架构对以下数据集成尤为重要：

1）内部系统和业务部门
2）组织及其外部业务合作伙伴
3）组织和监管机构

面向服务集成的架构模式（SOA），将要求不同于传统电子数据交换（EDI）集成体系架构的数据安全模式来实现。

度量指标

指标衡量流程的进度：
开展的审计量、安装的安全系统、报告的事件数、系统中未经检查的数据量

1、安全实施指标
2、安全意识指标
3、数据保护指标
4、安全事件指标
5、机密数据扩散

度量指标

1、安全实施指标

1）安装了最新安全补丁程序的企业计算机百分比

2）安装并运行最新反恶意软件的计算机百分比

3）成功通过背景调查的新员工百分比

4）在年度安全实践测验中得分超过80%的员工百分比

5）已完成正式风险评估分析的业务单位的百分比

6）在发生如火灾、地震、风暴、洪水、爆炸等其他灾难时，成功通过灾难恢复测试的业务流程百分比

7）已成功解决审计发现的问题百分比

度量指标

可以通过列表或统计数据的指标跟踪趋势：

1）所有安全系统的性能指标
2）背景调查和结果
3）应急响应计划和业务连续性计划状态
4）犯罪事件和调查
5）合规的尽职调查以及需要解决的调查结果数量
6）执行的信息风险管理分析以及导致的可操作变更的分析数量
7）制度审计的影响和结果，如清洁办公桌制度检查，由夜班安保人员在换班时执行
8）安全操作、物理安全和场所保护统计信息
9）记录在案的、可访问的安全标准（制度）
10）相关方遵守安全制度的动机
11）业务行为和声誉风险分析，包括员工培训
12）基于特定类型数据（如财务、医疗、商业机密和内部信息）的业务保健因素和内部风险
13）管理者和员工的信心和影响指标，作为数据信息安全工作和制度如何被感知的指标。

2、安全意识指标

1）风险评估结果
2）风险事件和配置文件
3）正式的反馈调查和访谈
4）事故复盘、经验教训和受害者访谈
5）补丁有效性审计

3、数据保护指标

1）特定数据类型和信息系统的关键性排名

2）与数据丢失、危害或损坏相关的事故、黑客攻击、盗窃或灾难的年损失预期

3）特定数据丢失的风险与某些类别的受监管信息以及补救优先级排序相关

4）数据与特定业务流程的风险映射，与销售点设备相关的风险将包含在金融支付系统的风险预测中。

5）对某些具有价值的数据资源机器传播媒介遭受攻击的可能性进行威胁评估

6）对可能意外或有意泄露敏感信息的业务流程中的特定部分进行漏洞评估

4、安全事件指标

1）检测到并阻止了入侵尝试数量

2）通过防止入侵节省的安全成本投资回报

5、机密数据扩散指标

应衡量机密数据的副本数量，以减少扩散。机密数据存储的位置越多，泄露的风险就越大。

本章完结 感谢观看

完整课程视频请扫描二维码咨询