数据安全治理实践

那贵昇
北京泰瑞特认证有限责任公司　北京　100015

摘　要：随着全球进入“数字经济”，大数据已经成为最主要的生产因素，各种不同的大数据应用环境对数据安全性提出了全新要求。因此，如何保障数据安全人员已经成为众多行业所关注的话题。本文将对数据安全治理实践进行分析，希望能够给相关人员带来一些帮助。

关键词：数据安全；特征；治理

Data security governance practices

Guisheng Na
Beijing Teret Certification Co., LTD., Beijing 100015

Abstract: As the world enters the “digital economy,” big data has become the most significant production factor, and various big data application environments pose new demands on data security. Consequently, ensuring data security has become a topic of concern in numerous industries. This article aims to analyze the practice of data security governance and hopes to provide some assistance to relevant personnel.

Keywords: data security; Characteristic; governance

前言：

当前，技术与产业的飞速发展，以数据为主要生产要素的数字经济正在迅速发展，它正在深刻地改变着人们的生产与生活模式，并对经济与社会发展产生了巨大影响。在数字经济中，数据是最主要的生产要素，也是最基本、最有价值的财富。随着数据越来越多地扮演着越来越重要的角色，其安全性问题也越来越突出，而且其影响已经从个人和企业扩展到了行业，乃至整个国家。因此，做好数据安全治理十分必要。

一、数据安全的内涵

在国际标准化组织中，计算机系统安全被界定为：为数据处理系统而设置并使用的技术和管理的安全保护，保护计算机硬件、软件和数据不受意外和恶意的影响而遭到破坏、更改和泄露。因此，可以将计算机网络的安全性定义为：利用多种技术和管理手段，保证网络系统的正常运转，进而保证网络中信息的可用性、完整性和保密性[1]。因此，设立网络安全性防护的目标就是要保证透过网络传送与交流之资料不出现增加、修改、遗失与外泄等现象。信息安全或数据安全有对立具有两个相互矛盾的内涵：一是数据自身的安全，它是通过使用“数据保密”“数据完整性”和“双向强身份验证”来实现数据安全的；二是数据保护的安全性，即通过使用“先进的数据储存技术”来实现对数据进行积极保护，如通过磁盘阵列、数据备份和异地容灾等方式来保障数据的安全性。

二、数据安全的主要特征

1. 可用性

数据安全的可用性是一种以用户为核心的设计理念，其核心是让用户可以根据自己的习惯和需要进行设计。例如网络网页设计，要避免使用者在浏览网页时有任何的紧张感与失落感，同时也要让使用者能够以最小的代价，获得最大的效果。正因为如此，世界上很多国家，包括美国和中国，都一直在呼吁让信息自由流动。

2. 完整性

数据的三大基础内容之一是信息的完整性，它是指在信息或资料的传输、存储过程中，保证信息或资料不会遭到未经许可的修改，或者在修改之后可以被及时地检测出来。在实际应用中，它与保密界限经常被混淆。

3. 机密性

保密性也就是所谓的又称机密性，即一个人或一个

组织的资料不能被他人所知。在计算机中有很多软件，包括邮件软件、网络浏览器等，都有一些与保密有关的设置，这些设置是为了保证用户信息的机密性[2]。除此之外，还有一些间谍文件或黑客也会引起保密问题。

三、数据安全治理的基本体系

1.数据安全治理的工作目的

本文所探讨的数据安全治理的目标仍然局限在1个或多个组织机构之内，针对重要数据或敏感信息的数据安全管理与控制等有关的措施，最常见的业务场景就是在数字政府中，各个政府部门的数据安全治理，其中既包含各个政府部门的数据安全治理，也包含跨部门在部门间资料分享层次上的资料安全管理，数据安全治理的目的为以下所示。

①数据安全性遵从的目的：要符合国家、地方及相关产业的各种资料安全性规范的规定。

②数据安全治理安全性保护的目的：要保证资料安全性，资料安全性管理所覆盖商业系统中的资料运作安全性，包含资料可靠性需求、资料防泄露需求和资料防误用需求等[3]。

③数据安全控制的目的是为资料安全控制之系统，包括技术及管理，以保障资料的安全性及资料商业之可持续成长。

2.数据安全治理的制度体系

本文提出一套将管理、技术、评估和运营组合在一起的数据安全治理体系框架，从多个方面，对数据安全治理实践机制进行研究，主要包括了技术、运营、管理以及评估四个方面。数据安全治理机制主要包括以下方面的数据安全治理实践机制：

①数据安全性的保障以及资料安全性的相关标准体系。

②数据安全管理技术：包括发现资料、给资料分类，划分数据的安全等级，资料安全防护策略等内容。

③资料安全管治效果的评定，在这方面要格外注意评价结果，并根据评价后之结论加以改善。

四、数据安全治理实践

1.建设数据安全治理制度

首先，做好组织建设工作。需要制定数据安全治理组织结构，对数据安全治理所涉及的业务范围的有关组织团队在数据安全治理工作中的相关职责和具体要求进行详细阐述，因此，至少应该制定以下几个数据安全治理组织角色：

①数据安全决策层。它是由整个组织的高级管理人员或数据安全官等构成，它要对整个组织的数据安全目标与规划、数据安全治理全过程的资源保障及重大事件协调与决策等职责，同时还要对该组织的数据安全进行最后的责任。

②数据安全管理层。它是由在该组织中的每个具体业务部门的管理人员等构成，要对该特定业务部门数据安全措施与决策的执行进行全面的指导，其中包含但不局限于制定数据安全管理规范、组织制定并落实数据安全技术方案、组织制定并落实数据安全事件监控及处置、数据安全漏洞排查及修复、数据安全事件溯源及分析等内容[4]。

③数据安全监督层。它是一个组织内与该业务部门没有隶属关系的第三方人员构成的，其主要任务是对数据安全治理的过程与结果进行监控和审计，从而保证数据安全治理组织执行的效果。

其次，制定规范化的制度。数据安全管理牵涉到许多标准系统，其中最重要的是：

①制定《数据安全管理制度》，规定每一种商业模式下的数据安全的职责和人员，并制定了相关的保护措施等。

②《数据分类分级规范》对企业中的各种经营数据进行了详细的划分，特别是对个人以及一些关键数据，进行了详细的划分，并进行相应的保密等级划分。

③《数据安全管理规范》对数据的各类和等级进行详细说明，并对数据的收集、传输、存储、处理、交换和销毁等环节进行了细致的阐述。

④《数据安全运营管理规范》中对数据安全风险的监测措施，数据安全风险的反应与紧急处理措施，数据安全漏洞的排查与恢复，以及数据安全的备份与恢复进行了详细的说明。

最后，做好人力资源保障。除了与之有关的技术工具和产品之外，数据安全治理还离不开与之相对应的人员保障。在组织建设中，每一个数据安全治理组织的角色都要对其进行明确，并对其进行详细的职责和考核要求，同时，为保证工作人员的数据安全业务技能与数据安全治理要求相一致，应该对相关人员开展技能培训及职业发展规划等工作[5]。

2.积极应用各种数据安全治理技术

（1）数据安全防护技术

数据安全管理的一个重要举措，就是针对不同等级的数据，采取有差异的数据安全防护策略，一般包括数据加密、数据脱敏、数据访问控制等。在数据安全管理中，数据安全保护策略必须要实现数据的全寿命周期的安全保护，也就是要以数据的分类和等级为基础，按照

类别和等级来控制数据安全保护，保证在数据流动的每一个环节都可以采取一模一样的数据安全控制措施，例如在分享一个数据的时候，将A部门的数据分享到B部门，那么B部门就必须根据其数据的种类和等级，采取与A部门一样的安全控制手段。

（2）数据发现技术

数据安全管理的目标是数据，所以如何精确、有效地挖掘出数据安全管理所需的核心数据就显得尤其重要。到目前为止，在针对静态数据的研究中，已取得大量成果，但是针对动态数据的挖掘与监测，以及针对个体的敏感与重要数据的精确辨识，仍面临着诸多技术难题[6]。其中，动态数据的挖掘依靠于与数据有关的数据，而与之对应的数据的精确辨识，则依靠于正则表示等的特征匹配技术，而现有的技术方法仍存在着误判、漏判，以及系统的性能瓶颈等问题。

（3）数据安全运行技术

数据安全运行是数据安全管理的重要组成部分，数据安全运行包括许多特定的技术，数据安全状态分析与预警报告是最常见的一种技术手段。数据安全状态分析的目的是收集与数据安全保护、数据安全风险管理等有关的数据，并根据这些数据安全状态对数据服务的影响确定危险等级，以保证高危险的安全事件可以被第一时间处理。数据安全状态分析还要求数据安全状态的闭环追踪，也就是说，数据安全状态的管理人员必须与数据安全状态下的数据服务人员建立联系，从而对基础安全状态下的数据服务进行应急处理。数据安全状态分析的目的是根据数据安全漏洞排查与数据安全威胁的情报，对数据服务中可能出现的数据安全威胁进行风险辨识与预警报告，从而预先对数据安全威胁做出有效的预防。

（4）数据划分技术

对数据展开合理的分类和分级，这是数据安全治理的根本，对于不同类型等级的数据，要采取不同的数据安全控制，这可以帮助人们防止对全部数据采取一视同仁的安全措施，从而减少总体上的数据安全管理费用，从而可以精确地对重要数据进行管理。进行数据分类和分级的先决条件是，要建立起数据分类和分级标准，接下来要对数据进行类别和等级上的数据打标。这个技术实施的困难是，怎样才能让数据标记随着数据的流动，在不会对正常的数据业务造成任何影响的情况下进行标记，并保证在数据流动的过程中，数据标记不会被业务抛弃或者被篡改。

3.完善数据安全治理评价制度

数据安全治理评估机制是检验数据安全治理效果最有效的方法，它包含两个部分：一个是评估与评价的对象，一个是改善与提升结果。数据安全评估措施的内容主要有：界定要被评估的对象以及所牵扯到的应用系统和人员，对数据的全生命周期流程以及所牵涉到的数据安全技术与管理措施进行整理，并对每一个数据流动环节中的数据安全措施的有效性进行分析，并将其输出出来。此外，DSMM标准还可以成为一种用于数据安全评估和评价的重要依据，从这个标准中提取出来的30个安全过程域，基本上覆盖了整个数据安全评估流程中的每一个步骤，而标准中对数据安全能力成熟度模型的定级，也可以成为评价结果的一个重要依据。针对数据安全评估与评价中出现的问题，要适时地提出一些改善与提高的方法，其中的工作内容如下：界定改善与提升的负责人，制订一个数据安全改进与提高的方案和工作计划，并对改进与提高后的结果进行审计和总结。如果数据业务发展相对稳定，那么可以考虑1个季度进行一次评估。

五、结束语

总体而言，数据是一种重要的生产因素，对大数据进行开发与应用，将会对促进我国数字经济发展起到积极作用。在整个数据发展过程中，还存在着各种不同的数据安全性问题，这些问题必须引起重视。数据安全不再只是一个技术问题，它还涉及法律、政策、管理和人才理论等多个层面，因此它面临着更多的新挑战，这就要求人们在实际工作中加深理解，加强科研创新。

参考文献：

[1]李雪莹，张锐卿，杨波，等.数据安全治理实践[J].信息安全研究，202211）：1069-1078

[2]杨超，郭刚，叶林佶，唐萍峰，任天雷，邱江.工业互联网数据安全治理实践[J].信息安全与通信保密，2022（9）：18-27

[3]马余静，王子廷，鲍姝睿.数据安全复合治理实践与治理科技[J].中国信息安全，2022（4）：55-57

[4]王庆德，吕欣，王慧钧，刘海洋，秦天雄.数据安全治理的行业实践研究[J].信息安全研究，2022（4）：333-339

[5]郑磊，胡能鹏，方木龙.“数安卫士”安全即服务数据安全治理应用研究[J].中国宽带，2022（12）：141-143

[6]张心怡.数据安全治理体系的构建与实践探索[J].大数据时代，2022（6）：30-45