大数据时代下的信息安全管理

杨晓丹

（漳州理工职业学院，福建 漳州 363000）

摘要：在数字经济环境下，数据已成为各行业产业实现转型升级、社会实现数字建设的重要生产因素。但是，数字经济在带来发展机遇的同时，也带来了一定的信息安全管理问题。大数据时代数据安全的实现需要数据安全治理，探索数据安全治理有效策略尤为关键。基于此，本文针对大数据时代下的信息安全管理策略进行分析，以期为相关从业者提供参考。

关键词：大数据时代；信息安全；管理；数据信息

随着社会的发展与科技的进步，信息数据之间的交互更加频繁，促使数据积累不断增多，大数据时代随之到来。与传统数据不同，大数据更具有多样性、高速性等特点，需要先进的处理工具与管理方案进行处理。近年来，国家相继实施各项信息安全保护政策，以此体现了国家对信息安全的高度重视，表明了信息安全在大数据时代的重要性。因此，探索信息安全防范相关策略尤为关键，有助于提升大数据时代下的信息质量

一、大数据概述

（一）大数据内涵及其作用

大数据是信息科技领域广泛被提及的概念，是指所涉及资料量规模巨大，没有时间与空间限制，通过常规软件工具进行数据集合，将大量信息资料进行处理与管理，为企业经营决策、工作推进等活动提供有效参考数据，为经济与社会的发展提供服务。大数据应用功能强大，其可以在较短时间内完成对特定领域内数据的整合与分析，以促使数据与各项活动有效结合。大数据技术在信息处理方面具有一定的决策力，其能够从海量信息中提炼出关键信息，洞察特定领域中相关的信息资源，对此类信息进行采集、整合与分析，以充分发挥其应有效用。大数据技术不仅是基于科学技术的高新技术，同时也是一种新型应用工具，可借助现代信息技术实现数据的创新应用。

（二）大数据的特点

大数据时代的发展带来了更加庞大的数据信息，促使数据呈现井喷式增长，同时也推动了时代的发展。当下正处于高速发展、信息流通便利的时代，人们之间的交流愈加紧密，生活便利性不断提升。大数据作为新时代产物，能够对各行业发展提供有效帮助，其主要具备以下特点：一是数据量大（Volume）。在信息化背景下，人们每时每刻都在产生数据信息，促使数据量不断增加。二是种类繁多（Variety）。数据的来源较为丰富，促使数据种类较多，包括网络日志、图片、地理信息等，多样化数据类型给数据处理工作带来了极大挑战。三是价值密度低（Value）。在新时代环境下，信息感知无处不在，信息产出较多，但信息价值密度相对较低，需要借助工具对数据信息进行筛选与分析。四是时效高（Velocity）。相较于传统数据挖掘，大数据能够高效处理海量数据，为各项信息应用活动提供有效支撑。

二、大数据背景下网络信息安全存在的问题

（一）信息泄漏问题

大数据时代为人们提供了极大的便利，促使信息传输更加迅速与频繁，人们可以通过互联网渠道获取海量信息，但同时也面临着个人隐私信息泄漏的隐患。比如人们应用社交软件时需要绑定个人手机号、填写个人信息等，此类设计平台为了解用户喜好情况，获取更加全面的动态信息，包括用户的浏览记录等，这些信息在面临黑客不正当入侵时，容易导致隐私泄漏问题，黑客会利用木马病毒获取用户信息，经过长时期潜伏导致信息泄漏。

（二）黑客攻击问题

在科学技术的不断发展中，黑客攻击技术也在不断提升。信息是大数据时代的重要资源，其具有较强的资源价值，对各项活动具有支撑与依据作用。黑客在攻击过程中，大多会应用代码隐藏方式进行攻击，给安全服务鉴别带来较大难度。在互联网技术的支持下，信息传播速度较快，用户也会在短时间提取各类信息进行使用，此过程用户的信息也会被收集，进而被黑客利用。对此，相关部门应设置相应安全管理措施，避免黑客对各类信息的窃取，以防用户个人隐私泄漏与生命财产安全损害等问题。

（三）病毒控制问题

在大数据环境下，人们加强了对各类智能终端产品的使用，社会移动终端设备的使用频率不断增加。智能终端需要即时获取用户适应信息，给用户的海量数据信息安全带来一定威胁。在实际使用中，移动终端设备容易被病毒所控制，进而导师终端设备被损坏或丢失，用户信息产生丢失等，避免影响信息安全。

三、大数据时代下信息安全管理实施策略分析

（一）及时更新升级软硬件配置，建立网络安全监督机制

为有效提升计算机网络信息安全管理效果，应加强对软硬件配置的建设，为各项管理活动提供保障。主要可从以下方面入手：一是及时更新软硬件系统，保障网络信息安全。随着网络信息的不断增加，网络黑客较为活跃，攻击方式不断升级，给安全管理工作带来较大威胁，传统计算机信息安全管理方法已经无法满足信息安全管理工作的需求，无法有效应对攻击威胁。对此，相关部门应加强对安全防护措施的探索，积极创新现有管理方案，及时优化与升级软件与硬件设置，通过优化发现其存在的漏洞，不断完善网络系统，避免黑客利用系统弱点或漏洞进行入侵的问题。二是建立网络安全监督机制。相关部门应结合自身需求建立专门的网络安全监督机制，比如数据保密性较强的企业事业单位、学校的档案管理部门等。完善的网络安全监督价值能够及时了解计算机软硬件设备的使用情况，促使使用人员按照工作要求合理应用网络与数据，阻止浏览高风险网站或访问无关信息网站的行为，降低病毒或木马程序借助高风险网站攻击系统的风险，避免部门重要信息遭受损害。在实际应用中，企业可在计算机应用系统中专门的安全防病毒软件，应用此软件查杀病毒与木马程序，在后续管理中，安排专业技术人员对整个系统进行维护，定期排查是否存在隐藏较深的病毒，并对其进行及时处理；定期查看系统是否存在漏洞，及时下载正版系统进行更新，维护系统安全性，避

免网络黑客的入侵。

（二）及时引进先进网络管理手段，增强数据信息监控

随着科学技术的不断发展，网络信息面领着较为严峻的外部环境，外部环境对计算机网络信息攻击较为隐秘，攻击手段较为多样，传统网络信息防护措施无法有效应对网络攻击。对此，应加强对先进网络管理技术的引进，积极创新保护手段，增强数据信息监控效果。大数据技术应具有强大算法与架构技术手段，能够对数据信息进行精简处理，同时也可以确保数据信息的完整性，保证数据信息不缺失，以此有效提升数据传输效率，促使数据之间形成相互关联。将此技术引进信息管理工作中，能够使数据信息在发生改变时，及时观察并进行处理。以企业生产信息管理为例，在实际应用中，主要可从以下方面入手：一是构建云存储空间。将企业相关信息存储于本地服务器，在存储过程中将其同步到云存储空间，以此构建出云平台数据库，确保数据的备份。二是数据加密处理。对数据信息进行加密处理，引进先进加密技术，并将密钥数据与加密信息进行分开管理。三是建立信息多重备份机制。为确保信息的完整性，可对部分重要信息设置多重备份流程。四是设置传输管理流程。针对重要数据信息的传输，可设置相应的管理流程，应用科学技术手段全方面监控数据传输过程，建立完善的数据信息处理分析模式，对所有数据进行数字化管理避免人为操作出现的数据偏差与存储遗漏等问题。五是设置相应的访问权限。数据访问是实现数据充分应用的重要环节，为确保数据访问过程的安全性，可设置相应的数据信息密钥，对不同使用人员设置不同等级，并对不同等级用户设置相应的访问权限，掌握不同密钥。在实际访问过程中严格审核访问用户信息，以避免非法分子的侵入，并对用户访问过程进行及时追踪，以此确保信息安全问题的可溯性，在出现信息泄露时可追溯至相关工作人员。完善的网络管理技术手段，能够有效增强信息管理效果，为数据信息监控与管理提供有效保障。

（三）完善网络安全代理服务器，最大限度降低安全风险

网络安全代理服务器是内网与外网数据信息传输的中转站，其对确保网络信息安全具有重要价值，直接影响着计算机数据的传输效率。其相较于计算机系统的主服务器具有一定差距，但在维护网络系统安全方面，两者的作用与功能基本相同。在实际应用中，网络安全代理服务器能够在外网与内网的数据传输中充当中转站作用，使得两大网络系统不能直接进行数据传输与交互，而是需要借助代理服务器进行数据交互。网络安全代理服务器在获得外网数据信息后会对此数据进行分析与处理，确保数据安全后则传输给内网，以此可有效筛选数据信息，确保网络信息安全。在信息安全管理工作中引进网络安全代理服务器，能够有效筛选数据，从根源上解决病毒与木马程序入侵网络系统的问题，防止不法分子侵入网络系统，进而有效保证数据安全。另外，在实际应用过程中，应设置相应的安全防护系统，包括防火墙技术等，为安全代理服务器增设屏障，安全管理工作提供多重保障，最大限度降低安全风险。防火墙技术与杀毒软件是大数据时代确保计算机网络信息安全的重要手段，其中防火墙技术可分为地址转换型与代理型，两者均可有效抵御病毒与木马程序，但在实际应用中存在一定区别，需要相关人员结合实际应用要求进行选择。杀毒软件则主要通过定期对计算机系统进行排查，以达到清理病毒的效果，在实际应用相关人员要加强对杀毒软件系统的更新与维护，使杀毒软件中的病毒信息库能够获取最新病毒信息，以实现对各类病毒的有效识别与处理，避免因更新不足使得病毒识别不全面问题，以此确保信息安全。针对此类软件的应用，相关部门在管理保密级别较高的数据时，还可在此基础上进一步优化计算机系统监督管理技术，及时对内部使用局域网进行监察与监督，以增强安全管理工作的效率。

（四）全面制定信息安全保护制度，增强全民信息安全意识

首先从法律法规制度层面分析，相关部门应全面制定个人信息保护制度，结合大数据时代特点，完善个人信息法律保护体系，为个人信息保护提供法律保障。在法律制度建设过程中，相关部门可汲取国外优质立法监督经验，以构建出区域化的信息安全保障。在法规落实过程中，应加强打击范围，注重扩大打击处罚力度，对非法违法信息泄露事件予以及时曝光，让不法分子在面对信息安全问题时能够望而生畏，以充分发挥法律法规制度作用。在此过程中国家还可设立专门的信息管理部门及其相关职位，针对网络信息安全问题进行专门调查与处理。其次，从公民意识层面分析，相关部门要加强对信息安全保护知识的宣传，有效增强全民信息安全意识。在大数据背景下，人们要加强对个人信息的保护，养成良好的信息使用习惯，对日常生活中具有隐私信息的物品进行及时处理，比如将快递单信息进行销毁后再行处理，注重使用安全浏览器上网，在下载文件后应及时清理电脑历史记录等，避免个人信息被窃取。再比如在公共场合时要慎用免费 WiFi，不要随意打开来路不明的文件，以免受到不明恶意软件的攻击。在宣传工作中，相关部门要通过多样化方式进行知识普及，在线上通过短视频或公众号方式告诫人们，在线下通过张贴宣传语、知识讲座等方式，普及生活中的个人信息安全常识。

四、结语

综上所述，大数据时代的到来给人们带来了诸多机遇与挑战，人们应用大数据技术实现了信息的高效处理，但随着社交网络信息数据的不断增加，越来越多的社交网络进行了数据公开，使得人们愈加关注信息安全问题。面对海量数据信息资源，计算机网络系统很容易受到多方面因素影响，进而造成网络信息安全问题。对此，相关部门应及时优化计算机软硬件配置，加强对先进防御技术的引进与应用，构建完善信息管理屏障，以确保网络信息的安全，让大数据时代下的社交网络更好地为人们服务。

参考文献：

[1] 马萱 . 大数据时代计算机网络信息安全管理研究——评《计算机网络信息安全（第 2 版）》[J]. 机械设计，2021（03）：028.

[2] 石书红 . 大数据背景下计算机网络信息安全管理及防范措施 [J]. 普洱学院学报，2020，36（06）：15-17.

[3] 陆康，刘慧，杜京容，任贝贝 . 我国图书馆大数据管理制度建设研究——以《信息安全技术大数据安全管理指南》为例 [J]. 图书馆，2020（11）：6-12.

[4] 宋芝美 . 解读大数据时代企业管理中信息安全研究的现状与展望 [J]. 中国新通信，2020，22（16）：139.

[5] 毛群英 . 大数据背景下农村网络信息安全管理的路径 [J]. 农业经济，2020（02）：38-40.

“漳州理工职业学院横向科研项目（项目编号：20210201K）”