

大数据时代网络信息通信安全管理的创新提升

杨鑫

(天津市武清区京津产业新城数据产业研究中心 天津 300000)

[摘要]随着社会经济的不断发展,人们的科学技术水平也在不断地提高,如今人类已经迈入到信息技术时代。信息技术时代给人们的生产生活带来了极大地便利,但也出现了诸如信息安全防护等问题,本文通过分析大数据时代信息安全防护中存在的风险,从通信网络安全保障及与社会发展相适应两个角度入手,探讨了如何对通信安全管理进行创新和改进。

[关键词]管理;网络安全;大数据

[DOI] 10.12252/j.issn.2096-6288.2021.03.1853

1 通信网络在大数据时代的安全风险

(1) 基础通信数据设备结构类型多样、通信数据网络结构复杂,因此逐渐形成了较为复杂的我国通信行业网络管理系统。为了有效解决存在的困难问题,政府部门出资组建了北京铁塔通信公司。但是所谓冰冻三尺非一日之寒,既有网络通信系统网络传输系统长期存在的各种复杂运行系统问题依然存在较多。因我国通信基础设备安全标准不统一,实时数据控制系统业务量及通信设备软件生产商管理压力过大,基础设施数据安全能力分散极易导致发生安全隐患问题。

(2) 在移动通信行业网络安全风险评估工作过程中大多数都需要人员依据风险分析者的具体个人工作经验情况做出具体相关风险判定,这会对风险评估过程结果的判定时效性与评估准确性产生有直接性的影响,导致网络安全系统风险分析评估的结果准确性、及时性无从得到保障,缺乏人员自主进行分析,自动判断发现风险能力。

(3) 除上述需要分析的环境因素之外,通信器和网络设备运行安全也可能同时受到外部环境因素等的干扰,比如天候气象、设备运行环境和工程施工管理条件等。局部网管通信系统故障常常会引发各类大型网管通信系统设备产生不同程度大小不一的告警信息,而在产生原因未完全确定时,监控者仅此即可基于自身的工作经验情况做出原因分析且向网络维护管理部门人员发出告警信息,请求后者进行处理,这类解决方法不但处理速度缓慢,而且工作效率低下,抢修工作时间常因此而被严重延误。现有很多风险评估分析技术都是没有形成多维度风险分析评估体系的这是其主要失败原因。信息技术通信行业网络发展较快速度不断加快日益巨大复杂化了信息通信网络结构,加大了安全数据信息分析风险评估技术工作量,而既使现有安全网络风险分析评估技术的工作准确度低、工作管理任务完成效率不高,必须探索改进信息通信行业网络安全数据风险分析评估技术应用于广大数据分析技术的新策略,扭转解决现有信息通信行业网络安全风险问题。

2 大数据分析技术与移动通信网安全性的风险如何判别

(1) 企业大数据分析技术理念概述。新数据处理技术模式在此基础上所发展形成的具有流程数据优化管理能力,即为企业大数据,其实质上也就是一种大数据处理技术的具体简称。以下为行业大数据的基本技术内容:以不同行业技术手段为主要依据,处理各种海量、分散的行业数据与技术信息。

(2) 基于应用大数据技术建立移动通信领域网络安全应用风险分级判别评估体系。大数据安全环境现已在我国通信行业内日益成熟形成,判断企业通信网络安全潜在风险标准应该要做到:第一,对产品研发生产应用中的大数据相关技术流程给予更多高度关注,成熟的体系化流程收集、分析并综合处理应用大数据。第二,研发网络大数据分析技术时,考虑对采用多维度自动关联数据分析网络通信中在网络中的数据状态给予更多维度关注,对当前网络通信运行中的状态信息展开全面跟踪监测,自动跟踪评估分析通信中的网络安全风险,辅助分析判断网络故障,并将风险告警信号及时发出。

3 基于大数据的通信网络安全风险应对措施

(1) 信息网络安全监督管理方面。通信的不同频段网络数据传输速和接入不同,预估通信安全网络事故故障概率

发生可能风险的大概率在此分析过程中,有必要由此从社会经济环境因素、人为因素等多个不同方面进行综合分析入手将故障风险概率分析由此再次展开。环境因素主要技术定义一般是指广泛泛指自然灾害、植物在公共运输交通线路上进行生长发育及其植物生长、潮湿及天气产生大量灰尘等。人为因素通常我所指的不仅是广泛的也指的会受到故意盗窃或被恶意破坏、直接预埋大型电力传输线缆内部基层埋深不够、架空高度不够、与其他直埋电力线缆传输线共同使用进行线缆架设、运输施工过程安全保护、施工运输过程服务质量等人为因素等的影响。

以联网大数据表现特征及分析前文对我国通信网络安全可能存在的网络干扰风险因素进行分析方法为统计依据,建立如下应对保障措施:第一,将安全风险分析评估评价指标与网络安全存在故障的分析算法结合确定;第二,完成风险分析评估指标精确设定,严密控制设定并精确的自定义数据,测试并在虚拟云盘存储空间内准确存储相关数据,基于云盘虚拟化存储技术快速提升通信网络平台安全数据;第三,以安全风险评价指标结果分析为统计依据,将我国通信信息网络的安全风险运行问题风险和特点通过评估体现出来,以此对我国通信信息网络中的运行安全问题风险做出准确性的分析,提高安全运行风险与技术隐患综合处理的技术针对性。

(2) 从业人员安全管理方面。通信安全的功能内涵广泛,人员安全保护是其重要功能构成的一部分。相关统计数据有可能将不同群体心理类比综合分析心理特征综合进行一种稳定性、关联性、秩序性的综合体现,即在普通人们的眼前可能呈现出群体更多的心理规律。部分操作人员的安全技术风险节点即可通过大规模数据技术分辨显示出来,为严格监督检查移动通信工程建设项目实施建设过程中的安全技术风险和节点。

(3) 网络数据安全保护方面。加强政府相关敏感信息数据收集管理、政府公共信息资源收集与使用管理控制、通信信息网络保护用户个人隐私等各个方面的安全体系等并构建全面性的平衡才使通信信息网络的大数据安全体系才能真正得到有效率的保障。

参考文献

- [1] 楚银杰.数据通信网络维护及网络安全研究[J].通讯世界,2017(07):37-38.
- [2] 曹红,郭峰,简振波.基于大数据分析技术的通信网络监控体系构建研究[J].信息与电脑(理论版),2017(14):130-131.
- [3] 陈坚.数据通信网络维护与网络安全问题的探讨[J].电子世界,2017(20):151+153.
- [4] 郭建英.数据通信网络维护与网络安全问题的探讨[J].科技资讯,2011(26):9+11.
- [5] 谢尧,吴柳,张思拓,辜晓波.基于大数据的电力通信网的安全防护系统及实现[J].电子设计工程,2017,25(19):131-135.

作者简介:

杨鑫(1991—),男,汉族,总经理,本科,大数据生态。