Universe Scientific Publishing
Mechanical Engineering,机械工程(2)2020,2
ISSN:2661-3530(Print);2661-3549(Online)

大数据背景下企业信息安全管理的技术应用研究

张　娜
沈阳职业技术学院　辽宁　沈阳　110045
作者简介:张娜　1981.1　女　汉族　辽宁　昌图　大学本科　讲师、网络规划设计师　研究方向:计算机系统结构
DOI:10.18686/jxgc.v2i2.21268

【摘要】人们生活中的通信社交从文字传输发展到图片传输,再到现在普遍流行的视频传输,可以说,我们已经进入到一个万物互联的信息化大数据时代。在这样的时代背景下,企业的经营方式和管理体系也在发生重大变革,越来越多的信息化技术开始在企业发展中发挥重要作用。一方面,企业可以借助信息化的技术实现线上、线下多渠道的营销变现;另一方面,企业的信息安全问题也开始更大程度地与企业的管理、用人、效益等多方面相关联。本文就大数据时代背景下的企业信息安全管理问题展开论述,主要分析当前企业信息安全管理存在的突出问题,并为解决这些问题提出一系列优化方案,尽可能避免我国一些企业在自身发展过程中遭遇信息安全的威胁,以促进我国各行各业的健康、和谐发展。
【关键词】大数据;企业信息安全;应用研究;优化方案

在信息化技术不断深入的市场环境下,许多企业赖以生存的经济线已经离不开信息技术的支撑。那么,安全地运用信息技术资源变得很重要。认识到当前企业信息安全管理存在哪些问题,是防患于未来的预见性举措,能为企业更好地发展打下基础。只有先发现问题,才能更好地解决问题,帮助企业在大数据时代科学、合理地规避风险。

1　大数据背景下企业信息安全管理存在的问题

1.1　不重视信息的“完整性”

当工作人员在正常工作过程中,突然遭遇断电、没有信号、网络差等状况,就会导致信息在存储或传输的过程中被破坏、来不及保存,甚至丢失。这种现象可以说并不少见,尤其是在初创型的中小型企业里,他们的防风险意识较差。由于平时不重视这些突发状况,没有积极的应对预案,有时候这种信息的丢失会给员工增加不必要的工作负担,也会给企业带来重大损失。尤其在大数据的信息化时代,有一些不遵纪守法的人还会专门故意制造这样的“突发意外”,阻碍竞争对手的正常办公,为自己赢得更好的发展机会。所以,为保障信息传输的完整性,企业信息安全管理不能只是强化信息安全技术,还要有一套自己的防风险预案,以备不时之需。

1.2　不设置信息的“可用性”

企业的办公场所一般人员流动性比较大,有些需要做市场、接待客户的企业,每天还会有各行各业的人前来洽谈、参观。那么,面对那么多的信息终端设备,其中哪些信息是可以被公开的,哪些信息是只有部分人才有权限接触的,这个需要提前设置、规划。而有的企业对这一块的信息安全管理并不重视,每一台电脑都可以无门槛进入、操作,随便一个陌生人都可以打开企业内部的电脑拷贝资料,这就会造成一些尴尬、误会的场景,比如竞争对手的数据分析报表被泄露,这种类型的数据报表很多企业都会研究,但真正被合作伙伴看到,或者同行看到,还是会有可能暴露企业内在的不足,有时候也容易泄露重要的商业数据,错失优质的市场资源。这些不良后果都是不设置企业信息的“可用性”造成的。

1.3　不要求员工的“保密性”

虽然说在大的社会环境下,各个企业的发展机遇是平等的,但毕竟市场资源是有限的,有时候为了抢占优质的市场资源,企业通常要消耗巨大的人力、物力、财力。那么,为了保护来之不易的市场资源、独家数据,企业员工要有很严格的“保密”意识,不能在茶余饭后,三五成群地聊天时,就把企业重要的机密内容随便扩散开去。在我国大大小小的企业中,由于员工不小心泄露商业机密,导致很好的创意被剽窃、公司的业务被抢占,这样的例子并不少见。高素质的保密人才是实现企业信息安全管理的基本保障,当前我

国企业信息安全管理工作之所以存在诸多问题,企业内部员工的保密意识薄弱是很重要的一个原因。如果企业管理者不在日常的管理工作中强化员工的“保密”意识,并设置相关奖惩制度,就很难引起大部分员工的重视,这种企业信息安全泄密的风险就会很高。

1.4 不评估信息的“可控性”

大数据的信息化时代,人们看到信息、备份信息、转发信息和炒作信息的途径很多、很便捷。有些企业看到自己成了“热搜”,才开始反思,才知道自己在哪个环节出了问题,才要去撤回一些言论,或者澄清一些事实,但这个时候,为时已晚。造成这个局面的原因,很大程度上就在于不评估信息的“可控性”。在现代化的企业里,企业领导对企业整体管理的架构中,要特别注重信息安全的可控性,具体来说,什么信息是只针对什么部门的,哪些信息是只针对员工的,有什么信息是需要规避管理层的,这些都要做具体区分。包括企业对外营销上的一些品宣工具包,如果发布渠道权威性较高,而且是不可撤回的,或者极难删除的,就要在发布之前慎重考虑、严格把关,确保宣传内容不出现原则性错误。否则,这样的品宣信息不仅不能达到正面宣传的效果,还会大大降低企业的专业形象。

2 针对大数据背景下企业信息安全管理的研究

2.1 确保信息“完整性”,设置防风险预案

企业作为一个工作场所,随时有可能会发生突发状况,对于有可能发生的突发状况要进行系统梳理、科学分类。比如,断电类、断网类、周边信号干扰等,要根据这些不同情况采取相应的解决措施。企业内部包含多种不同类型的终端设备,基于不同终端设备的通信特点,其信息安全保障策略也会不同。值得注意的是,国家对于信息安全保护是有相关标准的,企业应该先弄清楚这些标准、条例,在符合国家信息安全保护的标准下,再来制定企业内部的防风险预案措施。对于这些防风险预案的工作人员,每个企业可根据自身情况来具体安排。人数较多的大型企业,建议用专门的部门,专业的信息技术人才来管理。人数并不多的中小型企业,可以有1~2名法务人员重点研究政策和措施,执行的人员可由一些企业内的行政人员来实施。比如,在一些企业里,当行政人员接收到要断电或断网的通知后,就会把消息通知到企业各个部门,提醒大家提前做好工作资料的备份,避免信息丢失。每一个企业都希望运用信息化技术来更加高效地处理数据、分析模型、构建体系、开展工作、广泛营销、抢占资源,但每一个企业不可能只是运用信息化技术的优势,而无视其安全风险。由于忽略企业信息安全管理造成了企业风险的事例,国内的许多企业管理者已经吸取了惨痛的经验教训。

2.2 限制信息“可用性”,统一管理终端设备

让应该看到的人看到应该看到的信息,不论是对外,还是对内,都是企业信息安全管理的重要内容。为了避免每一个终端设备被随意打开,被不属于这台终端设备的管理者随意操作、更改数据,企业很有必要设置一个统一管理终端设备的管理体系。比如:部门与部门之间有竞争关系的,最好保持终端设备的隐私性;领导与领导之间管理范围不一样的,可以设置相应的职权可查范围;员工与员工之间的独立终端设备,可以设置密码由部门负责人统一管理。其实,这样的统一管理看似增加了终端设备使用的复杂性,实际上却有利于简化工作流程、提升工作效率。我们经常在企业里会遇到员工请假的情况,某个岗位的员工一旦突然请假,他所在的岗位就要由其他人临时顶替,这个时候,为了熟悉工作内容、交接工作资料,不可避免要用到对方的电脑设备。如果这个员工平时没有对电脑有一些私人设置,电脑就很好打开。但如果有设置,就会变得很麻烦。交接工作的人一边要打电话沟通,一边又要试密码。这个时候,集中统一管理终端设备的优势就显现出来了,即使某个员工临时缺席,其他员工也能很快打开他的电脑设备,搜集相关资料,快速投入到工作中。

2.3 强调信息“保密性”,制定奖惩制度

有一些企业发现员工泄露内部信息时,把所有的责任都归结到员工个人身上。其实,企业内部高层需要反思自己的管理体系,员工会不会轻易把企业内部的信息说出去,主要取决于员工在一个企业里的社交习惯,而这种习惯的培养,一方面需要企业管理者明确提出有这样的纪律要求,另一方面还需要有切实可行的奖惩制度。没有强大的制度约束,很难达到管理的卓越成效。举例来说,由于员工个人原因泄露了企业商业机密,并给企业带来重大损失的,企业可以制定相应的降薪、降职,甚至开除制度。当然,这样的要求主要是为了培养员工的信息安全保密意识,并不是以惩罚员工为目的,所以在制度试行之初,或者在员工初犯之时,企业应该给予宽容的处理,给予员工1~3次改正的机会。目前在我国的企业管理制度中,保密性贯彻的比较好的制度是“密薪制”,很多员工在企业的反复强调和制度要求下,已经形成不随意讨论薪资待遇的习惯。这样的员工即使到一个新的企业里,

即使新的企业没有这方面的要求,他也会尽可能避免这方面的麻烦产生。总之,强调信息的“保密性”,还是要从制度入手,从情感上感化。

2.4 预见信息“可控性”,采取规避方案

当我们看到明星的私人新闻满天飞,企业的负面报道被各个自媒体平台轮番轰炸时,企业确实要引起重视,要明白预见企业内部信息安全的“可控性”非常重要。什么是可控性?通俗来说就是把信息传输控制在自己可以控制的范围内,对信息的传播有可控权。在这一点上,国内有些企业其实已经做得很好了。在一些经常通过互联网线上方式交流工作的企业里,企业在每个员工第一天入职时,就会要求员工注册一个全新的QQ账号或者微信账号,并用这个新的账号处理一切工作事宜。同时要求,在工作期间不允许员工登录自己的私人账号,在工作结束后不允许员工登录自己的工作账号。等到员工离职时,会当着员工的面注销掉该账号。这就是对企业信息安全可控性做得非常好的企业,这样的措施实施起来很简单,不仅提高了员工工作的效率,避免员工用私人账号与工作不相关的人联系,同时也规避了员工工作期间一切工作内容的外漏、遗失。其实,类似这样的规避方案还有很多,每个企业根据自身特点都是可以科学制定的。随着信息技术的日益发达,在各行各业中的广泛应用,对企业来说,预见信息的可控性会越来越重要,会让企业在经营、销售、研发等多方面规避不必要的发展风险。在信息化大数据时代,对信息及其相关技术因素进行科学把控、安全预警,是企业指导和控制未来发展方向的重要战略布局。

3 结语

总体来说,我国企业信息安全管理防护与保障能力,还处于发展中阶段。其实,企业信息安全管理内容涉及方方面面,是很广泛的概念,这当中还包括“风险评估”。风险评估对企业发展来说起到重要的指导作用,通过企业信息安全的研究来进行科学合理的风险评估,确定产品定位,判断客户需求,最后再根据这些大数据结论选择具体可行的实施方案。从这个意义上来说,企业信息安全管理并不只是一个单纯的技术过程、管理过程,它还是一个企业发展的内在核心要素。尤其对于企业发展过程中加入的投资者来说,他们对一个企业未来价值的评估,很多时候会考虑信息安全风险,他们非常注重企业发展过程中的信息安全工作是否系统化、规范化,是否符合国家相关政策的要求。我们经常会看到一些企业的终端设备上使用防火墙、安全扫描等,企业管理者以为有了这些就是对信息安全的保障,其实这只是其中很小的一部分,企业信息安全管理应该是一个完整的体系,以安全策略为核心,向多个分支发散执行下去,最终获得综合的信息安全保障成效。与此同时,企业管理者要有坚定、执着的心态,要明白企业信息安全管理不是一成不变、停滞不前的,随着市场的变化、政策的变化、企业的变化,企业信息安全管理的内容也要做相应调整,只有不断保持这个动态的改进行为,才能让企业更持久、稳定地发展下去。

【参考文献】

[1]王瑾.基于信息安全的企业经济信息管理分析[J].经济研究导刊,2017(08):147-148.
[2]罗立曼,仲雯君.信息环境下的企业管理路径与信息安全探索[J].中国市场,2016(41):90-91.