安恒信息
DAS-security 安全中国

科创板：688023

教育行业网络安全白皮书

（2020年上半年度）

杭州安恒信息技术股份有限公司
DBAPPSecurity Co., Ltd.

官网：www.dbappsecurity.com.cn
电邮：info@dbappsecurity.com.cn
客服专线：+86-400-6059-110
直通专线：首席客户成功官 沈亚婷 18100188999
首席客户成功官 刘蓝岭 18100189888

安恒官方微信

杭州总部

地址：杭州市滨江区西兴街道联慧街188号安恒大厦
座机：0571-88380999/28860999
传真：0571-28863666

科创板：688023

杭州安恒信息技术股份有限公司
DBAPPSecurity Co., Ltd.

没有网络安全 就没有国家安全

教育是国家的主要防御力量

目 录

前 言

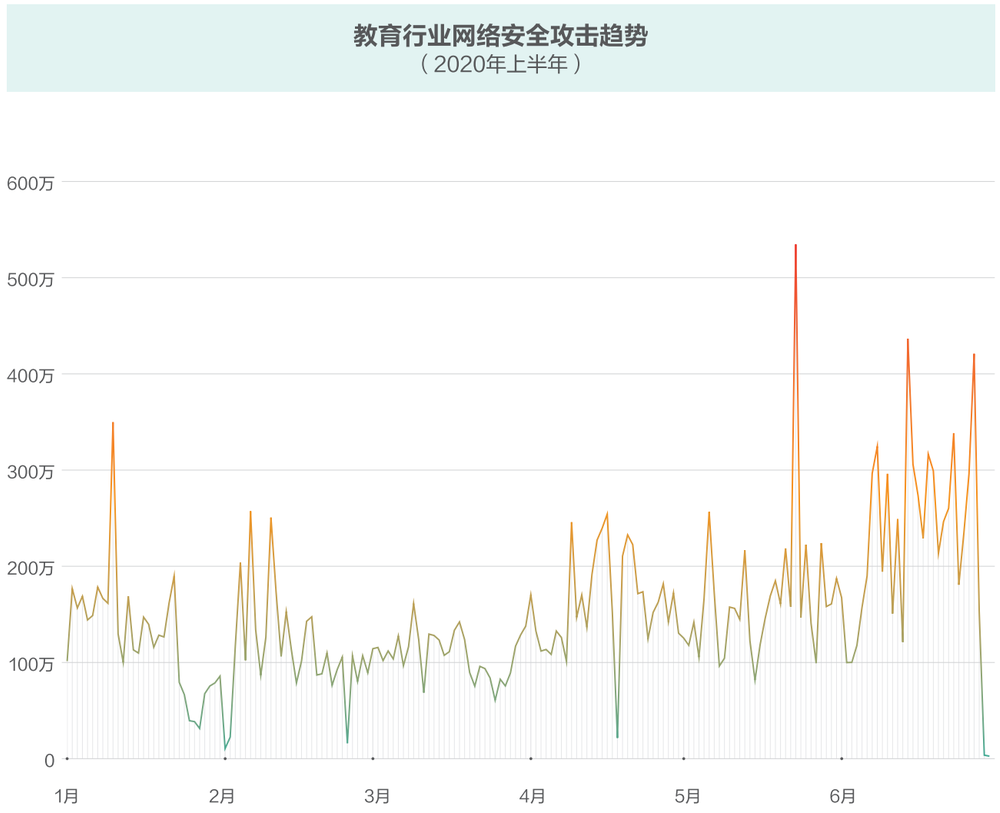
2014年，中华人民共和国教育部颁布《 教育部关于加强教育行业网络与信息安全工作的指导意见 》，提出我国教育行业网络于信息安全工作的总体目标是全面提高教育行业网络与信息安全意识，建立健全教育网络与信息安全工作的组织体系、管理规章和责任制度，落实国家信息安全等级保护制度，有效防范、控制和抵御信息安全风险，增强安全预警、应急处置和灾难恢复能力，提高各级教育部门和学校整体安全防护水平，形成与教育信息化发展相适应的、完备的网络与信息安全保障体系，支撑教育现代化事业健康持续发展。

伴随着教育行业信息化的逐渐发展，国家陆续颁布了《 教育部公安部关于全面推进教育行业信息安全等级保护工作的通知 》、《 教育信息化十年发展规划（2010-2020年）》、《 教育信息化专项-教育业务管理信息系统子项目管理细则（试行）》等重要文件。与此同时，教育部每月发布教育信息化工作月报，充分体现了教育行业信息化对我国的重要性。

2020年上半年，在疫情的严峻形势下，互联网为在线教育带来了契机，但也带来诸多安全威胁。根据统计，注入类攻击、漏洞利用、数据泄露等成为黑客对在线教育行业的突破口，境内外皆有针对教育行业的攻击，中国教育安全发展将在荆棘与鲜花中继续负重前行。

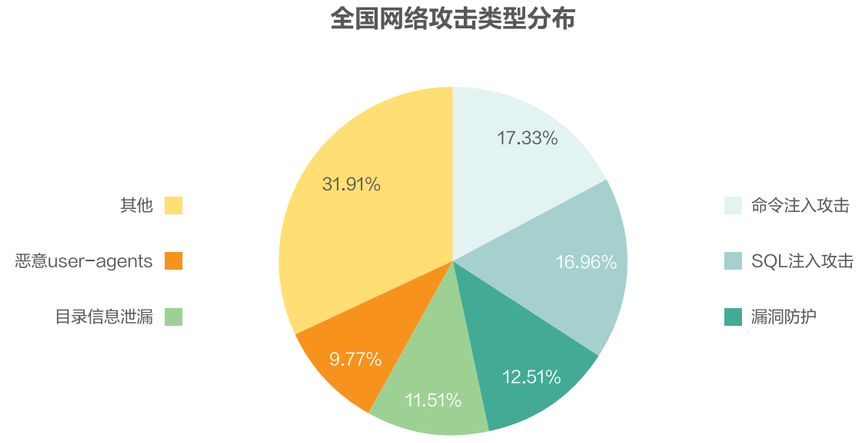
整体网络安全态势

2020年1月至6月期间，安恒信息安全数据大脑监测到来自188个国家对我国教育行业重要系统发起的攻击，攻击总数达到2.73亿次，整体攻击呈上升趋势，在5月25日攻击量达到顶峰，攻击次数达到534.6万次。下图为安恒信息教育行业对网络安全攻击趋势的监测情况：



攻击类型分析

安全数据大脑通过对攻击类型进行分析，发现捕获攻击以命令注入攻击、SQL注入攻击、漏洞防护、目录信息泄露、恶意user-agents等攻击类型为主。其中命令注入攻击类型的占比为17.33%，攻击次数达到4,736多万次；SQL注入攻击类型的占比为16.96%，攻击次数达到4,635多万次；漏洞防护类型的占比为12.51%，攻击次数达到3,419多万次。



主要攻击类型介绍：

命令注入攻击 攻击风险等级：高

由于用户输入了带有恶意代码的数据，且装载数据的系统并未设计良好的过滤过程，使恶意代码与正常数据一并进入系统，最终导致信息泄露或正常数据的破坏。

SQL注入攻击 攻击风险等级：高

Web应用程序对用户输入数据的合法性没有判断，攻击者可以在Web应用程序中事先定义好的查询语句的结尾上添加额外的SQL语句，以此来实现欺骗数据库服务器执行非授权的任意查询，从而进一步得到相应的数据信息。

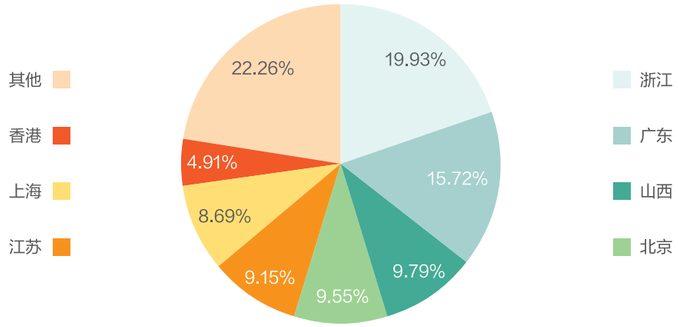
漏洞防护 攻击风险等级：高

Web系统中，远程攻击者会借助一些公开的漏洞对系统进行攻击，以达到获取数据库、控制服务器等目的，如struct2漏洞、tomcat解析漏洞等。

攻击源分布

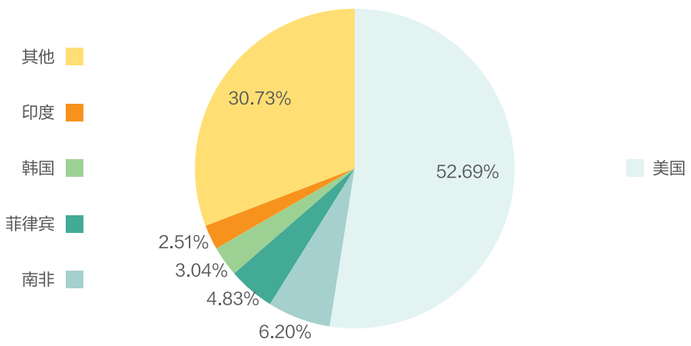
1.境内攻击源

根据安全数据大脑统计分析，2020年上半年我国教育行业重要系统受到的国内1.75亿次攻击，攻击源主要来自于东南沿海区域。进一步追踪发现，这些攻击数据绝大多数来源于运营主体单位的信息安全自检工作。



2.境外攻击源

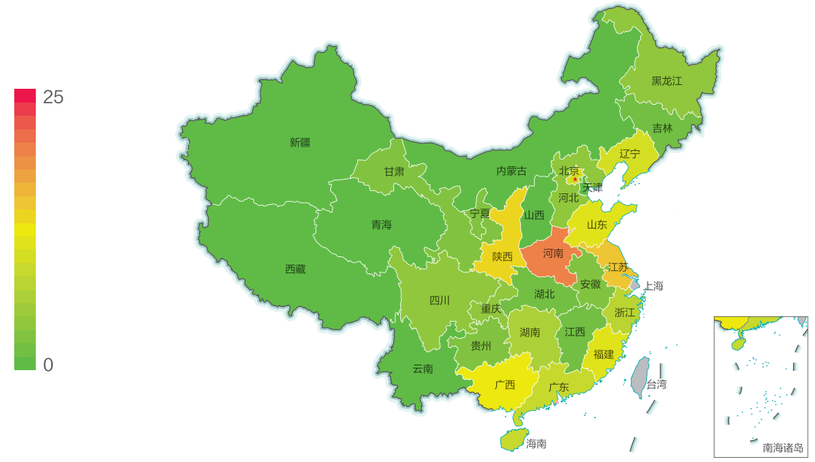
根据安全数据大脑安全统计分析，2020年上半年我国教育行业重要系统受到了来自境外攻击源2,067.9万次攻击，涉及到187个不同国家，主要境外攻击源来自美国、南非、菲律宾，其中来自美国的攻击最多，达到1,089.5万次，攻击占境外攻击源攻击数量的52.69%。



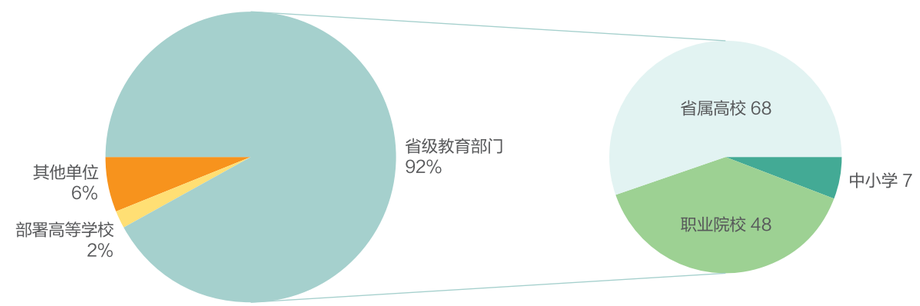
重要漏洞攻击分析

2020年4月，某OA系统存在一个任意用户登录漏洞，使得未经授权的攻击者可以通过该漏洞构造进行任意用户登录（包括admin），登录之后可进一步上传恶意文件控制网站服务器。

安全数据大脑分析：该漏洞为高风险漏洞，容易被利用于攻击教育系统并窃取重要数据。通过对全国教育系统受影响情况进行排查，安全数据大脑发现受影响的系统有212个，其中有142个未升级补丁。针对未升级补丁的网站系统均在第一时间通报给相关单位，影响的网站主要分布在河南、江苏、陕西、广西等地区。



受影响的教育机构类型主要为省级教育部门，部属高校和其他单位。其中省级教育部门最多，占比92.96%。在省级教育部门中省属高校数量最多，有68所，其次是职业院校和中小学。



教育行业网络信息安全现状

网络攻击趋利化，教育行业成重要攻击对象

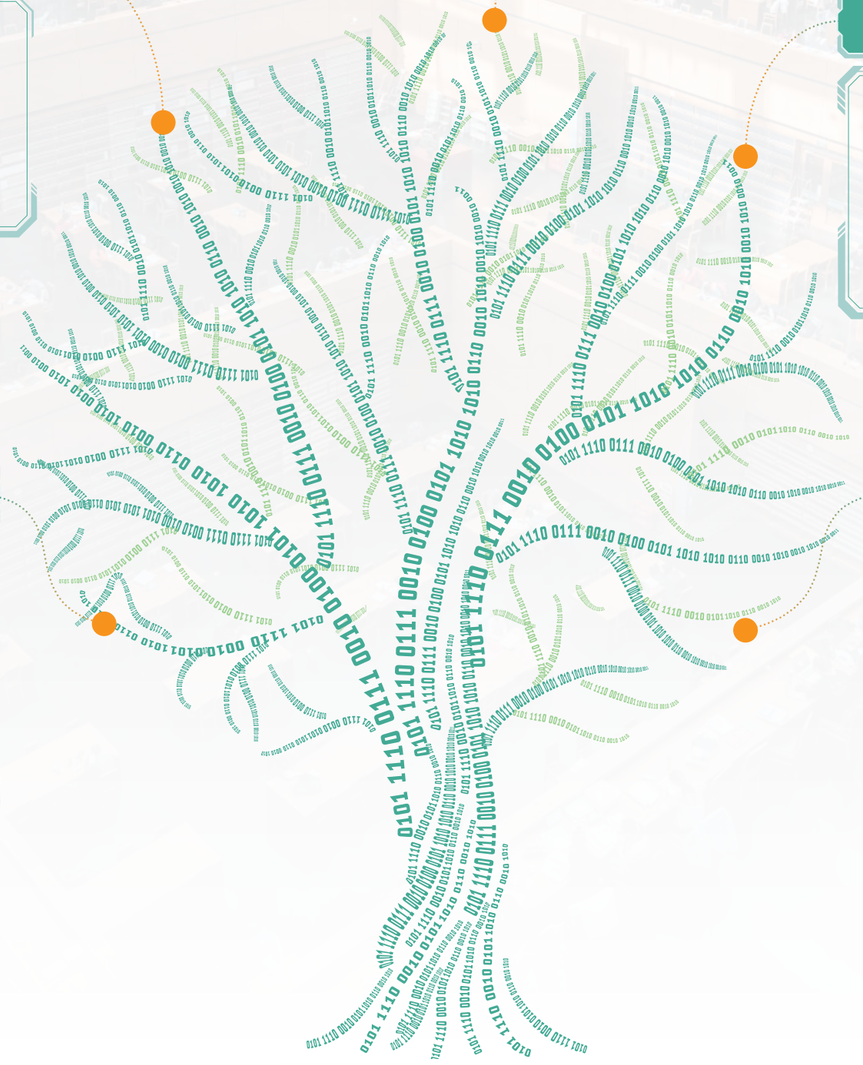
随着全球化进程的持续推进，网络攻击的发起地遍布全球，经验丰富且以盈利为目的性的犯罪团伙不断增加。基于明确的经济利益而发起的网络攻击现象逐年增加，特别是教育行业，一直以来都是网络犯罪团伙的重点攻击目标。电子商务的飞速发展、互联网空间的开放共享特征、网络技术知识的大众化普及，甚至暗网的宣传与活跃，也使得发起网络攻击的门槛大大降低。

教育信息化的快速发展，远程在线业务压力倍增

2020年初，新冠肺炎疫情爆发，为阻断疫情向校园蔓延，确保师生生命安全和身体健康，教育部下发通知要求2020年春季学期延期开学，在线实现“停课不停教、停课不停学”。本次疫情给远程教育带来重大机遇的同时，也不可避免地提出了更大的安全挑战，主要表现为：大规模的访问请求、师生的个人隐私保护、网络安全合规要求和网络空间的恶意攻击等问题。

教育系统的数据庞大且敏感，而数据泄露事件频发

随着教育信息化的深入，为了更好地开展高校教育教研工作，校园网涵盖的数据体系和网络资源异常丰富，覆盖面广泛，涉及人员众多，用户群体活跃且数据价值高。我们收集整理了部分2019年数据泄露事件后，发现教育行业的数据泄露主要由个人疏忽、电信诈骗、网络安全管理缺失、第三方机构非法贩卖以及黑客恶意攻击等情况导致。



对网络空间的安全保障问题已上升至国家高度

伴随5G、工业互联网、大数据中心、云计算等新一代数字基础设施规模化建设和应用，越来越多重要信息系统将承载与国家安全和经济发展密切相关的核心业务和海量数据。习总书记提出“没有网络安全，就没有国家安全”，近年来《中化人民共和国网络安全法》、《网络安全等级保护基本要求》、《网络安全审查办法》等相关法律法规陆续推出，为深化网络安全防护体系,构建全面主动、动态防御的网络安全态势提供了法律保障。

教育系统存在网络安全水平薄弱现象，安全水平参差不齐

为了方便广大师生学习生活所需，很多教育系统在公网中开放，主干网络中部署一些基础的安全策略，面临花样百出、持续迭代的网络攻击手法，这些安全策略已经不能有效应对，导致网络安全态势处于被动地位。同时，教育系统庞大复杂，涉及成千上万个系统和单位，各个单位网络安全工作重视层度不同，使得整体安全水平参差不齐。

教育行业网络信息安全建议

建设并完善安全合规监管体系

据安恒风暴中心2019年对网站安全风险监测与通报数据统计，大量的安全事件发生在管理不规范和监管盲区中。被反共黑客入侵的系统中有大量系统疑似盲区信息系统，长期未更新或无人管理。政府机关过期域名被抢注用于博彩传播，政府机关、事业单位等重要行业存在大量僵尸网站等问题。为有效解决这些问题，建立完善的资产准入、合规、备案体系势在必行。

因此，随着法律法规和信息化的不断推进，教育系统应制定各项安全标准规范体系，进行等级保护测评及风险评估，持续开展安全合规性检查和指导工作，构建安全合规及监管管理的体系。

安全标准规范建设

安全标准规范建设应依据国家等级保护第三级要求和区域范围内的安全标准，结合各地区信息系统和网络环境现状，以及未来安全合规及监管的实际需求出发，围绕着安全管理要求、安全技术标准、安全运营标准形成各区域自己的安全标准规范来指导建设、管理、运营工作的开展。加强准入标准检查，建立常态化的安全风险监测和预警机制，规范和完善云平台资产备案体系。

等级保护测评及风险评估

根据国家网络安全相关标准，在建设安全技术体系、安全管理体系、安全运营体系保障安全运行的过程中，统一实施等级保护测评及风险评估工作。做好网络风险评估工作，监测其服务可用性、风险情况、指纹和端口变更情况等，便于及时发现安全隐患，进行安全加固，保障业务系统的整体安全。

安全合规检查及指导

合规性检查及指导工作由区域监管机构指导各角色合规开展工作，在不同阶段、针对不同技术活动参照相应的标准规范开展，并对各业务单位的重要系统进行安全建设和整改指导，定期开展网络安全情况及能力建设情况检查。特别是针对上云的业务系统，不能让网站和业务系统带病上云，给云平台带来风险和隐患。检查内容包括网站上线前的代码审计、安全风险评估和敏感内容检查等，检查网站是否存在漏洞、挂马、后门、篡改等安全风险，以及是否存在涉政、涉暴恐、涉黄赌毒、信息泄露等内容风险等。

建设全流程的网络安全运营体系

摸清家底，全面梳理教育系统的网络资产

由于单位对网络资产掌握不够全面、资产历史变更和动态变化等原因，网络中存在较多的“资产盲区”现象。在2019年的重大安全事件发生情况中，我们分析发现75%以上的入侵事件都是由“盲区资产”引发，所以摸清家底变得尤为重要。通过测绘单位在互联网中网络资产的分布，弥补现有人工上报机制的不足，提升自动化的资产摸底能力，建设形成完整且可持续跟踪的网络资产底库。

监测预警，建设覆盖全方位的态势感知体系

通过对教育系统进行周期性安全监测、预警和感知，完成覆盖全方位的网络安全态势感知通报体系的总体框架建设，可实现教育系统基础资产数据、安全风险数据、安全事件数据的汇总和分析。同时结合第三方威胁共享数据，实现网络安全风险和安全事件及时发现、预警并进行通报处置，及时掌握重点网络安全态势，了解跨省、跨国的网络攻击行为和网络安全事件。

安全防护，构筑全天候的威胁攻击防御堡垒

移动互联网打破时空限制，安全边界逐渐消失，传统的靠堆砌各种安全设备的防护策略越发不具优势，容易出现安全死角和信息孤岛。通过部署安全防护系统，将教育系统纳入整体安全防护范围，建设云端防管控一体化防护机制，抵御包括网络层的大流量DDoS攻击、CC攻击和web应用层的各类注入攻击和跨站攻击等，实现业务系统的全天候全方位的安全防护堡垒建设。

威胁情报，取得网络攻防对抗的有力主动权

随着信息化的发展，安全攻防对抗不断升级，“网络战就是不宣而战”，因为这场没有硝烟的战争时时刻刻都在发生。若要取得主动权，则需要威胁情报的体系的支撑。通过建立威胁情报基础库、威胁情报联盟机构以及培养威胁情报数据生产能力并且将其在教育系统的安全运营工作中应用，这样能更进一步提升教育行业的网络安全水平，做到知己知彼、百战不殆。

应急响应，组建由专家组成的安全运营中心

在出现严重事件时，安全运营中心可提供应急响应能力，一方面将信息安全事件发生的原因以及可能造成的后果对各个单位进行通报，避免事件的蔓延，另一方面通过安全运营中心可协同网络监管部门、单位管理部门等完成安全事件技术分析、溯源跟踪、数据恢复以及灾害损失预估等服务，并且对信息安全事件处置的过程与结果进行协调、跟踪和监督，确保安全事件顺利处置。

构建数据安全全流程治理体系

教育系统全生命周期管控

对于教育系统的数据安全保护，应该建设数据安全全生命周期管控体系，以数据为中心，围绕着“管理规范”、“安全技术支撑”这两个主体，从数据分级分类、数据采集安全、数据接入安全、数据处理安全、数据组织安全和数据服务安全这七个方面实现全生命周期管控。

基于数据实际使用场景，在管理规范框架下形成完备的数据安全技术策略和落地措施，对实际业务场景中数据泄漏以及敏感信息非授权访问等风险形成有效的安全防护，最终实现数据安全防护的闭环管理链条，完成教育系统数据安全的防护目标。

教育单位数据重点关注

教育单位的数据问题主要表现在标准缺失、数据融合困难和数据质量存在挑战等问题，因此需要重点关注主数据管理、元数据和数据标准管理、数据质量这三个方面。

一、对于主数据管理，教育单位应该通过信息标准管理、数据模型管理、数据业务管理、数据照管管理、数据集成管理、数据采集管理、数据质量管理和数据安全管理等业务操作来提升学校主数据质量，保障主数据的完整性、一致性、准确性、相关性和及时性。

二、对于元数据和数据标准管理，教育单位应该基于教育部最新的信息化数据标准建设要求，结合学校的实际情况，建立一套科学、实用、完善的信息化标准模型。从而形成统一的数据定义，通过完整的数据资源地图，支持数据资源的组织管理，增加数据可信度，实现信息共享。

三、对于数据质量管理，从数据质量监控出发，构建数据质量规则体系，并且在数据质量规则体系的基础上，建立数据质量审核和监控的任务管理，调度和规则执行体系，构建规则执行引擎，由系统对各数据项进行审核，发现集中数据中存在的质量问题。对质量数据进行统计，并通报。

师生个人信息隐私保护

注重学生隐私保护，避免校园贷、信用欺诈、电信诈骗等引发的恶性事件。从数据隐私治理出发，构建隐私数据规则体系，在学生数据的使用、交换以及与第三方应用共享的过程中，应当使用数据脱敏、数据加密等技术。通过敏感数据识别字典和脱敏算法来处理数据表中的敏感信息，应用脱敏规则进行数据变形，保持数据的一致性和业务的关联性，实现数据的可用不可见，保障学生个人的隐私数据安全的同时，兼顾学习业务发展的需求。

根据公安机关近年来破获的数据泄露案件来看，大多数的教育行业数据泄露事件是由于相关人员职责疏忽、网络安全管理意识和《网络安全法》法律意识淡薄导致。因此在教育单位内部要定期开展单位内部员工培训活动，加强相关人员的数据安全、网络安全和相关法律意识，实行必要的终端安全管理，培养员工形成文明上网的好习惯。