奇安信
新一代网络安全领军者

安全内参
网络安全首席知识官

2024网络安全执法案例集

发布机构：安全内参、奇安信行业安全研究中心

2024年9月

报告简介

安全内参 网络安全首席知识官

奇安信 新一代网络安全领军者

- 本报告由《安全内参》和奇安信行业安全研究中心联合编写，旨在结合具体执法案例，帮助网络安全工作者、政企机构管理者加强网络安全合规建设水平。
- 报告收录的全部案例，均来自《安全内参》收集整理的2023年~2024年6月底互联网公开信息，每页案例备注部分均提供了相关新闻链接。您可以在《安全内参》官方网站上检索相关新闻原文：https://www.secrss.com/
- 本次报告共收录：政府与事业单位（2起）、能源（2起）、交通运输（3起）、教育培训（4起）、医疗卫生（8起）、IT信息技术（8起）、生活服务（4起）这七大行业的典型网络安全执法案例31起（包括行政处罚与刑事案件）。
- 其中，涉及数据安全的事件27起、涉及个人信息安全事件14起、一案双查事件18起，涉及个人及黑产团伙犯罪事件10起，涉及内鬼作案或内部人员违规事件5起。

主要观点

- 从公开的执法案例信息总结来看，数据已泄露或存在重大数据泄露风险，是政企机构遭到网络安全行政处罚的首要原因。涉事企业普遍存在未建立健全全流程数据安全管理制度、未组织开展数据安全教育培训、未采取相应的技术措施和其他必要措施、未对其数据处理活动开展风险监测等问题。
- 未履行必要的法律义务、安全建设与运维存在重大疏失，是造成涉事机构被处罚的主要原因。通常情况下，受处罚的不仅仅是涉事机构本身，其信息化主管人员或网络安全主要责任人个人，也会同样会遭到不同程度的处罚。就本次报告收录的案例而言，经济处罚（即罚款）仍然是当前最为主要的行政处罚形式。

主要观点

安全内参 网络安全首席知识官

奇安信 新一代网络安全领军者

- 黑产团伙的犯罪活动不容小觑。在本次报告收录的10起与网络犯罪活动相关的案例中，犯罪分子不仅会窃取相关机构的数据，还会进行篡改数据、操控系统、恶意抢号、盗刷医保卡等多种违法犯罪活动。而被攻击的政企机构，在事后还很有可能会遭到“一案双查”——被攻击的政企机构如果存在显著的未履行网络安全相关法律义务的行为，同样会遭到公安机关的行政处罚。
- 此外，内鬼作案也不容忽视。本次报告共收录4起内鬼作案案例和1起内部人员显著违规操作案例。内鬼的身份多种多样，有的内鬼是技术人员、有的内鬼是供应商或合作伙伴、还有的内鬼仅仅是医院的护工。

相关法律依据

- 本次报告收录的网络安全执法案例，处罚依据主要涉及以下几部法律法规
- 《中华人民共和国刑法》，简称：《刑法》
- 《中华人民共和国刑法修正案(七)》，简称：《刑法修正案(七)》
- 《中华人民共和国网络安全法》，简称：《网络安全法》
- 《中华人民共和国数据安全法》，简称：《数据安全法》
- 《中华人民共和国个人信息保护法》，简称：《个人信息保护法》
- 《信息安全等级保护管理办法》，简称：《等保条例》

安全内参
网络安全首席知识官

奇安信
新一代网络安全领军者

目录

安全内参
网络安全首席知识官

奇安信
新一代网络安全领军者

行业：政府与事业单位

政府与事业单位行业综述

安全内参 网络安全首席知识官

奇安信 新一代网络安全领军者

- 本次报告共收录政府与事业单位网络安全执法典型案例2起。
- 2起案例均为数据安全事件，一起为数据篡改事件、一起为数据泄露事件。其中，数据泄露事件将1.5万余条中国公民个人信息泄露至境外。
- 特别值得注意的是，导致某地政府数据泄露事件，是由于承包商违规将政务数据置于互联网进行测试而导致的。这再次提醒我们供应链安全的重要行，同时，即便是开发过程中，或者是短时间的线上测试过程中，也必须严格遵守安全规则，都则就有可能成为攻击者的目标。
- 与其他行业相比，政府及事业单位的数据安全事件，往往具有更大的社会影响面。但很多地方政府的网站平台，又恰恰缺乏有效的网络安全建设与运营，存在巨大安全风险。
- 本章节的信息来源为《安全内参》：https://www.secrss.com/

某单位重要信息系统数据遭严重篡改

安全内参 网络安全首席知识官

奇安信 新一代网络安全领军者

案例回顾
2023年9月，天津公安南开分局网络安全保卫支队接到线索：辖区内某单位的重要信息系统数据遭到恶意篡改，严重危害网络安全！南开分局网络安全保卫支队分析发现，该单位运营使用的信息系统存在多重问题：一是防范网络侵入技术措施不完善，物理网络环境内部存在监测漏洞；二是监测、记录网络运行状态的网络日志不足6个月；三是对于安全缺陷、漏洞等风险，该单位未立即采取补救措施亦未向有关部门报告，信息系统持续“带病”运营，给了不法分子可乘之机。依据《网络安全法》相关规定，南开分局对该单位及相关主管人员分别予以罚款5万元的行政处罚。
法律链接
据《网络安全法》相关要求：网络运营者应当防止网络数据泄露或者被窃取、篡改。采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

违法/犯罪 主体	黑产团伙、政企机构
违法/犯罪 性质	数据篡改、建设运维管理疏失
所属行业	政府与事业单位
影响范围	政企机构利益
关键词	信息系统数据遭篡改
触犯法条	《网络安全法》第二十一、五十九条
机构责任	未履行安全保护义务
涉及领域	数据安全

某政务系统测试期间泄露公民数据

安全内参 网络安全首席知识官

奇安信 新一代网络安全领军者

案例回顾
2023年9月，上海网信部门发布一则案例。某政府信息系统技术承包商违规将政务数据置于互联网进行测试期间，相关存储端存在高危漏洞，导致大量公民数据泄露，以致成为境外不法分子窃取政务数据的“供应链”入口。经查，该公司租用1台私有云服务器，存储了大量公民信息和政务信息，涉及公民个人信息数据1.5万余条。2022年7月，相关公民个人信息在境外黑客论坛被披露兜售。有关部门已要求该公司立即下线政府网站页面、关闭相关云服务端口、配合开展网络资产清查，并对该公司作出行政处罚。
法律链接
据《网络安全法》相关要求：网络运营者应当防止网络数据泄露或者被窃取、篡改。发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施。 据《数据安全法》相关要求：网络运营者不得泄露、篡改、毁损其收集的个人信息。 据《个人信息保护法》相关要求：发生或者可能发生个人信息泄露、篡改、丢失的，个人信息处理者应当立即采取补救措施。

违法/犯罪 主体	黑产团伙、政企机构
违法/犯罪 性质	数据窃取、建设运维管理疏失
所属行业	政府与事业单位
影响范围	公众利益
关键词	数据保护不力
触犯法条	《网络安全法》第二十一条、第二十二条 《数据安全法》第四十二条 《个人信息保护法》第五十七条
机构责任	未履行安全管理义务
涉及领域	数据安全

安全内参
网络安全首席知识官

奇安信
新一代网络安全领军者

行业：能源

能源央企行业综述

安全内参 网络安全首席知识官

奇安信 新一代网络安全领军者

- 本次报告共收录2023年能源央企行业网络安全行政执法典型案例2起。
- 其中1起案例是由于涉事企业存在建设运维管理疏失而遭到行政处罚，而另外一起案例则是黑产团伙的有组织犯罪，是通过制造作弊加油机，篡改系统数据，从而实现非法敛财的目的。
- 本章节的信息来源为《安全内参》：https://www.secrss.com/

某燃气公司缴费系统有数据泄露风险

安全内参 网络安全首席知识官

奇安信 新一代网络安全领军者

案例回顾

2023年3月，湖南省怀化市沅陵县公安局网安部门在工作中发现辖区某燃气公司缴费系统存有大量客户姓名、电话、身份证号、家庭住址等敏感数据。经查，该公司办公电脑未设置开机密码，缴费系统账号密码均为弱口令，并且该企业未制定数据安全管理制度、未充分落实网络安全等级保护制度。

怀化沅陵县公安局根据《数据安全法》第二十七条、第四十五条第一款之规定，给予该企业警告，并责令限期改正。

法律链接

据《数据安全法》相关要求：开展数据处理活动应当依照法律、法规的规定，建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全。。利用互联网等信息网络开展数据处理活动，应当在网络安全等级保护制度的基础上，履行上述数据安全保护义务。

据《网络安全法》相关要求：网络运营者应当防止网络数据泄露或者被窃取、篡改。

违法/犯罪 主体	企业
违法/犯罪 性质	建设运维管理疏失
所属行业	能源
影响范围	公众利益
关键词	存在数据泄露风险
触犯法条	《数据安全法》第二十七、四十五条 《网络安全法》第二十一条
机构责任	未履行安全保护义务
涉及领域	数据安全

某公司破坏加油机信息系统案

安全内参 网络安全首席知识官

奇安信 新一代网络安全领军者

案例回顾

2023年3月，黑龙江大庆公安机关在联合执法检查中发现，辖区内某加油站移动加油车存在偷油功能。经查，涉案作弊移动加油机系浙江某公司生产，该公司在生产移动车载加油机过程中，勾连技术人员实现遥控加油机达到“缺斤少两”功能。

4月9日至25日，黑龙江大庆公安机关组织在共3省4市开展抓捕行动，先后抓获关键环节犯罪嫌疑人26人，成功打掉一作弊移动加油机生产厂商，扣押作弊移动加油机主板2000余个。

法律链接

据《刑法》相关要求：违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能正常运行，后果严重的，处五年以下有期徒刑或者拘役；后果特别严重的，处五年以上有期徒刑。

据《网络安全法》相关要求：网络运营者应当防止网络数据泄露或者被窃取、篡改。

违法/犯罪 主体	黑产团伙、内部人员
违法/犯罪 性质	篡改数据
所属行业	能源
影响范围	国家利益
关键词	破坏加油机信息系统
触犯法条	《刑法》第二百八十六条 《网络安全法》第二十一条
机构责任	未履行安全管理义务
涉及领域	数据安全

安全内参
网络安全首席知识官

奇安信
新一代网络安全领军者

行业：交通运输

交通运输行业综述

安全内参 网络安全首席知识官

奇安信 新一代网络安全领军者

- 本次报告共收录交通运输行业网络安全执法典型案例3起。
- 这三个案例都是典型的“非法入侵”事件，即黑客或内部人员使用非法手段篡改数据或获取数据。
- 具体问题包括：黑客非法入侵计算机，篡改数据，获取信息；内部人员利用工作便利非法获取数据，非法售卖个人信息。
- 本章节的信息来源为《安全内参》：https://www.secrss.com/

某汽车服务公司侵犯公民个人信息案

安全内参 网络安全首席知识官

奇安信 新一代网络安全领军者

案例回顾

2023年3月，佛山公安机关破获一起非法盗卖公民个人信息案，抓获犯罪嫌疑人47名，涉案金额300余万元。

经查，当地一家汽车服务公司为拓展汽车维修中介业务，勾结保险公司、拖车公司以及路政部门工作人员，非法获取交通事故车主信息，并根据车辆品牌、事发地等联系特定汽车4S店、汽修厂，通过各种好处诱导事故车主前往指定地点维修，赚取信息“中介”费用。相关汽车修理机构通过故意夸大损失、以换代修等方式侵害相关保险公司及车主利益。

法律链接

据《刑法》相关要求：违反国家有关规定，向他人出售或者提供公民个人信息，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。

据《刑法修正案（七）》相关规定：国家机关或者金融、电信、交通、教育、医疗等单位的工作人员，违反国家规定，将本单位在履行职责或者提供服务过程中获得的公民个人信息，出售或者非法提供给他人……

违法/犯罪 主体	企业
违法/犯罪 性质	非法盗卖个人信息
所属行业	交通运输
影响范围	个人利益
关键词	非法出售个人信息
触犯法条	《刑法》第二百五十三条之一 《刑法修正案（七）》第二百五十三条
机构责任	未履行安全管理义务
涉及领域	个人信息

某市新能源车“克隆”电池案

安全内参 网络安全首席知识官

奇安信 新一代网络安全领军者

案例回顾

2023年5月，上海公安机关发现辖区某新能源车企动力电池数据存在异常。通过企业信息系统排查，有多个ID的动力电池在北京、江苏、上海、福建等多地同时出现并使用的情况。经深入分析发现，这些ID号的车辆在之前都因交通事故而被后台锁住了电池组，无法充电和行驶，相关电池组内的数据极有可能被人为盗刷篡改，破解锁定功能。此类被锁定的故障电池重新上路行驶，极有可能引发电池短路甚至起火等高危情况，严重危害驾乘人员生命安全，造成极大交通安全隐患。

法律链接

据《刑法》相关要求：对计算机信息系统中存储、处理或传输的数据和应用程序进行删除、修改、增加的操作影响计算机系统的正常运行，后果严重的行为根据刑法给予处罚。

据《网络安全法》相关要求：网络运营者应当防止网络数据泄露或者被窃取、篡改。

据《数据安全法》相关要求：发生数据安全事件时，应当立即采取处置措施，按照规定及时告知用户并向有关主管部门报告。

违法/犯罪 主体	黑产团伙
违法/犯罪 性质	数据篡改
所属行业	交通运输
影响范围	公众利益
关键词	篡改能源电池数据
触犯法条	《刑法》第二百八十六条 《网络安全法》第二十一条 《数据安全法》第二十九条
机构责任	未履行安全保护义务
涉及领域	数据安全

交管系统遭“黄牛党”入侵

安全内参 网络安全首席知识官

奇安信 新一代网络安全领军者

案例回顾

2023年10月消息，无锡江阴市检察院办理了一起破坏计算机信息系统案。10名犯罪嫌疑人均为二手车“黄牛”，他们通过非法手段，侵入某全国性交管平台系统，为不能正常过户的二手车，非法办理改绑手机号、补办行驶证、补办车牌等业务。

主犯杨某婷，在河北户籍地被警方抓获，其他9名二手车“黄牛”也相继在山东、北京等省市落网。

据《刑法》相关要求：违反国家规定，侵入计算机信息系统或者采用其他技术手段，获取该计算机信息系统中存储、处理或者传输的数据，或者对该计算机信息系统实施非法控制，都应得到相应处罚。

据《数据安全法》相关要求：任何组织、个人收集数据，应当采取合法、正当的方式，不得窃取或者以其他非法方式获取数据。

据《网络安全法》相关要求： 任何个人和组织不得从事非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动。

违法/犯罪 主体	黑产团伙
违法/犯罪 性质	系统入侵
所属行业	交通运输
影响范围	公众利益
关键词	非法入侵系统
触犯法条	《刑法》第二百八十六条 《数据安全法》第三十二条 《网络安全法》第二十七
机构责任	未履行安全保护义务
涉及领域	数据安全

安全内参
网络安全首席知识官

奇安信
新一代网络安全领军者

行业：教育培训

教育培训行业综述

安全内参 网络安全首席知识官

奇安信 新一代网络安全领军者

- 本次报告共收录2023年至2024年上半年，教育培训机构网络安全执法典型案例4起。
- 这4起案例均与安全漏洞有关，其中3起案例为数据泄露事件，数据泄露原因均为系统存在高危安全漏洞，且泄露数据均为个人信息。这些被泄露的信息，有的被黑产团伙在境外黑产平台上售卖，有的则直接被诈骗团伙用于网络诈骗。
- 根据《网络安全法》相关要求：“网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞……”。网络运营者缺乏对安全漏洞的有效运营和管理，被告知安全漏洞后不及时修复，都很容易使系统遭到攻击，相关政企机构及主要责任人，也会一并遭到处罚。
- 特别值得一提的是，其中1起案例，公安机关对某高校的行政处罚金额高达80万元。这页是本次报告收录的单次处罚金额最高的案例。
- 本章节的信息来源为《安全内参》：https://www.secrss.com/

某培训机构学员信息泄露

安全内参 网络安全首席知识官

奇安信 新一代网络安全领军者

案例回顾

2023年2月，多名在厦门某教育培训机构学习的学员接到自称是该机构工作人员的诈骗电话后报案。经查，犯罪嫌疑人朱某某利用系统漏洞，非法入侵该教育机构的办公管理系统，窃取近两万条包含学号、姓名、手机号、身份证号等内容的学员信息数据并售出，从中获利1380元。当年8月，朱某某因犯侵犯公民个人信息罪，被判处有期徒刑9个月，缓刑1年，并处罚金4000元。目前，购买信息的违法人员正在进一步追查中。同时，思明公安分局网安队对该案件采取“一案双查”，启动对该教育培训机构网络安全义务履行情况的监督检查。

法律链接

据《刑法》相关要求：侵入计算机信息系统或者采用其他技术手段，获取该计算机信息系统中存储、处理或者传输的数据……。

据《网络安全法》相关要求：网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击……。

据《数据安全法》相关要求：开展数据处理活动应当依照法律、法规的规定，建立健全全流程数据安全管理制度，组织开展数据安全教育培训……

据《个人信息保护法》相关要求：任何组织、个人不得非法买卖、提供或者公开他人个人信息。

违法/犯罪 主体	个人黑客、诈骗团伙、企业
违法/犯罪 性质	网络诈骗、建设运维管理疏失
所属行业	教育培训
影响范围	公众利益
关键词	数据保护不力
触犯法条	《刑法》第二百八十六条 《网络安全法》第二十一条、第五十九条 《数据安全法》第二十七条 《个人信息保护法》第十条
机构责任	未履行法定安全保护义务
涉及领域	数据安全

某软件学校网站存在数据泄露风险

安全内参 网络安全首席知识官

奇安信 新一代网络安全领军者

案例回顾

2023年3月，株洲市公安局荷塘分局网安大队接株洲市网络与信息安全信息通报中心通报，株洲某软件学校网站存在短文件名泄露漏洞。经网安大队检查发现，该网站系统中存在大量学生姓名、身份证号、电话号码、家庭住址等敏感信息，该学校未对前述数据采取应有的技术保护措施，未履行数据安全保护义务，存在数据泄露风险。

株洲市公安局荷塘分局根据《数据安全法》第四十五条，给予该学校警告，并责令限期改正。

法律链接

据《数据安全法》相关要求：开展数据处理活动应当依照法律、法规的规定，建立健全全流程数据安全管理制度……。

据《网络安全法》相关要求：网络运营者应当防止网络数据泄露或者被窃取、篡改。

据《个人信息保护法》相关要求：个人信息处理者应当对其个人信息处理活动负责，并采取必要措施保障所处理的个人信息的安全。

违法/犯罪 主体	企业
违法/犯罪 性质	建设运维管理疏失
所属行业	教育培训
影响范围	公众利益
关键词	存在数据泄露风险
触犯法条	《数据安全法》第二十七、四十五条 《网络安全法》第二十一条 《个人信息保护法》第九条
机构责任	未履行法定安全保护义务
涉及领域	数据安全

某中学路由器管理界面遭劫持篡改

安全内参 网络安全首席知识官

奇安信 新一代网络安全领军者

案例回顾

2023年7月，湖南省常德市公安局网技支队接到上级线索，鼎城区某中学智慧校园系统路由器被黑客攻击。经查，该校智慧校园系统l的路由器存在高危漏洞， 已 被入侵劫持并篡改，登录该路由器管理界面时会跳转到劫持后的界面。进一步调查显示：学校网络安全意识淡薄，系统网络安全防护不到位， 存 在 未制定切实有效的网络安全管理制度及应急处理方案、未按规定部署网络日志设备等多项违法行为。

依据《网络安全法》相关规定，鼎城区公安局对该校及相关主管人员分别依法予以罚款。对运维公司依法予以警告。

法律链接

据《数据安全法》相关要求：开展数据处理活动应当依照法律、法规的规定，建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施……。

据《网络安全法》相关要求：网络运营者应当按照网络安全等级保护制度的要求，履行安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。 网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险。

违法/犯罪 主体	个人黑客、学校
违法/犯罪 性质	非法入侵
所属行业	教育培训
影响范围	公众利益
关键词	存在漏洞导致信息被篡改
触犯法条	《数据安全法》第二十七条 《网络安全法》第二十一条、第五十九条
机构责任	未履行法定安全保护义务
涉及领域	数据安全

某高校发生大量数据泄露案件

安全内参 网络安全首席知识官

奇安信 新一代网络安全领军者

案例回顾

2024年1月，南昌公安网安部门在工作中发现，南昌某高校3万余条师生个人信息数据在境外互联网上被公开售卖。涉案高校存储教职工信息、学生信息、缴费信息等3000余万条信息的数据库被黑客非法入侵，其中3万余条教职工、学生个人敏感信息数据被非法兜售。南昌公安网安部门对该学校作出责令改正、警告并处80万元人民币罚款的处罚，对主要责任人作出人民币5万元罚款的处罚。

法律链接

据《数据安全法》相关要求：开展数据处理活动应当加强风险监测，发现数据安全缺陷、漏洞等风险时，应当立即采取补救措施；发生数据安全事件时，应当立即采取处置措施，按照规定及时告知用户并向有关主管部门报告。

据《网络安全法》相关要求：网络运营者应当按照网络安全等级保护制度的要求，履行安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。

据《个人信息保护法》相关要求：任何组织、个人不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息

违法/犯罪 主体	黑产团伙、学校
违法/犯罪 性质	非法入侵
所属行业	教育培训
影响范围	公众利益
关键词	敏感数据泄露并被售卖
触犯法条	《数据安全法》第二十七，二十九条、四十五条 《网络安全法》第二十一条 《个人信息保护法》第十条
机构责任	未履行法定安全保护义务
涉及领域	数据安全

安全内参
网络安全首席知识官

奇安信
新一代网络安全领军者

行业：医疗卫生

医疗卫生行业综述

安全内参 网络安全首席知识官

奇安信 新一代网络安全领军者

- 本次报告共收录2023年医疗卫生行业网络安全执法典型案例8起。
- 医疗卫生行业的内鬼作案特征非常明显。在8起案例中，有2起涉及内部人员监守自盗。其中1起为数据分析师作案，1起为医院护工作案。医院加强内部人员安全管理非常有必要。
- 黑产团伙针对医院的网络攻击活动也是多种多样。有的是黄牛党入侵系统，窃取数据，并利用黑客工具预约抢号。有的是利用AI换脸技术，冒充医生盗刷医保卡。
- 此外，完全因为安全建设运维管理疏失而遭到处罚的案例也有四起。其中，医院被定级为等保三级，却未按要求进行等保测评的案例最值得其他医院引以为戒。因为三级以上的医院，其很多信息系统都会被定级在等保三级。
- 本章节的信息来源为《安全内参》：https://www.secrss.com/

某团伙通过AI换脸盗刷他人医保卡

安全内参 网络安全首席知识官

奇安信 新一代网络安全领军者

案例回顾

2023 年 4月，重庆石油路派出接到某医院医生报案，称其医保卡在没有丢失的情况下，被盗刷42805元。石油路派出所迅速开展工作，当日即将犯罪嫌疑人段某抓获，随后有抓获其同伙袁某某、李某某，查获赃物价值6万余元。

经查，该团伙先由两名上家通过某境外聊天软件购买一批医生的信息（含身份证号码、名字、工作单位等），然后通过网络搜索查找能够匹配的医生照片，再利用AI换脸软件，把搜索到的受害人照片制作成平台所需的动态人脸识别视频，通过平台的实名认证后，获取电子医保支付二维码，进而盗刷受害人医保卡。

法律链接

据《刑法》相关要求：盗窃公私财物，数额较大的，或者多次盗窃、入户盗窃、携带凶器盗窃、扒窃的，处三年以下有期徒刑、拘役或者管制，并处或者单处罚金……

据《个人信息保护法》相关要求：任何组织、个人不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息……

违法/犯罪 主体	黑产团伙
违法/犯罪 性质	盗刷医保
所属行业	医疗卫生
影响范围	公众利益
关键词	黑产团伙盗刷他人医保
触犯法条	《刑法》第二百六十四条 《个人信息保护法》第十条
机构责任	未履行安全保护义务
涉及领域	数据安全

某市破坏疫苗预约系统案

安全内参 网络安全首席知识官

奇安信 新一代网络安全领军者

案例回顾

2023年5月，四川雅安公安机关在工作发现本地一预约HPV疫苗平台被黑客破坏，导致大量HPV疫苗资源被黑客非法预约给他人。经查，陈某某等人长期利用黑客技术手段，非法获取“分布在国内18个省、47个市的卫健委HPV疫苗预约平台加密传输的数据包，并对其进行解密、分析后，配置到自己编写的程序中，通过配置用户信息，在未经官方授权情况下伪造数据包，绕过官方后台服务器安全策略，以毫秒级间隔向服务器发送预约疫苗指令，为用户提高疫苗预约几率。

2023年5月，雅安公安机关对该系列案集中收网，抓获犯罪嫌疑人36人，涉案金额1000余万元。

法律链接

据《刑法》相关要求：侵入计算机信息系统或者采用其他技术手段，获取该计算机信息系统中存储、处理或者传输的数据，或者对该计算机信息系统实施非法控制，都应得到相应处罚。

据《网络安全法》相关要求：任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息。

据《数据安全法》相关要求：任何组织、个人收集数据，应当采取合法、正当的方式，不得窃取或者以其他非法方式获取数据。

违法/犯罪 主体	黑产团伙
违法/犯罪 性质	破坏系统、窃取数据
所属行业	医疗卫生
影响范围	公众利益
关键词	利用黑客技术破坏系统
触犯法条	《刑法》第二百八十五条 《网络安全法》第二十一条 《数据安全法》第三十二条
机构责任	未履行安全保护义务
涉及领域	数据安全

某医院数据保护不力造成数据泄露

安全内参 网络安全首席知识官

奇安信 新一代网络安全领军者

案例回顾

2023年6月，衡南县网信办在省、市网信办的指导下，对违反《数据安全法》的相关单位及责任人作出行政处罚。衡南县某医院未履行数据安全保护义务，造成部分数据泄露，违反《中华人民共和国数据安全法》第二十九条规定。衡南县网信办依据《中华人民共和国数据安全法》第四十五条规定，对该医院作出责令整改，给予警告，并处罚款5万元的行政处罚。同时，对第三方技术公司及相关责任人处以1.2万元罚款。

法律链接

据《数据安全法》相关要求：开展数据处理活动应当加强风险监测，发现数据安全缺陷、漏洞等风险时，应当立即采取补救措施；发生数据安全事件时，应当立即采取处置措施，按照规定及时告知用户并向有关主管部门报告。

违法/犯罪 主体	政企机构
违法/犯罪 性质	建设运维管理疏失
所属行业	医疗卫生
影响范围	公众利益
关键词	数据保护不力
触犯法条	《数据安全法》第二十九条
机构责任	未履行安全保护义务
涉及领域	数据安全

某医院未落实等保三级要求被处罚

安全内参 网络安全首席知识官

奇安信 新一代网络安全领军者

案例回顾

2023年7月，广州某医院建设运营的“电子病历EMR系统”确定为等保三级网络，并于2020年6月按规定到公安机关进行了网络安全等级保护备案。但该系统自投入运行以来，医院一直未按规定对其安全等级状况开展等级保护测评，经公安机关督促整改后仍未进行改正，且医院的相关负责人员对该信息系统的安全情况完全不了解、不清楚，更没有对系统安全风险及时进行排查整改，未落实网络安全等级保护制度，未履行网络安全保护义务，违反了《信息安全等级保护管理办法》第十四条之规定。

广州警方对该医院作出行政处罚，并责令其限期改正。

法律链接

据《信息安全等级保护管理办法》相关要求：信息系统建设完成后，运营、使用单位或者其主管部门应当选择符合本办法规定条件的测评机构，定期对信息系统安全等级状况开展等级测评。第三级信息系统应当每年至少进行一次等级测评。

违法/犯罪 主体	医院
违法/犯罪 性质	建设运维管理疏失
所属行业	医疗机构
影响范围	公众利益
关键词	未按照规定开展等保测评
触犯法条	《信息安全等级保护管理办法》第十四条
机构责任	未履行安全保护义务
涉及领域	数据安全

某医院护工出售“死者”信息获利

安全内参 网络安全首席知识官

奇安信 新一代网络安全领军者

案例回顾

2023年9月，广州市荔湾区人民法院公布了一起侵犯公民个人信息罪案件，两名医院护工利用工作便利出售死亡患者个人信息获利10万余元，最终被依法判刑。

易某和唐某是广州某医院护工，两人利用工作便利，在跟随医院救护车急救过程中，未经同意擅自将包括急救病人及丧者家属的居住住址、联系方式等公民个人信息，分别按照每条1000元、2000元的价格非法出售给某殡葬服务公司实际控制人劳某（另案处理）。经统计，易某先后违法获利87000元，唐某违法获利合计25000元。

法律链接

据《个人信息保护法》相关要求：任何组织、个人不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息；

据《网络安全法》相关要求：任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息。

违法/犯罪 主体	内部人员
违法/犯罪 性质	出售公民信息
所属行业	医疗卫生
影响范围	个人利益
关键词	非法提供个人信息
触犯法条	《刑法》第二百五十三条之一 《网络安全法》第四十四条
机构责任	未履行法定安全保护义务
涉及领域	个人信息

某医检机构不履行数据安全保护义务

安全内参 网络安全首席知识官

奇安信 新一代网络安全领军者

案例回顾

2023年9月，江苏宿迁公安网安部门对当地某医学检验机构检查时发现，该机构运营的医学检验信息平台存在SQL注入漏洞、弱口令等网络安全隐患，且未建立数据安全管理制度，未组织数据安全教育培训，未采取相应技术措施保障数据安全，未对其数据处理活动开展风险监测和定期风险评估，可致敏感业务数据泄露，涉嫌未履行数据安全保护义务。宿迁公安机关依据《数据安全法》第四十五条规定，对该机构予以行政警告并处罚款10万元。

法律链接

据《数据安全法》相关要求：开展数据处理活动应当依照法律、法规的规定，建立健全全流程数据安全管理制度，组织开展数据安全教育培训……

据《个人信息保护法》相关要求：发生或者可能发生个人信息泄露、篡改、丢失的，个人信息处理者应当立即采取补救措施……

据《网络安全法》相关要求：网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险。

违法/犯罪 主体	医院
违法/犯罪 性质	建设运维管理疏失
所属行业	医疗卫生
影响范围	公众利益
关键词	平台存在安全隐患
触犯法条	《数据安全法》第二十七、二十九、四十五条 《个人信息保护法》第五十七条 《网络安全法》第二十五条
机构责任	未履行安全保护义务
涉及领域	数据安全

某医药公司不履行数据安全保护义务

安全内参 网络安全首席知识官

奇安信 新一代网络安全领军者

案例回顾

2023年9月，江苏盐城公安网安部门在对当地某医药公司检查时发现，该公司医疗健康信息的会员管理系统存有大量公民个人信息，经现场检测发现该系统存在网络安全漏洞，且该公司未建立数据安全管理制度，未组织开展数据安全教育培训，也未采取相应技术措施保障数据安全，涉嫌未履行数据安全保护义务。

盐城公安机关依据《数据安全法》，对该公司予以行政警告并责令限期改正。

法律链接

据《数据安全法》相关要求：开展数据处理活动应当依照法律、法规的规定，建立健全全流程数据安全管理制度……

据《网络安全法》相关要求：网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险。

据《个人信息保护法》相关要求：个人信息处理者应当对其个人信息处理活动负责，并采取必要措施保障所处理的个人信息的安全。

违法/犯罪 主体	医院
违法/犯罪 性质	建设运维管理疏失
所属行业	医疗卫生
影响范围	公众利益
关键词	存在网络安全漏洞
触犯法条	《数据安全法》第二十七、二十九、四十五条 《网络安全法》第二十五条 《个人信息保护法》第九条
机构责任	未履行安全保护义务
涉及领域	数据安全

某大药房违反数据安全法被罚百万

安全内参 网络安全首席知识官

奇安信 新一代网络安全领军者

案例回顾

2023年10月，浙江温州公安网安部门查处了一起某大药房“内鬼”侵犯公民个人信息案。温州网安部门在日常工作中发现有人在暗网上售卖温州某大药房销售数据。通过侦查发现，该大药房数据分析师利用工作便利将大量交易数据导出并售卖。同时，该大药房也因未履行数据保护义务造成数据泄露的违法行为被公安机关罚款110万元

法律链接

据《刑法》相关要求：向他人出售或者提供公民个人信息，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。

据《数据安全法》相关要求：开展数据处理活动应当依照法律、法规的规定，建立健全全流程数据安全管理制度……

据《网络安全法》相关要求：网络运营者防止网络数据泄露或者被窃取、篡改。

违法/犯罪 主体	内部人员
违法/犯罪 性质	窃取数据
所属行业	医疗卫生
影响范围	公众利益
关键词	数据保护不力
触犯法条	《刑法》第二百五十三条之一 《数据安全法》第二十七、第二十九条 《网络安全法》第二十一条
机构责任	未履行安全保护义务
涉及领域	数据安全

安全内参
网络安全首席知识官

奇安信
新一代网络安全领军者

行业：IT信息技术

IT信息技术行业综述

安全内参 网络安全首席知识官

奇安信 新一代网络安全领军者

- 本次报告共收录IT信息技术相关企业网络安全执法典型案例8起。
- 所谓“IT信息技术”行业，主要是指从事软件、系统、IT服务的开发、运营工作的相关企业，其产品与服务主要服务于各类政企机构和互联网企业。一旦其开发的产品或系统存在安全漏洞或运营疏失，就很容易造成数据泄露，危害公民个人信息安全。
- 本次报告收录的8个典型案例，均与数据泄露有关。其中，仅一起案例是涉事企业存在风险，但数据尚未被证实泄露。而另外7起事件，均为已经发生较大规模数据泄露，而遭到查处。
- 被处罚的企业普遍存在：未建立健全全流程数据安全管理制度、未组织开展数据安全教育培训、未采取相应的技术措施和其他必要措施、未对其数据处理活动开展风险监测等问题。
- 相关机构被处罚的主要依据是《数据安全法》,涉事机构的罚款金额主要集中在5万元到10万元之间。其中1起案例，有相关责任人个人被罚款1万元。
- 本章节的信息来源为《安全内参》：https://www.secrss.com/

某科技公司泄露个人信息被罚款

安全内参 网络安全首席知识官

奇安信 新一代网络安全领军者

案例回顾

2023年1月，网信衡阳发文，北京某科技公司开发的应用网站数据库存在未授权访问漏洞，泄露了大量公民的个人信息。经查，该公司开发了一家教学网站，收集存储了包含用户姓名、手机号、电子邮箱在内的大量个人信息。但该公司未建立健全全流程数据安全管理制度，未组织开展数据安全教育培训，未采取相应的技术措施和其他必要措施，保障数据安全，并因安全漏洞造成个人信息泄露等问题。

衡阳市网信办依据《数据安全法》第四十五条有关规定，对该科技公司作出责令改正，给予警告，并处人民币10万元罚款的行政处罚。

法律链接

据《数据安全法》相关要求：开展数据处理活动应当依照法律、法规的规定，建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全。开展数据处理活动应当加强风险监测，……

据《网络安全法》相关要求：网络运营者应当防止网络数据泄露或者被窃取、篡改。

据《个人信息保护法》相关要求：发生或者可能发生个人信息泄露、篡改、丢失的，个人信息处理者应当立即采取补救措施……

违法/犯罪 主体	企业
违法/犯罪 性质	建设运维管理疏失
所属行业	IT信息技术
影响范围	公众利益
关键词	数据保护不力
触犯法条	《数据安全法》第二十七、二十九、四十五条 《网络安全法》第二十一条 《个人信息保护法》第五十七条
机构责任	未履行安全保护义务
涉及领域	数据安全

某生物技术公司泄露数据被处罚

安全内参 网络安全首席知识官

奇安信 新一代网络安全领军者

案例回顾

2023年6月，公安部网安局发文，昌平网安部门检查发现，昌平某生物技术有限公司存在数据泄漏的情况，其委托的另一软件公司研发的“基因外显子数据分析系统”，泄露了包含公民信息、技术等信息，涉及泄漏数据总量达19.1GB。经检查，该软件公司在开发系统互联网测试阶段，未对相关数据进行加密，未落实安全保护措施，属于未履行数据安全保护义务。北京市公安局昌平分局依据《数据安全法》第四十五条第一款规定，给予警告并处罚款5万元的行政处罚。

法律链接

据《数据安全法》相关要求：开展数据处理活动应当依照法律、法规的规定，建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全。开展数据处理活动应当加强风险监测，……

据《网络安全法》相关要求：网络运营者应当防止网络数据泄露或者被窃取、篡改。

据《个人信息保护法》相关要求：发生或者可能发生个人信息泄露、篡改、丢失的，个人信息处理者应当立即采取补救措施，并通知履行个人信息保护职责的部门和个人。

违法/犯罪 主体	企业
违法/犯罪 性质	建设运维管理疏失
所属行业	IT信息技术
影响范围	公众利益
关键词	数据保护不力
触犯法条	《数据安全法》第二十七，二十九、四十五条 《网络安全法》第二十一条 《个人信息保护法》第五十七条
机构责任	未履行安全保护义务
涉及领域	数据安全

某市两公司存在数据泄露隐患被处罚

安全内参 网络安全首席知识官

奇安信 新一代网络安全领军者

案例回顾

2023年6月，北京朝阳网安部门接市公安局网安总队通报，辖区某科技公司存在数据泄露隐患，分局迅速组织相关力量前往该科技公司进行现场网络安全检查。

经工作发现，该科技公司一款APP产品后台存储的客户姓名、手机号、微信账号、邮箱等信息46万余条数据被暴露在互联网上，该数据一旦被不法分子获取，将导致大量公民个人信息泄露，给广大人民群众个人合法权益造成重大影响。

法律链接

据《数据安全法》相关要求：开展数据处理活动应当依照法律、法规的规定，建立健全全流程数据安全管理制度……开展数据处理活动应当加强风险监测，发现数据安全缺陷、漏洞等风险时，应当立即采取补救措施。

据《网络安全法》相关要求：网络运营者应当防止网络数据泄露或者被窃取、篡改。

违法/犯罪 主体	企业
违法/犯罪 性质	建设运维管理疏失
所属行业	IT信息技术
影响范围	公众利益
关键词	数据保护不力
触犯法条	《数据安全法》第二十七条 《网络安全法》第二十一条
机构责任	未履行安全保护义务
涉及领域	数据安全

某企业因泄露大量数据被处罚

安全内参 网络安全首席知识官

奇安信 新一代网络安全领军者

案例回顾

2023年7月，网信重庆发文，渝中区网信办依法对属地一科技公司涉数据泄露等违法违规行为进行立案查处，作出责令限期五日改正，给予行政警告，并处10万元罚款的行政处罚。经查，该公司开发运营的某OA信息系统因未履行好网络数据安全保护义务，导致大量数据泄露，情节严重。且该公司作为网络数据处理者，未依法建立健全全流程网络数据安全管理制度，未依法组织开展网络数据安全教育培训，未采取相应的技术措施和其他必要措施等保障网络数据安全。

法律链接

据《数据安全法》相关要求：开展数据处理活动应当依照法律、法规的规定，建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全。开展数据处理活动应当加强风险监测，……

据《网络安全法》相关要求：网络运营者应当防止网络数据泄露或者被窃取、篡改。

据《个人信息保护法》相关要求：发生或者可能发生个人信息泄露、篡改、丢失的，个人信息处理者应当立即采取补救措施，并通知履行个人信息保护职责的部门和个人。

违法/犯罪 主体	企业
违法/犯罪 性质	建设运维管理疏失
所属行业	IT信息技术
影响范围	公众利益
关键词	数据保护不力
触犯法条	《数据安全法》第二十七，二十九、四十五条 《网络安全法》第二十一条 《个人信息保护法》第五十七条
机构责任	未履行安全保护义务
涉及领域	数据安全

某科技公司未履行数据安全保护义务

安全内参 网络安全首席知识官

奇安信 新一代网络安全领军者

案例回顾

2023年9月，公安部网安局发文，江苏苏州公安网安部门工作发现，成都某科技有限公司在为苏州某信息科技股份有限公司相关系统运维过程中，未建立健全全流程数据安全管理制度，为图工作方便，私自将该公司30余万条运营数据上传至互联网，且未落实任何技术防护措施保障数据安全，未对其数据处理活动开展风险监测，可致该批数据泄露，涉嫌未履行数据安全保护义务。苏州公安机关依据《数据安全法》第四十五条规定，对该公司予以行政警告并处罚款5万元。

法律链接

据《数据安全法》相关要求：开展数据处理活动应当依照法律、法规的规定，建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全……。开展数据处理活动应当加强风险监测，发现数据安全缺陷、漏洞等风险时，应当立即采取补救措施；发生数据安全事件时，应当立即采取处置措施，按照规定及时告知用户并向有关主管部门报告。

据《网络安全法》相关要求：网络运营者应当防止网络数据泄露或者被窃取、篡改。

违法/犯罪 主体	企业
违法/犯罪 性质	建设运维管理疏失
所属行业	IT信息技术
影响范围	公众利益
关键词	有数据泄露风险
触犯法条	《数据安全法》第二十七，二十九、四十五条《网络安全法》第二十一条
机构责任	未履行安全保护义务
涉及领域	数据安全

某科技公司未履行数据安全保护义务

安全内参 网络安全首席知识官

奇安信 新一代网络安全领军者

案例回顾

2023年10月，浙江省网信办依法对杭州某科技公司未履行数据安全保护义务的问题进行立案调查。经查实，该公司旗下某生活类APP相关数据库服务端口直接暴露在互联网环境中，存在未授权访问漏洞，未按要求履行数据安全保护义务，违反《数据安全法》第二十七条之规定。浙江省网信办依据《数据安全法》等法律法规，对杭州某科技公司作出罚款5万元的行政处罚，对该公司直接负责人作出罚款1万元的行政处罚。

法律链接

据《数据安全法》相关要求：开展数据处理活动应当依照法律、法规的规定，建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全。利用互联网等信息网络开展数据处理活动，应当在网络安全等级保护制度的基础上，履行上述数据安全保护义务。

据《网络安全法》相关要求：网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险。

违法/犯罪 主体	企业
违法/犯罪 性质	建设运维管理疏失
所属行业	IT信息技术
影响范围	公众利益
关键词	存在漏洞
触犯法条	《数据安全法》第二十七、四十五条 《网络安全法》第二十五条
机构责任	未履行安全保护义务
涉及领域	数据安全

某企业疑似发生删库勒索事件

安全内参 网络安全首席知识官

奇安信 新一代网络安全领军者

案例回顾

2023年10月，南昌市网信办通报，南昌县某企业存在数据漏洞风险，疑似出现删库勒索事件。经查，该企业运营的mongodb数据库存在未授权访问安全漏洞；该企业未采取相应的技术措施和其他必要措施保障数据安全，其运营的数据库被黑客删库并勒索；该企业未加强风险监测，发生删库勒索事件时未采取处置措施和履行主动报告义务。南昌市网信办依据《数据安全法》第四十五条的规定，对该企业作出警告并处罚款5万元、对直接负责的主管人员作出罚款1万元的行政处罚。

法律链接

据《网络安全法》相关要求：网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险。

据《数据安全法》相关要求：开展数据处理活动应当依照法律、法规的规定，建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全。开展数据处理活动应当加强风险监测，……

违法/犯罪 主体	企业
违法/犯罪 性质	建设运维管理疏失
所属行业	IT信息技术
影响范围	公众利益
关键词	数据保护不力
触犯法条	《网络安全法》第二十五条 《数据安全法》第二十七条、二十九条
机构责任	未履行安全保护义务
涉及领域	数据安全

某科技公司因数据库存在漏洞处罚

安全内参 网络安全首席知识官

奇安信 新一代网络安全领军者

案例回顾

2023年11月，网信上海发文，网信机构在工作中发现，某科技公司一台用于存储业务日志和大量个人信息的数据库服务器，因存在未授权访问漏洞，导致部分数据被窃并传输到境外。同时企业私自删除涉事数据库逃避责任，没有按照规定及时向网信部门报告，未有效履行数据安全保护义务。

上海市网信办依据《数据安全法》第二十七条、第四十五条，对该科技公司作出责令改正，给予警告，并处人民币8万元罚款的行政处罚；对公司直接责任人员作出罚款人民币1万元的行政处罚。

法律链接

据《数据安全法》相关要求：开展数据处理活动应当依照法律、法规的规定，建立健全全流程数据安全管理制度。开展数据处理活动应当加强风险监测，……

据《网络安全法》相关要求：网络运营者应当防止网络数据泄露或者被窃取、篡改。

据《个人信息保护法》相关要求：发生或者可能发生个人信息泄露、篡改、丢失的，个人信息处理者应当立即采取补救措施，并通知履行个人信息保护职责的部门和个人。

违法/犯罪 主体	企业
违法/犯罪 性质	建设运维管理疏失
所属行业	IT信息技术
影响范围	公众利益
关键词	泄露数据后删库
触犯法条	《数据安全法》第二十七条，四十五条 《网络安全法》第二十一条 《个人信息保护法》第五十七条
机构责任	未履行安全保护义务
涉及领域	数据安全

安全内参
网络安全首席知识官

奇安信
新一代网络安全领军者

行业：生活服务

生活服务行业综述

安全内参 网络安全首席知识官

奇安信 新一代网络安全领军者

- 本次报告共收录2023-2024年生活服务类企业网络安全执法典型案例4起。
- 相比于其他行业，生活服务类企业的网络安全建设与运营水平极其低下，普遍存在用户信息明文存储、办公终端与服务器裸奔、超级管理员账号随意发放等情况，导致电脑被黑客入侵和窃取数据非常的容易。
- 由于生活服务类企业，很多都是中小企业，甚至是小微企业，我们不可能要求他们像大企业一样进行系统性的网络安全建设。但是，安全意识的提升仍然是非常必要的。例如，为存储用户信息的文件加设密码，管理员权限要严格控制并且避免设置弱口令等，这些简单的要求就可以大大提升此类企业的网络安全管理水平。
- 在这四起案例中，有一起涉及黑产团伙与企业员工内外勾结，传播木马病毒，并窃取客户个人信息的典型案例。这与生活服务类企业人员流动性强，人员管理松散不无关系。
- 本章节的信息来源为《安全内参》：https://www.secrss.com/

某汽车4S店电脑被安装远程木马软件

安全内参 网络安全首席知识官

奇安信 新一代网络安全领军者

案例回顾

2023年1月，浙江省余姚某汽车4S店电脑被安装远程木马软件，导致客户信息泄露。余姚警方立即开展侦查，锁定该4S店内部工作人员潘某有重大作案嫌疑，并查明以李某虎为首的非法获取计算机信息系统数据犯罪团伙。4月11日，余姚警方组织警力赴安徽六安、江苏镇江等6省26地抓获李某虎、张某、黎某等犯罪嫌疑人38名，扣押电脑43台、手机75部、银行卡200余张，冻结资金100余万元，涉案资金达5000余万元。

法律链接

据《刑法》相关要求：故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行，后果严重的，应当得到处罚。

据《网络安全法》相关要求：网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失……

据《数据安全法》相关要求：开展数据处理活动应当依照法律、法规的规定，建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全。

违法/犯罪 主体	内部人员、黑产团伙
违法/犯罪 性质	传播病毒、窃取数据
所属行业	生活服务
影响范围	公众利益
关键词	泄露客户信息
触犯法条	《刑法》第二百八十六条 《网络安全法》第四十二条 《数据安全法》第二十七条
机构责任	未履行安全管理义务
涉及领域	个人信息

某足浴店用户信息未加密被责令整改

安全内参 网络安全首席知识官

奇安信 新一代网络安全领军者

案例回顾

2023年8月，江苏省淮安市公安局淮阴分局西坝派出所的两位民警依法对一家足浴会所进行检查，发现该场所的电脑存储有顾客姓名、手机号码、身份证号码等敏感数据且未设置密码，未制定数据安全管理制度，未采取必要措施保障数据安全。根据《数据安全法》第二十七条、第二十九条、第三十条、第四十五条之规定，决定对 该 足疗会所处以责令整改、警告的行政处罚。

法律链接

据《数据安全法》相关要求：开展数据处理活动应当依照法律、法规的规定，建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全 。 开展数据处理活动应当加强风险监测，发现数据安全缺陷、漏洞等风险时，应当立即采取补救措施。重要数据.....

据《网络安全法》相关要求：网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失.....

违法/犯罪 主体	企业
违法/犯罪 性质	建设运维管理疏失
所属行业	生活服务
影响范围	公众利益
关键词	数据保护不力
触犯法条	《数据安全法》第二十七，二十九，三十、四十五条《网络安全法》第四十二条
机构责任	未履行安全管理义务
涉及领域	违规整改

某火锅店数据保护不力被处罚

安全内参 网络安全首席知识官

奇安信 新一代网络安全领军者

案例回顾

2024年1月29日，上海市网信办通报，已依法对一批未有效履行消费者个人信息保护责任、存在严重问题的知名企业予以行政处罚。某 知名火锅连锁品牌违法违规行为集中体现在两个环节：在收集个人信息环节，其外送微信小程序仍在强制索取精准位置信息；在存储个人信息环节，其创设近30年来形成的1.5亿条会员个人信息以及18万条公司员工信息未加密存储，多年来一直处于‘裸奔’状态”；运营管理平台的“超级管理员”账号竟然高达20余个。

法律链接

据《数据安全法》相关要求：任何组织、个人收集数据，应当采取合法、正当的方式，不得窃取或者以其他非法方式获取数据。开展数据处理活动应当依照法律、法规的规定，建立健全全流程数据安全管理制度……

据《网络安全法》相关要求：网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失……

据《个人信息保护法》相关要求：个人信息处理者应当采取相应的加密、去标识化等安全技术措施……

违法/犯罪 主体	企业、内部人员
违法/犯罪 性质	建设运维管理疏失
所属行业	生活服务
影响范围	公众利益
关键词	未对敏感信息进行加密
触犯法条	《数据安全法》第二十七条，第三十二条 《网络安全法》第四十二条 《个人信息保护法》第五十一条
机构责任	未履行安全保护义务
涉及领域	数据安全

某超市电脑遭黑客远控变“肉鸡”

安全内参 网络安全首席知识官

奇安信 新一代网络安全领军者

案例回顾

2024年2月，南昌市网信办在日常的网络安全监测中发现，属地某连锁超市所属IP疑似被黑客远控，频繁对外发起网络爆破攻击。经过立案调查、现场勘验、远程勘验（采样技术分析）、笔录问询等工作，查明：所属的服务器和多台终端感染木马病毒；该连锁超市未及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险， 导致 所属网络持续对内对外发起大规模网络攻击，导致产生危害网络安全的后果。

南昌市网信办依据《网络安全法》，对该连锁超市作出罚款5万元、对直接负责的主管人员作出罚款1万元的行政处罚。

法律链接

据《网络安全法》相关要求：网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险，在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。

违法/犯罪 主体	企业
违法/犯罪 性质	建设运维管理疏失
所属行业	生活服务
影响范围	公众利益
关键词	远程控制
触犯法条	《网络安全法》第二十五、五十九
机构责任	未履行安全保护义务
涉及领域	数据安全

奇安信
新一代网络安全领军者

安全内参
网络安全首席知识官

谢谢
Thanks!

让网络更安全 让世界更美好