LINKS Law Offices
通力律师事务所

上海
上海市银城中路 68 号
时代金融中心 16/19 楼
电话: +86 21 3135 8666
传真: +86 21 3135 8600

北京
北京市建国门北大街 8 号
华润大厦 4 楼
电话: +86 10 8519 2266
传真: +86 10 8519 2929

香港
香港中环皇后大道中 5 号
衡怡大厦 27 楼
电话: +852 2592 1978
传真: +852 2868 0883

伦敦
1/F, 3 More London
Riverside, London SE1 2RE
T: +44 (0)20 3283 4337
D: +44 (0)20 3283 4323

通力法律评述 | 公司及并购
2020 年 3 月

浅析员工破坏企业信息系统风险及防范

作者：潘永建 | 尹庆 | 沙莎

2020 年 2 月 23 日，微盟研发中心运维部核心运维人员贺某通过个人 VPN 登入公司内网跳板机，对微盟的线上生产环境进行大肆破坏，并对部署在自建数据库上的核心业务数据进行不可逆的删除，导致系统中断 7 天。[1]虽然经过 7 天的数据恢复工作，数据全面找回，但微盟仍然准备人民币 1.5 亿元赔付拨备金赔偿给商户。[2]

“微盟删库”事件表明，破坏计算机信息系统的行为一旦发生，企业必将面临经济损失，日常生产经营也会受到影响，甚至遭受破坏性打击。本文结合相关法律规定与案例，对员工破坏企业信息系统的风险进行分析，并提出相应的防范建议供企业参考。

一. 破坏计算机信息系统罪概述

我国已经针对破坏计算机信息系统的行为进行立法，较为常见的罪名是《刑法》中的破坏计算机系统罪，其行为模式主要有以下三种类型:

如您需要了解我们的出版物，
请联系:

Publication@llinkslaw.com

[1] https://mp.weixin.qq.com/s/MFhnc4qPpxxxZY1O-uTk1g，最后访问时间为 2020 年 3 月 16 日。
[2] https://mp.weixin.qq.com/s/vZP5JHnjUk8GcwXahqflBw 最后访问时间为 2020 年 3 月 16 日。

	行为	对象	后果
1	删除、修改、增加、干扰	计算机系统功能	造成计算机信息系统不能正常运行，后果严重，或者后果特别严重
2	删除、修改、增加	计算机信息系统中存储、处理或者传输的数据和应用程序	后果严重，或者后果特别严重
3	故意制作、传播计算机病毒等破坏性程序	计算机系统(功能、数据、应用程序)	影响计算机系统正常运行，后果严重

《关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释》(法释〔2011〕19 号，以下简称"《解释》")对破坏计算机信息系统行为中的"后果严重"[3]"后果特别严重"，[4] 从计算机系统的损害数量、损失金额、损害行为及损害时间、行业及社会影响等方面进行了解释，并提供了具体的判断标准。另外，该罪的犯罪主体既可以是个人，也可以是单位，以单位名义或者单位形式实施危害计算机信息系统安全的犯罪，将追究直接负责的主管人员和其他直接责任人员的刑事责任。该罪的主观方面仅由故意构成，过失不构成犯罪，即行为人明知自己的行为会发生破坏计算机信息系统的后果，仍然希望或者放任这种危害结果的发生。

破坏计算机信息系统的行为，除了可能构成《刑法》中破坏计算机信息系统罪外，根据行为人侵害的客体和目的不同，还可能构成其他罪名[5]。此外，对于未达到追诉标准的行为，执法机关依然可以根据《治安管理处罚法》[6]《计算机信息系统安全保护条例》等法律法规追究行为人的法律责任。

二. 企业员工破坏计算机系统常见行为

1. 在职员工

(1) 员工为了自身利益修改数据的行为[7]

【案情】屈某利用工作期间处理某游戏玩家投诉问题时获得的后台管理员权限账户，采用登录后台修改服务器数据的方式，对五个游戏账号进行生成游戏道具操作，生成该游戏中的道具共计 16 亿个，折算价值约 569 万元人民币。之后，屈某通过游戏将私自生成的游戏道具兑换为游戏金币，通过网络销售给他人，销售获利 130 余万元人民币。

[3]"后果严重"是指: 1)造成十台以上计算机信息系统的主要软件或者硬件不能正常运行的; 2)对二十台以上计算机信息系统中存储、处理或者传输的数据进行删除、修改、增加操作的; 3)违法所得五千元以上或者造成经济损失一万元以上的; 4)造成为一百台以上计算机信息系统提供域名解析、身份认证、计费等基础服务或者为一万以上用户提供服务的计算机信息系统不能正常运行累计一小时以上的; 5)造成其他严重后果的。

[4] "后果特别严重"是指: 1)数量或者数额达到前款第(一)项至第(三)项规定标准五倍以上的; 2)造成为五百台以上计算机信息系统提供域名解析、身份认证、计费等基础服务或者为五万以上用户提供服务的计算机信息系统不能正常运行累计一小时以上的; 3)破坏国家机关或者金融、电信、交通、教育、医疗、能源等领域提供公共服务的计算机信息系统的功能、数据或者应用程序，致使生产、生活受到严重影响或者造成恶劣社会影响的; 4)造成其他特别严重后果的。

[5] 包括非法侵入计算机信息系统罪，非法获取计算机信息系统数据、非法控制计算机信息系统罪，提供侵入、非法控制计算机信息系统程序、工具罪等。

[6] 《治安管理处罚法》第二十九条

[7] (2018)粤 0305 刑初 1379 号

【点评】本案法院以职务侵占罪对屈某定罪处罚。在司法实践中，破坏计算机系统罪与其他罪名竞合的情况时有发生，《刑法》亦规定利用计算机实施金融诈骗、盗窃、贪污等其他犯罪时，应按照相应罪名进行处罚。[8]

(2) 员工为了企业利益修改数据的行为[9]

【案情】2018 年 7 月 2 日，某焦化有限公司环保联络员方某，发现其公司的 SCS-900C 烟气排放连续监测系统二氧化硫的实时上传数据超过国家标准 50 毫克/立方米，遂进入公司机房将工控机上的二氧化硫量程参数改至达标后上传。之后，方某又两次发现其公司的上述数据超标，并授意公司员工汪某进入在线监测设备机房将相关参数改至达标后上传。两人企图使公司逃避环境污染责任并修改数据的行为被认定为破坏计算机信息系统罪。

【点评】根据 2016 年《关于办理环境污染刑事案件适用法律若干问题的解释》(法释〔2016〕29 号，以下简称"《环境污染司法解释》")，修改参数或监测数据、干扰采样致使数据严重失真等破坏环境检测系统的行为按破坏计算机系统罪定罪；但重点排污单位实施上述行为，排放化学需氧量、氨氮、二氧化硫、氮氧化物等污染物，同时构成污染环境罪和破坏计算机信息系统罪的，依照处罚较重的规定定罪处罚，对实施上述行为的环境监测设施维护、运营人员从重处罚。[10]本案某焦化有限公司属于废气重点监控排污单位，是《环境污染司法解释》中环境污染罪的适格主体。重点排污企业主管人员以及环境监测人员破坏环境监测系统的行为可能同时构成污染环境罪、破坏计算机系统罪，其违法行为将面临刑期更高、刑罚更重的处罚。

2. 离职员工行为

(1) 离职员工利用公司管理缺陷破坏系统[11]

【案情】张某原系北京某信息技术有限公司数据库开发工程师，负责维护两家饮品公司的全国实时经销商零售管理系统。因不满公司的辞退决定，在离开公司前，张某利用工作期间使用的公司运维账户分别登录饮品公司的终端管理系统数据库服务器创建恶意定时任务脚本。该脚本被设置为每日执行，半个月后该脚本成功清除了两台服务器主机上的 Oracle 相关磁盘内容，并删除脚本自身，导致磁盘头损坏，造成两家饮品公司终端管理系统瘫痪，停止服务时间长达半月之久。

【点评】离职员工利用公司管理缺陷破坏计算机系统的案例屡见不鲜，出于报复、牟利甚至"恶搞"心理对公司服务器进行破坏，可能造成较大损失。在部分案例中，还存在员工在职期间在系统中嵌入"后门"程序以便离职后作案的行为。[12]应对这一可能的风险，公司应加强对账户和密码的管理，对系统权限的分配做到最小范围授权，在相关人员离职后应立即删

8 《刑法》第二百八十七条
9 (2019)豫 1025 刑初 126 号
10 《关于办理环境污染刑事案件适用法律若干问题的解释》第十条
11(2018)冀 0525 刑初 32 号
12 (2019)鲁 0203 刑初 217 号

除其在所有系统中的权限，同时应提醒员工在工作中使用密码登录时应注意保密，以防被他人通过不正当手段获得并恶意利用。

(2) 离职员工使用第三方软件删除公司数据库[13]

【案情】王某因与某动画制作有限公司存在劳资纠纷而心存不满，离职后使用“向日葵”远程控制软件登录该公司的服务器，删除了该服务器上存储的全部动画剧集、动画素材等数据，造成该公司长达 14 日无法正常工作。该公司称，王某行为导致的停产停业损失为人民币 4 万元，且公司可能因数据丢失而承担人民币 1000 万元的违约金。公诉机关以王某删除的 26 集动画片制作费为依据，指控王某造成财物损失为人民币 60 余万元；但法院最终仅认定损失金额为人民币 4 万元，即公司停产停业损失。

【点评】在经济损失认定方面，公司要求的经济赔偿与法院支持的实际损失相比相差甚远，主要原因可能有三:
第一，很难举证说明员工的行为是公司损失形成的唯一因素，存在举证难的困境。
第二，公司实际的损失与刑事法律认定的经济损失存在差别。《解释》指出，经济损失是指包括危害计算机信息系统犯罪行为给用户直接造成的经济损失，以及用户为恢复数据、功能而支出的必要费用。[14]根据上述规定，若干实际支出或成本将不被列入“经济损失”。例如，司法机关调查确定作案人的费用不属于直接经济损失。[15]
第三，公司潜在损失的金额不确定，故其无法要求作案人进行赔偿。

三. 风险防范建议

以上，笔者仅列举破坏计算机系统罪中较常见的几种手法。 实践中，破坏计算机系统的表现形式更为多样化。不同类型的企业、不同的计算机系统以及应用程序中的风险点有所不同，企业要根据自身的特点开展防范工作。通过对不同作案手法的总结，我们提出以下防范建议:

1. 有针对性地对员工特别是公司系统运营维护管理人员进行培训和普法教育，使之认识到破坏计算信息系统行为将会面临的处罚;
2. 建立有效的合规制度，鼓励、要求员工发现不正当行为时及时进行报告;
3. 加强对离职人员权限的管理，争取做到离职之日权限即取消，避免离职员工因对公司不满而恶意对计算机系统等进行破坏；同时，对离职前可操作接触企业核心业务信息系统的员工进行技术离职审计，追踪离职前对系统进行的操作，防止预置木马程序等风险;[16]
4. 建立业务持续性计划，当公司的核心系统受到损坏时确保备用系统可以及时启动，减少计算机系统安全风险，降低对公司运营产生的影响;
5. 对企业的核心信息系统，可以实行双人登录制度，减少破坏行为的发生。

[13] (2017)辽 0102 刑初 380 号
[14] 《关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释》第十一条
[15] (2018)京 0108 刑初 651 号
[16] 同时也需关注第三方公司服务过程中第三方公司的员工留“后门”或者直接对数据、应用系统等进行修改或破坏的行为。

如您希望就相关问题进一步交流，请联系：

潘永建
+86 21 3135 8701
david.pan@llinkslaw.com

如您希望就其他问题进一步交流或有其他业务咨询需求，请随时与我们联系：**master@llinkslaw.com**

上海	北京	香港	伦敦
T: +86 21 3135 8666 F: +86 21 3135 8600	T: +86 10 8519 2266 F: +86 10 8519 2929	T: +852 2592 1978 F: +852 2868 0883	T: +44 (0)20 3283 4337 D: +44 (0)20 3283 4323

www.llinkslaw.com

Wechat: LlinksLaw

本土化资源 国际化视野