教职工政治学习参考资料

（2022年第11期）

苏州大学党委宣传部编

2022年11月11日

教职工政治学习参考资料

（2022 年第 11 期）

苏州大学党委宣传部编　　2022 年 11 月 11 日

● 学习内容

网络安全专题学习

● 参考资料

一、2022 网络安全意识培训 1

二、苏州大学《数据安全法》解读及最佳实践..... 32

三、勒索病毒介绍和处置 53

2022
网络安全意识培训

目录

01 工作篇

02 生活篇

03 法律篇

1 工作篇

工作环境

网络边界完整性

要求：
遵守办公场所的管理制度，非工作设备不要接入到办公网络。

原因：

1、非工作设备接入办公网络后，可以访问共享资源，如机密或重要文件等，一旦被恶意修改、拷贝、删除，会形成巨大损失;

2、非工作设备可能携带病毒、木马等，接入局域网后传播给内网的其他电脑，造成恶劣影响;

3、非工作设备若下载文件或者在线游戏、在线视频等，挤占网速，影响正常工作秩序等。

1 工作篇

工作环境

网络边界完整性

要求：
不擅自增加网络设备及节点，如交换机、无线路由器等。

原因：

1、极易被非工作设备接入办公网络；

2、若网络设备存在漏洞或者后门，极易被利用，从而形成内网入侵；

3、无线网络设备若配置和管理不到位，会成为很大的风险点，容易被利用。

1 工作篇

工作环境

隐私数据保存

要求：
打印、传真完毕应立即取走文件。

原因：
如果打印或传真的机密文件没有被及时取走，可能会造成机密信息泄漏，有着巨大的安全隐患。

1 工作篇

工作环境

隐私数据保存

要求：

纸质文件妥善保管，切忌随意放置或丢弃含有敏感信息的纸质文件，废弃文件用碎纸机粉碎。

原因：

如果纸质文件含有敏感信息并随意放置或丢弃，可能会造成机密信息泄漏，有着巨大的安全隐患。

1 工作篇

工作环境

隐私数据保存

要求：
会议期间，禁止未授权的拍照、录音及录像，会后不要遗留重要文件，及时清理会议数据等。

原因：

利用会议讨论的一般都是主要思路、关键结论，这些重要内容如果泄漏给未授权知晓的人员，容易带来安全隐患。

工作环境

办公电脑

要求：
电脑一定要设置开机密码。

方式：

windows系统密码设置，依次使用鼠标点击“开始”菜单中的“控制面板”下的“用户账户”，选 择账户后点击“创建密码”，输入两遍密码后按“创建密码”按钮即可。确保输入的密码具有一 定的复杂度，包含字母、数字和特殊符号等。

工作环境
隐私数据保存

要求：
打开操作系统的自动更新。

方式：

windows系统自动更新设置，依次使用鼠标点击“开始”菜单中的“控制面板”下的“系统和安 全”，选择单击“Windows更新”下的启用或关闭自动更新，在弹出的更改设置对话框，选择重 要更新下拉菜单中的“自动安装更新（推荐）”。新版windows10操作系统强制开启系统更新 功能。

安装的防病毒软件也需要开启自动升级功能。

1 工作篇

工作环境

办公电脑

要求：

不要打开来历不明的网页、电子邮件链接或附件，不要随意接受陌生人的文件。

下载软件时尽量到官方网站或大型软件下载网站，在安装软件或打开来历不明的文件前先杀毒。

原因：

互联网上充斥着各种钓鱼网站、病毒、木马程序。不明来历的网页、电子邮件链接、附件中，很可能隐藏着大量的病毒、木马，一旦打开，这些病毒、木马会自动进入电脑并隐藏在电脑中，会造成文件丢失损坏甚至导致系统瘫痪。

工作环境
办公电脑

要求：
电脑插入移动存储设备时，如移动硬盘、U盘等，首先进行病毒扫描。

原因：
移动存储设备也是信息存储介质，所存的信息很容易带有各种病毒，如果将带有病毒的移动存储设备接入电脑，很容易将病毒传播到电脑中。

工作环境

办公电脑

要求：
临时离开电脑时，一定要将屏幕锁定，避免在离开期间电脑被人恶意利用。

方式：

离开电脑时，同时按下键盘上的Win键和L键即可完成立刻锁屏操作。

目录

01 工作篇

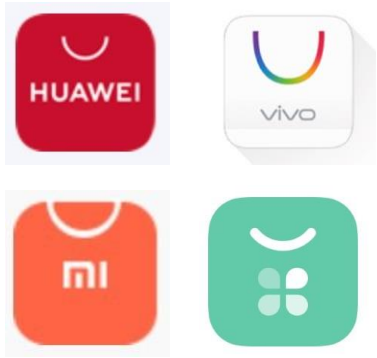
02 生活篇

03 法律篇

2 日常生活篇

移动设备
手机使用

安全要点：
下载应用软件，尽量去系统自带的官方应用商店或应用的官方网站下载，安装应用时，谨慎授予应用所需的权限。



2 日常生活篇

移动设备

手机使用

设置 → 安全 → 禁止安装未知来源应用

移动设备
手机使用

安全要点：
SIM卡设置PIN码，当手机重启或更换手机后必须输入PIN码才能正常使用这个号码。

PIN

- personal identification number

PUK

- PIN unlocking key

移动设备
手机使用

设置 → 电话 → SIM卡PIN码

2 日常生活篇

移动设备
手机使用

安全要点：
苹果手机可以开启双重认证功能，登录AppleID时需要同时输入密码和验证
码。

2 日常生活篇

移动设备

手机使用

安全要点：
谨慎扫描二维码和点击访问短网址。
恶意用户可能将二维码和短网址访问目标设置为木马程序，导致手机面临风险。

http://t.cn/h51HY

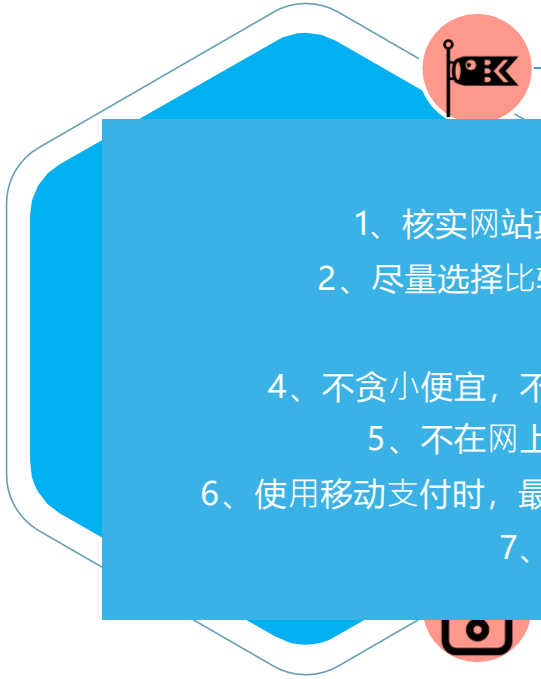
移动设备
手机使用

短网址查询真实网址方式：

- tool.chinaz.com/qrcode
- http://dwz.cn/
- http://sina.lt/

2 日常生活篇

移动设备
网络交易



钓鱼网站

将自己伪装成知名银行或者信用卡公司等可信的品牌，

小贴士：

1、核实网站真伪，尽量到知名、权威的网站购物，仔细甄别，严加防范。

2、尽量选择比较安全的第三方支付平台担保交易，切忌直接与卖家私下交易。

3、注意商家的信誉、评价和联系方式。

4、不贪小便宜，不要轻信网上低价推销广告，也不要随意点击未经核实的陌生链接。

5、不在网上购买非正当产品，如手机监听器、毕业证书、考题答案等。

6、使用移动支付时，最好绑定II类或II类的小额银行账户，以防账户被盗带来较大的资金损失。

7、删除有绑定银行卡的APP时，谨记先解绑银行卡。

访问
出伪
，然

当使用“ 弱密码” 时，且在多个网站上使用相同密码或者有限的几个密码， 容易遭受攻击者暴力破解。

2 日常生活篇

预防诈骗
骗术揭秘

1 **身份冒充**

冒充公检法工作人员拨打电话，以身份信息被盗用、 涉嫌洗钱、贩毒等理由，要求转入“安全账户 “。 冒充单位领导，要求快速转账汇款的指令等。

2 **金钱诱惑**

重金求子，引诱上当后，以检查费、诚意金等行骗。 高薪招聘，指定地点面试，交培训费、服装费，甚至陷 入传销团伙。
网络兼职，以打字员、刷单员为名义，要求缴纳信息费 等。

3 **有奖活动**

发布集赞、转发有奖等虚假活动，要求提供个人信 息，并缴纳保证金、所得税、快递费等。
以热播栏目节目组名义发短信，称被选为幸运观众， 有巨额奖品，要求缴纳所得税、快递费等。

2 日常生活篇

预防诈骗
骗术揭秘

消费退款

以系统卡单、故障、无货等理由，发来虚假退款　网址，如果按照要求填写信息，则支付宝、银行卡中 资产会被迅速转走。

群发假冒银行卡消费短信，以境外大额消费涉嫌　洗钱为由，套取个人信息和银行卡信息，通过第三方 支付的快捷支付进行消费。

以机票改签等，诱骗进行汇款操作。

恶意代码

利用伪基站群发网银升级、积分兑换等虚假链接，　点击后手机被植入木马程序，实施犯罪。

以互联网公司的名义群发短信，包含钓鱼网站链 接，进而获取帐号密码信息，转走帐号中的资金。

其他骗术

在公共场所设置与正规WiFi　类似的山寨免密　WiFi,一旦连接上，通过截取数据传输，轻松获取手机 上各类App的账号密码以及隐私。

骗子用受害者临时身份证办理补卡，同时用骚扰 软件打电话发短信轰炸受害者手机，以掩盖补卡业务提醒短信。然后用补办的手机卡登录网银、第三方支 付等平台，获取验证码盗取账户。

发布信用卡提额、低息贷款等广告，然后以验资、 中介、手续费等名义要求转账。

发布虚假色情服务广告，待有人联系后，称需要先付款保证人身安全才能提供服务 。

2 日常生活篇

移动设备
手机使用

网络防骗“十凡是”

凡是自称公检法等单位要求汇款的;
凡是要求汇款到“ 安全账户” 的;
凡是通知中奖、积分兑换要先交钱的;
凡是通知“ 亲朋好友” 出急事要求汇款的;凡是索要个人和银行卡信息及短信验证码的;
凡是说招聘又轻松、又高薪、还日结工作的;
凡是要求开通网银远程协助接受检查的;
凡是通知网购系统、订单错误需要进行操作的;
凡是自称领导要求突然汇款的;
凡是陌生网站要求输入银行卡信息的。

网络防骗“五不要”

1、不要轻信中奖、红包、违法、洗钱等;
2、不要回拨陌生信息提供的联系方式，不要致电联系;
3、不要点击免费领奖、红包链接、视频相册等陌生链接统统不点;
4、不要透露手机号、身份证号、银行卡号等一切隐私信息;
5、不要转账不经核实的情况统统不要转账。

网络防骗“两核实”

1、核实可疑信息
陌生可疑的短信、电话、QQ、微信、邮件、通知等等，只要拿不准情况，都通过官方渠道进行核实;
2、核实转账请求
他人要求借钱、打款、线上支付、充值等等，所有金钱往来，一定要当面或电话联系到本人进行确认。

2 日常生活篇

移动设备

手机使用

泄漏途径

- 正常的社会活动被泄露，如旅馆住宿、保险公司投保、 租赁公司、银行办证、电信、移动、联通、房 地产、邮政部门等需要身份证件实名登记的部门、场所，个别人员利用登记的便利条件，收集客户个 人信息，汇集成册，并按照一定的价格出售给需要购买的人;
- 利用各种活动引诱填写个人信息，如填写详细联系方式、收入情况、信用卡情况等内容就能参加抽奖 活动，可以获得不等奖次的奖品;
- 一些互联网公司由于安全防范措施不到位，其用户的个人信息被黑客窃取等。

个人信息用途

- 电信诈骗、网络诈骗等新型、非接触式犯罪。如犯罪分子利用非法获取的公民家庭成员信息，向学生 家长打电话谎称其在校子女遭绑架或突然生病，要求紧急汇款解救或医治，以此实施诈骗。
- 直接实施抢劫、敲诈勒索等严重暴力犯罪活动。如2012年初，广州发生犯罪分子根据个人信息资料，
冒充快递，直接上门抢劫，造成户主一死两伤的恶性案件。
- 实施非法商业竞争。如以信息咨询、商务咨询为掩护，利用非法获取的公民个人信息，收买客户、打
压竞争对手。
- 非法干扰民事诉讼。如利用购买的公民个人信息，介入婚姻纠纷、财产继承、债务纠纷等民事诉讼。
- 滋扰民众。通过网络人肉搜索、信息曝光等行为滋扰民众生活。

目录

01 工作篇

02 生活篇

03 法律篇

3 法律法规篇

《网络安全法》五大意义

1 明确了网络主权原则

2 关键信息基础设施

3 保障网络数据安全

4 打破部门壁垒

5 对个人信息的保护

3 法律法规篇

《网络安全法》四大焦点

如何规范个人信息收集行为?

第四十一条 网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。

如何斩断信息买卖利益链?

第四十四条 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。

个人信息泄露如何补救?

第四十二条 网络运营者不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外。

如何对网络诈骗溯源追责?

第六十四条 网络运营者、网络产品或者服务的提供者违反本法第二十二条第三款、第四十一条至第四十三条规定，侵害个人信息依法得到保护的权利的，由有关主管部门责令改正，可以根据情节单处或者并处警告、没收违法所得、处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款;情节严重的，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照。

3 法律法规篇

《网络安全法》六大看点

- 不得出售个人信息
- 严厉打击网络诈骗
- 明确网络实名制
- 重点保护关键信息基础设施
- 惩治破坏设施的组织和个人
- 网络通信管制

3 法律法规篇

《刑法》

网上不法行为认定为寻衅滋事罪

网上不法行为认定为敲诈勒索罪

网上不法行为认定为非法经营罪

为不法行为提供帮助以共同犯罪论处

《保密法》

互联网上的失泄密行为将受到法律惩处。

《国家安全法》

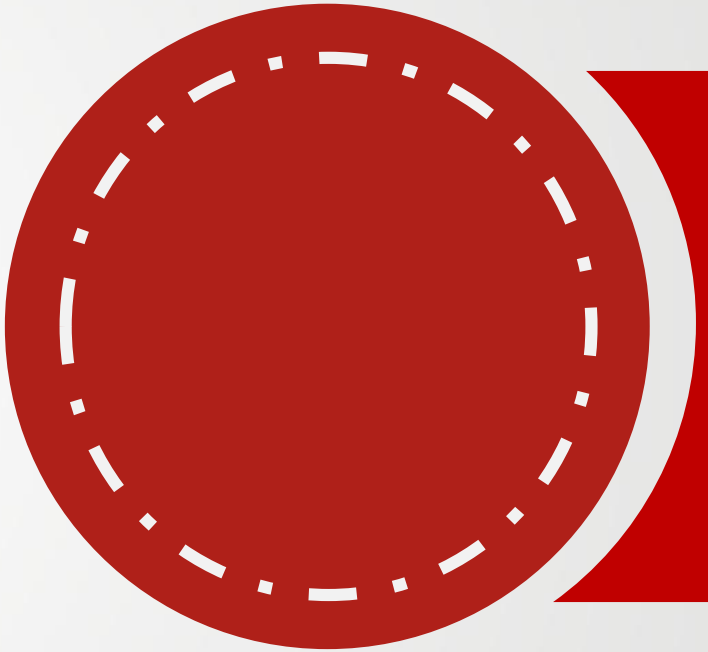
第二十五条国家建设网络与信息安全保障体系，提升网络与信息安全保护能力，加强网络和信息技术的创新研究和开发应用，实现网络和信息核心技术、关键基础设施和重要领域信息系统及数据的安全可控;加强网络管理，防范、制止和依法惩治网络攻击、网络入侵、网络窃密、散布违法有害信息等网络违法犯罪行为，维护国家网络空间主权、安全和发展利益。

巩固网络安全 共创和谐社会

苏州大学

苏州大学

《数据安全法》解读及最佳实践

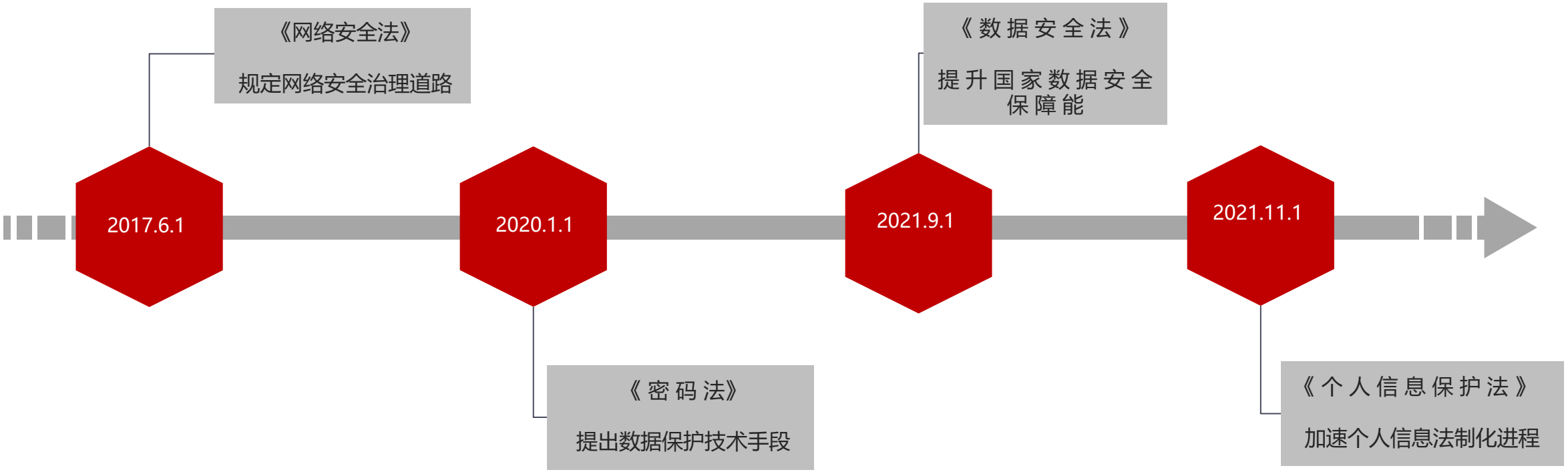


前言

近些年，因数据问题导致企业和公民的**权益受到侵害**的事件时有发生，结合当前数据业务发展态势，该类事件还会呈上升趋势，并未达到顶峰。这当然和数据主体(组织和个人）对于数据安全的意识在不断的提高有很大关系。另外，受利益驱使，某些组织或个人铤而走险，不当采集数据、滥用数据还是很常见的。因此，通过立法来维护数据主体的权益是非常有必要的。

2021年6月10日，《数据安全法》正式颁布，于2021年9月1日正式施行，作为我国数据安全领域的首部基础性法律，也是国家安全领域的一部重要法律，标志着我国以数据安全保障数据开发利用和产业发展全面进入法治化轨道。

数据安全领域里程碑


《网络安全法》
规定网络安全治理道路
2017.6.1
2020.1.1
《密码法》
提出数据保护技术手段
《数据安全法》
提升国家数据安全保障能
2021.9.1
2021.11.1
《个人信息保护法》
加速个人信息法制化进程

《数据安全法》总览

进程

《数据安全法》第十三届全国人民代表大会常务委员会第二十九次会议通过，共七章55条，2021年9月1日正式实施。

目的

为了规范数据处理活动，保障数据安全，促进数据开发利用，保护个人、组织的合法权益，维护国家主权、安全和发展利益，制定本法。

范围

1、在中华人民共和国境内开展数据处理活动及其安全监管，适用本法。
2、在中华人民共和国境外开展数据处理活动，损害中华人民共和国国家安全、公共利益或者公民、组织合法权益的，依法追究法律责任。

相关概念

数据

是指任何以电子或者其他方式对信息的记录。

解读：数据大体可分为结构化数据、非结构化数据、非电子形式数据

数据处理

包括数据的收集、存储、使用、加工、传输、提供、公开等。

解读：不再以数据生命周期为主线，而是数据场景和数据动作，行业、领域的不同，数据处理活动也 会有所不同，以数据场景和数据动作为防护点，边界清晰，也更容易落地

数据安全

通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

解读：数据加密、数据脱敏等工具可以有效保护数据，数据安全审计、安全态势分析可以保障持续安 全状态

不当使用

通过开展数据处理活动进行排除和限制竞争，或者损害个人、组织合法权益 。

解读：不论数据是何种形式、何种载体，开展数据处理活动只要不当使用，即违法

数据安全治理体系被提出

第四条 维护数据安全，应当坚持总体国家安全观，建立健全数据安全治理体系，提高数据安全保障能力。

分析：开展数据安全工作，需要具有国家安全观，要有一定的判别能力。另外，从国家层面， 已不再只关注数据安全的单体能力，而是要形成体系，大到国家，小到组织都应该从体系化思 维开展数据安全工作

解读：数据安全治理体系的建设基于数据处理活动，可以从组织、制度、措施、审计四个维度入手，从事前、事中、事后三个阶段对数据实施防护措施

数据安全责任

中央国家安全领导机构

负责国家数据安全工作的决策和议事协调，研究制定、指导实施国家数据安全战略和有关重大方针政策，统筹协调国家数据安全的重大事项和重要工作，建立国家数据安全工作协调机制。

国家网信部门：负责统筹协调网络数据安全和相关监管工作

各行业主管部门

承担本行业、本领域数据安全监管职责。

公安机关、国家安全机关

在各自职责范围内承担数据安全监管职责。

各地区、各部门

对本地区、本部门工作中收集和产生的数据及数据安全负责。

发展导向

建环境

第九条 国家支持开展数据安全知识宣传普及，提高全社会的数 据安全保护意识和水平，推动有关部门、行业组织、科研机构、企业 、个人等共同参与数据安全保护工作，形成全社会共同维护数据安全 和促进发展的良好环境。

促发展

第十三条 国家统筹发展和安全，坚持以数据开发利用和产业发展 促进数据安全，以数据安全保障数据开发利用和产业发展。

搞扶持

第十六条 国家支持数据开发利用和数据安全技术研究，鼓励数 据开发利用和数据安全等领域的技术推广和商业创新，培育、发展数 据开发利用和数据安全产品、产业体系。

养人才

第二十条 国家支持教育、科研机构和企业等开展数据开发利用技术 和数据安全相关教育和培训，采取多种方式培养数据开发利用技术和 数据安全专业人才，促进人才交流。

数据安全管理制度

分类分级

第二十一条 国家建立数据分类分级保护制度，根据数据在经济社会发展中的重要程度，以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益造成的危害程度，对数据实行分类分级保护。国家数据安全工作协调机制统筹协调有关部门制定重要数据目录，加强对重要数据的保护。

关系国家安全、国民经济命脉、重要民生、重大公共利益等数据属于国家核心数据，实行更加严格的管理制度。

各地区、各部门应当按照数据分类分级保护制度，确定本地区、本部门以及相关行业、领域的重要数据具体目录，对列入目录的数据进行重点保护 。

解读：国家层面建立数据分类分级保护制度，根据危害程度实行 不同的管控策略，并建立重要数据目录，针对重要数据的 处理，将采取更为严格的保护措施。重要数据目录的建立 需要依赖各地区、各部门的业务特征，确保没有遗漏，各 监管机构要加强监管重要数据的处理活动 。

风险评估与风险信息管理机制

第二十二条国家建立集中统一、高效权威的数据安全风险评估、报告、信 息共享、监测预警机制。国家数据安全工作协调机制统筹协调有关部门加强数 据安全风险信息的获取、分析、研判、预警工作 。

解读：一方面要建设风险评估、监测预警的机制，及时发现潜在 风险，一方面要加强对风险的识别和判定能力，并及时预 警，协助各行业、各领域快速采取补救措施，损失最小化 。

应急处置

第二十三条国家建立数据安全应急处置机制。发生数据安全事件，有关主管部门应当依法启动应急预案，采取相应的应急处置措施，防止危害扩大，消除安全隐患，并及时向社会发布与公众有关的警示信息。

解读：各地区、各部门均需要建议数据安全应急处置机制，要明 确处置方案和相关责任人，发生数据安全事件时，可及时 止损，并向社会发布，起到警示作用 。

数据安全保护义务

第二十七条 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。重要数据的处理者应当明确数据安全负责人和管理机构，落实数据安全保护责任。

解读：制定管理制度、开展教育培训、建设管控措施、明确重要数据责任是各行业、各领域应该履行的义务。数据安全方面，可基于等保，并高于等保。提倡数据安全防护体系化建设，合理运用技术措施。

第二十九条 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。

解读：要具备风险监测、风险感知的能力，持续建设和补充风险补救措施，有备无患；同时，要建立应急处置机制，制定应急处置方案，明确相关责任人，履行告知用户和上报主管部门的义务。

数据安全保护义务

第三十条 重要数据的处理者应当按照规定对其数据处理活动定期开展风险评估，并向有关主管部门报送风险评估报告。风险评估报告应当包括处理的重要数据的种类、数量，开展数据处理活动的情况，面临的数据安全风险及其应对措施等。

解读：重要数据一般是指某行业、某领域因业务而涉及到的高敏感数据，各行业、各领域应明确自身数据哪些是重要数据，定期开展风险评估，重要数据的处理应做到可控、可靠，保持与主管部门的同步。

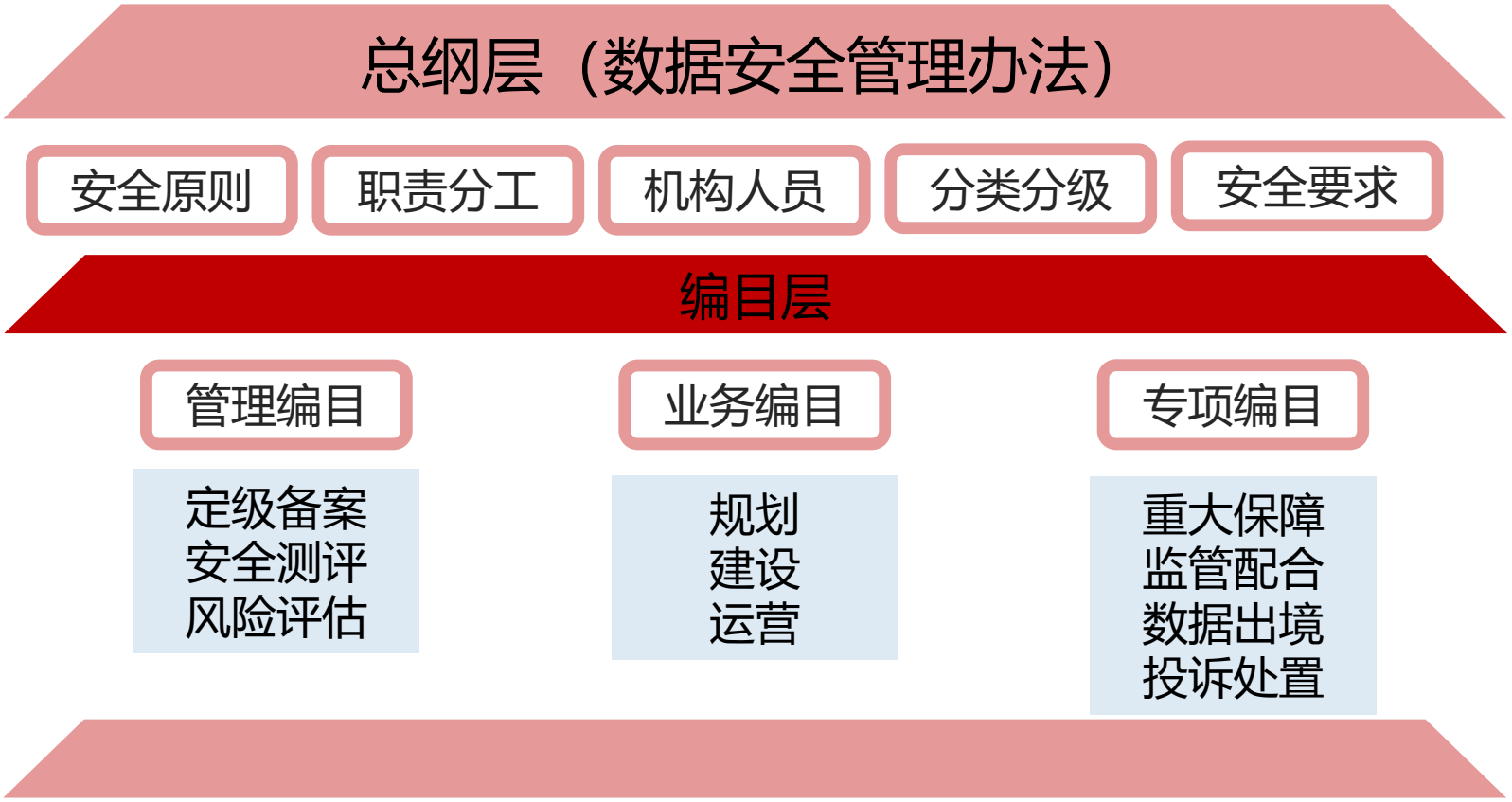
第三十三条 从事数据交易中介服务的机构提供服务，应当要求数据提供方说明数据来源，审核交易双方的身份，并留存审核、交易记录。

解读：数据交易合作时，数据提供方有义务说明数据来源的合法性，并提供相应的证明材料，最好纳入到协议中，同时应对数据交易双方的身份进行有效核实，并留存相关记录。

第三十五条 公安机关、国家安全机关因依法维护国家安全或者侦查犯罪的需要调取数据，应当按照国家有关规定，经过严格的批准手续，依法进行，有关组织、个人应当予以配合。

解读：配合公安机关、国家安全机关工作，是每个组织和个人的义务。提供数据时应保证过程安全，并留存相关的手续。

建立健全全流程数据安全管理制度



解读：建立健全完整的数据安全管理制度是企事业单位开展数据安全工作的基石。针对数据安全工作基础薄弱的企业，可以参考《数据安全法》进行数据安全管理制度体系设计，比如建立总纲层，编制宏观安全要求框架；梳理编目层，从管理、业务、专项等方面确定实施细则、作业规范等。

数据出境

境外追究

第二条 在中华人民共和国境外开展数据处理活动，损害中华人民共和国国家安全、公共利益或者公民、组织合 法权益的，依法追究法律责任。

出口管制

第二十五条 国家对与维护国家安全和利益、履行国际义 务相关的属于管制物项的数据依法实施出口管制。

数据出境

第三十一条 关键信息基础设施的运营者在中华人民共和 国境内运营中收集和产生的重要数据的出境安全管理，适 用《中华人民共和国网络安全法》的规定;其他数据处理 者在中华人民共和国境内运营中收集和产生的重要数据的 出境安全管理办法，由国家网信部门会同国务院有关部门 制定。

执法需要

第三十六条 非经中华人民共和国主管机关批准，境内的 组织、个人不得向外国司法或者执法机构提供存储于中华 人民共和国境内的数据。

解读：整体来看，国家对数据出境问题非常严苛和严谨，几乎很难实现。受国外局势影响，短期内应该也不会放松要求。另外，数据出境可能会以国家或地区为单位开放，并提出不同的要求和审查机制。

政务数据安全与开放

动作1:建立管理制度

第三十九条 国家机关应当依照法律、行政法规的规定，建立健全数据安全管理制度，落实数据安全保护责任，保障政务数据安全。

动作2:制定统一开放目录

第四十二条 国家制定政务数据开放目录，构建统一规范、互联互通、安全可控的政务数据开放平台，推动政务数据开放利用。

职责：监督受托方

第四十条 国家机关委托他人建设、维护电子政务系统，存储、加工政务数据，应当经过严格的批准程序，并应当监督受托方履行相应的数据安全保护义务。

解读：主要解决如下问题：

1. “不愿共享”、“不敢共享”、“不能共享”的困难
2. 加速政务数据的利用
3. 加大数据安全管控力度

法律责任

以下行为违法，面临警告、罚款、停业、吊销执照的处罚，组织与直接主管责任人并罚：

- 开展数据处理活动，未建立管理制度、未开展教育培训、未采取安全措施
- 没有数据安全缺陷和漏洞的补救措施，没有应急处置措施，瞒报、不报数据安全事件
- 处理重要数据未定期开展风险评估，未向主管部门上报报告
- 向境外提供重要数据，或未按规定向境外提供数据

第四十五条由有关主管部门责令改正，给予警告，可以并处五万元以上五十万元以下罚款，对直接负 责的主管人员和其他直接责任人员可以处一万元以上十万元以下罚款；拒不改正或者造成大量数据泄露等严重后果的，处五十万元以上二百万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五万元以上二十万元以下罚款。

法律责任

数据交易违法情形，面临没收所得、加倍罚款、停业、吊销执照的处罚，企业组织与直接主管责任人并罚：

- 数据提供方未说明数据来源，未提供相关材料
- 数据需求方未说明数据用途
- 数据交易中介机构未审核双方身份，未留存审核、交易记录

第四十七条 从事数据交易中介服务的机构未履行本法第三十三条规定的义务的，由有关主管部门责令改正，没收违法所得，处违法所得一倍以上十倍以下罚款，没有违法所得或者违法所得不足十万元的，处十万元以上一百万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

法律责任

以下行为属违法，将面临警告、罚款的处罚，企业组织与直接主管责任人并罚：

- 未配合公安机关、国家安全机关因依法维护国家安全或者侦查犯罪的需要调取数据

第四十八条 拒不配合数据调取的，由有关主管部门责令改正，给予警告，并处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

以下违法属违法，将面临警告、罚款、停业、吊销执照的处罚，企业组织与直接主管责任人并罚：

- 未经批准向外国司法或者执法机构提供存储于中华人民共和国境内的数据。

分析说明:无论是组织还是个人，无论是重要数据还是普通数据，只要是存储于境内的数据

第四十六条 违反本法第三十一条规定，向境外提供重要数据的，由有关主管部门责令改正，给予警告，可以并处十万元以上一百万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处一万元以上十万元以下罚款；情节严重的，处一百万元以上一千万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款。

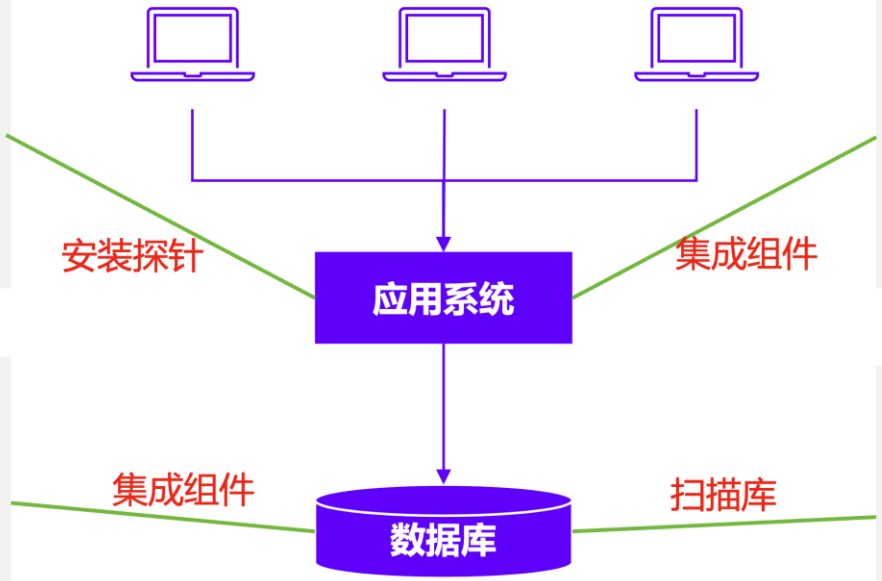
传统的数据安全解决方案

- **数据安全审计系统**

  对数据库中的数据使用情况进行审计，主要采用协议解析技术，对违规行业、高危行为进行识别，及时告警

- **数据库加密设备**

  对存储在数据库中的数据进行加密处理，防止高权限人员窃取原始数据，防止被拖库，根据账号权限进行解密



- **动态脱敏系统**

  根据权限和脱敏规则对原始数据采取遮蔽、替换等手段进行保护，降低数据的暴露面，防止数据泄露

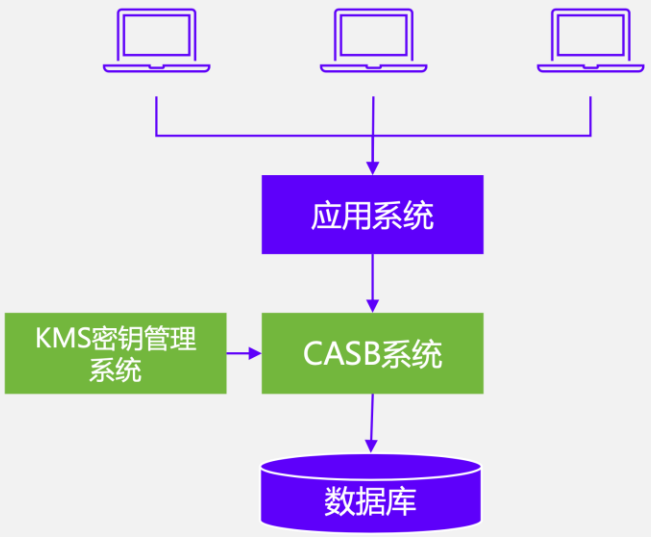
- **敏感数据发现系统**

  通过扫描的方式自动发现数据库中的敏感数据，以及敏感数据的使用情况，并对其进行管理，分类分级

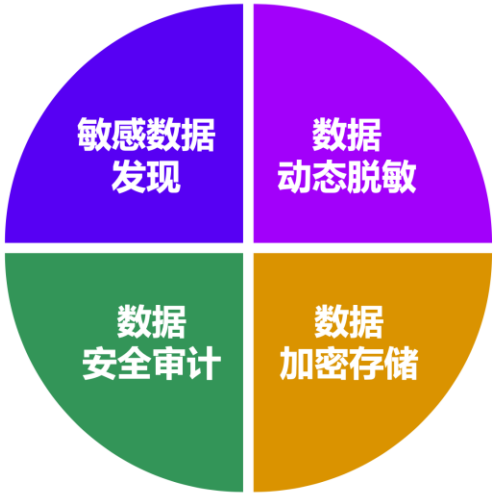
特点：数据库性能无损耗，能力冗余

数据库协议解析技术数据安全解决方案

方式一：网关式

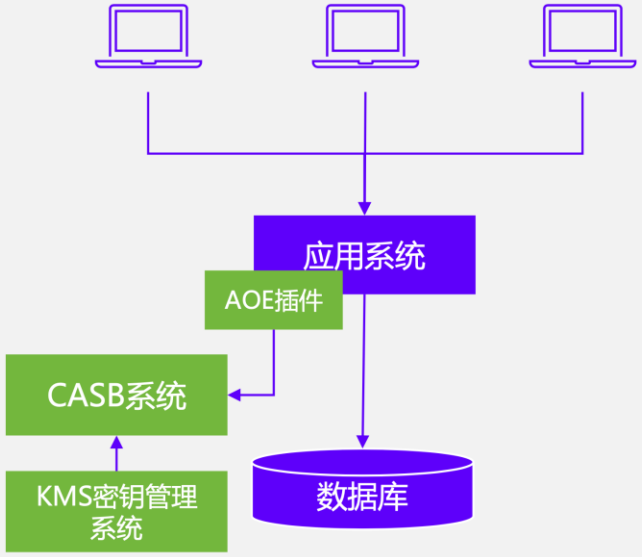


特点：数据库被隐藏、无需改造



通过CASB系统将能力进行融合
只需一次集成

方式二：插件式



特点：性能损耗低，微改造

方案思路

事前 敏感数据发现

价值：快速排查数据违规，辅助重要数据梳理，为管控和分类分级提供依据。

手段：访谈、问卷、人工查询、正则表达式、关键字、机器学习。

事中 加密存储、动态脱敏

价值：防拖库、防高权限人员泄露数据、防非授权人员窃取数据；在数据使用过程中对数据进行混淆、遮蔽处理，降低数据泄露风险。

手段：应用层开发、加密网关、数据库原生TDE、数据库文件加密；脱敏算法（遮蔽、随机替换、固定值替换、同义转换）。

事后 安全审计

价值：实时发现数据违规使用行为，及时止损，辅助溯源和取证。

手段：基于协议的数据安全审计，将应用帐号、数据库帐号、敏感信息进行关联，能够清晰地定位到敏感信息访问和操作的发起者，增强敏感信息审计的精确度，溯源能力强。

让数据遵规守序

让数据管理遵循法规，让数据流动遵守秩序

勒索病毒介绍和处置

部门：数据资源与信息化建设管理处　　时间：2022年11月2日

前言 | Introduction

勒索病毒威胁已经成为当前最受关注的网络安全风险之一。而结合信息窃取和泄露的二次勒索模式，使得勒索病毒的危害进一步加深。针对个人、企业、政府机关、各类机构的攻击层出不穷，在勒索病毒威胁面前，没有人能够置身事外。在勒索病毒处置中，如能及时正确处置，可有效降低勒索病毒带来的损失，避免病毒影响进一步扩散。

目录
CONTENTS

PART 01 什么是勒索病毒

PART 02 勒索病毒传播方式

PART 03 勒索病毒处置

PART 04 安全防护建议

什么是勒索病毒

什么是勒索病毒

勒索病毒是泛指一切通过锁定被感染者计算机系统或文件并施以敲诈勒索的新型计算机病毒。

计算机一旦感染勒索病毒，磁盘上几乎所有格式的文件都会被加密，并在桌面等明显位置生成勒索提示文件，被感染者需要通过缴纳高额赎金才能获取解密密钥恢复计算机系统和数据文件的正常使用，多数情况即使缴纳了高额的赎金也未必能正常恢复数据。因此，勒索病毒具有数据恢复代价大和数据恢复可能性低的特点。

勒索病毒使企业、学校和个人用户的大量重要文件无法使用甚至外泄，严重影响日常工作和生活。

2017年5月，WannaCry勒索软件肆虐。世界各地都有受到该勒索软件的攻击，几天时间内，150个国家的20多万台Windows电脑受到攻击，造成的损失达数十亿美元。

勒索病毒传播方式

勒索病毒传播方式

01 漏洞传播

攻击者利用弱口令、远程代码执行等安全漏洞，攻击入侵用户内部网络，获取管理员权限，进而主动传播勒索病毒。

02 邮件传播

攻击者在互联网上撒网式发送垃圾邮件、钓鱼邮件，一旦收件人点开带有勒索病毒的链接或附件，病毒将自动加载、安装，进而威胁整个网络安全。

03 网站挂马传播

用户浏览挂有木马病毒的网站，上网终端计算机系统极可能被植入木马并感染上勒索病毒。

04 介质传播

攻击者通过隐藏U盘、移动硬盘等移动存储介质原有文件，创建与移动存储介质盘符、图标等相同的快捷方式，一旦用户点击，将自动运行勒索病毒，或运行专门用于收集和回传设备信息的木马程序，便于未来实施针对性的勒索。

05 软件供应链传播

攻击者利用软件供应商与软件用户间的信任关系，通过攻击入侵软件供应商相关服务器设备，利用软件供应链分发、更新等机制，在合法软件正常传播、升级等过程中，对合法软件进行劫持或篡改，规避用户网络安全防护机制，传播勒索病毒。

06 漏洞传播

攻击者通常利用弱口令、暴力破解等方式获取攻击目标服务器远程登录用户名和密码，进而通过远程桌面协议登录服务器并植入勒索病毒。同时，攻击者一旦成功登录服务器，获得服务器控制权限，可以服务器为攻击跳板，在用户内部网络进一步传播勒索病毒。

勒索病毒处置

勒索病毒处置——断开网络

断开网络

发现计算机中毒，应在第一时间对中毒计算机进行断网处理，断开网络能阻止勒索病毒在内网横向传播以及攻击者对当前设备的持续控制，防止勒索病毒继续加密文件和进一步扩散。

勒索病毒处置——备份

备份

备份中毒后的重要数据，寻求专业人员协助破解。

勒索病毒处置——排查

排查中毒原因

查找可疑程序、病毒文件，找到病毒来源，以免二次中毒。如果发现可疑文件后，可以将可疑文件打包为一 个加密压缩包后再进行删除或转移。如自己无法排查原因，也可以拨打65880000，向数据资源与信息化建设管理处寻求帮助。

勒索病毒处置——解密

解密

寻找免费解密工具
找第三方技术支持
不推荐任何形式的交付赎金、购买密钥行为

若一定要购买密钥，应注意：

- **不建议直接向黑客交付赎金。**交付赎金后并不一定真的能解密文件，黑客还可能会再次甚至多次索要赎金。
- **通过第三方解密。**通过淘宝、搜索引擎或其它方式联系到的解密服务商，正式开展解密工作前一定要签订合同，明确解密不成功是否需要付款等问题，必要时可要求上门服务。
- **不要咨询过多第三方商家。**因为第三方大多都是去找黑客购买密钥。过多的联系第三方商家，会造成黑客收到多次关于你设备的咨询，这可能导致黑客觉察到你对数据恢复有强烈需求，从而提高赎金。
- **不透露文件重要性和自身经济实力。**不要过度描述自己文件的重要性或自身的经济实力，这可能会造成解密商或黑客提高佣金或赎金要求。

勒索病毒处置——格式化&重装系统

格式化&重装系统

在完成备份和排查工作后，格式化磁盘并重装系统，计算机可再次投入使用。

安全防护建议

养成良好的安全习惯

01 电脑应当安装具有高级威胁防护能力和主动防御功能的安全软件（推荐苏州大学天融信EDR，下载地址http://sd.suda.edu.cn)。不脱离管理中心、退出安全软件或关闭防护功能，对安全软件提示的各类风险行为不要轻易采取放行操作。

02 可使用安全软件的漏洞修复功能，第一时间为操作系统和浏览器，常用软件打好补丁，以免病毒利用漏洞入侵电脑。

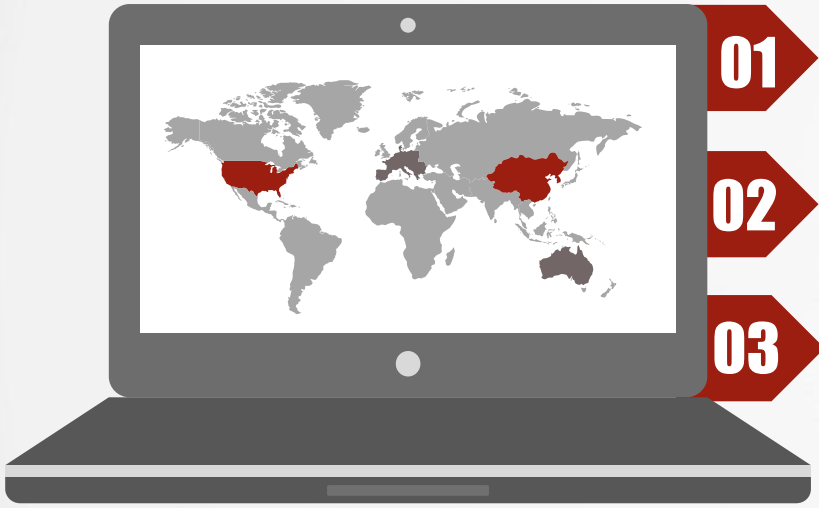
03 尽量使用安全浏览器，减少遭遇挂马攻击、钓鱼网站的风险。

04 重要文档、数据应经常做备份，一旦文件损坏或丢失，也可以及时找回。

05 电脑设置的口令要足够复杂，包括数字、大小写字母、符号且长度至少应该有8位，不使用弱口令，以防攻击者破解。

06 电脑连接移动存储设备（如U盘、移动硬盘等），应首先使用安全软件监测其安全性。

避免危险上网操作



01 不要浏览来路不明的色情、赌博等不良信息网站，此类网站经常被用于发起挂马、钓鱼攻击。

02 不要轻易打开陌生人发来的邮件附件或邮件正文中的网址链接。也不要轻易打开扩展名为js、vbs、wsf、bat、cmd、ps1等脚本文件和exe、scr、com等可执行程序，对于陌生人发来的压缩文件包，更应提高警惕，先使用安全软件进行检查后再打开。

03 对于安全性不确定的文件，可以选择在安全软件的沙箱功能中打开运行，从而避免木马对实际系统的破坏。

谢谢！

部门：数据资源与信息化建设管理处　　时间：2022年11月2日