数据安全研究 创刊号

Data security research

2015 年第一期

2015 年 06 月 15 日

数据安全研究院

新技能 U 盘数据恢复仅需 4 步

2015 青少年上网安全数据分析报告

数据安全与数字化

效率源科技 XLYTECHNOLOGY

Foreword 发刊词

安全感

地球公转一圈是一年，自转一圈是一天。

今天，《数据安全研究》(半月刊)与您初见。

我们生于成都。

成都就是成都，西部的焦点。

信息安全产业高地。

网络，连接你我 ta

信息的海洋中，谁也逃不了，躲不开。

焦虑、烦躁、六神无主，心不定。

我们希望传递清晰的声音。

清晰来自理性，理性来自专业。

我们把专业看成一种责任。

中国需要这份主流的责任。

我们严肃得体，不夸张，不浮躁，不讨巧，不回避，不苟且。

我们希望给您安全感、正能量。

这是我们对您的承诺。

Contents 目录

News 资讯

[本页资讯来源于网络]

第二届国家网络安全周

6 月 1 日至 7 日以“网络安全，共享网络文明”为主题国家网络安全宣传周在全国各地同步开展。期间精彩不断，安全意识的呐喊振聋发聩。

苹果安全漏洞持续增加

近期，苹果产品被曝出了一系列严重的信息安全漏洞。消息人士表示，苹果已意识到这些问题，而公司正试图改善与信息安全研究人员的沟通。目前主要的挑战在于，如何应对漏洞的快速增长。苹果会接到大量可能的漏洞报告，而苹果的信息安全团队希望优先关注更严重的漏洞，并区分真正的漏洞和误报。

83%网民网上支付行为存在安全隐患

工信部发布的首个公众网络安全意识调查报告显示，约 83%的网民网上支付行为存在安全隐患，网络安全意识亟需提升。报告显示，中国网民网络安全意识不强，这一点在网民网络应用和基础技能方面尤为突出。

银川寄递行业实行实名制度

银川市在辖区各寄递行业全面实行邮件、快件寄件人实名交寄、寄递企业实名收寄制度，让犯罪分子无机可乘。

四川省信息安全产业推介会

从本月 5 日召开的四川信息安全产业推进会获悉，我省将从集聚发展、重大项目实施、推动示范应用三大方面重点推进我省信息安全产业发展，确保今年 148 户信息安全企业完成投资 88 亿元。

公民网络身份识别系统

随着公民个人信息的泄露愈演愈烈，骚扰电话和各种诈骗令人防不胜防。记者近日从公安部第三研究所获悉，独立于公民身份信息系统之外的“公安部公民网络身份识别系统”，已通过国家密码管理局的安全审查，开始向公民签发 eID(公民网络电子身份标识)。虚拟身份的推广，避免公民个人信息的泄露。

信息安全股上涨明显

资料显示，信诚中证信息安全分级指基跟踪的中证信息安全指数专注信息安全板块。从波动性来看，根据 Wind 数据，中证信息安全指数近 60 个月的波动率为 32.10%，远超沪深 300 与中证 500 的 24.49%、27.20%，适合波段操作。

大数据环境下的数据安全研究

摘要：大数据蕴藏着价值信息，但数据安全亦因大数据而面临严峻挑战。本文将基于大数据基本特征，提出当前大数据面临的安全挑战，并从大数据的存储、应用和管理等方面阐述大数据安全的应对策略。

关键词：大数据；数据安全；云计算；数据挖掘

Abstract

The Big Data contain Valuable informationHowever, data security is facing serious challenge。

based on the analysis of the basic characteristics of the Big DataThe paper propose the current risk of Big Dataand further from the Big Datas storage, application and management expounds the Big Data Security strategy.

Key words：Big DataData security；Cloud Computing Data Mining

引言

随着互联网、物联网、云计算等技术的快速发展，以及智能终端、网络社会、数字地球等信息体的普及和建设，全球数据量出现爆炸式增长，仅在 2011 年就达到 1.8 万亿 GB。IDC 预计，到 2020 年全球数据量将增加 50 倍。毋庸赘疑，大数据时代已经到来。一方面，云平台为这些海量的、多样化的数据提供存储和运算平台，另一方面，数据挖掘和人工智能从大数据中发现知识、规律和趋势，为决者策提供信息参考。但是，大数据的发展将进一步扩大信息的开放程度，随之而来的隐私数据或敏感信息的泄露事件时有发生。面对大数据发展的新特点、新挑战，如何保障数据安全是我们需要研究的课题。

1 大数据的特征

大数据通常被认为是一种数据量很大、数据形式多样化的非结构化数据。随着对大数据研究的进一步深入，大数据不仅指数据本身的规模，也包括数据采集工具、数据存储平台、数据分析系统和数据衍生价值等要素。其主要特点有以下几点：

1.1 数据量大

大数据时代，各种传感器、移动设备、智能终端和网络社会等无时不刻都在产生数据，数量级别已经突破 TB，发展至 PB 乃至 ZB，统计数据量呈千倍级别上升。据估计，2012 年全球产生的数据量将达到 2.7ZB，2015 年将超过 8ZB[1]。

1.2 类型多样

当前大数据不仅仅是数据量的井喷性增长，而且还包含着数据类型的多样化发展。以往数据大都以二维结构呈现，但随着互联网、多媒体等技术的快速发展和普及，视频、音频、图片、邮件、HTML、RFID、GPS 和传感器等产生的非结构化数据，每年都以 60%的速度增长。预计，非结构化数据将占数据总量的 80%以上[1]。

1.3 运算高效

基于云计算的 Hadoop 大数据框架，利用集群的威力高速运算和存储，实现了一个分布式运行系统，以流的形式提供高传输率来访问数据，适应了大数据的应用程序。而且，数据挖掘、语义引擎、可视化分析等技术的发展，可从海量的数据中深度解析，提取信息，掌控数据增值的“加速器”。

1.4 产生价值

价值是大数据的终极目的。大数据本身是一个“金矿产”，人们可以从大数据的融合中获得意想不到的有价值的信息。特别是激烈竞争的商业领域，数据正成为企业的新型资产，追求数据最大价值化。同时，大数据价值也存在密度低的特性，需要对海量的数据进行挖掘分析才能得到真正有用的信息，形成用户价值。以监控视频为例，连续的播放画面，可以产生价值的数据可能是仅仅的一两秒。

2 大数据面临的安全挑战

正如 Gartner 所说：“大数据安全是一场必要的斗争”[2]。在大数据时代，鉴于无处不在的智能终端、互动频繁的社交网络和超大容量的数字化存储，我们不得不承认大数据已经渗透到各个行业领域，并逐渐成为一种生产要素，正发挥着重要作用，更将成为未来竞争的至高点。大数据所含信息量较高，虽然相对价值密度较低，但是对它里面所蕴藏的潜在信息而言，随着快速处理和分析提取技术的发展，可以快速捕捉到有价值的信息以提供参考决策。然而，大数据掀起新一轮生产率提高和消费者盈余浪潮的同时，随之而来的是信息安全的挑战。

2.1 网络化社会使大数据易成为攻击目标

网络化社会的形成，为大数据在各个行业领域实现资源共享和数据互通搭建了平台和通道。基于云计算的网络化社会为大数据提供了一个开放的环境，分布在不同地区的资源可以快速整合，动态配置，实现数据集合的共建共享。而且，网络访问便捷化和数据流的形成，为实现资源的快速弹性推送和个性化服务提供基础。正因为平台的暴露，使得蕴含着海量数据和潜在价值的大数据更容易吸引黑客的攻击。也就是说，在开放的网络化社会，大数据的数据量大且相互关联，对于攻击者而言，相对低的成本可以获得“滚雪球”的收益。近年来在互联网上发生的用户帐号信息失窃等信息安全事件的连锁反应可以看出，大数据更容易吸引黑客，而且一旦遭受攻击，失窃的数据量也是巨大的。

2.2 非结构化数据对大数据存储提出新要求

在大数据之前，我们通常将数据存储分为关系型数据库和文件服务器两种。而当前大数据汹涌而来，数据类型的千姿百态也使我们措手不及。对于将占数据总量 80%以上的非结构化数据，虽然 NoSQL 数据存储具有可扩展性和可用性等优点，利于趋势分析，为大数据存储提供了初步解决方案， 但是 NoSQL 数据存储仍存在以下问题：一是相对于严格访问控制和隐私管理的 SQL 技术，目前 NoSQL 还无法沿用 SQL 的模式，而且适应 NoSQL 的存储模式并不成熟；二是虽然 NoSQL 软件从传统数据存储中取得经验，但 NoSQL 仍然存在各种漏洞，毕竟它使用的是新代码；三是由于 NoSQL 服务器软件没有内置足够的安全，所以客户端应用程序需要内建安全因素，这又反过来导致产生了诸如身份验证、授权过程和输入验证等大量的安全问题。

2.3 技术发展增加了安全风险

计算机网络技术和人工智能的发展，服务器、防火墙、无线路由等网络设备和数据挖掘应用系统等技术的愈加成熟，为大数据自动收集效率以及智能动态分析性提供了便利。但是，技术发展也增加了大数据的安全风险。一方面，大数据本身的安全防护存在漏洞：虽然云计算对大数据提供了便利，但对大数据的安全控制力度仍然不够，API 访问权限控制以及密钥生成、存储和管理方面的不足都可能造成数据泄漏。而且大数据本身可以成为一个可持续攻击的载体，被隐藏在大数据中的恶意软件和病毒代码很难被发现，有心人士或组织藉此可达到长久攻击或窃取数据的目的；另一方面，攻击的技术提高了：在用数据挖掘和数据分析等大数据技术获取价值信息的同时，攻击者也在利用这些大数据技术进行攻击。

3 大数据安全的应对策略

当然，大数据也为数据安全的发展提供了新机遇。大数据正在为安全分析提供新的可能性，对海量数据的分析有助于更好地跟踪网络异常行为，对实时安全和应用数据结合在一起的数据进行预防性分析，可防止诈骗和黑客入侵。网络攻击行为总会留下蛛丝马迹，这些痕迹都以数据的形式隐藏在大数据中，从大数据的存储、应用和管理等方面层层把关，可以有针对性地应对数据安全威胁。

3.1 大数据存储安全策略

基于云计算架构的大数据，数据的存储和操作都是以服务的形式提供。目前，大数据的安全存储采用虚拟化海量存储技术来存储数据资源，涉及数据传输、隔离、恢复等问题。解决大数据的安全存储的第一种方法是数据加密。数据加密是指在大数据安全服务的设计中，大数据可以按照数据安全存储的需求，被存储在数据集的任何存储空间，通过 SSL（安全套接层）加密，实现数据集的节点和应用程序之间移动保护大数据。并在大数据的传输服务过程中，加密为数据流的上传与下载提供有效的保护，可以达到应用隐私保护和外包数据计算，屏蔽网络攻击。目前，PGP 和 TrueCrypt 等程序都提供了强大的加密功能。第二种方法是分离密钥和加密数据，即是以加密的方式把数据使用与数据保管分离，把密钥与要保护的数据隔离开[4]。同时，定义产生、存储、备份、恢复等密钥管理生命周

期。第三种方法是使用过滤器。过滤器的监控系统，一旦发现数据离开了用户的网络，就自动阻止数据的再次传输。第四种方法则是数据备份。通过系统容灾、敏感信息集中管控和数据管理等产品，实现端对端的数据保护，确保数据有备无患达到安全管控的目的。

3.2 大数据应用安全策略

随着大数据应用所需的技术和工具的快速发展，大数据应用安全策略主要从以下几方面着手：一是防止 APT 攻击。借助大数据处理技术，针对 APT 安全攻击隐蔽能力强 、长期潜伏、攻击路径和渠道不确定等特征，设计具备实时检测能力与事后回溯能力的全流量审计方案，提醒隐藏有病毒的应用程序。二是用户访问控制。大数据的跨平台传输应用在一定程度上会带来内在风险，可以根据大数据的密级程度和用户需求的不同，将大数据和用户设定不同的权限等级，并严格控制访问权限。而且，通过单点登录的统一身份认证与权限控制技术，对用户访问进行严格的控制，有效地保证大数据应用安全。三是整合工具和流程。通过整合工具和流程，确保大数据应用安全处于大数据系统的顶端。整合点平行于现有的连接的同时，减少通过连接企业或业务线的 SIEM 工具的输出到大数据安全仓库，以防止这些被预处理的数据被暴露算法和溢出加工后的数据集。同时，通过设计一个标准化的数据格式简化整合过程，同时也可以改善分析算法的持续验证。四是数据实时分析引擎。数据实时分析引擎融合了云计算、机器学习、语义分析、统计学等多个领域，通过数据实时分析引擎，从大数据中第一时间挖掘出黑客攻击、非法操作、潜在威胁等各类安全事件，第一时间发出警告响应。

3.3 大数据管理安全策略

云计算专家李志霄博士说：“数据安全三分靠技术，七分靠管理”[5]。通过技术来保护大数据的安全必然重要，但管理也很关键。大数据的管理安全策略主要有：一是规范建设。大数据建设是一项有序的、动态的、可持续发展的系统工程，一套规范的运行机制、建设标准和共享平台建设至关重要。规范化建设可以促进大数据管理过程的正规有序，实现各级各类信息系统的网络互连、数据集成、资源共享，在统一的安全规范框架下运行。二是建立以数据为中心的安全系统。基于云计算的大数据存储在云共享环境中，为了大数据的所有者可以对大数据使用进行控制，可以通过建设一个基于异构数据为中心的安全方法，从系统管理上保证大数据的安全。三是融合创新。大数据是在云计算的基础上提出的新概念，大数据时代应以智慧创新理念融合大数据与云计算 ，以智能管道与聚合平台为基础 ，提升数据流量规模 、层次及内涵，在大数据流中提升知识价值洞察力。积极创造大数据公司技术融合平台，寻找数据洪流大潮中新的立足点，特别是在数据挖掘、人工智能 、机器学习等新技术的创新应用融合创新。

4 结束语

大数据是信息化时代的“石油”。大数据转化为信息和知识的速度与能力将成为这个时代的核心竞争力之一，而大数据面临的安全挑战却不容忽视。只有大数据技术和大数据安全“两条腿”走路时，大数据才可以真正成为这个时代的驱动力量。

数据安全研究院

数据安全研究院（Data Security Institute），是“数据恢复四川省重点实验室”下设的研究机构，主要从事 DT 时代数据安全技术的发展、运用、解决方案等课题的学术与研究。以自主创新核心技术，从数据本身的安全技术和防御方案着手，重点研究第五空间国家安全战略中的数据安全保障谋略，并由此拓展到计算机发展未来的各行各业，为数据安全行业的发展提供强有力支持。

数据安全研究院在国家和四川省中长期科技发展战略指导下，瞄准国际国内数据安全领域的前沿课题，主要研究数据安全管理、数据应急恢复、数据防止拷贝、数据阅后即焚、数据彻底销毁、数据加密解密、数据安全咨询、数据资源协调；探索新的方法、技术和手段，力争在解决数据安全的关键问题取得标志性原创成果。

数据安全研究院将进一步加大对新一代信息安全新领域的技术和产品的投入力度，在数据恢复、电子物证、失泄密核查和手机数据安全等领域持续拓展。在不断提升与改造现有技术和产品中，不断探索技术的天花板，满足用户需求增长，推出数据安全领域的解决方案，通过科技成果的转化带动地方信息安全产业，充分发挥研究院在技术开发和技术创新领域的引擎作用，为信息安全发展提供数据安全技术支撑体系和创新平台，积极为中国乃至全球的信息安全事业发展做贡献。

数据安全与数字化

身处信息时代大环境，信息安全问题却日益突出。前不久，在中国较具影响力的在线票务平台携程沦陷了，真正的原因不管是否为其官方公布的问题(员工错误操作，删除了生产服务器上的执行代码)，始终，它还是沦陷了。霎时间，携程技术部急得像热锅上的蚂蚁，不知从何入手解决，直到 12 个小时后，问题才被修复。这起事故的发生，引发外界对携程的种种猜测。

其实，互联网企业的运行安全并不是绝对的，类似这样的事故也可以说是司空见惯。但是，就携程这种拥有超过 9000 万会员的平台而言，这起事故无疑让用户开始对自己的信息安全担忧。

实际上，互联网行业，保障用户的信息安全基本上是可以做到的。数据是信息的核心，数据安全就是信息安全的“核安全”，因此，保障数据安全，对数据进行加密或其他特殊处理，从一定程度上说，就是从根本上保障用户的信息安全。

大部分人不清楚信息安全的实质。具体来讲，信息安全包括数据安全、物理安全、应用安全、网络安全和行为安全，其中，数据安全是信息安全的“核安全”，其他为信息安全的“壳安全”，保障“核安全”就是根本保障信息安全。简而言之，数据是 0 和 1 的排列组合，信息的核心是数据，如果能对 0 和 1 进行相关处理，保障信息安全就不再是多大的难事!

据介绍，“数据安全中心”正是对数据底层的 0 和 1 进行二次打乱排列达到加密处理的效果来保障数据的安全性，这在数据安全领域已是较为领先的技术，加密效果极佳。另获悉，除数据加解密外，“数据安全中心”还具备数据检测、数据恢复、数据销毁等功能，能全面应对数据安全保障问题，主要应用于电脑数据安全保障。

大数据时代，信息的安全保障逐渐趋向浓缩为数据的安全保障，数据安全是信息安全的核心，各行各业在生产过程中，加强对底层数据的安全防护已成为保障企业健康、安全发展的必要措施。

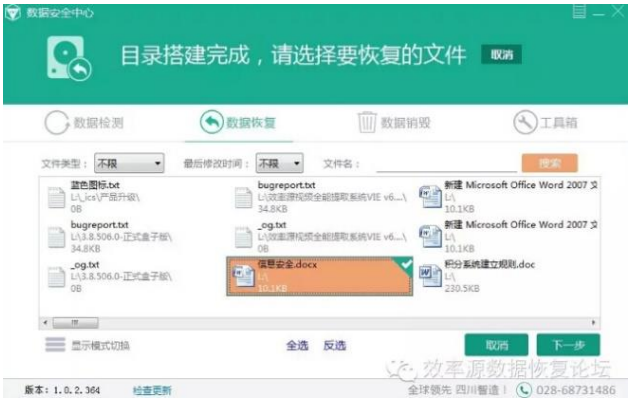
U 盘数据恢复仅需 4 步

U 盘是日常生活中常用的移动存储设备，我们利用 U 盘来转移以及存储一些数据。但是，U 盘并不像计算机有自带的回收站功能。所以，当您在 U 盘上删除数据时，无法还原被删除的数据。那么问题来了，如果您想要恢复 U 盘中删除的文件，那应该要怎么办呢？下面小编就教大家使用一款免费的数据恢复软件—**数据安全中心 DSC**，来恢复 U 盘中删除的文件，本刊还将与大家分享关于 U 盘的使用及保养技巧。

1、打开**数据安全中心 DSC** 应用软件，选中要恢复的分区，进行检测扫描。

2、选中文档文件进行“恢复”操作。

3、开始恢复后，在恢复完成的页面里找到测试用的删除文档进行选中。支持按文件名、文件类型、文件修改时间进行筛选。



4、点击“下一步”，选择恢复文件存放路径。仅需 4 步，数据恢复成功。

Windows 文件删除的原理及其在数据安全中的应用

存储在硬盘中的每个文件都可分为两部分 :文件头和存储数据的数据区。文件头用来记录文件名、文件属性、占用簇号等信息，文件头保存在一个簇并映射在 FAT 表（文件分配表）中。而真实的数据则是保存在数据区当中的。

平常所做的删除，其实是修改文件头的前 2 个代码，这种修改映射在 FAT 表中，就为文件作了删除标记，并将文件所占簇号在 FAT 表中的登记项清零，表示释放空间，这也就是平常删除文件后，硬盘空间增大的原因。

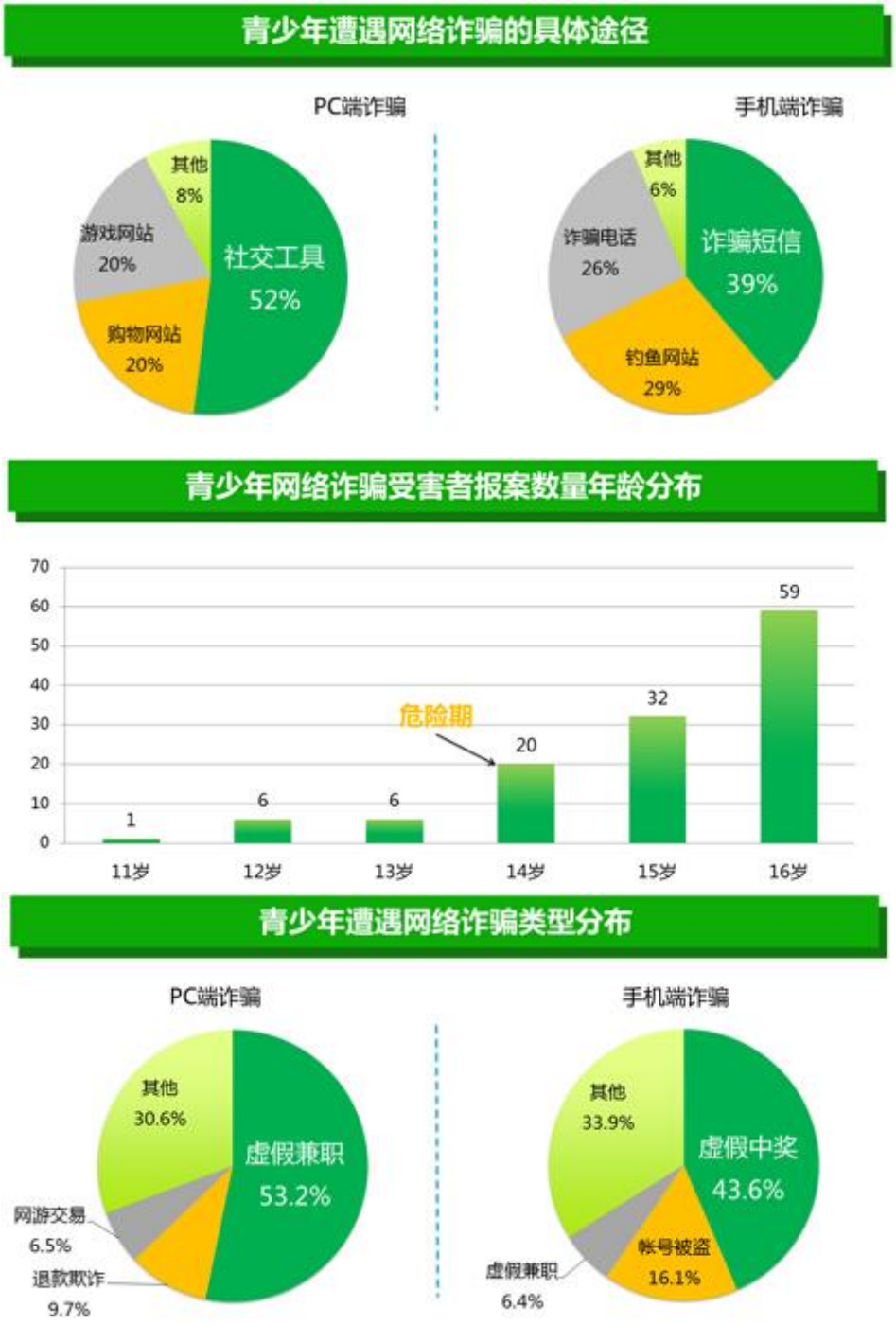
而真正的文件内容仍保存在数据区中，并未得以删除。要等到以后的数据写入，把此数据区覆盖掉，这样才算是彻底把原来的数据删除。如果不被后来保存的数据覆盖，它就不会从磁盘上抹掉。用 Fdisk 分区和 Format 格式化和文件的删除类似，前者只是改变了分区表，后者只是修改了 FAT 表，都没有将数据从数据区直接删除。

由文件删除的原理可知，要彻底删除数据，只有把删除文件所在的数据区完全覆盖掉。绝大部分彻底删除工具所使用的就是这个道理：把无用的数据反复写入删除文件的数据区， 并进行多次地覆盖，从而达到完全删除文件的目的。

Windows 的这种伪删除，虽然给我们带来了好处，让我们有后悔药可吃。但对于很机密的文件就有了麻烦，存在着被重新恢复的可能性。所以，删除机密文件，一定要借助彻底删除工具，让机密文件彻底“粉身碎骨”，这样你就可以高枕无忧了。

推荐一个好用的免费数据恢复软件 :效率源数据安全中心进行恢复，就算把硬盘格式化了，只要没有被覆盖，都可以恢复，而对于无需保留的机密文件 ,效率源数据安全中心提供了数据销毁功能进行彻底销毁，要保留的话，效率源数据安全中心还可以对机密文件进行加密。

2015 青少年上网安全数据分析



中国 16 岁以下的青少年网民数量约为 1 亿至 1.2 亿左右，占中国网民总数的 16%-20%,孩子们利用网络来学习相关的搜索内容仅为 0.6%，甚至比某些不良信息（0.8%）的搜索量还要低。由此可见，希望孩子通过上网获得更多知识和学习机会的想法是不现实的。

方存好：信息安全就在我们身边

摘要信息安全就在我们身边，哪里有网络，哪里就涉及信息安全。本文摘自《四川经济日报》

——四川省经济和信息化委员会副主任方存好

记者：当前四川信息安全产业发展情况如何？有何特点？

方存好：据调研统计，2014 年，我省 148 户信息安全企业实现工业总产值 1281.1 亿元，其中信息安全产业产值实现 183.4 亿元，较上年同期的 137.2 亿元增长 33.6%。

特点有四个方面：一是信息安全产值增速明显高于企业总产值增速。信息安全产业产值增速比企业总产值增速高 18.9 个百分点，信息安全产值对企业总产值增长的贡献率达到 28%，拉动企业总产值增长 4.1 个百分点；二是对电子制造业带动作用初步显现。据工信部初步反馈数据，2014 年，我省电子制造业完成销售产值 4048 亿元，同比增长 19.6%，据测算，信息安全产值对全省电子制造业增长的贡献率为 7%；三是信息安全产业企业形成集聚发展态势。按区域分布划分，全省共有 14 个市州有信息安全产业企业，信息安全产业企业超过八成集中在成都、绵阳两市，分别有 89 家和 38 家，分别占全省的 60.1%和 25.7%；四是企业发展增速明显加快。新增 6 户信息安全产值过亿元企业。2014 年企业总产值过亿元企业 49 户，比 2013 年净增 12 户，信息安全产值过亿元企业 25 户，比 2013 年新增 6 户。

记者：作为被省委省政府确立的五大高端成长型产业之一，就全国来讲，四川信息安全产业有何优势？

方存好：早在“一五”时期，四川就是国家布局的重要电子工业基地，主要从事元件、器件、整机研发和制造，在保密通信、抗干扰、信息安全领域极具特色。1995 年以前，四川信息安全产业长期排名全国第一。近年来，随着国家对这一产业越来越重视，一些项目被新纳入到信息安全产业中来，内涵和外延不断扩展，目前四川在全国排名第二，仅次于北京。

据最新的调研资料，四川信息安全产业技术链和产品链完整，技术水平国内领先。在信息安全系统产品与应用产业方面，主要有党、政、军、电信、金融等核心部门信息系统安全产品 12 类 80 余种。四川在国产密码、互联网安全监测与治理等细分领域的技术水平处于国内领先地位。据不完全统计，四川信息安全企业共获得省部级以上科技进步奖励 411 项，其中国家科技进步奖励 32 项（含一等奖 3 项）；企业大多取得党政和军队信息安全产品相关资质。截至 2014 年，四川信息安全企业共拥有国家授权专利 6585 项，其中发明专利 4346 项，占专利总数的 66%。

记者：信息安全产业是比较特殊的行业，与之联系比较紧密的党、政、军系统及敏感行业（如银行、证券等）对信息安全企业的产品和服务比较熟悉，但普通大众却了解甚少，也并不十分清楚信息安全的具体体现。在人人都需要、人人都已“触网”甚至人人都离不开网络的今天，面对众多的网络陷阱和网络诈骗信息等，四川如何加强信息安全知识在大众中的普及和推广？

方存好：信息安全就在我们身边，哪里有网络，哪里就涉及信息安全。

从层次上讲，信息安全可以分为三个层级：国家安全—行业安全—个人金融安全。前者的重要程度高过后者，这是大家都可以理解的。而从全国信息安全产业发展进程来讲，目前正处在从国家层面向敏感领域拓展完善阶段，比如除了大众所熟知的银行、证券等金融行业外，数量众多的工业企业，特别是自动化生产的企业也正在加紧建设信息安全保障体系，因为通过电源进行网络攻击早已不是新闻。这个过程积累到一定程度，安全服务也必定向大众拓展。但并不是说国家信息安全就不涉及行业和个人信息安全，这其中有很多交叉重合的地方，保障了国家信息安全、行业安全，同时也保障了个人信息安全。

对于信息安全知识在大众中的普及，一是要加强教育宣传，提高公民对信息安全知识的了解，如 6 月 1 日-7 日在省科技馆开展的第二届国家网络安全宣传周活动就是很好的载体；二是要积极引导和鼓励企业开展安全产品（服务）应用体验活动。据我所知，目前已有多家在川信息安全企业实施或者准备实施安全产品（服务）体验馆建设计划，免费向大众提供信息安全服务体验，相信大家很快就能近距离接触到。这方面的体验活动，在全国来说，四川也是走得比较早的。另外，企业也有很多面向大众的安全产品，比如国产的自主可控的北斗导航系列产品，只不过大众更多的是关注产品的实用性、应用性，并不特别去关注产品本身所具备的信息安全能力。

记者：诸多信息安全企业的经营者和参与者多乐见四川信息安全产业发展环境和发展前景，甚至不少投资者和创业者也非常关注这一产业，对此您有何建议？

方存好：建议谈不上，我说一下个人认识。一方面是基于信息安全产业的特殊性，很多重大项目都是国家项目，这一方面政府更多的是做好服务工作，引导企业积极参与到国家项目中去，企业通过参与这些项目来实现自身发展；同时，我们也将积极做好信息安全企业与国内相关部委领导、院校专家的对接交流工作，搭建好项目落地渠道。

数据恢复四川省重点实验室授牌成立

6月3日上午，由效率源牵头申报组建的“数据恢复四川省重点实验室”授牌仪式在内江师范学院隆重举行。。

“数据恢复四川省重点实验室”是在依托单位的强强合作、优势互补的基础上建立的，实验室充分进行资源整合，学科融合，交叉渗透，汇集人才，着力体制机制创新，注重自主创新、自主研发，着力打造国内知名的具有原创能力的研究基地、数据安全产品的生产基地、数据安全高层次人才的培养基地。

授牌仪式上，内江市副市长田文平表示，“数据恢复四川省重点实验室”获牌成立标志着我市校企合作共建的第一个省部级重点实验室顺利诞生，也标志着我市在数据安全技术的研究与应用上迈上了一个新的台阶。双方应以以授牌为契机，进一步加强校企合作，为数据安全方面的教学科研、人才培养、学科建设等方面起到积极的推动作用。

内江市科学技术与知识产权局局长王仕平宣读了立项文件，希望实验室能充分发挥校企合作的优点和特色，开展创新性研究，获得原始创新成果和自主知识产权，为解决经济和社会发展的突出问题提供战略性、基础性、前瞻性知识储备和技术支撑。

授牌结束后，公司总经理梁效宁表示，效率源与内江师范学院的合作是全新的起点，实验室将在数据安全课题上，探索新的方法、手段和技术，推出适合数据安全需要的解决方案，为数据安全提供技术支撑体系和创新平台，努力朝着国家重点实验室的目标迈进。

数据安全研究(半月刊)

每月 1 号，15 号定期相约

关于效率源

四川效率源信息安全技术有限责任公司是：

信息安全领域的创新者、数据安全行业的领军者

国家高新技术企业、双软认证企业、ISO9001 认证企业

知名数据恢复及司法取证设备的供应商

地址：中国四川省成都市高新区天府大道 1700 号新世纪环球中心 E3-E5 区 7 楼

电话：028-68731486；028-85055199

登录效率源官网：www.xlysoft.net

或效率源数据恢复论坛：bbs.xlysoft.net

微博搜索“四川效率源科技”关注我们，获取更多资讯和服务