

ERM捍卫知识产权

Protecting Intellectual Property

文/孙超

近日,历经了长达2年零3个月的调研,北京首钢国际工程技术有限公司(简称首钢国际工程)最终与北京思智泰克技术有限公司(简称思智泰克)达成ERM(企业权限管理)数据安全管理项目合作。身为我国勘察设计行业的龙头企业,尽管首钢国际工程较少涉猎公路交通领域,但对于公路交通勘察设计企业,这次慎重选择或许具有一定启示。

从知识产权说起

知识产权的英文为“intellectual property”,原意为“知识(财产)所有权”或者“智慧(财产)所有权”,也称为智力成果权,最早于17世纪中叶由法国学者卡普佐夫提出,后为比利时著名法学家皮卡第所发展。根据我国《民法通则》的规定,知识产权属于民事权利,是基于创造性智力成果和工商业标记依法产生的权利的统称。

对于个人而言,知识产权是一种特殊的财产权,需要通过对知识产权的保护,激励了人们的创新热情,促进科学技术生产力的发展。对现代企业而言,知识产权就如同生命,随着企业信息化程度的提高,企业的研发、生产等流程越来越依赖于信息系统。同时,企业的核心知识产权数字化程度也越来越高,这些多样的核心知识产权形态,可能是设计文档、图纸或者其它文件的形式。

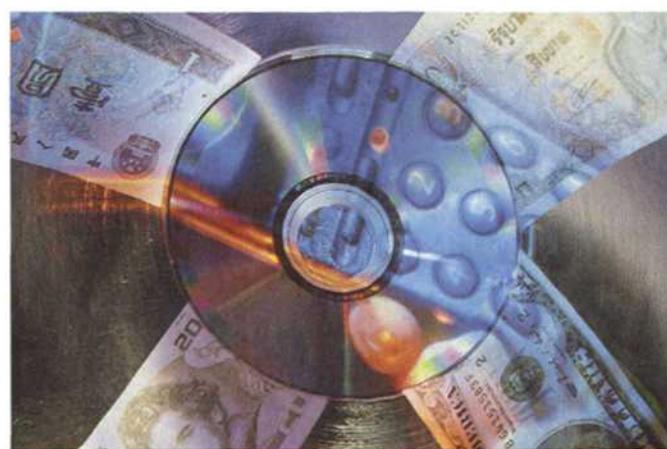
传统的数据保护方案主要有磁盘加密(FDE)、网络传输加密(NTE)、公司内容管理(ECM)、公共密钥架构(PKI)和数据防泄密系统(DLP),但在应用中都有其局限性,虽然他们能够允许或拒绝用户访问机密数据,但不能提供更加细分化的策略权限控制,也就是说它们不能限定用户具体的使用权限。例如PKI等加密技术能够确保只有授权用户可以打开被加密的文件,但是当文件被打开之后,企业便失去了对文件的控制,使用者可以对文件进行任意的操作,为信息的泄密创造了机会。

FBI(美国联邦调查局)和CSI(美国警察局犯罪现场鉴证科)曾对发生过机密信息泄露事件的企业进行调查。调查显示,97%的公司使用了防火墙,72%的公司使用了入侵探测系统,70%的公司使用了基于服务器的访问控制,68%的公司在数据传输过程中应用了加密技术。可见,上述技术没有一种能够从根本上解决电子文档的安全问题,防火墙、网络代理服务器、内容监控和过滤等网络控制手段,在一定程度上限制了网络的访问。但是,对于电子文档本身,这些网络控制手段几乎没有提供任何细分化的权限访问控制。由此可见,这类静态的提供“全部或零”权限的安全工具已经不能满足当今动态的业务需求。

什么是ERM

如今,专业的数据安全产品已经开始浮出水面,它集身份认证、分级管理、权限控制、加密解密、灾难备份、审计日志等多项安全技术于一身,在数据安全领域大显身手——它被称为ERM,也叫EDRM(企业数字权限管理),主要解决数字化资产(电子数据)的有效管理与控制问题。

于是,为了确保机密数据信息的安全,越来越多的公司借鉴数字版权管理解决方案,称为企业权限管理技术,即ERM。它主要用于公司的电子文档和邮件的安全管理,有效控制电子文档内容的具体使用权限。例如哪些人在什么时候,能够对文档进行哪些操作,这些操作权限包括阅读、拷



页，打印，转载，保存和编辑等等。

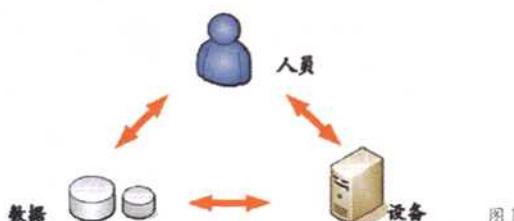
由于ERM通过保护文档本身来实现机密数据的安全，所以无论机密信息存储于哪一台计算机上，ERM所具备的访问保护和使用控制策略都能够将文档的应用权限准确细分给不同的用户，从而避免机密信息被流失，窃取和修改。ERM解决方案具备集中式管理，强大的报表和审计等符合企业管理需求的功能特点，并且整合了其他IT基础结构的主要功能，从而使这一方案从其它方案中脱颖而出。

我们需要ERM吗

勘察设计企业需要保护的知识产权范围很广，从勘察设计成果文件的创作权，到设计竞选方案和自行编制的设计手册、企业标准、导则、手册、资料、通用图的版权，从单位的注册名称、商标及图形标志，到专利、专有技术和科研成果，自编或二次开发的计算机应用软件和程序，以及能带来收益的经营管理信息及需要保护的来自知识活动的权利等。

对于勘察设计企业来说，图片文档设计是最终的生产成品，也是整个单位的知识产权、技术积累的载体。随着勘察设计企业信息化程度的提高，图片文档设计多以数据信息的形式存在，数据信息的载体电子文档的安全直接影响着勘察设计企业的数字信息安全。电子文档的易复制、易传播等特点导致了它的安全风险大大超过传统纸质文档。数据安全已成为勘察设计行业关注的焦点，建立健全数据安全管理体系对勘察设计企业的安全管理工作和发展意义重大。

目前，勘察设计企业信息管理主要有人员、设备、数据三个因素（见图1）。



从人员、设备、数据三个因素在信息安全管理中的管理方式及特点对比中（见表1）我们可以看出，对数据的管理是最安全最便捷的。

要素	角色	管理方式	具体特点
人员	信息应用者	被动式管理	主观性强，管理者很难了解制度的真正执行情况，管理难度大
设备	信息应用平台	被动式管理	由于设备的不断发展，管理手段容易滞后于设备发展，由此产生管理漏洞
数据	信息本身（载体）	主动式管理	对数据信息本身进行安全保护，可以确保无论在任何平台环境及使用者，数据信息都将被安全保护，全面摆脱了应用者和应用平台的限制

不同于传统的数据保护方案，ERM方案对机密数据的保护更贴近于数据的使用，同时也更广泛的覆盖了数据的整个生命周期。如图2所示：



图2

依据勘察设计企业数据安全保护特点，通过整合自身数据加密技术、数据生命周期管理技术，对机密数据在生命周期的五个阶段（图3）分别进行控制管理，形成了一套独具特色的数据安全管理解决方案，数据安全管理体系。

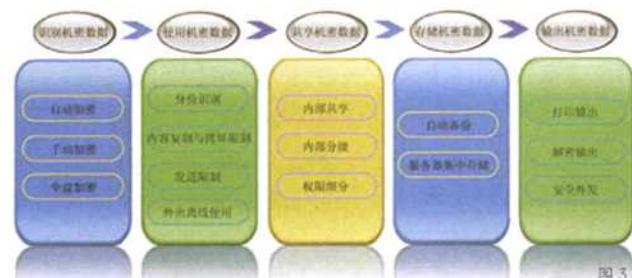


图3

ERM不但能够对 Microsoft Office、CAD、PDF 等任意格式的电子文档及设计图纸进行加密保护，并且能够对加密的文件进行细化的应用权限设置和备份保护，确保勘察设计企业的机密数据只能被经过授权的人，在授权的应用环境中（例如企业内部），在指定的时间内，进行指定的应用操作，并且整个过程会被详细、完整的记录下来，解决了数据安全管理中数据防泄密和机密信息权限管理这两个层面的问题。

由此可见，通过实施ERM，可以有效杜绝机密信息泄漏和窃取事件的发生，提升勘察设计企业的核心竞争力，优化流程，将管理的执行力度深入到数据信息的具体应用层面，从而推动勘察设计企业的发展。

表1