当数据丢失防范成企业必需思科认证 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/644/2021_2022__E5_BD_93_E6_95_B0_E6_8D_AE_E4_c101_644136.htm 数据丢失问题如今已经成为广大企业最关心的焦点问题之一，目前有两种主要的因素驱使企业进行数据丢失防范工作：要遵从的法规和知识产权保护。随着个人信息的泄漏事件的不断发生，各国对于这类事件不断发布了一系的安全法规，例如萨班斯法案和我国即将执行的《企业内部基本控制法》。通过这些法规，让企业对其所保存的员工个人信息、客户信息，以及供应商或合作伙伴的信息必需妥善保管，并且担负造成这信信息丢失的相关法律责任。因此，如果企业不想为此而引起法律诉讼的话，就不得不为它所保管的所有信息进行必要的丢失防范。 企业要想制定一个行之有效的数据丢失防范策略，在一开始就必需对企业当前各种引起数据丢失的因素有所了解，对数据的重要性和丢失带来的损失进行有效的评估等。 一、企业机密数据有哪些 不管怎么说，数据丢失防范的第一步总是从调查企业内部有哪些机密数据开始的。通常，对于处于现在这种高度竞争商业环境中的各类企业来说，知识产权数据是最重要的。企业知识产权包括：技术、方法、工作模式、处理流程、生产计划等，它们还可以是各种图表和流程图，供应商数据，定价数据和营销战略，或者程序源代码，营销数据和客户数据等等。 这些都是企业的商业机密，其中任何一部分数据的丢失，都会给企业带巨额的经济和声誉损失，有时还会带来法律诉讼。但是，使用这些数据的员工有时却并不知道它们是企业的商业机密数据，因而就有可能在有

意无意之中造成这些机密数据的丢失。 二、了解数据丢失问题 对于企业来说，现在企业数据最大的安全威胁是来自企业内部，例如企业内部员工的有心无心之过。而恶意软件、木马、垃圾邮件及黑客攻击是紧跟在其后的安全威胁之一。调查显示，由于内部原因造成的企业机密数据丢失，其数量要远远大于外部安全威胁所造成的损失。 那么，企业机密数据是如何从内部漏泄出去的?要了解这个问题，先来看看数据在企业内部网络中所处的方式。 它一共存在三种主要的方式：1、数据在移动之中，是指数据正在企业内部同网段之间，以及跨网段之间传输，并且随时会经过企业网关转发到Internet上。 2、数据在静止过程中，是指数据正驻留在企业内部文件服务器、数据库或其它存储设备中。来源：www.100test.com 3、数据在用户终端之中，这些用户终端包括USB设备、CD/DVD刻录机、MP3/MP3播放器、笔记本电脑，或其可移动存储设备等。 当数据处于用户终端设备之中时，绝大部分是在使用当中。而数据主要是在移动过程和在用户使用过程中，由于人为有心无心造成丢失的。因而，要防范企业机密数据丢失，主要是在这两个方面做足工作。但这也并不意味着企业机密数据只会通过这几种途径造成丢失，其它方式也有可能，例如打印机、数码复印机、传真机、无线产品等，以及一些Internet协议，例如HTTP、HTTPS、IM、WEBMAIL、电子邮件、FTP等都有可能会引起企业机密数据的丢失。也不是说数据在静止状态时没什么意义，我们可以通过数据扫描的方式来找到存在于企业网络中所有位置中的机密数据和敏感信息，以便了解要保护的数据存在什么位置之中，然后才能确定对什么设备进行重点防范。因此

，要防范数据丢失，与其它安全防范方式是不相同的，必需制定一个非常全面的安全防范策略才能够有效的解决这个问题。 三、为什么数据丢失非常普遍 无论是在途中，还是在办公定，或者在家中，我们都可以通过各种电子连接方式与近在咫尺，或远在天涯的人联系，电子访问方式已经越来越成为日常商务活动中最主要的途径。 我们在通过电子方式进行全球合作的时候，也为机密数据的丢失打开了潘多拉之盒。在过去的许多年以来，我们都将所有的安全防范精力集中在对外部威胁的防范之上，但根据调查显示，其实超过一半以上的企业机密数据是通过企业内部泄漏出去的。可是，一些企业现有的安全防范措施，例如防火墙或入侵检测防御系统(IDS/IPS)，对于来自内部的正常数据流都是完全放行的。这让企业花费大量心血的安全防范措施显得非常的可笑，也让企业内部机密数据的丢失变得只要点击一下鼠标这么简单。而且，大多数数据丢失都是无心之过，当员工将企业机密数据透露出去后，可能还不明白刚才发送的电子邮件或粘贴到博客上的图片及文本正是企业的机密数据呢! 同时，随着USB设备、MP3播放器、笔记本电脑等移动设备的大量使用，在这些设备之中，往往承载着企业大量的机密数据，而这些设备更加容易被带到企业外部。调查显示，移动设备也已经是造成企业机密数据丢失的主要原因之一。 四、数据丢失的核心是不受控制的通信 如今，电子通信无处不在，数据在移动时就很容易造成数据丢失。例如，员工将文件发送到他的电子邮箱中，以便他回家时一样能处理.医师将病人病历信息错误地发送给其他人；或者一个雇员将新产品还没有发布的图片贴到了自己的博客上。所有的这些，都可能造成企

业机密数据的丢失。 但是，这还不是数据在移动中造成丢失的唯一途径，另外还有其它的通信方式可以将企业机密数据或敏感信息由内转发到Internet上。所有的这些包括： 1、电子邮件 2、WEB邮件 3、QQ、MSN等即通信软件 4、P2P软件 5、论坛、留言板 6、博客 7、网络存储 8、FTP 但是现在的防火墙和其它安全解决方式对于数据丢失防范的能力还不够完善，数据丢失防范需要更加严格的控制。例如深入的内容扫描、阻止可能包含机密信息的通信会话，或者应用强力加密等措施。同时，如果企业对数据丢失防范做了许多重要的工作，但是没有对员工进行相应的安全教育，以及对其行为进行有效的管理和监控。那么，所有的数据丢失防范工作将变得一无事处，机密数据仍然会通信各种途径泄漏出去。 数据丢失解决方案必需降低数据在静止及处于终端设备上的风险，但是，对于任何一个发展健康的企业来说，任何时期都有机密数据在移动当中。这样，就要求企业必需制定一个更加全面的数据丢失防范解决方案，以防止雇员、企业顾员、供应商、合作伙伴或其它授权用户将企业机密数据发送到企业之外。与此同时，还必需进行深入多层次的解决方案，来防止机密数据通过电子邮件、WEB邮件、即时通信软件或P2P等途径泄漏出去。 不管怎么说，现在，数据丢失防范已经成为各类企业安全防范策略中的必需品，企业必需根据自己的实际需求，制定一个行之有效的数据丢失防范策略，然后将它由上至下全面执行，才能将数据丢失带来的安全风险降低到企业可以接受的水平。 编辑特别推荐: WindowsSBS2008实战之管理共享打印机 WindowsSBS2008实战之管理文件和文件夹 WindowsSBS2008实战之管理远程工作网站 100Test 下载频道开