警惕最棘手安全问题移动技术的安全风险 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/287/2021_2022__E8_AD_A6_E6_83_95_E6_9C_80_E6_c97_287901.htm 如果信息技术无处不在，谁来负责安全风险?读过本文，即便最棘手的风险问题也将迎刃而解。 今年2月，盗贼持枪抢劫了美国英提格瑞斯卫生署(Integris)一家家庭医疗服务商的笔记本电脑。英提格瑞斯卫生署的首席信息官(CIO)约翰迪兰诺(John Delano)面临两项首要任务：确保员工安全和保护笔记本电脑上的病人信息。幸运的是，员工安然无恙，加密过的病人信息也丝毫无损。到目前为止，该公司的移动技术风险战略发挥了重要作用。 近来，人们对笔记本电脑、智能手机、便携媒体等移动技术的使用大大增加，同时也使商业信息面临新的风险。根据安全咨询机构波耐蒙研究所(Ponemon Institute)在2006年发布的一份报告，超过54%的安全侵害行为是由于笔记本电脑、移动设备或电子备份数据丢失引起的。目前美国几个州政府已经制订了有关数据泄漏的法律条文--从另一个方面来看，这也促使CIO们对客户信息保护工作予以高度重视。 尽管使用移动设备存在风险，但由于他们能够提高工作效率，同时也因为基础设施更加完善，移动设备用户正在迅速增加。一份2006年的费雷斯特(Forrester)报告显示，几乎三分之二的美国公司正在使用无线网络，而移动通话和数据传输的费用在去年的通信预算中占到近四分之一。 危机四伏 移动技术、特别是那些被首席执行官(CEO)、公司高管、销售和顾问使用的移动技术，往往涉及销售额和电子邮件等极为敏感的公司资料。而最新的移动设备具有更大的储存容量和更强的互联

网访问功能。 存储量增大的后果是更多数据处于被盗、丢失或使用不当的风险之下，CIO们为此深感担忧。同样让他们担心的是，多数商业用户不会在非安全的环境中采取适当的安全措施。例如，2003年发生了一次令人担忧的事件：一台从eBay购得的黑莓无线设备被发现存储着1,000多人的姓名、电子邮件地址和电话号码，以及200多封公司内部邮件。出售这台设备的人想当然地认为，卸下电池以后数据就会被全部删除了，结果却出乎他的意料。 同时，更多人对移动环境发起攻击。去年，反病毒厂商发现了200多种手机病毒。间谍软件、网络钓鱼软件、域名欺骗软件、恶意软件、零时差浏览器攻击、以及僵尸网络等攻击软件正在迅速蔓延。据Trend Micro公司的调查显示，仅仅针对Windows智能手机设备，就已经发现了约30种恶意软件。微软估计有将近一千两百万人在使用智能手机。 美国《加州参议院1386号法案》和《1996年健康保险流通和责任法案》等隐私条例针对非公开的个人信息制定了披露标准和保护标准。法律规定，对那些获取并存储个人信息的公司来说，如果发现某个公司对个人身份信息处理不当，该公司必须向公众说明情况，这无疑是更大的挑战。 以医疗领域为例，病人的个人信息存储在医生和护士的多种移动设备上。今天，远程诊断中心可以向医生的智能手机发送病人的心电图。正因为移动设备已经变得不可缺少，《1996年健康保险流通和责任法案》将保护病人信息作为绝对强制性的要求。根据联邦法律，对医疗信息使用不当将牵涉到一定程度的刑事和民事责任，有可能遭到25万美元的罚款和长达10年的监禁。 在这一背景下，因为遭受数据侵害而丢失个人信息已经成为超越IT部门的商业问题。负面的公

众形象是昂贵而难堪的，这将使消费者和投资者失去信心。