经济危机时期提高企业安全性的十种方法Cisco认证考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/585/2021_2022__E7_BB_8F_E6_B5_8E_E5_8D_B1_E6_c101_585036.htm 当前，很多企业面临的挑战是如何找到安全与支出之间的平衡，当整个企业都在努力降低成本的时候，IT管理员要如何说服公司投资安全工具呢?人为错误通常是企业存储环境面临的最重要的安全错误，随着2009年网络犯罪和身份盗窃的不断增加，企业需要更加警惕防御抵制因为人为因素而导致的钓鱼攻击和社会工程攻击。 企业不能忽视安全问题，即使预算紧张，安全泄漏、数据丢失和停机时间造成的总成本损失都远远超过企业需要花在保护数据和网络上的钱。如果企业安全成为经济危机时期的另一个受害者，那么短期收益将可能造成长期损失。可以通过部署安全最佳做法组合来实现安全性，而下面的10个步骤可以帮助企业在严峻经济环境下解决安全威胁问题：1. 确定问题所在 对所有部署的安全措施和设备进行广泛的审计所有的硬件、软件和其他设备，并审核授予企业内员工的所有特权和文件权限。积极测试存储环境的安全性并检查网络和存储安全控制的日志，如防火墙、IDS和访问日志等，来了解所有可能的安全事件，事件日志是很重要的安全信息资源，但是常常被忽视。 2. 监测活动 全年全天候对用户的行为进行检测，对于单个管理员你，检测事件日志并定期进行审计是一项艰巨的任务。但是，检测存储环境比检测整个网络要更加现实。日志被认为是很重要的资源，因为如果安全泄漏发生的时候，日志可以用于随后展开的调查。日志分析能够帮助管理员更好地了解资源使用的方式并能够更好的管理

资源。 3. 访问控制 对数据的访问权限只能授予那些需要访问数据的人。 4. 维护信息 保护所有企业信息。使用不受控制的移动存储设备，如闪存驱动和DVD等，让大量数据处于威胁之中，这些设备很容易丢失，并且很容易被盗窃。在很多情况下，位于移动存储设备的数据经常没有使用加密技术来保护。 5. 需要知道和需要使用 制定技术政策，根据明确的政策来使用设备。最近的研究表明，当人们被炒鱿鱼的时候，这些人泄漏数据的比率不断增加。移动设备(如USB棒或者PDA)可以容纳大量数据，检测网络中这些设备的使用是降低数据泄漏风险或者不满员工的恶意行为的关键因素。仅限于真正需要使用移动设备的人使用移动设备。 6. 数据处理政策 实施严格的安全政策，包括数据是如何处理的、如何访问和转移等。单靠技术本身是不足以保护公司数据的。强有力的可执行的安全政策，以及员工和管理层对安全问题的认知，将能够提高企业内的存储安全水平。 7. 简单的员工沟通 用简单明确的语言向员工解释每一种政策的含义，和政策部署的方式。 8. 员工教育 员工需要注意，不应该将自己的密码写在粘贴在监视器的记事贴上，他们需要了解共享密码就像共享自己家里的要是一样。需要告诉员工不能在未经认证的情况下，将任何信息透露给第三方，他们需要对安全和最常见的威胁(如电子邮件钓鱼和社会工程)有基本的了解。另外，他们需要注意他们的行为正在被监视。 9. 备份所有的东西 备份所有通信和数据，定期检查备份以确保公司的网络崩溃的时候，能够在短时间内获取所有信息，你当然不希望备份遭到破坏。 10. 人员管理 存储安全比使用各种安全技术保护数据更加重要，这也是训练人事管理的机会。使用和创建数据的

人是最大的安全威胁和最薄弱的安全环节。 虽然安全开支整体预计将增长，“ 少花钱，多办事 ”仍然将成为2009年安全行业的主体。按照上面提供的基本技巧，企业可以在不损害IT安全的情况下，度过这段严峻的经济危机时期。 