信息安全管理

作者： Jim McCrory, Daniel Lohmeyer, Sofya Pogreb
来源：《麦肯锡高层管理论丛》 2002.2

信息安全的维护，不再只是 IT 部门的职责，与营运和科技也息息相关

骇客、计算机病毒和挟怨报复的员工攻击企业信息系统的事件层出不穷，让企业不得不花费大笔金钱以作因应。据报，美国企业去年共发生五万三千件系统遭侵入事件，比 2000 年增加了 150%。诚然，因考量事件曝光可能影响形象而秘而不宣的企业所在多有，因此实际数字高出许多，据估正式通报的系统侵入事件仅占真实数字的三分之一。

信息安全虽一向被视为 IT 部门的职责所在，但也有公司开始体认到这个问题事实上与营运和科技均有关联。今年我们针对财星 500 大企业在信息防护方面堪称最佳典范的公司进行研究，特别是其中新近指派资深业务主管负责信息安全事务的 30 家公司（根据 Gartner 2001 年 4 月的估计，全球 2000 大企业(Global 2000)中一半以上的公司在 2004 年前都会设置类似的职位）。已有不少财星 500 大企业开始着手在保护企业信息安全的现行措施中，加入策略、营运和组织面的安全防护考量。

技术部门经理人已坦承，今日的信息科技无法保证网络绝无遭渗透之虞，而在骇客不断的挑衅下，新的安全防护技术生命周期也越来越短，但是，大部分企业仍将信息安全视为只有技术性解决方案才能解决的技术性问题。

企业将维护信息安全的责任完全交给技术人员的同时，也忽略了一些只有业务部门经理人才能解决的基本问题。举例而言，公司各种信息资产的价值不尽相同，有些资产也许需要投注较多的心力维护。Egghead.com 是一家网络零售商，2000 年 12 月因其客户资料系统遭骇客破坏，造成 370 万组信用卡号外流，股票价值因而下挫了 25%。Egghead 这家公司事前当然建置了安全防护系统，事后并宣称资料并未被窃，但由于公司内部缺乏协调，未能提出一致的响应，因而无法说服客户和股东相信这些极为敏感的资料仍安全无虞。

在我们的调查中，美国线上时代华纳、美林证券、微软、旅行者产物意外保险（Travelers Property Casualty）和 Visa 国际组织等企业，均体认到信息安全不仅是技术问题，因此都设有一名信息安全长（chief security officer，CSO），和业务主管、IT 部门经理人共同合作，评估万一公司失去重要信息系统，将面临什么样的商业风险，并将信息安全防护方面的支出列为公司优先事项之一。信息安全长的任何决策，都是对于公司本身、及其愿意承担的风险性质和程度有充分了解之后，所做的决定。

典范企业里的信息安全长，不仅在信息安全事务方面较 IT 经理人具备更宏观的视野，也有

实质的权力改革公司的营运。例如，欧洲某家大型银行个人金融部门的信息安全长，在信息安全的顾虑下，即可下令暂停新产品的推出、分行或信息系统的建置。相反的，在一般公司里，IT 部门中负责安全事务的经理人除了信息安全问题外，几乎无法在整个系统内发挥更大的影响力。

信息安全长的决策只有执行长有权推翻—但这种情况很少发生。除此之外，在典范企业里，信息安全长都会进行严格的信息安全检查，确保员工得到信息防护措施相关的适当训练，并明订存取企业信息权限的管理程序。举例来说，一旦有员工离职或遭资遣，人力资源系统便同步进行资料更新，限制该名员工再度进入办公室、使用电子邮件和文件。

信息安全和信息安全长扮演的角色，因产业、公司资料的价值和其面临法律规定的松紧程度而异。医疗保健组织是诸多例子之一，其所保管之病历资料若有遗失或更动，都可能危害病患健康，导致伤亡－正因其属于可事先避免的风险，因此更不容许这种差错发生。

今天，大多数工商领袖对信息安全的重视程度，就如当年对信息科技一样不足，但如今信息科技在执行长心中的地位已不可同日而语，在企业的策略规划检讨会议中，也得到更多的关注，同样的趋势应该也会出现在信息安全的相关议题，要求高阶管理团队投注更多的心力。在现今网络连结的世界当中，盗取、破坏他人专有信息的骇客已然猖狂，导致企业营运暴露于高度风险之中，因此企业再也不能纯粹地认为这群人是令人厌恶的系统侵入者，以为单凭科技手段即可远离祸患，否则损失将十分惨重。