

如何通过安全教育和培训来降低 IT 风险

作者：Paula W. Hamm, Symantec 教育服务副总裁

IT 风险管理就是在以下两者之间找到平衡点：一方面，开发可靠而安全的 IT 基础架构需要成本，另一方面，要考虑如果发生事件企业可能会蒙受的损失。IT 风险管理通常分为四类：

- 安全性：将不受欢迎的内容阻挡在外，防止泄露重要信息。
- 可用性：维护系统并确保快速恢复。
- 性能：优化资源并确保正确的配置。
- 遵从性：确保适当的控制并实现证据收集自动化。

企业 IT 相关事件正日益受到公众的关注。笔记本电脑被盗导致未加密的个人信息丢失、信用卡号码从企业 IT 系统中被盗、计算机故障导致业务中断，以及 IT 基础架构由于不堪负载而无法为企业客户提供服务等，此类事件在头版头条新闻中时有所闻。

让员工充分参与整个流程

教育员工，使其了解 IT 风险对企业有何影响，这是正确管理这些风险不可或缺的步骤。企业往往注重通过投资引进新技术来降低风险，却没有充分利用最重要的资产——人。

企业 IT 相关事件的常见内部原因包括，密码保护不力、未更新防护软件、未扫描文件、在不适当的时间浏览网页 Web 和下载文件，以及陷入社交骗局（用于操纵他人行为或诱使泄露机密信息的技术）。这些事件的潜在影响是导致基础架构暴露在各种风险之下，使企业很容易遭受入侵、攻击并丢失专有信息。这些安全缺陷还会导致很高的病毒感染率（和再感染率）并降低网络的可用带宽。最终的结果将是因停机而导致生产率下降，以及因修复程序和更换丢失或被盜的设备而导致成本增加。

人是宝贵的资源，并且在确保 IT 基础架构安全方面扮演着重要角色。通过适当的培训和教育，员工可以在降低 IT 风险方面发挥重要作用。根据 Gartner 发布的报告，实施有效的安全意识计划可以减少花费在响应安全事件上的时间，并可因此提高 25% 的生产率。¹这也意味着员工可以专注于其最擅长的领域，即他们的本职工作。

通过教育降低风险

与通常的观念不同，管理风险的责任并不应该由 IT 部门独自承担。安全是每一个人的工作，并且在信息安全方面，人与技术、策略、流程和指导原则同样重要。但是，要求员工在毫无准备的情况下处理当前安全环境的复杂问题和细节并不现实。通过适当的教育和培训，员工可以成为组织最坚强的防线和最宝贵的安全资产。

在设计培训计划时，IT 组织应牢记四大风险管理类别：安全性、可用性、性能和遵从性。此外，还应该遵循下文所概述的一些最佳做法。

¹ Gartner: Information Security Awareness Training Is Essential to Protect IT Assets（信息安全意识培训对于保护 IT 资产至关重要）。Witty, Roberta J 等，2005 年 1 月 11 日

安全风险

- 改善事件的报告和处理方法
- 妥善区分并保护知识产权
- 减少使用即时消息传送等不安全的通讯方式
- 设计并实施更安全的应用程序和基础架构
- 教育全体员工了解安全意识的重要性

可用性风险

- 采取更主动的方法来处理 IT 可用性问题
- 展示合理的备份流程的重要性
- 增加对电子邮件附件和文件下载等常见病毒和特洛伊木马攻击载体的了解
- 教育应用程序开发人员了解构建可靠而稳定的应用程序的重要性

性能风险

- 示范如何正确使用网络资产（例如不在工作时间观看在线视频）
- 在 IT 系统设计中提高对系统性能的重视程度
- 加强应用程序架构师和开发人员的教育和培训，使他们在 IT 系统与性能相关的问题方面，能施加更多的正面影响

遵从性风险

- 支持并遵守内部 IT 安全防范和业务策略要求，以满足 FISMA、Gramm-Leach-Bliley、HIPAA、Sarbanes-Oxley、COBIT 和 ISO 17799:2000 等遵从性标准的要求

要成功地保护信息资产，从上到下的各级员工都要对安全风险和策略以及他们自己在保护公司资产方面相应的责任有一个基本的了解。否则，组织便无法要求员工负责保护组织的资源。

总是在安全事件发生后才进行处理的“被动”安全模型中已经无法满足当今的需要。如今的安全环境已变得非常复杂，采用被动安全模型的企业将始终处于穷于应付的状态。而与时俱进的企业必须积极应对，让员工更多地参与企业的 IT 风险管理策略。从长期来看，这是降低相关成本并保持安全水准的唯一方法。

###