

CIO 安全达标指南

这类消息令 CIO 们夜不能寐：据称，由于零售商未能对安全隐患做出补救，网络入侵者盗走了 80GB 客户数据，包括 1 亿多个信用卡和借记卡账号。¹

如果能够遵从支付卡行业数据安全标准(PCI DSS)--这一全球针对处理、传送或保存大量信用卡数据组织制定的要求，存在问题的企业可以避免不利的公众影响。但未达标的情况并不鲜见。尽管这些要求已实行多年，并对违规行为进行了严厉处罚和罚款，更不必说违背安全规定要接受严肃处理。但许多规模大小不等的组织，仍未能在规定的 2007 年 12 月 31 日最终期限满足 PCI DSS 标准。²

支付卡行业的重任

如果您的公司在最终期限达标，您可以确保至少满足最低要求，您的安全网络管理策略是行之有效的。不过，如果不能满足最终期限要求，也不必为此伤脑筋，而是可将其视为机遇加以利用。这是因为：PCI 标准完全可以成为整个安全风险管理体系的基础。正像迫使每一 IT 组织系统评估并应对各种挑战的“千年虫”(Y2K)问题一样，成为 PCI 达标企业也为您提高 IT 系统整体安全功能提供了机遇。

PCI DSS 将 12 项要求分为六个“控制目标”：³

- 构建并维护安全网络
- 保护持卡人数据
- 维护漏洞管理计划
- 实施可靠的访问控制措施
- 定期监控和测试网络
- 维护信息安全策略

正确的态度是，像保护企业信息资产一样，将保护卡商和客户落到实处。更重要的是，这一标准解决的事件识别、风险评估、风险响应与控制措施等关键领域的问题，也关系到遵从大量美国监管规定，这些规定适用于任何在美国开展业务的公司，其中包括萨班斯·奥克斯利法案、美国金融服务法案(GLBA)和健康保险流通与责任法案(HIPAA)⁴，以及美国 37 个州保护消费者个人身份信息(PII)的民事和刑事条例。

除提供安全保障外，PCI DSS 还有助于优化监管和遵从活动，从而节省您的资金。遵从 PCI DSS 标准可以帮助您将 IT 安全措施与整个业务流程全面整合，通过消除冗余建立更加有效的安全模式。但这并不是一劳永逸的，确保长期遵从标准是一个持续的过程，需要始终保持良好的安全状态。

从何处着手

无论您的遵从机制完善程度如何，都有必要评估您的安全现状，系统地完成 PCI DSS 任务：

- 根据 PCI 标准对比您的安全流程
- 了解您的系统与标准之间存在的差距
- 制定弥补差距的计划
- 确定实施计划所需资源
- 消除差距
- 遵守定期审计规定

大型组织实现达标是一项庞大的任务，不可能通过一个项目完成。考虑到由基层部门来执行这一因素，需要首先弥补创造收益最高的部门，或者风险最大的部门存在的差距。利用这种方法完成治理工作，便于在更可控的条件下实现企业达标。

同时还应认识到，PCI DSS 是一项很难完全通过内部管理来完成的任务。如果您的组织属于大量愈期未达标的企业之一，有必要依靠合作伙伴为您的补救计划提供技术和资源支持。拥有丰富经验的合作伙伴可以设计整体方法，帮助您满足监管规定，同时有效改造安全基础设施。

信息来源：

1. ["TJX 入侵者在未被查觉的情况下盗走 80GB 数据"](#) 作者 Evan Schuman, eWeek, 2007 年 10 月 25 日
2. ["Visa : 65% 的大型零售商 PCI 达标"](#) 作者 Evan Schuman, eWeek, 2007 年 10 月 25 日
3. ["支付卡行业 \(PCI\) 数据安全标准" 1.1 版](#), 2006 年 9 月
4. ["PCI 达标产生的效益"](#) IBM, 2007 年 9 月