银行金融信息安全概略(冯再；2004年1月19日)

文章作者：冯 再

加入世贸组织后，中国金融市场将逐步开放，进一步融入世界经济，中国的经济发展将进入新的发展阶段。作为中国经济发展的核心，中国银行业如何应对挑战，并抓住机遇，将成为中国经济向上提升的关键。而金融信息化和信息网络化是中国银行业顺利转型，迅速与世界金融体系接轨的必经之路。

中国银行业近年来已形成了向商业化发展的方向，即提供以顾客为中心的金融产品和服务，许多银行开始或已实现了数据集中，建立网络及提款终端，发行银行卡，甚至提供网上银行服务。这一发展方向是以金融信息化和信息网络化为基础的，并以此发展先进的网络化金融机构模式，增加加入世贸组织后的竞争力。

面对日益激烈的竞争，国外银行利用信息技术实行产品优化，产品层次也随网络技术的广泛应用不断提高，向客户提供知识管理和客户管理产品，加强银行和客户的关系和服务质量。

随着网络化的普及，通过商业网站向客户提供多种多样的银行服务在国外，尤其是欧美银行已相当普遍。市场研究显示，全天24小时的网上银行受到普遍的接受，上网管理个人账户在国外已开始流行。客户上网可查询信用卡账单，在不同的地点上网转账，打印月结单。

信息和网络技术的推广应用给人们带来方便的同时，利用信息网络技术犯罪也在迅速增长。据CERT统计，2002年中心接到的事件报告82094件，相比2001年度的52658件增加了36％。这些事件包括了电脑病毒、网络攻击以及利用电脑系统或应用软件进行的攻击事件。据美国联邦调查局揭露，一个东欧黑客团体于2001年非法侵入340多个商业网站，盗取了一百多万个信用卡号。美国联邦法院2003年所审理的一系列有关信息犯罪的案件中，至少有三件涉及金融机构。这些统计数字和报道出的事件相信只是我们面临信息安全威胁的冰山一角。

在加入世贸组织之后的大环境下，中国银行业不应仅仅看到信息网络化提升竞争力的一面，信息网络技术应用对银行金融业务带来的潜在威胁及安全隐患也应给予重视，对将面临的风险和可能导致的损失也应有足够的认识。参照国际通用的信息安全标准及国内外在信息安全方面的经验，制定适合中国银行业金融信息系统的安全法律、法规和策略，并加以有效的监管是提升中国银行业竞争力的重要一环。

以下对银行业的金融信息安全进行简单描述：

首先，政府的金融监管机构负责督导受监管的银行金融机构按照相关金融信息安全法规制定和实施各项具体的信息安全措施。

一、风险评估

风险评估是制定信息安全策略过程中的第一步。如何做好风险评估，关系到一个机构如何进一步制定和实施各项信息安全措施，检测并保持这些措施的实施。初步的风险分析完成后，并不意味着整个风险分析过程的结束，它仍将是后续信息安全工作的重要一环。

风险评估的三步骤：

1、收集数据：

数据收集的对象包括银行的重要资产，这些资产可能面临的威胁，机构中或者技术上存在的安全隐患，以及已实施的各项安全措施。收集数据时，应建立一份关于银行信息系统资产清单，列出所有相对应的安全隐患。可能涉及到的信息系统有：

系统软件、应用软件、数据库、网络、无线网络、服务器、工作站及远程接入设备等。

2、分析数据：

在收集数据的基础上，分析各信息系统的特点，找出并测定针对这些系统的威胁，分析评估各种已知及未知的威胁，分析各种威胁形成的条件和可能造成的后果。

3、评级排序：

在分析研究各项数据的基础上，对风险评级排序，制定可行的风险转移策略。

二、制定信息安全策略

机构领导应制定机构的信息安全策略，列出目标和实施方案。根据美国信息安全实施的经验，相关的法规和指导都强调有关机构的领导层参与机构的风险和信息安全管理的重要性。信息安全管理不仅是银行信息管理部门的职责，也是各级政府和机构领导应首先给与重视的议题。

建立安全措施，贯彻执行这些措施，并监督执行的有效性乃是安全策略能否成功的关键。有效的措施也包括与相关人员保持良好的沟通，具备积极应变、不断地自我审查和更新的能力。

三、实施安全措施

行政管理上的安全措施涉及到网络访问管理技术，包括通讯标准、端口、路径、TCP/IP数据包、及网路设置等，也涉及如何利用防火墙技术。

在不同的安全保护区域间的网络通讯都经过防火墙，也就是说防火墙对经过它的数据包按已制定的安全策略进行检查、筛选，向相关的网络提供安全保护。为了更有效的保护网络，通常共同使用防火墙与入侵探测技术。

如上所述，仅仅依靠防火墙技术提供网络安全是不全面的，实际上防火墙本身就面临许多攻击，如源地址欺骗，拒绝服务，网上侦测收集，隐蔽在正常程序包内的有害程序码，甚至防火墙本身的安全隐患所引致的攻击等等。防火墙技术和入侵检测技术的结合使用将提供更有效的网络安全。

四、安全机制测试

这一步骤是要求有关机构对已经实施的安全措施的有效性进行测试，具体的测试是对某一特定时间内安全状况的检测。安全机制检测是一项针对机构的信息安全系统长期不断的检测过程，安全机制测试与机构的风险形态相关联。对于风险高的系统使用安全机制检测的频率应

高于风险相对低的系统。当对敏感数据或处理的访问次数增加时，系统的风险相应提高，安全机制的测试次数也应相应增加。

安全机制检测的独立性非常重要，不应受到其他因素的影响，这应引起机构领导层的重视。

系统安全隐患评估是安全机制测试的重要一环。通过评估分析，发现系统安全隐患，找出相关的修复方法。安全机制测试有责任降低或消除所发现的隐患，如果测试的结果表明，某种风险超过机构的承受能力，测试结果应说明降低和防范这一风险应采用的方法。

五、持续监测并更新信息安全实施过程

为保证现有的安全机制持续发挥有效作用，有必要对新的威胁和隐患、已知的攻击、及机构安全措施的有效性进行数据整理和分析。

风险评估和安全措施实施的过程中，考虑新的因素对现有安全机制的影响，应建立一套具有动态连贯特点的信息安全机制。一成不变的信息安全机制将不能为银行的信息系统提供正确有效的保护。有许多产品提供自动监测技术，能更有效的完成对现有安全机制的检测和更新。金融信息系统技术繁杂，如果金融机构的信息安全人员能利用这类自动化监测产品，将大幅度提高信息安全实施水平。

美国联邦储蓄银行利用企业安全管理系统（ESM）达到不断监测和更新信息安全实施过程的目的。该系统的特点是为机构内各类系统所采用实施的安全措施提供管理，对实施在各类系统上的安全设置的状态作定期的监测、评估和报表。

文章出处：《金融时报》

地址： 北京市东城区建国门内大街5号 邮编：100732 电话：010-65136039 传真：010-65138307