doi 10.3969/j.issn.1671-1122.2010.10.005

金融信息系统面对的安全挑战及其对策

杨向东

（中国银行山西省分行，山西太原 030001）

摘 要 ：本文列举了金融信息系统面对的主要安全问题，分析了风险存在的因素，并提出了安全保障的对策。

关键词 ：金融 ；信息系统 ；安全

中图分类号 ：TP393.08 文献标识码 ：A

0 引言

随着社会信息化程度的提高以及银行广大客户对金融服务需求的提升，信息化已成为金融行业发展的必然，建设符合本行业特点，促进服务自主化、流程电子化、决策科学化、管理扁平化的现代化金融服务体系是金融行业提高自身综合竞争实力的最佳选择。然而，安全问题也日益成为金融行业信息化建设中的首要问题，金融行业在努力提高自身技术服务手段、向客户提供更加优质服务的同时，应始终将信息安全和防范计算机犯罪当作目前和今后工作的重中之重来抓。

1 我国银行业信息系统安全管理现状

在经济生活中，银行是最具有信息优势的部门，西方金融理论认为 ：银行就是“ 货币 + 信息 ”，英国《经济家》刊物曾预言 ：“ 21 世纪，信息将是银行的主要利润来源。” 银行是与信息行业结合最为紧密的行业之一，银行本身就是经营各种信息的特殊行业，如客户信息、帐户信息、交易信息、金融信息、产业信息、政策信息、资金信息、利率信息、汇率信息等，同时银行也是一个信息科技高需求、高投入、高配置、高输出的产业，是信息市场交换的主要参与者，在采用先进的信息技术方面一直走在各行业的前列。由于银行是社会的敏感部门，他通过生产和传递信息来提供金融服务，支配、引导社会资金运动，因而其安全性至关重要，银行经营的三性原则要求安全性始终是第一位的。银行的安全会直接影响到经济安全、社会安全和国家安全，银行在业务电子化过程中，一方面要利用先进的信息技术为客户提供优质服务，另一方面要确保数据安全，并防范金融计算机犯罪。

我国金融信息化建设经过近 30 年的发展，已取得显著的成就，为防范和化解银行技术风险，保证国家金融安全，金融系统初步建立起了由组织体系、制度体系和技术体系等组成的信息安全保障体系，随着我国金融信息化的深入，信息安全日益受到金融行业的重视。信息安全法制建设也初见成效，以《计算机信息系统安全保护条例》为基础的法律法规相继出台。随后，人民银行发布了《关于采取有效措施防范金融计算机犯罪的通知》，针对有关领导“ 银行家要抓电脑技术 ” 和“ 防范金融计算机犯罪 ” 的批示，明确把系统在投产过程中的风险防范要求放在首位，并开展全国范围的安全大检查。各行都成立了专职的安全生产机构，并从系统的需求设计、设备选型、软件开发、系统投产和推广、系统升级、系统归档等多方位介入，特别是在防火墙、防病毒软件、隔离卡、认证加密等方面进行了很大的投入。如中国银行在全行建立了统一的立体式网络化防病毒体系，在网络管理上实行业务网与办公网隔离、内部网与外部网隔离，资源分类别、分级别、分密级区别对待，信息的存储、传输实行严格的权限管理。

然而，目前金融行业同样还存在着极大的安全隐患，主要表现为信息传递的安全隐患和业务系统的安全隐患。具体来讲，前者诸如网络硬件的安全性缺陷、通讯链路的安全性缺陷、技术被动引起的安全缺陷、缺乏系统的安全标准引起的安全缺陷等 ；后者如非法用户对系统资源的非法使用或合法用户对系统资源的非法使用，特别是来自系统内部的安全威胁。

同时，银行的业务系统经过多年的发展和整合已经取得了很大的提高和飞跃，这对信息安全的建设也提出了更全面更深刻的要求，虽然旧的业务系统也可能考虑到安全机制，但那还只是停留在一个较浅的层次，还不可避免地存在很多的安全漏洞，信

作者简介 杨向东（1971-），男，高级工程师，经济师，主要研究方向 ：信息安全。

息安全建设应综合考虑信息在获取、存储、加工、传输等过程中的完整性、可靠性、机密性、可用性、可控性和可审计性，全方位考虑设计信息系统的安全方案和安全策略。

近年来，数据大集中成为我国银行业信息化工程的重点，也是银行管理的根本变革，数据集中带来了方便的经营管理，能有效控制外部风险，增强规模效益，但同时也带来了风险集中：数据中心的风险骤然加大，随着银行对计算机依赖程度的增强和数据中心规模的壮大，这种风险更加突出，一旦数据中心遭到灾难性打击停止服务，将引起大范围银行业务停顿或瘫痪，甚至引起法律纠纷和社会动荡。有人形象地将数据大集中比喻为把所有的鸡蛋都放在了一个篮子里，这是银行在“大集中”之后无法回避的安全问题。2002 年 5 月，由人民银行召开的“中国银行业首届灾难备份研讨会”上，有关领导指出：“实施数据大集中的银行，必须建立灾难备份，制定业务连续性计划并报人民银行备案。”

随着信息技术的进一步发展，会有越来越多的信息安全问题出现，入侵与反入侵的斗争也将会日益复杂，银行业对网络各级体系实施安全整合防护的需求也将会更加迫切。

2 树立正确的信息安全观念

信息安全的重要性毋庸质疑，它是继领土主权、政治主权和经济主权之后的另一主权。

首先，信息安全是一个特殊领域，从国家和民族立场来看，必须有自主的安全产品来切实保护我们的信息安全，这是根本。国家要加大对信息安全产业的投入与保护，开发具有自主知识产权的技术和产品。只有这样，才不会再出现我国 DVD 厂家被迫向外商交纳专利费的尴尬局面和类似“微软后门”之类的威胁。当今，拥有知识产权的数量和质量是衡量一个国家、地区或企业竞争力的重要指标和参与经济全球化的重要基础，我国 IT 领域自主知识产权极少，核心技术受制于人，明显处于劣势。在“市场换技术”的口号声中自我陶醉了 20 多年后忽然发现，不但市场被别人大量占领，而且我们的技术创新能力被“引进”所削弱，陷入了“引进再引进”的怪圈，产生了强烈的技术依赖性。

其次，金融行业在信息化建设中对国外的依赖程度很高，这也是现实，与我国目前在 IT 产业比较落后有关。不仅是安全产品，几乎所有的关键软硬件都从国外引进，而且在安全等级和技术先进性方面都明显受到限制，要求金融行业现在就完全自主进行安全建设也不太现实，但应作为目标统筹规划、分步实施。在信息安全建设上可区别对待，工、农、中、建四大国有商业银行规模大、实力强，信息化水平相对较高，宜采取自主建设或与供应商合作建设的策略，而实力相对较弱的股份制银行和城市商业银行可先采取外包或直接购买成熟产品的策略。

第三，对待信息安全要科学、客观、公正，既要正视安全漏洞问题，承认系统漏洞的客观存在，又要及时对漏洞加以修补，要正视信息系统的安全威胁和攻击。要充分认识到无论如何强化，构建一个天衣无缝的绝对安全的完善系统是不现实的，因为在任何时候安全都是相对的，系统的开放性与方便性和系统的安全性始终是一对矛盾。

第四，安全建设一定是多方位的和系统性的，安全建设不能局限于一种策略，单一的安全技术和产品已不能够满足行业用户保障网络安全的需求，防火墙、隔离卡、防病毒技术、信息加密技术、入侵检测技术、安全评估技术、等级管理体系、安全认证技术、漏洞扫描等相互配合，构成网络安全整体解决方案，并能在稳定性及协同性整体配合上加强。此外，安全建设也不仅仅是技术问题，而是一个涉及到技术和管理的复杂的系统工程，完善的制度、科学的管理和高素质的队伍也是确保提高信息系统安全性的重要保证。

第五，银行信息安全不只是购买几件安全产品，也不仅是防病毒、身份识别、安全认证和入侵检测等内容，更重要的是要保证业务的连续性和数据的完整性。就金融行业的特殊性来说，性能保证有时并不是最主要的，内容恢复功能尤其显得重要。

最后，在安全建设的组织保障方面，银行管理层要高度重视安全建设在金融信息化中的首要地位，要自上而下形成高层推动力，银行之间、银行与信息产业部门以及信息安全主管部门之间要通力协作。

3 科学投资，改善计算机安全环境

为确保计算机系统有一个安全的环境，硬件投入是必要的，但仔细分析我国银行业的硬件投入，似乎有些缺乏理性，在投入总量上对效率的考虑不多，几乎不考虑投入和产出的问题，在投入方向上重硬件、轻软件，认为计算机就是硬件，信息化就是购置先进的电脑设备。有人曾毫不客气地指出银行在“大把烧钱”，是“大马拉小车”。最后的结果是尽管国内银行在信息技术方面的投资不惜血本，甚至与其利润持平，但很多很容易解决的问题似乎并没有解决。

另外，长期以来，银行在信息安全基础设施方面的建设远远落后于信息系统的建设，即所谓的“重业务发展，轻安全管理”，这一方面是由于技术的发展所限，同时人们对信息安全的认识和理解也需要一个客观过程。事实上，不仅仅是信息安全，我国金融行业在整个信息化建设中都存在着各自为政、缺乏统一规划和统一标准的问题。这与我国商业银行条块分割、各自追求自身利益、缺乏协同、过分追求个性化有关，其中关键还是利益的驱动和分配。另外，IT 公司为

了满足银行的“ 需要 ”，往往也随声附和，比如信用卡建设、比如各地 CA 建设以及各行内部应用系统的建设，不仅造成银行间低水平重复建设，加大了建设成本，而且系统生命周期短、维护困难，高水平产品化应用很少，同时对银行间互通互联，以及银行与证券、保险等实现相互代理、混业经营带来了困难，“ 金卡工程 ” 未能实现预期目标就是一个很好的例子。其实个性化的前提必须是标准化，国际上许多银行和企业所强调的个性化是建立在高度发达的标准化基础上的，是在把好的成果都继承下来的基础上再去发展个性化，其主体还是标准化。

近年来，这种局面有了一定的改善，金融行业加强了信息化建设的标准化和统一化，按照“ 全局性、综合性、均衡性 ” 原则进行资源的合理配置，比如 CFCA 的建设、银联工程的启动，就充分体现了“ 统一规划、联合共建 ” 的原则，相信今后我国银行信息化，特别是信息安全基础建设必定会走上协同合作的良性轨道。

笔者认为银行业对待信息安全建设的投资应注意以下问题 ：

高度重视，积极推进。银行对计算机系统的依赖性与日俱增，数据意味着银行的生命，意味着银行的核心竞争力，安全建设是各金融机构必须做而且必须做好的工作。要作到未雨绸缪，确保安全，不能临时抱佛脚，俗话说“ 养兵千日，用兵一时 ”。

安全为先，稳妥实施。金融行业是社会的核心部门，也是一个十分敏感的部门，从银行的经营角度讲，安全性一直是首要问题，银行对安全性问题的重视程度可以说在各个行业中是最高的。因此，银行不应该贪新求洋、追赶时尚而置风险于不顾。

软硬结合，兼顾效率。信息系统的安全包括硬件安全、软件安全以及管理的安全，是一个全方位的安全体系，对信息安全建设的投入要充分结合制度、服务、人员、意识等管理理念，同时要对投入的有效性即投入产出进行科学的分析和预测。

货比三家，择优而取。在具体选择产品时要关心技术的成熟度如何，有无广泛的产品和市场 ；要了解产品的性能、可靠性如何 ；要选择经过长时间的市场考验、稳定性好、相对成熟的产品 ；另外还应注意产品的智能化、可管理化和易使用性。要充分了解合作厂商的实力、信誉，是否为业界知名公司，其售后服务、技术支持手段、服务响应情况如何。安全系统采用的技术、设备必须通过有关机构的认证。

注重扩展，保护投资。从保护投资的角度出发，安全产品的根本体系结构不能经常随着技术的发展而变化，而应该是随着技术的发展不断扩展和延伸，不宜对体系结构做频繁的调整，而应该将技术的发展作为自身体系结构的补充。

4 全面构建我国银行信息安全保障体系

构建银行信息安全保障体系是一项复杂的系统工程，决不是靠买几件安全产品就能解决的。信息安全防线的构成是多方面的，因此，安全管理的科学性和制度化就显得更加重要，俗话说“ 三分技术，七分管理 ” 就是这个道理。我国银行业应从法制、技术、管理、人员等几方面多管齐下。

首先，加强信息安全立法工作，将信息安全建设纳入法制化轨道。我国信息安全法制建设已具备基本框架，以《计算机信息系统安全保护条例》为基础的法律法规相继出台，新《刑法》中也增加了计算机犯罪及相应的惩处条款，今后要进一步完善我国信息安全法制建设。

其次，目前我国信息安全技术保障措施尚不成体系，不能有效防止手段复杂的各类信息系统攻击和威胁，因此，要加强信息安全技术和产品的研究、开发与应用，从技术角度构建信息安全保护体系。严格实施等级保护，健全安全控制机制 ；建立信息安全审核、评价、认证体系 建立信息安全产品跟踪、研发、推广应用的良性循环，特别是有自主知识产权的技术和产品 ；从机房、网络、监控、系统、设备、软件、病毒、黑客等各方面加强安全防护、访问控制、入侵检测、应急反应和系统恢复能力 ；从信息的采集、加工、存储、传输、应用等各个环节，从用户安全、站点安全、平台安全三个层面上进行建设 ；建设国家信息交换公共安全应用平台，建立高效安全的金融信息网，加强对金融信息犯罪的防范能力。

第三，以人为本，加强管理。人的因素是安全管理中最重要的因素。据有关资料显示，高达 70% 的信息安全事件是因为疏于管理由内部人员造成的。因此要制定完善的、操作性强的行业管理规定，明确责任并真正落到实处 ；坚持制度防内、技术防外，加强银行从业人员的思想道德建设，切实防范道德风险 ；加强银行从业人员的安全教育，提高信息安全人员的安全意识和对安全问题的了解程度、管理水平，以及对安全事件的处理能力，提高安全队伍的素质，建立信息安全人才的良性循环，并为进一步的安全建设提供发展的基础。（责编 杨晨）

华为赛门铁克 构建 UTM+ 统一安全解决方案

9 月 7 日，华为赛门铁克科技有限公司宣布推出全新 UTM+ 统一安全解决方案，此次推出 UTM+ 统一安全解决方案，在 UTM+ 设备内部融合了 Symantec 高质量的安全引擎和签名库，并在此基础上，进一步整合深度的应用程序识别和网站内容分类技术，从而实现应用检测与传统文件检测技术的紧密结合。（记者 杨晨）