Study on Mechanism Construction of Information Security Guarantee in Internet Bank

Yongqing MA
The School of Humanities and Social Sciences, Yunnan University of Nationalities, Kunming, China
Email: *mayonqing*2001@163.*com*

Abstract: In recent years, with the rapid development of internet bank, it has brought convenience to life. At the same time, hidden information security dangers exist in technique, network system and administration. To guarantee the interests of both bank and client, it is necessary to construct a security guarantee system with technique, auditing, administration and service, law, remediation and cooperation as the core.

Keywords: internet bank; information security; guarantee mechanism

网络银行信息安全保障机制构建研究

马永清
云南民族大学人文学院，昆明，中国，650031
Email: mayonqing2001@163.com

【摘要】 近年来，网络银行迅速发展，在带来方便的同时也存在着技术、网络系统和管理等方面的信息安全隐患。为维护客户和银行的利益，应构建以技术、检测审计、管理和服务、法律、补救处理、合作为核心的安全保障体系。

【关键词】 网络银行；信息安全；保障机制

1 引言

随着网络技术的快速发展，网络已经成为银行日常工作中不可缺少的工具。银行界掀起了一股网络银行风潮，目前全球约有 1000 多家银行提供网上服务。在中国，网络银行业也飞速发展。迄今，中国网络银行个人客户已达 4000 万，企业客户超过 10 万户，总交易金额超过 20 万亿。网络银行的业务品种也纷繁多样：如储蓄、信贷、信用卡、电子汇兑、网上交易、国际业务、移动银行等等。在网络银行为银行工作带来效率和效益，为客户提供方便快捷服务的同时，也带来了诸多弊端，信息安全就是其中一个重要的问题，并已经成为人们日益关注的焦点。对银行这样特殊性的行业，必须防患于未然，构建完整的信息安全机制来规范网络银行建设和化解网络银行安全风险。

2 网络银行信息安全风险的类型

2.1 技术风险

网络银行改变了传统银行的运作方式，以其虚拟性突破了时间和空间的限制，使交易轻松、方便、快捷地完成。但网络银行的正常运转必须依靠一些自动化程度较高的技术和设备，如计算机和互联网。但这些技术和设备又不可能绝对不会出问题，因此，相对于传统银行，技术风险成为网络银行所面临的最大、最特殊的风险。具体包括以下方面：

2.1.1 网络银行硬件系统风险

硬件系统是网络银行存在的物质载体，包括各类计算机（服务器、工作站等）、网络通信设备（路由器、交换机、集线器、加密机等）、存放数据的媒体（光盘、磁盘等）、终端设备（自动柜员机、销售终端等）、传输线路、供配电系统、抗干扰系统等。[1]如果银行硬件系统遭受人为、自然等损坏，就会影响网络银行的正常运行，甚至给客户和银行带来各种损失。

2.1.2 网络银行软件系统风险

软件系统是网络银行存在的信息载体，软件系统也会因各种原因出现问题，如软件设计缺陷、软件技术不足以支持网络银行的运作等，可能导致系统运行

978-1-935068-12-9

紊乱、出错等，造成支付、结算等业务出错而给客户造成损失或影响到网络银行服务质量。

2.2 网络系统运行风险

2.2.1 安全认证系统出现故障而造成的风险

为确保交易双方身份的真实性，网络银行采用了电子认证的方式来进行身份认证，是以认证管理机构对电子签名及其签署者的真实性进行验证。如果安全认证系统出现故障，客户或银行的利益将会受到损失。

2.2.2 互联网系统风险

网络银行交易系通过互联网直接或间接地与银行网络系统发生业务关系，由于互联网的广泛性、自由性等特点，因此很可能遭到黑客恶意攻击，或者病毒感染，严重破坏程序和数据，使网络效率大大降低，甚至导致计算机和网络系统瘫痪。

2.3 管理风险

网络银行是一个复杂的系统，包括人、物、信息、技术、法律等诸多方面，若缺乏有效的管理，也可能带来诸多风险。

2.3.1 软硬件、网络系统维护不善带来的风险

面对高新的电子网络技术，银行能若不具备相应的技术能力妥善维护，或疏于管理和维护，将带来技术故障，产生风险。

2.3.2 客户操作失误产生的风险

银行应向客户提供操作方便、简单、实用的服务终端，并且应向客户详细说明有关软硬件的操作方法。否则，如果客户操作上失误，将带来客户利益损失，或损坏网络银行软硬件系统，影响到网上银行的信誉和客户的信心。

2.3.3 来自银行员工、管理体制方面的风险

银行员工安全意识缺乏、保密观念不强、法律意识淡薄、业务不精，银行安全管理体制不健全，管理效率低下，银行法规不完善等，而造成的泄密、违章等事故，也会给网络银行安全带来风险。

2.3.4 法律法规不完善带来的风险

以高新技术为依托的网络银行，其发展十分迅速，而现行的法律法规往往显得滞后和不完善，这也给网络银行的顺畅运行带来风险。

3 网络银行信息安全构建的要求

网络银行信息安全的要求，概况起来有以下几个基本要素：保密性、完整性、可用性、可控性、可审查性。[2]

3.1 保密性

即确保信息不泄露给未授权的实体或进程，即使全部报文都被监听，必须使偷听者不能破解拦截到的信息和数据。例如，用于电子货币支付的信用卡帐号、密码等信息一经泄露，即可能被非法盗用。为了保证电子交易有效进行和各方的合法权益，交易信息必须具有保密性。

3.2 完整性

即接收主体接收到的数据必须与发送主体发送时的一致，要有抵抗不法者篡改数据的能力。再有是只有经过授权的实体或进程才能修改数据，并且能够判别出数据是否已被篡改 。

3.3 可用性

确保授权实体在需要时可访问数据，即攻击者不能占用所有的资源而阻碍授权者工作。必须保证运行于银行内部网络上的各主机、数据库、应用服务器系统不会遭受来自网络的非法访问、恶意入侵和破坏。

3.4 可控性

即对关键网络、系统和数据的访问必须得到有效的控制，可以控制授权范围内的信息流向及行为方式，这要求系统能够确认访问者的身份，谨慎授权，并对任何访问都可进行跟踪记录。

3.5 可审查性

网络安全系统应具备审计和日志功能，对相关重要操作提供可靠管理和维护功能。即能对出现的网络安全问题，提供调查的依据和手段。

4 网络银行信息安全保障机制的构建

4.1 技术保障机制

目前，网络银行主要的技术保障手段有以下方式：

加密。加密是一种最基本的技术安全机制，是在网络环境中，抵御被动攻击行之有效的安全机制。也是数字签名机制和鉴别机制等其他机制的基础，许多安全机制都是建立在加密机制的基础之上的。

数字签名。数字签名是手写签名的电子替代物，它提供了与手写签名相同或更多的功能。数字签名技术

可以证实信息发送者的身份以及信息的真实性，具有不可伪造性、真实性、不可更改性、不可重复使用性等特性。

数字证书。数字证书是由权威机构——数字证书认证中心发行的，在互联网通信中标识通信各方身份信息的一系列数据，其作用类似于日常生活中的身份证，人们依靠它可以在网上识别对方的身份。依靠数字证书技术，可以实现网上支付和结算服务信息传输的机密性、数据交换的完整性、发送信息的不可否认性安全服务。

此外还有访问控制机制，数据完整性机制，鉴别机制，通信业务填充机制，路由控制机制等[3]。

由此可见，网络银行所依托的基础之一就是高新技术和设备，因此全方位的技术保障机制，是网络银行信息安全的重要保证。主要包括：网络银行经营机构要选用安全程度高、性能及兼容性好的硬件设备、通信网络和操作系统；选择先进的安全技术，对系统合法使用进行保护；定期和不定期地检查和攻击监视，减少攻击的可能性；加强反病毒的安全措施；建立先进的银行数据异地备份系统，便于意外事故和灾难性事件发生后恢复系统正常运转；根据银行业务发展的需要，加强研发，及时更新系统安全保障技术和设备。

4.2 监测审计机制

构建系统的网络银行业务专业监管力量，配备专门的网络银行业务审计力量，定期不定期地对网上银行业务进行审计。

首先是建立银行外部监管机构，对网络银行采取有别于传统银行的监管方式。在完全开放的网络上建立一套新的金融交易规则，加强各银行之间的互相监督，防范个体银行行为，促进合理有序的网络银行运行和竞争。

其次是加强银行内部监测。应建立和加强内部稽核队伍，改进和提高内部检查手段，实时监控，事前检查，发挥稽核的风险预警作用。

再有是建立网络银行安全审计制度，确保网络银行安全顺畅运行。

4.3 管理和服务保障机制

为了避免或减少网络银行业务中可能产生的法律纠纷，商业银行开展网络银行业务，应遵守国家有关计算机信息系统安全、商用密码管理、消费者权利保护等方面的法律、法规、规章。商业银行开展网上银行业务，应根据有关法律、法规制定和实施全面、综合、系统的业务管理规章，加强对管理人员、业务操作人员的业务、法律知识培训。

在商业银行内部，应建立健全严密的内部安全管理制度，包括系统管理员的安全职责、网络操作安全规则、系统监控制度、系统外来攻击处置办法、系统失灵应急处置办法、密钥与密码管理制度、备份与恢复制度等系列安全管理制度等。以严格的规章规范网络银行的运行。

银行应加强对银行职员的职业素质教育和安全操作技能培训，杜绝因操作失误给客户和银行带来的损失。加强银行系统和帐户系统的安全性，尽力防范银行职员的内部作案。加强人才培养力度，进行有针对性的业务培训。加强职业道德教育，增强职工的金融防范意识，培养高素质的专业队伍。

树立网络银行的品牌形象，增强服务意识。为客户提供及时、高质、快捷、方便的服务，让客户在任何时间、任何地点、以任何一种方式都能享受到银行优质的服务。

再有，商业银行应以适当的方式向客户说明和公开各种网上银行业务品种的交易规则，应在客户申请某项网上银行业务时，向客户说明该品种的交易风险及其在具体交易中的权利和义务。

4.4 法律保障机制

网络银行作为金融领域的一种发展新兴事物，法律对其规范和界定还会有一些缺失，因此，健全和完善法律规范是一项重要任务。

首先要健全法制，实现网络银行业务的“有法可依”。在法制体系构架上，注重基础法制与专门法制的配套建设和协调，以弥补电子化交易基础法制的空白；在立法价值取向上，应重视对消费者，尤共是个人消费者的保护，禁止交易合同中各种对消费者的歧视或不公平的规定，并在具体风险的分担上给消费者以保护[4]。

此外，针对目前网络金融活动中出现的问题，网络银行立法还要解决网络交易的诸多法律问题，如网络交易的电子证据、及电子货币、电子银行的行为规范、跨国银行的法律问题等。再有，对计算机犯罪、计算机泄密、窃取商业和金融机密等也都要有相应的法律制裁，以逐步形成有法律许可、法律保障和法律约束

978-1-935068-12-9 © 2010 SciRes.

的网络银行运行法律环境[5]。

4.5 补救处理机制

处理机制是网络银行信息安全机制中的一个重要部分，若信息安全事件一旦发生，成为事实，就必须立即启动补救处理机制，保证网络银行维持或及时恢复正常运转，降低或避免客户、银行的利益损失。处理机制是否科学有效，在很大程度上体现了网络银行管理者的管理决策能力和危机应变能力。在此过程中，需要社会各部门以及银行各部门通力合作、协调运转、步调一致，各个部门应该预先将可能发生的信息安全事件分类，并做出对每类事件处理方式的预案。

另一个值得注意的是，处理信息安全事故的过程中，必须遵循危机管理的科学规律，只有采用科学的危机管理体系才能把事故的损害降到最低。补救处理机制建设包括三个方面的内容：一是建立与完善信息安全事故的收集系统与分析系统；二是建立起科学的事故决策系统；三是针对不同安全事故，采取恰当的补救措施。

4.6 合作保障机制

由于网络的虚拟性、全球性、无国界性等特点，加之，在一个知识、信息、技术、经济、政治乃至风险都日益全球化的时代，我们还应该高度关注单个网络银行自身的局限性。事实上，仅靠单个网络银行自身，很难抗拒和解决其信息安全问题。为此，有必要建立区域性、全国性、全球性的合作机制。不仅是银行业之间的合作，还包括银行与企业，银行与政府组织，银行与非政府组织，以及银行与个人之间的合作。这样，才能有效地保证网络银行的信息安全。

5 结语

网络银行信息安全保障机制的构建是一项系统工程，并且随着 IT 技术的日新月异和金融创新的发展，网络银行的安全威胁还会随之出现新变化。相应地，网络银行的安全需要也会随之提出新要求。进而，网络银行信息安全保障机制的内容也应作调整。但无论如何，品质过硬的技术、严密的检测、优秀的管理和服务、完善的法律、有效的补救处理、广泛的合作机制是网络银行信息安全保障机制的核心内容。

References (参考文献)

[1] Wang Zhen-bin., “Problems and suggestion of bank network security administration”, Financial Computer of Huanan, No.9, pp.70, 2008.
王振斌.银行网络信息安全管理存在的问题与建议[J].华南金融电脑，2008,(9):70.

[2] Zhou Yu-tang, “Data from commercial bank: a solution to network information security”, Computer security, No.3, pp.20, 2002.
周玉堂.商业银行数据集中：网络信息安全解决方案[J].计算机安全，2002,(3):20.

[3] Yuan Xu-feng and Yang Jian-zheng, “On security guarantee technique of network bank”, Northern Economy and Trade, No.1, pp.65, 2003.
袁旭峰,杨坚争.论网络银行的安全保障技术[J].北方经贸，2003,(1):65.

[4] Shu Hai-tang, “On risk and prevention of china’s network bank after WTO entrance”, Finance and Economy, No.6, pp.36, 2005.
舒海棠.试论入世后我国网络银行的风险及其防范[J].金融与经济,2005,(6):36.

[5] Huang Zheng-xin, “On risk and prevention of China’s network bank”, Asia-pacific Economic Review, No.5, pp.64, 2000.
黄正新.我国网络银行的风险及其防范[J].亚太经济，2000(5):64.