金融行业网络安全及其控制

李凤梅　山东省农村信用合作社联合社菏泽办事处科技中心　274000

【文章摘要】
网络的发展改变了传统的金融管理模式。我国金融网络化存在安全程度较低、安全问题较多的情况。我们必须增强金融工作者的安全的意识，加大计算机网络安全管理，确保我国金融行业健康发展。

【关键词】
金融行业；网络安全；信息；效益

网络的发展改变了传统的金融管理模式。随着我国信息产业对金融行业发展的支持力度逐渐加大，金融网络化已是大势所趋。但就当前的形式来说，我国金融网络化存在安全程度较低、安全问题较多的情况。而金融行业一旦受到信息安全的损害，必然会威胁金融行业安全、严重影响到国家经济的正常秩序。因此，加大金融行业网络安全及其控制，是保障金融行业安全发展、维护用户权益的重要保证。

一、金融行业网络安全的概念及特征

网络时代的金融网络安全是计算机系统的硬件、软件、数据受到保护，金融业务充分利用了先进的现代化技术与设备，提高金融活动的效率。使系统能连续正常地工作不因偶然或恶意的原因而遭到更改、破坏或造成机密信息泄露。计算机技术已经在所有的金融系统得到了广泛的应用。如；电子联行、同城票据清算、金卡工程、同城对公和储蓄通存通兑、信贷登记咨询等系统通过DDN网、帧中继网实现了人民银行及各商业银行之间的网络连通，极大地提高了效率，从技术上讲，网络安全分三种：即运行环境的安全性、金融机构的安全性、用户信息的安全性。新技术与金融业务结合可以明显地降低融资成本，据德国有关部门统计:同样一笔交易通过银行柜台交易成本为1.05美元，通过文传成本为32美分，电话交易成本为57美分，而通过安全的网络交易则只需10美分。可见，安全的网络在金融业务中的应用、提高金融行业竞争能力等方面具有相当重要的作用。

二、金融行业网络安全及其控制的重要性

随着计算机网络及信息通讯技术的快速发展，计算机网络技术在金融行业的系统中得到更加广泛的应用。金融业务社会化、全球化、信息化、网络化是金融行业发展的必然趋势。而金融行业网络安全则是金融行业面临的首要问题。由于金融行业网络发展的需要，要求金融网络与外部互联网相联，所以系统安全问题便显得更加重要。

金融行业的网络系统，覆盖范围大，硬件设备多，网络环境复杂。现今各金融行业为了提高自己的竞争优势，争取更大的经济效益，纷纷在丰富业务种类、完善服务功能、创新服务手段、提高服务效率等方面进行创新工作。电子联行、金卡工程、同城票据清算实现了各银行之间的网络沟通，极大地提高了效率。而要获得上述效益就必须利用高科技手段通过金融网络安全建设逐渐提升工作效率，扩大市场占有率，进而，获得更好的效益。

三、金融行业网络安全面临的威胁

1、攻击服务指令。它逐渐对金融服务网络系统进行干扰，执行无关程序，改变其正常的工作流程，使金融服务网络系统响应变慢甚至瘫痪，影响正常用户的使用；

2、破坏数据信息。以非法手段盗取对数据的使用权，插入、删除或重编某些核心信息，恶意添加、修改数据，以取得有益于盗取者的响应，造成干扰用户正常使用的情况；

3、非授权访问。没有预先经过系统同意就使用计算机资源或网络信息；

4、传播网络病毒。通过网络传播计算机病毒，其破坏性远远大于单机系统，并且用户很难防御与控制。

四、金融行业网络安全存在的问题

1、安全程度低。尽管金融信息系统网络安全状况较一般部门来说做得比较好，但从系统结构、防范方法等方面来看，还存在不少问题。互联网访问极易带来网络安全问题，如木马、垃圾邮件、恶意病毒等。又由于各个行业基本上是分开的，相互间缺乏联系，其网络是以纵向为主，所以安全措施程度不高。除了已经开展网上证券交易的证券公司使用了双网卡的隔离技术外，大部分单位没有使用内容检测、人侵检测、来源鉴别、信息屏蔽、访问控制等技术。同时员工可以通过互联网进行对外访问，而这些安全问题一旦带入金融行业的安全系统就会给系统带来很大安全风险。

2、各行信息隔绝。各银行的网络系统各自为政，各行间不能相互沟通，取长补短，就算是国有商业银行之间也是相互隐藏信息，就更不用说信息、资源、数据共享，造成了许多重复建设。就是银行网络系统拓朴结构、建设方案、实施步骤、发展构想等都作为商业秘密而被当做绝密。一家银行走过的弯路，另一家银行由于不知道，又重复走同一条弯路，造成不必要的损失与浪费。这一现象对金融行业自身、对国家都不利，既浪费了本已短缺的资金与资源，又延缓了金融行业的发展熟读，从而影响了整个国民经济的建设状况。

3、管理不当的风险。金融行业网络安全管理是安全保障体系中重要的环节，所以如果金融行业网络安全管理不善也同样会带来整个行业的安全风险。例如，分支机构员工与业务代理人需要通过互联网远程访问内部应用，那么远程访问将会带来安全风险。内部部分终端处理着重要数据，如财务处理。这些终端的数据丢失会对整个行业的业务造成巨大的损失。

五、金融行业网络安全及其控制措施

1、提高安全的可持续性。安全威胁是动态变化的，所以，我们应当部署可以持续更新、持续动态的产品或技术进行安全防护进而应对逐渐变化的安全威胁。例如，基于当前我国网络的安全与技术标准，并结合各行业的网络实际情况。首先，由于营业或机构调整扩大，可能会随时增大监控的规模，这就要求系统设计应该具有强大扩展能力；其次，必须保证网络安全监控系统24小时正常稳定地工作；再次，制订合理的访问控制权限与管理级别，保证整个网络安全监控系统的安全；最后，要求系统基于开放标准与技术，使系统可接入现有可用的网络安全设备。进而确保信息的完整性，使数据有效地、安全地传递与使用。

2、增强网络安全意识。计算机网络安

》转28页

个农村金融空白乡镇,占全省乡镇总数的9.3%,主要分布在46个县的边远贫困地区,涉及18个少数民族,130万人口，当地政府准备用两年的时间落实金融服务全覆盖的目标。当然，要覆盖类似这种空白市场首先要有基本的银行网点建设，但投放自助设备、使用电话银行和手机银行则可以迅速弥补网点建设的滞后和不足。电子银行的准入条件不高，一张借记卡一个手机几乎人人都有；使用成本也低，一般来说交易手续费免收或仅为柜台的一半，这对于低收入人群特别是需要经常寄钱回家的外出打工者来说能够节省不少的开支。因此，具有3A特性的电子银行弥补了传统物理网点的不足，使专业的金融服务惠及更多的地方和人群。

（三）电子银行渗透国计民生

许多电子银行都开通了“金融超市”，医疗、养老、住房、证券、基金、保险、外汇、黄金等多种业务一站式办理；遍布城乡的自助设备可以查询养老金明细、公积金余额，缴纳孩子上学费用，转账偿还住房贷款。连接各大银行网上银行的“超级网银”（网银互联平台），使中央银行的系统优势惠及到每一个公民。而针对国家推出的对所有农民实现全覆盖的新农保目标，农业银行依托金穗惠农卡产品，借助惠农支付通（转账电话）等电子机具为参保农民提供金融服务，实现了农户足不出户缴社保费、足不出村领养老金。针对社会关怀与自我关怀相结合的企业年金制度，工商银行的企业年金网上服务使年金信息、资产运作情况等都能简单明了地呈现在企业和职工的电脑上。因此，电子银行不是简单的银行业务支撑平台，它渗透到教育、医疗、住房、养老保险等国计民生的各个方面，使包容性增长效果更加到位。

四、 包容性增长理念下的电子银行发展建议

银行业的特性要求其发挥并承担更多的社会责任，主动把对经济、社会和环境和谐统一的追求纳入自身发展目标，包容性增长就是现阶段的目标之一。信息化时代里，电子银行辐射范围广，发展潜力大，是银行履行社会责任的一大支柱。从包容性增长目标出发，电子银行发展应该从以下几个方面入手：

（一） 加强电子银行普及和宣传

银行应该加强电子银行的营销推广，建设网银体验区，开展各种活动引导柜台向自助设备分流，多向客户宣传电子银行的低碳便捷特性，使越来越多的客户自然、习惯性地选择使用电子银行渠道获得银行服务。

（二） 加大电子银行包容性功能开发

银行应该在包容性功能上进行业务创新，主要有：重视功能的易用性，让更多的人可以马上学会使用电子银行，使电子银行渗透人群更广；针对特殊群体推出特色金融产品和功能，如农业银行为支持“三农”推出惠农卡的同时，也在网上银行和转账电话中增加了小额农户借贷款功能；多开辟支付缴费品种和渠道来吸引更多的用户，如在转账电话、自助设备和网银上设定学费、电话费、水电费功能。

（三） 增加自助机具在边远地区的投放

面对成本约束的要求，银行在县以下的乡镇大量建设物理网点难度较大，发展自助业务是适应偏远地区经济发展、满足客户金融交易需求、弥补金融缺失最有效的途径。截至2010年9月末，中国农业银行县域和农村地区投放现金类自助设备17938台，自助服务终端5183台；转账电话数量达88.4万台。

（四） 加速推广手机银行

据工信部最新数据显示，截至2010年8月底，我国手机用户总数累计已达8.23亿户，这表明手机银行可以让金融接触到中国的每一个家庭，同时，它在便利性，控制与信息方面大大超越了传统渠道甚至网上银行的效果，是最好的“金融包容性”电子银行产品之一。TR

【参考文献】
1、胡锦涛 深化交流合作?实现包容性增长 2010年9月16日在第五届亚太经合组织人力资源开发部长级会议上的致辞
2、刘亚南 印度金融行业引领“包容性增长”，经济参考报 2010-10-19
3、蔡荣鑫，“包容性增长”理念的形成及其政策内涵，经济学家，2009（1）

》接29页

全责任重大，它关系到金融行业的资金安全与信息安全。因此我们要提高安全意识，建立安全机构，落实安全责任制。同时必须成立网络安全领导小组，设立相应的计算机安全机构与岗位。另外还要建立计算机网络安全领导承担的责任，并确立相关指导、检查、监督的职责；应当积极组织网络技术培训，增强全体员工的安全意识，提安全管理人员在网络技术方面的专业水平，进一步地防范金融行业网络安全风险。

3、建立多层次管理方案。信息安全防护应从多个层次进行考虑，如终端、数据保密、网关、远程安全接入等。对于多个保护层面的安全方案应有相应的可管理性。例如，根据银行对网络监控系统的要求，将整个网络监控系统规划设计分为几大核心部分：远程信息传输系统、安全信息监控管理系统、报警信息处理系统、部门安全管理系统与综合信息管理系统。

我们可以对网络安全系统的设计与管理进行优化，加速与新用户、新网站的连接与沟通。帮助远程用户、分支机构、商业伙伴以及供应商与企业的内部网络建立可信的安全连接，并保证数据的安全传输。这在一定程度上减少了用户花费、有效地降低了系统的管理成本，还达到了多层次同步管理的效果，可谓一举多得。

综上所述，随着金融行业信息化的逐渐发展，金融行业的网络安全逐渐成为一个综合性问题。所以，在金融系统进行网络安全设计时，我们必须进行全面、系统地考虑，必须设计一个完整的安全框架。同时逐渐开发自保密、防病毒的系统，要不断检测网络入侵、审计系统的安全日志、检查是否存在安全漏洞，力争不断完善系统。加强计算机网络安全管理，制定严格的网络安全制度，采用先进的网络安全产品和技术，建立完善的网络安全体系，增强金融工作者的安全的意识，加大计算机网络安全管理，建立完善的网络安全体系，从而为社会提供更安全、更高质量的金融服务，确保我国金融行业健康发展。TR

【参考文献】
1、王子先，论金融全球化.经济科学出版社，2009年7月；
2、张 勇，金融行业与网络安全[J]，金融科技，2009年第5期
3、石亦歌，金融企业网络安垒体系新视点[J]，安防科技，2008年12月
4、史东明，经济一体化下的金融安全，中国经济出版社，2009年第5期
5、上海美宁计算机软件有限公司，网上交易安全实现策略，2009年10月