中国银行业监督管理委员会信息中心 编

银行业科技风险警示录

——银行业信息科技风险案件与事件汇编

Warning Bells on Banking Industry's IT Risks

—Case Studies on Banking Industry's IT Risks

Warning Bells on
Banking Industry's IT Risks

经济科学出版社
Economic Science Press

中国银行业监督管理委员会信息中心　编

银行业科技风险警示录

——银行业信息科技风险案件与事件汇编

Warning Bells on Banking Industry's IT Risks

—Case Studies on Banking Industry's IT Risks

Warning Bells on
Banking Industry's IT Risks

经济科学出版社
Economic Science Press

图书在版编目（CIP）数据

银行业科技风险警示录：银行业信息科技风险案件与事件汇编/中国银行业监督管理委员会信息中心编.
—北京：经济科学出版社，2011.11
ISBN 978-7-5141-1065-4

Ⅰ.①银… Ⅱ.①中… Ⅲ.①银行业-计算机犯罪-案例-汇编-中国 Ⅳ.①D924.335

中国版本图书馆 CIP 数据核字（2011）第 193676 号

责任编辑：齐伟娜
责任校对：王凡娥
版式设计：代小卫
技术编辑：李 鹏

银行业科技风险警示录
——银行业信息科技风险案件与事件汇编
中国银行业监督管理委员会信息中心 编
经济科学出版社出版、发行 新华书店经销
社址：北京市海淀区阜成路甲 28 号 邮编：100142
总编部电话：88191217 发行部电话：88191540
网址：www.esp.com.cn
电子邮件：esp@esp.com.cn
北京联兴盛业印刷股份有限公司印装
787×1092 16 开 10.5 印张 170000 字
2011 年 11 月第 1 版 2011 年 11 月第 1 次印刷
ISBN 978-7-5141-1065-4 定价：24.00 元
（图书出现印装问题，本社负责调换）
（版权所有 翻印必究）

序　言

当前，信息技术已经渗透到商业银行经营管理的各个领域，银行业已成为信息技术高度密集、高度依赖的行业，同时也是受信息科技风险影响最大的行业之一。信息系统的安全性、可靠性和有效性不仅是商业银行赖以生存和发展的重要基础，还关系到整个银行业的安全和国家金融体系的稳定。根据近几年国际上出现的信息系统故障事件分析，如果银行信息系统中断1小时，将直接影响该行的基本支付业务；中断1天，将对其声誉和市值造成极大伤害；中断2~3天以上不能恢复，将直接危及银行乃至整个金融系统的稳定。同时，随着网上银行、电子商务等网络金融服务的快速发展，利用网络信息技术的犯罪活动也日益增加，针对网上银行的案件呈上升趋势，对客户利益和银行声誉带来的危害不容忽视。

信息科技风险管理已成为银行全面风险管理体系中的重要组成部分，近年来，银监会对银行信息科技风险管理高度重视，并对银行信息科技风险管理提出了明确要求。各商业银行也普遍提高了对信息科技风险的关注程度，银行业的信息科技风险管理水平不断提高。

在取得成绩的同时，必须清醒地意识到存在的问题与不足。近年来国内外信息科技风险事件时有发生，如系统重大停机宕机、核心业务系统中断、网站安全漏洞、网上银行虚假交易、客户资金被窃取等，后果严重，教训深刻，网络与信息安全形势不容忽视。这些事件的发生再次向我们敲响警钟：信息科技工作一旦发生问题就是重大问题。信息科技风险就在身边，强化风险监管刻不容缓。

以史为镜知兴替，以案为鉴明得失。基于此，银监会组织专人对银行业金融机构计算机犯罪案件和信息安全事件进行了认真梳理，从中选择有代表性和借鉴意义的典型案例，开创性地编写了《银行业科技风险警示录》。该书在银行业计算机犯罪与信息安全事件研究方面迈出了可喜的一步，为银监会系统的信息科技风险监管工作提供了有效资料，为各银行业金融机构和广大员工提供了警示教材。这些素材新、内容全、深入浅出、富有新意的案例无论对银行风险管理部门、信息科技部门继续深入研究相关案例，还是对银行高管人员、审计人员以及从事相关业务的广大员工，都具有重要的借鉴价值和指导作用。《银行业科技风险警示录》汇编教材意义重大，值得肯定。

“前事昭昭，足为明戒”，银监会系统一定要高度重视信息科技风险管控工作，切实分析好、利用好这些案例，认真查找银行业金融机构在内控管理、安全防范、信息技术等方面存在的差距与不足，清醒把握当前防范计算机犯罪与信息安全面临的形势，采取有针对性的监管措施，指导银行业金融机构落实内控、提高信息安全管理能力，遏制计算机犯罪快速上升势头。各银行业金融机构要能够吸取这些案例的教训，警钟长鸣，积极开展多种形式的信息科技风险警示教育，做好计算机案件与信息安全事件防范工作，促进在更大范围和更高层次上提升信息科技风险防范水平。

我们坚信，通过提高信息科技风险防范意识，完善信息科技风险管理体制机制，加强风险监测和预警，加强安全技术防范与应急协作，计算机案件和信息安全事件的发生概率就会明显降低，所造成的影响和损失也将会明显减轻。

是为序。

郭利根

2011 年 1 月

此为试读，需要完整PDF请访问：www.ertongbook.com

前　言

随着信息科技在银行业金融机构客户服务、营销、内控、经营管理等工作中的应用不断深入，涉及信息技术的犯罪案件与信息安全事件不断发生，且呈现快速上升趋势。近年来出现的一些重大金融信息科技风险案例表明，信息系统为金融机构日常运营提供了重要的基础支持，银行业的稳健经营离不开对信息科技风险的有效管理。

2001 年 9 月 11 日恐怖分子劫持飞机撞击美国纽约世贸中心，这一事件瞬间彻底毁灭了数百家公司所拥有的重要数据，令近 900 家机构因此倒闭，美洲银行、德国银行、国际信托银行、帝国人寿保险公司、摩根斯坦利金融公司、美国商品期货交易所等数十家世界金融巨头遭受了重大损失。2009 年 11 月 8 日，黑客集团成功入侵苏格兰皇家银行（RBS）旗下信用卡公司的计算机网络，伪造假卡，在不足 12 小时内从全球至少 280 个城市的 2100 部提款机提取逾 900 万美元现金，使 RBS 集团短时间内损失惨重。这些事件昭示了信息科技风险管控的重要性，如果不能对信息科技风险进行有效管控，必将对银行业持续稳健运行带来重大威胁。

鉴于此，银监会信息中心组织专人对银行业金融机构计算机犯罪和信息安全事件进行认真梳理，从中选择部分有代表性和一定借鉴意义的典型案例，编写了这本《银行业科技风险警示录》。

本书收集了中国银行业金融机构 2004 年至 2011 年 6 月所发生的具有代表性的 107 个计算机犯罪案件和信息安全事件。入选案例通常在多家银行发生，并且是银行机构信息科技风险管理工作中普遍存在的薄弱环节、共性缺陷。汇编此书，意在举一反三，警示昭告，引发银行机构高管人员、风险管理部门、信息科技部门、审计部门以及各相关业务部门的高度重视，以认真吸取事故教训，采取措施，堵塞漏洞。

书中各案例内容分别包括“案例描述”、“案例分析”两个部分。“案例

描述”部分主要是以有关银行提供的事件分析报告为依据，简要介绍案例概况；“案例分析”部分深入浅出地对案件内部深层次原因进行剖析，以反映银行机构信息安全面临的严峻形势。在每章章节分析中包含“防范对策与建议”，通过各家银行的实际防范经验总结为银行建立解决方案提供借鉴。

本书着重突出了以下特点：一是素材新。入选的107个计算机犯罪案件和信息安全事件具有普遍典型意义，部分案例为国内首次披露。二是内容全。通过向全国银行业金融机构广泛征集案例，保证了内容的覆盖面和信息量，基本做到了案件与事件、历史与现状、中资银行与外资银行、不同规模银行业机构等的兼收并蓄。三是富有新意。本书对案例内容尝试性地引入了危害指数、影响指数和频度指数进行风险分级。其中，危害指数主要侧重从案件对行业的冲击力及对银行客户的影响面进行分析；影响指数主要侧重从事件对银行持续经营的影响度进行分析；而频度指数主要从发生概率（案件和事件）或作案难易度（仅针对案件）进行定性分析。案例的风险类型与发生根源分析则借鉴了巴塞尔新资本协议的要求和分类方式。四是深入浅出。注重技术深度和通俗易懂的结合，每个案例做到了情况描述全面细致、原因分析切中要害、对策建议切实可行，具有较好的完整性、前瞻性和实用性。同时，力避生硬技术性论述，数据主要以图、表形式进行罗列和分析，使读者一目了然。

中国银行业监督管理委员会信息中心

2011年7月

目　录

此为试读，需要完整PDF请访问：www.ertongbook.com

第一章　信息科技相关案件

一、案防形势

当今社会经济发展对信息科技的依赖程度愈来愈高，金融业信息系统和网络安全对国家安全、社会稳定和公众权益的影响逐渐增强。在全球范围内，网络窃密、网络攻击等利用计算机技术进行网络违法犯罪活动呈上升趋势。近年来，我国银行业信息科技相关案件频发，银行网络、信息系统已成为境内外敌对势力和不法分子攻击破坏的重要目标之一。攻击手段层出不穷，作案手法不断翻新，信息安全形势日益严峻。

二、案件类型及作案手段

按照案发区域，银行业信息科技相关案件可分为以下三类：

一是网上银行类案件。犯罪嫌疑人主要通过国际互联网等载体，以木马病毒、程序破解密码等多种技术手段获取银行客户账号和密码，再以非法转账或网上支付等方式，盗取客户资金。

二是内控缺陷类案件。犯罪嫌疑人借内部工作人员的身份和工作之便，利用银行管理制度、业务流程、交易系统等方面存在的漏洞作案，盗取客户或银行资金。

三是自助设备类案件。犯罪嫌疑人在银行自助设备上做手脚，利用读卡器、微型摄像机、假冒银行服务电话等各种手段盗取客户银行卡信息及密码，进而盗取客户资金。

上述三种类型案件在案发区域、损失度及防范难度等方面存在不同，作案手段也有所差异。见表1－1、表1－2。

表 1-1　　三种类型案件发案差异

序号	类型名称	案发区域	危害指数	频度指数
1	网上银行类案件	国际互联网	中	较高
2	内控缺陷类案件	银行内部	高	较低
3	自助设备类案件	ATM、CDM、POS	中	高

表 1-2　　三种类型案件的作案手段

序号	作案手段	网上银行类案件	内控缺陷类案件	自助设备类案件
1	通过国际互联网入侵银行系统，更改数据	√		
2	通过国际互联网窃听或截获客户银行卡账号及密码	√		
3	通过国际互联网、假冒银行服务电话、或银行自助设备窃取客户银行卡账号、密码	√		√
4	通过国际互联网破解客户网银密码	√		
5	通过国际互联网窃取客户网银证书	√		
6	内部人员非法使用业务系统		√	
7	内部人员非法访问系统或数据库，篡改系统数据		√	
8	内部人使用或拷贝恶意软件		√	

三、案件特点分析

据不完全统计，2004 年至 2011 年 6 月初，银行业信息科技案件中，最受关注的是利用网上银行作案；利用银行内部控制漏洞作案发案数相对较少，但涉案金额较高；发案率最高的是利用自助设备作案。如图 1-1 所示。

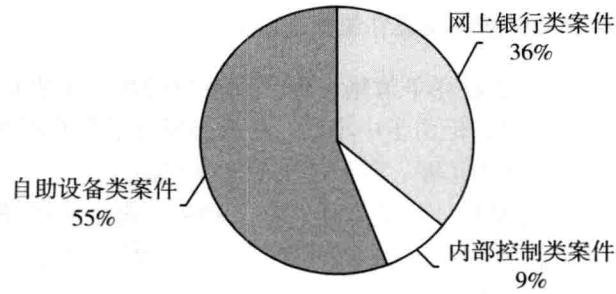

图 1－1　2004 年至 2011 年 6 月银行业信息科技相关案件统计

上述三类案件近年来呈以下变化趋势。

（一）利用网上银行作案发案率逐年递增

1. 利用网上银行作案具有任意时间、任意地点之特点，犯罪分子实施犯罪不容易受到事件时点的限制。

2. 由于技术的开放性，犯罪分子容易掌握一些技术含量较高的作案手法，且攻击手段不断翻新，犯罪行为更不易被察觉。

3. 银行为适应市场竞争的需要，网银产品开发周期缩短，相应内控手段难以适应业务快速发展的需要，风险敞口逐步累积。

（二）利用银行内部控制漏洞作案发案率逐年递减，但涉案金额较高

1. 银行内控体系逐步完善。随着对信息科技风险认识的不断提高，银行业金融机构逐步将信息科技风险纳入银行整体风险防范体系，促使银行内控机制日渐增强，风险管控能力和水平不断提升。例如，银行通过实施关键业务岗位隔离、信息科技生产和测试环境隔离、指纹识别仪取代柜员卡等制度和措施，堵塞了部分漏洞。

2. 外部环境对银行内部控制的合规要求日益严格。例如，近年来银监会相继出台了《商业银行信息科技风险管理指引》、《银行业重要信息系统突发事件应急管理规范》、《电子银行业务管理办法》等规范性文件，对银行内部控制合规提出了更为明确的要求。

3. 由于内部人员作案，熟悉银行控制体系，导致此类案件具有作案时间长、败露周期长、单笔涉案资金高的特点，危害性较高。

（三）利用自助设备作案案件呈高发趋势

1. 近几年，基于企业竞争策略，中小银行纷纷加大了借记卡、信用卡等客户市场的开拓力度，但由于中小银行科技研发力量参差不齐、对信息安全的风险防范意识和能力不足，导致相关犯罪案件高发。

2. 该类案件有向农村、乡镇蔓延转移之趋势。由于区域经济发展不平衡，犯罪分子利用农村乡镇区域银行客户风险意识薄弱的特点，专门选择银行县级支行或者农村中小金融机构自助设备作案。

3. 该类案件作案的技术门槛相对较低，目前我国仍大量使用安全级别较低的磁条卡，涉及相关案件较多。

四、危害及根源分析

（一）危害分析

各类信息科技犯罪案件会使银行面临多方面的风险，主要集中在以下三个方面。

1. 欺诈风险，例如敏感信息被盗取，包括银行卡号及密码、网银账号及密码等，导致银行、客户资金被盗。

2. 银行资产设施及信息系统受损，影响其正常提供对外服务。

3. 信誉风险和法律风险。具体分析见表 1－3。

表 1－3　　三种类型案件危害分析

序号	危害类型	网上银行类案件	内控缺陷类案件	自助设备类案件
1	银行资产设施遭到破坏			√
2	银行资金遭受损失	√	√	√
3	客户资金遭受损失	√	√	√
4	银行遭受法律诉讼	√	√	√
5	银行信誉受损	√	√	√

此为试读，需要完整PDF请访问：www.ertongbook.com