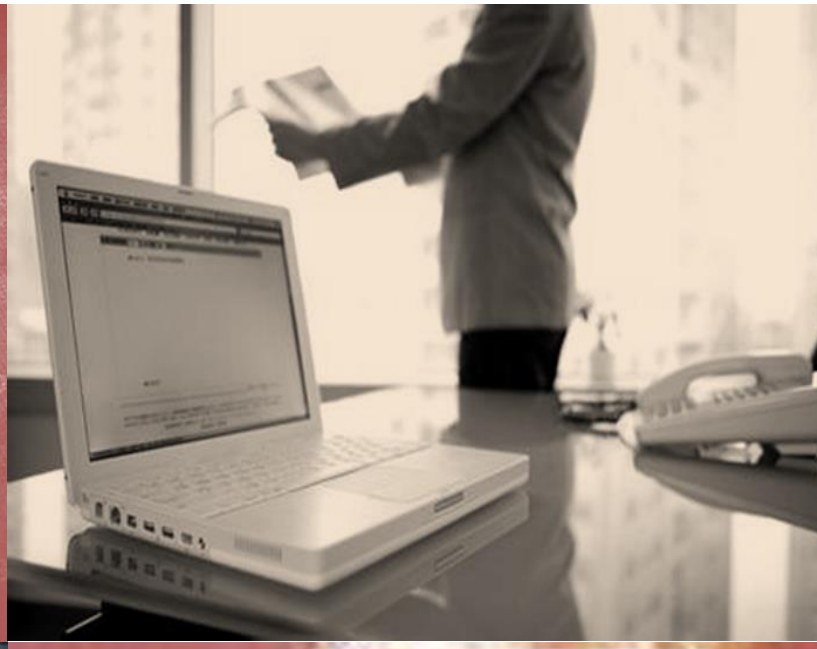
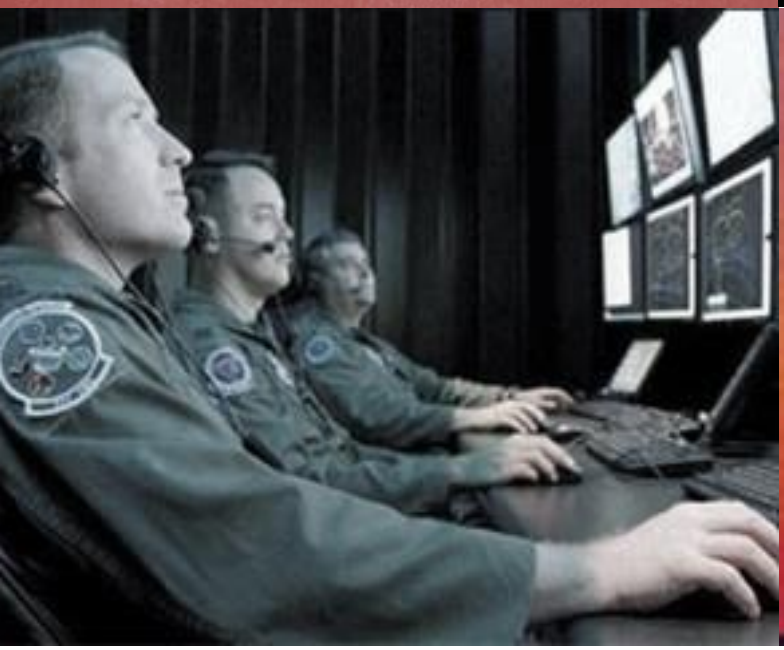




2013 年度重大信息安全事件回顾报告

2014 年 3 月

上海安言信息技术有限公司

目　　录

前　　言

2013 年，随着云计算、大数据、移动互联网等新技术的不断推广应用，以及国民经济和社会各领域信息化程度的不断提升，尤其是移动互联网的迅猛发展，网络日益呈现开放性、共享性特征，且互连程度不断扩大，但随之而来的网络安全问题也渗透到各个领域，攻与防的较量日趋白热化，网络已经成为一个新兴的战场。在国家安全层面，网络空间成为继陆、海、空、天之后的第五维作战空间，信息安全已经成为国家间战略博弈的焦点，“棱镜”事件充分表明国家间网络安全竞争与对抗日趋激烈，对网络空间主导权的争夺逐渐白热化。在城市运行安全层面，随着智慧城市建设的持续推进，涉及国计民生的重点行业以及城市的功能运转越来越依赖于基础网络和重要信息系统的安全可靠运行，信息安全风险也将对城市公共安全构成严重挑战。企业法人安全层面，一方面，国内外 IT 巨头企业日益掌握信息技术、产品、和服务的主导权，越来越多网络和信息系统的安全可靠运行受制于少数 IT 技术产品供应商提供的产品和服务，一旦此类企业本身发生安全事件，可能产生十分严重的影响；另一方面，企业核心数据、商业秘密和经济情报等信息资产日益成为网络黑客活动的目标，产生的安全事件可能严重扰乱社会经济秩序。在公民个人安全层面，市民的衣食住行与信息技术应用息息相关，网络欺诈、个人信息泄露、恶意应用传播等安

全隐患严重威胁到公民权益，如达到一定规模，将可能影响社会稳定。

为了深刻揭示信息安全事件所带来的影响，更好应对信息安全风险，安言咨询汇编了相关媒体上发布的公开信息，以提名和投票的方式将过去一年中发生的重大信息安全事件做一个回顾，从中选出 23 件大事，编辑成《2013 年度重大信息安全事件回顾报告》。本报告将从国家信息安全、城市运行公共信息安全、企业法人信息安全和公民个人信息安全四方面，汇总介绍 2013 年度具有典型意义的重大信息安全事件，并对事件进行了初步分级。

以下是事件影响范围、影响程度和影响时间的评分标准：

评分	影响范围	影响程度	影响时间
★☆☆☆☆	该事件影响范围很小，仅涉及个别公民	该事件对公民个人信息安全勾成威胁，造成公民个人财产损失、信息泄漏	该事件影响时间很短，时间跨度约为几小时
★★☆☆☆	该事件影响范围较小，涉及事件相关公民群体或企业法人	该事件对企业信息资产构成威胁，关乎企业的生存与发展	该事件影响时间较短，时间跨度约为几天
★★★☆☆	该事件影响范围中等，涉及部分省市或受影响人数达百万人次	该事件对城市信息系统可用性构成威胁，关乎市民日常生活	该事件影响时间中等，时间跨度约为几周
★★★★☆	该事件的影响范围较大，涉及国家范围或受影响人数达千万人次	该事件对城市公共基础设施构成威胁，与城市的日常运行紧密相关	该事件影响时间较长，时间跨度约为几月
★★★★★	该事件影响范围很大，涉及全球范围	该事件对国家信息安全构成威胁，对国计民生影响较大	该事件影响时间很长，时间跨度约为几年

国家信息安全

典型危及国家安全的信息安全事件

[本部分共选录了 5 个危及国家安全的典型信息安全事件，包括美国“棱镜门”、“.CN”域名大面积瘫痪、荷兰国家数字身份证明系统遭攻击、RSA 加密算法后门、金山 WPS 软件漏洞等。]

国家信息安全是指信息安全事件一旦发生，会对国家政治、军事、经济、文化、科技等造成严重威胁或危害。

这些事件主要反映了以下发展趋势：

一、网络空间将成为国家间竞争和博弈的焦点。网络安全问题曾被美国总统奥巴马形容为“美国所面临的最严重的经济和国家安全挑战之一”，美国已将信息安全作为国家战略的重要组成部分，在全球第一个建立网络战部队。美国“棱镜”计划的曝光更让人们认识到国际间网络信息对抗的真实性和严重性。我国虽然已经成为一个网络大国，但在 IT 技术自主创新方面还相对落后，关键基础设施防护上还相对薄弱，面对网络信息安全的新挑战，我们必须坚定决心，把信息安全问题作为事关国家安全和国家发展、事关广大人民群众工作生活的重大战略问题，从国际国内大势出发，总体布局，统筹各方，创新发展，努力把我国建设成为网络强国。

二、关键基础设施网络安全保护日益重要。随着信息技术的快速发展，国防、能源、金融、卫生、水务、电信等关键基础设施对计算机网络的依赖程度日渐提高，同时来自网络的安全威胁也日趋严重，以域名系统为例，在 2013 年全球范围内就发生了多起针对域名系统的攻击事件。而许多战略资源（如大多数根域名服务器、重要社交网络服务站点等）处于我国掌控范围之外，目前对于国家关键基础设施的保护也尚未制度化、标准化。据 CNNIC 的调查数据显示，我国 57%的域名解析服务处于有风险的状态，其中 11.8%的域名处于较高风险状态。

三、必须努力掌握信息技术主导权。“棱镜”计划的曝光使信息监视的问题公开化，在这样的情况之下，如何保证信息安全已经成为重大的国家安全问题。一个国家若想构筑起完备的网络安全屏障，必须发展自主独立的信息产业。为此，我国必须要制定全面的信息技术、网络技术研究发展战略，下大气力解决科研成果转化问题，在网络安全和信息化上真正做到技术先进、自主可控、安全可靠。

影响范围：★★★★★
影响程度：★★★★★
持续时间：★★★★★

关键字：
棱镜、电子邮箱、密码、黑客

美国“棱镜”灼伤全球公众隐私

事件回顾

6 月 5 日，英国《卫报》发表文章称，美国国家安全局有一项代号为“棱镜”的秘密项目，要求电信巨头威瑞森公司必须每天上交数百万用户的通话记录。一天之后，美国《华盛顿邮报》披露，在过去 6 年间，美国国家安全局和联邦调查局通过进入微软、谷歌、苹果、雅虎等九大网络巨头的服务器，监控美国公民的电子邮件、聊天记录、视频及照片等秘密资料。6 月 7 日，正在加州圣何塞视察的美国总统奥巴马做出回应，公开承认该项目。由此，这项由美国国家安全局自 2007 年起开始实施的绝密电子监听计划浮出水面。

“棱镜门”曝光以来，美国庞大的监控计划冰山一角暴露在各国面前，其几乎无孔不入地监控个人隐私，肆无忌惮地入侵他国网络等丑陋行为，受到全球广泛关注和谴责。

分析启示

事件对世界各国敲响了警钟，甚至连美国的盟友也不例外，除通过外交途径向美方表达不满外，也应重新审视国家安全保障策略。对国内而言，就像华为中兴事件一样，这又是一堂生动的信息安全教育课。而国内有关信息安全策略的深化，无疑是与之有着必然的联系。

这一事件所暴露的美国监听丑闻警醒人们，网络世界不太平，美国加紧扩张网络霸权，在网络世界一家独大，这样的格局短时间还难以改变，维护网络和平将是一项长期艰巨的工作。

“棱镜”项目的曝光为我国国家整体信息安全敲响了警钟，印证了此前我们对国家信息安全保障重大风险的忧虑。一方面，网络对抗日趋成为国家行为，网络空

间主导权的争夺将成为国际战略博弈的焦点问题；另一方面，在不掌握信息产品核心技术的情况下，忽视信息安全问题将使国家核心利益和安全面临严重威胁。针对本次事件，应注意以下三点。

✓ **国家行为已经成为重要的安全风险。**随着信息化的深入发展，网络空间日益受到各国政府的高度重视，为争夺网络空间主导权，以美国为首的各国政府努力发展网络监听、控制和作战能力，网络对抗日趋激烈，对我国数据资源安全、网络疆域主权形成了严重挑战。

✓ **国外信息产品安全问题突出。**美国之所以具备如此强大的监控能力，主要原因之一是全世界多数国家在使用美国的技术、产品和网络服务。目前，国内政府和企业对国外品牌的电子产品、信息技术产品过分依赖。据媒体报道，涉及“棱镜门”的思科产品在国内两大主干通讯网络中占据了 70%以上份额，应用于所有超级核心节点。从技术角度来讲，任何电子信息类产品都有被植入后门、窃取用户情报的可能。如果忽视这些产品本身的安全风险，将可能带来严重的信息安全问题。

✓ **BYOD（Bring Your Own Device，员工使用私人设备办公）安全风险不容小视。**BYOD 是指企业允许员工将自有的个人电脑、手机、平板电脑等终端设备接入企业内网进行办公。目前在国内，很多机构鼓励这种行为，多数是出于方便办公、节约办公成本的目的，然而这样的做法却使得办公数据与私人设备的物理边界消失，使得员工和外来人员可以接入内部网络，给数据安全带来威胁。美国情报机构拥有非常完备的信息保全制度，但仍无法拦住斯诺登将机密文件拷贝至自己的设备，这与 BYOD 不无关系。BYOD 虽然逐步成为信息化发展的趋势，但是在实施过程中仍需要建立完备的信息安全管理制度，落实相对应的技术防范措施，才能有效保护核心信息数据安全。

✓ **授权机制存严重安全风险。**《华盛顿邮报》曾做调查发现，美国有 84.5 万名政府和非政府人员有权查看绝密类信息。“斯诺登”事件之后，又有统计，美国获准参加与最高机密的安全许可约有 120 万人。在物联网环境下，如何确保应用方便性的同时，确保信息安全，对授权管理而言，无疑是严峻的挑战。

信息来源
中新网：
http://news.xinhuanet.com/tech/2013-06/15/c_124858525.htm

“.CN”域名遭据绝服务攻击大面积瘫痪

事件回顾

8 月 25 日凌晨，中国国家顶级域名“.cn”受到了史上最大规模的网络攻击，大量“.cn”域名和“.com.cn”域名网站解析受到影响，出现访问缓慢甚至中断。据工信部数据显示，攻击时峰值流量较平常激增近 1000 倍，而事件的始作俑者本意只是为了攻击一个游戏私服网。

此次攻击系某黑客团伙因商业利益驱动，采用僵尸网络向国家域名系统持续发起大量针对某游戏私服网站域名的查询请求，并针对国家域名系统的 6 个地址直接进行 DDoS 攻击（分布式拒绝服务攻击，Distributed Denial of Service Attack）。

分析启示

✓ **网络安全已经成为国家安全的重要组成部分。**一方面，国家应更加重视互联网基础设施的保护工作。顶级域名，省际、国际出入口，主干网等基础设施对于整个互联网运行都具有举足轻重的作用，一旦这些系统出现安全问题，将会成为影响部分地区乃至全国的重大安全事件。另一方面，国家应加强对网络犯罪行为的威慑力，自国内的互联网事业兴起以来，国内就有一些组织或个人，使用黑客手段进行犯罪活动，甚至形成了“网络黑帮”，逐步演变为黑色产业链。在此问题上，政府部门责无旁贷，必须加强网络空间治理和犯罪行为的打击。对此，工业和信息化部已率先行动起来，于 2013 年 7 月 30 日正式发布并实施了《防范治理黑客地下产业链专项行动方案》，与相关部委联合开展了一系列整治行动。

✓ **应高度重视信息时代数据战略资源保护。**目前 IP 地址、根域名服务器、搜索引擎、大型社交网络等已经成为信息时代的重要战略资源。美国凭借其信息技术的优势和在互联网运行体系中所处的“先入为主”的地位，掌控了大多数重要战略资源，美国仅凭所掌握的根域名服务器就能够对我国网络的正常运行造成影响。因此，我国应该充分利用技术体系更替的契机，通过技术、市场、外交、法律法规等综合策略逐步扭转这一局面，增强话语权，掌握主动

信息来源
比特网：
http://sec.chinabyte.com/418/12698918.shtml

影响范围：★★★★☆
影响程度：★★★★★
持续时间：★★☆☆☆

关键字：
数字身份证明

荷兰国家数字身份证明系统遭攻击 千万人网上支付中断

事件回顾

4 月 24 日，荷兰国家数字身份证明系统受到网络攻击，超过 1000 万荷兰人无法使用官方数字身份证明支付账单或纳税。数字身份证明系统用于在线确认荷兰公民身份，包括一个用户名和一组密码。荷兰民众使用数字身份证明系统纳税、支付账单、改变住址或索取官方文件。

内政部发言人弗兰克在一份声明中说，由于受到 DDoS 攻击，国家数字身份证明系统自 23 日晚无法使用。

分析启示

✓ **信息安全基础设施的保障能力亟待提升。**为保障基础网络和重要信息系统的安全，国家、地方、行业逐步建立了一批信息安全基础设施，如网络信任基础设施（数字身份证明系统）、密钥管理中心、灾难备份系统、应急响应系统、云安全服务系统等。数字身份证明系统是其中最为重要的信息安全基础设施，在电子政务、电子商务应用中正发挥着越来越大的作用，已经成为当前网络空间不可或缺的组成部分。可以预料的是，针对此类信息安全基础设施的安全威胁将不断增加，信息安全基础设施本身的安全保障显得尤为重要。荷兰国家数字身份证明系统遭攻击的安全事件，提醒我们应从技术手段、组织管理技术、法律等角度不断完善对信息安全基础设施的保障，确保其安全稳定运行。

信息来源
新华网：
http://news.xinhuanet.com/mrdx/2013-04/26/c_132341515.htm

影响范围：★★★★★
影响程度：★★★★★
持续时间：★★★★★

关键字：
加密算法、后门

RSA 被指受美政府控制 在加密算法中安后门

事件回顾

据国外媒体报道显示，美国国家安全局曾与业内影响力巨大的电脑安全公司 RSA 达成了一个价格高达 1000 万美元的秘密协议，美国国家安全局要求后者在被广泛使用的电脑加密算法中安置后门。

根据斯诺登泄露出的机密文档显示，美国国家安全局要求将自己提供的方程式作为 BSafe 安全软件设计的优先或默认随机数生成算法。此举将让美国国家安全局通过随机数生成算法 Bsafe 的后门程序轻易破解各种加密数据。简而言之就是，美国国家安全局首先利用美国国家标准研究所（NIST）认证了这种有明显漏洞的算法为安全加密标准，然后再让 RSA 基于这种算法推出安全软件 Bsafe。而企业级用户采购安全软件，则看到的是一个世界级企业采用 NIST 认证的加密标准开发的软件。

消息一经披露，许多计算机安全领域专家都感到十分震惊。因为 RSA 在保密用户隐私和安全方面一直表现出众，并且是上世纪 90 年代反对当时的美国国家安全局要求在电脑和通讯产品中安置一块特殊芯片以进行监控的主要公司之一。

分析启示

作为海外信息加密和安全认证领域的龙头企业，RSA 的客户遍布世界，拥有全球 70%的市场份额。超过 7,000 家企业，逾8000万用户均使用RSA认证产品保护企业资料，而超过 500 家公司在逾 1,000 种应用软件安装有 RSA Bsafe 软件，全球使用 RSA 产品的数量逾 1 亿份，RSA 的加密算法如果被安置后门，将影响到非常多的领域。可见即使是在业界拥有良好信誉的知名企业，在国家利益面前都有可能放弃所坚持的原则，重要信息系统的安全保障不能完全依赖于某些企业对商业道德的坚守。

✓ **信息安全产业发展必须坚持自主可控。**信息安全攸关国家安全，实现国家重点领域和关键环节信息安全自主可控是解决我国所面临信息安全威胁的核心所在。为此，必须要在关键应用领域中采用国产自主可控设备，从硬件逻辑、软件源代码及系统运维层面实现自主可控，消除国外设备存在的安全隐患，从根本上解决信息安全威胁。RSA 部分技术涉及“后门提供”的报道，显然将大大加强包括我国在内的各个国家推动信息安全行业的“国产化”，信息安全产业也将迎来重要的发展契机。即使在当前我国自主技术尚不能完全替代进口技术的情况下，也应该采取多方采购、重叠控制等策略，防止单个国家或企业的产品“一统天下”。

信息来源
新浪网：
http://tech.sina.com.cn/i/2013-12-21/13499028417.shtml

黑客利用金山 WPS 软件漏洞攻击政府部门

事件回顾

2013 年 12 月 3 日，国内安全公司瀚海源微博爆料，发现一个利用金山 WPS 软件 2012/2013 版本 0day 漏洞，针对中国政府部门的钓鱼邮件定向攻击事件，已确认在最新的 WPS 2012/2013 上都可以利用。

据瀚海源公司描述，攻击者会以《2014 中国经济形势解析高层报告》为标题向政府工作人员发送邮件，邮件附件为包含 0day 攻击代码的 WPS 格式文件。一旦使用 WPS 打开该文件，木马程序会自动释放运行，在电脑中安插后门，攻击者便可随时窃取电脑和网络中的机密数据。

目前，多家安全厂商已经紧急更新了防护规则，最新版杀毒软件均可防御包含此漏洞在内的多个 WPS 0day 漏洞攻击。

（4）分析启示

✓ **技术先进，安全可靠是对国产化技术、产品和服务的内在要求。**“棱镜门”事件后，国家信息安全被提到了战略高度，十八届三中全会对于国家安全提出了新的更高的要求，国家网络与信息安全被放到了更加突出的位置。软件、硬件国产化趋势对国内厂商来说是个多年难遇的机会，以 WPS 为代表的办公软件为例，在已完成正版办公软件采购的省级政府单位中，WPS 的市场份额达到 60%。但核心产品国产化也给国产化提出了更高的要求，毕竟国产化并不意味着更先进、更安全、更可靠，即使美国这样大量采用国产信息技术的国家，对自身安全防护能力的判断也不乐观。因此，国家相关部门在鼓励国产化的同时，应尽快在重点领域和关键环节建立起更加完备的信息安全审查、准入机制，建立相应的技术检测和服务专业队伍，掌握国家网络与信息安全的主动权。

✓ **多管齐下打造电子政务安全保障体系。**近年来，随着电子政务建设的不断深入，政府部门所构建的地理库、人口库、法人库以及应用系统在社会管理、公共服务的各个领域正发挥着越来越大的作用。与此同时，由于大部分信息极有价值，针对电子政务的安全威胁也不断增加，据 CNCERT 分析统计，2013 年上半年我国境内被篡改政府部门网站就达 1736 个，被植入后门的政府部门网站为 1342 个。而我国电子政务领域重建设、轻管理，依赖国外技术产品等信息安全问题仍然十分突出。这些事件提醒我们，应不断完善电子政务信息安全保障的组织机制、防护措施、产业策略和法律体系，尽快建设完善的国家信息安全基础设施，形成相应的信息安全保障能力。

信息来源
中新网：
http://finance.chinanews.com/it/2013/12-10/5603508.shtml

城市运行公共信息安全

典型危及城市运行的信息安全事件

[本部分共选录了 6 个对城市运行、经济建设和公众利益方面造成重大影响的信息安全事件，包括以色列公路控制系统被黑、GSM 存高危漏洞、“伪基站”致大量用户手机脱网、宁波医院收费系统故障、长三角铁路售检票系统大面积瘫痪、美国医保平台崩溃等。]

城市运行公共信息安全是指信息安全事件一旦发生，会对城市公共基础实施如：医疗、轨交、无线通信等领域造成严重威胁或危害。

随着智慧城市建设的推进，城市日常安全运行将更加直接地面临信息安全威胁，智慧城市安全风险加剧。有统计，到2020 年，大部分联网设备将是物联网设备。“智慧城市”、“智慧医疗”、“智慧交通”、等智能化物联系统的发展，客观上讲使物联网安全威胁集中浮出水面。

城市运行安全呈以下发展趋势：

一、智慧应用的信息安全问题不容忽视。智慧城市将信息技术与先进的城市经营服务理念进行有效融合，将水、电、油、气、交通等公共服务资源实现全面地物联，通过对城市的地理、资源、环境、经济等进行数字网络化管理，为城市提供更便捷、高效、灵活的公共管理创新服务模式。不过，智慧城市建设以物联网、云计算等大数据技术体系为支撑，数据信息体量庞大，并深入渗透到政务、商业、生活等方方面面，一旦出现信息安全问题，后果将不堪设想。

二、城市信息安全保障体系必须进一步完善。智慧城市的建设发展，对现有的城市信息安全保障体系同样构成了冲击，这主要体现在：信息基础设施仍然十分脆弱，物联网、大数据、云计算等应用在基础设施中的新技术是否安全需要更长的时间来进行验证；信息安全威胁向城市实体设施延伸，交通工具、管线、建筑等设施连接网络和信息系统，同样会引入信息安全风险；城市信息安全责任划分和协同机制将更加复杂，智慧城市可看做是一个复杂巨系统，政府部门作为信息安全管理者需要梳理政府部门、私人机构和市民之间的利益关系，明确各个政府部门之间的职责和协同关系。对此，城市信息安全保障体系需要在现有基础上进一步明确保障目标，完善职责划分和任务分工，执行相应的应急预案，有效应对智慧城市发展所带来的安全需求变化和技术不确定性。

三、工业控制系统信息安全管理亟待加强。各类工业控制系统作为信息化与城市实体设施间的纽带，安全可靠性问题十分突出。工业控制系统的复杂化、信息化和通用化加剧了系统的安全隐患，潜在的更大威胁是我国工业自动化等相关产业综合竞争力不强，嵌入式软件、总线协议、工业控制软件等核心技术受制于国外，缺乏自主的通信安全、信息安全、安全可靠性测试等标准。对此我们需要积极面对当前形势，分领域、分行业加强信息安全研究和投入，形成相应的解决方案和行业标准，不断提升重点领域工业控制系统信息安全保障能力，切实保护城市运行安全。

影响范围：★★★☆☆
影响程度：★★★★☆
持续时间：★★☆☆☆

关键字：

公路系统、交通拥堵

以色列公路控制系统被黑 导致大规模交通拥堵

事件回顾

据美联社的报道，以色列北部城市 Haifa 的公路控制系统遭到了网络攻击，这次攻击已经造成城市主干路上的交通拥堵和一系列严重的后续问题。攻击者使用恶意软件攻破了卡梅尔隧道收费公路的摄像系统，并以此为跳板获得了此条公路的系统控制权，攻击者在次日清晨关闭了整条公路的系统长达 8 小时，造成了大规模的拥堵。

分析启示

✓ **工控系统成黑客主要目标。**高级可持续大规模攻击已经把目标从传统的 IT 系统转向工业控制网络。除“震网病毒”事件外，在近两年全球能源、化工、交通网络频频受到 APT 攻击的大量案例中，这种趋势越来越明显。我国一些国外进口的工控设备中存在严重的安全漏洞，一旦这些漏洞被不法分子利用，能够导致工厂爆炸、火车碰撞、大面积停电等重大安全事故。

✓ **网络安全深刻影响城市运行安全。**公路系统等攸关城市运行安全的重要信息系统原本是相对封闭的应用系统，没有引起太多的信息安全问题。但随着互联网的迅猛发展，很多原本专网专控的重要信息系统已逐步依托互联网建设，采用了更加先进的大数据、云计算技术以降低运营管理成本。但是，这样的架构方式同样会带来病毒、黑客等互联网安全威胁，一旦这类系统遭到入侵甚至遭到破坏，将对城市运行带来严重的安全后果。

信息来源
比特网：
http://sec.chinabyte.com/306/12763306.shtml

GSM 存高危漏洞 无线通信安全受威胁

事件回顾

11 月 1 日，360 安全中心发布红色警报称，由于国内运营商没有对部分地区 GSM 制式的数据通信加密，黑客可以监听自己所在基站覆盖范围内所有 GSM 制式手机的通信内容。一旦手机短信内容被黑客获取，手机号码所绑定的网上支付、电子邮箱、聊天账号等信息将全部面临被盗风险。

GSM 是全球应用最广泛的移动电话标准，在中国更是占据主流地位，中国移动、中国联通的 2G 网络手机都是基于 GSM 数字移动通信标准，GSM 通信漏洞的影响范围和危害程度将空前严重。

分析启示

✓ **城市关键基础设施信息安全保护亟待加强。**目前，轨道交通、城市供电供水供气、移动通信等城市基础设施的信息化程度不断提高，然而这些基础设施运营者往往容易忽视其背后的安全风险，而一旦由于信息安全问题引发城市基础设施的安全事件，将会对城市整体运行安全构成严重威胁。对于此类事件，政府部门应该加强城市基础设施运营者的信息安全责任管理，通过建立安全检查和责任追究制度，制定行业信息安全标准准则，有效提升城市整体信息安全保障水平。

✓ **个人通信存安全风险。**随着微博、威信、社交网络、即时通信工具的广泛应用，以及 3G/4G 移动互联网、苹果/安卓智能终端的快速发展和规模化普及，隐私的泄露、数据的滥用、人员的定位、通信的窃听、信息的窃密等个人通信安全问题越来越严重。由于手机联络人之间的强信任关系，更容易受到社会工程方式的攻击，手机遂成为 APT 攻击的新的突破口。

信息来源
中新网：
http://finance.chinanews.com/it/2013/11-01/5455247.shtml

影响范围：★★★★☆
影响程度：★★★★☆
持续时间：★★★★☆

关键字：
伪基站、手机脱网

“伪基站”发百万条短信致大量用户手机脱网

事件回顾

9 月 11 日，上海市无线电管理局工作人员和静安公安分局民警将正在特卖会附近连续发送促销短信的王贵林当场查获，并对非法无线电发射设施予以暂扣。同伙范强得知群发短信设备被暂扣之后，只是“休息”了一段时间避避风头。一个月之后，范强再次铤而走险，拿出了另一套设备，为接下来两次特卖会做广告。结果，在第三次特卖会的第一天，即被警方当场抓获。

结合通信公司出具的评估报告，在三次特卖会期间案犯使用“伪基站”发送短信共计 100 余万条，严重影响了周边用户的正常通信。范强、王贵林利用“伪基站”设备，以非法占用电信频率的方式，破坏正在使用中的公用无线通信网络，在较大范围内较长时间造成用户通信中断，严重危害公共安全。最终，静安区检察院对两人以涉嫌破坏公用电信设施罪批准逮捕。这也是沪上首例“伪基站”案件。

分析启示

✓ **移动通信网络安全机制亟待完善。**由于目前 GSM 网络采用单向鉴权，仅有网络对用户终端鉴权，用户终端对网络不进行鉴权，“伪基站”的广播网号、广播频率只要同现有网络相同就会自动申请进网，用户手机很快会被“伪基站”抓取，“伪基站”便可以伪造任何号码向用户发送短信。随后，各种诈骗、垃圾短信就会源源不绝推送。若要根除“伪基站”，必须改善现有的安全机制，实现网络与用户终端的双向认证，来杜绝此类问题的发生和蔓延。同时也应看到，在商业利益的驱使下，越来越多的不法分子会利用现有安全机制的缺陷“发明”各类花样翻新的手段非法获利，原来未被关注的弱点很有可能成为新的突破口，需要举一反三，对原有系统的安全隐患进行排查，以防患于未然。

✓ **跨部门协同打击信息安全违法行为。**随着信息技术的发展，很多专用设备、黑客工作已经逐步平民化，导致此类信息安

全犯罪成本极低且难于被发现查处。就以此次案件为例，我国对于无线电的监管主要依靠设在各地的无线电管理部门，而伪基站设备的源头制造、中间销售等环节监管主要依赖于工商部门，对于违法犯罪行为的打击查处主要是公安部门的责任。本次“伪基站”上海首案的告破，就有赖于多个部门的整体协同配合。如果缺乏多部门协同合作，将成为监管无力的一个重要原因。

✓ **完善法律法规治理网络安全顽疾。**以防范“伪基站”为例，主要的法律依据《中华人民共和国无线电管理条例》制定于1993 年，至今未修订完善。其中对于类似使用“伪基站”干扰通信行为的处罚条款，主要是没收当事人设备并处罚款，最高不超过 5000 元。而这样的经济责任处罚，可能连一个“伪基站”一天的收入都不到。不法分子被抓后，其接受的处罚、缴纳的罚款与其非法所得相比微不足道。面对此类犯罪行为，政府部门应当从维护网络秩序和民众利益的角度出发，进一步增强法律法规建设，以适应目前信息化发展的需要。

信息来源

新浪网：

http://tech.sina.com.cn/t/2013-11-25/07328944989.shtml

影响范围：★★☆☆☆
影响程度：★★★☆☆
持续时间：★☆☆☆☆

关键字：

医院收费系统、故障频发

某城市多家医院收费系统故障频发

事件回顾

7 月 24 日，宁波市妇儿医院、宁波市中医院电脑系统相继瘫痪，造成门诊、收费出现拥堵。而在 7 月 14 日，这两家医院的电脑系统也发生过一次崩溃。其间，宁大附属医院、鄞州二院等医院也发生过类似的故障。这几家医院的门诊挂号收费系统均采用同一家公司的软件。经过初步调查，这几起故障均是由数据库中断服务引起的。

分析启示

✓ **信息安全保障要与“智慧应用”同步。**智慧城市的建设发展，带动了交通、电网、物流、医疗、政府、教育、农业等多行业的信息化提升，极大地方便了市民生活。但同时也应看到，由于这些行业服务于城市社会管理和公共服务的各个层面，对于系统的可用性要求极高，此类系统瘫痪往往会造成城市服务的“停摆”，而当前的信息技术尚不能完全避免错误和故障。为此，对于此类系统的信息安全保障，应该全面、系统、准确地了解其安全运行情况，进行有针对性的分析，研究拟定周全的解决方案，建立健全信息安全事件应急处置预案，规范信息系统运维制度。要以避免出现服务长时间中断为底线，对技术人员加强培训，进行系统故障排除演练，完善系统灾难备份措施，确保系统安全、可靠、平稳运行。

信息来源
中新网：
http://www.chinanews.com/sh/2013/07-25/5083743.shtml

影响范围：★★★☆☆
影响程度：★★★★☆
持续时间：★☆☆☆☆

关键字：

铁路售票系统、大面积瘫痪、人工通道放行

长三角铁路售票系统大面积瘫痪

事件回顾

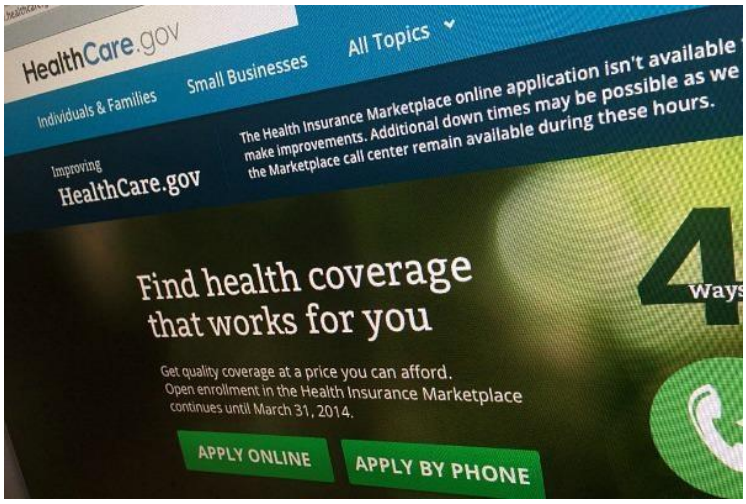
7 月 10 日下午，上海、南京、杭州、常州、镇江、苏州、无锡等多个长三角城市的铁路售票系统同时瘫痪，无论是人工还是自助都无法售票，时间在 1 个多小时左右。杭州站、杭州东站受此影响的始发列车有三四十趟，好在滞留的旅客最后被引导无票进站。浙江省内温州、绍兴等站也有不少乘客受到影响。据了解，此次事件与上海铁路局的售票服务器故障有关。

分析启示

✓ **重点领域工业控制系统安全基础薄弱。**2000 年后，通用开发标准与互联网技术的广泛使用，大幅度提升了工业控制系统的可靠性和可维护性。但与此同时，工业控制系统的信息安全问题并未引起业内的广泛重视，而针对工业控制系统攻击行为大幅度增长，导致系统安全问题频繁发生，甚至产生恶性安全事故，对人员、设备和环境造成严重的后果。针对关键的工业流程和城市基础设施，诸如核设施、钢铁、有色、化工、石油石化、电力、天然气、先进制造、水利枢纽、环境保护、铁路、城市轨道交通、民航、城市供水供气供热等，应探索开展工业控制系统的信息安全管理，以试点示范应用带动形成行业解决方案和标准规范；围绕工业控制系统的业务连续性要求，对其进行系统性的风险评估，制定针对性的风险控制对策和应急救援策略，并增设系统冗余服务，提升数据库、网络链路等系统核心模块的健壮性，降低系统运行风险，提高系统防范风险和应对突发事件的能力。

信息来源
网易：
http://news.163.com/13/0711/10/93GCAPVT00014AED.html

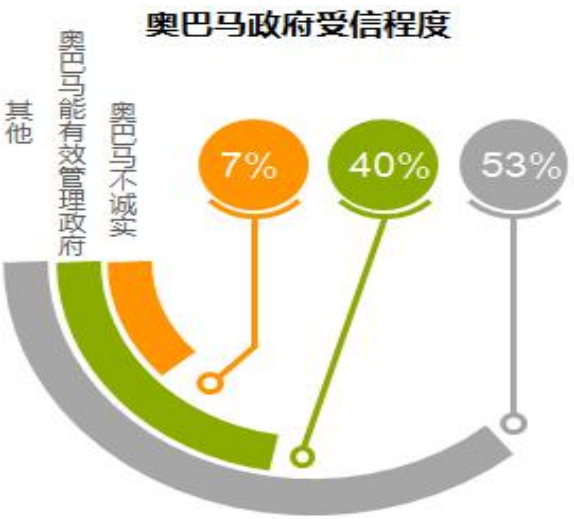
美医保平台崩溃重创奥巴马科技政府形象



事件回顾

美国医改核心工程“healthcare.gov”是作为奥巴马政府的重要政绩之一，但是自上线以来故障频频，给奥巴马竞选团队宣称的“科技政府”形象抹黑。《商业周刊》最新一期封面文章称，“healthcare.gov”的失败反应了政府的低效和官僚作风，政府须自身变革才能适应数字时代，做好 IT 项目。

报道称，作为奥巴马政府力推的新医保改革法案所包含的一项重要举措，医保网站自 10 月 1 日推出后，一直因网站服务器和软件平台故障频频，造成登录困难，导致民众怨声载道，引发舆论对奥巴马执政能力的质疑。经过一个多月的修复，饱受诟病的“奥巴马医改”医保网站终于在 11 月 30 日当天勉强重新上线，等待多时的美国民众也终于能够上网搜寻并注册适合自己的医保方案。美国白宫官员表示，该网站目前最多同时能够处理 5 万名用户的注册要求，每天能覆盖 80 万用户。据报道，在高峰时段，一些用户仍会收到“系统繁忙，请稍后再试”的提示。



因为网站问题，奥巴马政府 11 月 27 日甚至宣布将允许美国小型企业在线申请的日期再次延后一年，至明年 11 月，这已经是今年 4 月白宫宣布小型企业可以在线申请注册并购买医疗保险以来的第三次延期。这一决定立即遭到国会共和党人的强烈抗议，他们认为，此举预示着医保网站依旧无法正常运行。

美国医疗保险和医疗补助服务中心发言人巴塔伊发表的公开声明称，医保网站自重启后出错率降低，整体运行良好，但她也承认，未来一段时间网站仍有待进一步技术更新和修复。因此有人担心，原本计划在一年内实现注册 700 万人的目标恐怕难以最终达成。

美国有线电视新闻网最新民调显示，53%的受访者认为奥巴马不诚实或不值得信任。另外仅有 40%的人认为奥巴马能有效管理政府，这较今年 6 月时的比例下滑了 12 个百分点。此次民调是奥巴马执政 5 年来在关键领域表现最差的一次。奥巴马日前也坦言，医保网站的启动阶段“表现笨拙”。有分析人士指出，医保网站问题频出从侧面反映出奥巴马政府在医改法案中存在的设计缺陷。

分析启示

✓ **关键领域审慎采用尚未成熟的新技术、新应用。**美国“在线医保交易平台”由于无法注册购买、数据缺陷、系统故障、网站过载等诸多问题，给本已命运多舛的医疗改革蒙上了一层阴影。从本次事件同样可以看出，不论对于国家还是城市来讲，涉及国计民生的信息系统在采用新技术、新应用过程中应当注意存在的信息安全风险和隐患问题，提前进行风险测试和安全测评；必须充分考虑系统投入运营后的运营压力，提前预留潜力；在系统运营阶段，不断根据系统的运行情况适时进行优化调整，从而降低相关风险对系统稳定运行带来的影响。

信息来源
新浪网：
http://finance.sina.com.cn/stock/usstock/c/20131113/135617310055.shtml

企业法人信息安全

典型危及企业运行的信息安全事件

[本部分共选录了 7 个对企业法人造成重大影响的信息安全事件，具体包括保险公司泄露客户信息、ADOBE 遭黑客攻击、IBM 软件缺陷致工行业务中断、美联社推特账号遭入侵、美国运通被攻击、“乌龙指”事件、美国政府要求禁用 JAVA 插件等。]

企业法人信息安全是指信息安全事件一旦发生，会对企业正常运行造成严重威胁或危害。

随着信息技术和信息化应用的不断深化，企业信息安全将面临严峻挑战。企业法人信息安全以下趋势：

一、针对企业大数据的安全威胁将日趋严重。目前，数据已成为网络攻击的首要目标，在“大数据”概念迅速崛起的同时，企业更应关注数据安全问题。一方面，大数据意味着海量数据的归集，如果进行充分分析、整合、推理和加工，将产生更有价值、更加敏感的数据，这些数据会吸引更多的潜在攻击者。另一方面，数据大量汇集，使黑客只要成功实施一次攻击，就能获得更多数据，无形中降低了黑客的进攻成本。因此，大数据安全将成为企业信息安全保障的核心任务。

二、企业社交媒体应用安全风险凸现。社交媒体可以使企业以“邻居”和“朋友”的角色零距离与用户互动，这些活跃的社交媒体账号已成为企业发布信息的重要窗口之一。企业用户必须警惕社交媒体账号等“边缘”信息化应用的安全性，未经授权使用社交媒体向公众发布不准确或错误信息会导致公司声誉受损，甚至产生更大的经济社会影响。

三、企业内控不足成为导致信息安全事件的重要原因。光大“乌龙指”事件，快递、保险、医疗等行业企业信息的泄漏都是企业内部控制不足的表现。企业应重视自身内部控制环境的建设，设立有效的控制活动，加强内部信息的控制和监管，以降低因自身信息安全问题使用户蒙受损失的风险。

影响范围：★★☆☆☆
影响程度：★★★☆☆
持续时间：★☆☆☆☆

关键字：
客户信息泄露、罚款

某保险公司客户信息遭泄露 企业诚信面临挑战

事件回顾

3 月份北京警方连续破获两个有组织的侵害公民个人信息的犯罪团伙，抓获 92 名犯罪嫌疑人。在其中一起案件中，多名保险公司工作人员利用在保险公司就职的便利，先后出售 20 余万条客户信息。这些客户信息被诈骗团伙利用，导致大量客户受骗，被骗金额达 300 余万元。

据今年 3 月 15 日起正式施行的《征信业管理条例》规定，具有非法获取、采集个人信息，违法提供或出售信息、因过失泄露信息等行为的相关机构，企业法人将面临最高 50 万元罚款，直接责任人面临最高 10 万元罚款。

分析启示

这起事件中相关单位安全意识不强，忽视了自身业务信息的安全防护，对内部人员监管不力，导致用户敏感信息的外泄，造成了较为严重的影响。这警示我们，信息系统规划、建设、运维中的任一环节，都不能忽视安全问题。而对于企业信息资产的防护，可以从以下两方面加强管理：

✓ **加强内部信息安全管理。**企业应对信息系统和数据库建立资产管理制度，对资产进行分类分级，并在信息的采集、加工、存储、传输、检索等各方面进行安全管控。同时应加强相关标准和制度的宣导，对员工进行有效的信息安全培训和职业道德教育，提升员工对风险的识别能力，并通过签署保密协议等方式加强对内部人员的管理。

✓ **落实信息安全技术防范措施。**随着越来越多企业内部人员窃取倒卖用户隐私事件的曝光，数据防泄密已经成为很多企业关注的问题。企业应当结合各种技术手段，从审计、管控、加密等方面入手，形成完整的数据安全技术防护体系，这样可在很大程度上阻止类似恶意行为的发生，降低相应的违法风险。

信息来源
新华网：
http://news.xinhuanet.com/legal/2013-03/14/c_115028508.htm

影响范围：★★★★☆
影响程度：★★☆☆☆
持续时间：★★★★☆

关键字：

Adobe、黑客攻击、源代码失窃

Adobe 遭黑客攻击 海量源代码失窃

事件回顾

10 月 3 日，Adobe 公司首席安全官 Brad Arkin 通过官方博客发出警告称，黑客利用产品漏洞渗透到 Adobe 计算机网络，成功窃取了数十 GB 的软件源代码（其中包括 Adobe Acrobat，ColdFusion 和 ColdFusion Builder）和 3800 万客户信息。据初步调查，入侵时间发生在 8 月中旬，Adobe 公司正在为受影响的全球用户重置密码，并提醒用户更改在其他网站重复使用的密码。此外，Adobe 公司正与银行和联邦执法机构合作，以降低此次入侵带来的危害。这是微软在 2004 年被黑客入侵后，近 10 年来最大的源代码盗窃事件。

分析启示

IT 产品供应商自身信息安全问题凸现。Adobe 公司是国际知名的数字媒体和在线营销解决方案供应商。旗下多款产品都被广泛使用，包括 Adobe Photoshop，Adobe Flash Player 等。此次源代码泄露事件中的 Adobe Acrobat 是其知名的阅读器软件。大量源码泄露使黑客针对 Adobe 产品的漏洞挖掘变得更加容易，从而产生一大批相应的零日漏洞。对于 Adobe 这样的大型 IT 技术产品供应商来讲，信息安全就是企业的生命线，需要重视从信息系统的实体安全、软件安全到数据安全这样全方位的安全问题，保证所有信息资产不被窃取，免遭破坏。而对于用户而言，应关注大规模使用的软硬件产品安全，及时升级系统和软件版本，安装补丁程序，并定期进行安全测评。

信息来源
网易：
http://tech.163.com/13/1031/06/9CGC54EM000915BF.html

影响范围：★★★☆☆
影响程度：★☆☆☆☆
持续时间：★☆☆☆☆

关键字：
IBM、软件缺陷、工商银行、业务中断

IBM 软件缺陷导致某商业银行多处网点业务中断

事件回顾

6 月 23 日上午，全国多地工商银行柜台、ATM、网银业务出现故障，持续近 1 个小时。作为服务 2.92 亿个人客户及 400 多万公司客户的全国金融服务巨头，工行此次故障波及北京、上海、广州、武汉、哈尔滨等多个大中型城市。

针对此事，中国工商银行信息科技部就6月23日工行系统故障事件正式作出内部通报，这份通报称，此次事件归因于工行数据中心（上海）主机系统出现故障，是由于 IBM 提供的主机 DB2V10 版本内存清理机制存在缺陷引发。

分析启示

数据大集中安全风险不容小视。金融系统的数据大集中模式能够节约成本、便于管理，被许多大型企业采用，但缺点是每一次信息处理都要通过该数据中心，只要该数据中心系统中的一个关键模块出现故障，就有可能发生大范围的安全事件。数据大集中模式对于服务器的稳定性和安全性要求也相当高，只有拥有强大数据处理能力并且稳定的大型服务器（也称大型机）能满足这种模式的需求，而大型机市场长期以来被 IBM 所垄断，技术受制于人、服务依赖于人仍是国内企业面临的重大问题。此外，在业务连续性规划、业务恢复机制、风险化解和转移措施、技术恢复方案等方面，很多企业依然存在‘短板’，需要结合行业和企业实际需求，加强信息安全的规划建设与配套投入。

信息来源
东方网：
http://finance.eastday.com/m/20130623/u1a7472066.html

影响范围：★★★★☆
影响程度：★★★★☆
持续时间：★☆☆☆☆

关键字：
美联社、推特账号、入侵

黑客借美联社账号散布谣言 致股市大跌

事件回顾

4 月 24 日，黑客入侵美联社（Twitter）帐户，并发布消息称白宫发生两起爆炸，总统奥巴马受伤。在假消息出现后，道琼斯指数一度重挫逾 150 点。美联社随后发布声明：“美联社帐户遭攻击，有关白宫遭到攻击的消息是假的，我们将尽快公布更多讯息。”美联社也表示，推特帐户在遭黑后已暂停使用，并正致力于修复问题。

分析启示

社交网络信息安全问题应予以高度关注。由于微博、微信等社交媒体的实时性、准确性，近期社交媒体在新闻传播的过程中正扮演着越来越重要的角色，其影响程度甚至超过了传统报业。据统计，全球 500 强中，77%的公司有自己的 Twitter 账户并保持活跃，70%的公司有自己的 Facebook 主页；国内微博、微信也同样如此，很多政府机构、企事业单位也借助社交媒体得到了很好的发展。而这些活跃在社交媒体上的机构“大号”，往往成为黑客攻击的主要对象，比如此前汉堡王账号被黑，发出错误的信息称被麦当劳收购；哥伦比亚广播公司账号被黑，发布了一系列有关奥巴马以及美国政府协助基地组织的消息。这些事件暴露了各类社交网络安全保障水平的参差不齐。新技术、新应用在发展成熟之前，信息安全方面普遍存在脆弱性，企业在使用这些新技术、新应用开展业务的同时，也要充分意识到由此带来的风险，关注网络安全问题，防止其成为企业信息安全保障体系上的“短板”。

信息来源
中新网：
http://finance.chinanews.com/stock/2013/04-24/4758636.shtml

影响范围：★★★★★
影响程度：★★★☆☆
持续时间：★☆☆☆☆

关键字：

美国运通、网上银行、网络攻击、瘫痪

美国运通遭网络攻击后瘫痪 网上银行服务中止数小时

事件回顾

3 月，美国著名的金融公司美国运通公司遭到黑客组织的网络攻击，致使该公司的网上银行服务停顿了大约两个小时，信用卡客户无法访问账户中的信息。

据报道，这次对美国金融企业的网络攻击技巧高超。黑客并非遵循传统，利用一些个人电脑向每家银行发射网络流量，而是以高级的恶意软件侵入强大的商业数据中心，命令它们同步向每一家银行展开攻击。

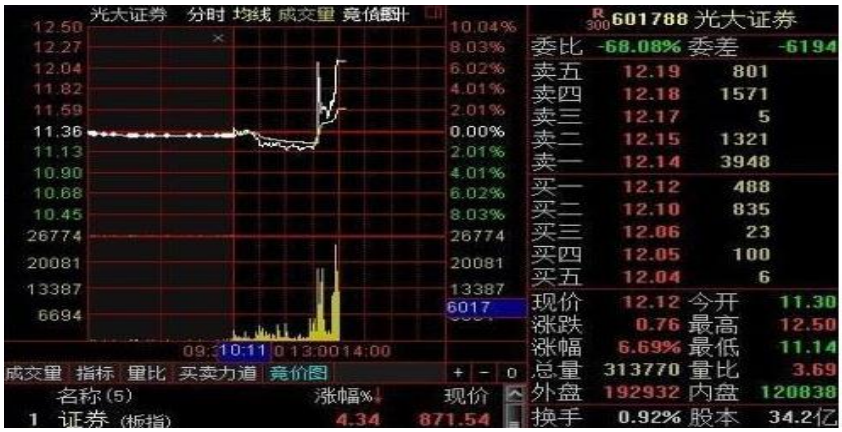
研究这些攻击的安全专家表示，此次攻击与此前 6 个月中，导致摩根大通、富国银行、美国银行和其他一些金融机构瘫痪的攻击是由同一批人发动的。

分析启示

信息安全保障需要专业化服务支撑。随着金融信息化的高速发展，电子银行、互联网金融等业务已在银行、证券、保险、基金等金融机构业务开展中扮演更加重要的作用。可以说，在金融领域，信息服务出问题就能导致整个企业的运转问题，有可能损失大笔业务，造成巨额赔偿和网络维修费用，更会降低客户体验。如何在愈加恶劣的生存环境和更为复杂的技术应用条件下增强应对灾难及各种突发事件的能力，保障业务连续性，已是各大企业面临的重点和难点问题。事实上，包括金融机构在内的大部分对业务连续性要求较高的企业均根据自身特点，构建了相应的信息化服务队伍和安全保障团队，但是在愈加有针对性、专业化、有组织的网络威胁面前，完全依靠自身的安全保障力量已经无法解决问题。为此，企业应首先了解可能导致业务中断的各个风险点，并以降低业务中断产生的影响、快速恢复业务为目标，依托外部专业化力量构建信息安全技术防范体系，并加强与政府部门、专业机构、网络运营商的工作协调和协同应急，建立有效的协作和联动机制，保障系统的安全可靠运行。

信息来源
比特网：
http://sec.chinabyte.com/37/12575537.shtml

券商“乌龙指” 致使 A 股离奇暴涨



事件回顾

2013 年 8 月 16 日 11 时 05 分，上证指数出现大幅拉升，大盘 1 分钟内涨幅超 5%，最高达 5.62%，指数最高报 2198.85 点，逼近 2200 点。11 时 44 分上交所称系统运行正常。下午 2 点，光大证券公告称策略投资部门自营业务在使用其独立的套利系统时出现问题，有媒体将此次事件称为“光大证券乌龙指事件”。

据事后调查通报：光大证券自营的策略交易系统包含订单生成系统和订单执行系统两个部分，存在程序调用错误、额度控制失效等设计缺陷，并被连锁触发，导致在 16 日 11 时 05 分 08 秒之后的 2 秒内，瞬间生成 26082 笔预期外的市价委托订单，直接发送至上交所，累计申报买入 234 亿元，实际成交 72.7 亿元。

分析启示

本次事件中，光大证券策略交易投资部门未纳入公司风险控制系统，交易系统自 7 月 29 日上线运行到事发仅 15 个交易日，其订单重下功能也从未被实盘测试过。而正是此功能直接造成了错单事件。此次事件充分表明：

企业信息化风险管控亟待加强。对于证券业这样的高风险、高信息化行业，加强信息系统的风险防范并定期进行风险评估是至关重要的。企业在推进信息化过程中，若不注意业务本身的风险防范，必将承受巨大损失。对于重要的网络、信息系统和关键岗位，要通过管理、技术手段加强风险控制，对于存在重大风险的事件还应建立相应的预警与拦截机制。

IT 审计和内控不能流于形式。光大证券曾于 2013 年 3 月发布《2013 年内部控制评价报告》。在万余字的报告中，光大证券称其操作风险管理“通过严格论证及公司审批，保证制度及流程的全面性、合理性与可执行性。”由此可见，企业内部审计等监控措施应当切实落到实处。一方面，企业应重视内部控制环境的建设，加强风险评估，保证控制活动的有效性，发挥内部监督的作用；另一方面，引进第三方专业机构开展安全审计，通过专业化、标准化的信息系统审计，能够有效保护信息资产的完整和安全。

信息来源
新浪网：
http://finance.sina.com.cn/zl/fund/20130818/093716482588.shtml

影响范围：★★★★★
影响程度：★★☆☆☆
持续时间：★★★☆☆

关键字：
Java 插件、漏洞、禁用

漏洞层出不穷 美政府禁用浏览器 Java 插件

事件回顾

1 月 12 日，据国外媒体报道，美国国土安全部警告电脑用户禁止使用甲骨文的 Java 软件。一些警告称，黑客已经发现了如何检测到 Java 软件，并通过该软件来安装恶意程序，从而使他们能够开展各种网络犯罪，包括盗窃用户身份证号，将被感染的计算机作为网络的一部分，以此来攻击其它网站等。

美国国土安全部计算机应急准备小组发布通告表示：“Java 新的和之前的漏洞已成为黑客广泛的攻击目标，Java 新的漏洞很容易被发现。为了防范 Java 这一新的及未来的漏洞，计算机用户应在其 Web 浏览器中禁用 Java 插件。”

分析启示

通用软硬件产品安全不容忽视。甲骨文的 Java 等被广泛使用的软件，虽然其技术保障力量同样比较强大，但是一些难以发现、时效性强的漏洞仍然具有很大的危害性。对此各大 IT 技术产品供应商应当对自身产品的安全性进行有效控制，积极修补软件漏洞，以通知的形式告知用户，对更新包也应进行安全性检测，以免造成新的软件漏洞。作为用户，同样应使用正版软件，及时更新软件、系统补丁以降低系统安全风险，并从边界安全、中间件安全和终端安全的角度，部署相应的技术安全产品，对不熟悉的软件不要轻易下载安装，陌生人发送的链接不要随便打开，以降低自身遭到攻击的可能性。

信息来源
腾讯网：
http://tech.qq.com/a/20130112/000037.htm

公民个人信息安全

典型危及公民个人的信息安全事件

[本部分共选录了 5 个对公民个人造成重大影响的信息安全事件，包括搜狗浏览器泄密、2000 万个人开房记录遭泄、7000 多万个 QQ 群数据遭泄露、电信诈骗频发、史上最大规模 DNS 劫持等。]

公民个人信息安全是指信息安全事件一旦发生，会对公民个人隐私、生活造成严重威胁或危害。

本年度发生的危害公民个人信息安全事件体现了以下特点：

一是大数据风险。大数据时代的到来凸显出“信息供应链”的安全风险。从今年的情况看，各类数据安全事件集中爆发，政府、金融、企业数据被拖库、信息被窃、隐私被泄露事件层出不穷。“斯诺登”事件爆出的美国的一系列网络监控项目，更是突出了针对网络海量数据的搜集、获取、分析和控制带来的信息霸权威胁，集中反映了大数据时代全球治理的安全困境。随着物联网、大移动时代的到来，数据和信息的失控问题不能不令人担忧。如何保证海量、结构复杂的数据本身和网络化共享的安全，是需要我们重新思考并认真研究的重大战略难题和现实战术问题。

二是公众信息安全意识急需提升。2013 年度发生的多起典型安全事件在一定程度上体现了公众普遍缺乏信息安全意识，缺少信息安全基础知识和实践动手能力。面对复杂的网络环境，有必要发动全社会各方面力量，有针对性地开展信息安全意识宣传工作。

三是个人信息泄露已成为公民面临的首要信息安全问题。伴随着信息技术和互联网新业态的发展，位置、购物记录、手机及身份证号等公民个人信息已成为实实在在的“生意”。由于利益驱动，产生了大量针对公民个人信息的违法犯罪行为。对此，社会各方面需要共同关注和通力合作，保护好公民个人信息安全。

四是针对公民个人的信息安全威胁层出不穷。数字生活使得普通民众的生活与网络的连接越来越紧密，普通公民个人在面对病毒、木马、网络钓鱼、电信诈骗等传统网络安全威胁的同时，新技术也为网络攻击提供了新的管道。除了个人电脑、平板电脑、智能手机之外，其它具备网络应用能力的设备（如智能电视）也可能成为新的攻击目标。

2013 年 2 月 1 日，我国首个个人信息保护国家标准——《信息安全技术 公共及商用服务信息系统个人信息保护指南》已正式实施。该指南明确了个人信息处理原则和个人信息主体的权利，提出了个人信息的收集、加工、转移、使用、屏蔽和删除等行为要求，显示了国家对于保护公民个人电子信息安全的决心。广大政府部门、企事业单位都应该按照要求，提高对于公民个人信息的保护力度，共同维护好安全可信的信息消费环境。

影响范围：★★☆☆☆
影响程度：★★☆☆☆
持续时间：★★☆☆☆

关键字：
搜狗、泄密、网站密码

搜狗浏览器泄漏众多网站账号密码信息

事件回顾

11 月 5 日，有网友发帖称，使用最新版本的搜狗浏览器可以获得其他用户的账户信息，泄密范围包括淘宝网、人人网和各类电子邮箱。获取密码后，可以直接登录甚至用别人的账号购物。

在 11 月 5 日晚的中央电视台新闻频道的《24 小时》节目中，也对此事进行了报道。央视记者报道其进行了成功操作，获取了上千个其他用户信息，并且使用其中一条信息成功登录了他人的淘宝账户。这些用户信息中包括公积金、各类电子邮箱、淘宝等，也有一些政府部门网上管理系统的密码。

分析启示

✓ **云计算信息安全引起多方关注。**本次事件的发生与厂商使用云计算技术提供在线服务不无关系。云服务能够有效降低设备成本，还有着高效的计算能力，只要用户能够接入高速的网络，云端的强大设备便能迅速处理出结果并发送给用户实时信息，而云端存储服务也将用户数据都释放到了云端。虽然云服务的供应商都一再保证其安全性，但用户存放在云端服务器上的数据安全性仍然存疑。如何保证这些服务的可用性、安全性将是不得不面对的新挑战。对此，用户应该有更加足够的信息安全风险意识，对于通讯录、通话记录、短信、账号密码等个人隐私信息，应审慎选择存储方式，即便确实需要安全备份，也应尽量选择备份软件进行本地备份，或者对上传云端的数据进行加密处理，防止数据上传云端导致的隐私泄露问题。网络服务提供商、终端软件供应商等在获取用户信息并传送至非预期的后台管理服务端或云端时，应有明确的提示，使用户对存在的风险知情。

信息来源
新华网：
http://news.xinhuanet.com/yzyd/local/20131107/c_118047539.htm

影响范围：★★★★☆
影响程度：★★☆☆☆
持续时间：★★★★★

关键字：
开房记录、泄露

2000 万个人宾馆入住记录被盗

事件回顾

国内一家安全漏洞监测平台 8 月 21 日上传、10 月 5 日公布的报告称，如家等大量酒店客户开房记录被第三方存储并因漏洞导致泄露。这些酒店包括如家、咸阳国贸大酒店、杭州维景国际大酒店等，全部或部分使用了浙江慧达驿站网络有限公司的酒店 WiFi 管理、认证管理系统。

北京盈科律师事务所易胜华律师昨天表示，从目前的情况判断，网上流传的 2000 万个人开房信息基本属实，他认为警方该介入调查。

易胜华称，该事件不要光盯着“开房”这个噱头，这件事情最严重的是大量隐私被泄露，2000 万个人数据，意味着我国每 75 个人里面就会有 1 个人的基本信息完全曝光。

分析启示

涉及泄密的酒店全部或者部分使用了浙江慧达驿站网络有限公司开发的酒店 WiFi 管理和认证系统。涉及此事的酒店并没有把用户认证数据传入酒店服务器，而是传入了第三方企业的服务器，用户认证数据包括客户名、身份证号、开房日期、房间号等大量敏感、隐私信息，且在传输过程中加密处理不足，最终造成了客户信息的泄露。此次事件提醒各类企业对客户信息安全应引起足够重视，必须采取措施对此类数据进行严格保护。

✓ **“最少够用”应成为个人信息保护重要原则。**2 月起实施的“个人信息保护指南”中明确提出了“最少够用”与“安全保障”原则，即只处理与处理目的有关的最少信息，达到处理目的后，在最短时间内删除个人信息。并采取适当的管理措施和技术手段，保护个人信息安全。而涉及该事件的浙江慧达驿站网络有限公司显然没有满足这两项基本原则。企业在提供服务时应当遵循“个人信息保护指南”，对个人信息收集、加工、转移和删除等环节进行严格控制。当企业将部分带有个人信息的数据交由外包服务公司进行处理时，相应的个人信息保护责任应该通过具有法律效力的契约方式传递到外包服务承接方，并对其进行有效监督。此外，政府部门也应进一步加强个人信息保护力度，严厉打击此类个人信息泄露、倒卖、侵权等犯罪行为。

信息来源
网易：
http://news.gmw.cn/newspaper/2013-10/23/content_2283437.htm

影响范围：★★★★☆
影响程度：★★☆☆☆
持续时间：★★★★★

关键字：
QQ 群、泄露

7000 万 QQ 群数据遭泄露

事件回顾

国内知名安全漏洞监测平台乌云在 11 月 20 日公布报告称，腾讯 QQ 群关系数据被泄露，数据下载链接很轻易在迅雷快传找到。根据 QQ 号，可以查询到备注姓名、年龄、社交关系网甚至从业经历等大量个人隐私。

此次数据泄露涉及 7000 多万个 QQ 群、12 亿个部分重复的 QQ 号。专家表示，“当黑客掌握用户的社交关系后，可以完整了解用户个人情况，利用社交圈的信任关系进行诈骗，成功率很高。”

腾讯公司回应记者称，此次 QQ 群数据库泄露确有其事，但这一漏洞是 2011 年发现的问题，当时已及时修复，不影响现有用户正常使用。与此同时，他们也正在全力防范减少此前数据库泄露可能带来的危害。

分析启示

✓ **公民个人信息保护意识亟待提高。**各种即时通讯工具、社交软件成为了人们日常社交或工作中重要的组成部分，这些应用不仅是一个人与人沟通交流的平台，更形成了一张巨大的人际关系网络。当黑客掌握用户的社交关系后，可以完整了解用户个人情况，利用社交圈的信任关系进行诈骗，或被用于精准营销。广大个人用户使用此类应用过程中，应该给予此类软件合理的系统权限，在发布与自身有关的信息时应注意知晓范围，并严防银行卡、手机号、网站账号、密码等敏感信息公布在网络上。

信息来源
网易：
http://news.163.com/13/1122/04/9E8OR0VS00014Q4P.html

影响范围：★★★★☆
影响程度：★★★☆☆
持续时间：★★★★★

关键字：
电信诈骗、冒充亲友

电信诈骗频发 接听电话需警惕

事件回顾

近年来，电信诈骗层出不穷，形式各种各样。有冒充亲朋好友借钱，有假冒银行短信，更有冒充法院传票等。据统计，2013 年 1 至 9 月，仅上海市就破获电信诈骗案件 2220 起，上海全市各级公安机关联手商业银行共成功劝阻电信诈骗案件 5536 起。

分析启示

如今的电信诈骗，已经呈现以下几种趋势：犯罪场所隐蔽化。诈骗团伙在境外设计骗局，诈骗大陆居民，他们借助 VOIP 等拨号软件，有针对性地诈骗企业中、高层管理人士，得手后在境外分层转账，隐蔽性更强。欺诈方式多样化。传统诈骗手法如冒充亲友、老板、房东要求汇款或者假扮邮局、社保、税务和公检法人员等，还有一些案例中，犯罪分子利用高科技仪器（如伪基站），冒充银行客服号码发送诈骗短信，或是通过其他途径得到客户信息，有针对性的实施诈骗。诈骗犯罪产业化。现在的电信诈骗往往会事先编写好“诈骗剧本”，设计好诈骗时的对白和语音播报内容；针对不同地区的诈骗，行骗人员还会冒充不同地区不同单位的工作人员，所提供的单位名、电话号码等都与当地信息吻合；诈骗人员“上岗”前还会接受培训，由培训师讲授业务知识，并有资深骗子“现身说法”讲述自己行骗“成功案例”。电信诈骗几乎成为一条环环相扣的“产业链”。

✓ **治理电信诈骗需“打防并举”。**广大民众应主动提高安全意识，如遇到可疑电话或短信，千万不要轻易汇款、转账，应及时与公安机关联系；相关部门也应加大宣传力度，拓宽宣传渠道，扩大受众范围，揭露诈骗伎俩，提升广大公民防骗识骗能力。同时，公安、通信管理政府部门与银行等金融机构应该针对电信诈骗特点，加强可疑电话拦截、提醒等技术防范措施落实，并共同打击防范电信诈骗行为。

信息来源
新华网：
http://news.xinhuanet.com/legal/2013-10/29/c_117919308.htm

影响范围：★★★★☆
影响程度：★★☆☆☆
持续时间：★★★★★

关键字：
DNS 劫持、感染

史上最大规模 DNS 劫持“吸金” 千万用户被钓鱼

事件回顾

6 月，中国电信集团官方微博发出安全预警，称中国电信网络安全中心（SOC，Security Operation Center）的技术专家近期发现国内网民家用宽带路由器中的 DNS 配置可能被黑客篡改，导致 DNS 钓鱼。同时，国内 DNS 服务提供商“114DNS”通过其官方微博发出安全预警，称新一轮 DNS 钓鱼攻击已经突破国内安全防线，或已导致数百万用户感染。已监测到约有 4%的全网用户可能已经处于此次 DNS 钓鱼攻击威胁当中。若按全网用户 2 亿规模估算，每天受到此次 DNS 钓鱼攻击的用户已达到 800 万，而如此大规模的 DNS 钓鱼攻击在以往十分罕见，可能是史上最大规模黑客攻击。

分析启示

✓ **个人网络接入设备安全问题突出。**随着智能手机、平板电脑、智能电视盒等数码产品的普及，无线网络成为市民离不开的重要工具。但是目前，我国大部分设备仍使用默认设置，使无线网络、物联网遭遇到与互联网同样的信息安全威胁。黑客往往利用家用数码产品使用默认用户名、口令的弱点，在某些网页中嵌入了恶意代码，从而修改设备设置进行网络钓鱼。广大用户应尽量自定义设备设置，防止使用默认设置来配置设备；相关厂商在设置初始账号时也不应使用固定的账号和口令，并在发现设备漏洞时应及时发布相应的补丁程序。此外，部分网络运营商在向用户提供宽带路由器等接入设备时，并未将设备的最高管理权限交给用户，所有接入设备的控制权由运营商统一掌握，一旦安全机制被突破将影响所有用户，在这种情况下运营商应承担起安全防护的职责，对此类事件采取相应的防范措施。

信息来源
腾讯网：
http://tech.qq.com/a/20130614/019786.htm

结束语

2013年是不平凡的一年，国际国内信息安全事件不断，信息安全问题已上升为国家安全问题，与人们生活也息息相关，信息疆域保护问题也将成为国家主权维护的重要内容。安言咨询认为，2014年的热点和趋势主要涉及一下几方面：

安全威胁将渗透任何一个角落。随着社交媒体和移动终端持续升温，人们的生活越来越离不开信息设备。在信息化带给人们便利的同时，也带来了严重的安全隐患。小到个人，大到国家都将继续面临数据安全与隐私问题，甚至威胁生命。

国产软件迎来机遇。美情报部门入侵中国互联网引发国内信息安全防护软硬件设备的需求关注，进而加大国内政府及企业对国内安全产品及服务的采购力度，棱镜事件在国内的影响将持续发酵，给国内信息设备提供商带来机遇。中国国内信息安全基础设施包括计算、网络、存储、安全四条主线，将加速推进国产替代，给浪潮信息、星网锐捷、国脉科技、东土科技、同有科技、数码视讯等公司带来替代国外供应商的机遇。

信息安全机制重塑并广泛协作。 对数据的重视和应用不足、信息化法律法规缺失等问题，成为制约大数据发展的障碍和威胁信息安全的隐患。以往建立的各类监管、检测和

验证机制日益显出其孤立、封闭、片面、狭义的特性。信息安全亟需从上至下、广泛协作、软硬并施的大格局。随着《中共中央关于全面深化改革若干重大问题的决定》的提出、国安委以及中央网安小组的成立，后续立法、管理、保障市场秩序的建立工作势必将逐一推展。与此同时，民众的普遍意识，企业的积极应对，社会的共同参与，若能与国家顶层设计相符相应，信息安全将真正做到全面开花。