二十、上海信天通信有限公司审核案例

推荐机构：北京新世纪检验认证有限公司

认证类型：信息安全管理体系

认证人员：葛嘉炜

一、案例背景

客户名称：上海信天通信有限公司

审核类型：第一次监督审核

审核时间：2013-11-13~~11-15AM

审核依据：GB/T22080-2008/ISO/IEC27001:2005

审核组成员：组长：胡显国，组员：葛嘉炜

上海信天通信有限公司创立于 2000 年 12 月，由中国电信股份有限公司 、美国 AT&T 公司、上海市信息投资股份有限公司投资组建。

作为国内首家合资的电信运营企业，信天通信依赖其中国本土电信网络资源、美国 AT&T 环球网络资源和技术管理经验、以及政府产业政策的扶植、发挥强强合作的优势，悉心打造能跨越地理界限、超越文化背景而进行商务运作的综合信息平台。

此次审核主要是信息安全体系的过去一年中的实施情况，特别是信息安全控制措施的落实情况。

二、主要审核发现、沟通过程

1） 在运营服务中心审核，该部门主管公司日常的办公网络运行，查对恶意代码的防护，现场抽查工作电脑，安装了 360 杀毒软件和安全卫士，但利用安全卫士体检结果为 33 分，存在高危漏洞，杀毒软件日志显示超过 30 天未进行扫描；

现场与网管沟通，公司制定了《恶意软件管理规定》，规定由运营服务中心网管负责全公司防病毒软件的安装及病毒库的更新管理，为各部门信息处理设施的防范恶意软件提供技术性支持；但日常工作中网管未能明确杀毒软件使用的要求，日常检查的力度不够，导致部分工作电脑未能定期进行扫描和体检，对恶意代码的防范存在隐患。

2） 在审核过程中发现公司工作电脑上网未能实施 IP 地址和 MAC 地址绑定，无法对员工网络访问进行监管，也不符合公司《信息安全适用性声明（SoA)》中相关条款控制措施的要求；

公司网管介绍日常工作为了移动办公和上网方便，没有制定 IP 地址和 MAC 地址绑定的策略，忽略了信息安全方面的问题。

三、标准解读及问题分析

1） GB-T22080-2008 A.10.4.1 条款要求应实施恶意代码的检测、预防和恢复的控制措施，以及适当的提高用户安全意识；

工作电脑是日常办公时员工与内外部沟通的渠道，安装了内部管理的信息系统，并且存放了重要的工作资料；日常除了需要对进行物理防护外，对恶意代码的检测和预防也十分关键，如果电脑遭到恶意代码攻击导致系统损坏，不仅会影响个人正常工作还会引起与其他有过文件传输的工作电脑之间的恶意代码传播；安装杀毒软件，定期进行病毒库更新和全盘扫描、体检可以有效的防止工作电脑受到恶意软件和病毒的影响，并通过磁盘清理、优化设置提升工作电脑的运行速度，从而提高工作效率；

公司制定了相应的管理制度并明确了责任人，但是在实际工作中的执行力度有所欠缺，未能定期进行监督检查；另外员工的信息安全意识较为薄弱，对公司管理制度学习不够，未能意识到恶意代码防范不当所带来的安全问题。

2）GB-T22080-2008 A.11.4.3 条款要求应考虑设备的标示，将其作为鉴别特定位置和设备连接的方法；

对上网电脑要求 IP 地址和 MAC 地址绑定可以实现静态 IP，防止 ARP 攻击，从而防止未获得网络访问权限的电脑通过修改 IP 地址来连接公司网络；同时便于网管对各员工电脑的网络使用情况进行监管；

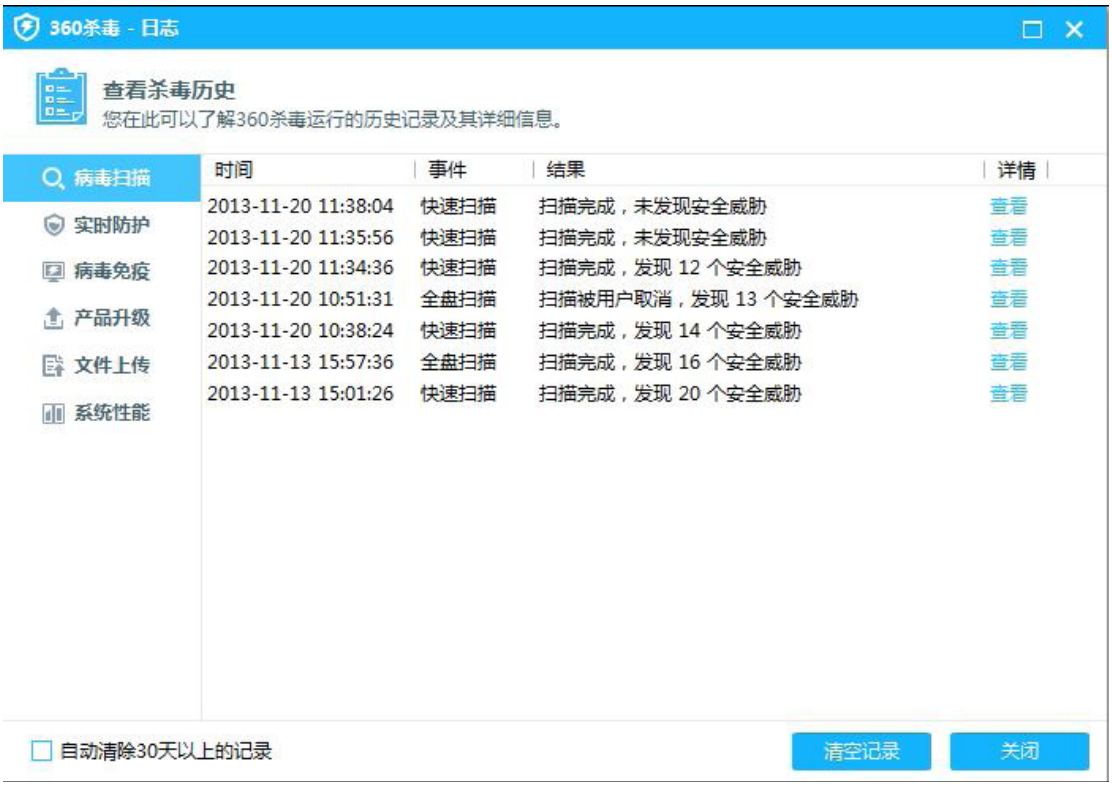
公司的《适用性声明 SOA》A.11.4.3 条款的控制措施中要求计算机全部采用固定 IP 与 MAC 地址绑定，网管为了工作中集团公司人员来公司开会时以及移动办公时网络使用的便利，暂时没有对上网电脑实施 IP 地址和 MAC 地址绑定，从而导致对网络访问控制的管理不当。

四、改进过程及取得的成效

基于以上事实和沟通，受审核组织领导对我们发现的问题欣然接受，并表示此次审核人员指出的问题工作中没有关注到，但却存在很大的安全隐患和风险,一定认真整改。现场审核后，受审核组织对提出的不符合项均进行原因分析并制定了纠正措施，并举一反三，排查所有信息处理设施，取得了良好的管理成效。

1）对于 A.10.4.1 条款提出的不符合采取的纠正措施包括：立即对工作电脑进行体检，对漏洞进行修复，更新病毒库进行一次全盘扫描，并将病毒的查杀策略设置为每周一上午 9 点定期检查；

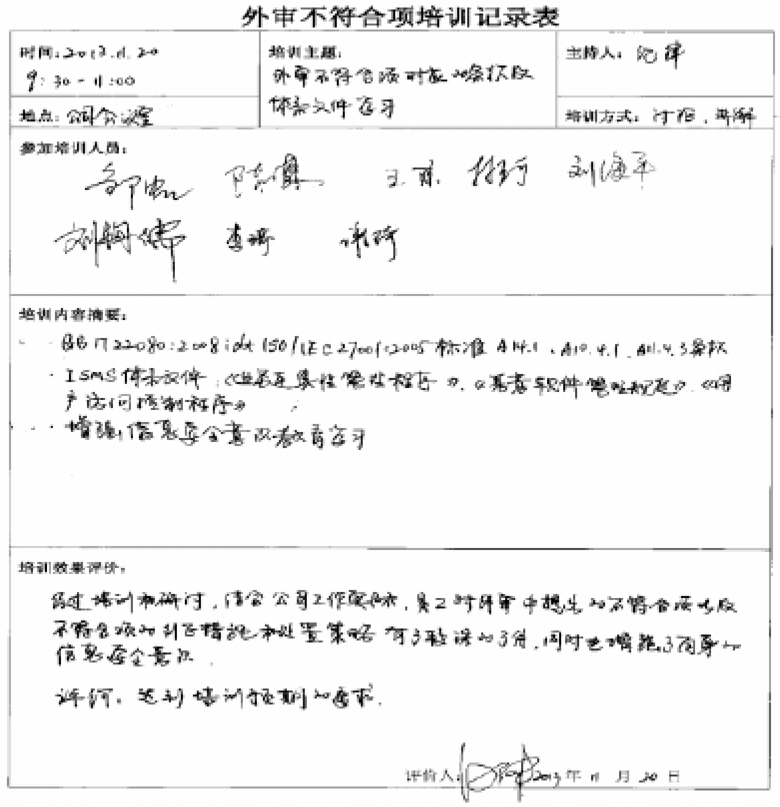
组织员工学习公司对于恶意代码防护的管理制度文件，增强员工的信息安全意识。



2） 对于 A.11.4.3 条款提出的不符合采取的纠正措施包括：由网管立即实施工作电脑 IP 地址和 MAC 地址绑定的策略，并在《员工计算机 IP 分配登记表》中进行登记;对于外来人员使用公司网络需在网管处进行登记，由网管分配上网权限；

并对员工进行公司体系文件的培训，增强其信息安全意识；

1	ISMS-4112-员工计算机IP分配登记表													
2	制表人：											密级：秘密		
3	序号	姓名	部门	设备	MAC地址	IP	外网权限	内网权限	USB	Internet权限定期评审				
4										评审日期	评审人	用户状态	是否恰当	评审结果
9	5	邹 妘Cecilia	GA	便携式电脑			✓	✓	✓	2013.11.20	刘海平	活动	是	通过
10	6	张坚霞 Sara	GA	便携式电脑			✓	✓	✓	2013.11.20	刘海平	活动	是	通过
11	7	纪 律 Ji Lv	SP&D/GMO	便携式电脑			✓	✓	✓	2013.11.20	刘海平	活动	是	通过
12	8	王 萌 Wang Meng	SP&D/GMO	台式机			✓	✓	✓	2013.11.20	刘海平	活动	是	通过
13	9	林 珂 Steven	SP&D/GMO	台式机			✓	✓	✓	2013.11.20	刘海平	活动	是	通过
14	10	王 卫 Delia	FIN	台式机			✓	✓	✓	2013.11.20	刘海平	活动	是	通过
15	11	仲建英 Jane	FIN	台式机			✓	✓	✓	2013.11.20	刘海平	活动	是	通过
16	12	付晓鸣 Milly	SE	便携式电脑			✓	✓	✓	2013.11.20	刘海平	活动	是	
17	13	曾其武 Joye	SE	便携式电脑			✓	✓	✓	2013.11.20	刘海平	活动	是	通过



取得成效：

通过此次审核，受审核方领导和员工充分意识之前虽然已进行了信息安全管理体系的贯标，但是在日常工作中对标准要求的理解实施还有所欠缺，员工更多的关心本职工作及业务上的事，忽略了信息安全的要求，员工总体信息安全意识较为薄弱，利用对审核中提出不符合整改的机会重新对公司的体系文件进行了培训学习，加强全员的信息安全意识；

同时通过审核，受审核方对信息安全标准中的要求有了更深入的认识，也发现了在日常工作过程中实际存在的信息安全隐患和信息安全管理漏洞，经过与企业领导层以及各部门人员沟通交流后，企业认可了认真执行标准中规定的控制措施对公司的信息安全管理带来帮助，并表示今后会对信息安全更加重视，结合实际工作加强培训教育，做到持续改进，不断提升信息安全体系的实施效果和公司信息安全的管理水平。