北京市政务信息安全监控预警系统的经验之谈

解决方案

根据用户不同的信息安全需求，提供因需而变，因御而安的整体安全解决方案

背景介绍

不夸张的说，电子政务为政府部门的沟通和管理方式带来的前所未有的革命性的变化，它打破了组织单位之间的界限，改变了以往层层关卡、书面作业、繁琐复杂的事务办理流程和审核方式，借助信息化的技术手段，以虚拟化机关的形式提供着各种与人们息息相关的服务。信息技术为人们带来的便捷再次作为一个大大的好处被凸显出来，而与之并行的危险却在阴暗的角落不断上演，信息安全保障成为电子政务系统发挥其职能和优势的根本前提。

在各省的电子政务建设中，政务外网是非常重要的一部分，它支撑着众多省级政务用户和重要的政务应用的运行，因此一旦政务外网出现了病毒传播、敏感信息传播等信息安全事件，其影响是非常严重的，尤其是在一些重大的活动期间，例如：奥运、世博、亚运等，政务外网尤其成为被重点关注的对象。那么，电子政务外网一般都会遇到哪些威胁？出现这些问题之后又会由哪些部门来处理？电子政务外网的安全管理如何建设？北京市政务信息安全应急处理中心安全监控部副部长刘鹏就此类问题给出了他的理解和最近的一些感受。

北京市政务外网的防御之道

据了解，北京市政务安全应急处置中心（简称应急中心）承担着北京市所有政务相关的信息安全监控与应急响应方面的工作，随着应急工作的逐年深入开展，应急中心发现，这种被动事件响应与处置的工作机制存在着诸多隐患：安全问题不能及时发现和有效控制；安全监控分析能力较差；政府网页攻击日趋严重；无法全面掌握政务信息系统的安全状况。

鉴于以上问题的存在，北京市从2006年开始进行政务外网的安全监控建设工作。由北京市政务安全应急处置中心牵头，建设了“北京市政务信息安全监控预警系统”。这是一个以SOC系统为核心的安全监控与应急处置平台。整个项目共分三期进行，第一期选择了几个政务外网汇聚节点作为试点，并建立了SOC系统；二期又增加了多个政务外网汇聚节点，并把北京市最大的政务网站首都之窗网站群作为重要信息系统纳入监控范围，为后期监控所有的重要信息系统做技术储备；2010年的三期项目建设中，将所有政务外网的汇聚节点、100多个信息系统和政务网站，以及多个政务互联网接入节点作为互联网接入试点纳入监控范围，为后期监控所有的互联网接入点做好铺垫。

2011年1月初，电子政务信息安全监控预警系统（SOC系统）上线运行。截止到2011年3月底，共发现、预警并协助处置了各类安全事件94起，其中网站篡改、挂马相关的安全事件33起……

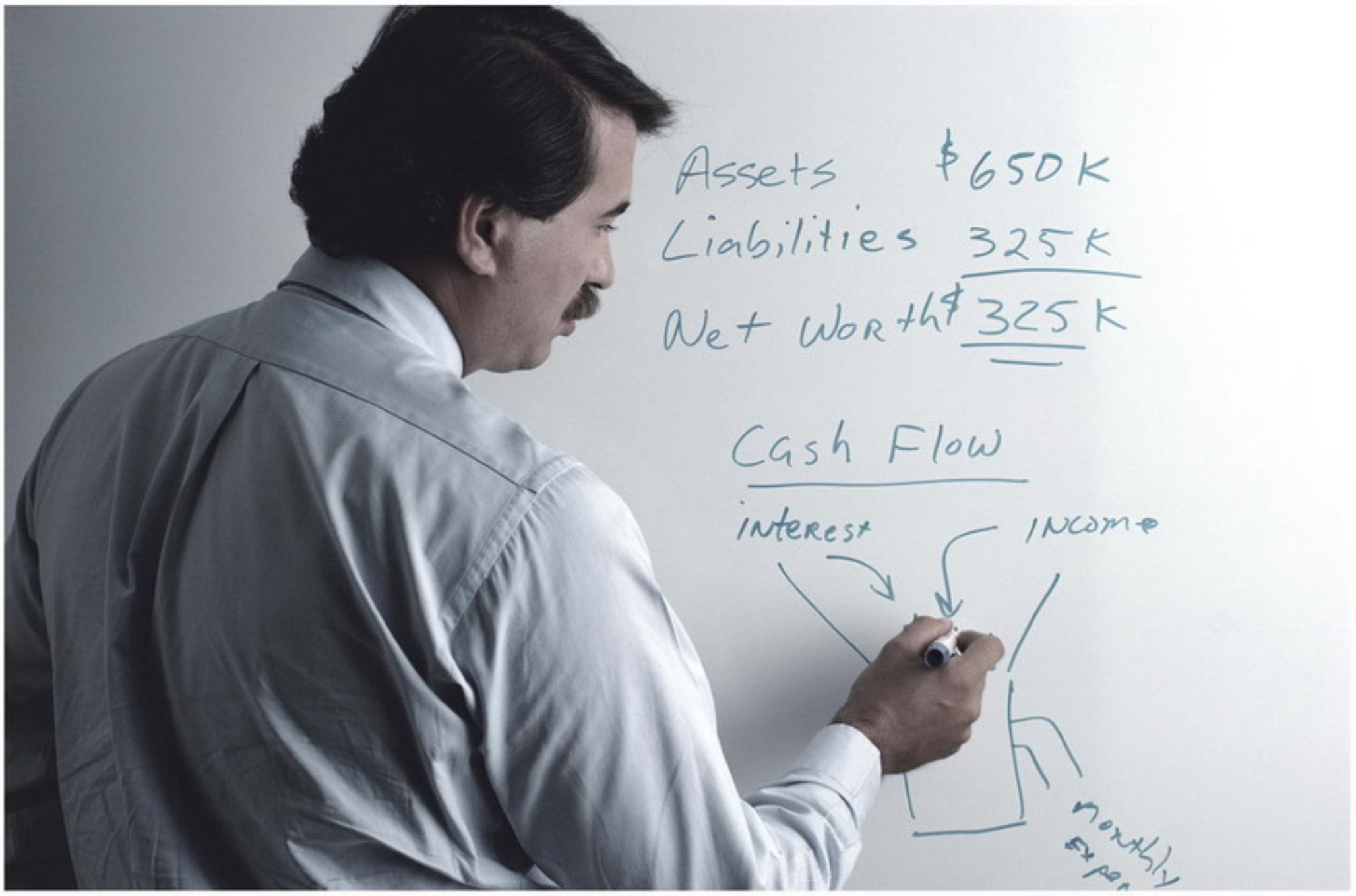
SOC系统部署不是一蹴而就

SOC的部署和业务体系以及现有信息安全架构的粘合度更高，因此相对其他来说也更加复杂，不是短期能够建设成功的，需要做大量的、足够的前期调研，那么国内电子政务行业部署SOC时需要注意什么呢？刘鹏副部长认为：“首先，SOC这种产品要成规模，如果不成规模的话，它的效益没那么大。如果节点太少的话，相对投入的效果就没那么好。其次，相比国外来说，中国用户对SOC产品的认识还存在一定差距。现在大多数单位还在做系统的加固、保护和设备部署这些事情，深层次的东西可能还没开始做，但可以看到SOC类产品在国内正处在发展期间。现在很多成功的商业机构都在做这个事情，那么我认为，至少在政府行业来说，我们希望把成功的体系纳入到电子政务建设中，打造一个高效的安全服务平台，更好的为不同的部门提供服务。”

当然，由于SOC系统的复杂性和特殊性，在挑选SOC服务商时也应考虑周全，刘鹏副部长解释道：“首先选择国产品牌是肯定的，像SOC这种产品，定制性很强，肯定不是一期能够建完的，而且后期的维护相对来说也更多更久些。因此，我们在挑选服务商方面更考虑能够长期合作的合作伙伴，当然，服务商的技术实力、公司规模也是我们考虑较多的因素。比如这次选择东软NetEye作为我们的SOC系统服务商，正是看重了它在国内软件开发行业中的突出技术实力和经验。”

在采访的最后刘鹏副部长提到，部署了SOC系统之后，北京市政务信息安全应急处置中心从日常复杂而繁琐的监控管理工作中解放出来，安全运维管理平台(SOC)通过统一的平台集中管理整个网

案例研究



络中的安全信息，对安全事件进行实时监视和事件关联、深入调查、报告、通知，并提供其他安全管理功能，实现了在整个网络范围内所有节点的统一管理、控制、预警，并及时给予合理化建议。

记者手记

之前更多的将 SOC 看做一个产品，其实 SOC 更偏向为整体的解决方案，主要是通过与其它安全产品协同合作，结合安全策略、安全运维等管理组织体系，及时发现网络中的安全问题、安全隐患，并提供预警和响应，是安全风险的处理和监控过程中的一种更为有效的智能化运维手段，而此次北京市政务外网安全运维管理平台系统的成功搭建和运作，确实为其他省市的电子政务信息安全管理提供了很好的示范，和诸多可以借鉴的宝贵经验。