达州市商业银行信息安全风险评估服务

“ 新系统刚上线，现在还不能给出确定的防护数据。通过这次评估，我们最大的收获是提升了信息安全的响应速度，以及信息安全风险管控意识。” 达州市商业银行（以下简称达州商行）现在正根据东软提供的信息安全评估报告，对自己在信息安全方面的问题进行整改。达州商行副行长杨廷军表示，“ 东软为我们将评估过程中暴露出的问题进行了风险分级，指出哪些是必须马上解决的，哪些是可以稍后解决的。”

一场信息安全教育

2009 年，达州商行挂牌开业。在新系统上线前，达州商行用的还是信用社时期使用了多年的旧系统，比较落后。根据《商业银行信息科技风险管理指引》、《银行业金融机构重要信息系统投产及变更管理办法》等文件的相关要求，达州商行在更新系统前，必须邀请第三方公司对达州商行的信息安全状况进行评估。在不到一个月的评估工作中，东软作为此次安全评估服务的提供商，对达州商行的管理制度、网络环境、系统环境和安全策略等进行了梳理和攻击性测试，并且给出了安全评估报告和整改意见。

东软的信息安全风险评估服务采用目前权威的 ISO 27001、GB/T 20984-2007 信息安全风险评估规范（中国国家标准）以及国家信息安全等级保护指南等安全标准作为风险评估的准则，在评估对象已有安全措施的基础上，对外网业务服务进行渗透测试和扫描，并对网络日志进行审计，帮助用户了解客观真实的自身网络系统安全现状，发现相关漏洞与脆弱点，给出整改建议和系统层面加固方案。

东软通过攻击性测试，发现了达州商行网络安全方面存在的一些漏洞，东软的安全专家通过模拟黑客的攻击行为，对达州商行的网络进行了非破坏性的入侵测试，发现达州商行原来的网络安全密码略显简单，容易被黑客攻破。现在，达州商行已经设置了相对复杂的密码，难以被外界破译。

信息安全的防范不是一成不变的，需要随着网络环境的变化不断完善和细化。目前，由于人员缺乏，技术实力较弱，我国城市商业银行的 IT 系统主要靠外包，包括财务等各种系统的研发，都需要外包给 IT 厂商。这就给银行的网络系统造成了一定的安全隐患。因此，加强对外包服务提供商的管理，提升银行自身的抗风险能力和风险策略管理能力，是城市商业银行不可忽视的问题。

评估过程中，东软认为达州商行在外包合同中的一些法律关系和法律责任描述得不是很清晰，不够具体，过于原则化。东软建议用户根据中国银监会的要求，加强外包管理，进一步明确外包双方的法律责任，与外包厂商签订保密协议，做好风险把关。

城市商业银行的信息安全问题，不仅表现在信息安全防护能力相对较弱，而且表现在信息安全部门的投入少、管理欠缺，更主要的是管理者的信息安全防护意识不强，各个部门的功能不完善，导致很多风险管理的责任都由技术部门分管，缺乏监督机制。

通过评估，东软发现达州商行最主要的安全隐患并非 IT 系统的老化，而是缺乏统一规划的安全防范策略，管理部门的安全防护意识薄弱，在系统操作管理、机房软硬件管理和银行的科技风险管理等方面存在一定不足，管理的组织架构也需要调整和改进。东软的评估结果提出达州商行的管理层应有专人负责风险管控工作，明确职责并且建立监督机制。

对达州商行而言，东软安全评估的意义不仅是指出了银行在安全方面存在的漏洞，更是对全行进行了一场信息安全教育。

专业赢得尊重

达州商行信息安全评估项目有四家公司投标，通过对递交的投标材料进行分析，对其以往案例进行调查，了解客户的评价，达州商行最终选择了东软。之所以选中东软，用户一是看重东软的技术力量和认证资质，二是觉得东软的技术专家很专业。

达州商行希望能跟东软建立长期的合作关系。“ 东软的安全评估反映出了城市商业银行在安全方面的核心问题，指出了症结所在，对我们今后的工作帮助非常大 ”，用户感慨道。

东软的专业，一方面体现在反应迅速，服务态度好，另一方面是因为东软的安全专家坚持以信息安全保障为最高目标，不为外界所干扰。达州商行谈到：“ 尽管存在安全漏洞，但未必都因此出现了问题，所以技术部门对信息安全的重视程度不高，当东软提出整改意见时，他们认为不一定非要这样做。但是东软称信息安全具有突发性，不能掉以轻心，所以比较坚持。”

另外，出于银行管理和运营等方面的综合考虑，对于一些安全问题，达州商行认为不适宜揭露。但东软认为，既然是做安全评估，就要把能够发现的问题全部揭示出来，并给出合理的建议。对不适宜披露的部分，东软也尊重银行的意见，只给出意见，不进行披露。正是这种专业的态度，让达州商行对东软的工作非常认可。

授人以鱼不如授人以渔

与国有银行相比，地方城市商业银行的技术部门实力较弱，资金投入少，并且缺乏连续性投入。因此，城市商业银行往往并不具有信息安全方面的高端技术和研发能力，技术部门工作人员人数少、技术水平有限。

“ 授人以鱼，不如授人以渔。” 城市商业银行需要的不仅仅是 IT 外包服务，更是提升自身的 IT 运维能力，提升银行科技人员的技术水平。因此，对工作人员进行信息安全方面的业务培训，对于城市商业银行的风险管理来说必不可少。

据了解，东软拥有 CISP 国家级信息安全专业认证培训机构最高级资质，以及近二十名的 CISP 认证工程师和多名资深培训讲师。目前东软提供一系列面向组织内管理者以及技术人员的个性化的培训方案，并且在大连、成都、南海、沈阳等地建立了培训基地。

目前，达州商行正在就技术人员培训等方面的合作与东软进行沟通，希望东软能够提供信息安全技术和策略方面的培训，并且 “ 在网络环境发生变化，网络技术不断提升的过程中提供相关信息，使达州商行的 IT 系统管理人员增强鉴别能力，不再盲从 ”，将达州商行的 IT 系统管理员也培养成网络安全专家。