

2016年高校网络信息安全学术年会

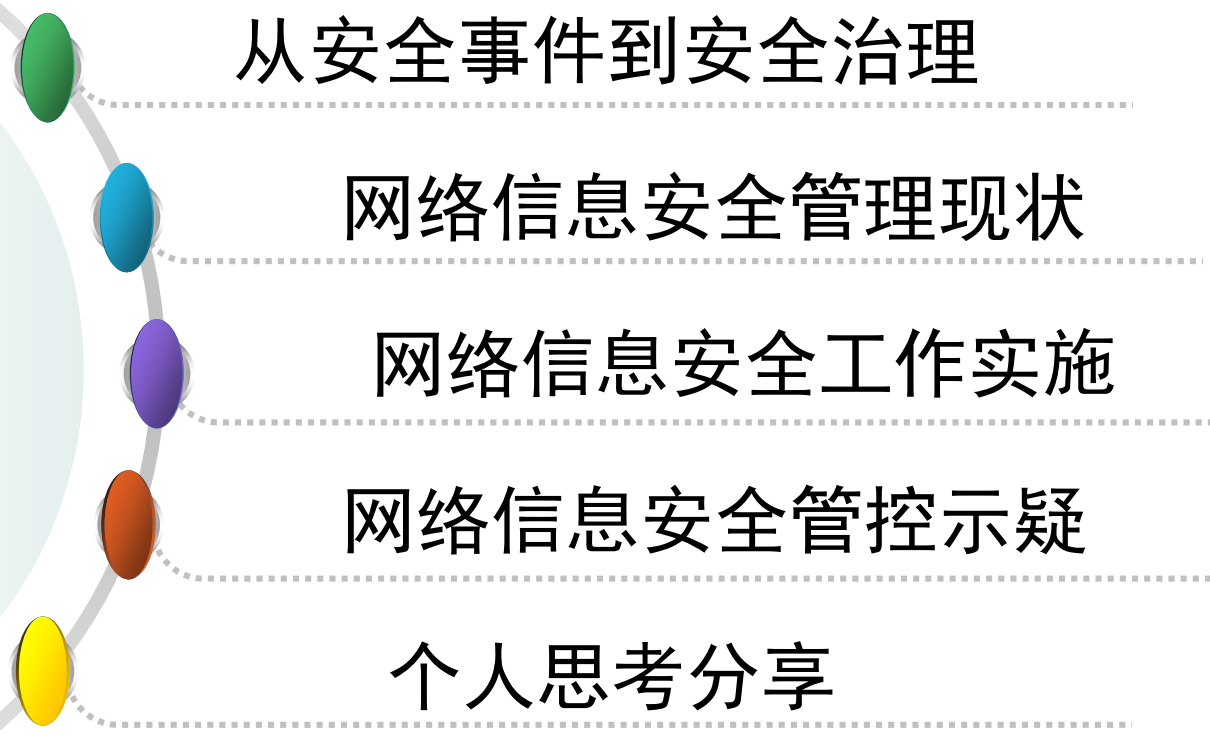
从事件响应到安全治理

——高校信息安全管理水平提升之路

东北大学信息技术研究院（网络中心）王宇

2016年12月9日

汇报提纲



从安全事件到安全治理

网络信息安全管理现状

网络信息安全工作实施

网络信息安全管理管控示疑

个人思考分享



从安全事件到安全治理



从安全事件到安全治理

- 核心理念：在较充分的技术和心态准备基础上，把握安全事件带来的机遇，推动和促成信息安全管理的实质提升
- 基础条件：正能量，积极主动，乐于沟通与“挖坑”，关注结果与心态管控
- 努力实现信息安全管理跃升
 - 事件响应——被动；权责划分模糊，承担实际责任；
 - 安全治理——主动；主动承担部分责任，实现责任分担。



网络信息安全管理现状



网络信息安全管理现状

政策背景



组织架构



制度建设



工作进展



□ 国家：《中华人民共和国网络安全法》

- 2017年6月1日起施行
- 坚持网络安全与信息化发展并重（第三条）
- 实行网络安全等级保护制度：确定责任人，做好防范措施（第二十一条）
- 实行网络实名制（第二十四条）
- 做好网络安全应急预案（第二十五条）
- 明确关键信息基础设施的运行安全（第二节）
- 发生网络安全事件要做预警、通报和控制风险



□ 教育部

■ 文件、通知

- 教育部办公厅关于开展教育系统信息安全等级保护工作专项检查的通知, 2010
- 教育部关于加强教育行业网络与信息安全工作的指导意见, 2014
- 教育部办公厅关于印发《信息技术安全事件报告与处置流程（试行）》的通知, 2014
- 教育部关于进一步加强直属高校直属单位信息技术安全工作的通知, 2015
- 教育部办公厅关于组织开展部属单位信息安全等级保护工作的通知, 2015
- 教育部办公厅关于做好重要时期信息技术安全工作的通知, 2016
- 教育部办公厅关于启动信息系统安全监测的通知, 2016
- 教育部办公厅关于印发《配合做好公安机关网络安全执法检查工作的工作方案》的通知, 2016
- 教育部办公厅关于开展关键信息基础设施安全检查, 2016



□ 教育部（续）

■ 重要时期安全保障

- 2008年北京奥运会、高招、六四、93胜利阅兵、G20等

■ 各类安全检查与信息上报

- 重要信息系统和门户网站安全专项检查自查，2013
- 教育网络安全检查、教育行业网络安全信息系统和网站情况调查、教育行业网络安全管理工作自评，2014，2015
- 关于开展国家级重点信息系统和重点网站安全检查工作的通知，2015

■ 直属培训

- 教育部“2015年度教育行业信息技术安全专题培训班”，2015

■ 情况通报

- 教育部办公厅关于北京邮电大学网络安全事件的通报，2015
- 教育网站与信息系统安全监测周报



□ 东北大学

■ 文件

- 关于加强各类网站内容发布和管理的通知，2015
- 东北大学关于加强网络与信息安全工作的指导意见，2015
- 关于成立东北大学网络安全管理与信息化建设工作领导小组的通知，2015
- 关于成立东北大学网络安全专家委员会的通知，2016
- 关于加强网站和信息系统安全管理工作的通知，2016

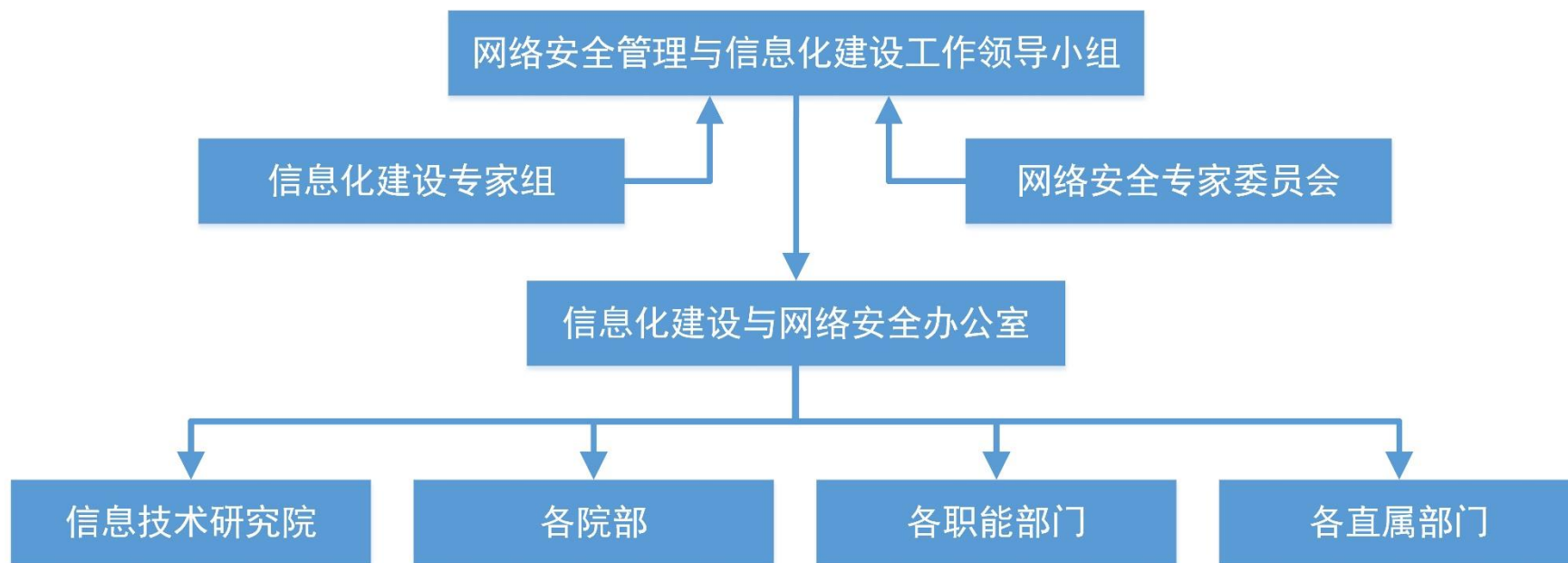
■ 上报各类安全措施和经验

- 平安校园、反恐、全运会保障、维护稳定

■ 安全协查

- 网安、安全局、保密局





□ 网络信息安全管理与信息化建设工作领导小组

	人员组成
组长	书记，校长
副组长	主管学生管理的副书记 主管安全和保密的副书记 主管信息化的副校长
成员	主要业务部处的一把手， 网络中心历任和现任主要领导，等
设办公室，及主任	



□ 信息化建设专家组

- 校内信息学科专家、网络中心历任和现任主要领导、网络中心技术骨干，等

□ 网络安全专家委员会

	人员组成
主任	主管信息化的副校长
副主任	所在地公安系统领导
成员	校内网络信息安全学科专家，所在地市网安，网络中心历任和现任主要领导，等



- 学校加强网络安全管控相关文件
 - 东北大学关于加强网络与信息安全工作的指导意见，2015
 - 关于加强网站和信息系统安全管理工作的通知，2016
- 学校组织机构调整及相关文件
 - 关于成立东北大学网络安全管理与信息化建设工作领导小组的通知，2015
 - 关于成立东北大学网络安全专家委员会的通知，2016
- 网络信息安全相关管理制度
 - 域名管理，对外信息发布（包括学校主页）管理，信息化建设项目统筹管理，虚拟主机统筹管理等



网络信息安全管理现状

工作进展

- 梳理校内域名、信息系统，明确使用部门，确定责任部门
 - 基于DNS记录梳理和清理学校二级域名
 - 规范域名资源申请
 - 鼓励域名自主合并

The image shows a screenshot of the Northeast University Network Center & IT Service (ITS) website and a 'Domain Management Registration Form'.

Website Screenshot:

- URL: <http://network.neu.edu.cn/>
- Page Title: 东北大学网络中心 & 东北大学IT服务 (ITS)
- Navigation: 网站首页, 中心概况, 建设成果与规划, 校园网络IT服务, 网络资源, 技术支持, 现行政
- Quick Links: 校园网络IT服务门户
- Calendar: 2016年十二月
- Domain Management Section: 域名管理
- Form Fields: 域名范围, 纸质备案表, 域名申请, 域名删除, 备案信息更新都须填写《
- Footer: 更新时间: 2015年12月30日, 合计107个

Domain Management Registration Form:

东北大学域名管理登记备案表			
域名:	psyn.neu.edu.cn 202.118.17.212		
域名使用单位名称:	心理健康教育中心		
隶属二级单位名称:	学生指导服务中心		
域名用途分类:	<input type="checkbox"/> 网站 <input type="checkbox"/> 业务系统 <input type="checkbox"/> 电子邮件域 <input type="checkbox"/>		
域名用途说明:	心理健康教育宣传网站		
登记备案事项:	<input type="checkbox"/> 继续使用 <input type="checkbox"/> 停用		
域名管理员:	姓名:	工号:	09489
职务:	心理健康教育中心工作人员	办公电话:	81101-2
手机:	13166776965		
电子邮箱/QQ:	61012671@qq.com 61012671		
负责人(签字):	公室:		
年 月 日			



- 以安全应急响应为抓手，促使职能部门和学院部处提高网络安全意识
 - 技术部门与信网办沟通确定安全应急响应操作流程，涉及安全事件、安全漏洞
 - 强化安全应急响应的职责归属，遇到问题第一事件处置，通知责任部门整改和反馈
 - 获取和处置学校相关网络安全事件2016年度累计46次，并提供信息安全支持工作20次

12. 网络信息安全处置

- 因网络信息安全事件或漏洞处置后的校内IP地址，整改后申请恢复互联网访问：
 - 申请：根据安全事件或漏洞情况及整改工作的实际情况，填写《东北大学IT服务相关情况说明》并加盖所属二级部门公章，经学校网络信息安全管理部审批后，交到网络中心人工服务窗口办理。
 - 使用：



- 以等级保护建设为契机，推动整体安全加固专项建设
 - 切实推进和实施信息系统等级保护建设
 - 以等级保护建设为抓手，实施“东北大学网络安全防范工程”
 - 统筹推进信息系统定级、备案、测评、整改、整体安全管控



□ 加强网络信息安全相关信息的宣传推广工作

■ 开展“辽宁省网络安全宣传周”活动

□ 举办网络安全讲座

□ 举办网络安全知识竞赛

■ 在线发布和推广安全资料

□ 国家网络安全宣传周宣传画

□ 网络信息安全科普

■ 网络信息世界的你，该知道这些事

□ 参见：<http://network.neu.edu.cn/>



网络信息安全工作实施



网络信息安全工作实施

资源统筹管理



等级保护开展



安全事件响应



安全团队建设



- 信息化建设相关项目的统筹管理
 - 归口单位管理
 - 年度专家小组评审
 - 按阶段推进项目实施
- 基础IT环境的统筹管理
 - 技术部门提供托管主机、虚拟主机服务
 - 80%以上业务系统实现集中托管管理
 - 网络信息安全防护统一管控



- 信息系统等级保护工作开始于2010年
 - 教育部办公厅关于开展教育系统信息安全等级保护工作专项检查的通知，2010
 - 2010—2013年，校内动员讲解、信息系统汇总与梳理、相关工作小组决策、上报省教育厅和与公安系统沟通
 - 对学校网络信息安全工作推进的帮助有限



- 信息系统等级保护工作加快推进在2015年
 - 教育部办公厅关于组织开展部属单位信息安全等级保护工作的通知，2015
 - 参照《教育行业信息系统安全等级保护定级工作指南（试行）》
 - 2015-2016年，组建机构、出台制度、明确责任，并推动和实施定级备案测评及整改项目
 - 各项工作由东北大学网络安全专家委员会进行评审



信息系统安全等级保护备案情况

等级	信息系统列表	
	总数	列表
三级	12	图书馆、团委、网络中心、校办、宣传部、学工处、学生指导服务中心、研究生院、资产处、科技处、教务处、计财处综合平台
二级	22	人事处、档案馆、继续教育学院、创新创业学院综合平台，所有学院部综合平台



- 建立技术部门与管理部门协调的安全事件响应
 - 安全漏洞和安全事件的信息获取
 - 安全事件判定
 - 安全事件处置
 - 主机层面关闭
 - 路由层面关闭
 - 校园网出口关闭
 - 情况告知
 - 使用部门（责任部门）整改
 - 提交整改报告
 - 恢复服务



- 以“2016年寒假网络信息安全工作计划”为例
 - 安全事件分级
 - 安全事件，学校相关主机或服务发生页面被篡改、数据泄漏、网站被挂木马、主机被入侵等状况。
 - 政治类，涉及反党、反国家、反人类等相关信息，如反共黑客组织对某学院的攻击；
 - 非政治类，不涉及政治相关内容。
 - 安全隐患，通过各种途径获知的学校相关主机或服务存在可被黑客利用的漏洞，即存在被攻击风险，但是尚未被黑客利用。



- 以“2016年寒假网络信息安全工作计划”为例
 - 安全情报信息来源
 - 补天、乌云、漏洞盒子等主流漏洞平台获取的学校相关的漏洞信息
 - 通过电子邮件（security@mail.neu.edu.cn）或网站浏览获取漏洞信息。
 - 中国高等教育学会教育信息化分会网络信息安全工作组
 - 在线漏洞发现与检测平台（<http://202.112.26.107/>），网络信息安全工作组信息交流微信群和QQ群（224539320），国家信息安全漏洞共享平台（<http://www.cnvd.org.cn/>）教育行业待验证漏洞信息。
 - CERNET应急响应组
 - 依托清华大学的CERNET应急响应组会第一时间电话、QQ和邮件告知我校相关的漏洞信息。
 - 网络中心自有漏洞扫描设备、360免费企业平台或人工扫描获取。
 - 教育部科技司和教育管理信息中心、辽宁省教育厅信息化处等信息安全事件通报。



□ 以“2016年寒假网络信息安全工作计划”为例

■ 处置手段

- 断开网络服务（包括面向互联网和校园网内）：IP地址封锁系统，网络中心人员在登录后操作，主要供值班人员第一时间进行处置；在该系统中处置后，访问相应的网站或信息系统将跳转到指定页面，在页面中提示具体的封禁原因，并记录详细操作日志。
- 断开互联网访问（校内可以访问）：主要是两种方式，一种是在出口计费系统后台，封锁对应透明IP地址账号；一种是在出口网络设备上，增加安全策略。实际处置过程中，主要通过计费系统操作。
- 关闭物理主机：需要网络中心值班人员手工操作。
- 关闭虚拟主机：在线登录虚拟主机管理平台操作。



- 以“2016年寒假网络信息安全工作计划”为例
 - 安全事件响应、处置、通知和监督整改
 - 安全事件：政治类
 - 第一时间（从安全事件信息获取到处置力争不超过30分钟）从网络中心能力范围断开网站和信息系统的互联网访问，主机托管在网络中心的第一时间关闭相关的关闭物理或虚拟主机，第一时间汇报给信网办（电话）；
 - 网络中心安全、网络和信息团队提供后续技术支撑；
 - 相关部门报送整改报告（学院部处主要领导签字，并加盖处级单位公章）到信网办，网络中心根据实际情况恢复互联网访问。



□ 以“2016年寒假网络信息安全工作计划”为例

■ 安全事件响应、处置、通知和监督整改

□ 安全事件：非政治类

- 第一时间（从安全事件信息获取到处置力争不超过6小时）从网络中心能力范围断开网站和信息系统的互联网访问，第一时间汇报给信网办（发送电子邮件或手机短信）；
- 根据网络中心托管联系人信息或查找的校内联系方式，告知相关部处人员进行处置，尽可能通知到单位领导加快整改；
- 网络中心安全、网络和信息团队提供后续技术支撑；
- 相关部门报送整改报告（学院部处主要领导签字，并加盖处级单位公章）到信网办，网络中心根据实际情况恢复互联网访问。



□ 以“2016年寒假网络信息安全工作计划”为例

■ 安全事件响应、处置、通知和监督整改

□ 安全隐患

- 对于面向互联网提供信息发布功能的网站或系统，第一时间（从安全隐患信息获取到确认不超过24小时）确认安全隐患是否属实，确认属实后第一时间（从安全隐患确认到处置力争不超过6小时）从网络中心能力范围断开网站和信息系统的互联网访问，防止漏洞被利用出现安全事件，第一时间汇报给信网办（发送电子邮件或手机短信）；
- 根据网络中心托管联系人信息或查找的校内联系方式，告知相关部处人员进行处置，尽可能通知到单位领导加快整改；
- 网络中心安全、网络和信息团队提供后续技术支撑；
- 对于断开互联网访问的系统，相关部门报送整改报告（学院部处主要领导签字，并加盖处级单位公章）到信网办，网络中心根据实际情况恢复互联网访问；
- 对于没有面向互联网提供信息发布功能的网站或系统，主要履行告知义务，网络中心安全、网络和信息团队提供技术支持。



- 建立跨网络、运维、开发的与学生团队合作的网络信息安全团队
 - 技术部门内跨网络、运维、开发
 - 发现、培育、支持校内学生团队
 - 开展与东北大学绿盟科技俱乐部学生团队合作，探索网络中心运维老师与学生团队的联合成长模式，组队参加2016年“安恒杯”高校安全运维挑战赛获得全国二等奖及东北地区一等奖



网络信息安全工作实施

安全团队建设





网络信息安全管理控示疑



网络信息安全管控示疑

□ 网络信息安全工作推进的动力

- 长期准备：投入、技术、人员、制度……
- 借安全事件契机和政策环境
 - “正能量”看待网络信息安全工作
 - 关注和跟进安全技术发展
 - 做好准备，把握机会
 - 正确看待安全事件
 - 应该更关注数据安全
 - 应该将安全事件成为变革推手



网络信息安全管控示疑

□ 信息技术部门发挥什么作用

■ 技术支持

■ 非安全责任

□ 网络信息安全领域日新月异，攻守不平衡，没有绝对的安全

□ 使用单位、建设单位，应该承担更大责任

■ 责任要清晰

□ 需要制度明确

□ 需要顶层设计



网络信息安全管控示疑

□ 技术团队如何组建与培育

■ 立足已有技术团队

- 网络、运维、开发人员

- 信息安全人才培养周期长，就业形势好，招聘困难

■ 与学生团队合作

- 学生有热情

- 对学生毕业就业也有帮助

- 学生与老师知识和经验互补明显

■ 动手与理论相结合

- CTF比赛



网络信息安全管控示疑

- 业务部门等安全漏洞和事件处置缺少能力
 - 在政策背景下，以责任为先
 - 技术部门提供必要支持
 - 技术部门可以统一采购第三方安全服务
 - 技术部门不能缺位，应以业务为主，这才是网络和信息服务的价值体现



网络信息安全管控示疑

- 网络信息安全组织协调是否顺畅
 - 初期存在矛盾
 - 后期处置过程关注业务，适度管控，主动合作，协调推进有所改善
 - 长期良性发展还受到技术团队的规模、能力、专职程度等影响
 - 有待建设契约式的业务部门与技术部门间的合作模式



个人思考分享



个人思考分享

□ 高校IT资源统筹管控

- 渐进过程，从掌握的资源入手
 - 管理网络出口，管理机房环境，管理数据交换……
- 站群-整合简化系统入口，降低整体风险
- 制度现行，明确提供IT资源的技术部门与使用IT资源的业务部门间的责权利



个人思考分享

□ 网络信息安全情报利用

- 校内师生、高校间、安全厂商、社会组织等
- 补天、漏洞盒子……
- 主动参与到安全信息交流、信息分享、安全竞赛等活动
- 现阶段建议提供一定的安全信息回报
- 第一时间分析和处置安全情报相关安全事件



个人思考分享

□ 转换网络信息安全工作思路

- 与信息化建设结合，充分利用政策环境推动良性发展理念实现
- 变被动为主动
- 可以成为统筹推进学校信息化建设的契机
- 不怕事，因为怕也躲不了
- 认真总结，珍惜每次安全事件整改过程



个人思考分享

□ 重视安全服务的采购和实施

- 咨询、防护、应急响应、安全评估等，而不是以设备为主
- 要去了解专业安全公司能提供的解决方案，对各类安全设备的数据分析和先期预警才有助于提高应急响应响应速度
- 等保测评和整改，要落到实处，至少成为学习的过程



附录

- 中国高等教育学会-教育信息化分会-网络信息安全工作组
 - <http://sec.edu-info.edu.cn/>
 - 安全百科: <http://secwiki.neu.edu.cn/wiki/>
 - 漏洞信息库: <https://loudong.sjtu.edu.cn/>
 - IPDB 基础数据库: <http://ipdb.sec.edu-info.edu.cn/ipdb>
 - Vul Tracker: <http://vul.sec.edu-info.edu.cn/>
 - 微信群: 网络信息安全工作组信息交流群, 500人
 - 微信公众号: eduinfosec 安全工作组
 - QQ群: 网络信息安全交流群, 群号224539320, 403人
 - 申请加入, 请注明所在学校名称



中国高等教育学会教育信息化分会
网络信息安全工作组
Education Information Security Working Group



附录



- 王宇
- 东北大学信息技术研究院（网络中心）院长助理
- 目前主要负责东北大学智慧校园相关规划、建设与运维工作，以及配合网络信息安全应急响应工作
- 电子邮件: wangy@mail.neu.edu.cn
- QQ: 10662877
- 微信: wangyuneu
- 个人主页: <http://faculty.neu.edu.cn/wangy/>
- 办公电话: 024-83684926



谢 谢！

