大连理工大学
DALIAN UNIVERSITY OF TECHNOLOGY

网络信息技术安全工作管理实践

大连理工大学 张巍

2017年9月26日 无锡

汇报提纲 CONTENTS

汇报提纲 CONTENTS

没有信息化，就没有现代化

没有网络安全，就没有国家安全

我国第一部全面规范网络空间安全管理方面问题的基础性法律

网络安全为人民　网络安全靠人民

高校网络信息安全面临的问题

- 攻击全方位：攻防极不对称，防不胜防
- 法律要求高：网络安全法，落实法律问责
- 重视程度不够：工作落实不够
- 专业化程度低：极度缺乏专业人才
- 师生参与度低：勒索病毒、“肉鸡”、僵尸网络

高校网络信息安全事件主要表现

网络系统安全

- 网络系统安全
- 漏洞、黑客、
- 病毒、勒索
- 非授权访问
- 拒绝服务攻击
- ……

网站安全

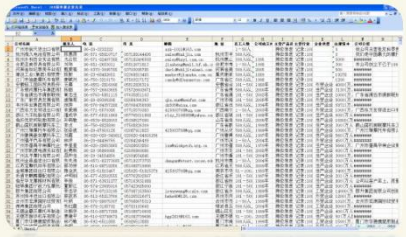
- 篡改
- 暗链
- 非法指向
- 恶意注册
- 内容
- ……

数据安全

- 非法采集
- 非法窃取
- 非法使用
- 泄露篡改
- 工作疏忽
- ……

个人安全

- 个人PC防护
- 补丁升级
- 弱密码
- 钓鱼邮件
- 恶意网站
- ……



高校信息化部门的困境

1. 工作压力山大

工作自身的压力、上级监管的压力、法律责任的压力
（重大活动、敏感时期、节假日、大规模病毒爆发等）

2. 责权利不对等

有限的权利、经费、人力，无限的责任
业务部门出现安全问题，信息化部门怎么也脱不了干系

3. 岗位角色混淆

保镖？消防员？警察？法官？—全能型
信息化部门到底该做什么？

信息化部门

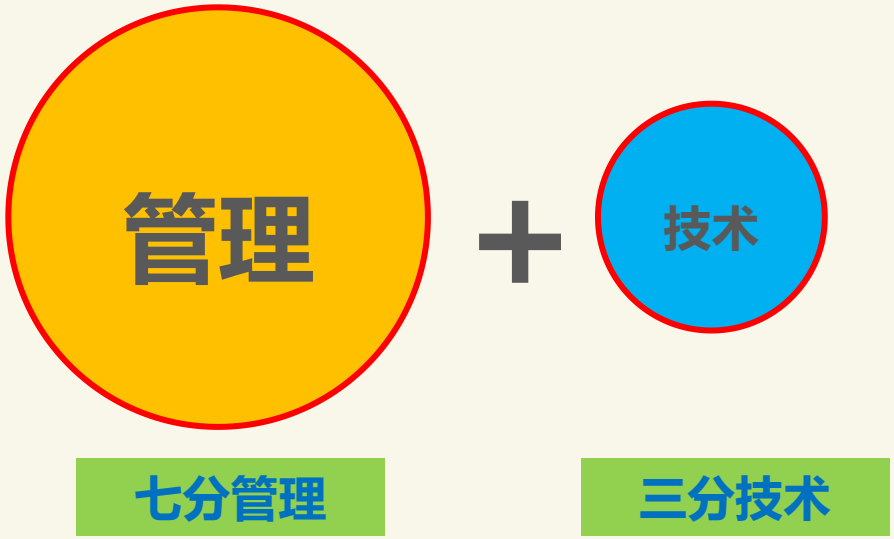
业务部门

4. 职能定位不清

谁主管谁负责、谁运维谁负责、谁使用谁负责？
真发生安全事件业务部门躲的远远

我们对网络信息安全工作的认识

- 漏洞和安全威胁永远会客观存在；
- 道高一尺，魔高一丈，绞尽心思，防不胜防
- 没有一劳永逸的解决方案
- 没有一个厂商可以解决所有的问题
- 技术解决不了的问题管理解决
- 管理解决不了的问题技术解决

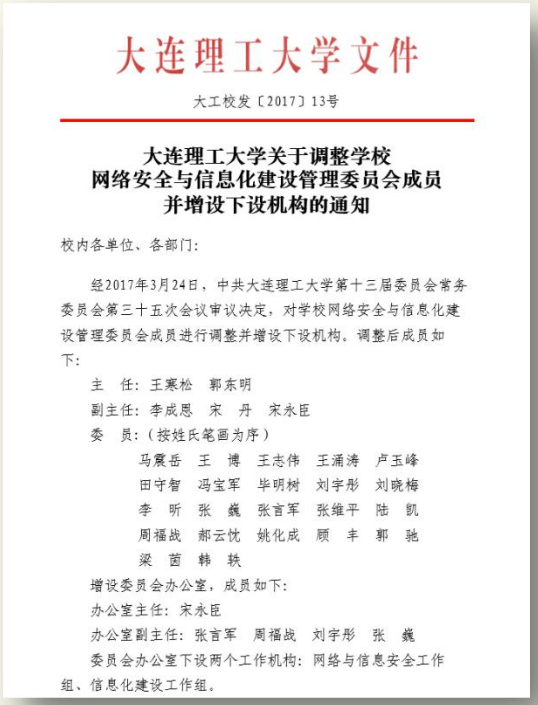


网络安全的工作的实质是**风险管理**，通过**管理手段**和**技术手段**降低安全风险

汇报提纲 CONTENTS

1. 组织保障

网络信息安全工作必须自上而下有一套完整的组织架构和人员队伍，这样才能在规则制定、安全防范、问题处理等各环节切实加强网络信息安全工作。



大连理工大学文件

大工校发〔2017〕13号

大连理工大学关于调整学校网络安全与信息化建设管理委员会成员并增设下设机构的通知

校内各单位、各部门：

经2017年3月24日，中共大连理工大学第十三届委员会常务委员会第三十五次会议审议决定，对学校网络安全与信息化建设管理委员会成员进行调整并增设下设机构。调整后成员如下：

主　任：王寒松　郭东明

副主任：李成恩　宋　丹　宋永臣

委　员：（按姓氏笔画为序）

马震岳　王　博　王志伟　王涌涛　卢玉峰

田守智　冯宝军　毕明树　刘宇彤　刘晓梅

李　昕　张　巍　张言军　张维平　陆　凯

周福战　郝云忱　姚化成　顾　丰　郭　驰

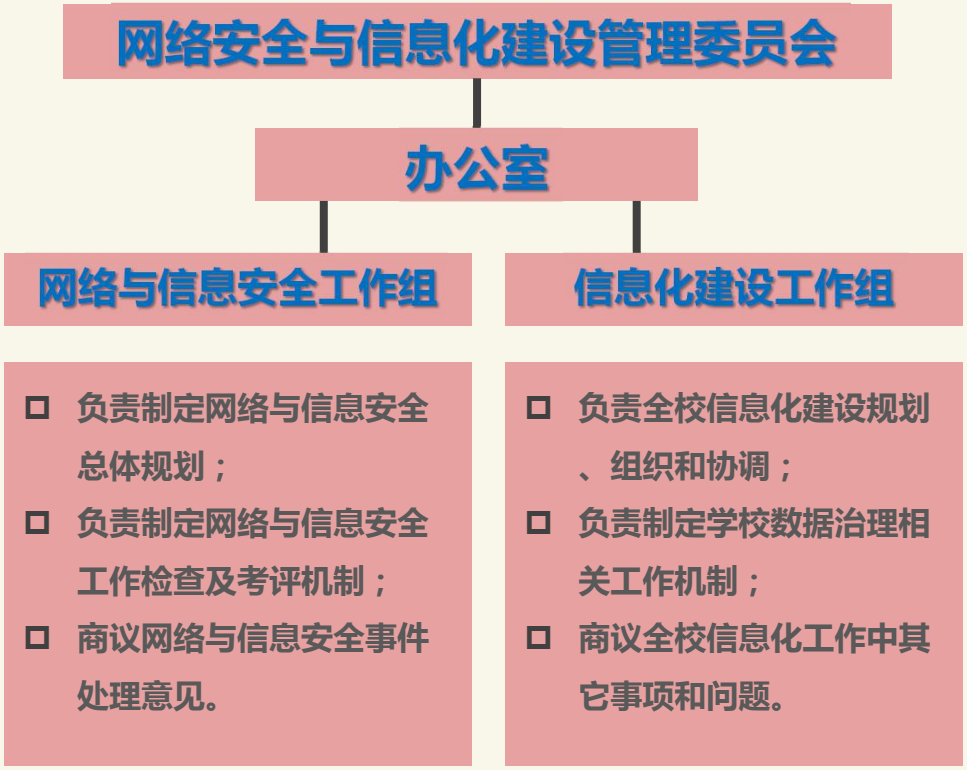
梁　茵　韩　轶

增设委员会办公室，成员如下：

办公室主任：宋永臣

办公室副主任：张言军　周福战　刘宇彤　张　巍

委员会办公室下设两个工作机构：网络与信息安全工作组、信息化建设工作组。



2. 制度保障

推动网络信息安全工作必须制度先行

为什么建立制度？

- 规范流程
- 明确责任
- 约束别人
- 约束自己
- 满足内控
- 推动工作

- 大连理工大学信息技术安全事件处置预案
- 大连理工大学网络信息技术安全管理办法
- 大连理工大学信息化数据资源管理办法
- 大连理工大学校内网站建设管理办法
- 大连理工大学信息化建设管理办法
- 大连理工大学中文主页建设管理办法
- 大连理工大学电子邮箱管理办法
- 大连理工大学域名管理办法
- 大连理工大学校园网云空间服务管理办法
- ……

3. 管理保障

3.1 网络基础设施和信息系统管理

- 学校统一建设互联网出口，校内各单位及个人不得自行建设（**避免运营商接入**），不得私接外网出口；
- 校内信息系统的建设必须**依托于网信中心的数据中心**，使用学校域名、IP地址；
- 校内**非数据中心IP不得提供互联网服务**，特殊情况需审批，只能是用于科研需要；
- 正在实施数据中心**白名单制度**，数据中心只允许已登记的应用提供服务。
- 面向全校师生使用的校内信息系统**必须实行统一身份认证**，不允许出现多套用户认证体系，屏蔽各业务系统自带登陆地址和页面；
- 各信息化项目上线、**验收前必须通过必要的信息安全检测**；

3. 管理保障

3.1 网络基础设施和信息系统管理

- 信息化项目建设应由专业的软硬件厂商按标准软件项目管理流程建设，不允许委托个人建设（**特别不允许老师带学生建设**）；
- 信息化项目合同模板中，明确要求**承建厂商**必须负责解决项目**全生命周期内系统自身的安全问题**；
- 网络安全等级保护工作由**网信中心组织协调**，**各单位具体负责**；
- 网信中心有权对网络安全事件进行处理，直至**停止网络信息服务**、追究责任等。

3. 管理保障

3.2 网站管理

- 校内网站主要提供信息发布功能，只发布**静态网页**，各类**应用系统应与网站分离**；
- 各类网站不得设置**论坛、留言板**等互动栏目；
- 所有校内网站需统一使用学校域名（**避免“双非”网站出现**）；
- 校内网站必须依托学校**网站群系统**建设和管理，不得使用其他方式建设；
- 校内网站如在技术和管理上有特殊需求，不能部署在学校网站群系统中，网站主管单位签署**《自建网站安全承诺书》**，自行建设网站，承担网站的全部安全责任；
- 校内网站全部登记注册，不再使用时需及时**注销相关域名及服务**，不得弃管网站等

3. 管理保障

3.3 数据安全管理

- 明确数据共享的原则，即以**全面共享为根本，不共享为例外**，学校各单位可合法、合理、依规使用共享数据；
- 数据资源共享分为**普遍共享类**、**有条件共享类**、**不共享类**三种类型（后两类应有明确的政策依据）；
- 全校性业务系统必须**与公共数据平台对接**，对接以接口方式为主要途径；
- 校内共享数据只能通过公共数据平台获得，**不得重复采集**，不得在业务部门间以**离线文件**形式传递；
- 加强**数据管理和更新**，严格数据管理授权，**保留数据运维日志记录**；

3. 管理保障

3.3 数据安全管理

- 各部门有权利根据履职需要**提出信息化数据需求**，同时也**有义务提供共享数据**；
- 数据使用申请上，普遍共享类数据向网信中心申请，审批后提供；有条件共享类数据向网信中心申请，**业务主管部门审批后**确认是否提供；
- 数据使用管理上按照**“谁使用，谁负责”**的原则，做好数据全过程管理，有疑问数据提交到**数据产生部门校核修正**；
- 个人隐私数据保护方面，**所有数据采集须有明确用途**，且师生个人应**知情同意**；
- 使用数据资源应保护个人隐私，**只能用于申请的授权用途**；
- 违反数据资源办法行为要**追责**等。

4. 技术保障

4.1 实行“最小化访问”和“零信任VPN服务” 原则

- 校园网边界启用状态防火墙，默认只允许**校内向校外单向访问**，除数据中心和特殊审批的地址外均无法对校外提供服务；
- 只对校内师生提供的服务，均**不提供校外访问权限**；
- 校外访问校内资源只能通过**VPN**，大并发容量（2000个），集成下一代防火墙和攻击防护，只允许网页、电子邮件、即时通讯等应用；
- 校内**高风险端口访问隔离**（445等）；数据中心对校外**开放特定端口**（80、8080、443），数据中心对校内及数据中心之间**关闭特定端口**（3389、22、445、135、136、137、139）；

4. 技术保障

4.1 实行“最小化访问”和“零信任VPN服务” 原则

- 个别**非数据中心服务及非标准端口开放服务**需要经过**审批**，所有数据中心的应用需要经过安全评估后才允许上线（内部评测、外部评测）；
- **数据中心云平台进行统一的安全防护**（WAF、无代理防病毒、虚拟补丁、包过滤防火墙、IPS）；
- 建立**内部、外部运维审计制度**，对校内校外运维工作都进行审计，内部关键业务逐步强制通过**内部运维堡垒机运维管理**，外部服务商**必须通过外部运维堡垒机**以口令+二次认证的方式登录使用；
- 在重大事件、敏感时期等的应急响应技术部分**外包给专业公司承担**等。

4. 技术保障

4.2 网站安全技术防范

- 所有网站必须在**网站群平台搭建**，**静态页面发布**，限制动态组件，**开启防篡改功能**；
- 在服务器配置上，开发、管理、发布**三套独立服务器**分开，开发、管理服务器严格限制访问，发布服务器仅开80端口；
- 网站群实行**集群部署**，保证负载能力和可扩展性，集群分区管理（学校主页、新闻网、二级单位网站）；
- 严格**区分网站开发人员、网站管理人员权限**。开发人员有开发平台权限，临时账号（非统一身份认证），网站管理员有管理平台权限（统一身份认证）；
- **网站开发、修改原则上都在开发服务器上进行**，完成后由平台管理员导入管理服务器并发布，网站管理人员在管理服务器进行日常管理。

5. 平台保障

为解决学校信息化无序和重复建设，避免低质量建设导致的安全隐患和问题，学校有必要建设一些信息化公共平台，统一进行安全管理，满足学校各单位、师生的信息化应用需求。

- 建设**私有云平台**，将分散的资源集中管理和部署，集中进行云平台的安全防护。学校不允许各部门购买应用级服务器，规定学校所有（不含科研）信息化应用必须部署在学校云平台中。
- 私有云平台统一整合管理，统一安全管理，集中打包对内外部提供云主机服务，给用户完全的控制权限。用户通过云管理平台，可以自助申请，选择CPU核数、内存、存储以及操作系统后，平台自动为用户配置生成虚拟云主机。

5. 平台保障

- 建设**网站群集群平台**，将学校所有网站集中部署并进行分类管理。目前学校所有二级单位、学部、学院、研究所、实验室等网站已经全部部署到网站群集群中。
- 建设**教师个人主页平台**，将全校教师的科研、教学、招生和学生等信息在平台中集中展示，平台的安全由网信中心统一管理。
- 建设**会议网平台**，为学校各单位组织举办的国际国内各类会议提供一站式网站建设服务。
- 建设**调查问卷平台**，用于学校各类问卷调查、数据收集、投票评比等用途。
- 建设**校内活动网平台**，用于学校举办的各类报告会、学术讲座、论坛、各类活动的线上审批和网站集中发布，并可实现按活动类型、精品活动内容、按月、周、日查询等功能。

5. 平台保障


大连理工大学 网站群管理平台
DALIAN UNIVERSITY OF TECHNOLOGY
系统登录
模板预览
使用手册
综合门户
校内网站


大连理工大学 教师主页
首页
杰出人才
单位列表
学科列表
教师查询
关于主页
English


大连理工大学 会议网
精彩会议
期待加入

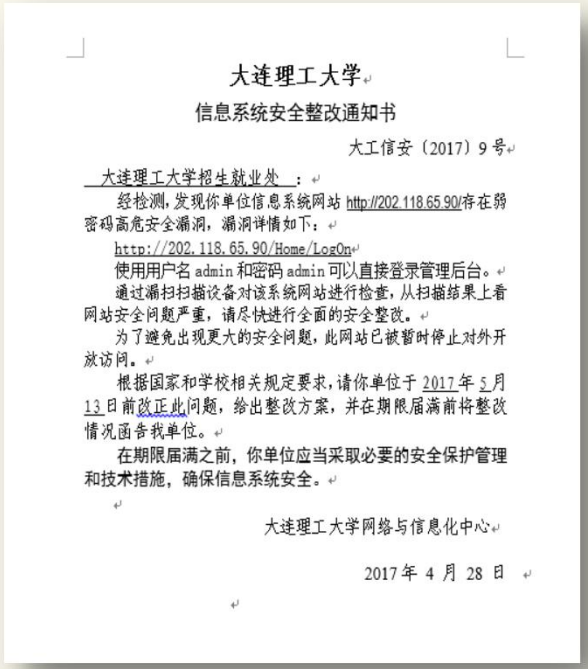

大连理工大学 综合调查问卷系统
问卷管理员入口

6. 措施保障

大连理工大学网络安全事件应急预案

- 基本原则：**预防为主、快速反应、分级负责、定期演练**
- 网络安全事件分级：由高到低：Ⅰ级（特别重大）、Ⅱ级（重大）、Ⅲ级（较大）和Ⅳ级（一般）
- **Ⅳ级由各部门自行处理**，Ⅰ级网信中心报学校网络安全工作组，其他由网信中心组织相关部门处理
- 应急处置必须及时、恰当；基本手段-**关停、限制**
- **所有安全事件均需及时报网信中心**
- 材料：整改通知书及回执、情况报告、整改报告及上级部门要求提交的材料
- 预警、重大活动保障、演练、培训

6. 措施保障



大连理工大学

信息系统安全整改通知书

大工信安（2017）9号

大连理工大学招生就业处：

经检测，发现你单位信息系统网站 http://202.118.65.90/存在弱密码高危安全漏洞，漏洞详情如下：

http://202.118.65.90/Home/LogOn

使用用户名 admin 和密码 admin 可以直接登录管理后台。

通过漏扫扫描设备对该系统网站进行检查，从扫描结果上看网站安全问题严重，请尽快进行全面的安全整改。

为了避免出现更大的安全问题，此网站已被暂时停止对外开放访问。

根据国家和学校相关规定要求，请你单位于 2017 年 5 月 13 日前改正此问题，给出整改方案，并在期限届满前将整改情况函告我单位。

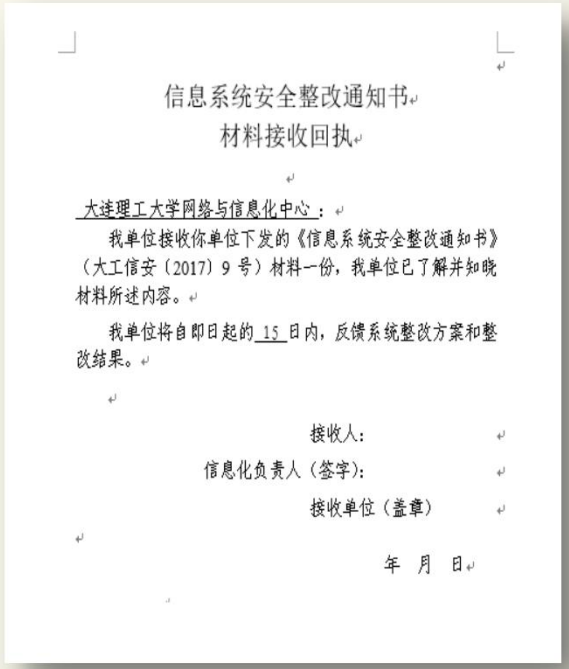
在期限届满之前，你单位应当采取必要的安全保护管理和技术措施，确保信息系统安全。

大连理工大学网络与信息化中心

2017 年 4 月 28 日

处理流程

- 第一时间停止服务
- 发出书面整改通知
- 整改回执反馈接收
- 业务部门整改
- 检测合格恢复服务



信息系统安全整改通知书

材料接收回执

大连理工大学网络与信息化中心：

我单位接收你单位下发的《信息系统安全整改通知书》（大工信安（2017）9 号）材料一份，我单位已了解并知晓材料所述内容。

我单位将自即日起的 15 日内，反馈系统整改方案和整改结果。

接收人：

信息化负责人（签字）：

接收单位（盖章）

年 月 日

汇报提纲 CONTENTS

我们现在关心的问题

- **数据安全责任重大**

  信息化是双刃剑，集中了业务和数据的同时也集中了风险和责任

  法律和伦理的地带，大数据使用与隐私保护（离校预警、学业预警、离群预警、轨迹跟踪等应用，内部使用是否合法？已经有的预警没发挥作用怎么办？）

- **完整的云战略（混合云）**

  外部公有云使用的原则（什么公有云可以用，什么数据敢放到公有云中？公有云中数据资产的所有权？）

  存在潜在的风险，风险如何管理（如何防止数据泄露，数据泄露了怎么办？数据灾难怎么恢复？）

谢谢！请批评指正！