中国传媒大学B903实验室信息系统风险评估项目实施方案

设计人员：郭韵婷、刘彦延、宋雅文、文喬、柳晓丽

# 概述

实验室信息系统是高校内常见的信息系统，主要为计算机学院各位老师和同学们提供研究平台。我们通过对此实验室的背景资料以及内部的管理系统进行了解，通过资产识别与评估，威胁识别与评估，脆弱点识别与评估，风险分析与等级划分以及安全措施的选取五个方面对实验室信息管理系统进行了风险评估。

1. 风险评估方法以及内容

本次评估采用资产识别与评估->威胁识别与评估->脆弱点识别与评估->风险分析与等级

划分以及安全措施的选取的流程顺序进行

1. 资产分析

1 资产

（1）物理资产：

实验室

计算机及网络设备：服务器两台 路由器三台 交换机两台 个人PC 10 台传输设备：光纤及双绞线若干

移动存储设备：移动硬盘 u盘

保障电子设备：中央空调 文件柜 消防设施 门锁 监控

安全保障设备：防火墙 身份验证 访问控制 考勤机

其他电子设备：打印机 投影仪

（2）云服务：

文档存储平台 ：存储、共享数据内

（包括考勤数据、监控资料）

云服务器平台 ：提供高性能实验平台

日志审计平台 ：网络日志生成、分析、报警、存储平台

（3）人员：导师一名，研究生四名

（4）信息/数据及文档：

学生及导师信息

软件源代码及文档

财务报表等

（5）服务：

网络服务 实验室内部服务器提供内部人员的专用网络，还有路由器用于外网链接，同时提供防火墙、日志审计等服务

信息服务 通过实验室网站的对外开放向外宣传实验室

注： 5 特别重要 尽量不要出现任何错误

4 很重要 允许出现可以弥补的错误

3 一般重要 可以出现一些不可弥补不影响集体利益的错误

2 可以出现暂时性地影响集体利益的错误

1 可以出现永久性地影响集体利益的错误

表一：资产统计表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 编号 | 设备名称 | 资产机密性 | 资产完整性 | 资产可用性 |
| A\_1 | 实验室 | 4 | 5 | 5 |
| A\_2 | 服务器 | 5 | 5 | 5 |
| A\_3 | 路由器 | 3 | 4 | 5 |
| A\_4 | 交换机 | 3 | 4 | 5 |
| A\_5 | PC | 4 | 4 | 5 |
| A\_6 | 双绞线及光纤 | 2 | 3 | 5 |
| A\_7 | U盘 | 4 | 4 | 4 |
| A\_8 | 移动硬盘 | 4 | 4 | 4 |
| A\_9 | 中央空调 | 2 | 2 | 4 |
| A\_10 | 文件柜 | 4 | 4 | 4 |
| A\_11 | 消防设施 | 2 | 2 | 5 |
| A\_12 | 门锁 | 2 | 5 | 5 |
| A\_13 | 防火墙 | 5 | 5 | 5 |
| A\_14 | 监控 | 3 | 4 | 4 |
| A\_15 | 考勤机 | 3 | 4 | 4 |
| A\_16 | 身份验证 | 5 | 5 | 4 |
| A\_17 | 访问控制 | 4 | 3 | 3 |
| A\_18 | 投影仪 | 2 | 2 | 3 |
| A\_19 | 打印机 | 2 | 2 | 3 |
| A\_20 | 文档存储平台 | 5 | 5 | 4 |
| A\_21 | 云服务器平台 | 4 | 5 | 5 |
| A\_22 | 日志审计平台 | 4 | 5 | 4 |
| A\_23 | 导师 | 5 | 5 | 5 |
| A\_24 | 研究生 | 4 | 4 | 4 |
| A\_25 | 学生及导师信息 | 4 | 5 | 4 |
| A\_26 | 软件源代码及文档 | 5 | 5 | 5 |
| A\_27 | 财务报表 | 3 | 5 | 3 |
| A\_28 | 网络服务 | 5 | 5 | 5 |
| A\_29 | 信息服务 | 2 | 3 | 4 |

# 威胁识别与评估

根据小组内部的讨论，通过对上述各类资产的主要安全威胁进行分析，将出现的威胁分为自然威胁，环境威胁，系统威胁，内部人员威胁，外部人员威胁，并依据其出现的可能性大小，频率高低对各类威胁进行评估，评估结果如下：

表二：威胁识别与评估



威胁赋值标准

5—很高：威胁出现的频率很高，在大多数情况下几乎不可避免或者可以证实经常发生过

4—高：威胁出现的频率较高，在大多数情况下很有可能会发生或者可以证实多次发生过

3—中：威胁出现的频率中等，在某种情况下可能会发生或被证实曾经发生过

2—低：威胁出现的频率较小，一般不太可能发生，也没有被证实发生过

1—很低：威胁几乎不可能发生，仅可能在非常罕见和例外的情况下发生

# 脆弱点识别与评估

* 物理环境脆弱性识别

物理环境脆弱性主要是对信息系统所处的物理环境即机房、线路、客户端的支撑设施等进行脆弱性识别，为后续脆弱性分析及综合风险分析提供参考数据。

依据：GB/T 9361-2011《计算机场地安全要求》

工作方式：问卷调查、现场检查。

* 安全管理脆弱性识别

主要从以下几方面分析被评估信息系统：策略、组织架构、企业人员、安全控制、资产分类与控制、系统接入控制、网络与系统管理、业务可持续性发展计划、应用开发与维护及可适应性。同时为后续脆弱性分析及综合风险分析提供参考数据。

依据：ISO/IEC 17799-2013 《Code of practice for information security management》

参考链接：https://wenku.baidu.com/view/63a7e7762f60ddccdb38a049.html

工作方式：人工问询、调查问卷、现场查看。

* 技术脆弱性识别

依据检查清单，对评估工作范围内的网络设备、操作系统和数据库、信息系统进行系统脆弱性评估，评估方式又分为手工检查评估和远程脆弱性识别。同时为后续脆弱性分析及综合风险分析提供参考数据。

依据：GB17859-1999《计算机信息系统安全保护等级划分准则》

工作方式：安全扫描、手动检查、问卷调查、人工问询。

表三：脆弱点识别内容

|  |  |  |
| --- | --- | --- |
| 类型 | 识别对象 | 识别内容 |
| 物理环境脆弱点 | 场地 | 计算机场地位置、场地抗震级别、场地防火级别 |
| 内部装修 | 装修材料、活动地板、地毯 |
| 供配电系统 | 供电线路、供电电源、电缆 |
| 空气调节系统 | 安放位置、冷量和风量、空调材料 |
| 机房防护系统 | 机房防水、机房防静电、机房防雷、火灾自动报警系统、火灾自动灭火系统、灭火器、入侵报警系统、视频监控系统、出入口控制系统、防电磁干扰、防噪声、防鼠害、集中监控系统 |
| 安全管理脆弱点 | 技术管理 | 物理和环境安全、通信与操作管理、访问控制、系统开发与维护、业务连续性 |
| 组织管理 | 安全策略、组织管理、资产分类与控制、人员安全 |
| 技术脆弱点 | 操作系统 | 物理保护、用户账号、口令策略、资源共享、事件审计、访问控制、新系统配置、注册表加固、网络安全 |
| 数据库 | 补丁安装、鉴别机制、口令机制、访问控制、网络和服务设置 |
| 应用系统 | 审计机制、访问控制、数据完整性、密码保护 |
| 网络结构 | 设计、边界保护、网络设备安全配置 |

表四：脆弱点识别与评估表

|  |  |  |  |
| --- | --- | --- | --- |
| 可能威胁 | 脆弱点 | 评估等级 | |
| 地震，飓风，火山，洪水，海啸，泥石流，暴风雪，雪崩，雷电等 | 硬件物理保护不足 | 高 | 4 |
| 供电中断 | 没有备用电源 | 中 | 3 |
| 中央空调出现故障 | 没有相应降温设备 | 低 | 2 |
| 光纤以及双绞线耗损 | 未准备可替换光纤 | 低 | 2 |
| 火灾 | 没有部署消防设施或没有进行消防设施使用的知识普及 | 高 | 4 |
| 水灾，供水故障、污染、极端温度或湿度 | 未安装除湿设备 | 中 | 3 |
| 计算机、投影仪及网络设备出现故障 | 机器未及时检修，没有安排相关检修人员 | 低 | 2 |
| 恶意代码，计算机病毒 | 杀毒软件或一些应用软件没有及时升级 | 高 | 4 |
| 系统软件、应用软件故障 | 软件的安装与卸载权限管理机制不严，软件未能及时更新 | 高 | 4 |
| 存在弱口令等不安全后门 | 实验室成员的账号密码或机密数据没有有效防护 | 很高 | 5 |
| 移动存储设备出现故障，损坏，丢失 | 没有备用 U 盘和移动硬盘，且没有对移动硬盘和U 盘中的数据进行备份 | 高 | 4 |
| 网络故障 | 没有备用服务器，未配备检修人员 | 中 | 3 |
| 盗窃 | 没有相应安保人员到岗，盗窃物品没有备份 | 高 | 4 |
| 误操作 | 未设置回滚机制，数据未备份 | 高 | 4 |
| 物理硬件破坏 | 没有相关数据备份和可替换硬件 | 高 | 4 |
| 内部人员泄密 | 实验室成员的账号密码或者身份证泄露 | 很高 | 5 |

脆弱点严重程度：

5—很高：威胁被利用将对资产造成完全损害

4—高：威胁被利用将对资产造成重大损害

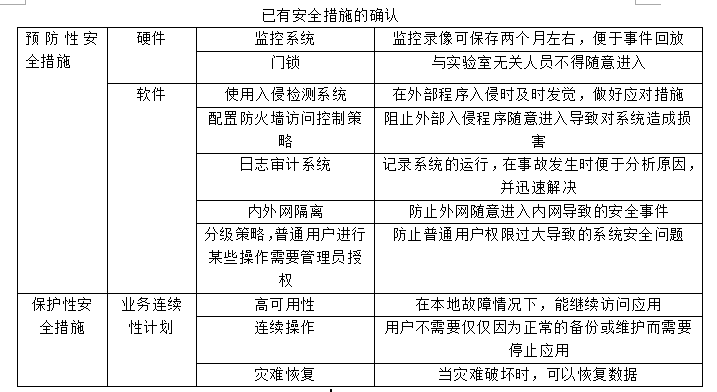
3—中：威胁被利用将对资产造成一般损害

2—低：威胁被利用将对资产造成较小损害

1—很低：威胁被利用将对资产造成的损害可忽略

1. 已有安全措施确认与评价

表五：已有安全措施评估表



\* 注：因未找到较合理的等级评估依据，故未对已有安全措施进行评分

# 风险分析与等级评估

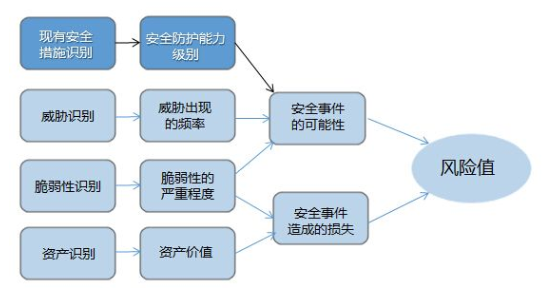
风险分析就是利用资产、威胁、脆弱点识别与评估结果以及已有安全措施的确认与分析结果，对资产面临的风险进行分析。

根据资产识别、威胁识别、脆弱点识别的结果，通过考察可能出现的资产-威胁脆弱点三元组可获取系统面临的安全风险。若风险事件发生后，造成关键硬件损坏，风险影响级别为“很高”；若未损坏硬件但系统不能够使用，风险影响级别为“高”；若未损坏硬件但系统使用不方便，风险影响级别为“中”；若影响不大，则为“低”。

风险计算参照我国《信息安全风险评估指南》，在风险分析方面采用了简化的处理办法，风险值为VR=(R(A,T,V)=R[L(T,V),F(Ia,Va)]

其中，Ia表示安全事件所作用的资产重要程度；Va表示脆弱点的严重程度；R表示风险，A表示资产，T表示威胁，V表示脆弱点。

其风险分析流程如下：



表六：风险的影响分析

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 风险标识 | 资产 | 威胁 | 脆弱点 | 影响分析 | 影响等级 | |
| R1 | 系统 | 供电中断 | 没有备用电源 | 系统无法使用 | 高 | 4 |
| R2 | 误操作 | 未设置回滚机制，数据未备份 | 硬件损害，软件被删除 | 高 | 4 |
| R3 | 自然威胁  （地震、海啸等） | 硬件物理保护不够 | 设备物理破坏 | 低 | 2 |
| R4 | 硬件 | 光纤以及双绞线耗损出现故障 | 使用寿命，无备用 | 设备无法正常使用 | 中 | 3 |
| R5 | 移动存储设备出现故障，损坏，丢失 | 无备用品，无备份 | 信息资源丢失 | 高 | 4 |
| R6 | 火灾 | 未部署防火设施 | 系统被烧毁 | 极高 | 5 |
| R7 | 计算机、投影仪及网络设备出现故障 | 未配备检修人员 | 系统使用不正常 | 中 | 3 |
| R8 | 极端温度、供水故障、污染、  水灾、或湿度 | 未安装除湿设备 | 系统使用不正常 | 中 | 3 |
| R9 | 软件 | 软件故障 | 软件安装卸载权限管理机制问题 | 软件不能正常使用 | 高 | 4 |
| R10 | 不安全后门 | 未及时打软件补丁 | 系统被攻击 | 高 | 4 |
| R11 | 恶意代码 、计算机病毒 | 杀毒软件，办公软件未及时升级 | 系统运行慢 | 高 | 4 |
| R12 | 人员 | 盗窃 | 技术支持不能及时到位 | 系统不能随时被使用 | 高 | 4 |
| R13 | 社会工程学管理员密码破解攻击 | 违规对数据操作失去真实可靠性 | 泄露篡改学校机密 | 很高 | 5 |

可能性分析主要依据威胁评估等级。最后根据影响分析及可能性分析的结果来进行风险评估，此处采用“风险=可能性\*影响”的方法计算。

表七：实验室信息系统风险评估

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 风险标识 | 资产 | 威胁 | 影响评估 | 可能性评估 | 风险值 | 风险等级 |
| R1 | 系统 | 供电中断 | 4 | 3 | 12 | 中 |
| R2 | 误操作 | 4 | 2 | 8 | 低 |
| R3 | 自然威胁 | 5 | 1 | 5 | 可忽略 |
| R4 | 硬件 | 光纤以及双绞线耗损出现故障 | 3 | 2 | 6 | 中 |
| R5 | 移动存储设备出现故障，损坏，丢失 | 4 | 3 | 12 | 中 |
| R6 | 火灾 | 5 | 2 | 10 | 低 |
| R7 | 水灾，供水故障、污染、极端温度或湿度 | 3 | 2 | 6 | 低 |
| R8 | 计算机、投影仪及网络设备出现故障 | 4 | 4 | 16 | 高 |
| R9 | 软件 | 软件故障 | 4 | 4 | 16 | 高 |
| R10 | 不安全后门 | 4 | 3 | 12 | 中 |
| R11 | 恶意代码 、计算机病毒 | 4 | 3 | 12 | 中 |
| R12 | 人员 | 盗窃 | 4 | 3 | 12 | 中 |
| R13 | 密码攻击 | 5 | 4 | 20 | 很高 |

表八：风险等级划分方法

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 风险 | |  | 可能性 | |  |  |  |
| 可忽略 1 | 低 2 | 中 3 | 高 4 | 很高 5 |
| 影响程度 | 很高 | 5 | 5 | 10 | 15 | 20 | 25 |
| 高 | 4 | 4 | 8 | 12 | 16 | 20 |
| 中 | 3 | 3 | 6 | 9 | 12 | 15 |
| 低 | 2 | 2 | 4 | 6 | 8 | 10 |
| 可忽略 | 1 | 1 | 2 | 3 | 4 | 5 |

八、安全措施的选取

风险评估的结果表明，软件被植入不安全后门、内部人员的信息泄露、火灾导致的风险等级为“很高”，由于人员误操作、盗窃等行为的物理破坏、软件故障和恶意代码对应的安全风险为“高”，供电中断、移动硬盘 U 盘丢失损坏、门禁故障、利用传真机恶意攻击和未及时到岗的风险级别为“中”，自然威胁、双绞线光纤磨损、火灾和极端湿度的风险级别为“低”。对风险级别“高”以上的应重点考虑采取向的安全措施，而对风险级别为低的可以不用处理，对于风险级别“中”的可以有选择性地处理。

评估建议

建议采取全方位的安全措施来确保实验室设备的正常运行，越早发现问题，越早处理，才可将风险和损失降到最低。同时提高实验室内部同学和老师的安全意识，加强培训，减少无意识不安全行为的发生。并且注意提高管理权限，如设立分级制度，普通用户执行某些操作需获得管理员统一，设防火墙，内外网隔离等。