节能型公司企业信息管理系统风险评估报告

一：概述

企业信息管理系统是企业常用的信息系统，它为企业内部管理信息，数据，文档，重要机密，以及人员提供了一个信息化的平台，本次实践选择了位于东四环恒通商务园中一家小型节能型公司（以下简称该公司）为调查对象进行信息安全系统的分析，力图通过此次分析能够让此公司的信息安全系统更加稳健茁壮。我们通过对此公司的背景资料以及公司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企业信息管理系统进行了风险评估。

二：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

三：资产分析

1　资产

（1）物理资产：

办公室

计算机及网络设备：服务器一台 路由器两台 交换机 2 台 个人 PC 20 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：动力保障 UPS 中央空调 文件柜 门禁 消防设施

安全保障设备：防火墙 身份验证 访问控制

其他电子设备：打印机 复印机 扫描仪 传真机

（2）系统软件：windows7 操作系统 CAD 软件

应用软件：OA 办公系统

源程序：自主开发的能源消耗监测系统

（3）人员：高管 5 名主管公司核心业务　在职员工共 15 名根据所在部门掌握相关资料 其其中负责网络运营及维护有 2 人

（4）信息/数据及文档：存储员工信息的数据 自主开发的软件系统源代码 系统文档 公司运营商务计划书 每季度公司的汇报文档 公司财务报表等内容

（5）服务：

网络服务 公司内部服务器进行内部网络的上传下载 还有路由器用于外网链接服务

信息服务 通过开发的系统进行项目实施从而获得的收益的相关服务

		资产机密性		资产完整性		资产可用性	
办公室		3		5		5	
服务器		3		4		5	
路由器		3		4		5	

交换机		3		4		5	
PC		5		5		5	
光纤及双绞线		1		5		5	
移动硬盘		4		5		5	
u 盘		4		4		5	
动力保障 UPS		1		3		3	
中央空调		1		3		3	
文件柜		2		3		3	
门禁		3		4		5	
消防设施		1		3		3	
防火墙		5		5		5	
身份验证		5		5		4	
访问控制		3		3		4	
打印机		2		4		4	
复印机		2		4		4	
扫描仪		2		4		4	
传真机		2		4		4	
windows 7 操作系统		3		5		5	
CAD 软件		3		3		3	
OA 办公系统		5		5		5	
高管		5		5		5	
在职员工		3		3		4	
网络运营及维护人员		5		5		5	
存储员工信息的数据		3		3		4	
自主开发的软件系统源代码		5		5		5	
系统文档		4		4		4	
公司运营商务计划书		5		5		5	
公司财务报表等内		5		5		5	

容							
网络服务		5		5		5	
信息服务		4		3		3	

等级 5 极高
4 高
3 中等
2 低
1 可忽略

四：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棉铃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：

威胁识别与评估表

威胁类型	威胁表现形式	评估等级	
自然威胁	地震，飓风，火山，洪水，海啸，泥石流，暴风雪，雪崩，雷电等	很低	1
环境威胁	供电中断	低	2
	光纤以及双绞线耗损，出现故障，中央空调出现故障	中	3
	水灾，供水故障，污染，极端温度或湿度	低	2
	火灾	低	2
系统威胁	计算机及网络设备出现故障	中	3
	保障电子设备，安全保障设备等电子设备出现故障	低	2
	移动存储设备出现故障，损坏，丢失	中	3
	系统软件故障，应用软件故障，自主开发的能源消耗监测系统故障	高	4
	恶意代码，计算机病毒	很高	5
	系统存在弱口令以及不安全的后门	很高	5
	网络故障	中	3
	信息服务故障	中	3
外部人员威胁	盗窃	高	4
	利用传真机恶意攻击	高	4
	利用恶意代码，计算机病毒，或系统不安全后门侵入系统，查看或窃取公司机密	高	4
内部人员威胁	物理硬件被破坏	中	3
	误操作	高	4
	疾病或其他原因导致不能及时到岗	中	3

	打印失误，直接将其丢弃	很高	5
	内部人员泄密	高	4

五：脆弱点识别与评估

脆弱点识别主要从技术和管理两个方面进行，技术脆弱点涉及物理层，网络层，新系统层，应用层等各个层面的安全问题 ，本次调研的对象在技术层面上问题简单，主要是表现在管理方面的脆弱性。脆弱点识别与评估图表如下：

脆弱点识别与评估表

可能威胁	脆弱点	评估等级	
供电中断	没有备用电源或动力 UPS 出故障	中	3
双绞线或光纤磨损	使用寿命问题以及没有备用双绞线以及光纤	低	2
移动硬盘或 U 盘丢失或损坏	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
发生火灾	部署了消防设施，却没有进行消防设施使用的知识普及	高	4
门禁出现故障	在门禁检修期间，无“备用”检查证件人员	中	3
极端湿度	未安装除湿设备	中	3
软件故障	软件的安装与卸载权限管理机制不严，对人员使用软件的注意培训做的不到位	高	4
因疾病或其他原因导致不能及时到岗	网络运营维护人员没有备份	高	4
利用传真机恶意攻击	传真机病毒，在传真机外部通信时被拦截，机密信息泄露	高	4
打印失误，直接将其丢弃	缺少碎纸机等重要销毁机器，使得公司机密或重要信息泄露的风险加大	很高	5
恶意代码	杀毒软件或一些应用软件没有及时升级	高	4
不安全后门	没有及时为软件打补丁，系统存在弱口令	很高	5
误操作	办公人员对公司信息系统的使用注意事项不清楚	高	4
自然威胁	硬件物理保护不够	高	4
盗窃，物理破坏	安全保卫机制不健全	高	4

六：风险分析与等级划分

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	人员对系统使用不熟悉	硬件损害，软件被删除	高	4
R3		自然威胁	硬件物理保护不够	设备物理破坏	很高	5
R4	硬件	双绞线光纤磨损	使用寿命，无备用	设备无法正常使用	低	2
R5		移动硬盘 U 盘丢失损坏	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	高	4
R7		门禁故障	门禁检修	外部人员进入	中	3
R8		极端湿度	未安装除湿设备	系统使用不正常	中	3
R9		盗窃物理破坏	安全保卫机制不健全	硬件破坏或被盗	高	4
R10		利用传真机恶意攻击	传真机病毒	泄露公司机密	高	4
R11	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
R12		不安全后门	未及时打软件补丁	系统被攻击	很高	5
R13		恶意代码	杀毒软件，办公软件未及时升级	系统运行慢	高	4
R14	人员	未及时到岗	技术支持不能及时到位	系统不能随时被使用	高	4
R15		信息泄露	打印材料未粉碎就丢弃	泄露公司机密	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。

企业信息系统风险评估

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	5	20	高
R3		自然威胁	5	1	5	低
R4	硬件	双绞线光纤磨损	2	2	4	低
R5		移动硬盘 U 盘丢失损坏	4	3	12	中
R6		火灾	4	2	8	低
R7		门禁故障	3	3	9	中

R8		极端湿度	3	2	6	低
R9		盗窃物理破坏	4	4	16	高
R10		利用传真机恶意攻击	4	3	12	中
R11	软件	软件故障	4	4	16	高
R12		不安全后门	5	5	25	很高
R13		恶意代码	4	4	16	高
R14	人员	未及时到岗	4	3	12	中
R15		信息泄露	5	5	25	很高

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

七、安全措施及其有效性分析

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，而对风险级别为中的可以有选择地处理。

安全措施的选取

风险标识	资产	威胁	风险等级	安全措施
R1	系统	供电中断	中	配置备用电源
R2		误操作	高	系统、应用软件操作培训
R5	硬件	移动硬盘 U 盘丢失损坏	中	备份企业信息资料，重要计划有 planB
R7		门禁故障	中	检修期间配备证件检查人员
R9		盗窃物理破坏	高	加强安全保卫工作
R10		利用传真机恶意攻击	中	及时检查传真机是否关闭
R11	软件	软件故障	高	加强权限管理，采用系统“一键还原”机制
R12		不安全后门	很高	检查软件的 MD5 值，采用可信的软件
R13		恶意代码	高	定期升级病毒库，科学上网等
R14	人员	未及时到岗	中	采用到岗检查机制，奖惩机制

R15		信息泄露	很高	配备碎纸机，提高管理权限等

评估建议

尽量采取更先进、高科技、全方位的安全措施来确保公司的正常运行，最好有公司系统的监测系统，越早发现问题，越早处理，将风险和损失降到最低。同时提高公司人员的安全意识和素质，加强培训。核心资料提高管理权限，设防火墙，监测路由流量，文件最好加密，采用 PKI 基于公钥加密算法保障网络安全。

数字证书：保证业务用户或者是系统服务器的身份认证

数据加密：保证业务数据的保密性

☐ 数据签名+数字时间戳：保证业务操作的不可抵赖性

数据签名：保证数据的完整性

☐ 数字证书扩展应用：结合业务逻辑方便的实现访问控制