GooAnn

您身边的IT风险管理专家

谷安天下信息安全意识推广方案

目　录

Web:www.gooann.com Tel:010-51626887

文档信息

文档名称：	谷安天下信息安全意识推广方案建议书	文档编号：	
文档起草人：	李华	起草日期：	2010-10-05
当前版本编号：	V1.0	版本日期：	2010-10-05
相关文档：			

版本记录

版本号	版本日期	修改者	说 明	文件名
V1.0	2010-10-05		谷安天下信息安全意识推广方案	谷安天下信息安全意识推广方案建议书.doc

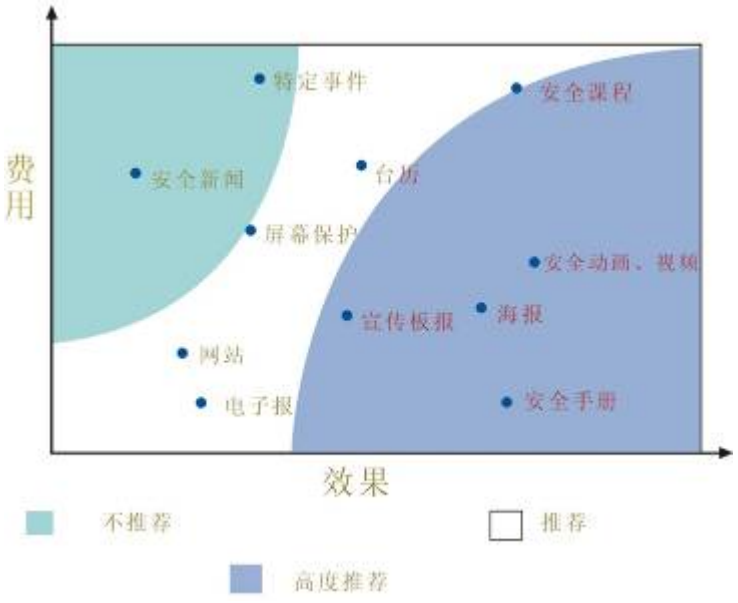
1 信息安全意识工程

1.1谷安天下的认识

- 世界头号黑客 Kevin Mitnick 曾说过“人是最薄弱的环节。你可能拥有最好的技术、防火墙、入侵检测系统、生物鉴别设备，可只要有人给毫无戒心的员工打个电话……”技术无法保护每一个人远离每一种可能存在的安全风险，信息安全管理人员要教会员工安全思考的方式。投资员工，让他们建立起保持数据正确的责任感，是企业面对安全威胁的最佳方式。
- 实际上一个企业的整体安全水平不仅要看专职的安全管理与技术人员的能力，还要看全体员工的安全意识是否到位，这与持续的安全意识推广是密不可分的。
- 提高和维持所有员工的信息安全意识和技能，对员工理解信息安全对企业的意义，开展信息安全工作，在企业内逐步建立和融入信息安全的文化，提高整体安全水平是非常重要的。当然，这可能是一个漫长而艰难的过程。

1.2谷安天下的观点

- 谷安天下根据丰富的为企业提供信息安全咨询服务的经验，总结出对于信息安全意识推广不同方式的特点和效果，可以为公司开展信息安全意识推广提供参考建议。



- 对于全员的信息安全意识推广，必须结合企业的文化和具体情况和要求，辅以生动、形象、简洁的方式进行，传统的教科书的方式是不能达到设想的培训目标的。
- 企业开展信息安全意识推广，是否能够达到预期设想的目的，是否能够看到实际的效果，必须通过有效的方式来进行衡量。一方面可以通过课程测试的方式看员工是否掌握了需要了解的基本知识，另一方面企业可以通过一段时间（如半年）持续的安全事件（如违规行为、病毒爆发等）发生率来进行跟踪。

2 谷安天下信息安全意识推广方式与工具

谷安天下在企业信息安全咨询服务，以及安全教育培训的过程中积累了大量的信息安全意识推广实战经验。

2.1安全易视

安全易视以大众化信息安全意识培养作为信息安全工作重点，主要用于企业对全体员工进行长期信息安全意识培养。安全易视内置了大量的信息安全基本知识普及与意识培养 Flash 动画与电子海报，由资深信息安全顾问团队，对信息安全知识进行全面、科学地编排，并及时进行热点更新；安全易视通过强化视觉与听觉的冲击力，可放置在企业入口、休息室、前台大厅、食堂等地进行播放，通过生动、幽默、实用和高效的信息安全知识宣传，让员工随时随地的轻松掌握信息安全基本知识，理解信息安全对实现组织目标的重要性，消除员工对安全制度的厌烦感觉，提醒员工时时关注重要的信息安全实践，并使员工切身感觉到安全事件与自己息息相关，达到“人人受到宣传教育、人人增强防范意识、人人掌握基本常识”的目标，构建企业信息安全文化氛围，潜移默化地让员工成为组织信息安全政策的忠实执行者，构筑最牢固的信息安全意识防火墙。

Web:www.gooann.com Tel:010-51626887

安全易视内的知识内容主要由大量信息安全Flash动画、电子海报组成。

信息安全Flash动画、电子海报内容包括：人员安全、物理安全、网络安全、系统安全、应用安全、企业信息安全、个人电脑安全配置操作、攻击防范、通讯设备、信息保密安全常识等数十个主题方向，并将以上主题细化分为更多的和企业员工工作与生活相关的信息安全主题。

◆ Flash 样例：

◆ 电子海报样例：

知识内容可根据企业现状，搭配以下不同的播放器硬件：

播放方式一：广告机

支持22寸、26寸、32寸多尺寸播放器硬件。液晶规格为全新品牌A规液晶屏，画质清晰，屏幕显示参数要求达到16：9或4：3显示方案。可长时间工作，适应环境强，防震环境强，外观简单美观大方，从视觉和触觉都让人耳目一新。并具备超强的定制播放功能，设置可设定多个时段自动开、关的时间自动播放节目，全年全天候无需专人值守。支持节目断电记忆，可设定重新来电后，节目从断电前第几秒继续播放。

适用于企业没有现有的播放器硬件的情况。

播放方式二：加密U盘

适用于企业已经有播放器硬件的情况。可将知识内容存储在加密U盘中，企业直接利用已有的播放器硬件读取加密U盘中的内容进行播放。

Web:www.gooann.com Tel:010-51626887

2.2信息安全手册

制作手册，融入信息安全基础知识、信息安全意识警示、信息安全操作技能等内容，使员工对信息安全有一个全面的认识和了解。

- **优点：**在内容上是关于信息安全知识全面、详细的介绍，但知识的展现形式生动有趣；便于员工深入学习，普及面广
- 信息安全手册样例

2.3信息安全意识培训活动和专题讲座

优点：摒弃呆板的培训方式，寓教于乐，把现有制度、流程、安全要求等融入意识培训中，通过大家熟知的电影视频和专门制作的动画视频来形象展现信息安全基础知识、信息安全的重要性及平时应该注意的事项等。

- **全员信息安全课程内容**

课　　件　　内　　容		
主 题	**内 容**	**目 标**
一、桌面安全操作	1、案例分析	通过一个入侵案例来分析个人电脑的安全问题，阐述公司安全策略与制度规范关于此方面的内容，使员工了解公司的具体要
	2、公司要求	
	3、防病毒软件安装	

Web:www.gooann.com Tel:010-51626887

	4、补丁安装	求，简介个人病毒防范、补丁管理、防火墙使用、系统安全配置的基本操作，使员工掌握个人电脑安全的基本知识和技能。
	5、防火墙软件	
	6、Windows安全配置	
二、安全上网	1、案例分析	通过一个案例来分析上网安全问题，阐述公司安全策略与制度规范关于此方面的内容，使员工了解公司的具体要求，简介浏览器安全配置的基本操作，使员工掌握上网安全的基本知识和技能，并通过测试检验培训的效果。
	2、公司要求	
	3、浏览器安全建议	
	4、习题测试	
三、电子邮件安全	1、案例分析	通过一个案例来分析电子邮件安全问题，阐述公司安全策略与制度规范关于此方面的内容，使员工了解公司的具体要求，简洁电子邮件安全配置的基本操作，使员工掌握上网安全的基本知识，并通过测试检验培训的效果。
	2、公司要求	
	3、电子邮件安全建议	
	4、习题测试	
四、安全数据管理	1、案例分析	通过一个案例来分析电子数据安全问题，阐述公司安全策略与制度规范关于此方面的内容，使员工了解公司的具体要求，简介数据分类、共享、备份、销毁的基本过程，使员工掌握数据安全的基本知识，并通过测试检验培训的效果。
	2、公司要求	
	3、数据安全建议	
	4、习题测试	
五、安全事件报告	1、案例分析	分析安全事件报告对于企业信息安全的意义和重要性，阐述公司安全策略与制度规范关于此方面的内容，使员工了解公司的具体要求，简介事件识别、现场保护、报告信息的基本过程，使员工掌握安全事件处理的基本知识，并通过测试检验培训的效果。
	2、公司要求	
	3、安全事件报告过程	
	4、习题测试	
六、移动介质安全	1、案例分析	通过一个案例来分析移动介质安全问题，阐述公司安全策略与制度规范关于此方面的内容，使员工了解公司的具体要求，简介移动介质安全的注意事项，使员工掌握移动介质安全的基本知识，并通过测试检验培训的效果。
	2、公司要求	
	3、移动介质安全建议	
	4、习题测试	
七、社会工程学	1、案例分析	通过几个实例来分析社会工程学典型的攻

	2、典型攻击方式	击手段，，使员工掌握预防社会工程学攻击的基本知识，并通过测试检验培训的效果。
	3、相关安全建议	
	4、习题测试	

◆ 某证券公司信息安全电子课件样例（截图）

◆ 某海关信息安全意识课件样例

2.4信息安全意识屏幕保护程序

将日常工作中有关信息安全的知识通过图画来展现，制作成电脑桌面或者屏幕保护程序，员工在打开电脑时和待机时即可接收到生动的信息安全知识。

- **优点：**视觉冲击感强烈，高频率提醒员工，且有利于公司的形象统一，在公众中打造公司注重信息安全的形象，提高公信力。
- 样例：

2.5信息安全意识宣传板报

在员工经常逗留或者经过的区域，粘贴具有意识效果的纸质招贴画，例如走廊、餐厅、会议室、电梯口，随时随地灌输员工信息安全知识

- **优点：**展现方式生动有趣，内容简单易懂，便于理解记忆；占用员工时间少；员工普及面广
- 某银行客户信息安全宣传板报样例

Web:www.gooann.com Tel:010-51626887

2.6信息安全新闻

谷安天下可提供常年的信息安全新闻递送服务，将有关信息安全方面的漏洞、新闻等制作成通告发送客户

- **优点：**动态的追踪信息安全现状及发展，养成员工长期注重信息安全的习惯。
- 谷安天下信息安全通告样例

2.7信息安全电子报

定期由信息安全组织成员发信息安全电子报邮件给员工，在不过多占用员工工作时间的基础上不断灌输信息安全知识给员工，加深其印象，并引起其兴趣和重视。

- **优点：**可以告知所有员工，并且占用员工的时间少。内容简洁易懂、容易记忆，画面吸引人，生动有趣，让员工在尽可能短的时间内阅读完所有内容并能留下较深刻的印象。
- 某电信服务企业信息安全电子报样例（多期）

Web:www.gooann.com Tel:010-51626887

2.8信息安全台历

- **优点：**12 张台历页面可以系统性、有步骤的给员工灌输信息安全知识，并且台历放在员工的工作区域内，可以让员工随时随刻进行学习，没有任何任务负担。
- 某海关客户信息安全台历样例

Web:www.gooann.com Tel:010-51626887

3 信息安全意识推广辅助工具——ITRM 软件

谷安天下依据在企业、证券、保险、电信、移动、政府、能源、软件等行业积累了大量 IT 风险管理服务案例，总结分析了众多标准与实践经验，进行了系列理论创新与技术创新，创造性的提出了适合国内企业实际情况的 IT 风险管理实践框架，并在此基础上研发了 IT 风险管控系列工具软件，从组织，流程和资产三个维度来全方位的进行风险分析、建立体系、运营管理和监控优化。

- ITRM 是用于帮助企业自己建立信息安全管理体系的软件平台；
- ITRM 是将信息安全管理过程固化，建立控制体系并持续运营的 IT 风险管控平台；
- ITRM 目前涵盖了风险评估、体系建立、运营管理、监控审计与意识提升五大模块。

3.1信息安全管理工具简介

谷安天下信息安全管理工具能够实现如下主要功能：

信息安全风险评估-GOO-Risk

GOORisk 安全风险评估软件提供了系统化的风险评估方法论和行业风险知识库，包括评估范围定义，安全现状调查，资产威胁分析、漏洞分析、风险综合分析、风险控制措施等主要功能，帮助客户快速自动化的评估自身的资产风险与流程风险。

信息安全体系建设-GOO-ISMS

GOOISMS 安全体系建设软件提供了信息安全体系规划与管理体系建设的方法论和行业模板库，包括体系规划，体系设计，体系实施，体系保障等主要功能，帮助客户快速建立安全管理体系，通过内部审计、管理评审等管理过程，保障体系的有效运行。

信息安全流程管理-GOO-Process

GOOProcess 安全运营管理软件提供了基本的信息安全日常运作流程，通过自动化工作流引擎，可自主定义帐号管理、权限管理、人员安全、设备安全、物理安全、安全检查、安全事件、安全培训、通知公告等流程，将安全管理流程真正落地。

信息安全审计管理-GOO-Audit

GOOAudit 安全审计管理软件提供了信息安全审计检查工具与审计管理流程，包括了各种业务、系统、设备的安全检查列表，符合性测试、实质性测试工具，定期审计管理流程，以及审计底稿、审计报告的管理

信息安全知识管理-GOO-Awareness

GOOAwareness 安全知识管理软件为企业提供了信息安全相关知识的管理与共享平台，包括

Web:www.gooann.com Tel:010-51626887

安全通告、内部知识库、外部资料库、标准与法规、案例警示、常用模板、知识地图、个人知识库等基本功能，方便安全知识的获取与管理，全面提高员工信息安全意识。

3.2系统特点

完整的行业知识库：提供完整的行业知识库支持，并且对知识库进行持续更新；知识库包括行业业务流程、业务系统、信息资产、威胁类型、漏洞类别、风险指标、安全策略、管理流程、行业法规等，目前支持政府、央企、电信、银行、保险、证券和软件等行业。目前知识库涵盖 **8 个准则，10 个行业，2500 多个控制措施。**

遵从各类监管要求:紧密结合企业信息安全与内部控制要求,遵从ISO27001、等级保护、COBIT等标准，引导公司信息安全与IT控制工作，协助信息安全与内部控制体系建立，并管理文档记录、测评、评估、改进、测试等阶段的工作；全面符合国际标准ISO27001、国家标准GB20984《信息安全风险评估规范》，以及公安部等级保护测评要求

统一控制框架： 采取Unified Control Framework设计，可将超过2,000个“既定的”控制目标与等级保护、ISO27000:2005、COBIT、 COSO、ITIL、NIST、SOX、BASELII和PCI等几十个标准和法律法规相挂钩，并可通过全面的可配置性和可扩展性应用到知识库中；

操作简单安全：基于B/S架构，通过浏览器的轻松灵活的使用、导航界面，能够根据组织要求调节界面外观，基于角色授权指派相关人士负责控制工作，轻松添加各种控制与遵从标准版本(等级保护、CMM、Prince2等)，支持本机Excel电子数据表输入。

自动化工作流引擎：基于管理软件常用的功能和基础要素进行抽象，包括用户类、权限类、消息类、工作流引擎等，满足企业各种安全管理流程等。

产品稳定成熟：谷安是国内唯一进入全面信息安全风险管理与内部控制系统软件领域的厂商，产品的最新版本为2.0，并于年底前推出3.0版本；

Web:www.gooann.com Tel:010-51626887