三零卫士

www.30wish.net

GB/Z 20986-2007

《信息安全事件分类分级指南》

标准解读

闵京华

2011年11月3日

www.30wish.net

内容纲要

1. 信息安全事件最新数据
2. 信息安全事件基本概念
3. 信息安全事件管理过程
4. 信息安全事件分类分级
5. 信息安全事件标准应用

一、信息安全事件最新数据

- 数据来源
  - 《中国信息安全》杂志（2011年第10期）
- 最新案例
  - 人民网海南视窗遭黑客攻击
    - 9月14日上午10时许，人民网海南视窗遭黑客攻击，访问者通过搜索引擎打开该网站，竟弹出含有色情内容的网页。经全力破解，网站于当天中午1时许恢复正常。
  - 黑龙江：哈药六厂官网被黑
    - 9月11日，哈药六厂官网首页全部内容被篡改，只留下了249字的黑客宣言，下午5时左右，网站恢复正常。

一、信息安全事件最新数据

- 最新案例
  - 香港：破获计算机犯罪集团
    - 近日，香港警方破获一个入侵网上“缴费灵”用户盗款的计算机犯罪集团，先后拘捕14名犯罪分子。警方称，犯罪分子利用点对点分享软件和计算机病毒，盗取他人网上“缴费灵”数据和密码犯罪，最少已有5名市民中招，最高损失者达10万元。
  - 台湾：选举广告链到成人网站 蓝绿阵营尴尬回应
    - 据台湾联合报报道，2012年“大选”抢选票，台当局领导人马英九和民进党主席蔡英文的网络广告，不约而同地出现在岛内大型成人网站讨论区，“双英”阵营9月5日尴尬表示，网络广告是委托代理商购买，一定会要求撤广告。

一、信息安全事件最新数据

- 最新数字
  - 被挂马网站：11339
    - 根据中国国家信息安全漏洞库（CNNVD）2011年9月抽样监测发现，我国大陆地区11339个网站被挂马，其中数量较多的地区为江苏省、北京市和广东省。
  - 被篡改网站：2525和2114
    - 根据国家互联网应急中心（CNCERT）2011年8月网络安全监测数据显示，我国大陆被篡改网站的数量为2525个，与上月的2613个相比下降3.4%。
    - 其中，最多的分别是.com和.com.cn为1706个，.gov.cn为233个，.net和.net.cn为175个，共为2114个。

一、信息安全事件最新数据

- 最新数字
  - 新增漏洞：413
    - 8月15日至9月11日，我国境内新增信息安全漏洞413个，其中高危漏洞192个。
  - 被篡改政府网站：177
    - 8月15日至9月11日，我国境内共计177个政府网站被篡改。
  - 感染飞客蠕虫主机：6051000
    - 8月15日至9月11日，我国境内感染飞客（Confiker）蠕虫的主机约为6051000台。
  - 被木马或僵尸程序控制主机：430000
    - 8月15日至9月11日，我国境内被木马或僵尸程序控制的主机约为430000台。

一、信息安全事件最新数据

- 结论
  - 现状：信息安全措施不是万全，安全事件难避免
  - 原因：信息安全新威胁新漏洞，安全措施未健全
  - 意识：信息安全形势始终严峻，决不可掉以轻心
  - 对策：加强信息安全事件管理，有效防范和处置

二、信息安全事件基本概念

- 两个需要区分的基本概念
  - information security event
  - information security incident
- 如何区分？
  - 当黑客猜测你的登录密码，但还没有成功，当然不会给你造成损失，但这是违规甚至违法行为——这称之为发生了信息安全event
  - 一旦黑客成功登入你的系统，极大可能实施恶意破坏行为，如植入木马或病毒，盗取你的敏感信息、破坏你的重要文件、篡改你的网页页面等——这称之为发生了信息安全incident

二、信息安全事件基本概念

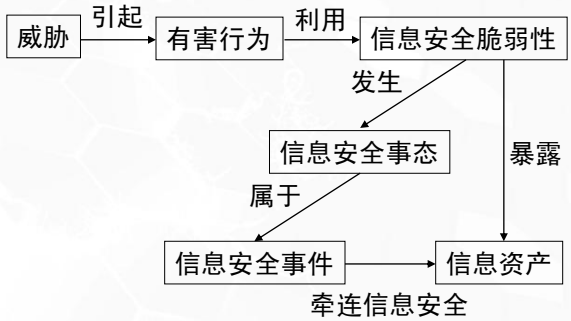
- ISO/IEC 27000:2009的定义（原文）
  - information security event
    - identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of controls, or a previously unknown situation that may be security relevant
  - information security incident
    - single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security

二、信息安全事件基本概念

- ISO/IEC 27000:2009的定义（翻译）
  - 信息安全事态/information security event
    - 已识别的一种系统、服务或网络状态的发生，指出可能违反信息安全方针或控制措施失效，或者一种可能与安全相关但以前不为人知的情况
  - 信息安全事件/information security incident
    - 一个或一系列意外或不期望的信息安全事态，它或它们极有可能损害业务运行并威胁信息安全
  - 翻译说明
    - 媒体上通常不区分“event”和“incident”均译为“事件”
    - 专业上信息安全事件管理需要区分两者
    - 将“event”译为“事态”仅作为信息安全领域的专业术语

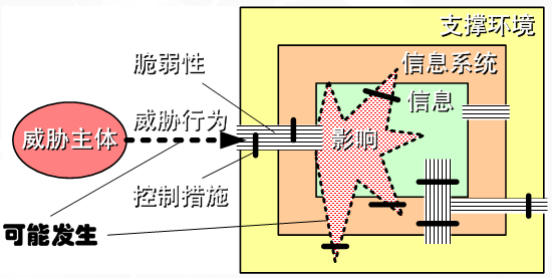
二、信息安全事件基本概念

- 信息安全事件链



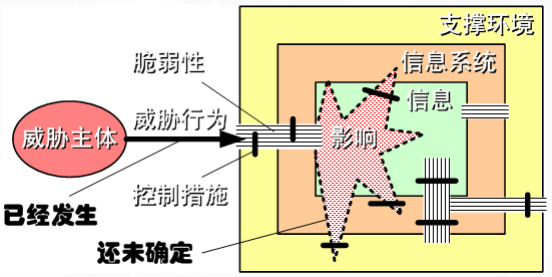
二、信息安全事件基本概念

- 信息安全事件与信息安全风险的关系
  - 信息安全风险/information security risk



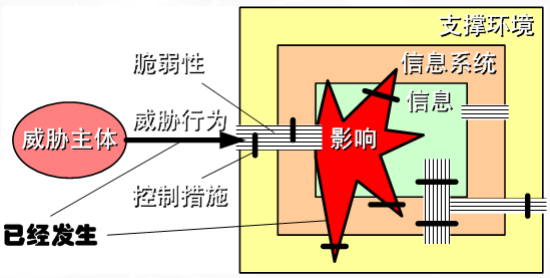
二、信息安全事件基本概念

- 信息安全事件与信息安全风险的关系
  - 信息安全事态/information security event



二、信息安全事件基本概念

- 信息安全事件与信息安全风险的关系
  - 信息安全事件/information security incident



二、信息安全事件基本概念

- 信息安全事件与信息安全风险的关系

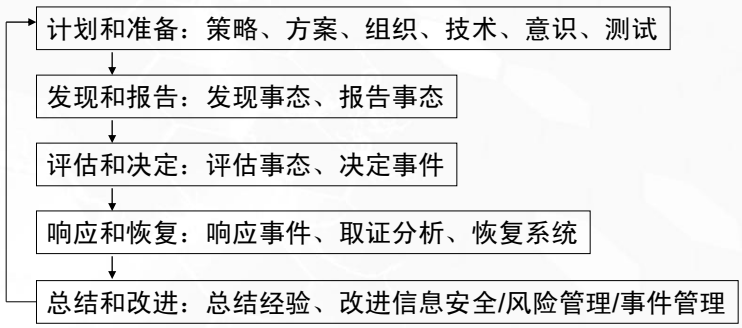
	信息安全风险 risk	演变	信息安全事态 event	属于	信息安全事件 incident
特征	潜在危险 攻击未发生 影响未发生		显在危险 攻击已发生 影响未确定		产生损害 攻击已发生 影响已发生
措施	防患未然 风险控制		防微杜渐 监视报告		有备无患 事件响应

三、信息安全事件管理过程

- 信息安全事件管理标准
  - 国家标准
    - GB/Z 20985-2007 信息技术 安全技术 信息安全事件管理指南（2007年6月14日发布）
    - 修改采用技术报告类国际标准ISO/IEC TR 18044:2004
  - 国际标准
    - ISO/IEC TR 18044:2004 Information technology - Security techniques - Information security incident management（被ISO/IEC 27035:2011取代）
    - ISO/IEC 27035:2011 Information technology - Security techniques - Information security incident management（2011年9月1日发布）
      - 我国代表作为共同编辑直接参与了该标准编写工作
      - 采纳了我国国家标准GB/Z 20986-2007的相关内容

三、信息安全事件管理过程

- 信息安全事件管理过程



四、信息安全事件分类分级

- 信息安全事件分类分级是开展信息安全事件管理，快速有效处置信息安全事件的基础之一，其目的是：
  - 促进安全事件信息的交流和共享
  - 提高安全事件通报和应急处理的自动化程度
  - 提高安全事件通报和应急处理的效率和效果
  - 利于安全事件的统计分析
  - 利于安全事件严重程度的确定

四、信息安全事件分类分级

- 信息安全事件分类分级标准
  - 国家标准
    - GB/Z 20986-2007 信息安全技术 信息安全事件分类分级指南（2007年6月14日发布）
    - 自主研制标准
  - 国际标准
    - ISO/IEC 27035:2011 Annex C Example approaches to the categorization and classification of information security events and incidents（2011年9月1日发布）
      - 基于我国国家标准GB/Z 20986-2007

四、信息安全事件分类分级

- GB/Z 20986-2007文本结构
  - 前言
  - 引言
  - 1 范围
  - 2 术语和定义
  - 3 缩略语
  - 4 信息安全事件分类
  - 5 信息安全事件分级

四、信息安全事件分类分级

- GB/Z 20986-2007文本结构
  - 4 信息安全事件分类
    - 4.1 考虑要素与基本分类
    - 4.2 事件分类
      - 4.2.1 有害程序事件（MI）
      - 4.2.2 网络攻击事件（NAI）
      - 4.2.3 信息破坏事件（IDI）
      - 4.2.4 信息内容安全事件（ICSI）
      - 4.2.5 设备设施故障（FF）
      - 4.2.6 灾害性事件（DI）
      - 4.2.7 其他事件（OI）

四、信息安全事件分类分级

- GB/Z 20986-2007文本结构
  - 5 信息安全事件分级
    - 5.1 分级考虑要素
      - 5.1.1 概述
      - 5.1.2 信息系统的重要程度
      - 5.1.3 系统损失
      - 5.1.4 社会影响
    - 5.2 事件分级
      - 5.2.1 概述
      - 5.2.2 特别重大事件（Ⅰ级）
      - 5.2.3 重大事件（Ⅱ级）
      - 5.2.4 较大事件（Ⅲ级）
      - 5.2.5 一般事件（Ⅳ级）

四、信息安全事件分类分级

- GB/Z 20986-2007标准范围
  - 本指导性技术文件为信息安全事件的分类分级提供指导，用于信息安全事件的防范与处置，为事前准备、事中应对、事后处理提供一个基础指南，可供信息系统和基础信息传输网络的运营和使用单位以及信息安全主管部门参考使用。

四、信息安全事件分类分级

- GB/Z 20986-2007术语和定义
  - 信息系统/information system
    - 由计算机及其相关的和配套的设备、设施（含网络）构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。
    - 出自《中华人民共和国计算机信息系统安全保护条例》中对“计算机信息系统”的定义。
  - 信息安全事件/information security incident
    - 由于自然或者人为以及软硬件本身缺陷或故障的原因，对信息系统造成危害，或对社会造成负面影响的事件。

四、信息安全事件分类分级

- GB/Z 20986-2007缩略语
  - 采用英文缩略词对信息安全事件类别进行编码
    - MI：有害程序事件（Malware Incidents）
    - CVI：计算机病毒事件（Computer Virus Incidents）
    - WI：蠕虫事件（Worms Incidents）
    - THI：特洛伊木马事件（Trojan Horses Incidents）
    - BI：僵尸网络事件（Botnets Incidents）
    - BAI：混合攻击程序事件（Blended Attacks Incidents）
    - WBPI：网页内嵌恶意代码事件（Web Browser Plug-Ins Incidents）
    - NAI：网络攻击事件（Network Attacks Incidents）

四、信息安全事件分类分级

- GB/Z 20986-2007缩略语
  - 采用英文缩略词对信息安全事件类别进行编码
    - DOSAI：拒绝服务攻击事件（Denial of Service Attacks Incidents）
    - BDAI：后门攻击事件（Backdoor Attacks Incidents）
    - VAI：漏洞攻击事件（Vulnerability Attacks Incidents）
    - NSEI：网络扫描窃听事件（Network Scan & Eavesdropping Incidents）
    - PI：网络钓鱼事件（Phishing Incidents）
    - II：干扰事件（Interference Incidents）
    - IDI：信息破坏事件（Information Destroy Incidents）

四、信息安全事件分类分级

- GB/Z 20986-2007缩略语
  - 采用英文缩略词对信息安全事件类别进行编码
    - IAI：信息篡改事件（Information Alteration Incidents）
    - IMI：信息假冒事件（Information Masquerading Incidents）
    - ILEI：信息泄漏事件（Information Leakage Incidents）
    - III：信息窃取事件（Information Interception Incidents）
    - ILOI：信息丢失事件（Information Loss Incidents）
    - ICSI：信息内容安全事件（Information Content Security Incidents）

四、信息安全事件分类分级

- GB/Z 20986-2007缩略语
  - 采用英文缩略词对信息安全事件类别进行编码
    - FF：设备设施故障（Facilities Faults）
    - SHF：软硬件自身故障（Software and Hardware Faults）
    - PSFF：外围保障设施故障（Periphery Safeguarding Facilities Faults）
    - MDA：人为破坏事故（Man-made Destroy Accidents）
    - DI：灾害性事件（Disaster Incidents）
    - OI：其他事件（Other Incidents）

四、信息安全事件分类分级

- GB/Z 20986-2007信息安全事件分类
  - 分类要素：多种
    - 起因
      - 人为（故意、过失）、非人为（自然、人造）
    - 表现
      - 植入病毒、蠕虫、木马等恶意代码，利用后门和漏洞进行攻击，网上扫描或窃听，网上欺骗（钓鱼），技术干扰，设备设施故障，信息内容有害，水灾、台风、地震等自然灾害，恐怖袭击、战争等人为灾害
    - 结果
      - 服务被拒绝，信息被篡改、假冒、泄露、窃取、丢失等

四、信息安全事件分类分级

- GB/Z 20986-2007信息安全事件分类
  - 基本类别：七个
    - 有害程序事件
    - 网络攻击事件
    - 信息破坏事件
    - 信息内容安全事件
    - 设备设施故障
    - 灾害性事件
    - 其他事件

四、信息安全事件分类分级

- GB/Z 20986-2007信息安全事件分类
  - 有害程序事件（MI）
    - 计算机病毒事件（CVI）
    - 蠕虫事件（WI）
    - 特洛伊木马事件（THI）
    - 僵尸网络事件（BI）
    - 混合攻击程序事件（BAI）
    - 网页内嵌恶意代码事件（WBPI）
    - 其它有害程序事件（OMI）

四、信息安全事件分类分级

- GB/Z 20986-2007信息安全事件分类
  - 网络攻击事件（NAI）
    - 拒绝服务攻击事件（DOSAI）
    - 后门攻击事件（BDAI）
    - 漏洞攻击事件（VAI）
    - 网络扫描窃听事件（NSEI）
    - 网络钓鱼事件（PI）
    - 干扰事件（II）
    - 其他网络攻击事件（ONAI）

四、信息安全事件分类分级

- GB/Z 20986-2007信息安全事件分类
  - 信息破坏事件（IDI）
    - 信息篡改事件（IAI）
    - 信息假冒事件（IMI）
    - 信息泄漏事件（ILEI）
    - 信息窃取事件（III）
    - 信息丢失事件（ILOI）
    - 其它信息破坏事件（OIDI）

四、信息安全事件分类分级

- GB/Z 20986-2007信息安全事件分类
  - 信息内容安全事件（ICSI）
    - 违反宪法和法律、行政法规的信息安全事件
    - 针对社会事项进行讨论、评论形成网上敏感的舆论热点，出现一定规模炒作的信息安全事件
    - 组织串连、煽动集会游行的信息安全事件
    - 其他信息内容安全事件
  - 设备设施故障（FF）
    - 软硬件自身故障（SHF）
    - 外围保障设施故障（PSFF）
    - 人为破坏事故（MDA）
    - 其它设备设施故障（IF-OT）

四、信息安全事件分类分级

- GB/Z 20986-2007信息安全事件分类
  - 灾害性事件（DI）
    - 水灾、台风、地震、雷击、坍塌、火灾、恐怖袭击、战争等不可抗力对信息系统造成物理破坏而导致的信息安全事件
  - 其他事件（OI）

四、信息安全事件分类分级

- ISO/IEC 27035:2011信息安全事件分类
  - Natural disaster incident
    自然灾害事件
    - 地震、火山、洪水、暴风、雷电、海啸、塌陷等
  - Social unrest incident
    社会动乱事件
    - 示威游行、恐怖袭击、战争等
  - Physical damage incident
    物理损坏事件
    - 火灾、水灾、静电、恶劣环境（如污染、灰尘、腐蚀、冻结）、设备破坏、媒介破坏、设备盗窃、媒介盗窃、设备丢失，媒介丢失、设备篡改，媒介篡改等

四、信息安全事件分类分级

- ISO/IEC 27035:2011信息安全事件分类
  - Infrastructure failure incident
    基础设施故障事件
    - 供电故障、网络故障、空调故障、供水故障等
  - Radiation disturbance incident
    辐射干扰事件
    - 电磁辐射、电磁脉冲、电子干扰、电压波动、热辐射等
  - Technical failure incident
    技术故障事件
    - 硬件故障、软件故障、过载（信息系统能力饱和）、维护不足等

四、信息安全事件分类分级

- ISO/IEC 27035:2011信息安全事件分类
  - Malware incident
    恶意代码事件
    - 计算机病毒、网络蠕虫、特洛伊木马、僵尸网络、混合式攻击、恶意代码嵌入网页、恶意代码托管网站等
  - Technical attack incident
    技术攻击事件
    - 网络扫描、漏洞利用、后门利用、登录尝试、干扰、拒绝服务等
  - Breach of rule incident
    违规事件
    - 资源未授权使用、版权侵犯等

四、信息安全事件分类分级

- ISO/IEC 27035:2011信息安全事件分类
  - Compromise of functions incident
    功能损害事件
    - 权限滥用、权限伪造、功能拒绝、操作不当、人员缺位等
  - Compromise of information incident
    信息损害事件
    - 截取、刺探、窃听、信息泄露、假冒、社会工程、网络钓鱼、数据窃取、数据丢失、数据篡改、数据错误、数据流分析、位置检测等
  - Harmful contents incident
    有害内容事件
    - 非法内容、恐慌内容、恶意内容、诽谤内容等

四、信息安全事件分类分级

- ISO/IEC 27035:2011信息安全事件分类
  - Other incidents
    其他事件

四、信息安全事件分类分级

- 国家标准vs国际标准：信息安全事件分类

GB/Z 20986-2007	ISO/IEC 27035:2011
有害程序事件（MI）	恶意代码事件
网络攻击事件（NAI）	技术攻击事件、辐射干扰事件
信息破坏事件（IDI）	信息损害事件
信息内容安全事件（ICSI）	有害内容事件
设备设施故障（FF）	物理损坏事件、基础设施故障 技术故障事件
灾害性事件（DI）	自然灾害事件、社会动乱事件
其他事件（OI）	违规事件、功能损害事件 其他事件

四、信息安全事件分类分级

- GB/Z 20986-2007信息安全事件分级
  分级要素及其级别
  - 信息系统的重要程度
    - 特别重要、重要、一般
    - 对应信息系统等级保护：
      五级和四级、三级、二级和一级
  - 系统损失
    - 特别严重、严重、较大、较小
  - 社会影响
    - 特别重大、重大、较大、一般

四、信息安全事件分类分级

- GB/Z 20986-2007信息安全事件分级
  事件级别及准则
  - 特别重大事件（Ⅰ级）
    - 特别重要信息系统 and 特别严重系统损失 or
    - 特别重大社会影响
  - 重大事件（Ⅱ级）
    - 特别重要信息系统 and 严重系统损失 or
    - 重要信息系统 and 特别严重系统损失 or
    - 重大社会影响

四、信息安全事件分类分级

- GB/Z 20986-2007信息安全事件分级
  事件级别及准则
  - 较大事件（Ⅲ级）
    - 特别重要信息系统 and 较大系统损失 or
    - 重要信息系统 and 严重系统损失 or
    - 一般信息系统 and 特别严重系统损失 or
    - 较大社会影响
  - 一般事件（Ⅳ级）
    - 特别重要信息系统 and 较小系统损失 or
    - 重要信息系统 and 较大系统损失 or
    - 一般信息系统 and 严重或严重以下级别系统损失 or
    - 一般社会影响

四、信息安全事件分类分级

- ISO/IEC 27035:2011信息安全事件分级
  分级要素及其级别
  - information system importance/信息系统重要性
    - especially important, Important, Ordinary
      特别重要、重要、一般
  - business loss/业务损失
    - especially serious, serious, considerable, minor
      特别严重、严重、较大、较小
  - social impact/社会影响
    - especially important, important, considerable, minor
      特别重大、重大、较大、较小

四、信息安全事件分类分级

- ISO/IEC 27035:2011信息安全事件分级
  分级要素级别关系

可能存在（√） 不会存在（×）		信息系统重要性		
		特别重要	重要	一般
业务损失	特别严重	√	×	×
	严重	√	√	×
	较大	×	√	√
	较小	×	×	√

四、信息安全事件分类分级

- ISO/IEC 27035:2011信息安全事件分级
  事件级别及准则
  - Very serious (Class IV)/非常严重（Ⅳ级）
    - 特别重要信息系统 and
    - 特别严重业务损失 or
    - 特别重大社会影响
  - Serious (Class III)/严重（Ⅲ级）
    - 特别重要信息系统 or 重要信息系统 and
    - 严重业务损失 or
    - 重大社会影响

四、信息安全事件分类分级

- ISO/IEC 27035:2011信息安全事件分级
  事件级别及准则
  - Less serious (Class II)/不太严重（Ⅱ级）
    - 重要信息系统 or 一般信息系统 and
    - 较大业务损失 or
    - 较大社会影响
  - Small (Class I)/不严重（Ⅰ级）
    - 一般信息系统 and
    - 较小业务损失 or 无业务损失 and
    - 较小社会影响 or 无社会影响

四、信息安全事件分类分级

- 国家标准vs国际标准：信息安全事件分级
  分级要素及其级别

GB/Z 20986-2007	ISO/IEC 27035:2011
信息系统的重要程度： 特别重要、重要、一般	信息系统重要性： 特别重要、重要、一般
系统损失： 特别严重、严重、较大、较小	业务损失： 特别严重、严重、较大、较小
社会影响： 特别重大、重大、较大、一般	社会影响： 特别重大、重大、较大、较小

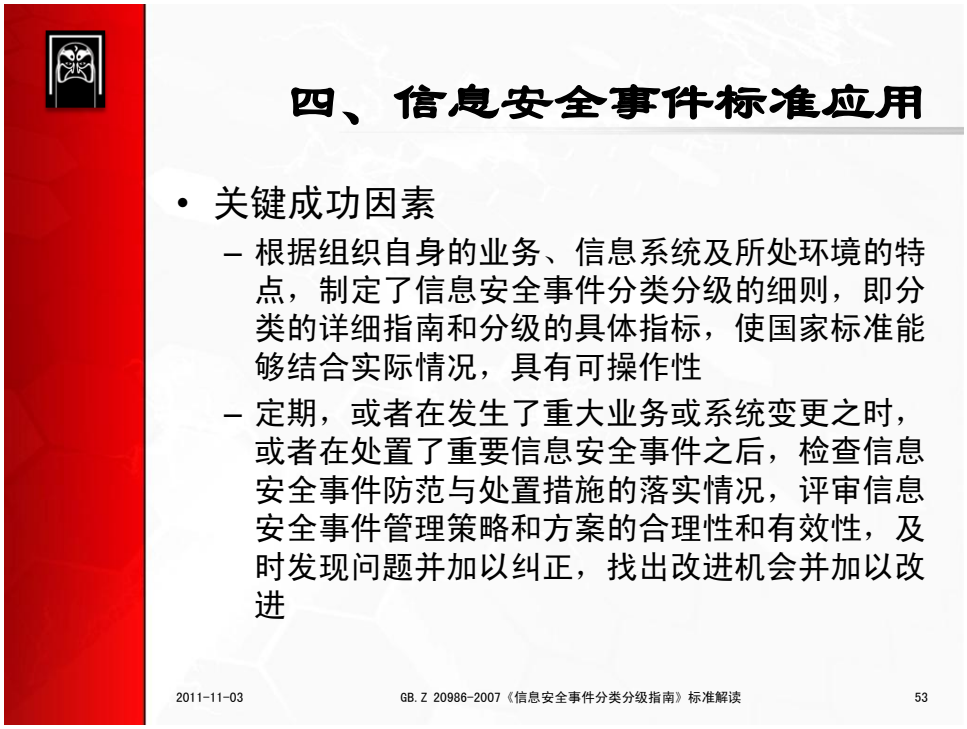
四、信息安全事件分类分级

- 国家标准vs国际标准：信息安全事件分级事件级别及准则

GB/Z 20986-2007	ISO/IEC 27035:2011
特别重大事件（Ⅰ级）	非常严重（Ⅳ级）
重大事件（Ⅱ级）	严重（Ⅲ级）
较大事件（Ⅲ级）	不太严重（Ⅱ级）
一般事件（Ⅳ级）	不严重（Ⅰ级）

四、信息安全事件标准应用

- 关键成功因素
  - 制定了信息安全事件管理策略和方案，并得到了组织最高管理层的批准和资源保障承诺
  - 向组织内外的所有相关人员强调了防范和响应信息安全事件的重要性，并告知了信息安全事件管理策略和方案，做到能够及时发现和报告可能的或明显的信息安全事件
  - 建立了信息安全事件响应小组(ISIRT)，并具备响应和处置各种信息安全事件的专业知识和技能，做到能够正确分析和判断信息安全事件的发生及其类别和级别，进而确定适合的应对措施


四、信息安全事件标准应用
• 关键成功因素
– 根据组织自身的业务、信息系统及所处环境的特点，制定了信息安全事件分类分级的细则，即分类的详细指南和分级的具体指标，使国家标准能够结合实际情况，具有可操作性
– 定期，或者在发生了重大业务或系统变更之时，或者在处置了重要信息安全事件之后，检查信息安全事件防范与处置措施的落实情况，评审信息安全事件管理策略和方案的合理性和有效性，及时发现问题并加以纠正，找出改进机会并加以改进
2011-11-03
GB. Z 20986-2007《信息安全事件分类分级指南》标准解读
53


谢谢！
www.30wish.net