2011中国最佳呼叫中心
CHINA CONTACT CENTER AWARD 2011

呼叫中心信息安全保护

胡铁君 教授

中国信息安全测评中心
广东测评中心

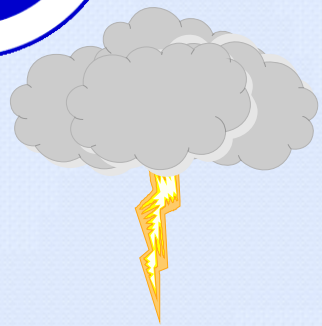
www.itsec.gov.cn

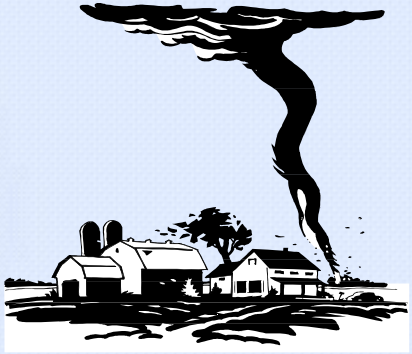
中国电子商会
呼叫中心与客户关系管理专业委员会
China Call Center&CRM Association

我国信息安全领域
主要安全威胁来源分析

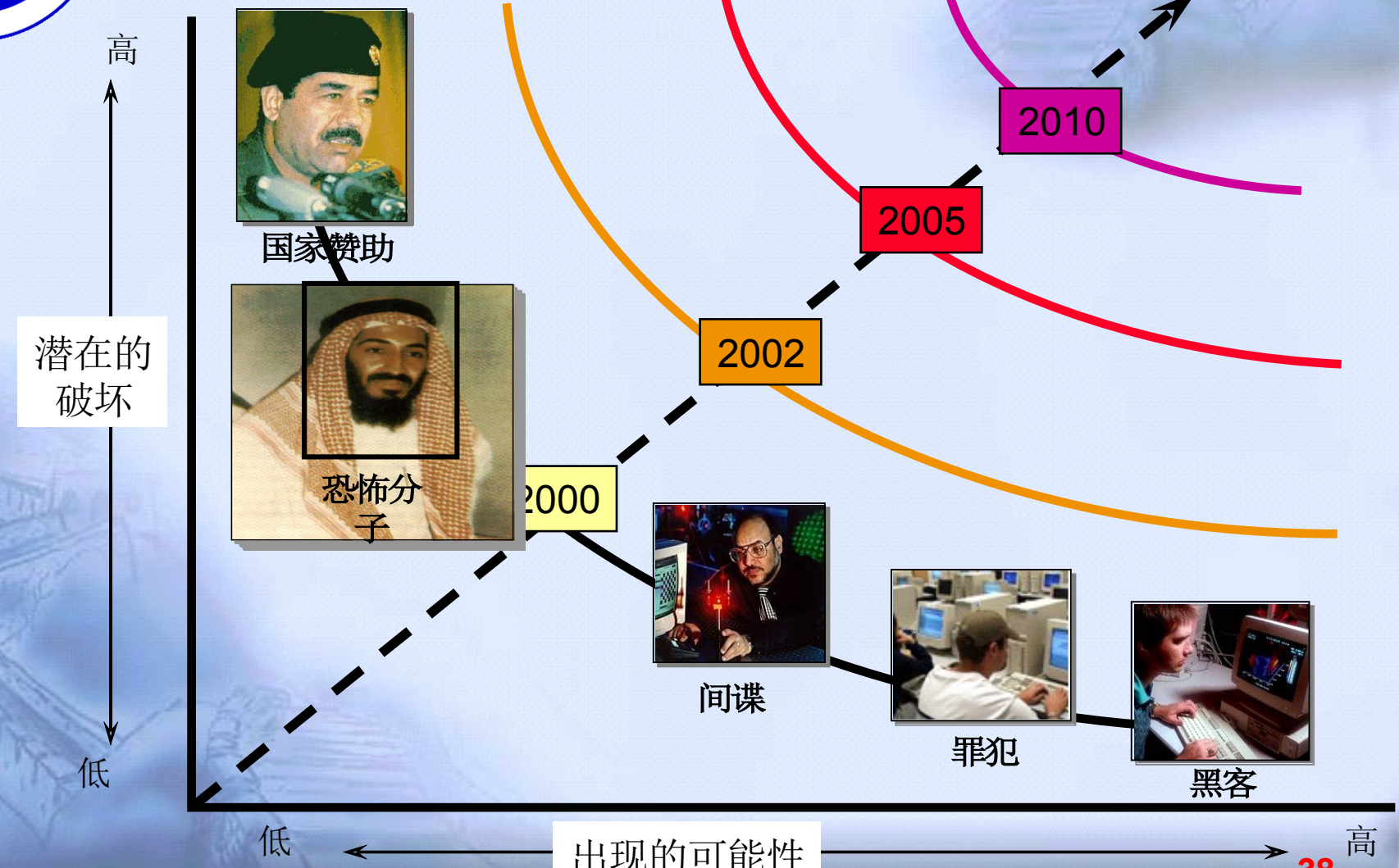
- 主要威胁源：人为破坏、自然灾害
- 不同组织或个人的动机、能力和掌握的资源各不相同
  - 发泄不满情绪者
  - 黑客组织或个人
  - 疆独、藏独、台独、民运、法轮功
  - 国际恐怖组织
  - 西方反华势力
  - 境外间谍情报机构

威胁的来源：人、自然环境



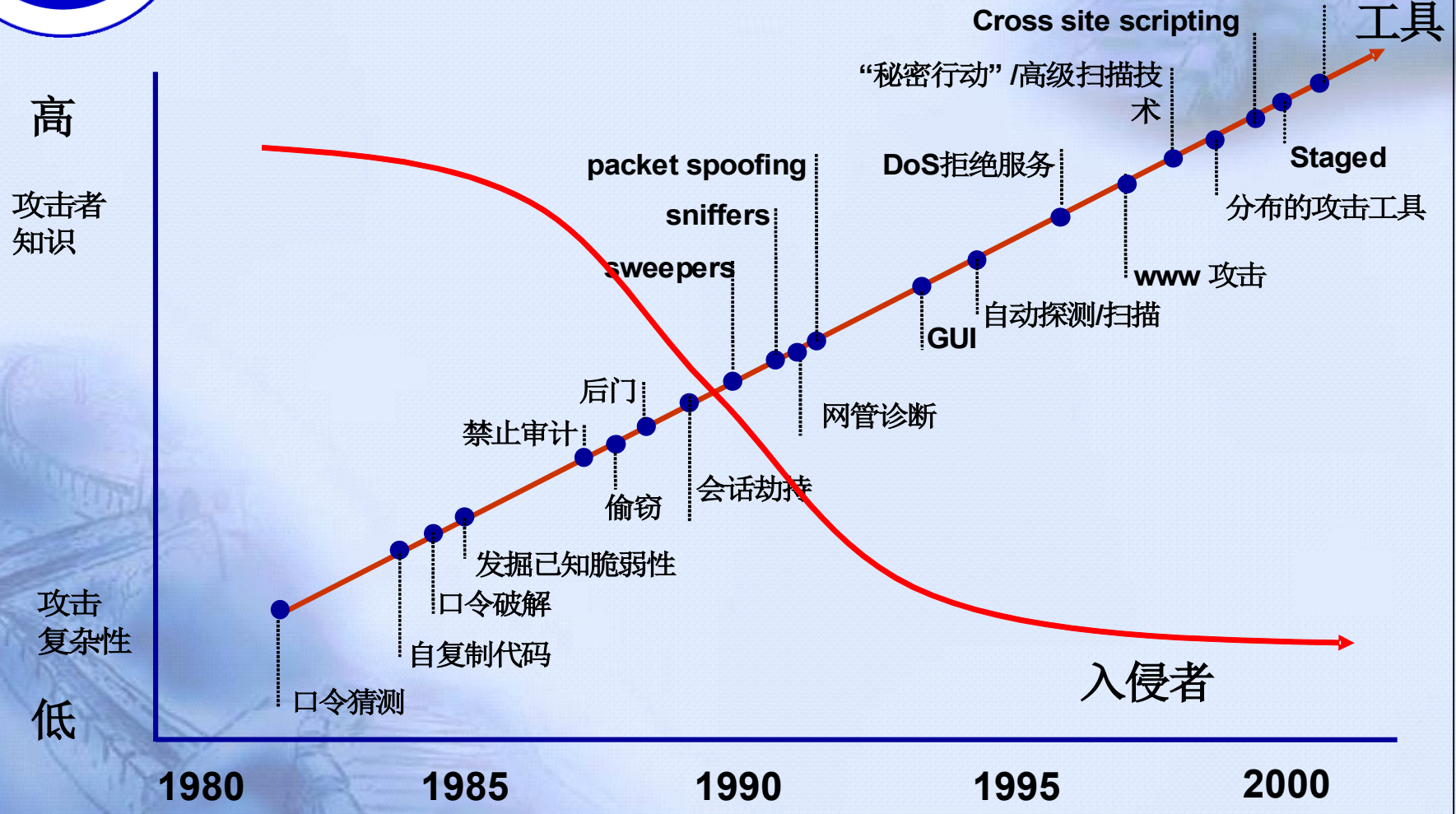


不断增加的外部安全威胁



来源: DSB研究报告

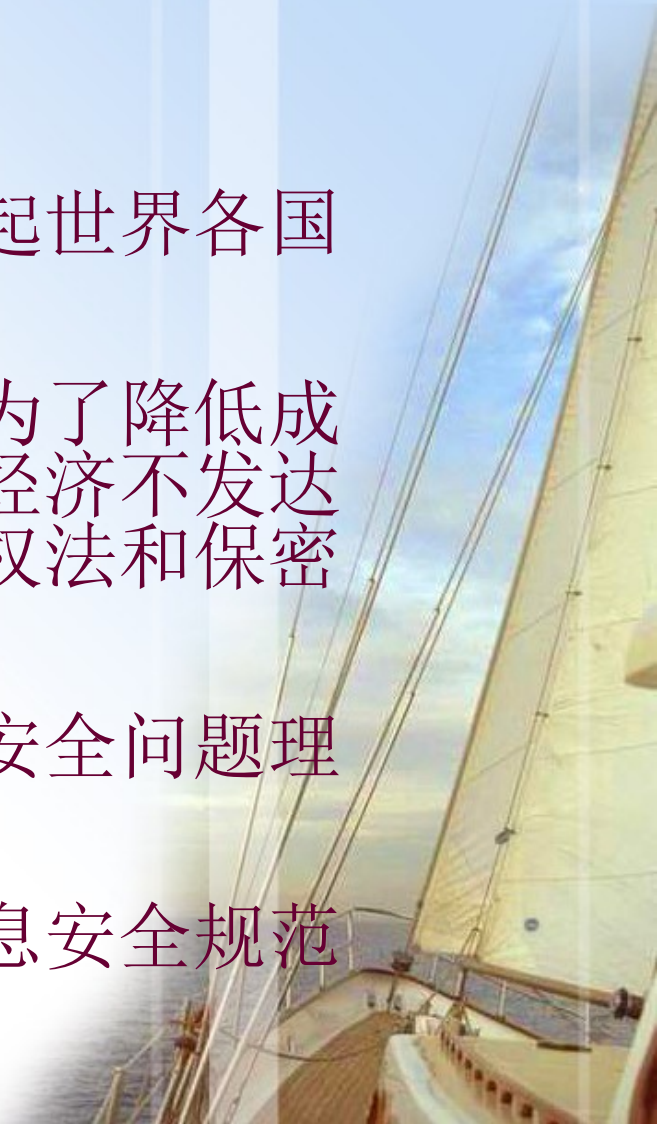
攻击复杂性vs入侵者技术知识能力



资料来源：CERT Coordination Center

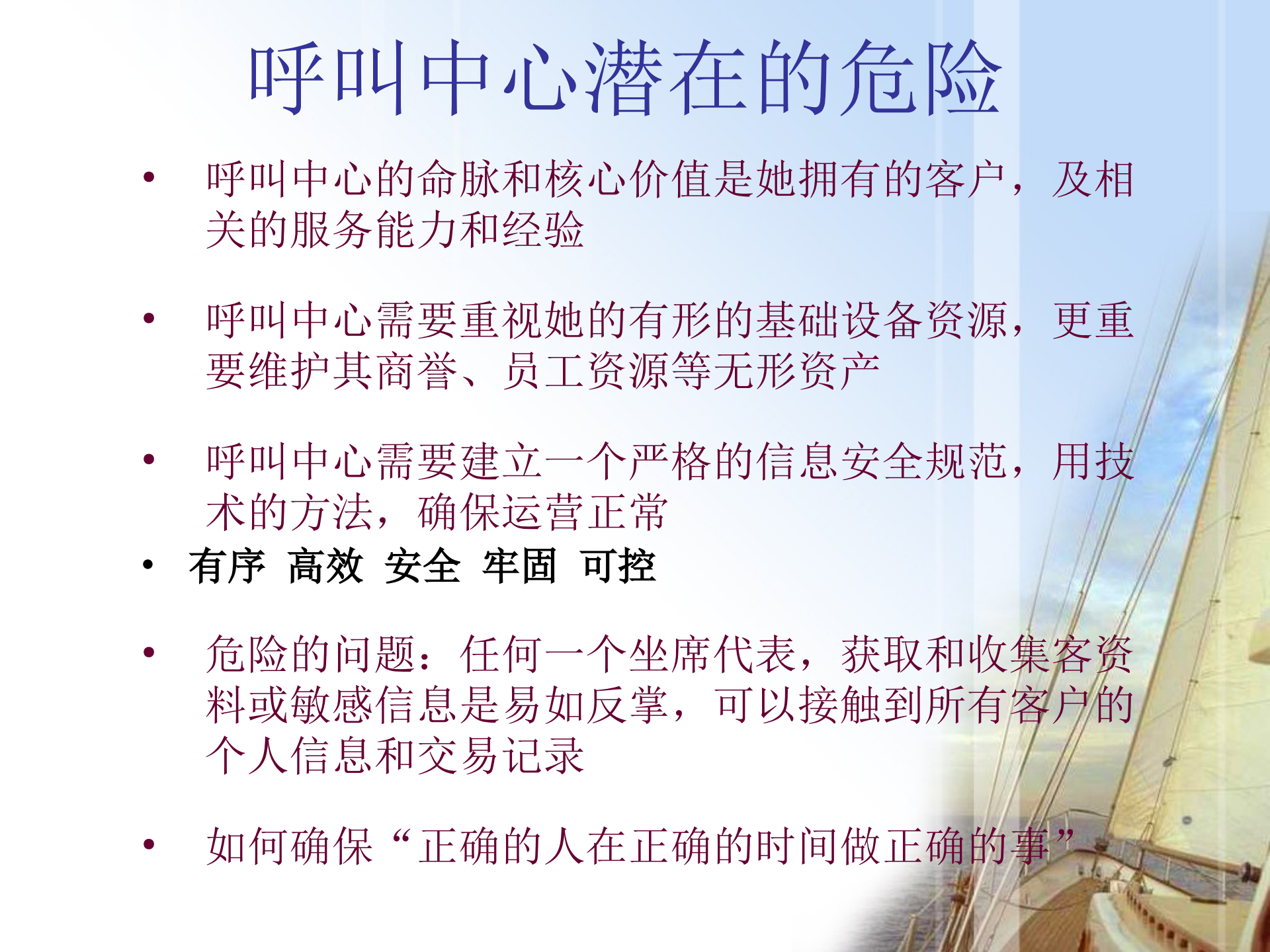
呼叫中心的信息安全

- 呼叫中心安全问题至关重要
- 任何机密的客户信息丢失
- 有可能要承担着巨大的法律风险
- 信息安全问题越来越多，引起世界各国的密切关注
- 经济发达国家的呼叫中心，为了降低成本，把呼叫中心业务转移到经济不发达国家，但这些国家的知识产权法和保密法规并不是严格
- 呼叫中心的管理人员对信息安全问题理解水平
- 没有一套完善的呼叫中心信息安全规范



呼叫中心潜在的危险

- 呼叫中心的命脉和核心价值是她拥有的客户，及相关的服务能力和经验
- 呼叫中心需要重视她的有形的基础设备资源，更重要维护其商誉、员工资源等无形资产
- 呼叫中心需要建立一个严格的信息安全规范，用技术的方法，确保运营正常
- **有序 高效 安全 牢固 可控**
- 危险的问题：任何一个坐席代表，获取和收集客资料或敏感信息是易如反掌，可以接触到所有客户的个人信息和交易记录
- 如何确保“正确的人在正确的时间做正确的事”



计算机带来的信息安全问题

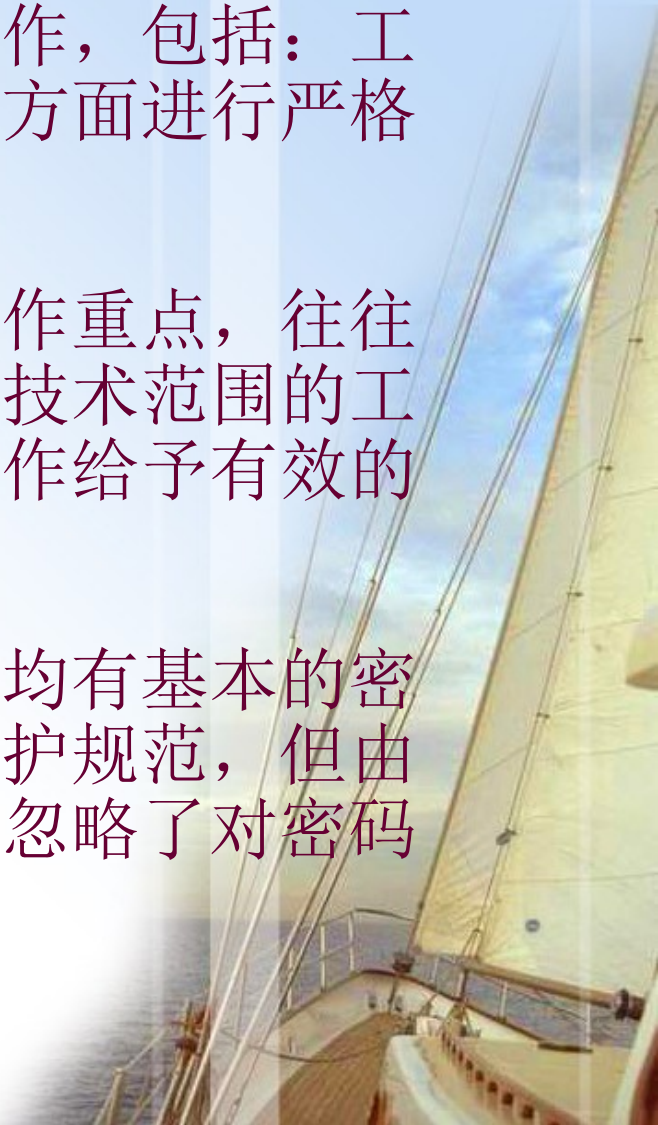
- 呼叫中心业务需要借助计算机完成
- 计算机数据安全保护成为呼叫中心的信息安全的工作重点
- 业务核心数据会聚到呼叫中心的平台，涉及比较敏感的数据，数据中心的安全问题需要更高的要求
- 银行的信用卡业务
- 保险公司
- 证券公司
- 计算机技术的变化引起的安全问题
- 开放性，
- 结构标准化，
- 网络化，
- 普及化
- 业务数据处理的安全问题、
- 传输和存储
- 数据丢失、泄漏
- 人为破坏、窜改
- 计算机病毒的感染
- 网络黑客的袭击

计算机带来的信息安全问题

- 电子数据作为业务信息处理的主要载体，保存了企业或客户的机密数据
  - 计算机硬体，网络，文件
  - 工作人员笔记本电脑
  - 移动存储介体
- 建立数据安全规范的同时，需要满足数据使用的特殊性
  - 保密性
  - 可控性
  - 可用性
  - 完整性
  - 易用性

数据安全管理规范

- 全面统筹的呼叫中心数据保护工作，包括：工作人员，工作流程，技术设施等方面进行严格管理。
- 许多呼叫中心把生产业务视为工作重点，往往认为信息安全的管理，属于工程技术范围的工作，没有对企业整个数据保护工作给予有效的支持。
- 密码管理准则，许多呼叫中心，均有基本的密码使用和管理方法等信息安全保护规范，但由于呼叫中心的人员流动性很大，忽略了对密码进行严格管理，如同虚设。



数据安全管理规范

- 呼叫中心需要建立一个有效的数据保护机制
- 重点集中在客户、财务、及呼叫中心业务有关的知识产权方面。
- 建立完善的数据保护目录，包括公开的数据、内部的数据和保密的数据，列明使用这些数据的规范
- 为客户提供服务
- 满足业务的需要
- 防止一些敏感信息泄露
- 有效控制和保护

安全的数据使用流程

- 制定一个严格的数据结构，
- 为业务建立一套严格的数据安全使用流程
- 例如，信用卡服务热线中心的数据管理，按照信用卡行业的安全管理标准而制定的数据管理方法
- 严格的流程确保

- 数据使用方便同时对数据进行有效的保护
- 即使网络被黑客闯入，也不能盗窃信用卡的完整资料

业务系统开发的问题

- 保护数据的安全措施和安全认证机制
- 由软件程序编写员设计
- 程序员编写程序的重点是针对应用系统的逻辑功能，
- 对系统的安全架构没有足够的认识。为避免程序开发过程出现漏洞，

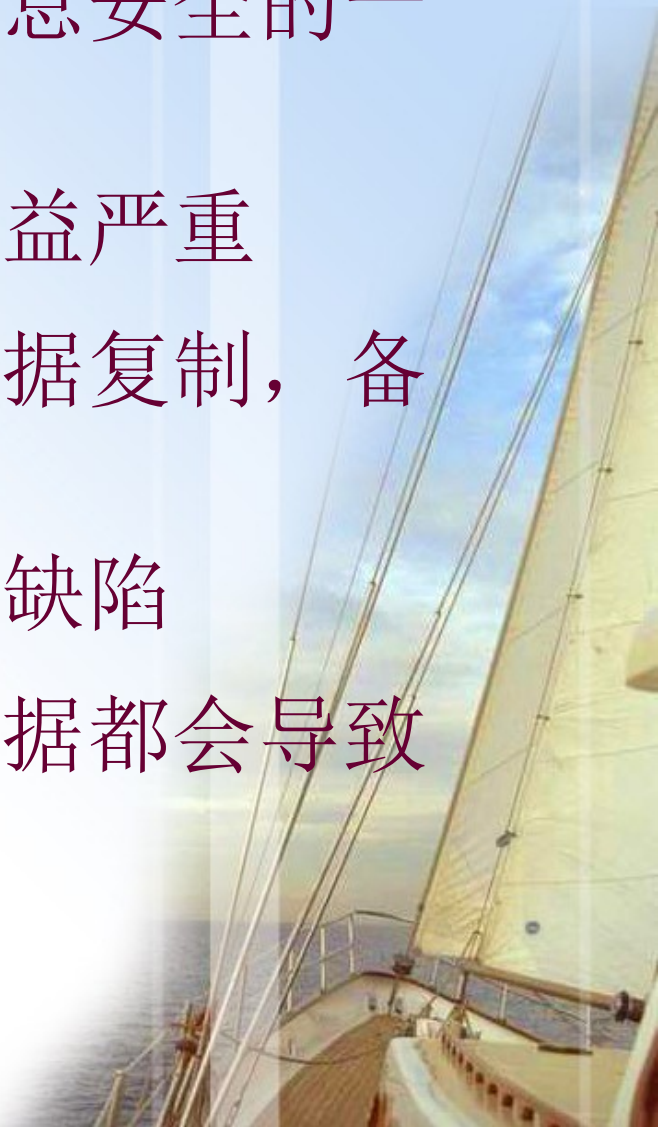
- 开发软件之前
- 对程序员进行信息安全培训

- 程序开发完成后
- 通过专用的二进制代码分析工具对程序代码进行安全检测

- 软件交付使用前消除安全隐患

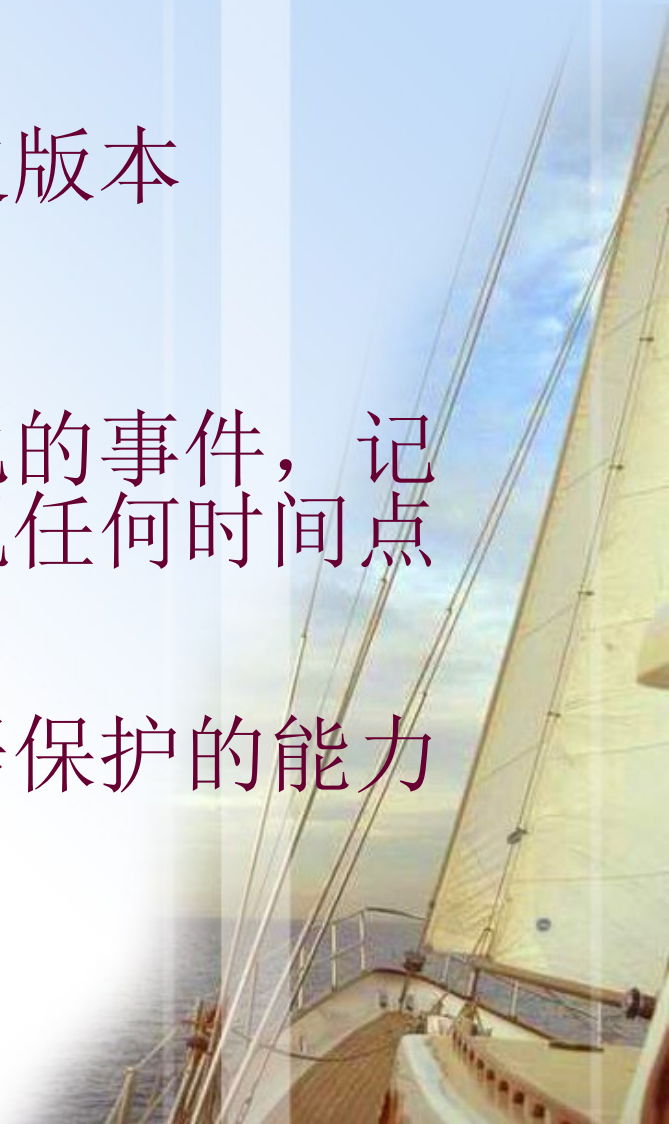
呼叫中心容灾能力

- 呼叫中心容灾能力，是信息安全的一个重要问题
- 数据丢失所造成的损失日益严重
- 一般容灾的方法是采用数据复制，备份，恢复等保护技术
- 固定时间的备份方法存有缺陷
- 短时间的停机或者丢失数据都会导致巨大的损失



呼叫中心容灾能力

- 呼传统的数据备份技术
- 自动建立文件操作的历史版本
- 连续数据保护技术
- 捕捉文件系统的数据变化的事件，记录文件的变化信息，实现任何时间点的文件恢复
- 恢复的精细程度衡量数据保护的能力



呼机中心容灾能力

- 建立完善的应急防护手段信息系统的备份与恢复体系，在紧急情况下将损失减到最低

- 灾难恢复设施的设立问题
- 忽略了对业务和数据的重要程度进行分析
- 快速恢复的计划没有按照业务的重要性安排次序

- 解决方法是对业务进行灾难影响的评估
- 那些业务进程关系到企业的生存命脉
- 那些业务进程可以慢慢恢复

- 不是由 IT 部门负责安排，而是由相关的业务部门的使用者、公司的风险评估部门和使用数据的业务人员作出裁定。

- 相关的容灾恢复的投资预算，根据业务的需求，选择合理的灾难恢复时间和资源投放的平衡点。

数据库技术发展的安全问题

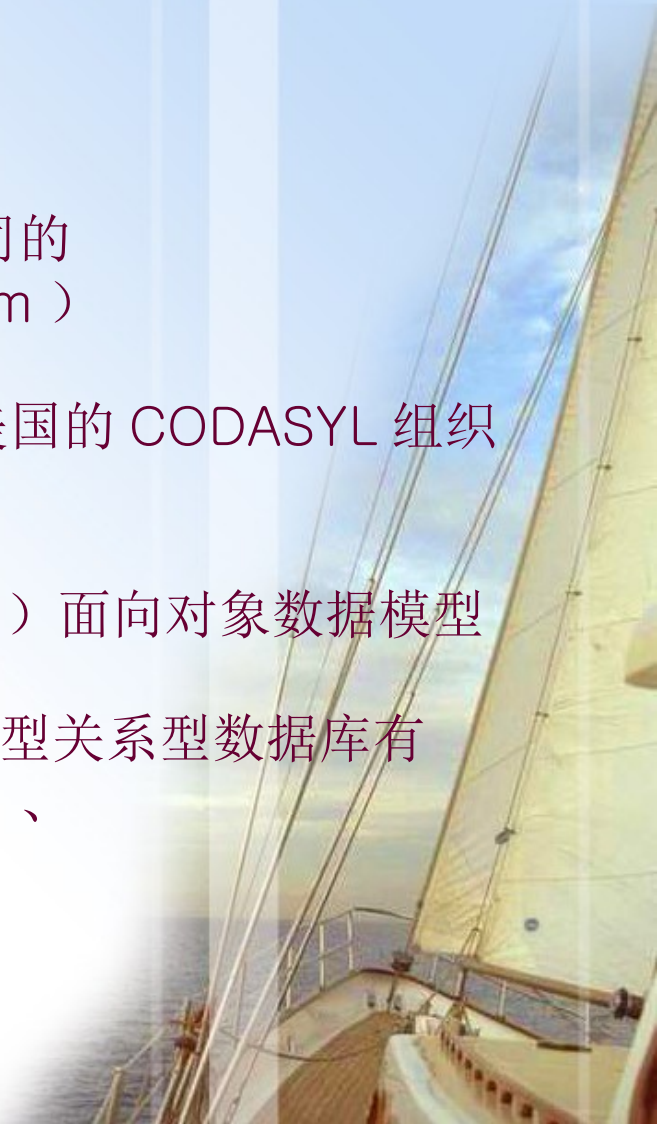
- 传统数据库

- 层次模型 hierarchical model ） IBM 公司的 IMS （ Information Management System ）

- 网状模型（ network model ） 1969 年美国的 CODASYL 组织提 DBTG 系统

- 面向对象模型（ object-oriented model ）面向对象数据模型

- 关系模型（ relational model ）流行的大型关系型数据库有 IBM DB2 、 IBM UDB 、 Oracle 、 SQL 、 Server 、 SyBase 、 Informix 等。



数据库技术发展的安全问题

云计算数据安全

Hadoop

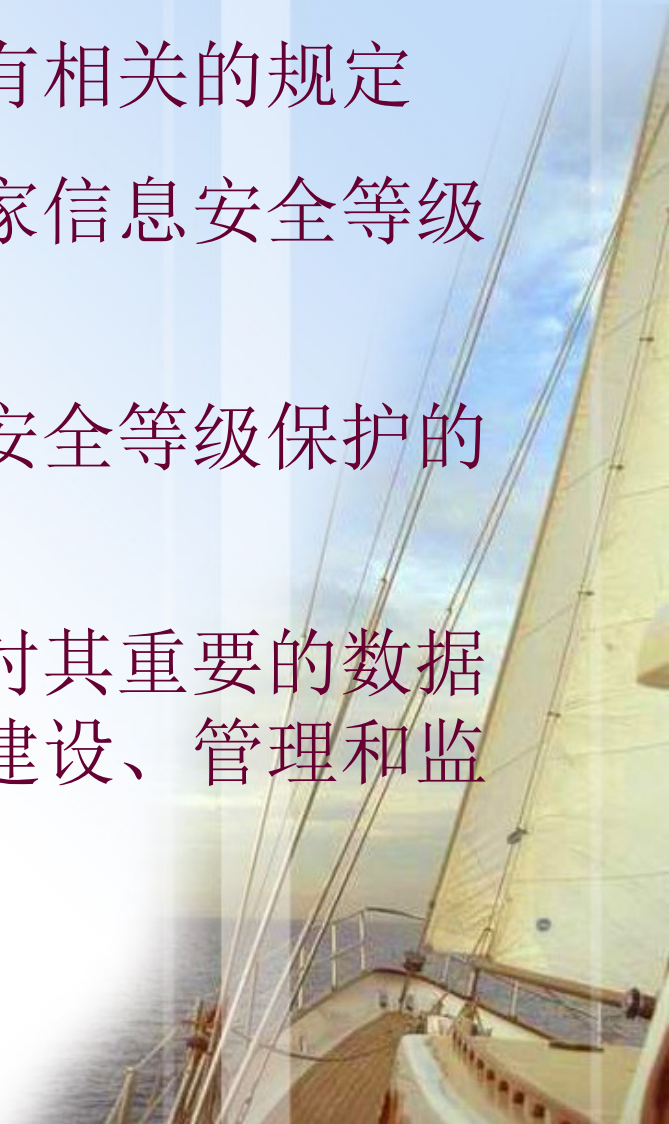
Google， Micorsoft 在 Internet 上对搜索关键字进行内容分类的工具，可以解决许多要求极大伸缩性的数据需求

NoSQL

eBay， Twitter， AmazonS3 的经验是建立在硬盘、机器和网络都会失效这些假设之上的数据结构，系统能够在即使非常极端的条件下也能应付这些失效

国家的信息安全管理规定

- 国家对信息系统的安全管理有相关的规定
- 重要的信息系统必须纳入国家信息安全等级保护。
- 呼叫中心可以按照国家信息安全等级保护的基础原则
- 围绕呼叫中心的业务流程，对其重要的数据进行等级划分，按标准进行建设、管理和监督。

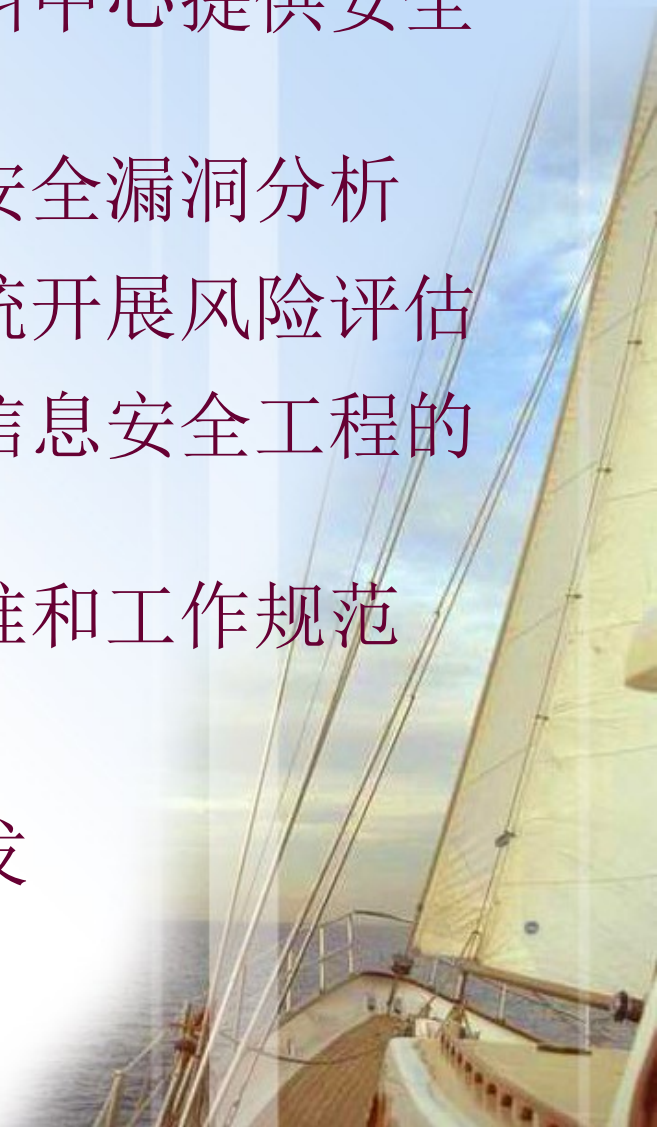


我国信息安全相关法规

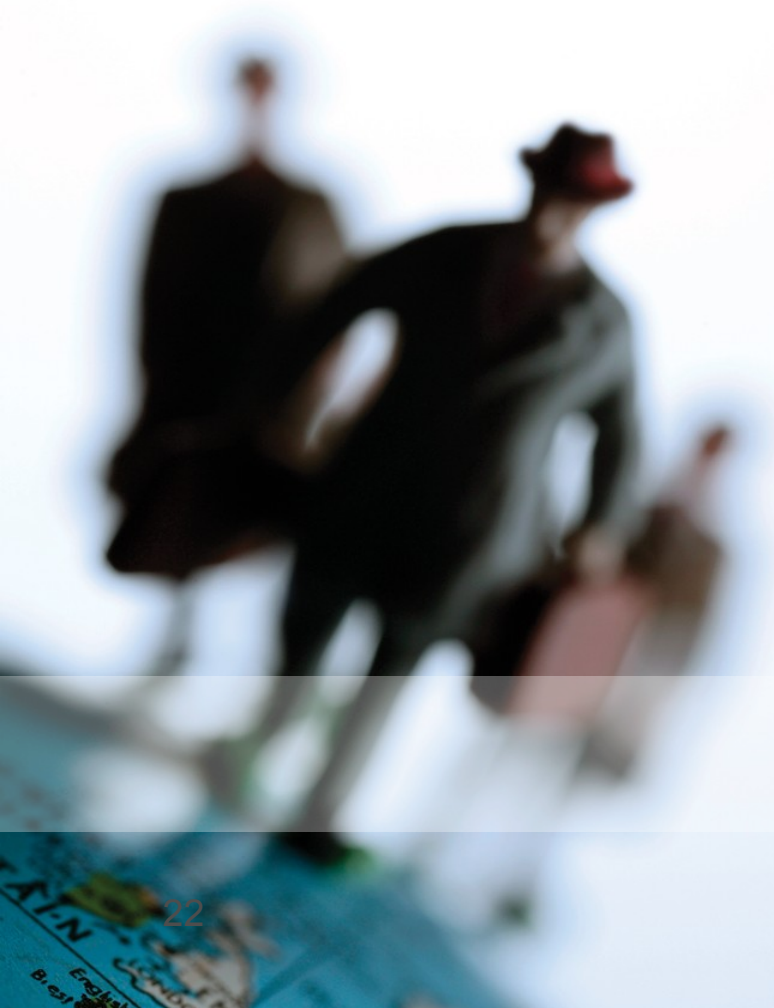
- 《中华人民共和国计算机信息系统安全保护条例》（国务院令第147号）(1994-02-18)
- 《中华人民共和国计算机信息网络国际联网管理暂行规定》（国务院令第195号）(1996-02-01)
- 《计算机信息系统安全专用产品检测和销售许可证管理办法》（公安部令第32号）(1997-12-12)
- 《计算机信息网络国际联网安全保护管理办法》（公安部令第33号）(1997-12-30)
- 《计算机病毒防治管理办法》（公安部令第51号）(2000-04-26)
- 《互联网信息服务管理办法》（国务院令第292号）(2000-09-20)
- 《互联网电子公告服务管理规定》(2000-11-07)
- 《互联网安全保护技术措施规定》（公安部令第82号）(2006-03-01)
- 《信息安全等级保护管理办法》（公通字[2007]43号）(2007-06-22)
- 《广东省计算机信息系统安全保护条例》 2008年2月
- 2010年9月“国家标准化管理委员会批准18项信息安全技术国家标准”

国家信息安全测评机构

- 国家信息安全测评中心为呼叫中心提供安全测评服务
- 负责信息安全产品和系统的安全漏洞分析
- 面向重要信息网络和信息系统开展风险评估
- 开展信息技术产品，系统和信息安全工程的测试评估
- 制定信息安全测评的相关标准和工作规范
- 信息安全服务资质审核
- 信息安全测评理论研究和开发



谁可以帮忙？



坚持积极防御、综合防范，探索

把握信息化与信息安全的内在规律

主动应对信息安全挑战

保障客户信息安全的服务

创造客户价值、创造社会价值

为客户及国家的信息化建设提供安全保障

“服务创造价值，进取成就客户”

www.itsec.gov.cn