数据库保护：建立一个安全健康的数据库环境

孟国伟，首席顾问

SZBOWEB Company Limited

内容分布

- 三部份
- 第一部份
  - 序言：数据保护
- 第二部份
  - 主题：建立安全环境
- 第三部份
  - 结语：行业发展

以下数字暗示什么？

Source: Enterprise Strategy Group

43% 的数据库保存关键数据

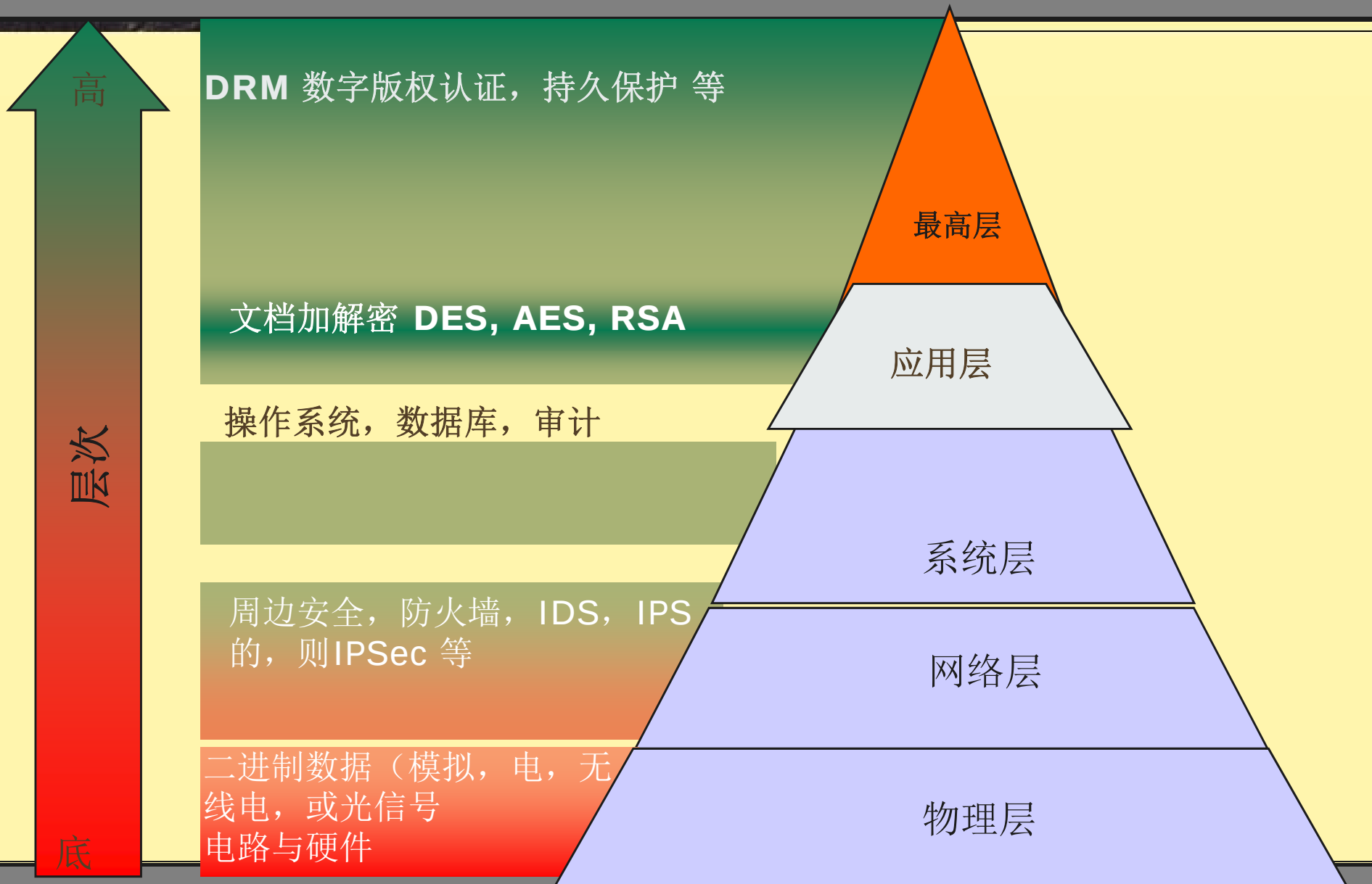
84% 的公司认为数据库安全已足够

56%的公司在之前一年曾出现安全事件

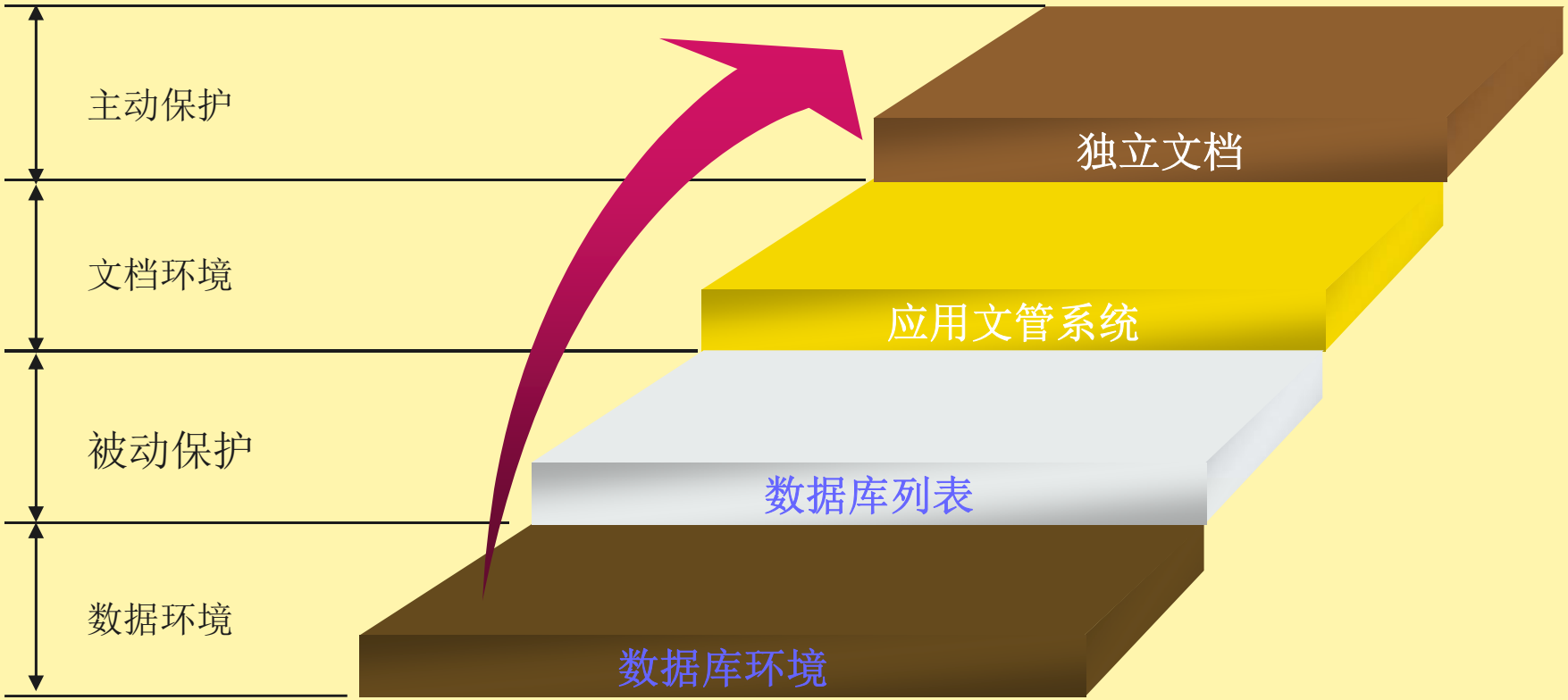
73%的公司预计数据库攻击会增加

错误观念，感觉安全不如知道已经安全

第一部份：数据保护


高
层次
底
DRM 数字版权认证，持久保护 等
文档加解密 DES, AES, RSA
操作系统，数据库，审计
周边安全，防火墙，IDS，IPS
的，则IPSec 等
二进制数据（模拟，电，无
线电，或光信号
电路与硬件
最高层
应用层
系统层
网络层
物理层

第一部份：数据保护



第二部份：建立健康的数据库环境

第二部份：建立健康的数据环境

- 四个部份
- 第一部份
  - 访问控制
- 第二部份
  - 应用程序的完整性
- 第三部份
  - 识别或密码控制
- 第四部份
  - 操作系统的完整性

健康环境：访问控制

- 处理决定那些用户可以执行那些操作
  - 例如：读，更新，更改，执行 等
- 设计概念是限制：
  - 权力
  - 没有被授权的用户
- 目的是：
  - 控制已授权用户的权限
- 内部威胁
  - 内部数字犯罪趋势增加
  - 例如：程序员，管理员，外包员工，临时，商业间谍 等
- 外部威胁
  - 不能只注重外来威胁
  - 权力适当分配

访问控制：Oracle 实例

- Privilege on database link table
  - 找出对 SYS.LINK$ 表有读或修改权限的用户或角色
- SYS.LINK$ 表包含一些用来访问数据库连接的密码，这些密码以原文存在
  - 对这个表的访问必须严密控制
  - 任何一个用户可以利用这些信息去访问远程的数据库
- 数据库连接是 Oracle里边对远程数据库的一个指针 Pointer
  - 包含远程数据库的一些位置信息，在哪里
- SYS.LINK$ 表包括六个列
  - USERNAME,PASSWORD,AUTHUSR, AUTHPWD, PASSWORDX, AUTHPWDX
  - 明文或者容易被解密
- 审查那些用户可以访问 SYS.LINK$，撤销某些用户权限如下：
  - Revoke [permission] on SYS.LINK$ FROM [username/role]

健康环境：应用程序的完整性

- 指的是：
  - 一个完整，真正的状态
- 如果完整性受损：
  - 安全功能无效
  - 没意义
- 例如：
  - 安装了木马
- 如何保证完整性
  - 审计日志完整
  - 没有可以超越审计的机制

应用程序的完整性 MSSQL实例

- Global Temp stored Procedure
  - 检查这个程序是否存在 tempdb 数据库
- 每个人都可以修改这个程序
  - 允许攻击者在程序里插入自己的命令, 控制ＳＱＬ服务器
  - 当另外一个用户运行已加入命令的程序时，造成攻击者权限增加或改变
- 它可以利用#&##前缀创建
  - 创建 proc ## test as select 1
  - 允许 Public 组 读, 执行和写的权限
- 任何一个用户可以改或加上自己的命令：
  - Alter proc ## test as EXEC sp_addsrvrolemember ”attacker” “sysadmin”” select 1
  - 攻击者的权限会因此改变，扩大，在下一次这个程序被执行之后
- 不建议使用这个程序

应用程序的完整性 Oracle 实例

- Database link buffer overflow
  - 断定当对数据库连接运行SELECT命令时数据库是否存在缓冲区溢出
- 允许攻击者覆盖堆栈（zhan）和执行任意代码
  - 当对一个定义长字符串的数据库连接运行 SELECT 命令时出现
- 数据库连接 DB link 是一个 Oracle 机制，提供在对另外一个数据库读取数据时的位置透明
  - 到另一个数据库的指针
  - 在数据字典中的条目包括远程服务器，连接字符串，来验证远程系统的用户名和密码的名称
- 用以下命令行创建：
  - CREATE DATABASE LINK [linkname] CONNECT TO [username] IDENTIFIED BY [password] USING '[connection string]'
- 如果字符串超过 1000，在数据字典保留，当运行SELECT命令时溢出便会出现
  - SELECT *FROM TEST@[linkname]
  - 不会造成数据库崩溃，但会造成远程服务器地址被覆盖
  - 必须要有 CONNECT角色特权
  - 采用最新补丁

健康环境：识别或密码控制

- 密码强度认证
  - 复杂度，位数
- 密码过期
  - 有效期
  - 更换
- 目的是：
  - 限制，减少密码被破解的机率
- 多强才算安全
  - 根据实际情况
  - 易于管理，接受

识别或密码控制 Oracle实例

- Easily guessed DB password
  - 把从密码哈希字典的哈希和数据库做比较而猜出密码
- 密码攻击：
  - 在密码字典提取一个字
  - 一个一个试
  - 如果密码和字典一样，密码猜测成功
- 允许多长时间
  - 60 天, 90 天, 密码强度必须相对应
- 最有效： 设置 FAILED_LOGIN_ATTEMPTS =10次
  - 最少八个字长
  - 在字典找不到
  - 结合数字，字母，特殊字符

健康环境：操作系统的完整性

- 应用依赖操作系统

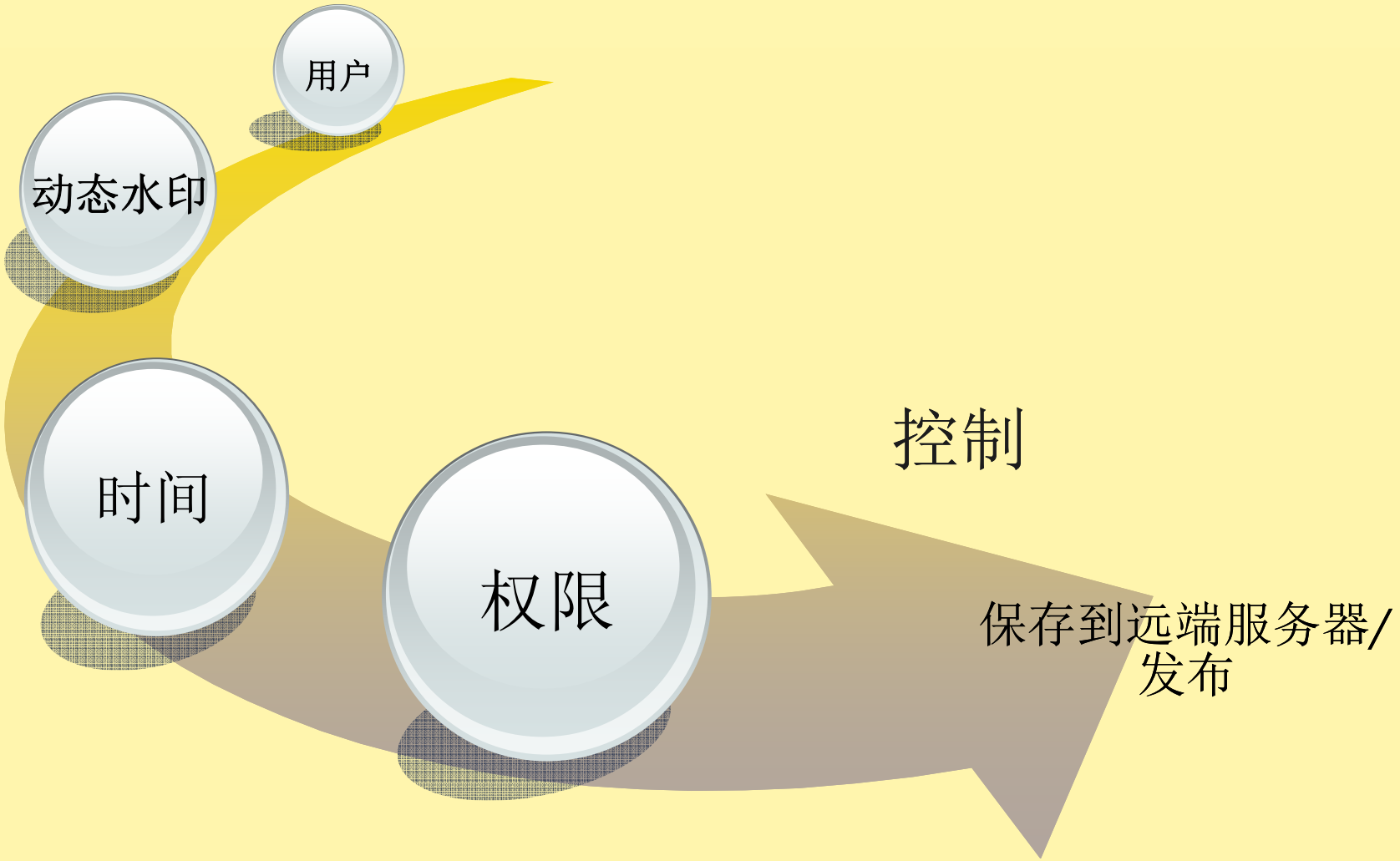
- 操作系统出现问题：
  - 安全机制会被绕过
  - 不可靠
- 目的是：
  - 找出和应用相关的安全问题
- 例如：
  - Setuid
  - 文件权限设置
- 不能让 OS 用户控制数据库，相反不能让数据库用户控制 OS

操作系统的完整性 MSSQL实例

- Registry permission
  - 检查过多的权限没有被授予对mssql 的注册表/值
- 只有某些授权的操作系统用户才可以有访问 MSSQL注册表/值的权限
  - 否则操作系统用户会很容易攻击 MSSQL 服务器
- MSSQL利用一套注册表去管理 SQL 服务器
  - 必须有严格的访问控制权限
  - 如果控制不严，会造成来自操作系统用户的攻击
  - 不可以授权给 built-in user Everyone 用户组
- 取消过多权限如下：
  - 运行 regedit.exe,导航到问题发生处
  - 右键点击改变的项目
  - 选择 “permission”
  - 取消 Everyone 组的任何一个人

第三部份：结语 行业发展

静态数据保护介绍



中文简介

TCP retransmissions on very lousy net

技 术 简 介

随着政府部门电子政务和企业电子商务的推进，政府和企
络的信息化平台，人们通过互联网浏览器就可以处理日常的
程数据共享管理和控制技术手段成为必然。

当前，对于企业和政府而言，拥有一套让管理者和员工无
位重要数据文档信息的安全管理系统，使这些敏感和重要信
到安全有效的管理控制和保护，减小集体的安全风险，提高
孜孜追求的目标。同时，频频出现的计算机网络泄密事件也给

动态数据保护介绍： 数据库安全生命周期

生命周期部分	目的
发现	寻找数据库
分类	选择那个数据库载有重要数据
评估	数据库漏洞扫描，配置和缺陷分析
排优先次序	已找出问题，比较好坏
修补	制造SQL语句修补问题，更新补丁，生成新监控政策增加监管度
监控	非法，擅自入侵监控，可疑，不平常行为监控

- 多谢各位！
- 联系我们：
  - larry@szboweb.com
  - www.szboweb.com
  - www.egoseal.com.cn