ISAT网络安全意识

第1课 数据安全

国家网络安全意识培训

数据安全

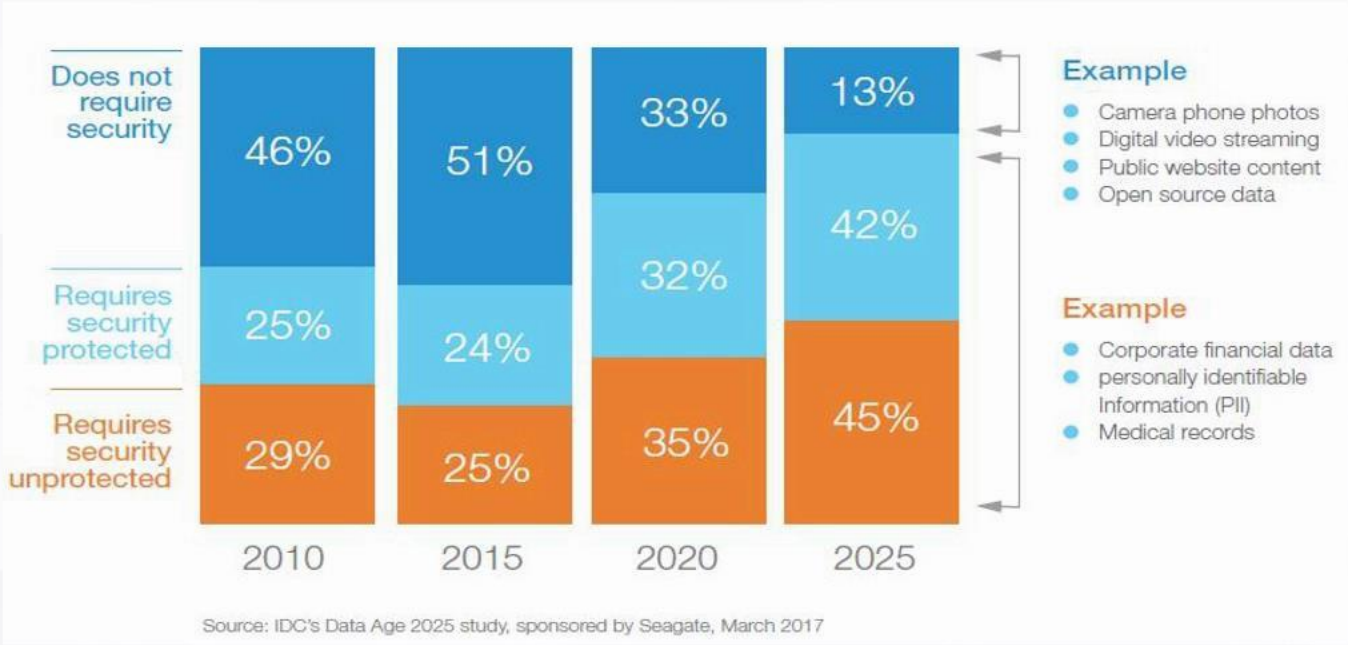
数据安全重要性

互联网时代，大量的数据被生产出来

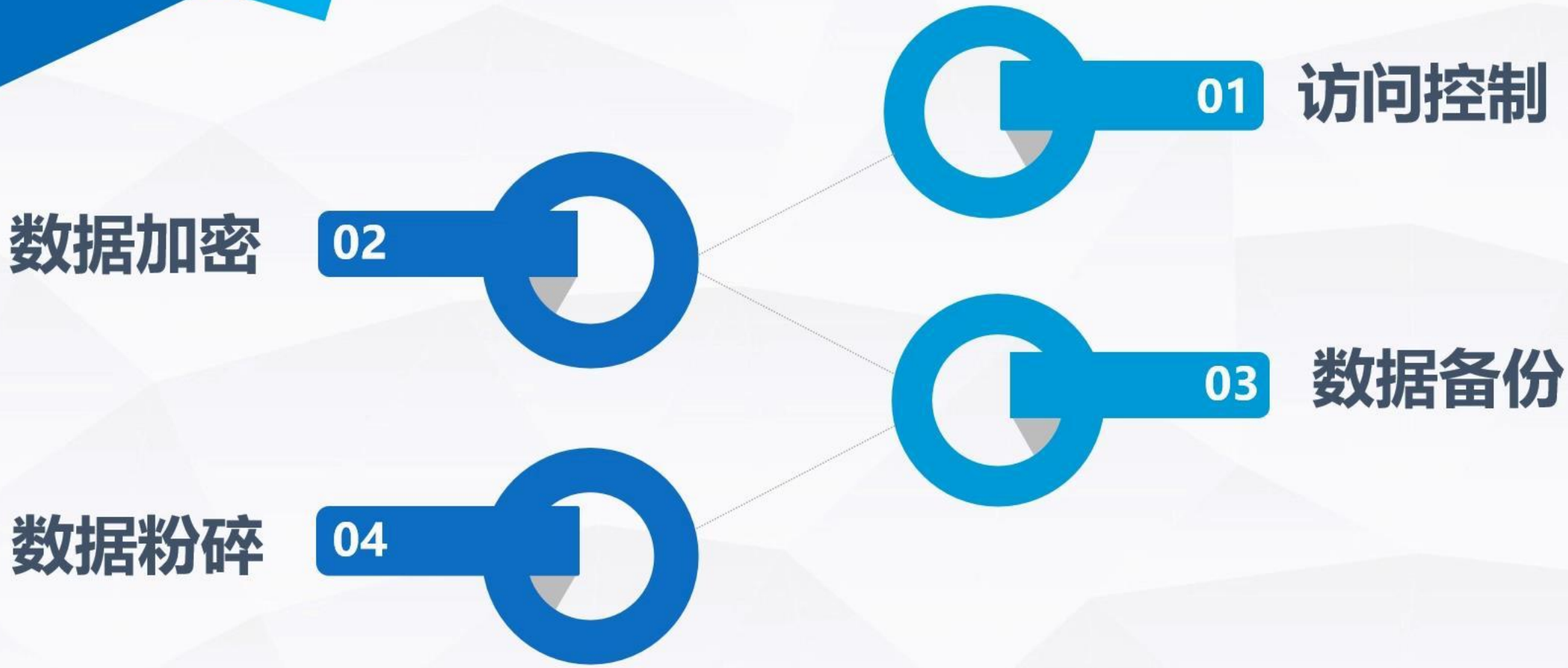
数据都是有价值的

数据面临各种安全风险

- **数据泄漏**
  设备丢失、被盗
  非法恢复
- **数据丢失**
  设备故障
  误操作
- **数据篡改**



数据安全防护措施



访问控制—确保只有授权人才能访问

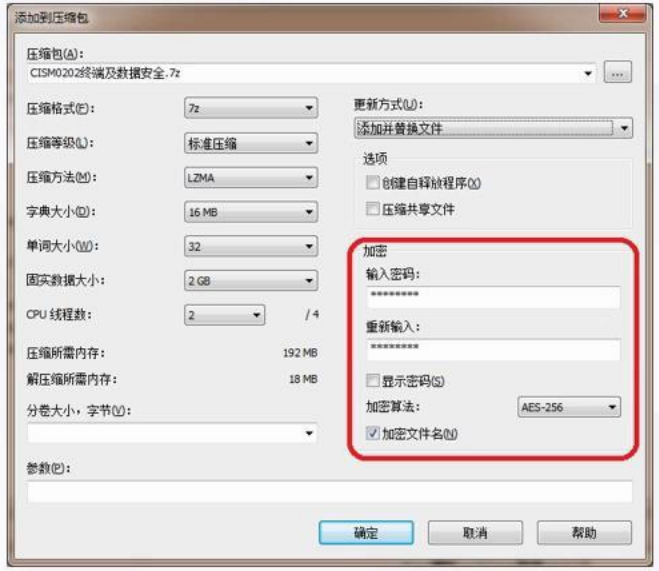
操作系统层访问

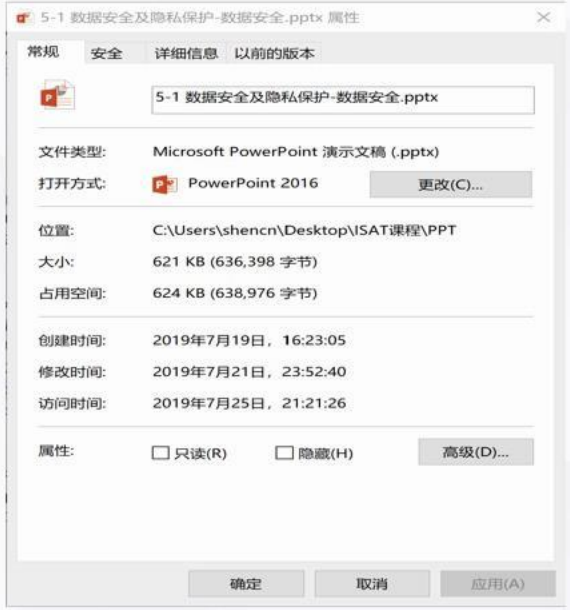
- 文件夹、文件中的安全属性可设置访问权限
- 系统内置访问控制，依赖操作系统的用户和权限管理体系

访问控制—确保只有被授权的人才能访问

文件层的访问控制

使用压缩软件提供的解压密码，压缩软件可在压缩时设置解压密码，只有提供正确的密码才能解开压缩的文件。
使用文档自带的密码保护功能， Office、WPS等文档软件可以设置保护，只有提供正确的密码才能打开文档。





数据加密—有效的应对数据泄露问题

数据加密价值

- 看不懂：没有密钥无法查看数据

数据加密的实现（Bitlocker）

- Windows系统内置
- 可对整个硬盘或分区进行加密
- 可对应硬盘丢失问题

数据备份—确保数据不会丢失

数据备份价值

- 避免数据丢失

数据备份实现

- 手工操作
- 专业工具
- 脚本执行

数据备份实现

- U盘、固态硬盘
- 光盘
- 硬盘
- 云盘

数据粉碎—确保数据不会被非法恢复

数据粉碎价值

- 避免数据非法还原（正常的删除文件、格式化硬盘的数据可被还原）

需要进行数据粉碎的情况

- 敏感数据的删除、存储敏感数据介质格式化
- 存储敏感数据的存储介质废弃
- 存储敏感数据的设备维修/借用

更彻底的方法：物理破坏、电子消磁

数据粉碎实现

原理：反复覆盖

- Gutmann算法 35次，理论上绝对无法恢复
- 美国国防部硬盘数据擦除标准（DOD）5220.22-M/ 我国保密局BMB21-2007标准：7次，基本无法恢复
- 其他要求：3次、1次等

文件粉碎操作（使用文件粉碎软件）

- PGP Shedder
- Eraser

数据安全小结

1、数据面临的风险是数据泄露、数据丢失和数据篡改；

2、给我们的系统和设备做好用户的权限管理；

3、给敏感数据加密；

4、重要数据要备份；

5、需要删除的敏感数据要做数据粉碎。

树立网安意识
构筑网络空间安全人民防线

谢谢观赏