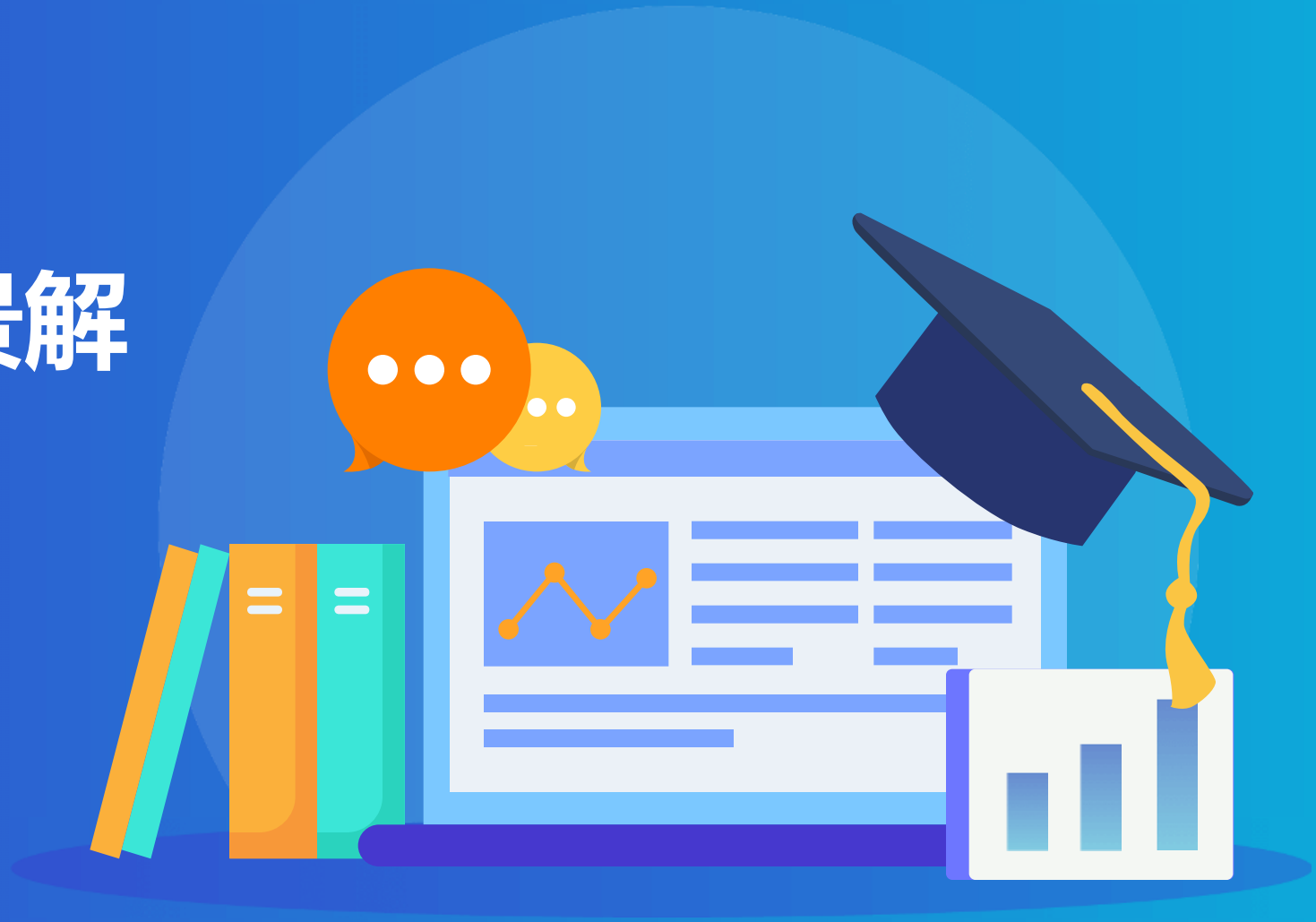
企业信息安全全景解析

从威胁识别到安全战略实施



Presenter name

Agenda

1. 信息安全威胁
2. 安全管理原则
3. 信息安全管理
4. 员工培训和意识
5. 评估信息安全现状
6. 安全管理挑战
7. 安全管理最佳实践
8. 信息安全策略
9. 投资信息安全

01.信息安全威胁

企业信息安全的威胁和风险

内部威胁

内部人员威胁

员工安全意识

员工对信息安全重要性认识不足，容易发生安全事故

员工离职带走数据

员工离职时携带敏感数据增加数据丢失风险

员工不当使用权限

员工滥用权限导致数据泄露风险增加

数据泄露

数据泄露的风险

员工操作失误

缺乏对敏感数据的正确处理意识

外部攻击

黑客入侵企业系统获取数据

内部泄露

员工故意或不慎泄露数据

网络攻击

网络攻击的类型

01 **黑客攻击**

通过入侵企业网络系统获取敏感数据

02 **恶意软件攻击**

利用恶意软件感染企业计算机系统

03 **社会工程攻击**

通过欺骗手段获取企业敏感信息

02.安全管理原则

信息安全管理的基本原则和流程

安全政策：保护数据

安全政策和控制措施

风险评估和管理

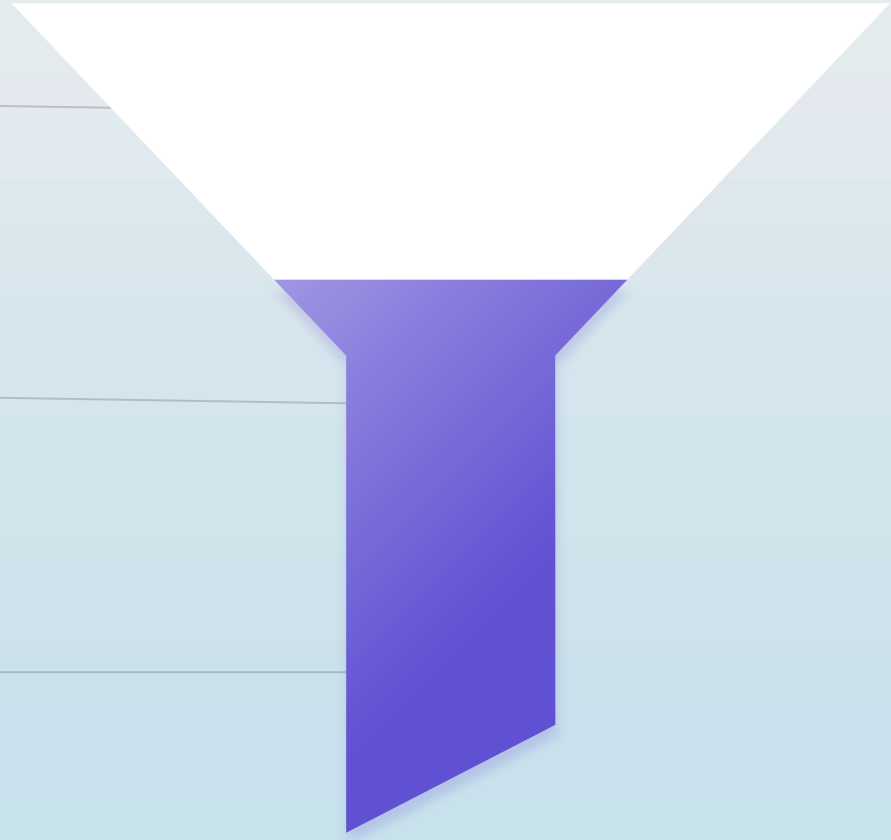
识别和减轻潜在风险

控制措施制定

保护企业敏感信息

建立安全政策

规范员工行为和责任



风险评估和风险管理：风险控制

风险评估和风险管理

风险评估的目的

确定信息安全威胁和潜在风险

风险管理的方法

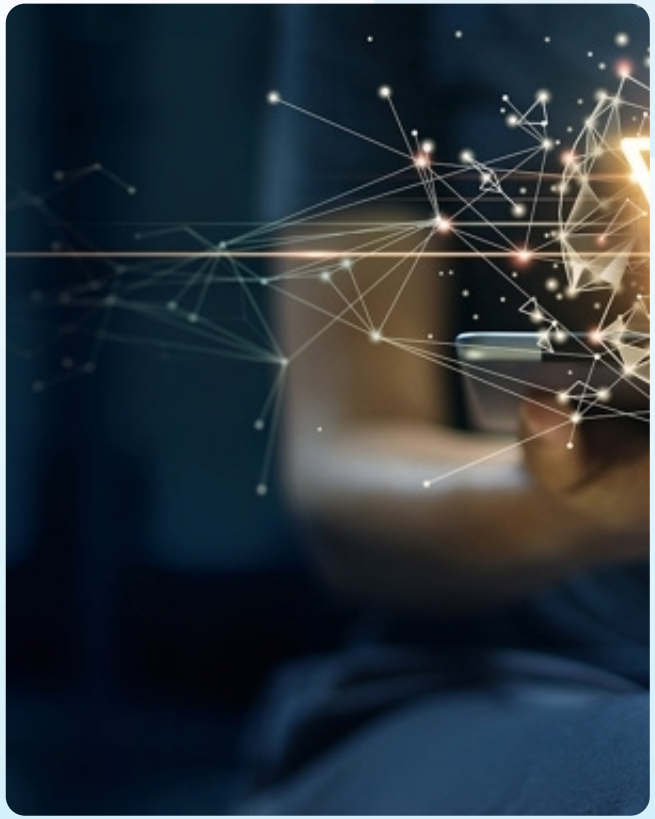
采取措施减轻和控制风险

风险评估的步骤

识别、分析、评估和优先处理风险

信息安全要求

信息安全管理原则



保密性

保护信息不被未授权访问或泄露。

完整性

保证信息的准确性和完整性，防止未经授权的修改或篡改

可用性

确保信息和系统可用，及时满足业务需求

03.信息安全管理

信息安全管理的基础

高层决策：支持网络安全

高层决策支持

建立信息安全文化

全员参与信息安全保护

分配足够资源

保障信息安全措施的实施

制定信息安全策略

明确信息安全目标和方向

长期战略

建立安全策略

明确信息安全目标，制定详细策略。

实施安全措施

采取必要的技术和管理措施来保护信息安全

推广安全意识

培养员工的安全意识，提高整体安全水平

信息安全管理的长期规划

全员参与和持续改进

全员参与

安全意识培训计划

提高员工对信息安全的认识和理解

定期评估

对企业信息安全措施进行定期检查和评估

持续改进

不断优化和完善信息安全管理体系

04.员工培训和意识

员工培训和信息安全文化

安全培训计划
加强培训效果

01
定期培训计划
确保员工持续接受信息安全培训

02
灵活的培训方式
结合在线培训和面对面培训

03
培训内容全面
包括网络安全、数据保护等方面

推广安全意识：全员参与

推广安全意识

加强培训计划

提供信息安全培训，包括网络安全知识和应对策略。

定期测试和评估

通过定期测试和评估员工的信息安全知识，发现并解决潜在的安全隐患

建立奖惩机制

设立奖励机制以激励员工积极参与信息安全，同时建立违规处罚制度

建立安全文化

信息安全文化的重要性

培养全员参与

所有员工都应参与信息安全工作

持续改进措施

不断优化安全策略和措施

推广安全意识

提高员工对信息安全的认知和警惕性

05.评估信息安全现状

企业信息安全现状评估和策略制定