

云计算及网络安全保险介绍

目录页

Contents Page



信息安全现状

—

风险防范实践

—
—

人保财险解决方案

—
—
—

PART
1

信息安全现状

网络安全事件频发

运维人员过失及系统故障不可避免

运维圈内有句话：70%故障来自内部人员的操作失误。



- 由于IT基础设施投资不足，遇到IT故障在所难免。
- 系统更新更迭过程，可能存在巨大的风险隐患。
- 硬件设备故障引发连锁效应，导致系统不可用。

网络风险趋势

信息泄露成为企业及个人网络安全的第一威胁



Facebook 爆出隐私泄露问题，为Cambridge Analytica在2016年美国总统大选前获得了5000万名Facebook用户的数据

万豪旗下喜达屋酒店5亿余消费者从2014年以来的消费数据，包括：姓名、电子邮箱、邮寄地址、电话号码、护照号码、账户信息、出生日期、性别、旅行信息、住宿信息、信用卡信息等。

华住酒店集团：泄露1.3亿消费者住宿及消费信息：卡号、姓名、手机号、邮箱、身份证号、登录密码、入住时间、离开时间、房间号、消费金额

网络安全事件频发



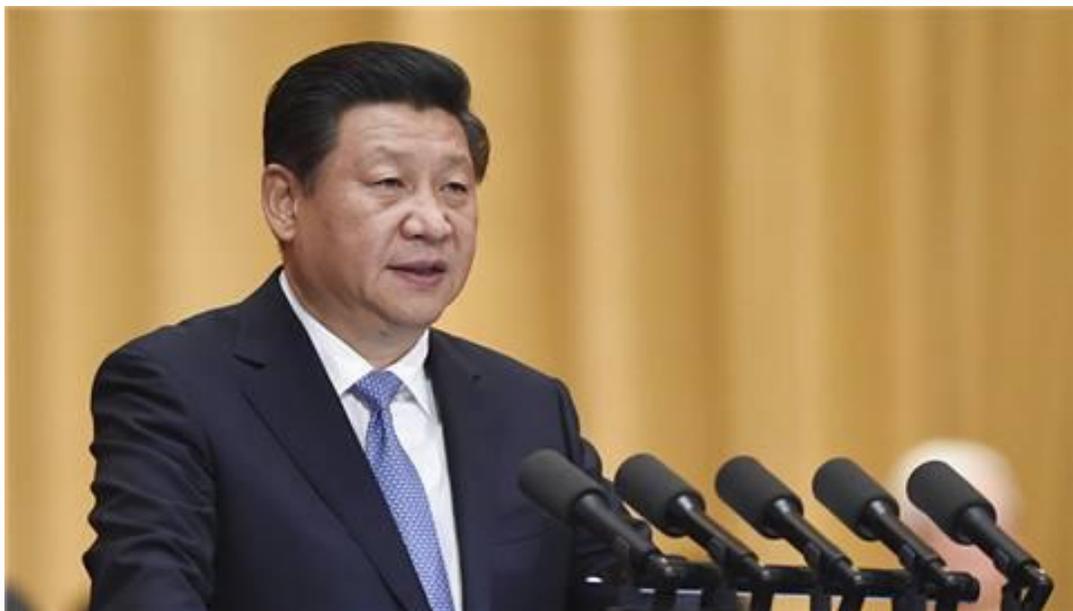
系统漏洞、网络勒索事件频发

2018年，波音生产工厂就曾遭到WannaCry勒索病毒的攻击，对部分生产设备造成了损害。波音在监测到恶意软件入侵后，第一时间停止了飞机组装，担心病毒由生产设备向飞机软件扩散。

云平台成为发生网络攻击的重灾区

根据某网络安全权威机构指出，在各类型网络安全事件数量中，云平台上的 DDoS 攻击次数、被植入后门的网站数量、被篡改网站数量均占比超过 50%。

法律环境



没有网络安全就没有国家安全，没有信息化就没有现代化。

-----习近平在中央网络安全和信息化领导小组第一次会议上讲话（2014年2月27日）

2017年6月1日，《中华人民共和国网络安全法》施行，网络安全法是为保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展制定。

《电子商务法》

《网络安全等级保护条例（征求意见稿）》

《关键信息基础设施安全保护条例》

《数据安全管理办法（征求意见稿）》

企业和个人重视网络安全

- **Gartner** 2018年，全球公司企业花在信息安全产品及服务上的开支将达1140亿美元，比去年增加12.4%。
- **2019年，信息安全市场规模预期再增8.7%，达1240亿美元。**

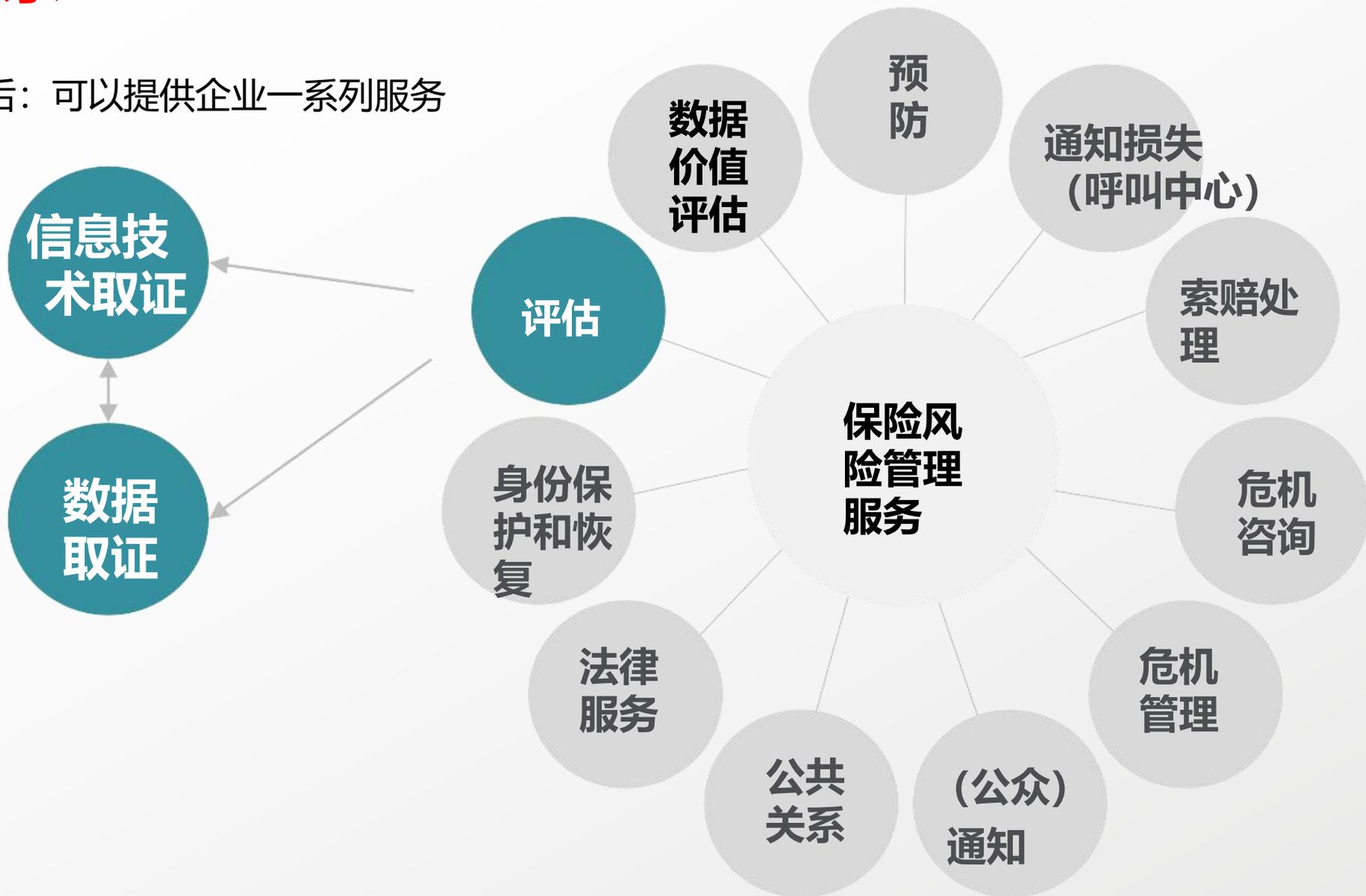
风险防范实践

PART
2



服务体系

事中与事后：可以提供企业一系列服务



网络安全风险减量管理

事前

风险管理
能力评估

对企业风险管理能力进行评估，客观梳理企业风险点和抵御风险能力。

事中

风险
防控

建立风险防控机制，通过系统监测、定期监测，做到风险早知道早预防。

事后

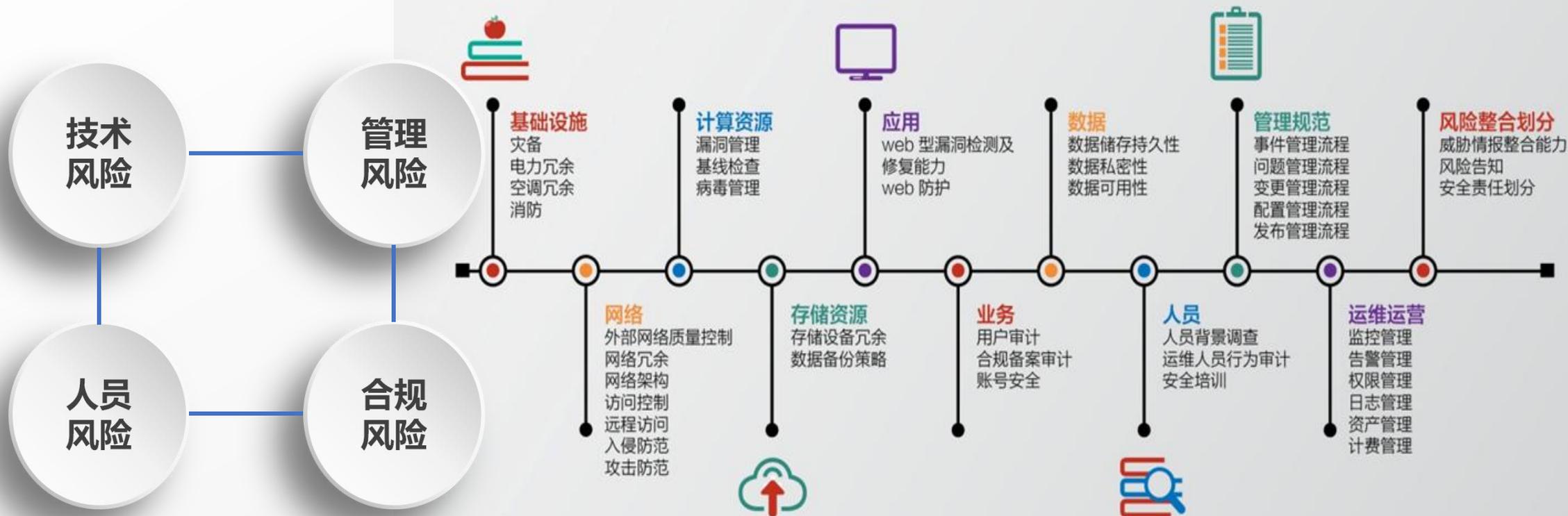
风险
转移

通过保险机制建立事后经济手段降低风险事故损失

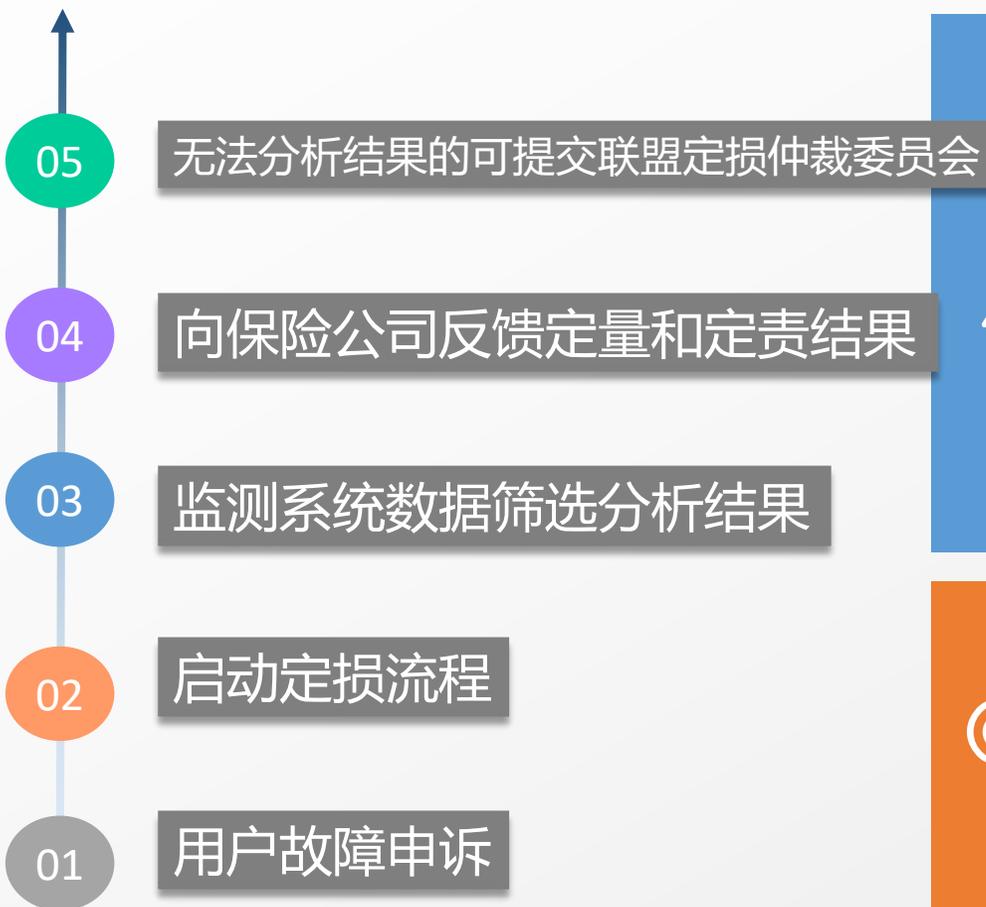
保险实践

事前：风险减量管理

- **标准依据：**《云计算风险管理框架》、《云计算风险评估方法》标准；
- **意义：**用于指导基于云计算相关企业进行有效的风险管理，控制服务不可用、数据丢失、信息泄露的风险事故。
- **完成企业：**中国电信、中国移动、联通云数据、百度云、Ucloud、讯达云、浪潮云、黑龙江移动、曙光云、睿江云等企业已完成首轮评估。



定损流程



出现风险事故由第三方提供技术支持排查问题

● 定量

- 服务状态
- 服务中断次数
- 服务中断时间
- 硬盘状态
- 采集Agent客户端，服务商提供数据接口或API

● 定责

- 堡垒机运维记录
- 只监测云服务商堡垒机最高权限管理员行为，保证堡垒机数据无修改



PART

3

保險保障信息安全

保险产品概述

外部
风险

自然环境风险

地震、火灾等自然灾害

第三方风险

电力、网络风险

网络攻击风险

DDos攻击
寄生式攻击

+

运营
系统
风险

风险

共享技术风险

迁移风险

接入风险

薄弱的证书、识别、接入管理
导致非法用户切入

物理设备风险

服务器、交换机等硬件故障

软件风险

系统软件、数据库软件等
bug风险

+

运营
主体
风险

商业风险

投资成本大

法律风险

用户隐私、知识产权方面法
律不够健全

操作风险

运维人员误操作
内部员工恶意破坏

保险产品概述

保险 责任

风险事故企业自身费用补偿

数据恢复费用
网络勒索
营业中断费用损失
危机管理费用
法律费用
数据丢失

风险事故企业责任保险保障

数据丢失
恶意软件;
黑客行为;
拒绝服务攻击;
非法使用或访问;
误操作;
设备故障。
侵犯他人著作权及相关

除外 责任

侵犯专利权或商业秘密

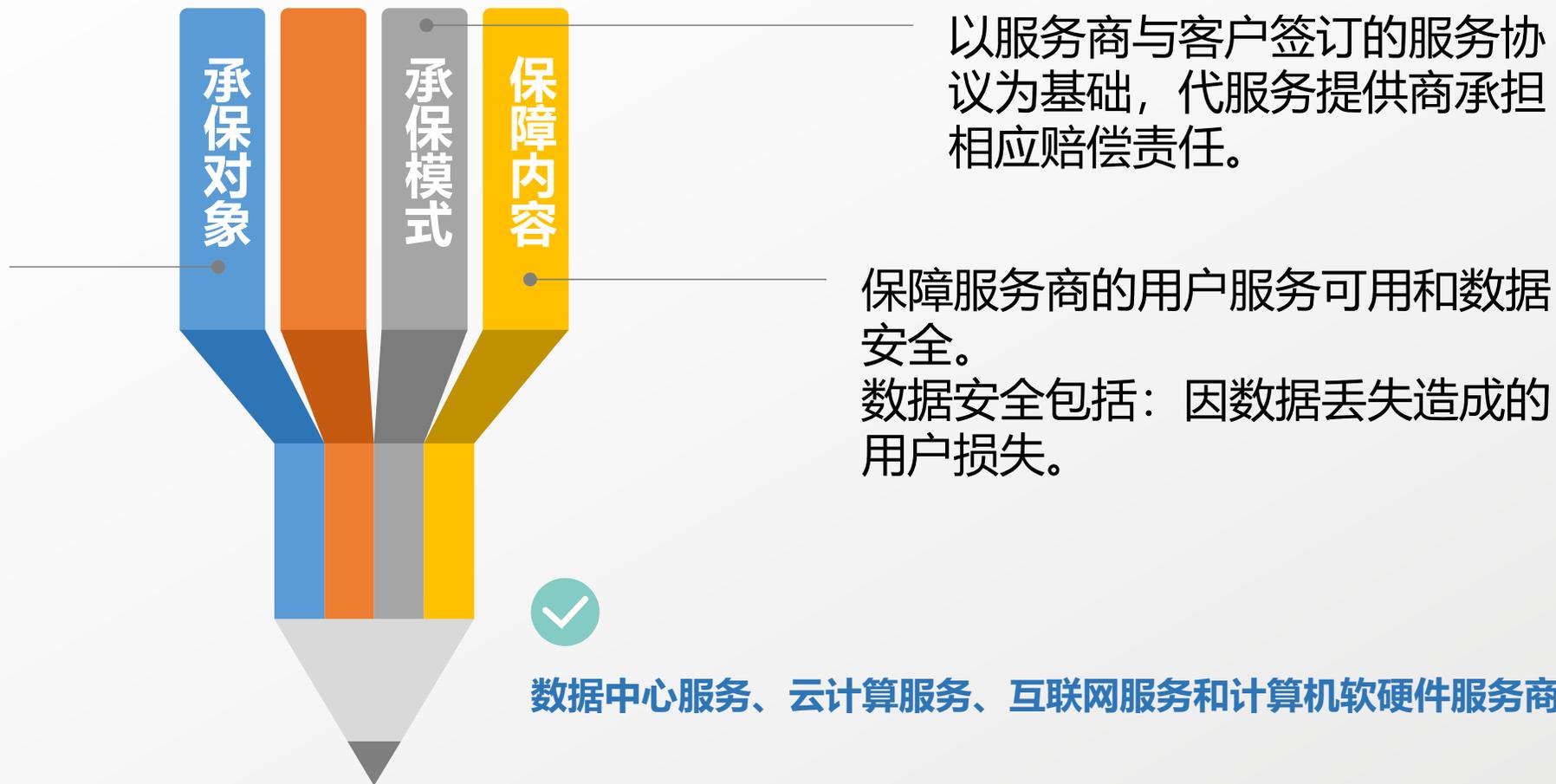
罚款、罚金及惩罚性赔偿;

被保险人的间接损失;

因设备故障、损坏发生的维修、更换费用;

关联企业之间提出的索赔申请

云计算服务商
(IaaS、PaaS、SaaS)



保障的责任范围

1

故障责任

被保险人软件故障；主机、存储等设备故障；自有网络、电力、空调等数据中心设备故障。

2

误操作责任

因其技术人员操作失误造成主机、存储、网络设备重启、关机，网络、软件配置变更等。

3

第三方责任

供电公司供电电力故障、电信运营商的网络中断、第三方数据中心电力故障或网络中断等

4

数据丢失责任

因被保险人存储设备损坏，数据无法恢复，导致委托人数据丢失

对原云计算服务责任保险进行升级，主要增加了黑客攻击、网络勒索等责任，扩展了被保险人范围。



第三者损失

- 恶意软件、黑客攻击、Ddos、非法使用、误操作、设备故障。



媒体责任： 在出版、发行或传播媒体内容时因下列疏忽或者过失行为导致第三者的财产损失。

- 包括：侵犯他人著作权、创意、名誉权等



外部服务商

- 经保险人认可的，基于服务协议或者法律规定代表被保险人收集或者处理数据信息的外部服务商发生保险事故造成第三者的财产损失。

保障对象

- 云保险2.0是企业自己给自己买的一份保障。
- 只要具备信息技术应用服务的企业，经过保险评估，都可以投保。
- 中国信息通信研究院为第三方平台企业进行风险评估。

保障内容

- 服务中断
- 信息安全：数据丢失和信息泄露

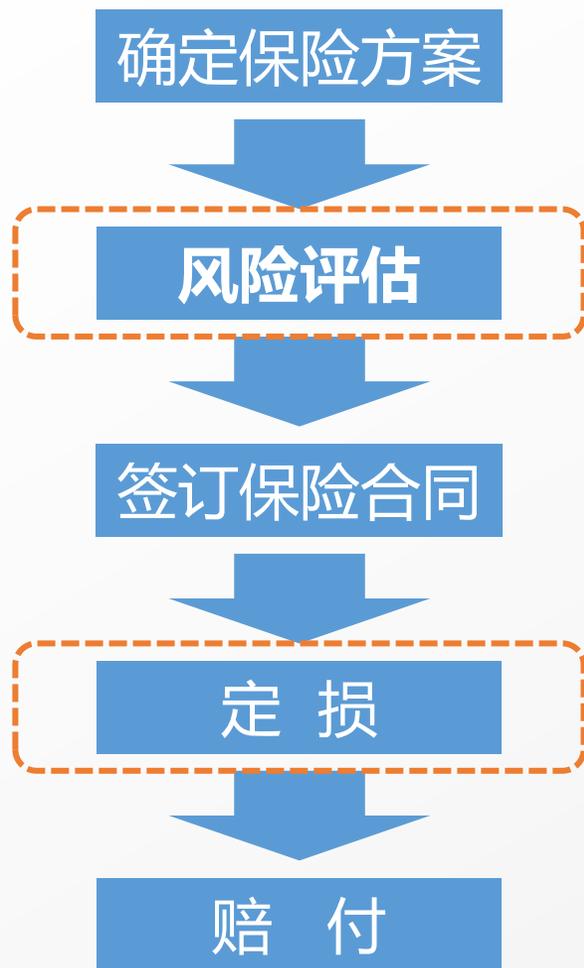


附加应急响应费用保险条款

被保险人为减少损失、确定事故原因、维护或者恢复名誉而支付的下列费用：

- 鉴定费用：聘请第三方机构确定保险事故发生原因和影响范围；
- 通知费用：为维护或恢复声誉，被保险人通过新闻或电视等大众媒体或者聘请第三者机构，说明事故发生状况、处理方式或表示歉意所需的通知费用；
- 监测费用：为用户提供信用监测、身份盗窃监测、社交媒体监测、信用冻结、欺诈预警服务或防欺诈软件所需的监测费用。

服务流程



对发生服务中断、数据丢失、黑客攻击等事故的概率的估算

在服务中断、数据丢失、黑客攻击等事故后，对责任和损失的确定过程



中国信息通信研究院

**保险将贯穿IT风险管理始终
帮助云服务商提升IT风险管理能力
客户选择云服务商的依据**

用客观数据中立地判断事故责任和损失界定，可以最大化保障用户和云企业的利益

谢谢

THANKS FOR YOUR ATTENTION